Raad van de
Europese Unie

Brussel, 10 juli 2026
(OR. en)

11772/26
ADD 1

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

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	1 juli 2026
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	C(2026) 4534 annex
Betreft:	BIJLAGEN bij GEDELEGEERDE VERORDENING (EU) .../... VAN DE COMMISSIE tot aanvulling van Richtlijn (EU) 2024/2841 wat betreft het bepalen van de QR-code op de fysieke versie van de Europese kaart voor personen met een handicap en het bepalen van de QR-code op de fysieke versie van de Europese parkeerkaart voor personen met een handicap en het vaststellen van gemeenschappelijke technische specificaties die de beveiliging van de fysieke versie van de Europese parkeerkaart voor personen met een handicap waarborgen, alsook interoperabiliteitskwesties

EUROPESE
COMMISSIE

Brussel, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

BIJLAGEN

bij

GEDELEGEERDE VERORDENING (EU) .../... VAN DE COMMISSIE

tot aanvulling van Richtlijn (EU) 2024/2841 wat betreft het bepalen van de QR-code op de fysieke versie van de Europese kaart voor personen met een handicap en het bepalen van de QR-code op de fysieke versie van de Europese parkeerkaart voor personen met een handicap en het vaststellen van gemeenschappelijke technische specificaties die de beveiliging van de fysieke versie van de Europese parkeerkaart voor personen met een handicap waarborgen, alsook interoperabiliteitskwesties

BIJLAGE I

SPECIFICATIES VAN DE QR-CODE VOOR DE FYSIEKE VERSIE VAN DE EUROPESE GEHANDICAPTENKAART

1. **Format van de QR-code voor de fysieke versie van de Europese kaart voor personen met een handicap (European Disability Card, EDC)**

a) **Format QR-code Model 2**, overeenkomstig de internationale QR-codespecificaties ISO/IEC 18004:2024 of gelijkwaardig.

b) **Foutcorrectieniveau M** (15 % redundantie), waardoor een gedrukte QR-code bestand is tegen krassen of gedeeltelijke beschadiging.

c) **Coderingsmodus:** De QR-payload bestaat uit de gecombineerde structuur van de issuerSigned Concise Binary Object Representation (CBOR) en het overeenkomstige issuerAuth COSE_Sign1-handtekeningobject zoals gedefinieerd in CBOR object signing and encryption (COSE, RFC 9052 punten 3.1, 4.2 en 4.4), volgens het mDOC-gegevensmodelpatroon voor issuerSigned items, maar aangepast voor statisch gebruik op fysieke kaarten. De issuerAuth moet een COSE_Sign1-object zijn met alg = ES256 en een beschermde header die x5t bevat (de hashheaderparameter van het COSE X.509-certificaat zoals gedefinieerd in RFC 9360 (punt 2); met het oog op interoperabiliteit is het in x5t gebruikte hashalgoritme SHA-256).

d) Voordat de QR-code wordt gecodeerd, wordt het gecombineerde CBOR/COSE-object **gecomprimeerd in ZLIB-format** (RFC 1950, punt 2.2) **met het deflate-algoritme** (RFC 1951, punten 3.2 en 4). De resulterende gecomprimeerde byte-array wordt gecodeerd in **QR-code Byte Mode**, zodat de binaire CBOR/COSE-payloads en de interoperabiliteit van de scanner volledig worden ondersteund.

Voor alle tekstvelden die in de QR-payload zijn opgenomen, coderen uitgevende instellingen tekens als Unicode UTF-8 in CBOR-tekststrings. Transliteratie wordt niet toegepast op ondertekende payloadgegevens. Met het oog op interoperabiliteit passen uitgevende instellingen vóór ondertekening Unicode Normalisation Form C (NFC) toe op alle tekstvelden.

e) **Voorvoegsel:** De QR-string van de EDC begint met “ED1:MDOC:”. Dit identificeert het kaarttype en het codeerprofiel. Voorvoegsels zijn hoofdlettergevoelig en moeten aanwezig zijn. Onbekende of niet-ondersteunde voorvoegsels worden afgekeurd. Het voorvoegsel en de gecomprimeerde payload worden in de QR-code gecodeerd als één datasegment in Byte Mode.

f) **Minimale modulegrootte ≥ 0,25 mm** om de leesbaarheid op gedrukte kaarten te waarborgen.

g) **Maximaal versie 20;** met maximaal 97 × 97 modules aan beide zijden.

2. **Specificaties voor het aanmaken van EDC-handtekeningen**

Het gekwalificeerde elektronische zegel (QSeal) dat wordt gebruikt om EDC-QR-codes te verzegelen, waarborgt dat de gecodeerde gegevens afkomstig zijn van de bevoegde autoriteit van afgifte en niet zijn gewijzigd.

a) **Algoritme van de handtekening:** Het handtekeningalgoritme is ES256 (Elliptische krommealgoritme voor digitale handtekening — Elliptic Curve Digital Signature

Algorithm (ECDSA) met SHA-256 met de P-256-curve), zoals gedefinieerd in RFC 9053 (punt 2.1); in COSE wordt het algoritme geïdentificeerd aan de hand van de alg-headerparameter in RFC 9052 (punt 3.1).

b) **Ondertekeningssleutel:** De QR-payload wordt ondertekend met behulp van de privésleutel die overeenkomt met een gekwalificeerd certificaat voor elektronische zegels (QSealC).

c) **COSE-structuur:** De drager van de handtekening moet een COSE_Sign1-object zijn. De beschermde header bevat alg (ES256) en x5t (de hashheaderparameter van het COSE X.509-certificaat zoals gedefinieerd in RFC 9360 (punt 2)); met het oog op interoperabiliteit is het in x5t gebruikte hashalgoritme SHA-256). De verificatie is gebaseerd op het gebruik van de x5t-waarde om het overeenkomstige certificaat te lokaliseren in het vertrouwensarchief in de lokale cache van de verificateur dat is opgebouwd op basis van informatie uit de vertrouwenslijst, en valideert vervolgens de certificaatketen en de certificaatstatus overeenkomstig het eIDAS-vertrouwenskader.

d) **Handtekeningstandaard**: De payload van de QR-code wordt ondertekend als een COSE_Sign1-object overeenkomstig RFC 9052 (punt 4), CBOR Object Signing and Encryption. Het COSE_Sign1-object wordt meegenomen in issuerAuth en gecodeerd zonder de CBOR-tag voor COSE_Sign1. Het payloadveld van het COSE_Sign1-object moet worden losgemaakt en gecodeerd als CBOR null. Voor het genereren en verifiëren van handtekeningen is de externe payload de deterministisch CBOR-gecodeerde structuur met de docType-waarde en de issuerSigned-waarde van de CBOR-toplevelmap.

e) **Hashalgoritme**: SHA-256 wordt gebruikt als onderdeel van ES256 voor het genereren van handtekeningen en het verifiëren van de integriteit.

f) **Codering:** De payload wordt gecodeerd met behulp van CBOR (RFC 8949, punt 4.2), zoals vereist door de COSE- en mDOC-specificaties, waarbij de codering en reproduceerbaarheid van de ondertekende gegevens wordt gewaarborgd.

3. **Specificaties voor het drukken**

a) **Stille zone:** De QR-code wordt aan alle zijden omgeven door een duidelijke marge van **4 modules**, zonder gedrukte tekst, patroon of achtergrond.

b) **Contrast**: De QR-code wordt gedrukt op een witte achtergrond, met een minimale contrastverhouding van **4:1**, om een hoge leesbaarheid onder wisselende verlichtingsomstandigheden te waarborgen.

c) De QR-code wordt gedrukt in de in bijlage I bij Richtlijn (EU) 2024/2841 gedefinieerde kleur, zodat het contrast maximaal is.

d) **Plaatsing en grootte:** De QR-code, inclusief de stille zone, moet 26,25 mm × 26,25 mm bedragen en zich op de achterzijde van de kaart rechts onderaan bevinden. De QR-code is maximaal versie 20 (modules van 97 × 97), met een modulegrootte van 0,25 mm of groter.

De QR-code, inclusief de stille zone, moet ten minste 5 mm van de rechterrand en ten minste 5 mm van de onderrand van de kaart worden geplaatst.

4. **Gegevens in de QR-code van de EDC**

De QR-code bevat een minimale, offline verifieerbare gegevensset overeenkomstig het beginsel van minimale gegevensverwerking van artikel 5, lid 1, punt c), van Verordening (EU) 2016/679. De payloadstructuur is als volgt:

a) Kaartattributen worden in CBOR gecodeerd binnen een issuerSigned-object.

b) De structuur wordt ingepakt en ondertekend door het QSeal van de autoriteit van afgifte als een issuerAuth (COSE_Sign1, ES256, met inbegrip van x5t, de hashheaderparameter van het COSE X.509-certificaat).

c) Het resulterende CBOR/COSE-object wordt gecomprimeerd overeenkomstig punt 1, d), van deze bijlage. De payload van de QR-code bestaat uit het voorvoegsel "ED1:MDOC:", gevolgd door de resulterende gecomprimeerde byte-array, en de volledige payload wordt gecodeerd met Byte Mode als één datasegment van de QR-code.

De inhoud van de gegevens bestaat uit een subset van zichtbare gegevens uit de in bijlage I bij Richtlijn (EU) 2024/2841 genoemde velden aan de voorkant van de kaart (voornaam, achternaam, serienummer van de kaart, vervaldatum), samen met de identificatiecode voor intrekking, de elektronische handtekening en de schema-informatie.

De **elektronische handtekening** bevat:

i) issuerAuth — een COSE_Sign1-object ondertekend met de **QSealC-privésleutel** van de autoriteit van afgifte;

ii) beschermde header met alg = ES256 (handtekeningalgoritme) en x5t (de hashheaderparameter van het COSE X.509-certificaat).

5. **Facultatieve gegevens**

In de QR-code mogen geen facultatieve gegevens worden opgenomen.

6. **Identificatiecode voor intrekking**

Naast het zichtbare serienummer van de kaart moet de QR-code een specifieke identificatiecode voor intrekking (Revocation Identifier, RID) bevatten.

De RID wordt gebruikt voor het bepalen van de intrekkingsstatus en voor het beheer van de intrekkingslijsten. De RID mag niet op de kaart worden afgedrukt en mag niet aan de kaartverificateurs worden getoond.

6.1. *Voorschriften voor de RID*

De RID:

a) wordt opgenomen in de ondertekende QR-payload;

b) is uniek, ten minste binnen het domein van uitgifte van de autoriteit van afgifte;

c) wordt niet op de kaart afgedrukt en is niet bedoeld om leesbaar te zijn voor de mens;

d) onthult geen persoonsgegevens en heeft geen directe betekenis;

e) kan niet rechtstreeks worden afgeleid van het zichtbare serienummer van de kaart; en

f) is cryptografisch gebonden aan de QR-payload door het gekwalificeerde elektronische zegel.

6.2. *Formaat en grootte van de RID*

De RID wordt gecodeerd als een CBOR-bytestring (bstr). De RID is 16 bytes (128 bits) lang.

De RID wordt gegenereerd door de autoriteit van afgifte met behulp van een methode die onder haar controle staat en die voldoende entropie en resistentie tegen raden of opsommen waarborgt.

6.3. *Intrekkingslijsten*

Voor verificatiedoeleinden gepubliceerde intrekkingslijsten verwijzen alleen naar de RID van ingetrokken kaarten. Serienummers van kaarten worden niet gepubliceerd in intrekkingslijsten.

7. CBOR-payload (binnen de QR-code) van de EDC

Alleen de volgende gegevens worden opgenomen in de QR-payload, in overeenstemming met de zichtbare EDC-gegevensvelden die zijn vastgesteld in bijlage I bij Richtlijn (EU) 2024/2841.

Inhoud van het hoogste niveau:

a) docType = “eu.edc”

b) issuerSigned.nameSpaces.“eu.edc” met de attributen die in de volgende tabel worden weergegeven

c) issuerAuth = COSE_Sign1 (QSeal)

Veld	**mDOC-pad**	**Type/format**
Versie van het gegevensschema	issuerSigned.nameSpaces.“eu.edc”.ver	String (bv. “1.0”)
Kaarttype: EDC	docType	Enum (“eu.edc”)
Serienummer van de kaart	issuerSigned.nameSpaces.“eu.edc”.sub	String
Identificatiecode voor intrekking	issuerSigned.nameSpaces.“eu.edc”.rid	CBOR bstr (16 bytes)
Voornaam van de kaarthouder	issuerSigned.nameSpaces.“eu.edc”.givenName	Unicode-tekststring (UTF-8)
Achternaam van de kaarthouder	issuerSigned.nameSpaces.“eu.edc”.familyName	Unicode-tekststring (UTF-8)

Datum waarop de geldigheidsduur van de kaart verstrijkt	issuerSigned.nameSpaces.“eu.edc”.exp	CBOR-tag 1004, zoals gedefinieerd in RFC 8943 (punt 2.1), met een UTF-8-tekststring die een RFC 3339 full-date weergeeft in formaat JJJJ-MM-DD.

De elektronische handtekening wordt meegenomen in issuerAuth (een COSE_Sign1-object). De certificaatketen wordt niet ingebed in de payload van de QR-code; in plaats daarvan bevat de beschermde COSE-header x5t, een duimafdruk van het certificaat die wordt gebruikt om de overeenkomstige QSealC te vinden in het vertrouwensarchief in de cache van de verificateur.

8. **Voorbeeld van de payload van de QR-code van een EDC: becommentarieerde logische weergave in de stijl JavaScript Object Notation**

Het volgende voorbeeld is een voor mensen leesbare JSON-weergave (JavaScript Object Notation) van een logische view van een EDC. In de praktijk is deze structuur niet leesbaar voor de mens, aangezien zij:

a) gecodeerd moet zijn in CBOR (RFC 8949, punt 3);

b) ondertekend moet zijn met gebruikmaking van een niet-getagde COSE_Sign1-structuur met een losgemaakte payload (RFC 9052, punt 4),

c) de vervaldatum moet vermelden als een CBOR-tag 1004 full-date-waarde overeenkomstig RFC 8943 (punt 2.1);

d) de x5t-protected-headerparameter moet bevatten overeenkomstig RFC 9360, waarbij SHA-256 wordt gebruikt over de DER-gecodeerde end-entity QSealC; en

e) moet worden gecomprimeerd en als voorvoegsel de string ED1: MDOC: moet krijgen alvorens te worden gecodeerd in de QR-code.

```
{
 //alleen door mensen leesbare logische weergave van het EDC in JSON-stijl.
 //De werkelijke QR-payload is deterministisch-CBOR, niet JSON.
 “docType”: "eu.edc", // EDC credential. De docType-waarde wordt opgenomen, samen met
  //issuerSigned, in de externe payload COSE_Sign.

 “issuerSigned”: {
  //Gegevens beschermd door issuerAuth; gebruikt als losgemaakte payload.
  //Voor het genereren en verifiëren van handtekeningen dekt de losgemaakte externe payload beide
  // docType and issuerSigned.
  “nameSpaces”: {
   “eu.edc”: {
    “ver”: “1.0”, // QR-profiel/schemaversie

    // Serienummer van de kaart, door de afgever gedefinieerd, max. 24 tekens.
    “sub”: “AB123456789012345678 90CD”,
```

```
    // Identificatiecode voor intrekking: feitelijke CBOR bstr., 16 bytes/128 bits.
    //Hier weergegeven als 32 hex-tekens voor de leesbaarheid.
    "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

    "givenName": "Ann",//voornaam gedrukt op het EDC
    "familyName": "Other",//achternaam gedrukt op het EDC

    //Feitelijke CBOR-codering maakt gebruik van tag 1004 voor full date RFC 3339.
    "exp": "2030-12-31"
   }
  }
},

"issuerAuth": {
 //Feitelijke vorm: niet-getagde COSE_Sign1, geen JSON-object.
 "type": "COSE_Sign1",
 "tagged": fout, ......//gecodeerd zonder COSE_Sign1 CBOR-tag
 "payload": "detached",//COSE payload-veld is CBOR null

 "protectedHeader": {
  // alg: ES256; equivalente COSE-headerparameter 1 = -7.
  "alg": "ES256",

  // x5t: duimafdruk van het certificaat; COSE-headerparameter 34.
  "x5t": {
   "hashAlg": "SHA-256", // equivalente COSE-hashwaarde -16
```

//SHA-256 hash van met DER-gecodeerde end-entity QSealC.

//32 bytes weergegeven als 64 hex-tekens.

“hashValue”:
“0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

},

“unprotectedHeader”: {} ,// Leeg in dit voorbeeld

// ES256 COSE-handtekening: 64 bytes = 128 hex-tekens.

“signature”:
“0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”

}

}

9. Gebruik van cryptografische mechanismen

Het gebruik van cryptografische mechanismen in het kader van deze bijlage is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) gepubliceerde “Agreed Cryptographic Mechanisms”.

BIJLAGE II

SPECIFICATIES VAN DE QR-CODE VOOR DE FYSIEKE VERSIE VAN DE EUROPESE PARKEERKAART VOOR PERSONEN MET EEN HANDICAP

1. **Format van de QR-code op de fysieke versie van de Europese parkeerkaart voor personen met een handicap ("European Parking Card", EPC)**

a) **Format QR-code Model 2**, overeenkomstig de internationale QR-codespecificaties ISO/IEC 18004:2024 of gelijkwaardig.

b) **Foutcorrectieniveau M** (15 % redundantie), waardoor een gedrukte QR-code bestand is tegen krassen of gedeeltelijke beschadiging.

c) **Coderingsmodus:** De QR-payload bestaat uit de gecombineerde structuur van de issuerSigned Concise Binary Object Representation (CBOR) en het overeenkomstige issuerAuth COSE_Sign1-handtekeningobject zoals gedefinieerd in CBOR object signing and encryption (COSE, RFC 9052 punten 3.1, 4.2 en 4.4), volgens het mDOC-gegevensmodelpatroon voor issuerSigned items, maar aangepast voor statisch gebruik op fysieke kaarten. De issuerAuth moet een COSE_Sign1-object zijn met alg = ES256 en een beschermde header die x5t bevat (de hashheaderparameter van het COSE X.509-certificaat zoals gedefinieerd in RFC 9360 (punt 2); met het oog op interoperabiliteit is het in x5t gebruikte hashalgoritme SHA-256).

d) Voordat de QR-code wordt gecodeerd, wordt het gecombineerde CBOR/COSE-object **gecomprimeerd in ZLIB-format (RFC 1950, punt 2.2) met het deflate-algoritme** (RFC 1951, punten 3.2 en 4). De resulterende gecomprimeerde byte-array wordt gecodeerd in **QR-code Byte Mode**, zodat de binaire CBOR/COSE-payloads en de interoperabiliteit van de scanner volledig worden ondersteund.

Voor alle tekstvelden die in de QR-payload zijn opgenomen, coderen uitgevende instellingen tekens als Unicode UTF-8 in CBOR-tekststrings. Transliteratie wordt niet toegepast op ondertekende payloadgegevens. Met het oog op interoperabiliteit passen uitgevende instellingen vóór ondertekening Unicode Normalisation Form C (NFC) toe op alle tekstvelden.

e) **Voorvoegsel**: De QR-string van de Europese parkeerkaart voor personen met een handicap begint met "EP1:MDOC:". Dit identificeert het kaarttype en het codeerprofiel. Voorvoegsels zijn hoofdlettergevoelig en moeten aanwezig zijn. Onbekende of niet-ondersteunde voorvoegsels worden afgekeurd. Het voorvoegsel en de gecomprimeerde payload worden in de QR-code gecodeerd als één datasegment in Byte Mode.

f) **Minimale modulegrootte ≥ 0,35 mm** om de leesbaarheid op gedrukte kaarten te waarborgen.

g) **Maximaal versie 20**; met maximaal 97 x 97 modules aan beide zijden.

2. **Specificaties voor het aanmaken van EPC-handtekeningen**

Het gekwalificeerde elektronische zegel (QSeal) dat wordt gebruikt om EPC-QR-codes te verzegelen, waarborgt dat de gecodeerde gegevens afkomstig zijn van de bevoegde autoriteit van afgifte en niet zijn gewijzigd.

a) **Algoritme van de handtekening:** Het handtekeningalgoritme is ES256 (ECDSA met SHA-256 met de P-256-curve), zoals gedefinieerd in RFC 9053 (punt 2.1); in

COSE wordt het algoritme geïdentificeerd aan de hand van de alg-headerparameter in RFC 9052 (punt 3.1).

b) **Ondertekeningssleutel:** De QR-payload wordt ondertekend met behulp van de privésleutel die overeenkomt met een gekwalificeerd certificaat voor elektronische zegels (QSealC).

c) **COSE-structuur**: De drager van de handtekening moet een COSE_Sign1-object zijn. De beschermde header bevat alg (ES256) en x5t (de hashheaderparameter van het COSE X.509-certificaat zoals gedefinieerd in RFC 9360 (punt 2)); met het oog op interoperabiliteit is het in x5t gebruikte hashalgoritme SHA-256). De verificatie is gebaseerd op het gebruik van de x5t-waarde om het overeenkomstige certificaat te lokaliseren in het vertrouwensarchief in de lokale cache van de verificateur dat is opgebouwd op basis van informatie uit de vertrouwenslijst, en valideert vervolgens de certificaatketen en de certificaatstatus overeenkomstig het eIDAS-vertrouwenskader.

d) **Handtekeningstandaard**: De payload van de QR-code wordt ondertekend als een COSE_Sign1-object overeenkomstig RFC 9052 (punt 4), CBOR Object Signing and Encryption. Het COSE_Sign1-object wordt meegenomen in issuerAuth en gecodeerd zonder de CBOR-tag voor COSE_Sign1. Het payloadveld van het COSE_Sign1-object moet worden losgemaakt en gecodeerd als CBOR null. Voor het genereren en verifiëren van handtekeningen is de externe payload de deterministisch CBOR-gecodeerde structuur met de docType-waarde en de issuerSigned-waarde van de CBOR-toplevelmap.

e) **Hashalgoritme**: SHA-256 wordt gebruikt als onderdeel van ES256 voor het genereren van handtekeningen en het verifiëren van de integriteit.

f) **Codering:** De payload wordt gecodeerd met behulp van CBOR (RFC 8949, punt 4.2), zoals vereist door de COSE- en mDOC-specificaties, waarbij de codering en reproduceerbaarheid van de ondertekende gegevens wordt gewaarborgd.

3. **Specificaties voor het drukken**

a) **Stille zone:** De QR-code wordt aan alle zijden omgeven door een duidelijke marge van **4 modules**, zonder gedrukte tekst, patroon of achtergrond.

b) **Contrast**: De QR-code wordt gedrukt op een witte achtergrond, met een minimale contrastverhouding van **4:1**, om een hoge leesbaarheid onder wisselende verlichtingsomstandigheden te waarborgen.

c) De QR-code wordt gedrukt in de in bijlage I bij Richtlijn (EU) 2024/2841 gedefinieerde kleur, zodat het contrast maximaal is.

d) **Plaatsing en grootte:** De QR-code, inclusief de stille zone, moet **37 mm** x **37 mm** bedragen en zich op de voorzijde van de kaart, iets rechts van het midden, richting de onderrand bevinden. De QR-code is maximaal versie 20 (modules van 97 × 97), met een modulegrootte van 0,35 mm of groter.

De QR-code, inclusief de stille zone, moet ten minste 5 mm van de onderrand van de kaart worden geplaatst.

4. **Gegevens in de QR-code van de Europese parkeerkaart**

De QR-code bevat een minimale, offline verifieerbare gegevensset overeenkomstig het beginsel van minimale gegevensverwerking zoals vervat in artikel 5, lid 1, punt c), van Verordening (EU) 2016/679. De payloadstructuur is als volgt:

a) Kaartattributen worden in CBOR gecodeerd binnen een issuerSigned-object.

b) Deze structuur wordt ingepakt en ondertekend door het QSeal van de autoriteit van afgifte als een issuerAuth (COSE_Sign1, ES256, met inbegrip van x5t, de hashheaderparameter van het COSE X.509-certificaat).

c) Het resulterende CBOR/COSE-object wordt gecomprimeerd overeenkomstig punt 1, d), van deze bijlage. De payload van de QR-code bestaat uit het voorvoegsel "EP1:MDOC:", gevolgd door de resulterende gecomprimeerde byte-array, en de volledige payload wordt gecodeerd met Byte Mode als één datasegment van de QR-code.

De inhoud van de gegevens bestaat uit een subset van zichtbare gegevens uit de in bijlage II bij Richtlijn (EU) 2024/2841 genoemde velden aan de voorkant van de kaart (vervaldatum, serienummer van de kaart), samen met de identificatiecode voor intrekking, de elektronische handtekening en de schema-informatie.

De **elektronische handtekening** bevat:

i) issuerAuth — een COSE_Sign1-object ondertekend met de **QSealC-privésleutel** van de autoriteit van afgifte;

ii) beschermde header met alg = ES256 (handtekeningalgoritme) en x5t (de hashheaderparameter van het COSE X.509-certificaat).

5. **Facultatieve gegevens**

In de QR-code mogen geen facultatieve gegevens worden opgenomen.

6. **Identificatiecode voor intrekking**

De identificatiecode voor intrekking van de Europese parkeerkaart voldoet aan punt 6 van bijlage I.

Intrekkingslijsten van ingetrokken Europese parkeerkaarten verwijzen alleen naar de RID. Serienummers van kaarten worden niet gepubliceerd in intrekkingslijsten.

7. **CBOR-payload (binnen de QR) van de Europese parkeerkaart**

Alleen de volgende gegevens worden opgenomen in de QR-payload, in overeenstemming met de zichtbare gegevensvelden van de Europese parkeerkaart die zijn vastgesteld in bijlage II bij Richtlijn (EU) 2024/2841:

Veld	**mDOC-pad**	**Type/format**
Versie van het gegevensschema	issuerSigned.nameSpaces."eu.epc".ver	String (bv. "1.0")
Kaarttype:	docType	Enum

Europese parkeerkaart		(“eu.epc”)
Serienummer van de kaart	issuerSigned.nameSpaces.“eu.epc”.sub	String
Identificatiecode voor intrekking	issuerSigned.nameSpaces.“eu.epc”.rid	CBOR bstr (16 bytes)
Datum waarop de geldigheidsduur van de kaart verstrijkt	issuerSigned.nameSpaces.“eu.epc”.exp	CBOR-tag 1004, zoals gedefinieerd in RFC 8943 (punt 2.1), met een UTF-8-tekststring die een RFC 3339 full-date weergeeft in formaat JJJJ-MM-DD.

De elektronische handtekening wordt meegenomen in issuerAuth (een COSE_Sign1-object). De certificaatketen wordt niet ingebed in de payload van de QR-code; in plaats daarvan bevat de beschermde COSE-header x5t, een duimafdruk van het certificaat die wordt gebruikt om de overeenkomstige QSealC te vinden in het vertrouwensarchief in de cache van de verificateur.

8. Voorbeeld van de payload van de QR-code van een EPC: becommentarieerde logische weergave in de stijl JavaScript Object Notation

Het volgende voorbeeld is een voor mensen leesbare JSON-weergave (JavaScript Object Notation) van een logische view van een EPC. In de praktijk is deze structuur niet leesbaar voor de mens, aangezien zij:

a) gecodeerd is in CBOR (RFC 8949, punt 3),

b) ondertekend moet zijn met gebruikmaking van een niet-getagde COSE_Sign1-structuur met een losgemaakte payload (RFC 9052, punt 4),

c) de vervaldatum moet vermelden als een CBOR-tag 1004 full-date-waarde overeenkomstig RFC 8943 (punt 2.1);

d) de x5t-protected-headerparameter moet bevatten overeenkomstig RFC 9360, waarbij SHA-256 wordt gebruikt over de DER-gecodeerde end-entity QSealC; en

e) moet worden gecomprimeerd en als voorvoegsel de string EP1: MDOC: moet krijgen alvorens te worden gecodeerd in de QR-code.

```
{
 //alleen door mensen leesbare logische weergave van het EPC in JSON-stijl.
 //De werkelijke QR-payload is deterministisch-CBOR, niet JSON.
 “docType”: “eu.epc”, // EPC credential. De docType-waarde wordt opgenomen, samen met
  //issuerSigned, in de externe payload COSE_Sign.

 “issuerSigned”: {
  //Gegevens beschermd door issuerAuth; gebruikt als losgemaakte payload.
 //Voor het genereren en verifiëren van handtekeningen dekt de losgemaakte externe payload beide
  // docType and issuerSigned.
  “nameSpaces”: {
   “eu.epc”: {
    “ver”: “1.0”, // QR-profiel/schemaversie

    // Serienummer van de kaart, door de afgever gedefinieerd, max. 24 tekens.
    “sub”: “EF123456789012345678 90GH”,

    // Identificatiecode voor intrekking: feitelijke CBOR bstr., 16 bytes/128 bits.
    //Hier weergegeven als 32 hex-tekens voor de leesbaarheid.
    “rid”: “4a8d9c112233445566778899aabbccdd”,

    //Feitelijke CBOR-codering maakt gebruik van tag 1004 voor full date RFC 3339.
    “exp”: “2030-12-31”
   }
  }
 },
```

```
  “issuerAuth”: {
    //Feitelijke vorm: niet-getagde COSE_Sign1, geen JSON-object.
    “type”: “COSE_Sign1”,
    “tagged”: fout, ......//gecodeerd zonder COSE_Sign1 CBOR-tag
    “payload”: “detached”,//COSE payload-veld is CBOR null

    “protectedHeader”: {
      // alg: ES256; equivalente COSE-headerparameter 1 = -7.
      “alg”: “ES256”,

      // x5t: duimafdruk van het certificaat; COSE-headerparameter 34.
      “x5t”: {
        “hashAlg”: “SHA-256”, // equivalente COSE-hashwaarde -16

        //SHA-256 hash van met DER-gecodeerde end-entity QSealC.
        //32 bytes weergegeven als 64 hex-tekens.
        “hashValue”:
“0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”
      }
    },

    “unprotectedHeader”: {} ,// Leeg in dit voorbeeld

    // ES256 COSE-handtekening: 64 bytes = 128 hex-tekens.
    “signature”:
“0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef”
  }
```

}

9. Gebruik van cryptografische mechanismen

Het gebruik van cryptografische mechanismen in het kader van deze bijlage is in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) gepubliceerde “Agreed Cryptographic Mechanisms”.

BIJLAGE III

KENNISGEVING VAN INFORMATIE BEDOELD IN ARTIKEL 6, LID 2

1. De lidstaten verstrekken de volgende informatie aan de Commissie over elke bevoegde autoriteit die of elk bevoegd orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese kaart voor personen met een handicap of de Europese parkeerkaart voor personen met een handicap:

   a) de naam van de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap;

   b) een registratienummer van de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap;

   c) het e-mailadres en het telefoonnummer van de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart en de Europese parkeerkaart voor personen met een handicap;

   d) een of meer certificaten die kunnen worden gebruikt om het elektronische zegel te verifiëren dat is aangemaakt door de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap, en waarvoor de gecertificeerde identiteitsgegevens de naam en het registratienummer van de instantie van afgifte bevatten, zoals gespecificeerd in respectievelijk de punten a) en b);

   e) de URL van de locatie waar de instantie van afgifte de geldigheidsstatus van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap publiceert.

2. De lidstaten kunnen de volgende informatie aan de Commissie verstrekken over elke bevoegde autoriteit die of elk bevoegd orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap:

   a) de URL van de webpagina met de beleidslijnen en voorwaarden van de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart of de Europese parkeerkaart voor personen met een handicap die van toepassing zijn op de verstrekking en het gebruik van de fysieke versies van de Europese gehandicaptenkaart en de Europese parkeerkaart voor personen met een handicap die door de autoriteit of het orgaan wordt verstrekt;

   b) waar van toepassing, de URL van de webpagina met aanvullende informatie over de bevoegde autoriteit die of het bevoegde orgaan dat verantwoordelijk is voor de afgifte van de fysieke versies van de Europese gehandicaptenkaart en de Europese parkeerkaart voor personen met een handicap.

BIJLAGE IV

TECHNISCHE SPECIFICATIES VOOR EEN INTREKKINGSLIJST VOOR DE FYSIEKE VERSIES VAN DE EUROPESE KAART VOOR PERSONEN MET EEN HANDICAP OF DE EUROPESE PARKEERKAART VOOR PERSONEN MET EEN HANDICAP

1. Voor de toepassing van deze bijlage komt de identificatiecode overeen met de in bijlage I, punt 6, en bijlage II, punt 6, gedefinieerde identificatiecode voor intrekking (RID).

2. Een intrekkingslijst wordt geïmplementeerd als een identificatielijst-token in CWT-format (RFC 8392, punt 7) overeenkomstig clausule 5.2 van de specificatie van de tokenstatuslijst (draft-ietf-oauth-status-list-14) met de volgende wijzigingen:

   a) de waarde van de typeclaim is “application/identifierlist+cwt”;

   b) de vervaltijd-claim is aanwezig;

   c) de StatusList-claim is niet aanwezig in de CWT-claimset;

   d) de in punt 3 gedefinieerde structuur van de IdentifierList is als een claim aanwezig in de CWT-claimset met behulp van sleutel 65530;

   e) de CWT is een COSE_Sign1-object dat voor het berekenen van de handtekening gebruikmaakt van een handtekeningalgoritme in overeenstemming met de door de Europese Groep voor cyberbeveiligingscertificering goedgekeurde en door het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) gepubliceerde “Agreed Cryptographic Mechanisms”;

   f) de CWT bevat de x5chain-parameter zoals gedefinieerd in RFC 9360 (punt 2) in de beschermde header die het certificaat of de keten van certificaten bevat om de handtekening van de intrekkingslijst te verifiëren;

   g) de Extended Key Usage-OID die in de specificatie van de tokenstatuslijst is vermeld (draft-ietf-oauth-status-list-14) kan worden gebruikt voor het ondertekeningscertificaat van de identificatielijst en het wordt aanbevolen dat verificateurs de Extended Key Usage-OID zoals vermeld in de specificatie van de tokenstatuslijst ondersteunen en dat de infrastructuren van de autoriteit van afgifte het veld voor Extended Key Usage niet kritiek maken bij het gebruik van de Extended Key Usage-OID zoals vermeld in de specificatie van de tokenstatuslijst.

3. De structuur van de IdentifierList is een CBOR-structuur met de volgende Concise Data Definition Language (CDDL):

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

IdentifierInfo = {
```

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

Identifier = bstr

Aggregation_uri = tstr
```