Consiliul
Uniunii Europene

Bruxelles, 10 iulie 2026
(OR. en)

11772/26
ADD 1

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	1 iulie 2026
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	C(2026) 4534 annex
Subiect:	ANEXE la REGULAMENTUL DELEGAT (UE) .../... AL COMISIEI de completare a Directivei (UE) 2024/2841 în ceea ce privește stabilirea codului QR de pe versiunea fizică a cardului european pentru dizabilitate și stabilirea codului QR și a unor specificații tehnice comune care să asigure securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, precum și a aspectelor legate de interoperabilitate

COMISIA
EUROPEANĂ

Bruxelles, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ANEXE

la

REGULAMENTUL DELEGAT (UE) .../... AL COMISIEI

de completare a Directivei (UE) 2024/2841 în ceea ce privește stabilirea codului QR de pe versiunea fizică a cardului european pentru dizabilitate și stabilirea codului QR și a unor specificații tehnice comune care să asigure securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, precum și a aspectelor legate de interoperabilitate

ANEXA I

SPECIFICAȚIILE CODULUI QR PENTRU VERSIUNEA FIZICĂ A CARDULUI EUROPEAN PENTRU DIZABILITATE

1. **Formatul codului QR pentru versiunea fizică a cardului european pentru dizabilitate (EDC)**

(a) **Formatul Modelului 2 al codului QR**, în conformitate cu specificațiile internaționale ale codului QR ISO/IEC 18004:2024 sau echivalent.

(b) **Nivelul M de corectare a erorilor** (redundanță 15 %) care asigură rezistența la zgârieturi sau la deteriorarea parțială a unui cod QR imprimat.

(c) **Mod de codificare:** Sarcina utilă QR constă în structura combinată issuerSigned Concise Binary Object Representation (reprezentare concisă a obiectelor binare – CBOR) și obiectul de semnătură issuerAuth COSE_Sign1 corespunzător, astfel cum este definit în CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR) (COSE, RFC 9052 secțiunile 3.1, 4.2 și 4.4), urmând modelul de date mDOC pentru elementele issuerSigned, dar adaptat pentru utilizarea statică a cardului fizic. IssuerAuth este un obiect COSE_Sign1 cu alg = ES256 și un antet protejat care conține x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256].

(d) Înainte de codificarea codului QR, obiectul CBOR/COSE combinat se **comprimă utilizând formatul zlib** (RFC 1950, secțiunea 2.2) cu algoritmul de **deflatare** (RFC 1951 secțiunile 3.2 și 4). Seria de octeți comprimați rezultată se codifică în **modul de octeți cu cod QR**, asigurând sprijin deplin pentru sarcinile utile binare CBOR/COSE și interoperabilitatea scanerului.

Pentru toate câmpurile de text incluse în sarcina utilă QR, emitenții trebuie să codifice caracterele ca Unicode UTF-8 în șirurile de text CBOR. Transliterația nu se aplică datelor privind sarcina utilă semnate. Din motive de interoperabilitate, emitenții aplică formularul de normalizare Unicode C (NFC) tuturor câmpurilor textuale înainte de a semna.

(e) **Prefix:** Șirul QR al EDC începe cu „ED1:MDOC:”. Această formulă identifică tipul cardului și profilul de codificare. Prefixele respectă regimul de litere mici și mari și trebuie să fie prezente. Prefixele necunoscute sau neacceptate conduc la respingere. Prefixul și sarcina utilă comprimată se codifică sub forma unui singur segment de date în modul de octeți în codul QR.

(f) **Dimensiunea minimă a modulului ≥ 0,25 mm** pentru a asigura lizibilitatea pe cardurile imprimate.

(g) **Versiunea maximă 20;** cu până la 97 × 97 de pe fiecare parte.

2. **Specificații privind generarea semnăturii EDC**

Sigiliul electronic calificat (QSeal) utilizat pentru sigilarea codurilor QR ale EDC asigură faptul că datele codificate provin de la autoritatea emitentă autorizată și nu au fost modificate.

(a) **Algoritmul de semnătură**: Algoritmul semnăturii este ES256 [algoritmul de semnătură digitală bazat pe curbe eliptice (*Elliptic Curve Digital Signature*

Algorithm – ECDSA) cu SHA-256 utilizând curba P-256], astfel cum este definit în RFC 9053 (secțiunea 2.1); în COSE, algoritmul este identificat prin parametrul antetului alg din RFC 9052 (secțiunea 3.1).

(b) **Cheia de semnătură**: Sarcina utilă a codului QR se semnează utilizând cheia privată corespunzătoare unui certificat calificat pentru semnături electronice (QSealC).

(c) **Structura COSE:** Containerul cu semnătură este un obiect COSE_Sign1. Antetul protejat include alg (ES256) și x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256]. Verificarea se bazează pe utilizarea valorii x5t pentru a localiza certificatul corespunzător în registrul de încredere stocat local în memoria cache a verificatorului, creat pe baza informațiilor din lista sigură, și apoi validează lanțul de certificate și statutul certificatului în conformitate cu cadrul de încredere eIDAS.

(d) **Standardul de semnătură**: Sarcina utilă a codului QR se semnează ca obiect COSE_Sign1 în conformitate cu RFC 9052 (secțiunea 4), CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR). Obiectul COSE_Sign1 se stochează în issuerAuth și se codifică fără eticheta CBOR pentru COSE_Sign1. Câmpul sarcinii utile al obiectului COSE_Sign1 se detașează și se codifică drept CBOR null. Pentru generarea și verificarea semnăturii, sarcina utilă externă este structura CBOR codificată determinist, care conține valoarea docType și valoarea issuerSigned din harta CBOR de prim nivel.

(e) **Algoritmul hash**: SHA-256 se utilizează ca parte a ES256 pentru generarea semnăturii și verificarea integrității.

(f) **Codificare**: Sarcina utilă se codifică utilizând CBOR (RFC 8949, secțiunea 4.2), astfel cum se prevede în specificațiile COSE și mDOC, asigurând codificarea și reproductibilitatea datelor semnate.

3. **Specificații de imprimare**

(a) **Zonă liniștită**: O margine liberă de **4 module** trebuie să înconjoare codul QR pe toate laturile, fără niciun fel de text imprimat, model sau fundal.

(b) **Contrast**: Codul QR se imprimă pe fond alb, cu un raport de contrast de cel puțin **4:1**, pentru a asigura o lizibilitate ridicată în condiții de iluminare variabile.

(c) Codul QR se imprimă utilizând culoarea definită în anexa I la Directiva (UE) 2024/2841 care asigură contrastul maxim.

(d) **Amplasare și dimensiune**: Codul QR, inclusiv zona liniștită, este de 26,25 mm × 26,25 mm, amplasat pe versoul cardului, în colțul din dreapta-jos. Codul QR este versiunea maximă 20 (97 × 97 de module), cu o dimensiune a modulului de 0,25 mm sau mai mare.

Codul QR, inclusiv zona sa liniștită, este amplasat la cel puțin 5 mm față de marginea din dreapta și la cel puțin 5 mm față de marginea inferioară a cardului.

4. Datele din codul QR al EDC

Codul QR conține un set de date minim, verificabil offline, în conformitate cu principiul reducerii la minimum a datelor prevăzut la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Structura sarcinii utile este următoarea:

(a) Atributele cardului sunt codificate în CBOR în cadrul unui obiect issuerSigned.

(b) Structura este sigilată și semnată de QSeal al autorității emitente ca issuerAuth (COSE_Sign1, ES256, inclusiv x5t, parametrul antetului hash al certificatului COSE X.509).

(c) Obiectul CBOR/COSE rezultat se comprimă în conformitate cu punctul 1 litera (d) din prezenta anexă. Sarcina utilă a codului QR constă în prefixul „ED1:MDOC:”, urmat de seria de octeți comprimați rezultată, iar sarcina utilă completă se codifică utilizând modul de octeți sub forma unui singur segment de date în codul QR.

Conținutul datelor constă într-un subset de date vizibile din câmpurile de pe fața cardului enumerate în anexa I la Directiva (UE) 2024/2841 (nume, prenume, numărul de serie al cardului, data expirării), împreună cu identificatorul de revocare, semnătura electronică și informații privind schema.

Semnătura electronică conține:

(i) issuerAuth – un obiect COSE_Sign1 semnat cu **cheia privată QSealC** a autorității emitente;

(ii) antet protejat care include alg = ES256 (algoritm de semnătură) și x5t (parametrul antetului hash al certificatului COSE X.509).

5. Date opționale

În codul QR nu se includ date opționale.

6. Identificatorul de revocare (RID)

Pe lângă numărul de serie vizibil al cardului, codul QR include un identificator de revocare dedicat (RID).

RID se utilizează pentru determinarea statutului de revocat și pentru gestionarea listei de revocare. RID nu se imprimă pe card și nu se afișează pentru verificatorii de carduri.

6.1. *Cerințe aplicabile RID*

RID:

(a) se include în sarcina utilă QR semnată;

(b) este unic cel puțin în cadrul domeniului de emitere al autorității emitente;

(c) nu se imprimă pe card și nu este destinat să fie lizibil pentru om;

(d) nu dezvăluie date cu caracter personal și nu are o semnificație directă;

(e) nu se poate deduce direct din numărul de serie vizibil al cardului și

(f) este legat criptografic de sarcina utilă QR prin sigiliul electronic calificat.

6.2. *Formatul și dimensiunea RID*

RID se codifică sub formă de șir de octeți CBOR (bstr). RID are o lungime de 16 octeți (128 de biți).

RID se generează de autoritatea emitentă utilizând o metodă aflată sub controlul său care asigură o entropie și o rezistență suficiente la ghicire sau enumerare.

6.3. *Liste de revocare*

Listele de revocare publicate în scopul verificării fac trimitere numai la RID-ul cardurilor revocate. Numerele de serie ale cardurilor nu se publică în listele de revocare.

7. Sarcina utilă CBOR (în interiorul codului QR) a EDC

Numai următoarele date se includ în sarcina utilă QR, în concordanță cu câmpurile de date ale EDC vizibile prevăzute în anexa I la Directiva (UE) 2024/2841.

Conținuturile de nivel superior:

(a) docType = „eu.edc”

(b) issuerSigned.nameSpaces.„eu.edc” cu atributele prezentate în tabelul de mai jos

(c) issuerAuth = COSE_Sign1 (QSeal)

Câmp	**Calea mDOC**	**Tip/Format**
Versiunea schemei de date	issuerSigned.nameSpaces.„eu.edc”.ver	Șir (de exemplu, „1.0”)
Tipul cardului: EDC	docType	Enum („eu.edc”)
Numărul de serie al cardului	issuerSigned.nameSpaces.„eu.edc”.sub	Șir
Identificator de revocare	issuerSigned.nameSpaces.„eu.edc”.rid	CBOR bstr (16 octeți)
Prenumele titularului cardului	issuerSigned.nameSpaces.„eu.edc”.givenName	Șir de text Unicode (UTF-8)
Numele titularului cardului	issuerSigned.nameSpaces.„eu.edc”.familyName	Șir de text Unicode (UTF-8)
Data expirării cardului	issuerSigned.nameSpaces.„eu.edc”.exp	Eticheta CBOR 1004, astfel cum este definită în RFC 8943

		(secțiunea 2.1), conținând un șir de text UTF-8 care reprezintă o dată completă conform RFC 3339 în format AAAA-LL-ZZ.

Semnătura electronică este stocată în issuerAuth (un obiect COSE_Sign1). Lanțul de certificate nu se integrează în sarcina utilă a codului QR; în schimb, antetul protejat COSE include x5t, o amprentă a certificatului utilizată pentru a localiza QSealC corespunzător în registrul de încredere stocat în memoria cache a verificatorului.

8. **Exemplu de sarcină utilă a codului QR al EDC: reprezentare logică comentată de tipul JavaScript Object Notation**

Următorul exemplu este o reprezentare JavaScript Object Notation (JSON – notarea obiectelor în JavaScript) lizibilă pentru om a vizualizării logice a EDC. În practică, această structură nu trebuie să fie lizibilă pentru om, deoarece:

(a) este codificată în CBOR (RFC 8949, secțiunea 3);

(b) este semnată utilizând structura COSE_Sign1 neetichetată cu o sarcină utilă detașată (RFC 9052, secțiunea 4.),

(c) include data expirării ca etichetă CBOR 1004, valoarea datei complete, în conformitate cu RFC 8943 (secțiunea 2.1);

(d) include parametrul antetului protejat x5t în conformitate cu RFC 9360, utilizând SHA-256 pe entitatea finală QSealC codificată în DER; și

(e) este comprimată și prefixată cu șirul ED1:MDOC: înainte de a fi codificată în codul QR.

```
{
 // Numai vizualizare logică lizibilă pentru om a EDC, de tip JSON.
 // Sarcina utilă efectivă a codului QR este în format CBOR determinist, nu JSON.
 „docType”: „eu.edc”, // acreditare EDC. Valoarea docType este inclusă, împreună cu
  //issuerSigned, în sarcina utilă externă COSE_Sign1.

 „issuerSigned”: {
  // Date protejate de issuerAuth; utilizate ca sarcină utilă detașată.
  // Pentru generarea și verificarea semnăturii, sarcina utilă externă detașată acoperă atât
  // docType, cât și issuerSigned.
  „nameSpaces”: {
   „eu.edc”: {
    „ver”: „1.0”, // versiunea profilului/schemei codului QR

    // Numărul de serie al cardului; definit de emitent, maximum 24 de caractere.
    „sub”: „AB123456789012345678 90CD”,
```

// Identificator de revocare: CBOR bstr efectiv, 16 octeți/128 de biți.

// reprezentat aici sub formă de 32 de caractere hexadecimale pentru lizibilitate.

„rid”: „9f8c4d3a7b1e2c0a55aa33ff8899ee11”,

„givenName”: „Ann”, // prenumele imprimat pe EDC

„familyName”: „Other”, // numele de familie imprimat pe EDC

// Codificarea CBOR efectivă utilizează eticheta 1004 pentru data completă conform RFC 3339.

„exp”: „31-12-2030”

}

}

},

„issuerAuth”: {

// Forma efectivă: COSE_Sign1 neetichetată, nu un obiect JSON.

„type”: „COSE_Sign1”,

„tagged”: fals, // codificat fără eticheta CBOR COSE_Sign1

„payload”: „detached”, // câmpul sarcinii utile COSE este CBOR null

„protectedHeader”: {

// alg: ES256; parametrul antetului COSE echivalent 1 = -7.

„alg”: „ES256”,

// x5t: amprenta certificatului; parametrul antetului COSE 34.

„x5t”: {

„hashAlg”: „SHA-256”, // valoarea hash COSE echivalentă -16

// hash SHA-256 al entității finale QSealC codificate în DER.

// 32 de octeți reprezentați de 64 de caractere hexadecimale.

„hashValue”: „0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

},

„unprotectedHeader”: {}, // gol în acest exemplu

// semnătură COSE ES256: 64 de octeți = 128 de caractere hexadecimale.

„signature”: „0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

}

9. Utilizarea mecanismelor criptografice

Utilizarea mecanismelor criptografice în contextul prezentei anexe este în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

ANEXA II

SPECIFICAȚIILE CODULUI QR PENTRU VERSIUNEA FIZICĂ A CARDULUI EUROPEAN DE PARCARE PENTRU PERSOANELE CU DIZABILITĂȚI

1. **Formatul codului QR de pe versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități (EPC)**

(a) **Formatul Modelului 2 al codului QR**, în conformitate cu specificațiile internaționale ale codului QR ISO/IEC 18004:2024 sau echivalent.

(b) **Nivelul M de corectare a erorilor** (redundanță 15 %) care asigură rezistența la zgârieturi sau la deteriorarea parțială a codului QR imprimat.

(c) **Mod de codificare:** Sarcina utilă QR constă în structura combinată issuerSigned Concise Binary Object Representation (reprezentare concisă a obiectelor binare – CBOR) și obiectul de semnătură issuerAuth COSE_Sign1 corespunzător, astfel cum este definit în CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR) (COSE, RFC 9052 secțiunile 3.1, 4.2 și 4.4), urmând modelul de date mDOC pentru elementele issuerSigned, dar adaptat pentru utilizarea statică a cardului fizic. IssuerAuth este un obiect COSE_Sign1 cu alg = ES256 și un antet protejat care conține x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256].

(d) Înainte de codificarea codului QR, obiectul CBOR/COSE combinat **se comprimă utilizând formatul zlib (RFC 1950, secțiunea 2.2) cu algoritmul de deflatare** (RFC 1951, secțiunile 3.2 și 4). Seria de octeți comprimați rezultată se codifică în **modul de octeți cu cod QR**, asigurând sprijin deplin pentru sarcinile utile binare CBOR/COSE și interoperabilitatea scanerului.

Pentru toate câmpurile de text incluse în sarcina utilă QR, emitenții trebuie să codifice caracterele ca Unicode UTF-8 în șirurile de text CBOR. Transliterația nu se aplică datelor privind sarcina utilă semnate. Din motive de interoperabilitate, emitenții aplică formularul de normalizare Unicode C (NFC) tuturor câmpurilor textuale înainte de a semna.

(e) **Prefix**: Șirul QR al EDC începe cu „EP1:MDOC:”. Această formulă identifică tipul cardului și profilul de codificare. Prefixele respectă regimul de litere mici și mari și trebuie să fie prezente. Prefixele necunoscute sau neacceptate conduc la respingere. Prefixul și sarcina utilă comprimată se codifică sub forma unui singur segment de date în modul de octeți în codul QR.

(f) **Dimensiunea minimă a modulului ≥ 0,35 mm** pentru a asigura lizibilitatea pe cardurile imprimate.

(g) **Versiunea maximă 20**; cu până la 97 × 97 de module pe fiecare parte.

2. **Specificații privind generarea semnăturii EPC**

Sigiliul electronic calificat (QSeal) utilizat pentru sigilarea codurilor QR ale EPC asigură faptul că datele codificate provin de la autoritatea emitentă autorizată și nu au fost modificate.

(a) **Algoritmul de semnătură**: Algoritmul semnăturii este ES256 [ECDSA cu SHA-256 utilizând curba P-256], astfel cum este definit în RFC 9053 (secțiunea 2.1); în COSE, algoritmul este identificat prin parametrul antetului alg din RFC 9052 (secțiunea 3.1).

(b) **Cheia de semnătură**: Sarcina utilă a codului QR se semnează utilizând cheia privată corespunzătoare unui certificat calificat pentru semnături electronice (QSealC).

(c) **Structura COSE**: Containerul cu semnătură este un obiect COSE_Sign1. Antetul protejat include alg (ES256) și x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256]. Verificarea se bazează pe utilizarea valorii x5t pentru a localiza certificatul corespunzător în registrul de încredere stocat local în memoria cache a verificatorului, creat pe baza informațiilor din lista sigură, și apoi validează lanțul de certificate și statutul certificatului în conformitate cu cadrul de încredere eIDAS.

(d) **Standardul de semnătură**: Sarcina utilă a codului QR se semnează ca obiect COSE_Sign1 în conformitate cu RFC 9052 (secțiunea 4), CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR). Obiectul COSE_Sign1 se stochează în issuerAuth și se codifică fără eticheta CBOR pentru COSE_Sign1. Câmpul sarcinii utile al obiectului COSE_Sign1 se detașează și se codifică drept CBOR null. Pentru generarea și verificarea semnăturii, sarcina utilă externă este structura CBOR codificată în CBOR determinist, care conține valoarea docType și valoarea issuerSigned din harta CBOR de prim nivel.

(e) **Algoritmul hash**: SHA-256 se utilizează ca parte a ES256 pentru generarea semnăturii și verificarea integrității.

(f) **Codificare**: Sarcina utilă se codifică utilizând CBOR (RFC 8949, secțiunea 4.2), astfel cum se prevede în specificațiile COSE și mDOC, asigurând codificarea și reproductibilitatea datelor semnate.

3. **Specificații de imprimare**

(a) **Zonă liniștită**: O margine liberă de **4 module** trebuie să înconjoare codul QR pe toate laturile, fără niciun fel de text imprimat, model sau fundal.

(b) **Contrast**: Codul QR se imprimă pe fond alb, cu un raport de contrast de cel puțin **4:1**, pentru a asigura o lizibilitate ridicată în condiții de iluminare variabile.

(c) Codul QR se imprimă utilizând culoarea definită în anexa II la Directiva (UE) 2024/2841 care asigură contrastul maxim.

(d) **Amplasare și dimensiune:** Codul QR, inclusiv zona liniștită, este de **37 mm** × **37 mm**, amplasat pe fața cardului, ușor în afara centrului către dreapta, spre marginea inferioară. Codul QR este versiunea maximă 20 (97 × 97 module), cu o dimensiune a modulului de 0,35 mm sau mai mare.

Codul QR, inclusiv zona sa liniștită, este amplasat la cel puțin 5 mm față de marginea inferioară a cardului.

4. **Datele din codul QR al EPC**

Codul QR conține un set de date minim, verificabil offline, în conformitate cu principiul reducerii la minimum a datelor cuprins la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Structura sarcinii utile este următoarea:

(a) Atributele cardului sunt codificate în CBOR în cadrul unui obiect issuerSigned.

(b) Această structură este sigilată și semnată de QSeal al autorității emitente ca issuerAuth (COSE_Sign1, ES256, inclusiv x5t, parametrul antetului hash al certificatului COSE X.509).

(c) Obiectul CBOR/COSE rezultat se comprimă în conformitate cu punctul 1 litera (d) din prezenta anexă. Sarcina utilă a codului QR constă în prefixul „EP1:MDOC:”, urmat de seria de octeți comprimați rezultată, iar sarcina utilă completă se codifică utilizând modul de octeți sub forma unui singur segment de date în codul QR.

Conținutul datelor constă într-un subset de date vizibile din câmpurile de pe fața cardului enumerate în anexa II la Directiva (UE) 2024/2841 (data expirării, numărul de serie al cardului), împreună cu identificatorul de revocare, semnătura electronică și informații privind schema.

Semnătura electronică conține:

(i) issuerAuth – un obiect COSE_Sign1 semnat cu **cheia privată QSealC** a autorității emitente;

(ii) antet protejat care include alg = ES256 (algoritm de semnătură) și x5t (parametrul antetului hash al certificatului COSE X.509).

5. Date opționale

În codul QR nu se includ date opționale.

6. Identificatorul de revocare (RID)

Identificatorul de revocare al EPC este conform cu punctul 6 din anexa I.

Listele de revocare pentru EPC-urile revocate fac trimitere numai la RID. Numerele de serie ale cardurilor nu se publică în listele de revocare.

7. Sarcina utilă CBOR (în interiorul codului QR) a EPC

În sarcina utilă QR se includ numai următoarele date, care sunt în concordanță cu câmpurile cardului EPC vizibile prevăzute în anexa II la Directiva (UE) 2024/2841:

Câmp	**Calea mDOC**	**Tip/Format**
Versiunea schemei de date	issuerSigned.nameSpaces.„eu.epc”.ver	Șir (de exemplu, „1.0”)
Tipul cardului: EPC	docType	Enum („eu.epc”)
Numărul de serie al cardului	issuerSigned.nameSpaces.„eu.epc”.sub	Șir
Identificator de revocare	issuerSigned.nameSpaces.„eu.epc”.rid	CBOR bstr (16 octeți)

Data expirării cardului	issuerSigned.nameSpaces.„eu.epc”.exp	Eticheta CBOR 1004, astfel cum este definită în RFC 8943 (secțiunea 2.1), conținând un șir de text UTF-8 care reprezintă o dată completă conform RFC 3339 în format AAAA-LL-ZZ.

Semnătura electronică se stochează în issuerAuth (un obiect COSE_Sign1). Lanțul de certificate nu se integrează în sarcina utilă a codului QR; în schimb, antetul protejat COSE include x5t, o amprentă a certificatului utilizată pentru a localiza QSealC corespunzător în registrul de încredere stocat în memoria cache a verificatorului.

8. Exemplu de sarcină utilă a codului QR al EPC: reprezentare logică comentată de tipul JavaScript Object Notation

Următorul exemplu este o reprezentare JavaScript Object Notation (JSON – notarea obiectelor în JavaScript) lizibilă pentru om a vizualizării logice a EPC. În practică, această structură nu trebuie să fie lizibilă pentru om, deoarece este:

(a) codificată în CBOR (RFC 8949, secțiunea 3);

(b) este semnată utilizând structura COSE_Sign1 neetichetată, cu o sarcină utilă detașată (RFC 9052, secțiunea 4.),

(c) include data expirării ca etichetă CBOR 1004, valoarea datei complete, în conformitate cu RFC 8943 (secțiunea 2.1);

(d) include parametrul antetului protejat x5t în conformitate cu RFC 9360, utilizând SHA-256 pe entitatea finală QSealC codificată în DER; și

(e) este comprimată și prefixată cu șirul EP1:MDOC: înainte de a fi codificată în codul QR.

```
{
 // Numai vizualizare logică lizibilă pentru om a EPC, de tip JSON.
```

// Sarcina utilă efectivă a codului QR este în format CBOR determinist, nu JSON.

„docType”: „eu.epc”, // acreditare EPC. Valoarea docType este inclusă, împreună cu

//issuerSigned, în sarcina utilă externă COSE_Sign1.

„issuerSigned”: {

// Date protejate de issuerAuth; utilizate ca sarcină utilă detașată.

// Pentru generarea și verificarea semnăturii, sarcina utilă externă detașată acoperă atât

// docType, cât și issuerSigned.

„nameSpaces”: {

„eu.epc”: {

„ver”: „1.0”, // versiunea profilului/schemei codului QR

// Numărul de serie al cardului; definit de emitent, maximum 24 de caractere.

„sub”: „EF123456789012345678 90GH”,

// Identificator de revocare: CBOR bstr efectiv, 16 octeți/128 de biți.

// reprezentat aici sub formă de 32 de caractere hexadecimale pentru lizibilitate.

„rid”: „4a8d9c11223344556677 8899aabbccdd”,

// Codificarea CBOR efectivă utilizează eticheta 1004 pentru data completă conform RFC 3339.

„exp”: „31-12-2030”

}

}

},

„issuerAuth”: {

// Forma efectivă: COSE_Sign1 neetichetată, nu un obiect JSON.

„type”: „COSE_Sign1”,

„tagged”: fals, // codificat fără eticheta CBOR COSE_Sign1

„payload”: „detached”, // câmpul sarcinii utile COSE este CBOR null

„protectedHeader”: {

// alg: ES256; parametrul antetului COSE echivalent 1 = -7.

„alg”: „ES256”,

// x5t: amprenta certificatului; parametrul antetului COSE 34.

„x5t”: {

„hashAlg”: „SHA-256”, // valoarea hash COSE echivalentă -16

// hash SHA-256 al entității finale QSealC codificate în DER.

// 32 de octeți reprezentați de 64 de caractere hexadecimale.

„hashValue”:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

},

„unprotectedHeader”: {}, // gol în acest exemplu

// semnătură COSE ES256: 64 de octeți = 128 de caractere hexadecimale.

„signature”:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

}

9. Utilizarea mecanismelor criptografice

Utilizarea mecanismelor criptografice în contextul prezentei anexe este în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

ANEXA III

NOTIFICAREA INFORMAȚIILOR MENȚIONATE LA ARTICOLUL 6 ALINEATUL (2)

1. Statele membre furnizează Comisiei următoarele informații cu privire la fiecare autoritate sau organism competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități:

   (a) denumirea autorității sau a organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (b) numărul de înregistrare al autorității sau al organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (c) adresa de e-mail și numărul de telefon de contact ale autorității sau ale organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (d) unul sau mai multe certificate care pot fi utilizate pentru a verifica sigiliul electronic creat de autoritatea sau organismul competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități pe care le emite și pentru care datele de identitate certificate includ numele și numărul de înregistrare al emitentului, astfel cum se precizează la litera (a) și, respectiv, la litera (b);

   (e) adresa URL a site-ului pe care emitentul publică statutul valabilității versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități.

2. Statele membre pot furniza Comisiei următoarele informații cu privire la fiecare autoritate sau organism competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități:

   (a) adresa URL a paginii web care conține politicile și condițiile autorității sau ale organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități care se aplică furnizării și utilizării versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități pe care le furnizează;

   (b) după caz, adresa URL a paginii web care conține informații suplimentare cu privire la autoritatea sau organismul competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități.

ANEXA IV

SPECIFICAȚII TEHNICE PRIVIND LISTA DE REVOCARE PENTRU VERSIUNILE FIZICE ALE CARDULUI EUROPEAN PENTRU DIZABILITATE SAU ALE CARDULUI EUROPEAN DE PARCARE PENTRU PERSOANELE CU DIZABILITĂȚI

1. În sensul prezentei anexe, identificatorul corespunde identificatorului de revocare (RID) definit la punctul 6 din anexa I și la punctul 6 din anexa II.

2. O listă de revocare se implementează sub forma unui token de tip „listă de identificatori” în format CWT (RFC 8392, secțiunea 7), în conformitate cu clauza 5.2 din specificația listei privind statutul tokenurilor (draft-ietf-oauth-status-list-14), cu următoarele modificări:

   (a) valoarea revendicării de tip este „application/identifierlist+cwt”;

   (b) este prezentă revendicarea privind termenul de expirare;

   (c) revendicarea StatusList nu este prezentă în setul de revendicări CWT;

   (d) structura IdentifierList definită la punctul 3 este prezentă ca revendicare în setul de revendicări CWT, utilizând cheia 65530;

   (e) CWT este un obiect COSE_Sign1 care utilizează, pentru calcularea semnăturii, un algoritm de semnătură în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA);

   (f) CWT conține parametrul x5chain, astfel cum este definit în RFC 9360 (secțiunea 2), în antetul protejat care conține certificatul sau lanțul de certificate pentru a verifica semnătura listei de revocare;

   (g) OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor (draft-ietf-oauth-status-list-14) poate fi utilizat pentru certificatul de semnare a listei de identificatori și se recomandă ca verificatorii să accepte OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor și ca infrastructurile autorităților emitente să nu considere câmpul de utilizare extinsă a cheii ca fiind critic atunci când utilizează OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor.

3. Structura IdentifierList este o structură CBOR cu următorul limbaj de definire a datelor concise (*Concise Data Definition Language* – CDDL):

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

IdentifierInfo = {
```

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

Identifier = bstr

Aggregation_uri = tstr
```