Rada
Evropské unie

Brusel 10. července 2026
(OR. en)

11772/26
ADD 1

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

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	1. července 2026
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	C(2026) 4534 annex
Předmět:	PŘÍLOHY NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) .../..., kterým se doplňuje směrnice (EU) 2024/2841, pokud jde o stanovení QR kódu pro fyzickou verzi evropského průkazu osoby se zdravotním postižením a stanovení QR kódu a zavedení společných technických specifikací pro zajištění bezpečnosti fyzické verze evropského parkovacího průkazu pro osoby se zdravotním postižením, jakož i o interoperabilitu

EVROPSKÁ
KOMISE

V Bruselu dne 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

PŘÍLOHY

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) .../...,

kterým se doplňuje směrnice (EU) 2024/2841, pokud jde o stanovení QR kódu pro fyzickou verzi evropského průkazu osoby se zdravotním postižením a stanovení QR kódu a zavedení společných technických specifikací pro zajištění bezpečnosti fyzické verze evropského parkovacího průkazu pro osoby se zdravotním postižením, jakož i o interoperabilitu

PŘÍLOHA I

SPECIFIKACE QR KÓDU PRO FYZICKOU VERZI EVROPSKÉHO PRŮKAZU OSOBY SE ZDRAVOTNÍM POSTIŽENÍM

1. **Formát QR kódu pro fyzickou verzi evropského průkazu osoby se zdravotním postižením**

a) **QR kód ve formátu Model 2** v souladu s mezinárodními specifikacemi QR kódu ISO/IEC 18004:2024 nebo rovnocennými specifikacemi.

b) **Korekce chyb na úrovni M** (15% redundance) zajišťující odolnost vůči poškrábání nebo částečnému poškození tištěného QR kódu.

c) **Režim kódování:** Datový obsah QR kódu sestává z kombinace struktury issuerSigned ve formátu Concise Binary Object Representation (CBOR) a odpovídajícího objektu podpisu issuerAuth ve formátu COSE_Sign1 definovaném v CBOR Object Signing and Encryption (COSE, RFC 9052, oddíly 3.1, 4.2 a 4.4), přičemž položky issuerSigned se řídí vzorem datového modelu mDOC, ale přizpůsobeným pro statické použití na fyzickém průkazu. Objekt issuerAuth je objekt COSE_Sign1 s alg = ES256 a chráněnou hlavičkou obsahující x5t (parametr hlavičky COSE pro hash certifikátu X.509 definovaný v RFC 9360 (oddíl 2); pro účely interoperability se jako hashovací algoritmus v x5t použije SHA-256).

d) Před kódováním do QR kódu se kombinovaný objekt CBOR/COSE **komprimuje s použitím formátu zlib** (RFC 1950, oddíl 2.2) a algoritmu **deflate** (RFC 1951, oddíly 3.2 a 4). Výsledné komprimované pole bajtů se kóduje v **bajtovém režimu QR kódu**, aby byla zajištěna plná podpora binárního datového obsahu CBOR/COSE a interoperabilita se skenery.

Ve všech textových polích zahrnutých do datového obsahu QR kódu vydavatelé kódují znaky jako Unicode UTF-8 v textových řetězcích CBOR. Na podepsané údaje v datovém obsahu se nepoužije transliterace. Pro účely interoperability použijí vydavatelé před podpisem pro všechna textová pole normalizaci Unicode Normalisation Form C (NFC).

e) **Předpona:** Řetězec QR kódu pro evropský průkaz osoby se zdravotním postižením začíná předponou „ED1:MDOC:“, která identifikuje typ průkazu a kódovací profil. Předpony musí být přítomny a rozlišují se v nich malá a velká písmena. Neznámé nebo nepodporované předpony vedou k odmítnutí. Předpona a komprimovaný datový obsah se v QR kódu kódují v bajtovém režimu jako jeden datový segment.

f) **Minimální velikost modulu ≥ 0,25 mm** k zajištění čitelnosti na tištěných průkazech.

g) **Maximální verze 20**; nejvýše 97 × 97 modulů na každé straně.

2. **Specifikace generování podpisu pro evropský průkaz osoby se zdravotním postižením**

Kvalifikovaná elektronická pečeť (QSeal) používaná k pečetění QR kódů pro evropské průkazy osoby se zdravotním postižením zajišťuje, že zakódované údaje pocházejí od oprávněného vydávajícího orgánu a nebyly změněny.

a) **Algoritmus podpisu**: Algoritmem podpisu je ES256 (Elliptic Curve Digital Signature Algorithm, ECDSA) s SHA-256 a křivkou P-256), jak je definován v RFC

9053 (oddíl 2.1); v COSE je algoritmus určen parametrem hlavičky alg v RFC 9052 (oddíl 3.1).

b) **Podpisový klíč**: Datový obsah QR kódu se podepisuje pomocí soukromého klíče odpovídajícího kvalifikovanému certifikátu pro elektronickou pečeť (QSealC).

c) **Struktura COSE**: Kontejner s podpisem je objekt COSE_Sign1. Chráněná hlavička obsahuje alg (ES256) a x5t (parametr hlavičky COSE pro hash certifikátu X.509 definovaný v RFC 9360 (oddíl 2); pro účely interoperability se jako hashovací algoritmus v x5t použije SHA-256). Ověření spočívá v použití hodnoty x5t k nalezení příslušného certifikátu v místní mezipaměti úložiště důvěry ověřovatele vytvořeného na základě informací z důvěryhodného seznamu a následné validaci řetězce certifikátů a stavu certifikátu v souladu s rámcem pro důvěryhodnost podle nařízení eIDAS.

d) **Standard podpisu**: Datový obsah QR kódu se podepisuje jako objekt COSE_Sign1 v souladu s RFC 9052 (oddíl 4), CBOR Object Signing and Encryption. Objekt COSE_Sign1 je obsažen v issuerAuth a kódován bez tagu CBOR pro COSE_Sign1. Pole datového obsahu objektu COSE_Sign1 se oddělí a kóduje jako CBOR null. Pro generování a ověření podpisu je externím datovým obsahem deterministická struktura kódovaná jako CBOR a obsahující hodnotu docType a hodnotu issuerSigned z mapy CBOR nejvyšší úrovně.

e) **Hashovací algoritmus**: Pro generování podpisu a ověření integrity se jako součást ES256 použije SHA-256.

f) **Kódování**: Datový obsah se kóduje pomocí CBOR (RFC 8949, oddíl 4.2), jak vyžadují specifikace COSE a mDOC, čímž se zajistí kódování a reprodukovatelnost podepsaných údajů.

3. **Specifikace pro tisk**

a) **Ochranná zóna**: Kolem QR kódu musí být na všech stranách volný okraj o šířce **čtyř modulů** bez jakéhokoli tisku, vzoru nebo pozadí.

b) **Kontrast**: QR kód musí být vytištěn na bílém pozadí s minimálním kontrastním poměrem **4:1**, aby byla zajištěna vysoká čitelnost za různých světelných podmínek.

c) Pro tisk QR kódu se použije barva definovaná v příloze I směrnice (EU) 2024/2841, která zajišťuje maximální kontrast.

d) **Umístění a velikost**: QR kód včetně ochranné zóny musí mít rozměry 26,25 mm × 26,25 mm a být umístěn na zadní straně průkazu v pravém dolním rohu. Verze QR kódu je maximálně 20 (97 × 97 modulů) s velikostí modulu 0,25 mm nebo větší.

QR kód včetně ochranné zóny musí být umístěn alespoň 5 mm od pravého okraje a alespoň 5 mm od spodního okraje průkazu.

4. **Údaje v QR kódu pro evropský průkaz osoby se zdravotním postižením**

V souladu se zásadou minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 obsahuje QR kód minimální datový soubor, který je ověřitelný off-line. Struktura datového obsahu:

a) Atributy průkazu jsou kódovány ve formátu CBOR v objektu issuerSigned.

b) Struktura je zabalena a podepsána pomocí pečetě QSeal vydávajícího orgánu jako issuerAuth (COSE_Sign1, ES256, včetně x5t – parametru hlavičky COSE pro hash certifikátu X.509).

c) Výsledný objekt CBOR/COSE se komprimuje v souladu s bodem 1 písm. d) této přílohy. Datový obsah QR kódu sestává z předpony „ED1:MDOC:“, za níž následuje výsledné komprimované pole bajtů, a celý datový obsah se kóduje v bajtovém režimu jako jediný datový segment QR kódu.

Datový obsah sestává z podmnožiny viditelných údajů z polí na přední straně průkazu uvedených v příloze I směrnice (EU) 2024/2841 (jméno, příjmení, sériové číslo průkazu, datum skončení platnosti) spolu s identifikátorem zneplatnění, elektronickým podpisem a informací o schématu.

Elektronický podpis musí obsahovat:

i) issuerAuth – objekt COSE_Sign1 podepsaný pomocí **soukromého klíče QSealC** vydávajícího orgánu;

ii) chráněnou hlavičku zahrnující alg = ES256 (algoritmus podpisu) a x5t (parametr hlavičky COSE pro hash certifikátu X.509).

5. Nepovinné údaje

QR kód neobsahuje žádné nepovinné údaje.

6. Identifikátor zneplatnění (RID)

Kromě viditelného sériového čísla průkazu musí QR kód obsahovat vyhrazený identifikátor zneplatnění (RID).

RID se použije k určení stavu zneplatnění a ke správě seznamu zneplatněných průkazů. RID není na průkazu vytištěn a ověřovatelům průkazu se nezobrazí.

6.1. *Požadavky na RID*

RID:

a) musí být zahrnutý do podepsaného datového obsahu QR kódu;

b) musí být jedinečný alespoň v rámci oblasti vydávání vydávajícího orgánu;

c) nesmí být na průkazu vytištěn a není určen k tomu, aby byl čitelný člověkem;

d) nesmí odhalovat osobní údaje a být přímo smysluplný;

e) nesmí být přímo odvoditelný z viditelného sériového čísla průkazu a

f) musí být kryptograficky svázán s datovým obsahem QR kódu pomocí kvalifikované elektronické pečeti.

6.2. *Formát a velikost RID*

RID se kóduje jako řetězec bajtů CBOR (bstr). Délka RID činí 16 bajtů (128 bitů).

RID je generován vydávajícím orgánem za použití metody pod jeho kontrolou, která zajišťuje dostatečnou entropii a odolnost vůči uhodnutí nebo enumeraci.

6.3. *Seznamy zneplatněných průkazů*

Seznamy zneplatněných průkazů zveřejněné pro účely ověřování musí odkazovat pouze na RID zneplatněných průkazů. Sériová čísla průkazů se v seznamech zneplatněných průkazů nezveřejňují.

7. Datový obsah CBOR (uvnitř QR kódu) evropského průkazu osoby se zdravotním postižením

Do datového obsahu QR kódu se zahrnou pouze následující údaje, které jsou v souladu s viditelnými datovými poli evropského průkazu osoby se zdravotním postižením stanovenými v příloze I směrnice (EU) 2024/2841:

Obsah nejvyšší úrovně:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" s atributy uvedenými v tabulce níže

c) issuerAuth = COSE_Sign1 (QSeal)

Pole	**Cesta mDOC**	**Typ/formát**
Verze datového schématu	issuerSigned.nameSpaces."eu.edc".ver	Řetězec (např. "1.0")
Typ průkazu: evropský průkaz osoby se zdravotním postižením	docType	Enum ("eu.edc")
Sériové číslo průkazu	issuerSigned.nameSpaces."eu.edc".sub	Řetězec
Identifikátor zneplatnění	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bajtů)
Jméno držitele průkazu	issuerSigned.nameSpaces."eu.edc".givenName	Textový řetězec Unicode (UTF-8)
Příjmení držitele průkazu	issuerSigned.nameSpaces."eu.edc".familyName	Textový řetězec Unicode (UTF-8)
Datum skončení platnosti	issuerSigned.nameSpaces."eu.edc".exp	Tag CBOR 1004, jak je definován v RFC 8943 (oddíl 2.1),

průkazu		obsahující textový řetězec UTF-8 představující úplné datum podle RFC 3339 ve formátu RRRR-MM-DD

Elektronický podpis je obsažen v issuerAuth (objekt COSE_Sign1). Řetězec certifikátů není do datového obsahu QR kódu začleněn; namísto toho musí chráněná hlavička COSE obsahovat x5t, otisk certifikátu umožňující nalézt příslušnou pečeť QSealC v mezipaměti úložiště důvěry ověřovatele.

8. **Příklad datového obsahu QR kódu na evropském průkazu osoby se zdravotním postižením: logická reprezentace ve stylu JSON s komentáři**

Následující příklad představuje logický náhled na evropský průkaz osoby se zdravotním postižením v člověkem čitelné reprezentaci JSON (JavaScript Object Notation). V praxi není tato struktura čitelná člověkem, neboť musí:

a) být zakódovaná v CBOR (RFC 8949, oddíl 3);

b) být podepsaná pomocí netagované struktury COSE_Sign1 s odděleným datovým obsahem (RFC 9052, oddíl 4);

c) zahrnovat datum skončení platnosti jako tag CBOR 1004 s úplným datem v souladu s RFC 8943 (oddíl 2.1);

d) zahrnovat parametr chráněné hlavičky x5t v souladu s RFC 9360, s použitím SHA-256 na pečeť QSealC koncového subjektu kódovanou ve formátu DER a

e) být komprimovaná a opatřená předponou s řetězcem ED1:MDOC: před zakódováním do QR kódu.

```
{
 // Pouze člověkem čitelný logický náhled na EDC ve stylu JSON.
 // Skutečný datový obsah QR kódu je deterministický CBOR, nikoli JSON.
 "docType": "eu.edc", // doklad EDC. Hodnota docType je zahrnuta spolu s
  // issuerSigned v externím datovém obsahu COSE_Sign1.

 "issuerSigned": {
  // Údaje chráněné issuerAuth; použité jako oddělený datový obsah.
  // Pro generování a ověření podpisu zahrnuje oddělený externí datový obsah
  // docType i issuerSigned.
  "nameSpaces": {
   "eu.edc": {
    "ver": "1.0", // Verze QR profilu / schématu

    // Sériové číslo průkazu; definované vydavatelem, maximálně 24 znaků.
    "sub": "AB123456789012345678 90CD",
```

```
      // Identifikátor zneplatnění: ve skutečnosti CBOR bstr, 16 bajtů / 128 bitů.
      // Zde uveden jako 32 hexadecimálních znaků kvůli čitelnosti.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Anna",    // jméno vytištěné na EDC
      "familyName": "Nováková", // příjmení vytištěné na EDC

      // Skutečné kódování CBOR používá tag 1004 pro úplné datum podle RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Skutečná forma: netagovaný COSE_Sign1, nikoli objekt JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // kódováno bez tagu CBOR COSE_Sign1
  "payload": "detached", // pole datového obsahu COSE je CBOR null

  "protectedHeader": {
    // alg: ES256; ekvivalentní parametr hlavičky COSE 1 = –7.
    "alg": "ES256",

    // x5t: otisk certifikátu; parametr hlavičky COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // ekvivalentní hodnota hashe COSE –16
```

```
        // hash SHA-256 pečeti QSealC koncového subjektu kódované v DER.
        // 32 bajtů reprezentovaných jako 64 hexadecimálních znaků.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // v tomto příkladu prázdná

    // podpis COSE ES256: 64 bajtů = 128 hexadecimálních znaků.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. Používání kryptografických mechanismů

Používání kryptografických mechanismů v kontextu této přílohy musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

PŘÍLOHA II

SPECIFIKACE QR KÓDU PRO FYZICKOU VERZI EVROPSKÉHO PARKOVACÍHO PRŮKAZU PRO OSOBY SE ZDRAVOTNÍM POSTIŽENÍM

1. **Formát QR kódu pro fyzickou verzi evropského parkovacího průkazu pro osoby se zdravotním postižením**

a) **QR kód ve formátu Model 2** v souladu s mezinárodními specifikacemi QR kódu ISO/IEC 18004:2024 nebo rovnocennými specifikacemi.

b) **Korekce chyb na úrovni M** (15% redundance) zajišťující odolnost vůči poškrábání nebo částečnému poškození tištěného QR kódu.

c) **Režim kódování:** Datový obsah QR kódu sestává z kombinace struktury issuerSigned ve formátu Concise Binary Object Representation (CBOR) a odpovídajícího objektu podpisu issuerAuth ve formátu COSE_Sign1 definovaném v CBOR Object Signing and Encryption (COSE, RFC 9052, oddíly 3.1, 4.2 a 4.4), přičemž položky issuerSigned se řídí vzorem datového modelu mDOC, ale přizpůsobeným pro statické použití na fyzickém průkazu. Objekt issuerAuth je objekt COSE_Sign1 s alg = ES256 a chráněnou hlavičkou obsahující x5t (parametr hlavičky COSE pro hash certifikátu X.509 definovaný v RFC 9360 (oddíl 2); pro účely interoperability se jako hashovací algoritmus v x5t použije SHA-256).

d) Před kódováním do QR kódu se kombinovaný objekt CBOR/COSE **komprimuje s použitím formátu zlib (RFC 1950, oddíl 2.2) a algoritmu deflate** (RFC 1951, oddíly 3.2 a 4). Výsledné komprimované pole bajtů se kóduje v **bajtovém režimu QR kódu**, aby byla zajištěna plná podpora binárního datového obsahu CBOR/COSE a interoperabilita se skenery.

Ve všech textových polích zahrnutých do datového obsahu QR kódu vydavatelé kódují znaky jako Unicode UTF-8 v textových řetězcích CBOR. Na podepsané údaje v datovém obsahu se nepoužije transliterace. Pro účely interoperability použijí vydavatelé před podpisem pro všechna textová pole normalizaci Unicode Normalisation Form C (NFC).

e) **Předpona**: Řetězec QR kódu pro evropský parkovací průkaz pro osoby se zdravotním postižením začíná předponou „EP1:MDOC:“, která identifikuje typ průkazu a kódovací profil. Předpony musí být přítomny a rozlišují se v nich malá a velká písmena. Neznámé nebo nepodporované předpony vedou k odmítnutí. Předpona a komprimovaný datový obsah se v QR kódu kódují v bajtovém režimu jako jeden datový segment.

f) **Minimální velikost modulu ≥ 0,35 mm** k zajištění čitelnosti na tištěných průkazech.

g) **Maximální verze 20**; nejvýše 97 × 97 modulů na každé straně.

2. **Specifikace generování podpisu pro evropský parkovací průkaz pro osoby se zdravotním postižením**

Kvalifikovaná elektronická pečeť (QSeal) používaná k pečetění QR kódů pro evropské parkovací průkazy pro osoby se zdravotním postižením zajišťuje, že zakódované údaje pocházejí od oprávněného vydávajícího orgánu a nebyly změněny.

a) **Algoritmus podpisu**: Algoritmem podpisu je ES256 (ECDSA s SHA-256 a křivkou P-256), jak je definován v RFC 9053 (oddíl 2.1); v COSE je algoritmus určen parametrem hlavičky alg v RFC 9052 (oddíl 3.1).

b) **Podpisový klíč**: Datový obsah QR kódu se podepisuje pomocí soukromého klíče odpovídajícího kvalifikovanému certifikátu pro elektronickou pečeť (QSealC).

c) **Struktura COSE**: Kontejner s podpisem je objekt COSE_Sign1. Chráněná hlavička obsahuje alg (ES256) a x5t (parametr hlavičky COSE pro hash certifikátu X.509 definovaný v RFC 9360 (oddíl 2); pro účely interoperability se jako hashovací algoritmus v x5t použije SHA-256). Ověření spočívá v použití hodnoty x5t k nalezení příslušného certifikátu v místní mezipaměti úložiště důvěry ověřovatele vytvořeného na základě informací z důvěryhodného seznamu a následné validaci řetězce certifikátů a stavu certifikátu v souladu s rámcem pro důvěryhodnost podle nařízení eIDAS.

d) **Standard podpisu**: Datový obsah QR kódu se podepisuje jako objekt COSE_Sign1 v souladu s RFC 9052 (oddíl 4), CBOR Object Signing and Encryption. Objekt COSE_Sign1 je obsažen v issuerAuth a kódován bez tagu CBOR pro COSE_Sign1. Pole datového obsahu objektu COSE_Sign1 se oddělí a kóduje jako CBOR null. Pro generování a ověření podpisu je externím datovým obsahem deterministická struktura CBOR kódovaná jako CBOR a obsahující hodnotu docType a hodnotu issuerSigned z mapy CBOR nejvyšší úrovně.

e) **Hashovací algoritmus**: Pro generování podpisu a ověření integrity se jako součást ES256 použije SHA-256.

f) **Kódování**: Datový obsah se kóduje pomocí CBOR (RFC 8949, oddíl 4.2), jak vyžadují specifikace COSE a mDOC, čímž se zajistí kódování a reprodukovatelnost podepsaných údajů.

3. **Specifikace pro tisk**

a) **Ochranná zóna**: Kolem QR kódu musí být na všech stranách volný okraj o šířce **čtyř modulů** bez jakéhokoli tisku, vzoru nebo pozadí.

b) **Kontrast**: QR kód musí být vytištěn na bílém pozadí s minimálním kontrastním poměrem **4:1**, aby byla zajištěna vysoká čitelnost za různých světelných podmínek.

c) Pro tisk QR kódu se použije barva definovaná v příloze II směrnice (EU) 2024/2841, která zajišťuje maximální kontrast.

d) **Umístění a velikost:** QR kód včetně ochranné zóny musí mít rozměry **37 mm** × **37 mm** a být umístěn na přední straně průkazu mírně napravo od středu směrem ke spodnímu okraji. Verze QR kódu je maximálně 20 (97 × 97 modulů) s velikostí modulu 0,35 mm nebo větší.

QR kód včetně ochranné zóny musí být umístěn alespoň 5 mm od spodního okraje průkazu.

4. **Údaje v QR kódu pro evropský parkovací průkaz pro osoby se zdravotním postižením**

V souladu se zásadou minimalizace údajů stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 obsahuje QR kód minimální datový soubor, který je ověřitelný off-line. Struktura datového obsahu:

a) Atributy průkazu jsou kódovány ve formátu CBOR v objektu issuerSigned.

b) Struktura je zabalena a podepsána pomocí pečetě QSeal vydávajícího orgánu jako issuerAuth (COSE_Sign1, ES256, včetně x5t – parametru hlavičky COSE pro hash certifikátu X.509).

c) Výsledný objekt CBOR/COSE se komprimuje v souladu s bodem 1 písm. d) této přílohy. Datový obsah QR kódu sestává z předpony „EP1:MDOC:“, za níž následuje výsledné komprimované pole bajtů, a úplný datový obsah se kóduje v bajtovém režimu jako jediný datový segment QR kódu.

Datový obsah sestává z podmnožiny viditelných údajů z polí na přední straně průkazu uvedených v příloze II směrnice (EU) 2024/2841 (datum skončení platnosti, sériové číslo průkazu) spolu s identifikátorem zneplatnění, elektronickým podpisem a informací o schématu.

Elektronický podpis musí obsahovat:

i) issuerAuth – objekt COSE_Sign1 podepsaný pomocí **soukromého klíče QSealC** vydávajícího orgánu;

ii) chráněnou hlavičku zahrnující alg = ES256 (algoritmus podpisu) a x5t (parametr hlavičky COSE pro hash certifikátu X.509).

5. Nepovinné údaje

QR kód neobsahuje žádné nepovinné údaje.

6. Identifikátor zneplatnění (RID)

Identifikátor zneplatnění evropského parkovacího průkazu pro osoby se zdravotním postižením musí být v souladu s bodem 6 přílohy I.

Seznamy zneplatněných průkazů musí odkazovat pouze na RID. Sériová čísla průkazů se v seznamech zneplatněných průkazů nezveřejňují.

7. Datový obsah CBOR (uvnitř QR kódu) evropského parkovacího průkazu pro osoby se zdravotním postižením

Do datového obsahu QR kódu se zahrnou pouze následující údaje, které jsou v souladu s viditelnými poli evropského parkovacího průkazu pro osoby se zdravotním postižením stanovenými v příloze II směrnice (EU) 2024/2841.

Pole	**Cesta mDOC**	**Typ/formát**
Verze datového schématu	issuerSigned.nameSpaces."eu.epc".ver	Řetězec (např. "1.0")
Typ průkazu: evropský	docType	Enum ("eu.epc")

parkovací průkaz pro osoby se zdravotním postižením		
Sériové číslo průkazu	issuerSigned.nameSpaces."eu.epc".sub	Řetězec
Identifikátor zneplatnění	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bajtů)
Datum skončení platnosti průkazu	issuerSigned.nameSpaces."eu.epc".exp	Tag CBOR 1004, jak je definován v RFC 8943 (oddíl 2.1), obsahující textový řetězec UTF-8 představující úplné datum podle RFC 3339 ve formátu RRRR-MM-DD

Elektronický podpis je obsažen v issuerAuth (objekt COSE_Sign1). Řetězec certifikátů není do datového obsahu QR kódu začleněn; namísto toho musí chráněná hlavička COSE obsahovat x5t, otisk certifikátu umožňující nalézt příslušnou pečeť QSealC v mezipaměti úložiště důvěry ověřovatele.

8. Příklad datového obsahu QR kódu na evropském parkovacím průkazu pro osoby se zdravotním postižením: logická reprezentace ve stylu JSON s komentáři

Následující příklad představuje logický náhled na evropský parkovací průkaz pro osoby se zdravotním postižením v člověkem čitelné reprezentaci JSON (JavaScript Object Notation). V praxi není tato struktura čitelná člověkem, neboť musí:

a) být zakódovaná v CBOR (RFC 8949, oddíl 3);

b) být podepsaná pomocí netagované struktury COSE_Sign1 s odděleným datovým obsahem (RFC 9052, oddíl 4);

c) zahrnovat datum skončení platnosti jako tag CBOR 1004 s úplným datem v souladu s RFC 8943 (oddíl 2.1);

d) zahrnovat parametr chráněné hlavičky x5t v souladu s RFC 9360, s použitím SHA-256 na pečeť QSealC koncového subjektu kódovanou ve formátu DER a

e) být komprimovaná a opatřená předponou s řetězcem EP1:MDOC: před zakódováním do QR kódu.

```
{
 // Pouze člověkem čitelný logický náhled na EPC ve stylu JSON.
 // Skutečný datový obsah QR kódu je deterministický CBOR, nikoli JSON.
 "docType": "eu.epc", // doklad EPC. Hodnota docType je zahrnuta spolu s
  // issuerSigned v externím datovém obsahu COSE_Sign1.

 "issuerSigned": {
  // Údaje chráněné issuerAuth; použité jako oddělený datový obsah.
// Pro generování a ověření podpisu zahrnuje oddělený externí datový obsah
  // docType i issuerSigned.
  "nameSpaces": {
   "eu.epc": {
    "ver": "1.0", // Verze QR profilu / schématu

    // Sériové číslo průkazu; definované vydavatelem, maximálně 24 znaků.
    "sub": "EF123456789012345678 90GH",

    // Identifikátor zneplatnění: ve skutečnosti CBOR bstr, 16 bajtů / 128 bitů.
    // Zde uveden jako 32 hexadecimálních znaků kvůli čitelnosti.
    "rid": "4a8d9c112233445566778899aabbccdd",

    // Skutečné kódování CBOR používá tag 1004 pro úplné datum podle RFC 3339.
    "exp": "2030-12-31"
   }
  }
```

```
  },

  "issuerAuth": {
    // Skutečná forma: netagovaný COSE_Sign1, nikoli objekt JSON.
    "type": "COSE_Sign1",
    "tagged": false,       // kódováno bez tagu CBOR COSE_Sign1
    "payload": "detached", // pole datového obsahu COSE je CBOR null

    "protectedHeader": {
      // alg: ES256; ekvivalentní parametr hlavičky COSE 1 = –7.
      "alg": "ES256",

      // x5t: otisk certifikátu; parametr hlavičky COSE 34.
      "x5t": {
        "hashAlg": "SHA-256", // ekvivalentní hodnota hashe COSE –16

        // hash SHA-256 pečeti QSealC koncového subjektu kódované v DER.
        // 32 bajtů reprezentovaných jako 64 hexadecimálních znaků.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // v tomto příkladu prázdná

    // podpis COSE ES256: 64 bajtů = 128 hexadecimálních znaků.
```

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Používání kryptografických mechanismů

Používání kryptografických mechanismů v kontextu této přílohy musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

PŘÍLOHA III

OZNAMOVÁNÍ INFORMACÍ UVEDENÝCH V ČL. 6 ODST. 2

1. Členské státy poskytnou Komisi o každém příslušném orgánu nebo subjektu odpovědném za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením tyto informace:

   a) název příslušného orgánu nebo subjektu odpovědného za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením;

   b) registrační číslo příslušného orgánu nebo subjektu odpovědného za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením;

   c) kontaktní e-mailovou adresu a telefonní číslo příslušného orgánu nebo subjektu odpovědného za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením;

   d) jeden nebo více certifikátů, které lze použít k ověření elektronické pečeti vytvořené příslušným orgánem nebo subjektem odpovědným za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením, které vydává, a u nichž certifikované identifikační údaje obsahují název a registrační číslo vydavatele, jak je uvedeno v písmenech a) a b);

   e) URL místa, kde vydavatel zveřejňuje informace o stavu platnosti fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením.

2. Členské státy mohou Komisi poskytnout o každém příslušném orgánu nebo subjektu odpovědném za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením tyto informace:

   a) URL internetové stránky, která obsahuje informace o politikách a podmínkách příslušného orgánu nebo subjektu odpovědného za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením, které se vztahují na poskytování a používání fyzických verzí evropského průkazu osoby se zdravotním postižením a evropského parkovacího průkazu pro osoby se zdravotním postižením, které tento orgán nebo subjekt poskytuje;

   b) v relevantních případech URL internetové stránky, která obsahuje doplňující informace o příslušném orgánu nebo subjektu odpovědném za vydávání fyzických verzí evropského průkazu osoby se zdravotním postižením nebo evropského parkovacího průkazu pro osoby se zdravotním postižením.

PŘÍLOHA IV

TECHNICKÉ SPECIFIKACE SEZNAMU ZNEPLATNĚNÝCH FYZICKÝCH VERZÍ EVROPSKÉHO PRŮKAZU OSOBY SE ZDRAVOTNÍM POSTIŽENÍM NEBO EVROPSKÉHO PARKOVACÍHO PRŮKAZU PRO OSOBY SE ZDRAVOTNÍM POSTIŽENÍM

1. Pro účely této přílohy musí identifikátor odpovídat identifikátoru zneplatnění (RID) vymezenému v bodě 6 přílohy I a v bodě 6 přílohy II.

2. Seznam zneplatněných průkazů je implementován jako token se seznamem identifikátorů ve formátu CWT (RFC 8392, oddíl 7) v souladu s bodem 5.2 specifikace seznamu stavů tokenů (draft-ietf-oauth-status-list-14) s těmito změnami:

   a) hodnota tvrzení o typu je „application/identifierlist+cwt“;

   b) musí být uvedeno tvrzení o době skončení platnosti;

   c) tvrzení StatusList nesmí být uvedeno v souboru tvrzení CWT;

   d) struktura IdentifierList definovaná v bodě 3 musí být uvedena jako tvrzení v souboru tvrzení CWT s použitím klíče 65530;

   e) CWT je objekt COSE_Sign1 používající k výpočtu podpisu algoritmus podpisu, který je v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA);

   f) CWT obsahuje v chráněné hlavičce parametr x5chain, definovaný v RFC 9360 (oddíl 2), který obsahuje certifikát nebo řetězec certifikátů pro ověření podpisu seznamu zneplatněných průkazů;

   g) pro podpisový certifikát seznamu identifikátorů lze použít identifikátor OID rozšíření „Extended Key Usage“ uvedený ve specifikaci seznamu stavů tokenů (draft-ietf-oauth-status-list-14) a doporučuje se, aby ověřovatelé podporovali OID rozšíření „Extended Key Usage“ uvedený ve specifikaci seznamu stavů tokenů a aby infrastruktury vydávajícího orgánu při používání OID rozšíření „Extended Key Usage“ uvedeného ve specifikaci seznamu stavů tokenů neučinili pole „Extended Key Usage“ kritickým.

3. Struktura IdentifierList je strukturou CBOR s následujícím CDDL (Concise Data Definition Language):

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

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

Identifier = bstr

Aggregation_uri = tstr