Europeiska unionens råd

Bryssel den 10 juli 2026
(OR. en)

11772/26
ADD 1

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

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	1 juli 2026
till:	Thérèse BLANCHET, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	C(2026) 4534 annex
Ärende:	BILAGOR till KOMMISSIONENS DELEGERADE FÖRORDNING (EU) .../... om komplettering av direktiv (EU) 2024/2841 vad gäller fastställande av QR-koden på den fysiska versionen av EU-intyget om funktionsnedsättning och fastställande av QR-koden och av gemensamma tekniska specifikationer som säkerställer säkerheten för den fysiska versionen av EU-parkeringstillståndet för personer med funktionsnedsättning samt interoperabilitetsfrågor

EUROPEISKA
KOMMISSIONEN

Bryssel den 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

BILAGOR

till

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) .../...

om komplettering av direktiv (EU) 2024/2841 vad gäller fastställande av QR-koden på den fysiska versionen av EU-intyget om funktionsnedsättning och fastställande av QR-koden och av gemensamma tekniska specifikationer som säkerställer säkerheten för den fysiska versionen av EU-parkeringstillståndet för personer med funktionsnedsättning samt interoperabilitetsfrågor

BILAGA I

QR-KODSPECIFIKATIONER FÖR DEN FYSISKA VERSIONEN AV EU-INTYGET OM FUNKTIONSNEDSÄTTNING

1. **Format för QR-koden för den fysiska versionen av EU-intyget om funktionsnedsättning**

(a) **Format för QR-kod modell 2**, i enlighet med de internationella QR-kodspecifikationerna ISO/IEC 18004:2024 eller motsvarande.

(b) Felkorrigeringsnivå M (15 % redundans) som säkerställer motståndskraft mot repor eller partiell skada på en tryckt QR-kod.

(c) **Kodningsmetod:** QR-nyttolasten ska bestå av den kombinerade strukturen issuerSigned Concise Binary Object Representation (CBOR) och motsvarande signaturobjekt issuerAuth COSE_Sign1 enligt definitionen i CBOR Object Signing and Encryption (COSE, RFC 9052 avsnitt 3.1, 4.2 och 4.4), i enlighet med datamodellen mDOC för issuerSigned-delar, men anpassad till statisk användning av ett fysiskt intyg. issuerAuth ska vara ett COSE_Sign1-objekt med alg = ES256 och en skyddad rubrik som innehåller x5t (COSE X.509-certifikatets hashrubrikparameter som definieras i RFC 9360 [avsnitt 2]; i interoperabilitetssyfte ska den hashalgoritm som används i x5t vara SHA-256).

(d) Före QR-kodningen ska det kombinerade CBOR/COSE-objektet **komprimeras med hjälp av zlib-format** (RFC 1950, avsnitt 2.2) med algoritmen **Deflate** (RFC 1951, avsnitt 3.2 och 4). Den komprimerade bytesträng som uppstår härigenom ska kodas i **QR-kodbyteläge**, så att fullt stöd för binära CBOR/COSE-nyttolaster och skannerinteroperabilitet säkerställs.

För alla textfält som ingår i QR-nyttolasten ska utfärdare koda tecken som Unicode UTF-8 inom CBOR-textsträngar. Translitterering ska inte tillämpas på signerade nyttolastuppgifter. I interoperabilitetssyfte ska utfärdare tillämpa Unicode Normalisation Form C (NFC) på alla textfält före signering.

(e) **Prefix:** QR-strängen för EU-intyget om funktionsnedsättning ska börja med ”ED1:MDOC:”. Härigenom identifieras handlingens typ och kodningsprofilen. Prefixen är skiftlägeskänsliga och måste finnas med. Prefix som är okända eller saknar stöd ska resultera i avslag. Prefixet och den komprimerade nyttolasten ska kodas som ett enda bytelägedatasegment i QR-koden.

(f) **Minsta modulstorlek ≥ 0,25 mm** för att säkerställa läsbarhet på tryckta handlingar.

(g) **Max version 20** med upp till 97 × 97 moduler på respektive sida.

2. **Specifikationer för signaturgenerering för EU-intyget om funktionsnedsättning**

Den kvalificerade elektroniska stämpel (QSeal) som används för att stämpla QR-koder på EU-intyget för funktionsnedsättning säkerställer att de kodade uppgifterna kommer från den behöriga utfärdande myndigheten och inte har ändrats.

(a) **Signaturalgoritm**: Signaturalgoritmen ska vara ES256 (Elliptic Curve Digital Signature Algorithm [ECDSA] med SHA-256 och P-256-kurvan), enligt definitionen i RFC 9053 (avsnitt 2.1); i COSE identifieras algoritmen med hjälp av rubrikparametern alg i RFC 9052 (avsnitt 3.1).

(b) **Signeringsnyckel**: QR-nyttolasten ska signeras med hjälp av den privata nyckel som motsvarar ett kvalificerat certifikat för elektroniska stämplar (QSealC).

(c) **COSE-struktur:** Signaturbehållaren ska vara ett COSE_Sign1-objekt. Den skyddade rubriken ska innehålla alg (ES256) och x5t (COSE X.509-certifikatets hashrubrikparameter som definieras i RFC 9360 [avsnitt 2]; i interoperabilitetssyfte ska den hashalgoritm som används i x5t vara SHA-256). Kontrollen ska med hjälp av x5t-värdet lokalisera motsvarande certifikat i kontrollörens lokalt cachade trust store som bygger på information från förteckningar över betrodda tjänsteleverantörer och ska därefter validera certifikatkedjan och certifikatstatusen i enlighet med eIDAS-förordningens tillitsramverk.

(d) **Signaturstandard**: QR-kodnyttolasten ska signeras som ett COSE_Sign1-objekt i enlighet med RFC 9052 (avsnitt 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet ska finnas i issuerAuth och kodas utan CBOR-taggen för COSE_Sign1. COSE_Sign1-objektets nyttolastfält ska avskiljas och kodas som CBOR null. För generering och verifiering av signaturer ska den externa nyttolasten vara den deterministiska kodade CBOR-strukturen som innehåller docType-värdet och issuerSigned-värdet från CBOR-kartan på högsta nivå.

(e) **Hashalgoritm**: SHA-256 ska användas som en del av ES256 för signaturgenerering och integritetskontroll.

(f) **Kodning**: Nyttolasten ska kodas med hjälp av CBOR (RFC 8949, avsnitt 4.2), enligt kraven i COSE- och mDOC-specifikationerna, så att kodning och reproducerbarhet säkerställs för de signerade uppgifterna.

3. Specifikationer för tryckning

(a) **Ljusmarginal**: En tom marginal på **4 moduler** ska omge QR-koden på alla sidor, utan tryck, mönster eller bakgrund.

(b) **Kontrast**: QR-koden ska tryckas på vit bakgrund, varvid kontrastförhållandet ska vara minst **4:1**, så att hög läsbarhet säkerställs under olika ljusförhållanden.

(c) QR-koden ska tryckas med den färg som fastställs i bilaga I till direktiv (EU) 2024/2841 och som säkerställer maximal kontrast.

(d) **Placering och storlek**: QR-koden, inklusive ljusmarginalen, ska vara 26,25 mm × 26,25 mm och placeras på intygets baksida i nedre högra hörnet. QR-koden får högst vara version 20 (97 × 97 moduler), med en modulstorlek på minst 0,25 mm.

QR-koden, inklusive dess ljusmarginal, ska placeras minst 5 mm från intygets högra kant och minst 5 mm från intygets nedre kant.

4. Uppgifter i QR-koden på EU-intyget om funktionsnedsättning

QR-koden ska innehålla en så liten uppsättning som möjligt av uppgifter som går att kontrollera offline i enlighet med den princip om uppgiftsminimering som fastställs i artikel 5.1 c i förordning (EU) 2016/679. Nyttolaststrukturen ska vara följande:

(a) Intygsattribut kodas i CBOR inom ett issuerSigned-objekt.

(b) Strukturen inpackas och signeras av den utfärdande myndighetens QSeal som en issuerAuth (COSE_Sign1, ES256, inklusive x5t, COSE X.509-certifikatets hashrubrikparameter).

(c) Det CBOR/COSE-objekt som uppstår härigenom ska komprimeras i enlighet med punkt 1 d i denna bilaga. QR-kodnyttolasten ska bestå av prefixet ”ED1:MDOC:”, följt av den komprimerade bytesträng som uppstår, och den fullständiga nyttolasten ska kodas med byteläge som ett enda QR-koddatasegment.

Uppgiftsinnehållet ska bestå av en delmängd synliga data från de fält på intygets framsida som förtecknas i bilaga I till direktiv (EU) 2024/2841 (förnamn, efternamn, intygets serienummer, sista giltighetsdag), tillsammans med identifikatorn för återkallelse, den elektroniska signaturen och schemainformationen.

Den **elektroniska signaturen** ska innehålla följande:

i) Ett issuerAuth – ett COSE_Sign1-objekt signerat med den utfärdande myndighetens **privata QSealC-nyckel**.

ii) En skyddad rubrik som omfattar alg = ES256 (signaturalgoritm) och x5t (COSE X.509-certifikatets hashrubrikparameter).

5. Frivilliga uppgifter

Inga frivilliga uppgifter får inkluderas i QR-koden.

6. Identifikator för återkallelse (RID)

Utöver intygets synliga serienummer ska QR-koden innehålla en särskild identifikator för återkallelse (RID).

Denna identifikator ska användas för att fastställa återkallelsestatus och för hantering av förteckningar över återkallelser. Identifikatorn ska inte tryckas på intyget och ska inte visas för intygskontrollörerna.

6.1. *Krav för identifikatorn för återkallelse*

Identifikatorn för återkallelse ska

(a) ingå i den signerade QR-nyttolasten,

(b) vara unik åtminstone inom den utfärdande myndighetens utfärdandedomän,

(c) inte vara tryckt på intyget och inte avsedd att vara läsbar för människor,

(d) inte avslöja personuppgifter och inte ha en omedelbart begriplig innebörd,

(e) inte kunna härledas direkt från intygets synliga serienummer,

(f) vara kryptografiskt bunden till QR-nyttolasten genom den kvalificerade elektroniska stämpeln.

6.2. *Identifikatorns format och storlek*

Identifikatorn för återkallelse ska kodas som en CBOR-bytesträng (bstr). Identifikatorn ska vara 16 bytes (128 bitar) lång.

Identifikatorn ska genereras av den utfärdande myndigheten med hjälp av en metod som den kontrollerar och som säkerställer tillräcklig entropi och motståndskraft mot gissningar eller uppräkningar.

6.3. *Förteckningar över återkallelser*

Förteckningar över återkallelser som offentliggörs för kontrolländamål ska endast hänvisa till återkallade intygs identifikator för återkallelse. Intygens serienummer ska inte offentliggöras i förteckningar över återkallelser.

7. CBOR-nyttolast (inom QR-koden) på EU-intyget om funktionsnedsättning

Endast följande uppgifter ska ingå i QR-nyttolasten, i överensstämmelse med de synliga datafält på EU-intyget för funktionsnedsättning som anges i bilaga I till direktiv (EU) 2024/2841.

Innehåll på högsta nivå:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces. ”eu.edc” med de attribut som visas i tabellen nedan

(c) issuerAuth = COSE_Sign1 (QSeal)

Fält	**mDOC-kanal**	**Typ/format**
Dataschemaversion	issuerSigned.nameSpaces."eu.edc".ver	Sträng (t.ex. ”1.0”)
Typ av handling: EU-intyget om funktionsnedsättning	docType	Enum ("eu.edc")
Intygets serienummer	issuerSigned.nameSpaces."eu.edc".sub	Sträng
Identifikator för återkallelse	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bytes)
Intygsinnehavarens förnamn	issuerSigned.nameSpaces."eu.edc".givenName	Unicode-textsträng (UTF-8)
Intygsinnehavarens efternamn	issuerSigned.nameSpaces."eu.edc".familyName	Unicode-textsträng (UTF-8)
Intygets sista giltighetsdag	issuerSigned.nameSpaces."eu.edc".exp	CBOR-tagg 1004, enligt definitionen i RFC 8943 (avsnitt 2.1), som innehåller en UTF-8-textsträng föreställande ett

		fullständigt datum enligt RFC 3339 i ÅÅÅÅ-MM-DD-format.

Den elektroniska signaturen finns i issuerAuth (ett COSE_Sign1-objekt). Certifikatkedjan får inte infogas i QR-kodnyttolasten; i stället ska den skyddade COSE-rubriken innehålla x5t, ett certifikatfingeravtryck som används för att lokalisera motsvarande QSealC i kontrollörens cachade trust store.

8. **Exempel på QR-kodnyttolast på EU-intyget om funktionsnedsättning: kommenterad logisk återgivning av JSON-typ**

Följande exempel är en för människor läsbar JSON-återgivning (JavaScript Object Notation) av en logisk bild av EU-intyget om funktionsnedsättning. I praktiken ska denna struktur inte vara läsbar för människor, eftersom den ska

(a) kodas i CBOR (RFC 8949, avsnitt 3),

b) signeras med hjälp av en otaggad COSE_Sign1-struktur med en avskild nyttolast (RFC 9052, avsnitt 4),

c) inkludera utgångsdatumet som CBOR-tagg 1004 (fullständigt datumvärde) i enlighet med RFC 8943 (avsnitt 2.1),

d) inkludera den skyddade rubrikparametern x5t i enlighet med RFC 9360, med hjälp av SHA-256 över den DER-kodade QSealC-slutenheten, och

e) komprimeras och prefixeras med strängen ED1:MDOC:, innan den kodas in i QR-koden.

```
{
  // Endast en för människor läsbar logisk bild av EU-intyget om funktionsnedsättning av JSON-typ.
  // Den faktiska QR-nyttolasten är deterministisk CBOR, inte JSON.
  "docType": "eu.edc", // Identifieringsuppgift för EU-intyget om funktionsnedsättning. docType-värdet är inkluderat, tillsammans med
    // issuerSigned, i den externa COSE_Sign1-nyttolasten.

  "issuerSigned": {
    // Uppgifter som skyddas av issuerAuth och används som avskild nyttolast.
    // För generering och verifiering av signaturer omfattar den avskilda externa nyttolasten både
    // docType och issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // QR-profilen/QR-schemaversionen

        // Intygets serienummer: fastställd av utfärdaren, högst 24 tecken.
```

```
    "sub": "AB123456789012345678 90CD",

    // Identifikator för återkallelse: faktisk CBOR-bstr, 16 bytes/128 bitar.
    // Här i form av 32 hexadecimaler i läsbarhetssyfte.
    "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

    "givenName": "Ann",    // Förnamn tryckt på EU-intyget om funktionsnedsättning
    "familyName": "Other", // Efternamn tryckt på EU-intyget om funktionsnedsättning

    // Faktisk CBOR-kodning använder tagg 1004 för fullständigt datum enligt RFC 3339.
    "exp": "2030-12-31"
   }
  }
},

"issuerAuth": {
 // Faktisk form: otaggad COSE_Sign1, inte ett JSON-objekt.
 "type": "COSE_Sign1",
 "tagged": false,       // kodad utan COSE_Sign1 CBOR-tagg
 "payload": "detached", // COSE-nyttolastfältet är CBOR null

 "protectedHeader": {
  // alg: ES256; motsvarande COSE-rubrikparameter 1 = -7.
  "alg": "ES256",

  // x5t: certifikatfingeravtryck; COSE-rubrikparameter 34.
  "x5t": {
```

"hashAlg": "SHA-256", // motsvarande COSE-hashvärde -16

// SHA-256-hash av DER-kodad QSealC-slutenhet.

// 32 bytes i form av 64 hexadecimaler.

"hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

”unprotectedHeader”: {}, // tomt i det här exemplet

// ES256 COSE-signatur: // 64 bytes = 128 hexadecimaler.

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Användning av kryptografiska mekanismer

Användningen av kryptografiska mekanismer inom ramen för denna bilaga ska överensstämma med den överenskommelse om kryptografiska mekanismer (*Agreed Cryptographic Mechanisms*) som godkänts av europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Europeiska unionens cybersäkerhetsbyrå (Enisa).

BILAGA II

QR-KODSPECIFIKATIONER FÖR DEN FYSISKA VERSIONEN AV EU-PARKERINGSTILLSTÅNDET FÖR PERSONER MED FUNKTIONSNEDSÄTTNING

1. **Format för QR-koden på den fysiska versionen av EU-parkeringstillståndet för personer med funktionsnedsättning**

(a) **Format för QR-kod modell 2**, i enlighet med de internationella QR-kodspecifikationerna ISO/IEC 18004:2024 eller motsvarande.

(b) **Felkorrigeringsnivå M** (15 % redundans) som säkerställer motståndskraft mot repor eller partiell skada på en tryckt QR-kod.

(c) **Kodningsmetod:** QR-nyttolasten ska bestå av den kombinerade strukturen issuerSigned Concise Binary Object Representation (CBOR) och motsvarande signaturobjekt issuerAuth COSE_Sign1 enligt definitionen i CBOR Object Signing and Encryption (COSE, RFC 9052 avsnitt 3.1, 4.2 och 4.4), i enlighet med datamodellen mDOC för issuerSigned-delar, men anpassad till statisk användning av ett fysiskt intyg. issuerAuth ska vara ett COSE_Sign1-objekt med alg = ES256 och en skyddad rubrik som innehåller x5t (COSE X.509-certifikatets hashrubrikparameter som definieras i RFC 9360 [avsnitt 2]; i interoperabilitetssyfte ska den hashalgoritm som används i x5t vara SHA-256).

(d) Före QR-kodningen ska det kombinerade CBOR/COSE-objektet **komprimeras med hjälp av zlib-format (RFC 1950, avsnitt 2.2)** med algoritmen **Deflate** (RFC 1951, avsnitt 3.2 och 4). Den komprimerade byteträng som uppstår härigenom ska kodas i **QR-kodbyteläge**, så att fullt stöd för binära CBOR/COSE-nyttolaster och skannerinteroperabilitet säkerställs.

För alla textfält som ingår i QR-nyttolasten ska utfärdare koda tecken som Unicode UTF-8 inom CBOR-textsträngar. Translitterering ska inte tillämpas på signerade nyttolastuppgifter. I interoperabilitetssyfte ska utfärdare tillämpa Unicode Normalisation Form C (NFC) på alla textfält före signering.

(e) **Prefix**: QR-strängen för EU-parkeringstillståndet för personer med funktionsnedsättning ska börja med ”EP1:MDOC:”. Härigenom identifieras handlingens typ och kodningsprofilen. Prefixen är skiftlägeskänsliga och måste finnas med. Prefix som är okända eller saknar stöd ska resultera i avslag. Prefixet och den komprimerade nyttolasten ska kodas som ett enda bytelägedatasegment i QR-koden.

(f) **Minsta modulstorlek ≥ 0,35 mm** för att säkerställa läsbarhet på tryckta handlingar.

(g) **Max version 20** med upp till 97 × 97 moduler på respektive sida.

2. **Specifikationer för signaturgenerering för EU-parkeringstillståndet för personer med funktionsnedsättning**

Den kvalificerade elektroniska stämpel (QSeal) som används för att stämpla QR-koder på EU-parkeringstillståndet för personer med funktionsnedsättning säkerställer att de kodade uppgifterna kommer från den behöriga utfärdande myndigheten och inte har ändrats.

(a) **Signaturalgoritm**: Signaturalgoritmen ska vara ES256 (ECDSA med SHA-256 och P-256-kurvan), enligt definitionen i RFC 9053 (avsnitt 2.1); i COSE identifieras algoritmen med hjälp av rubrikparametern alg i RFC 9052 (avsnitt 3.1).

(b) **Signeringsnyckel**: QR-nyttolasten ska signeras med hjälp av den privata nyckel som motsvarar ett kvalificerat certifikat för elektroniska stämplar (QSealC).

(c) **COSE-struktur**: Signaturbehållaren ska vara ett COSE_Sign1-objekt. Den skyddade rubriken ska innehålla alg (ES256) och x5t (COSE X.509-certifikatets hashrubrikparameter som definieras i RFC 9360 [avsnitt 2]; i interoperabilitetssyfte ska den hashalgoritm som används i x5t vara SHA-256). Kontrollen ska med hjälp av x5t-värdet lokalisera motsvarande certifikat i kontrollörens lokalt cachade trust store som bygger på information från förteckningar över betrodda tjänsteleverantörer och ska därefter validera certifikatkedjan och certifikatstatusen i enlighet med eIDAS-förordningens tillitsramverk.

(d) **Signaturstandard**: QR-kodnyttolasten ska signeras som ett COSE_Sign1-objekt i enlighet med RFC 9052 (avsnitt 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet ska finnas i issuerAuth och kodas utan CBOR-taggen för COSE_Sign1. COSE_Sign1-objektets nyttolastfält ska avskiljas och kodas som CBOR null. För generering och verifiering av signaturer ska den externa nyttolasten vara den deterministiska kodade CBOR-strukturen som innehåller docType-värdet och issuerSigned-värdet från CBOR-kartan på högsta nivå.

(e) **Hashalgoritm**: SHA-256 används som en del av ES256 för signaturgenerering och integritetskontroll.

(f) **Kodning**: Nyttolasten ska kodas med hjälp av CBOR (RFC 8949, avsnitt 4.2), enligt kraven i COSE- och mDOC-specifikationerna, så att kodning och reproducerbarhet säkerställs för de signerade uppgifterna.

3. **Specifikationer för tryckning**

(a) **Ljusmarginal**: En tom marginal på **4 moduler** ska omge QR-koden på alla sidor, utan tryck, mönster eller bakgrund.

(b) **Kontrast**: QR-koden ska tryckas på vit bakgrund, varvid kontrastförhållandet ska vara minst **4:1**, så att hög läsbarhet säkerställs under olika ljusförhållanden.

(c) QR-koden ska tryckas med den färg som fastställs i bilaga II till direktiv (EU) 2024/2841 och som säkerställer maximal kontrast.

(d) **Placering och storlek:** QR-koden, inklusive ljusmarginalen, ska vara **37 mm** × **37 mm** och placeras på tillståndets framsida, strax till höger om mittpunkten i närheten av den nedre kanten. QR-koden får högst vara version 20 (97 × 97 moduler), med en modulstorlek på minst 0,35 mm.

QR-koden, inklusive dess ljusmarginal, ska placeras minst 5 mm från tillståndets nedre kant.

4. **Uppgifter i QR-koden på EU-parkeringstillståndet för personer med funktionsnedsättning**

QR-koden ska innehålla en minimal uppsättning uppgifter, vilka ska gå att kontrollera offline, i enlighet med den princip om uppgiftsminimering som fastställs i artikel 5.1 c i förordning (EU) 2016/679. Nyttolaststrukturen ska vara följande:

(a) Tillståndsattribut kodas i CBOR inom ett issuerSigned-objekt.

(b) Denna struktur inpackas och signeras av den utfärdande myndighetens QSeal som en issuerAuth (COSE_Sign1, ES256, inklusive x5t, COSE X.509-certifikatets hashrubrikparameter).

(c) Det CBOR/COSE-objekt som uppstår härigenom ska komprimeras i enlighet med punkt 1 d i denna bilaga. QR-kodnyttolasten ska bestå av prefixet ”EP1:MDOC:”, följt av den komprimerade bytesträng som uppstår, och den fullständiga nyttolasten ska kodas med byteläge som ett enda QR-koddatasegment.

Uppgiftsinnehållet ska bestå av en delmängd synliga data från de fält på tillståndets framsida som förtecknas i bilaga II till direktiv (EU) 2024/2841 (sista giltighetsdag, tillståndets serienummer), tillsammans med identifikatorn för återkallelse, den elektroniska signaturen och schemainformationen.

Den **elektroniska signaturen** ska innehålla följande:

i) Ett issuerAuth – ett COSE_Sign1-objekt signerat med den utfärdande myndighetens **privata QSealC-nyckel**.

ii) En skyddad rubrik som omfattar alg = ES256 (signaturalgoritm) och x5t (COSE X.509-certifikatets hashrubrikparameter).

5. Frivilliga uppgifter

Inga frivilliga uppgifter får inkluderas i QR-koden.

6. Identifikator för återkallelse (RID)

Identifikatorn för återkallelse för EU-parkeringstillståndet för personer med funktionsnedsättning ska vara förenlig med punkt 6 i bilaga I.

Förteckningar över återkallelser för återkallade EU-parkeringstillstånd för personer med funktionsnedsättning ska endast hänvisa till identifikatorn för återkallelse. Tillståndets serienummer ska inte offentliggöras i förteckningar över återkallelser.

7. CBOR-nyttolast (inom QR-koden) på EU-parkeringstillståndet för personer med funktionsnedsättning

Endast följande uppgifter ska ingå i QR-nyttolasten, i överensstämmelse med de synliga datafält på EU-parkeringstillståndet för personer med funktionsnedsättning som anges i bilaga II till direktiv (EU) 2024/2841.

Fält	**mDOC-kanal**	**Typ/format**
Dataschemaversion	issuerSigned.nameSpaces."eu.epc".ver	Sträng (t.ex. ”1.0”)
Typ av handling:	docType	Enum

EU-parkeringstillståndet för personer med funktionsnedsättning		("eu.epc")
Tillståndets serienummer	issuerSigned.nameSpaces."eu.epc".sub	Sträng
Identifikator för återkallelse	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bytes)
Tillståndets sista giltighetsdag	issuerSigned.nameSpaces."eu.epc".exp	CBOR-tagg 1004, enligt definitionen i RFC 8943 (avsnitt 2.1), som innehåller en UTF-8-textsträng föreställande ett fullständigt datum enligt RFC 3339 i ÅÅÅÅ-MM-DD-format.

Den elektroniska signaturen ska finnas i issuerAuth (ett COSE_Sign1-objekt). Certifikatkedjan får inte infogas i QR-kodnyttolasten; i stället ska den skyddade COSE-rubriken innehålla x5t, ett certifikatfingeravtryck som används för att lokalisera motsvarande QSealC i kontrollörens cachade trust store.

8. Exempel på QR-kodnyttolast på EU-parkeringstillståndet för personer med funktionsnedsättning: kommenterad logisk återgivning av JSON-typ

Följande exempel är en för människor läsbar JSON-återgivning (JavaScript Object Notation) av en logisk bild av EU-parkeringstillståndet för personer med funktionsnedsättning. I praktiken ska denna struktur inte vara läsbar för människor, eftersom den ska

(a) kodas i CBOR (RFC 8949, avsnitt 3),

(b) signeras med hjälp av en otaggad COSE_Sign1-struktur med en avskild nyttolast (RFC 9052, avsnitt 4),

(c) inkludera utgångsdatumet som CBOR-tagg 1004 (fullständigt datumvärde) i enlighet med RFC 8943 (avsnitt 2.1),

(d) inkludera den skyddade rubrikparametern x5t i enlighet med RFC 9360, med hjälp av SHA-256 över den DER-kodade QSealC-slutenheten, och

(e) komprimeras och prefixeras med strängen EP1:MDOC:, innan den kodas in i QR-koden.

```
{
  // Endast en för människor läsbar logisk bild av EU-parkeringstillståndet för personer med funktionsnedsättning av JSON-typ.
  // Den faktiska QR-nyttolasten är deterministisk CBOR, inte JSON.
  "docType": "eu.epc", // Identifieringsuppgift för EU-parkeringstillståndet för personer med funktionsnedsättning. docType-värdet är inkluderat, tillsammans med
    // issuerSigned, i den externa COSE_Sign1-nyttolasten.

  "issuerSigned": {
    // Uppgifter som skyddas av issuerAuth och används som avskild nyttolast.
 // För generering och verifiering av signaturer omfattar den avskilda externa nyttolasten både
    // docType och issuerSigned.
    "nameSpaces": {
      "eu.epc": {
        "ver": "1.0", // QR-profilen/QR-schemaversionen

        // Tillståndets serienummer: fastställd av utfärdaren, högst 24 tecken.
        "sub": "EF123456789012345678 90GH",

        // Identifikator för återkallelse: faktisk CBOR-bstr, 16 bytes/128 bitar.
        // Här i form av 32 hexadecimaler i läsbarhetssyfte.
        "rid": "4a8d9c112233445566778899aabbccdd",

        // Faktisk CBOR-kodning använder tagg 1004 för fullständigt datum enligt RFC 3339.
        "exp": "2030-12-31"
      }
```

```
    }
  },

  "issuerAuth": {
    // Faktisk form: otaggad COSE_Sign1, inte ett JSON-objekt.
    "type": "COSE_Sign1",
    "tagged": false,       // kodad utan COSE_Sign1 CBOR-tagg
    "payload": "detached", // COSE-nyttolastfältet är CBOR null

    "protectedHeader": {
      // alg: ES256; motsvarande COSE-rubrikparameter 1 = -7.
      "alg": "ES256",

      // x5t: certifikatfingeravtryck; COSE-rubrikparameter 34.
      "x5t": {
        "hashAlg": "SHA-256", // motsvarande COSE-hashvärde -16

        // SHA-256-hash av DER-kodad QSealC-slutenhet.
        // 32 bytes i form av 64 hexadecimaler.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    ”unprotectedHeader”: {}, // tomt i det här exemplet

    // ES256 COSE-signatur: // 64 bytes = 128 hexadecimaler.
```

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Användning av kryptografiska mekanismer

Användningen av kryptografiska mekanismer inom ramen för denna bilaga ska överensstämma med den överenskommelse om kryptografiska mekanismer (*Agreed Cryptographic Mechanisms*) som godkänts av europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Europeiska unionens cybersäkerhetsbyrå (Enisa).

BILAGA III

INLÄMNING AV INFORMATION SOM AVSES I ARTIKEL 6.2

1. Medlemsstaterna ska till kommissionen inlämna följande information om varje behörig myndighet eller behörigt organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning:

   (a) Namnet på den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning.

   (b) Ett registreringsnummer för den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning.

   (c) Kontaktuppgifter (e-postadress och telefonnummer) för den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning.

   (d) Ett eller flera certifikat som kan användas för att kontrollera den elektroniska stämpel som skapats av den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av det EU-intyg om funktionsnedsättning eller det EU-parkeringstillstånd för personer med funktionsnedsättning som den eller det utfärdar, och för vilka de certifierade identitetsuppgifterna inbegriper utfärdarens namn och registreringsnummer, i enlighet med vad som anges i punkt a respektive punkt b.

   (e) Den webbadress där utfärdaren offentliggör giltighetsstatusen för de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning.

2. Medlemsstaterna får till kommissionen inlämna följande information om varje behörig myndighet eller behörigt organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning:

   (a) Adressen till den webbsida där den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning anger de policyer, villkor och bestämmelser som gäller tillhandahållandet och användningen av de fysiska versionerna av dessa handlingar.

   (b) I förekommande fall adressen till den webbsida som innehåller övrig information om den behöriga myndighet eller det behöriga organ som ansvarar för utfärdandet av de fysiska versionerna av EU-intyget om funktionsnedsättning eller EU-parkeringstillståndet för personer med funktionsnedsättning.

BILAGA IV

TEKNISKA SPECIFIKATIONER FÖR EN FÖRTECKNING ÖVER ÅTERKALLELSER FÖR DE FYSISKA VERSIONERNA AV EU-INTYGET OM FUNKTIONSNEDSÄTTNING ELLER EU-PARKERINGSTILLSTÅNDET FÖR PERSONER MED FUNKTIONSNEDSÄTTNING

1. Vid tillämpningen av denna bilaga ska identifikatorn motsvara den identifikator för återkallelse som fastställs i punkt 6 i bilaga I och punkt 6 i bilaga II.

2. En förteckning över återkallelser ska uppföras som en token för en identifikatorförteckning i CWT-format (RFC 8392, avsnitt 7) i enlighet med punkt 5.2 i specifikationen för förteckningar över tokenstatus (draft-ietf-oauth-status-list-14) med följande ändringar:

   (a) Värdet för typkravet ska vara ”application/identifierlist+cwt”.

   (b) Kravet på sista giltighetstidpunkt ska finnas med.

   (c) StatusList-kravet får inte ingå i CWT-kraven.

   (d) IdentifierList-strukturen som definieras i punkt 3 ska ingå som ett krav i CWT-kraven med hjälp av nyckel 65530.

   (e) CWT:n ska vara ett COSE_Sign1-objekt som, vid beräkning av signaturen, använder en signaturalgoritm som överensstämmer med den överenskommelse om kryptografiska mekanismer (*Agreed Cryptographic Mechanisms*) som godkänts av europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Europeiska unionens cybersäkerhetsbyrå (Enisa).

   (f) CWT:n ska innehålla den x5chain-parameter som definieras i RFC 9360 (avsnitt 2) i den skyddade rubrik som innehåller certifikatet eller kedjan av certifikat för att kontrollera signaturen i förteckningen över återkallelser.

   (g) Den utökade nyckelanvändningens OID som anges i specifikationen för förteckningar över tokenstatus (draft-ietf-oauth-status-list-14) kan användas för identifikatorförteckningens signeringsintyg, och det rekommenderas att kontrollörerna stöder den utökade nyckelanvändningens OID som anges i specifikationen för förteckningar över tokenstatus och att utfärdande myndigheters infrastruktur inte gör fältet för utökad nyckelanvändning kritiskt vid användning av den utökade nyckelanvändningens OID som anges i specifikationen för förteckningen över tokenstatus.

3. IdentifierList-strukturen ska vara en CBOR-struktur med följande Concise Data Definition Language (CDDL):

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

IdentifierInfo = {
```

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

Identifier = bstr

Aggregation_uri = tstr
```