Rådet for
Den Europæiske Union

Bruxelles, den 10. juli 2026
(OR. en)

11772/26
ADD 1

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

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	1. juli 2026
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	C(2026) 4534 annex
Vedr.:	BILAG til KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/… om supplerende regler til direktiv (EU) 2024/2841 for så vidt angår QR-koden på den fysiske udgave af EU-handicapkortet og QR-koden på og de fælles tekniske specifikationer til sikring af den fysiske udgave af EU-parkeringskortet for personer med handicap samt interoperabilitetsaspekter

EUROPA-
KOMMISSIONEN

Bruxelles, den 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

BILAG

til

KOMMISSIONENS DELEGEREDE FORORDNING (EU) …/…

om supplerende regler til direktiv (EU) 2024/2841 for så vidt angår QR-koden på den fysiske udgave af EU-handicapkortet og QR-koden på og de fælles tekniske specifikationer til sikring af den fysiske udgave af EU-parkeringskortet for personer med handicap samt interoperabilitetsaspekter

BILAG I

SPECIFIKATIONER FOR QR-KODEN PÅ DEN FYSISKE UDGAVE AF EU-HANDICAPKORTET

1. Formatet for QR-koden på den fysiske udgave af EU-handicapkortet

(a) **Formatet for en QR-kode af Model 2** skal være i overensstemmelse med de internationale QR-kodespecifikationer ISO/IEC 18004: 2024 eller tilsvarende.

(b) Der kræves **Error Correction Level M** (fejl ved korrektionsniveau M) (15 % redundans), hvilket sikrer modstandsdygtighed over for ridser eller delvis beskadigelse af en trykt QR-kode.

(c) **Encoding Mode (indkodningsmodus):** QR payload'en (QR-informationsfeltet) skal bestå af den kombinerede struktur issuerSigned Concise Binary Object Representation (CBOR) og det tilsvarende issuerAuth COSE_Sign1-signatur-objekt som defineret i CBOR Object Signing and Encryption (COSE, RFC 9052, afdeling 3.1, 4.2 og 4.4), der følger mDOC data-modelmønstret for issuerSigned-elementer, men er tilpasset statisk brug af fysiske kort. IssuerAuth skal være et COSE_Sign1-objekt med alg = ES256 og en beskyttet header, der indeholder x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256).

(d) Inden indkodning af QR-koden **komprimeres det kombinerede CBOR/COSE-objekt ved hjælp af zlib-formatet** (RFC 1950, afdeling 2.2) **med deflatoralgoritmen** (RFC 1951, afdeling 3.2 og 4). Den komprimerede byte-array skal indkodes i **QR code Byte Mode**, hvilket sikrer fuld støtte til de binære CBOR/COSE-informationsfelter og scannerinteroperabilitet.

Udstederne skal for alle tekstfelter i QR-informationsfeltet indkode tegn som Unicode UTF-8 i CBOR-tekststrenge. Der må ikke anvendes translitteration på underskrevne data i informationsfelterne. Af hensyn til interoperabiliteten skal udstederne anvende Unicode Normalisation Form C (NFC) på alle tekstfelter, inden de underskriver.

(e) **Præfiks:** QR-strengen for EU-handicapkort begynder med "ED1: MDOC:". Dette identificerer korttype og indkodningsprofil. I præfikserne skelnes der mellem store og små skrifttegn, og de skal angives. Ukendte eller ikke-understøttede præfikser skal medføre afvisning. Præfikset og det komprimerede informationsfelt skal indkodes i QR-koden som ét enkelt Byte Mode-datasegment.

(f) Den **mindste modulstørrelse er ≥ 0,25 mm** for at sikre læsbarheden på trykte kort.

(g) **Maksimumversion 20** med op til 97 × 97 moduler på hver side.

2. Specifikationer for generering af underskrift på EU-handicapkort

Det kvalificerede elektroniske segl (QSeal), der anvendes til at forsegle QR-koder i EU-handicapkort, sikrer, at de indkodede data stammer fra den godkendte udstedende myndighed og ikke er blevet ændret.

(a) **Underskriftsalgoritme**: Underskriftsalgoritmen skal være ES256 (Elliptic Curve Digital Signature Algorithm (ECDSA) (digital underskriftsalgoritme med elliptisk

kurve (ECDSA)) med SHA-256 ved hjælp af P-256-kurven som defineret i RFC 9053 (afdeling 2.1); i COSE identificeres algoritmen ved algheaderparameteren i RFC 9052 (afdeling 3.1).

(b) **Signing Key** (signeringsnøgle): QR-informationsfeltet skal underskrives ved hjælp af den private nøgle, der svarer til et kvalificeret certifikat for elektronisk segl (QSealC).

(c) **COSE-struktur:** Signaturcontaineren skal være et objekt af typen COSE_Sign1. Den beskyttede header skal omfatte en alg (ES256) og x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256). Kontrollen skal baseres på anvendelsen af x5t-værdien til at lokalisere det tilsvarende certifikat i kontrollørens lokalt cachede tillidslager (trust store), der består af oplysninger fra positivlisten, hvorefter certifikatkæden og certifikatstatus skal valideres i overensstemmelse med eIDAS-tillidsrammen.

(d) **Underskrift - standard**: QR-kodens informationsfelt skal underskrives som et COSE_Sign1-objekt i overensstemmelse med RFC 9052 (afdeling 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet skal forefindes i issuerAuth og indkodes uden et CBOR-tag til COSE_Sign1. COSE_Sign1-objektets informationsfelt skal være særskilt og indkodes som CBOR null. Det eksterne informationsfelt skal med henblik på generering og kontrol af underskrift være den deterministiske CBOR-indkodede struktur, der indeholder docType-værdien og issuerSigned-værdien fra topniveau-CBOR-map-strukturen.

(e) **Hashalgoritme**: SHA-256 anvendes som en del af ES256 til generering af underskrifter og integritetskontrol.

(f) **Indkodning**: Informationsfeltet skal indkodes ved hjælp af CBOR (RFC 8949, afdeling 4.2) som krævet i COSE- og mDOC-specifikationerne, hvilket sikrer indkodning og reproducerbarhed af de underskrevne data.

3. Trykningsspecifikationer

(a) **Quiet Zone** (tomt område): QR-koden skal være omgivet af en tom margen på **4 moduler** på alle sider uden tryk, mønster eller baggrund.

(b) **Kontrast**: QR-koden skal trykkes på hvid baggrund med et kontrastforhold på mindst **4:1** for at sikre høj læsbarhed under forskellige lysforhold.

(c) QR-koden skal trykkes i den farve, der er defineret i bilag I til direktiv (EU) 2024/2841, og som sikrer størst mulig kontrast.

(d) **Placering og størrelse**: QR-koden, inklusive det tomme område, skal være 26,25 mm × 26,25 mm og skal forefindes på bagsiden af kortet i nederste højre hjørne. QR-koden må højst være version 20 (97 × 97 moduler) med en modulstørrelse på 0,25 mm eller derover.

QR-koden, inklusive det tomme område, skal forefindes mindst 5 mm fra kortets højre kant og mindst 5 mm fra kortets nederste kant.

4. Data i QR-koden på EU-handicapkort

QR-koden skal indeholde et minimumsdatasæt, der kan kontrolleres offline, jf. princippet om dataminimering som fastsat i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679. Strukturen for informationsfeltet skal være som følger:

(a) Kortattributter indkodes i CBOR i et issuerSigned-objekt.

(b) Strukturen indpakkes og underskrives ved hjælp af den udstedende myndigheds QSeal i form af en issuerAuth (COSE_Sign1, ES256, herunder x5t, COSE X.509-certifikatets hashheaderparameter).

(c) Det deraf følgende CBOR/COSE-objekt skal komprimeres i overensstemmelse med dette bilags punkt 1, litra d). QR-kodens informationsfelt skal bestå af præfikset "ED1:MDOC:" efterfulgt af den deraf følgende komprimerede byte-array, og det komplette informationsfelt skal indkodes ved brug af Byte Mode som ét enkelt QR-kodedatasegment.

Dataindholdet skal bestå af en undergruppe af synlige data fra de felter på kortets forside, der er opført i bilag I til direktiv (EU) 2024/2841 (fornavn, efternavn, kortets serienummer, udløbsdato), sammen med inddragelsesidentifikatoren, den elektroniske underskrift og skemaoplysningerne.

Den **elektroniske underskrift** skal indeholde:

i) et issuerAuth — Et COSE_Sign1-objekt, der er underskrevet med den udstedende myndigheds QSeal-privatnøgle (**QSealC private key**)

ii) en beskyttet header, der omfatter en alg = ES256 (signaturalgoritme) og x5t (COSE X.509-certifikatets hashheaderparameter).

5. Valgfrie data

QR-koden må ikke indeholde valgfrie data.

6. Inddragelsesidentifikator (Revocation Identifier -— RID)

Ud over kortets synlige serienummer skal QR-koden indeholde en særlig inddragelsesidentifikator (RID).

RID'en anvendes til at fastslå inddragelsesstatus og til forvaltning af listen over inddragne kort. RID'en må ikke trykkes på kortet og må ikke være synlig for kortkontrollørerne.

6.1. *Krav til RID'en*

RID'en:

(a) skal indgå i det underskrevne QR-informationsfelt

(b) skal være entydig, som minimum inden for den udstedende myndigheds udstedelsesdomæne

(c) må ikke trykkes på kortet og ikke være beregnet til at være menneskeligt læsbar

(d) må ikke afsløre personoplysninger og må ikke være umiddelbart forståelig

(e) må ikke kunne udledes direkte af kortets synlige serienummer og

(f) skal være kryptografisk knyttet til QR-informationsfeltet ved hjælp af det kvalificerede elektroniske segl.

6.2. *RID'ens format og størrelse*

RID'en skal indkodes som en CBOR-byte-streng (bstr). RID'en skal være 16 byte (128 bit) lang.

RID'en skal genereres af den udstedende myndighed ved hjælp af en metode, som denne har kontrol over, og som sikrer tilstrækkelig entropi og modstandsdygtighed over for gætteri eller optælling.

6.3. *Lister over inddragne kort*

I de lister over inddragne kort, der offentliggøres med henblik på kontrol, må der kun henvises til RID'en for inddragne kort. Kortenes serienumre må ikke offentliggøres i lister over inddragne kort.

7. CBOR-informationsfeltet (inden for QR-koden) på EU-handicapkort

Alene følgende data må medtages i QR-informationsfeltet i overensstemmelse med EU-handicapkortets synlige datafelter som fastsat i bilag I til direktiv (EU) 2024/2841.

Indhold på øverste niveau:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces."eu.edc" med attributter som vist i tabellen nedenfor

(c) issuerAuth = COSE_Sign1 (QSeal)

Felt	**mDOC path**	**Type/format**
Dataskemaversion	issuerSigned.nameSpaces."eu.edc".ver	Streng (f.eks. "1.0")
Korttype: EDC (EU-handicapkort)	docType	Enum ("eu.edc")
Kortets serienummer	issuerSigned.nameSpaces."eu.edc".sub	Streng
Inddragelsesidentifikator	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 byte)
Kortindehaverens fornavn	issuerSigned.nameSpaces."eu.edc".givenName	Unicode-tekststreng (UTF-8)
Kortindehaverens efternavn	issuerSigned.nameSpaces."eu.edc".familyName	Unicode-tekststreng (UTF-8)
Kortets udløbsdato	issuerSigned.nameSpaces."eu.edc".exp	CBOR-tag af typen 1004 som defineret i RFC 8943

		(afdeling 2.1), der indeholder en UTF-8-tekststreng, der repræsenterer en fuldstændig RFC 3339-dato (full-date) angivet i formatet ÅÅÅÅ-MM-DD.

Den elektroniske signatur forefindes i issuerAuth (et COSE_Sign1-objekt). Certifikatkæden må ikke være indlejret i QR-kodens informationsfelt; i stedet skal den beskyttede COSE-header indeholde x5t, et certifikat med thumbprint, der bruges til at lokalisere det dertil svarende QSealC i kontrollørens trustlager i cachen.

8. **Eksempel på QR-kodens informationsfelt på EU-parkeringskort: logisk præsentation i JavaScript Object Notation-stil med kommentarer**

Følgende eksempel er en menneskeligt læsbar JavaScript Object Notation (JSON)-gengivelse af den logiske præsentation af EU-handicapkortet. I praksis må denne struktur ikke være menneskeligt læsbar, da den skal:

(a) være indkodet i CBOR (RFC 8949, afdeling 3)

b) være underskrevet ved hjælp af en COSE_Sign1-struktur uden tag med et særskilt informationsfelt (RFC 9052, afdeling 4.)

c) indeholde udløbsdatoen som et CBOR-tag af typen 1004 med full-date-værdi i overensstemmelse med RFC 8943 (afdeling 2.1)

d) indeholde den x5t-beskyttede headerparameter i overensstemmelse med RFC 9360, idet der bruges SHA-256 hen over det DER-indkodede end-entity QSealC og

e) være komprimeret og forsynet med præfiksstrengen ED1:MDOC: før den indkodes i QR-koden.

```
{
 // JSON-style, kun menneskeligt læsbar logisk præsentation af EU-handicapkortet.
 // Det faktiske QR-informationsfelt er en deterministisk simulation af CBOR, ikke JSON.
 "docType": "eu.edc", // EU-handicapkort-credential. DocType-værdien er sammen med
  //issuerSigned indeholdt i det eksterne COSE_Sign1-informationsfelt.

 "issuerSigned": {
  // Data, der er beskyttet af issuerAuth; bruges som et særskilt informationsfelt.
  // Det særskilte eksterne informationsfelt dækker både generering og kontrol af underskrift
  // docType og issuerSigned.
  "nameSpaces": {
   "eu.edc": {
    "ver": "1.0", // QR-profil/skemaversion

    // Kortets serienummer, issuer-defined, maks. 24 tegn.
    "sub": "AB123456789012345678 90CD",
```

```
      // Inddragelsesidentifikator: faktisk CBOR bstr, 16 byte/128 bit.
      // Vist her som 32 hex-tegn af hensyn til læsbarheden.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Jens", // det fornavn, der er trykt på EU-handicapkortet
      "familyName": "Jensen", // det efternavn, der er trykt på EU-handicapkortet

      // Ved den faktiske CBOR-indkodning bruges tagget af typen 1004 med henblik på angivelse af en fuldstændig RFC 3339-dato (full date).
      "exp": "2030-12-31"
    }
   }
 },

 "issuerAuth": {
  // Faktisk format: COSE_Sign1 uden tag, ikke et JSON-objekt.
  "type": "COSE_Sign1",
  "tagged": falsk, // indkodet uden COSE_Sign1 CBOR-tag
  "payload": "detached", // COSE-informationsfeltet er CBOR null

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

   // x5t: certifkat-thumbprint; COSE-headerparameter 34.
   "x5t": {
    "hashAlg": "SHA-256", // tilsvarende COSE-hashværdi -16
```

```
        // SHA-256-hashfunktionen af det DER-indkodede end-entity QSealC.
        // 32 byte, der repræsenteres ved 64 hex-tegn.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // tom i dette eksempel

    // ES256 COSE-signatur: 64 byte = 128 hex-tegn.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. Brug af kryptografiske mekanismer

Anvendelsen af kryptografiske mekanismer i forbindelse med dette bilag skal ske i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

BILAG II

SPECIFIKATIONER FOR QR-KODEN PÅ DEN FYSISKE UDGAVE AF EU-PARKERINGSKORTET FOR PERSONER MED HANDICAP

1. **Formatet for QR-koden på den fysiske udgave af EU-parkeringskort for personer med handicap**

(a) **Formatet for en QR-kode af Model 2** skal være i overensstemmelse med de internationale QR-kodespecifikationer ISO/IEC 18004: 2024 eller tilsvarende.

(b) Der kræves **Error Correction Level M** (fejl ved korrektionsniveau M) (15 % redundans), hvilket sikrer modstandsdygtighed over for ridser eller delvis beskadigelse af en trykt QR-kode.

(c) **Encoding Mode (indkodningsmodus):** QR payload'en (QR-informationsfeltet) skal bestå af den kombinerede struktur issuerSigned Concise Binary Object Representation (CBOR) og det tilsvarende issuerAuth COSE_Sign1-signatur-objekt som defineret i CBOR Object Signing and Encryption (COSE, RFC 9052, afdeling 3.1, 4.2 og 4.4), der følger mDOC data-modelmønstret for issuerSigned-elementer, men er tilpasset statisk brug af fysiske kort. IssuerAuth skal være et COSE_Sign1-objekt med alg = ES256 og en beskyttet header, der indeholder x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256).

(d) Inden indkodning af QR-koden **komprimeres det kombinerede CBOR/COSE-objekt ved hjælp af zlib-formatet (RFC 1950, afdeling 2.2) med deflatoralgoritmen** (RFC 1951, afdeling 3.2 og 4). Den således komprimerede byte-array skal indkodes i **QR code Byte Mode**, hvilket sikrer fuld støtte til de binære CBOR/COSE-informationsfelter og scannerinteroperabilitet.

Udstederne skal for alle tekstfelter i QR-informationsfeltet indkode tegn som Unicode UTF-8 i CBOR-tekststrenge. Der må ikke anvendes translitteration på underskrevne data i informationsfelterne. Af hensyn til interoperabiliteten skal udstederne anvende Unicode Normalisation Form C (NFC) på alle tekstfelter, inden de underskriver.

(e) **Præfiks**: QR-strengen for EU-parkeringskort begynder med "EP1:MDOC:". Dette identificerer korttype og indkodningsprofil. I præfikserne skelnes der mellem store og små skrifttegn, og de skal angives. Ukendte eller ikke-understøttede præfikser skal medføre afvisning. Præfikset og det komprimerede informationsfelt skal indkodes i QR-koden som ét enkelt Byte Mode-datasegment.

(f) Den **mindste modulstørrelse er ≥ 0,35 mm** for at sikre læsbarheden på trykte kort.

(g) **Maximumversion 20** med op til 97 x 97 moduler på hver side.

2. **Specifikationer for generering af underskrift på EU-parkeringskort**

Det kvalificerede elektroniske segl (QSeal), der anvendes til at forsegle QR-koder i EU-parkeringskort, sikrer, at de indkodede data stammer fra den godkendte udstedende myndighed og ikke er blevet ændret.

(a) **Underskriftsalgoritme**: Underskriftsalgoritmen skal være ES256 (ECDSA med SHA-256 ved hjælp af P-256-kurven) som defineret i RFC 9053 (afdeling 2.1); i COSE identificeres algoritmen ved algheaderparameteren i RFC 9052 (afdeling 3.1).

(b) **Signing Key** (signeringsnøgle): QR-informationsfeltet skal underskrives ved hjælp af den private nøgle, der svarer til et kvalificeret certifikat for elektronisk segl (QSealC).

(c) **COSE-struktur**: Signaturcontaineren skal være et objekt af typen COSE_Sign1. Den beskyttede header skal omfatte en alg (ES256) og x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256). Kontrollen skal baseres på anvendelsen af x5t-værdien til at lokalisere det tilsvarende certifikat i kontrollørens lokalt cachede tillidslager (trust store), der består af oplysninger fra positivlisten, hvorefter certifikatkæden og certifikatstatus skal valideres i overensstemmelse med eIDAS-tillidsrammen.

(d) **Underskrift - standard**: QR-kodens informationsfelt skal underskrives som et COSE_Sign1-objekt i overensstemmelse med RFC 9052 (afdeling 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet skal forefindes i issuerAuth og indkodes uden et CBOR-tag til COSE_Sign1. COSE_Sign1-objektets informationsfelt skal være særskilt og indkodes som CBOR null. Det eksterne informationsfelt skal med henblik på generering og kontrol af underskrift være den deterministiske CBOR-indkodede CBOR-struktur, der indeholder docType-værdien og issuerSigned-værdien fra topniveau-CBOR-map-strukturen.

(e) **Hashalgoritme**: SHA-256 anvendes som en del af ES256 til generering af underskrifter og integritetskontrol.

(f) **Indkodning**: Informationsfeltet skal indkodes ved hjælp af CBOR (RFC 8949, afdeling 4.2) som krævet i COSE- og mDOC-specifikationerne, hvilket sikrer indkodning og reproducerbarhed af de underskrevne data.

3. **Trykningsspecifikationer**

(a) **Quiet Zone** (tomt område): QR-koden skal være omgivet af en tom margen på **4 moduler** på alle sider uden tryk, mønster eller baggrund.

(b) **Kontrast**: QR-koden skal trykkes på hvid baggrund med et kontrastforhold på mindst **4:1** for at sikre høj læsbarhed under forskellige lysforhold.

(c) QR-koden skal trykkes i den farve, der er defineret i bilag II til direktiv (EU) 2024/2841, og som sikrer størst mulig kontrast.

(d) **Placering og størrelse:** QR-koden, inklusive det tomme område, skal være **37 mm × 37 mm** og skal forefindes på forsiden af kortet, lidt til højre for midten, nederst på kortet. QR-koden må højst være version 20 (97 × 97 moduler) med en modulstørrelse på 0,35 mm eller derover.

QR-koden, inklusive det tomme område, skal forefindes mindst 5 mm fra kortets nederste kant.

4. **Data i QR-koden på EU-parkeringskort**

QR-koden skal indeholde et minimumsdatasæt, der kan kontrolleres offline, jf. princippet om dataminimering som fastsat i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679. Informationsfeltets struktur er som følger:

(a) Kortattributter indkodes i CBOR i et issuerSigned-objekt.

(b) Strukturen indpakkes og underskrives ved hjælp af den udstedende myndigheds QSeal i form af en issuerAuth (COSE_Sign1, ES256, herunder x5t, COSE X.509-certifikatets hashheaderparameter).

(c) Det deraf følgende CBOR/COSE-objekt skal komprimeres i overensstemmelse med dette bilags punkt 1, litra d). QR-kodens informationsfelt skal bestå af præfikset "EP1:MDOC:" efterfulgt af den deraf følgende komprimerede byte-array, og det komplette informationsfelt skal indkodes ved brug af Byte Mode som ét enkelt QR-kodedatasegment.

Dataindholdet skal bestå af en undergruppe af synlige data fra de felter på kortets forside, der er opført i bilag II til direktiv (EU) 2024/2841 (udløbsdato, kortets serienummer), sammen med inddragelsesidentifikatoren, den elektroniske underskrift og skemaoplysningerne.

Den **elektroniske underskrift** skal indeholde:

i) et issuerAuth — Et COSE_Sign1-objekt, der er underskrevet med den udstedende myndigheds QSeal-privatnøgle (**QSealC private key**)

ii) En beskyttet header, der omfatter en alg = ES256 (signaturalgoritme) og x5t (COSE X.509-certifikatets hashheaderparameter).

5. Valgfrie data

QR-koden må ikke indeholde valgfrie data.

6. Inddragelsesidentifikator (Revocation Identifier -— RID)

Inddragelsesidentifikatoren i EU-parkeringskortet skal være i overensstemmelse med bilag I, punkt 6.

I listerne over inddragne EU-parkeringskort må der kun henvises til RID'en. Kortenes serienumre må ikke offentliggøres i lister over inddragne kort.

7. CBOR-informationsfeltet (inden for QR-koden) på EU-parkeringskort

Alene følgende data må medtages i QR-informationsfeltet, hvilket er i overensstemmelse med EU-handicapkortets synlige datafelter som fastsat i bilag II til direktiv (EU) 2024/2841:

Felt	**mDOC path**	**Type/format**
Dataskemaversion	issuerSigned.nameSpaces."eu.epc".ver	Streng (f.eks. "1.0")
Korttype: EPC (EU-parkeringskort)	docType	Enum ("eu.epc")
Kortets serienummer	issuerSigned.nameSpaces."eu.epc".sub	Streng

Inddragelsesidentifikator	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 byte)
Kortets udløbsdato	issuerSigned.nameSpaces."eu.epc".exp	CBOR-tag af typen 1004 som defineret i RFC 8943 (afdeling 2.1), der indeholder en UTF-8-tekststreng, der repræsenterer en fuldstændig RFC 3339-dato (full-date) angivet i formatet ÅÅÅÅ-MM-DD.

Den elektroniske signatur skal forefindes i issuerAuth (et COSE_Sign1-objekt). Certifikatkæden må ikke være indlejret i QR-kodens informationsfelt; i stedet skal den beskyttede COSE-header indeholde x5t, et certifikat med thumbprint, der bruges til at lokalisere det dertil svarende QSealC i kontrollørens trustlager i cachen.

8. Eksempel på QR-kodens informationsfelt på EU-parkeringskort: logisk præsentation i JavaScript Object Notation-stil med kommentarer

Følgende eksempel er en menneskeligt læsbar JavaScript Object Notation (JSON)-gengivelse af den logiske præsentation af EU-parkeringskortet. I praksis må denne struktur ikke være menneskeligt læsbar, da den skal:

(a) være indkodet i CBOR (RFC 8949, afdeling 3)

(b) være underskrevet ved hjælp af en COSE_Sign1-struktur uden tag med et særskilt informationsfelt (RFC 9052, afdeling 4.)

(c) indeholde udløbsdatoen som et CBOR-tag af typen 1004 med full-date-værdi i overensstemmelse med RFC 8943 (afdeling 2.1)

(d) indeholde den x5t-beskyttede headerparameter i overensstemmelse med RFC 9360, idet der bruges SHA-256 hen over det DER-indkodede end-entity QSealC og

(e) være komprimeret og forsynet med præfiksstrengen EP1:MDOC: før den indkodes i QR-koden.

```
{
 // JSON-style, kun menneskeligt læsbar logisk præsentation af EU-parkeringskortet.
 // Det faktiske QR-informationsfelt er en deterministisk simulation af CBOR, ikke JSON.
 "docType": "eu.epc", // EU-parkeringskort-credential. DocType-værdien er sammen med
   //issuerSigned indeholdt i det eksterne COSE_Sign1-informationsfelt.

 "issuerSigned": {
   // Data, der er beskyttet af issuerAuth; bruges som et særskilt informationsfelt.
   // Det særskilte eksterne informationsfelt dækker både generering og kontrol af underskrift
   // docType og issuerSigned.
   "nameSpaces": {
     "eu.epc": {
       "ver": "1.0", // QR-profil/skemaversion

       // Kortets serienummer, issuer-defined, maks. 24 tegn.
       "sub": "EF123456789012345678 90GH",

       // Inddragelsesidentifikator: faktisk CBOR bstr, 16 byte/128 bit.
       // Vist her som 32 hex-tegn af hensyn til læsbarheden.
       "rid": "4a8d9c112233445566778899aabbccdd",

       // Ved den faktiske CBOR-indkodning bruges tagget af typen 1004 med henblik på
angivelse af en fuldstændig RFC 3339-dato (full date).
       "exp": "2030-12-31"
     }
   }
 },
```

```
 "issuerAuth": {
  // Faktisk format: COSE_Sign1 uden tag, ikke et JSON-objekt.
  "type": "COSE_Sign1",
  "tagged": falsk, // indkodet uden COSE_Sign1 CBOR-tag
  "payload": "detached", // COSE-informationsfeltet er CBOR null

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

   // x5t: certifkat-thumbprint; COSE-headerparameter 34.
   "x5t": {
    "hashAlg": "SHA-256", // tilsvarende COSE-hashværdi -16

    // SHA-256-hashfunktionen af det DER-indkodede end-entity QSealC.
    // 32 byte, der repræsenteres ved 64 hex-tegn.
    "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // tom i dette eksempel

  // ES256 COSE-signatur: 64 byte = 128 hex-tegn.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
```

}

}

9. Brug af kryptografiske mekanismer

Anvendelsen af kryptografiske mekanismer i forbindelse med dette bilag skal ske i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

BILAG III

MEDDELELSE AF DE OPLYSNINGER, DER ER OMHANDLET I ARTIKEL 6, STK. 2

1. Medlemsstaterne meddeler Kommissionen følgende oplysninger om hver af de kompetente myndigheder eller organer, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap:

   (a) navnet på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   (b) registreringsnummeret på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   (c) e-mailadressen og telefonnummeret på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   (d) et eller flere certifikater, der kan anvendes til at kontrollere det elektroniske segl, der er genereret af den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet eller EU-parkeringskortet for personer med handicap, og for hvilke de certificerede identitetsdata omfatter udstederens navn og registreringsnummer, jf. henholdsvis litra a) og b)

   (e) den URL, hvor udstederen offentliggør oplysninger om gyldighedsstatus for de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap.

2. Medlemsstaterne kan meddele Kommissionen følgende oplysninger om hver af de kompetente myndigheder eller hvert af de kompetente organer, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap:

   (a) URL'en på den webside, der indeholder de politikker, vilkår og betingelser, der finder anvendelse på leveringen og brugen af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, som udstedes af den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af disse kort

   (b) hvis det er relevant, URL'en på den webside, der indeholder yderligere oplysninger om den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap.

BILAG IV

TEKNISKE SPECIFIKATIONER FOR INDDRAGELSESLISTEN OVER DE FYSISKE UDGAVER AF EU-HANDICAPKORTET ELLER EU-PARKERINGSKORTET FOR PERSONER MED HANDICAP

1. Med henblik på dette bilag skal identifikatoren svare til den inddragelsesidentifikator (RID), der er defineret i bilag I, punkt 6, og bilag II, punkt 6.

2. Der opstilles en liste over inddragne kort i form af en identifikatorliste-token (identifier list token) i CWT-format (RFC 8392, afdeling 7) i overensstemmelse med punkt 5.2 i "token status list specification" (draft-ietf-oauth-status-list-14) med følgende ændringer:

   (a) Værdien af typekravet skal være "application/identifierlist+cwt"

   (b) Kravet "udløbstidspunkt" (expiration time claim) skal forefindes

   (c) Der må ikke forefindes et StatusListe-krav i CWT-kravene

   (d) Identikatorliste-strukturen, der er defineret i punkt 3, skal være til stede som et krav i de CWT-krav, der er fastsat ved hjælp af 65530-nøglen

   (e) CWT'en skal være et COSE_Sign1-objekt, der med henblik på beregning af underskriften bruger en underskriftsalgoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)

   (f) CWT'en skal med henblik på kontrol af underskriften på listen over inddragne kort indeholde den x5chain-parameter, der er defineret i RFC 9360 (afdeling 2), i den beskyttede header, der indeholder certifikatet eller kæden af certifikater

   (g) den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten (draft-ietf-oauth-status-list-14), kan anvendes til certifikatet til underskrivelse af identifikatorlisten, og det anbefales, at kontrollørerne understøtter den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten, og at den udstedende myndigheds infrastrukturer ikke sætter feltet for den udvidede nøgleanvendelses til kritisk, når de anvender den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten.

3. Identifikatorlistens struktur skal være en CBOR-struktur med følgende Concise Data Definition Language (CDDL):

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

IdentifierInfo = {
```

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

Identifier = bstr

Aggregation_uri = tstr
```