Rada
Unii Europejskiej

Bruksela, 10 lipca 2026 r.
(OR. en)

11772/26
ADD 1

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

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	1 lipca 2026 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	C(2026) 4534 annex
Dotyczy:	ZAŁĄCZNIKI do ROZPORZĄDZENIA DELEGOWANEGO KOMISJI (UE) …/… uzupełniającego dyrektywę (UE) 2024/2841 w odniesieniu do określenia kodu QR na fizycznej wersji europejskiej karty osoby z niepełnosprawnością oraz określenia kodu QR i ustanowienia wspólnych specyfikacji technicznych zapewniających bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, a także w odniesieniu do kwestii interoperacyjności

KOMISJA
EUROPEJSKA

Bruksela, dnia 1.7.2026 r.
C(2026) 4534 final

ANNEXES 1 to 4

ZAŁĄCZNIKI

do

ROZPORZĄDZENIA DELEGOWANEGO KOMISJI (UE) …/…

uzupełniającego dyrektywę (UE) 2024/2841 w odniesieniu do określenia kodu QR na fizycznej wersji europejskiej karty osoby z niepełnosprawnością oraz określenia kodu QR i ustanowienia wspólnych specyfikacji technicznych zapewniających bezpieczeństwo fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami, a także w odniesieniu do kwestii interoperacyjności

ZAŁĄCZNIK I

SPECYFIKACJE KODU QR NA POTRZEBY FIZYCZNEJ WERSJI EUROPEJSKIEJ KARTY OSOBY Z NIEPEŁNOSPRAWNOŚCIĄ

1. **Format kodu QR na potrzeby fizycznej wersji europejskiej karty osoby z niepełnosprawnością (EDC)**

a) **Format kodu QR Model 2**, zgodny z międzynarodowymi normami ISO/IEC 18004:2024 dotyczącymi kodów QR lub równoważnymi.

b) **Poziom korekcji błędów M** (15 % redundancji) zapewniający odporność na zarysowania lub częściowe uszkodzenie wydrukowanego kodu QR.

c) **Tryb kodowania:** ładunek QR składa się z połączonej struktury issuerSigned w formacie Concise Binary Object Representation (CBOR) oraz odpowiadającego jej obiektu podpisu issuerAuth COSE_Sign1, zgodnie ze specyfikacją CBOR Object Signing and Encryption (COSE, RFC 9052 sekcje 3.1, 4.2 i 4.4), według wzorca modelu danych mDOC dla elementów issuerSigned, dostosowanego jednak do użycia w statycznej fizycznej karcie. issuerAuth jest obiektem COSE_Sign1 z parametrem alg = ES256 oraz chronionym nagłówkiem zawierającym x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2)); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256).

d) Przed zakodowaniem w kodzie QR połączony obiekt CBOR/COSE **jest kompresowany w formacie zlib** (RFC 1950, sekcja 2.2) z **wykorzystaniem algorytmu deflate** (RFC 1951, sekcje 3.2 i 4). Powstałą w ten sposób skompresowaną tablicę bajtów koduje się w **trybie bajtowym kodu QR**, co zapewnia pełną obsługę binarnych ładunków CBOR/COSE oraz interoperacyjność skanerów.

Dla wszystkich pól tekstowych zawartych w ładunku QR wydawcy kodują znaki jako Unicode UTF-8 w ciągach tekstowych CBOR. Do danych ładunku podpisywanego nie stosuje się transliteracji. Do celów interoperacyjności wydawcy stosują formę normalizacji Unicode C (NFC) do wszystkich pól tekstowych przed podpisaniem ładunku.

e) **Prefiks:** ciąg QR EDC rozpoczyna się od „ED1:MDOC:”. Pozwala to zidentyfikować typ karty oraz profil kodowania. Prefiksy są wrażliwe na wielkość liter i muszą być obecne. Nieznane lub nieobsługiwane prefiksy powodują odrzucenie. Prefiks i skompresowany ładunek są kodowane w kodzie QR jako pojedynczy segment danych w trybie bajtowym.

f) **Minimalny rozmiar modułu ≥ 0,25 mm** w celu zapewnienia czytelności na drukowanych kartach.

g) **Wersja maksymalna 20;** z maksymalnie 97 × 97 modułów z każdej strony.

2. **Specyfikacje generowania podpisu EDC**

Kwalifikowana pieczęć elektroniczna (QSeal) stosowana do zabezpieczenia kodów QR EDC zapewnia, by zakodowane dane pochodziły od upoważnionego organu wydającego i nie zostały zmienione.

a) **Algorytm podpisu**: algorytmem podpisu jest ES256 (algorytm podpisu cyfrowego krzywej eliptycznej – ECDSA – z wykorzystaniem SHA-256 przy użyciu krzywej P-256), jak określono w RFC 9053 (sekcja 2.1); w COSE identyfikacja algorytmu odbywa się za pomocą parametru nagłówka alg zgodnie z RFC 9052 (sekcja 3.1).

b) **Klucz podpisu**: ładunek QR jest podpisywany przy użyciu klucza prywatnego odpowiadającego kwalifikowanemu certyfikatowi pieczęci elektronicznej (QSealC).

c) **Struktura COSE:** kontenerem podpisu jest obiekt COSE_Sign1. Chroniony nagłówek zawiera alg (ES256) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256). Weryfikacja polega na wykorzystaniu wartości x5t do odnalezienia odpowiedniego certyfikatu w lokalnym repozytorium zaufania weryfikatora, utworzonym na podstawie informacji z zaufanej listy, a następnie na sprawdzeniu łańcucha certyfikatów oraz statusu certyfikatu zgodnie z ramami zaufania eIDAS.

d) **Standard podpisu**: ładunek kodu QR jest podpisywany jako obiekt COSE_Sign1 zgodnie z RFC 9052 (sekcja 4), CBOR Object Signing and Encryption. Obiekt COSE_Sign1 jest zawarty w issuerAuth i kodowany bez tagu CBOR dla COSE_Sign1. Pole ładunku obiektu COSE_Sign1 jest oddzielone i kodowane jako CBOR null. Do celów generowania i weryfikacji podpisów zewnętrzny ładunek jest strukturą zakodowaną w deterministycznym formacie CBOR, zawierającą wartość docType oraz wartość issuerSigned z mapy CBOR najwyższego poziomu.

e) **Algorytm skrótu**: SHA-256 jest stosowany jako część ES256 do generowania podpisów i weryfikacji integralności.

f) **Kodowanie**: ładunek jest kodowany przy użyciu CBOR (RFC 8949, sekcja 4.2), zgodnie z wymaganiami specyfikacji COSE i mDOC, co zapewnia poprawne kodowanie i odtwarzalność podpisanych danych.

3. **Specyfikacje druku**

a) **Strefa ciszy**: kod QR jest otoczony z każdej strony czystym marginesem o szerokości **4 modułów**, wolnym od jakiegokolwiek druku, wzoru lub tła.

b) **Kontrast**: kod QR jest drukowany na białym tle, przy minimalnym współczynniku kontrastu **4:1**, aby zapewnić wysoką czytelność w różnych warunkach oświetleniowych.

c) Kod QR jest drukowany przy użyciu koloru zdefiniowanego w załączniku I do dyrektywy (UE) 2024/2841, który zapewnia maksymalny kontrast.

d) **Umiejscowienie i rozmiar**: kod QR, wraz ze strefą ciszy, ma wymiary 26,25 mm × 26,25 mm i znajduje się na rewersie karty w prawym dolnym rogu. Kod QR jest stosowany maksymalnie w wersji 20 (97 × 97 modułów), przy czym rozmiar modułu wynosi co najmniej 0,25 mm.

Kod QR, wraz ze strefą ciszy, jest umieszczony w odległości przynajmniej 5 mm od prawego brzegu kraty i w odległości przynajmniej 5 mm od dolnego brzegu karty.

4. **Dane w kodzie QR EDC**

Kod QR zawiera minimalny zestaw danych możliwych do weryfikacji offline, zgodnie z zasadą minimalizacji danych określoną w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Struktura ładunku jest następująca:

a) atrybuty karty są kodowane w formacie CBOR w ramach obiektu issuerSigned;

b) struktura ta jest opakowana i podpisana QSeal organu wydającego jako issuerAuth (COSE_Sign1, ES256, z uwzględnieniem x5t, czyli parametru nagłówka skrótu certyfikatu COSE X.509);

c) Powstały obiekt CBOR / COSE jest kompresowany zgodnie z pkt 1 lit. d) niniejszego załącznika. Ładunek kodu QR składa się z prefiksu „ED1:MDOC:", po którym następuje skompresowana tablica bajtów, a cały ładunek jest kodowany w trybie bajtowym jako pojedynczy segment danych kodu QR.

Zawartość danych obejmuje podzbiór danych widocznych z pól na awersie karty wymienionych w załączniku I do dyrektywy (UE) 2024/2841 (imię, nazwisko, numer seryjny karty, termin ważności), wraz z identyfikatorem unieważnienia, podpisem elektronicznym oraz informacjami o schemacie.

Podpis elektroniczny zawiera:

(i) issuerAuth – obiekt COSE_Sign1 podpisany przy użyciu **klucza prywatnego QSealC** organu wydającego;

(ii) chroniony nagłówek zawierający alg = ES256 (algorytm podpisu) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509).

5. Dane nieobowiązkowe

Kod QR nie może zawierać żadnych danych nieobowiązkowych.

6. Identyfikator unieważnienia (RID)

Oprócz widocznego numeru seryjnego karty kod QR zawiera specjalny identyfikator unieważnienia (RID).

RID jest wykorzystywany do określania statusu unieważnienia oraz do zarządzania wykazem unieważnionych kart. RID nie jest drukowany na karcie ani wyświetlany weryfikatorom kart.

6.1. *Wymogi dotyczące RID*

RID:

a) jest uwzględniony w podpisanym ładunku QR;

b) jest niepowtarzalny co najmniej w obrębie domeny wydawania danego organu wydającego;

c) nie jest drukowany na karcie ani nie jest przeznaczony do odczytu przez człowieka;

d) nie ujawnia danych osobowych ani nie ma bezpośredniego znaczenia;

e) nie może bezpośrednio wynikać z widocznego numeru seryjnego karty; oraz

f) jest kryptograficznie powiązany z ładunkiem QR za pomocą kwalifikowanej pieczęci elektronicznej.

6.2. *Format i rozmiar RID*

RID jest kodowany jako ciąg bajtów CBOR (bstr). RID ma długość 16 bajtów (128 bitów).

RID jest generowany przez organ wydający przy użyciu metody znajdującej się pod jego kontrolą, która to metoda zapewnia wystarczającą entropię i odporność na odgadnięcie lub wyliczenie.

6.3. *Wykazy unieważnionych kart*

Wykazy unieważnionych kart publikowane do celów weryfikacji odnoszą się wyłącznie do RID unieważnionych kart. Numery seryjne kart nie są publikowane w wykazach unieważnionych kart.

7. Ładunek CBOR (w kodzie QR) EDC

W ładunku QR uwzględnia się wyłącznie następujące dane, zgodnie z widocznymi polami danych EDC określonymi w załączniku I do dyrektywy (UE) 2024/2841.

Zawartość najwyższego poziomu:

a) docType = "eu.edc";

b) issuerSigned.nameSpaces."eu.edc" z atrybutami podanymi w tabeli poniżej;

c) issuerAuth = COSE_Sign1 (QSeal).

Pole	**Ścieżka mDOC**	**Rodzaj/Format**
Wersja schematu danych	issuerSigned.nameSpaces."eu.edc".ver	Ciąg znaków (np. „1.0”)
Rodzaj karty: EDC	docType	Enum ("eu.edc")
Numer seryjny karty	issuerSigned.nameSpaces."eu.edc".sub	Ciąg znaków
Identyfikator unieważnienia	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bajtów)
Imię posiadacza karty	issuerSigned.nameSpaces."eu.edc".givenName	Ciąg tekstowy Unicode (UTF-8)
Nazwisko posiadacza karty	issuerSigned.nameSpaces.„eu.edc”.familyName	Ciąg tekstowy Unicode (UTF-8)
Termin ważności karty	issuerSigned.nameSpaces."eu.edc".exp	tag CBOR 1004, zdefiniowany w RFC 8943 (sekcja 2.1),

		zawierający ciąg tekstowy w UTF-8 przedstawiający pełną datę w formacie RFC 3339: RRRR-MM-DD.

Podpis elektroniczny jest zawarty w issuerAuth (obiekt COSE_Sign1). Łańcuch certyfikatów nie jest osadzany w ładunku kodu QR; zamiast tego chroniony nagłówek COSE zawiera x5t, odcisk palca certyfikatu umożliwiający odnalezienie odpowiedniego certyfikatu QSealC w lokalnym repozytorium zaufania weryfikatora.

8. **Przykład ładunku kodu QR EDC: reprezentacja logiczna w konwencji JavaScript Object Notation (JSON) z komentarzem**

Poniższy przykład stanowi czytelną dla człowieka reprezentację logicznego widoku EDC w JavaScript Object Notation (JSON). W praktyce struktura ta nie ma postaci czytelnej dla człowieka, ponieważ:

a) jest kodowana w CBOR (RFC 8949, sekcja 3);

b) jest podpisana przy użyciu struktury COSE_Sign1 bez tagów z oddzielonym ładunkiem (RFC 9052, sekcja 4.),

c) zawiera termin ważności jako wartość stanowiącą pełną datę w formacie tagu CBOR 1004 zgodnie z RFC 8943 (sekcja 2.1);

d) zawiera parametr x5t w nagłówku chronionym zgodnie z RFC 9360, przy użyciu skrótu SHA-256 do zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC; oraz

e) jest kompresowana i opatrzona prefiksem w postaci ciągu ED1:MDOC: zanim zostanie zakodowana w kod QR.

```
{
 // konwencja JSON, jedynie logiczny widok EDC czytelny dla człowieka.
 // Faktyczny ładunek QR to deterministyczny format CBOR, a nie JSON.
 "docType": "eu.edc", // poświadczenie EDC. Zawiera wartość docType, wraz z
    //issuerSigned, w ładunku zewnętrznym COSE_Sign1.

 "issuerSigned": {
    // dane chronione przez issuerAuth; użyte jako oddzielony ładunek.
    // Do celów generowania i weryfikacji podpisów oddzielony ładunek zewnętrzny obejmuje
zarówno
    // docType jak i issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // wersja profilu/schematu kodu QR

        // Numer seryjny karty; określony przez wydawcę, maksymalnie 24 znaki.
        "sub": "AB123456789012345678 90CD",
```

```
      // Identyfikator unieważnienia: rzeczywista wartość CBOR bstr, 16 bajtów/128 bitów.
      // dla czytelności pokazana tutaj jako 32-znakowy ciąg heksadecymalny.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Anna",    // imię wydrukowane na EDC
      "familyName": "Kowalska", // nazwisko wydrukowane na EDC

      // Faktyczne kodowanie CBOR wykorzystuje tag 1004 dla pełnej daty w formacie RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Faktyczny format: COSE_Sign1 bez tagów, a nie obiekt JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // zakodowany bez tagu COSE_Sign1 CBOR
  "payload": "detached", // pole ładunku COSE to CBOR null

  "protectedHeader": {
    // alg: ES256; równoważny parametr nagłówka COSE 1 = -7.
    "alg": "ES256",

    // x5t: odcisk palca certyfikatu; parametr nagłówka COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // równoważna wartość skrótu COSE -16
```

// skrót SHA-256 zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC.

// 32 bajty reprezentowane jako 64-znakowy ciąg heksadecymalny.

"hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

"unprotectedHeader": {}, // pusty w tym przykładzie

// podpis COSE z algorytmem ES256: 64 bajty = 128-znakowy ciąg heksadecymalny

"signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Stosowanie mechanizmów kryptograficznych

Stosowanie mechanizmów kryptograficznych w kontekście niniejszego załącznika odbywa się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

ZAŁĄCZNIK II

SPECYFIKACJE KODU QR DLA FIZYCZNEJ WERSJI EUROPEJSKIEJ KARTY PARKINGOWEJ DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI

1. **Format kodu QR na fizycznej wersji europejskiej karty parkingowej dla osób z niepełnosprawnościami (EPC)**

a) **Format kodu QR Model 2**, zgodny z międzynarodowymi normami ISO/IEC 18004:2024 dotyczącymi kodów QR lub równoważnymi.

b) **Poziom korekcji błędów M** (15 % redundancji) zapewniający odporność na zarysowania lub częściowe uszkodzenie wydrukowanego kodu QR.

c) **Tryb kodowania:** ładunek QR składa się z połączonej struktury issuerSigned w formacie Concise Binary Object Representation (CBOR) oraz odpowiadającego jej obiektu podpisu issuerAuth COSE_Sign1, zgodnie ze specyfikacją CBOR Object Signing and Encryption (COSE, RFC 9052 sekcje 3.1, 4.2 i 4.4), według wzorca modelu danych mDOC dla elementów issuerSigned, dostosowanego jednak do użycia w statycznej fizycznej karcie. issuerAuth jest obiektem COSE_Sign1 z parametrem alg = ES256 oraz chronionym nagłówkiem zawierającym x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2)); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256).

d) Przed zakodowaniem w kodzie QR połączony obiekt CBOR/COSE **jest kompresowany w formacie zlib** (RFC 1950, sekcja 2.2) z **wykorzystaniem algorytmu deflate** (RFC 1951, sekcje 3.2 i 4). Powstałą w ten sposób skompresowaną tablicę bajtów koduje się w **trybie bajtowym kodu QR**, co zapewnia pełną obsługę binarnych ładunków CBOR/COSE oraz interoperacyjność skanerów.

Dla wszystkich pól tekstowych zawartych w ładunku QR wydawcy kodują znaki jako Unicode UTF-8 w ciągach tekstowych CBOR. Do danych ładunku podpisywanego nie stosuje się transliteracji. Do celów interoperacyjności wydawcy stosują formę normalizacji Unicode C (NFC) do wszystkich pól tekstowych przed podpisaniem ładunku.

e) **Prefiks**: ciąg QR EPC rozpoczyna się od „EP1:MDOC:”. Pozwala to zidentyfikować typ karty oraz profil kodowania. Prefiksy są wrażliwe na wielkość liter i muszą być obecne. Nieznane lub nieobsługiwane prefiksy powodują odrzucenie. Prefiks i skompresowany ładunek są kodowane w kodzie QR jako pojedynczy segment danych w trybie bajtowym.

f) **Minimalny rozmiar modułu ≥ 0,35 mm** w celu zapewnienia czytelności na drukowanych kartach.

g) **Wersja maksymalna 20**; z maksymalnie 97 x 97 modułów z każdej strony.

2. **Specyfikacje generowania podpisu EPC**

Kwalifikowana pieczęć elektroniczna (QSeal) stosowana do zabezpieczenia kodów QR EPC zapewnia, by zakodowane dane pochodziły od upoważnionego organu wydającego i nie zostały zmienione.

a) **Algorytm podpisu**: algorytmem podpisu jest ES256 (ECDSA z wykorzystaniem SHA-256 przy użyciu krzywej P-256), jak określono w RFC 9053 (sekcja 2.1); w COSE identyfikacja algorytmu odbywa się za pomocą parametru nagłówka alg zgodnie z RFC 9052 (sekcja 3.1).

b) **Klucz podpisu**: ładunek QR jest podpisywany przy użyciu klucza prywatnego odpowiadającego kwalifikowanemu certyfikatowi pieczęci elektronicznej (QSealC).

c) **Struktura COSE**: kontenerem podpisu jest obiekt COSE_Sign1. Chroniony nagłówek zawiera alg (ES256) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509 określony w RFC 9360 (sekcja 2); do celów interoperacyjności algorytmem skrótu stosowanym w x5t jest SHA-256. Weryfikacja polega na wykorzystaniu wartości x5t do odnalezienia odpowiedniego certyfikatu w lokalnym repozytorium zaufania weryfikatora, utworzonym na podstawie informacji z zaufanej listy, a następnie na sprawdzeniu łańcucha certyfikatów oraz statusu certyfikatu zgodnie z ramami zaufania eIDAS.

d) **Standard podpisu**: ładunek kodu QR jest podpisywany jako obiekt COSE_Sign1 zgodnie z RFC 9052 (sekcja 4), CBOR Object Signing and Encryption. Obiekt COSE_Sign1 jest zawarty w issuerAuth i kodowany bez tagu CBOR dla COSE_Sign1. Pole ładunku obiektu COSE_Sign1 jest oddzielone i kodowane jako CBOR null. Do celów generowania i weryfikacji podpisów zewnętrzny ładunek jest strukturą zakodowaną w deterministycznym formacie CBOR, zawierającą wartość docType oraz wartość issuerSigned z mapy CBOR najwyższego poziomu.

e) **Algorytm skrótu**: SHA-256 jest stosowany jako część ES256 do generowania podpisów i weryfikacji integralności.

f) **Kodowanie**: ładunek jest kodowany przy użyciu CBOR (RFC 8949, sekcja 4.2), zgodnie z wymaganiami specyfikacji COSE i mDOC, co zapewnia poprawne kodowanie i odtwarzalność podpisanych danych.

3. **Specyfikacje druku**

a) **Strefa ciszy**: kod QR jest otoczony z każdej strony czystym marginesem o szerokości **4 modułów**, wolnym od jakiegokolwiek druku, wzoru lub tła.

b) **Kontrast**: kod QR jest drukowany na białym tle, przy minimalnym współczynniku kontrastu **4:1**, aby zapewnić wysoką czytelność w różnych warunkach oświetleniowych.

c) Kod QR jest drukowany przy użyciu koloru zdefiniowanego w załączniku II do dyrektywy (UE) 2024/2841, który zapewnia maksymalny kontrast.

d) **Umiejscowienie i rozmiar:** kod QR, wraz ze strefą ciszy, ma wymiary **37 mm** × **37 mm** i jest umieszczony na awersie karty, nieco na prawo od środka, w pobliżu dolnej krawędzi. Kod QR jest stosowany maksymalnie w wersji 20 (97 × 97 modułów), przy czym rozmiar modułu wynosi co najmniej 0,35 mm.

Kod QR, wraz ze strefą ciszy, jest umieszczony w odległości przynajmniej 5 mm od dolnego brzegu karty.

4. **Dane w kodzie QR EPC**

Kod QR zawiera minimalny zestaw danych możliwych do weryfikacji offline, zgodnie z zasadą minimalizacji danych zawartą w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Struktura ładunku jest następująca:

a) atrybuty karty są kodowane w formacie CBOR w ramach obiektu issuerSigned;

b) struktura ta jest opakowana i podpisana QSeal organu wydającego jako issuerAuth (COSE_Sign1, ES256, z uwzględnieniem x5t, czyli parametru nagłówka skrótu certyfikatu COSE X.509);

c) Powstały obiekt CBOR / COSE jest kompresowany zgodnie z pkt 1 lit. d) niniejszego załącznika. Ładunek kodu QR składa się z prefiksu „EP1:MDOC:", po którym następuje skompresowana tablica bajtów, a cały ładunek jest kodowany w trybie bajtowym jako pojedynczy segment danych kodu QR.

Zawartość danych obejmuje podzbiór danych widocznych z pól na awersie karty wymienionych w załączniku II do dyrektywy (UE) 2024/2841 (termin ważności, numer seryjny karty), wraz z identyfikatorem unieważnienia, podpisem elektronicznym oraz informacjami o schemacie.

Podpis elektroniczny zawiera:

(i) issuerAuth – obiekt COSE_Sign1 podpisany przy użyciu **klucza prywatnego QSealC** organu wydającego;

(ii) chroniony nagłówek zawierający alg = ES256 (algorytm podpisu) i x5t (parametr nagłówka skrótu certyfikatu COSE X.509).

5. Dane nieobowiązkowe

Kod QR nie może zawierać żadnych danych nieobowiązkowych.

6. Identyfikator unieważnienia (RID)

Identyfikator unieważnienia EPC jest zgodny z pkt 6 załącznika I.

Wykazy unieważnionych kart EPC zawierają jedynie odniesienie do RID. Numery seryjne kart nie są publikowane w wykazach unieważnionych kart.

7. Ładunek CBOR (w kodzie QR) EPC

W ładunku QR uwzględnia się wyłącznie następujące dane, zgodnie z widocznymi polami karty EPC określonymi w załączniku II do dyrektywy (UE) 2024/2841:

Pole	**Ścieżka mDOC**	**Rodzaj/Format**
Wersja schematu danych	issuerSigned.nameSpaces."eu.epc".ver	Ciąg znaków (np. „1.0")
Rodzaj karty: EPC	docType	Enum ("eu.epc")
Numer seryjny	issuerSigned.nameSpaces."eu.epc".sub	Ciąg znaków

karty		
Identyfikator unieważnienia	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bajtów)
Termin ważności karty	issuerSigned.nameSpaces."eu.epc".exp	tag CBOR 1004, zdefiniowany w RFC 8943 (sekcja 2.1), zawierający ciąg tekstowy w UTF-8 przedstawiający pełną datę w formacie RFC 3339: RRRR-MM-DD.

Podpis elektroniczny jest zawarty w issuerAuth (obiekt COSE_Sign1). Łańcuch certyfikatów nie jest osadzany w ładunku kodu QR; zamiast tego chroniony nagłówek COSE zawiera x5t, odcisk palca certyfikatu umożliwiający odnalezienie odpowiedniego certyfikatu QSealC w lokalnym repozytorium zaufania weryfikatora.

8. Przykład ładunku kodu QR EPC: reprezentacja logiczna w konwencji JavaScript Object Notation (JSON) z komentarzem

Poniższy przykład stanowi czytelną dla człowieka reprezentację logicznego widoku EPC w JavaScript Object Notation (JSON). W praktyce struktura ta nie ma postaci czytelnej dla człowieka, ponieważ:

a) jest kodowana w CBOR (RFC 8949, sekcja 3);

b) jest podpisana przy użyciu struktury COSE_Sign1 bez tagów z oddzielonym ładunkiem (RFC 9052, sekcja 4.),

c) zawiera termin ważności jako wartość stanowiącą pełną datę w formacie tagu CBOR 1004 zgodnie z RFC 8943 (sekcja 2.1);

d) zawiera parametr x5t w nagłówku chronionym zgodnie z RFC 9360, przy użyciu skrótu SHA-256 do zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC; oraz

e) jest kompresowana i opatrzona prefiksem w postaci ciągu EP1:MDOC: zanim zostanie zakodowana w kod QR.

```
{
 // konwencja JSON, jedynie logiczny widok EPC czytelny dla człowieka.
```

```
// Faktyczny ładunek QR to deterministyczny format CBOR, a nie JSON.
"docType": "eu.epc", // poświadczenie EPC. Zawiera wartość docType, wraz z
  //issuerSigned, w ładunku zewnętrznym COSE_Sign1.

"issuerSigned": {
  // dane chronione przez issuerAuth; użyte jako oddzielony ładunek.
  // Do celów generowania i weryfikacji podpisów oddzielony ładunek zewnętrzny obejmuje zarówno
  // docType jak i issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0", // wersja profilu/schematu kodu QR

      // Numer seryjny karty; określony przez wydawcę, maksymalnie 24 znaki.
      "sub": "EF123456789012345678 90GH",

      // Identyfikator unieważnienia: rzeczywista wartość CBOR bstr, 16 bajtów/128 bitów.
      // dla czytelności pokazana tutaj jako 32-znakowy ciąg heksadecymalny.
      "rid": "4a8d9c112233445566778899aabbccdd",

      // Faktyczne kodowanie CBOR wykorzystuje tag 1004 dla pełnej daty w formacie RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
```

```
  // Faktyczny format: COSE_Sign1 bez tagów, a nie obiekt JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // zakodowany bez tagu COSE_Sign1 CBOR
  "payload": "detached", // pole ładunku COSE to CBOR null

  "protectedHeader": {
    // alg: ES256; równoważny parametr nagłówka COSE 1 = -7.
    "alg": "ES256",

    // x5t: odcisk palca certyfikatu; parametr nagłówka COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // równoważna wartość skrótu COSE -16

      // skrót SHA-256 zakodowanego w formacie DER certyfikatu podmiotu końcowego QSealC.
      // 32 bajty reprezentowane jako 64-znakowy ciąg heksadecymalny.
      "hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // pusty w tym przykładzie

  // podpis COSE z algorytmem ES256: 64 bajty = 128-znakowy ciąg heksadecymalny
  "signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Stosowanie mechanizmów kryptograficznych

Stosowanie mechanizmów kryptograficznych w kontekście niniejszego załącznika odbywa się zgodnie z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

ZAŁĄCZNIK III

PRZEKAZYWANIE INFORMACJI, O KTÓRYCH MOWA W ART. 6 UST. 2

1. Państwa członkowskie przekazują Komisji następujące informacje na temat każdego właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami:

   a) nazwę właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   b) numer rejestracyjny właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   c) adres e-mail i numer telefonu właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami;

   d) co najmniej jeden certyfikat, który można wykorzystać do weryfikacji pieczęci elektronicznej utworzonej przez właściwy organ lub podmiot odpowiedzialny za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami i w odniesieniu do którego poświadczone dane dotyczące tożsamości obejmują nazwę i numer rejestracyjny wydawcy, jak określono odpowiednio w lit. a) i b);

   e) adres URL miejsca, w którym wydawca publikuje informacje o statusie ważności fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami.

2. Państwa członkowskie mogą przekazywać Komisji następujące informacje na temat każdego właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami:

   a) adres URL strony internetowej zawierającej polityki i warunki właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami, które to polityki i warunki mają zastosowanie do wydawania fizycznych wersji europejskiej karty osoby z niepełnosprawnością i europejskiej karty parkingowej dla osób z niepełnosprawnościami i korzystania z nich;

   b) w stosownych przypadkach adres URL strony internetowej zawierającej dodatkowe informacje na temat właściwego organu lub podmiotu odpowiedzialnego za wydawanie fizycznych wersji europejskiej karty osoby z niepełnosprawnością lub europejskiej karty parkingowej dla osób z niepełnosprawnościami.

ZAŁĄCZNIK IV

SPECYFIKACJE TECHNICZNE WYKAZU UNIEWAŻNIONYCH KART DLA FIZYCZNYCH WERSJI EUROPEJSKIEJ KARTY OSOBY Z NIEPEŁNOSPRAWNOŚCIĄ LUB EUROPEJSKIEJ KARTY PARKINGOWEJ DLA OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI

1. Na potrzeby niniejszego załącznika identyfikator odpowiada identyfikatorowi unieważnienia (RID) zdefiniowanemu w pkt 6 załącznika I i pkt 6 załącznika II.

2. Wykaz unieważnionych kart wdraża się jako token listy identyfikatorów w formacie CWT (RFC 8392, sekcja 7), zgodnie z pkt 5.2 specyfikacji listy statusu tokenów (draft-ietf-oauth-status-list-14), z następującymi zmianami:

   a) wartość elementu „type” wynosi „application/identifierlist+cwt”;

   b) obecny jest element czasu wygaśnięcia;

   c) element StatusList nie jest obecny w zbiorze elementów CWT;

   d) struktura IdentifierList określona w pkt 3 jest obecna jako element w zbiorze elementów CWT przy użyciu klucza 65530;

   e) CWT stanowi obiekt COSE_Sign1, przy czym do obliczenia podpisu stosuje się algorytm podpisu zgodny z uzgodnionymi mechanizmami kryptograficznymi zatwierdzonymi przez Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa i opublikowanymi przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA);

   f) CWT zawiera parametr x5chain zdefiniowany w RFC 9360 (sekcja 2) w chronionym nagłówku zawierającym certyfikat lub łańcuch certyfikatów służący do weryfikacji podpisu wykazu unieważnionych kart;

   g) rozszerzone użycie klucza OID określone w specyfikacji listy statusu tokenów (draft-ietf-oauth-status-list-14) można stosować na potrzeby certyfikatu podpisującego listę identyfikatorów; zaleca się, aby weryfikatorzy obsługiwali ten identyfikator OID oraz aby infrastruktury wydawców nie oznaczały pola rozszerzonego użycia klucza jako krytycznego w przypadku stosowania identyfikatora OID rozszerzonego użycia klucza.

3. Struktura IdentifierList stanowi strukturę CBOR zdefiniowaną przy użyciu języka Concise Data Definition Language (CDDL) w następujący sposób:

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

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

Identifier = bstr

Aggregation_uri = tstr