Euroopan unionin neuvosto

Bryssel, 10. heinäkuuta 2026
(OR. en)

11772/26
ADD 1

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

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	1. heinäkuuta 2026
Vastaanottaja:	Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	C(2026) 4534 annex
Asia:	LIITTEET asiakirjaan KOMISSION DELEGOITU ASETUS (EU) .../... direktiivin (EU) 2024/2841 täydentämisestä siltä osin kuin on kyse eurooppalaisen vammaiskortin fyysiseen versioon sisällytettävän QR-koodin vahvistamisesta, eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysiseen versioon sisällytettävän QR-koodin vahvistamisesta ja kyseisen fyysisen version turvallisuuden varmistavien yhteisten teknisten eritelmien vahvistamisesta sekä yhteentoimivuuteen liittyvistä seikoista

EUROOPAN
KOMISSIO

Bryssel 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

LIITTEET

asiakirjaan

KOMISSION DELEGOITU ASETUS (EU) .../...

direktiivin (EU) 2024/2841 täydentämisestä siltä osin kuin on kyse eurooppalaisen vammaiskortin fyysiseen versioon sisällytettävän QR-koodin vahvistamisesta, eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysiseen versioon sisällytettävän QR-koodin vahvistamisesta ja kyseisen fyysisen version turvallisuuden varmistavien yhteisten teknisten eritelmien vahvistamisesta sekä yhteentoimivuuteen liittyvistä seikoista

LIITE I

EUROOPPALAISEN VAMMAISKORTIN FYYSISESSÄ VERSIOSSA OLEVAN QR-KOODIN ERITELMÄT

1. **Eurooppalaisen vammaiskortin fyysisessä versiossa olevan QR-koodin muoto**

a) **QR-koodin Model 2 -muoto** QR-koodin kansainvälisen eritelmän ISO/IEC 18004:2024 tai vastaavan mukaisesti.

b) **Virheenkorjaustaso M** (15 %:n redundanssi), jolla varmistetaan, että painettu QR-koodi kestää naarmuja tai osittaista vahingoittumista.

c) **Koodaustila:** QR-hyötykuorma koostuu yhdistetystä issuerSigned Concise Binary Object Representation (CBOR) -rakenteesta ja vastaavasta issuerAuth COSE_Sign1 -allekirjoitusobjektista, sellaisina kuin ne on määritelty CBOR Object Signing and Encryption -standardissa (COSE, RFC 9052, kohdat 3.1, 4.2 ja 4.4). IssuerSigned-elementeissä noudatetaan mDOC-datamallinnusmallia, mutta mukautettuna fyysisen kortin staattiseen käyttöön. IssuerAuth on COSE_Sign1-objekti, jonka alg = ES256 ja jossa on suojattu otsikko, joka sisältää x5t:n (COSE X.509 -varmenteen hash-otsikkoparametri, joka on määritelty standardissa RFC 9360 (2 jakso); yhteentoimivuuden vuoksi x5t:ssä käytettävän hajautusalgoritmin on oltava SHA-256).

d) Ennen QR-koodin koodausta yhdistetty CBOR/COSE-objekti on **pakattava käyttäen zlib-muotoa** (RFC 1950, kohta 2.2) ja **Deflate-algoritmia** (RFC 1951, kohdat 3.2 ja 4). Tuloksena saatu tiivistetty tavutaulukko on koodattava **QR-koodin tavutilassa**, jotta varmistetaan täysi tuki binäärisille CBOR/COSE-hyötykuormille ja skannereiden yhteentoimivuudelle.

Myöntäjien on kaikissa QR-hyötykuormaan sisältyvissä tekstikentissä koodattava merkit Unicode UTF-8 -merkkeinä CBOR-tekstijonoissa. Allekirjoitettuihin hyötykuormatietoihin ei saa soveltaa translitterointia. Yhteentoimivuuden vuoksi myöntäjien on ennen allekirjoittamista sovellettava kaikkiin tekstikenttiin Unicode-normalisointimuotoa C (NFC).

e) **Etuliite:** Eurooppalaisen vammaiskortin QR-jonon alussa on oltava ”ED1:MDOC:”. Tämä yksilöi kortin tyypin ja koodausprofiilin. Etuliitteet ovat aakkoskoosta riippuvaisia, ja ne on esitettävä. Tuntemattomat tai tukemattomat etuliitteet aiheuttavat hylkäämisen. Etuliite ja tiivistetty hyötykuorma on koodattava QR-koodiin yhtenä tavutilan datasegmenttinä.

f) **Moduulin vähimmäiskoko ≥ 0,25 mm** luettavuuden varmistamiseksi painetussa kortissa.

g) **Enintään versio 20;** enintään 97 × 97 moduulia kullakin sivulla.

2. **Eurooppalaisen vammaiskortin allekirjoituksen luomista koskevat eritelmät**

Eurooppalaisen vammaiskortin QR-koodien leimaamiseen käytettävällä hyväksytyllä sähköisellä leimalla (Qseal) varmistetaan, että koodatut tiedot ovat peräisin valtuutetulta myöntävältä viranomaiselta eikä niitä ole muutettu.

a) **Allekirjoitusalgoritmi**: Allekirjoitusalgoritmin on oltava ES256 (Elliptic Curve Digital Signature Algorithm, ECDSA, SHA-256-hajautusalgoritmilla käyttäen P-

256-käyrää), sellaisena kuin se on määritelty standardissa RFC 9053 (2.1 kohta); COSE:ssa algoritmi yksilöidään RFC 9052:n alg-otsikkoparametrilla (3.1 kohta).

b) **Allekirjoitusavain**: QR-hyötykuorma on allekirjoitettava käyttäen sähköisen leiman hyväksyttyä varmennetta (QSealC) vastaavaa yksityistä avainta.

c) **COSE-rakenne:** Allekirjoitussäilön on oltava COSE_Sign1-objekti. Suojatun otsikon on sisällettävä alg (ES256) ja x5t (COSE X.509 -varmenteen hash-otsikkoparametri, joka on määritelty standardissa RFC 9360 (2 jakso); yhteentoimivuuden vuoksi x5t:ssä käytettävän hajautusalgoritmin on oltava SHA-256). Todentamisessa käytetään x5t-arvoa vastaavan varmenteen paikantamiseksi tarkastajan paikallisesti välimuistiin tallentamassa luotettujen varmenteiden säilössä, joka on rakennettu luotetun luettelon tiedoista, ja sen jälkeen varmenneketjun ja varmenteen tilan validoimiseksi eIDAS-luottamuskehyksen mukaisesti.

d) **Allekirjoitusstandardi**: QR-koodin hyötykuorma on allekirjoitettava COSE_Sign1-objektina standardin RFC 9052 (4 jakso), ”CBOR Object Signing and Encryption” mukaisesti. COSE_Sign1-objektin on oltava mukana issuerAuth-objektissa ja se on koodattava ilman CBOR-tunnistetta COSE_Sign1-rakennetta varten. COSE_Sign1-objektin hyötykuormakenttä on irrotettava ja koodattava CBOR-arvoksi ”null”. Allekirjoituksen luomisessa ja todentamisessa käytetty ulkoinen hyötykuorma on deterministinen CBOR-koodattu rakenne, joka sisältää docType-arvon ja issuerSigned-arvon ylätason CBOR-kartasta.

e) **Hajautusalgoritmi**: SHA-256:ta on käytettävä osana ES256:ta allekirjoituksen luomisessa ja eheyden todentamisessa.

f) **Koodaus**: Hyötykuorma on koodattava käyttäen CBOR:ta (RFC 8949, 4.2 kohta), kuten COSE- ja mDOC-eritelmissä edellytetään, jotta varmistetaan allekirjoitettujen tietojen koodaus ja toistettavuus.

3. **Painamista koskevat eritelmät**

a) **Tyhjä tila**: QR-koodin kaikilla sivuilla on oltava selkeä **neljän moduulin** levyinen marginaali, jossa ei ole painatusta, kuviota tai taustaa.

b) **Kontrasti**: QR-koodi on painettava valkoiselle taustalle siten, että kontrastisuhde on vähintään **4:1**, jotta varmistetaan hyvä luettavuus erilaisissa valaistusolosuhteissa.

c) QR-koodi on painettava käyttäen direktiivin (EU) 2024/2841 liitteessä I määriteltyä väriä, jolla varmistetaan mahdollisimman suuri kontrasti.

d) **Sijainti ja koko**: QR-koodin, tyhjä tila mukaan luettuna, koon on oltava 26,25 mm × 26,25 mm, ja sen on sijaittava kortin kääntöpuolella oikeassa alakulmassa. QR-koodi saa olla enintään versio 20 (97 × 97 moduulia), ja moduulin koon on oltava vähintään 0,25 mm.

QR-koodi, tyhjä tila mukaan luettuna, on sijoitettava vähintään 5 mm:n etäisyydelle kortin oikeasta reunasta ja vähintään 5 mm:n etäisyydelle kortin alareunasta.

4. **Eurooppalaisen vammaiskortin QR-koodissa olevat tiedot**

QR-koodin on sisällettävä vähimmäismäärä verkon ulkopuolella todennettavia tietoja asetuksen (EU) 2016/679 5 artiklan 1 kohdan c alakohdassa säädetyn tietojen minimoinnin periaatteen mukaisesti. Hyötykuorman rakenne on seuraava:

a) Kortin attribuutit koodataan CBOR-rakenteena issuerSigned-objektiin.

b) Rakenne kääritään ja allekirjoitetaan myöntävän viranomaisen Qseal-leimalla issuerAuth-objektina (COSE_Sign1, ES256, mukaan lukien x5t, COSE X.509 -varmenteen hash-otsikkoparametri).

c) Tuloksena saatu CBOR/COSE-objekti on pakattava tämän liitteen 1 kohdan d alakohdan mukaisesti. QR-koodin hyötykuorma koostuu etuliitteestä ”ED1:MDOC:”, jota seuraa tuloksena saatu tiivistetty tavutaulukko, ja koko hyötykuorma koodataan tavutilaa käyttäen yhtenä QR-koodin datasegmenttinä.

Tietosisältö koostuu direktiivin (EU) 2024/2841 liitteessä I lueteltujen kortin etupuolen kenttien näkyvien tietojen osajoukosta (etunimi, sukunimi, kortin sarjanumero, viimeinen voimassaolopäivä) sekä peruuttamistunnisteesta, sähköisestä allekirjoituksesta ja skeematiedoista.

Sähköisen allekirjoituksen on sisällettävä

i) issuerAuth - COSE_Sign1-objekti, joka on allekirjoitettu myöntävän viranomaisen **QSealC-yksityisavaimella**.

ii) suojattu otsikko, johon sisältyy alg = ES256 (allekirjoitusalgoritmi) ja x5t (COSE X.509-varmenteen hash-otsikkoparametri).

5. Valinnaiset tiedot

QR-koodi ei saa sisältää valinnaisia tietoja.

6. Peruuttamistunniste (RID)

Kortin näkyvän sarjanumeron lisäksi QR-koodissa on oltava erityinen peruuttamistunniste.

Peruuttamistunnistetta käytetään peruuttamistilan määrittämiseen ja peruuttamisluettelon hallintaan. Peruuttamistunnistetta ei saa painaa korttiin, eikä se saa olla kortin tarkastajien nähtävissä.

6.1. *Peruuttamistunnistetta koskevat vaatimukset*

Peruuttamistunnistetta koskevat seuraavat vaatimukset:

a) sen on sisällyttävä allekirjoitettuun QR-hyötykuormaan;

b) sen on oltava ainutkertainen ainakin alueella, jolla myöntävä viranomainen myöntää kortteja;

c) sitä ei saa painaa korttiin eikä se saa olla tarkoitettu ihmisen luettavaksi;

d) siinä ei saa paljastaa henkilötietoja eikä se saa olla suoraan merkityksellinen;

e) se ei saa ole suoraan johdettavissa kortin näkyvästä sarjanumerosta; ja

f) sen on oltava salausteknisesti sidottu QR-hyötykuormaan hyväksytyllä sähköisellä leimalla.

6.2. *Peruuttamistunnisteen muoto ja koko*

Peruuttamistunniste on koodattava CBOR-tavujonona (bstr). Peruuttamistunnisteen pituuden on oltava 16 tavua (128 bittiä).

Myöntävän viranomaisen on luotava peruuttamistunniste käyttämällä valvonnassaan olevaa menetelmää, jolla varmistetaan riittävä entropia ja kyky kestää arvaamista tai sähköistä tuottamista.

6.3. *Peruuttamisluettelot*

Todentamista varten julkaistuissa peruuttamisluetteloissa on viitattava ainoastaan peruutettujen korttien peruuttamistunnisteisiin. Korttien sarjanumeroita ei saa julkaista peruuttamisluetteloissa.

7. Eurooppalaisen vammaiskortin CBOR-hyötykuorma (QR-koodin sisällä)

QR-hyötykuormaan on sisällytettävä ainoastaan seuraavat tiedot direktiivin (EU) 2024/2841 liitteessä I vahvistettujen eurooppalaisen vammaiskortin (EDC) näkyvien tietokenttien mukaisesti.

Ylimmän tason sisältö:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc", jonka attribuutit esitetään jäljempänä olevassa taulukossa

c) issuerAuth = COSE_Sign1 (QSeal)

Kenttä	**mDOC-polku**	**Tyyppi/muoto**
Tietoskeeman versio	issuerSigned.nameSpaces."eu.edc".ver	Merkkijono (esim. ”1.0”)
Korttityyppi: EDC	docType	Enum ("eu.edc")
Kortin sarjanumero	issuerSigned.nameSpaces."eu.edc".sub	Merkkijono
Peruuttamistunniste	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 tavua)
Kortinhaltijan etunimi	issuerSigned.nameSpaces."eu.edc".givenName	Unicode-tekstijono (UTF-8)
Kortinhaltijan sukunimi	issuerSigned.nameSpaces."eu.edc".familyName	Unicode-tekstijono (UTF-8)
Kortin viimeinen voimassaolopäivä	issuerSigned.nameSpaces."eu.edc".exp	CBOR-tunniste 1004, sellaisena kuin se on määriteltynä standardissa RFC 8943 (2.1

		kohta), joka sisältää UTF-8-tekstijonon, joka edustaa RFC 3339:n mukaista full-date-arvoa muodossa VVVV-KK-PP.

Sähköinen allekirjoitus on mukana issuerAuth-objektissa (COSE_Sign1-objekti). Varmenneketjua ei saa upottaa QR-koodin hyötykuormaan; sen sijaan suojatun COSE-otsikon on sisällettävä x5t, varmenteen sormenjälki, jota käytetään vastaavan QSealC-varmenteen paikantamiseen tarkastajan välimuistissa olevassa luotettujen varmenteiden säilössä.

8. Esimerkki eurooppalaisen vammaiskortin QR-koodin hyötykuormasta: kommentoitu JavaScript Object Notation -tyylinen looginen esitys

Seuraava esimerkki on ihmisen luettavissa oleva JavaScript Object Notation (JSON) -esitys eurooppalaisen vammaiskortin loogisesta näkymästä. Käytännössä tämä rakenne ei ole ihmisen luettavissa, koska sen on

a) oltava koodattu CBOR-rakenteena (RFC 8949, 3 jakso);

b) oltava allekirjoitettu käyttäen tunnisteetonta COSE_Sign1-rakennetta, jossa hyötykuorma on irrotettu (RFC 9052, 4 jakso);

c) sisällettävä voimassaolon päättymispäivä CBOR-tunnisteen 1004 full-date-arvona RFC 8943:n mukaisesti (2.1 kohta);

d) sisällettävä RFC 9360:n mukainen suojattu x5t-otsikkoparametri käyttäen SHA-256:ta DER-koodatussa loppukäyttäjän QSealC-varmenteessa; ja

e) oltava pakattu ja sen etuliitteenä on oltava merkkijono ED1:MDOC: ennen kuin se koodataan QR-koodiin.

{

// Vain JSON-tyylinen, ihmisen luettavissa oleva eurooppalaisen vammaiskortin looginen näkymä.

// Todellinen QR-hyötykuorma on deterministinen CBOR, ei JSON.

"docType": "eu.edc", // eurooppalaisen vammaiskortin valtuustieto. Sisältää docType-arvon sekä

// issuerSigned-objektin, COSE_Sign1-muotoisen ulkoisen hyötykuorman.

```
  "issuerSigned": {
    // IssuerAuth-objektilla suojatut tiedot; käytetään irrotettuna hyötykuormana.
    // Allekirjoituksen luomisen ja todentamisen osalta irrotettu ulkoinen hyötykuorma kattaa sekä
    // docType:n että issuerSigned:n.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // QR-profiilin/skeeman versio

        // Kortin sarjanumero; myöntäjän määrittelemä, enintään 24 merkkiä.
        "sub": "AB123456789012345678 90CD",

        // Peruuttamistunniste: tosiasiallisesti CBOR bstr, 16 tavua/128 bittiä.
        // Näytetään tässä 32:na hex-merkkinä luettavuuden vuoksi.
        "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

        "givenName": "Kari", // eurooppalaiseen vammaiskorttiin painettu etunimi
        "familyName": "Virtanen", // eurooppalaiseen vammaiskorttiin painettu sukunimi

        // Tosiasiallisessa CBOR-koodauksessa käytetään tunnistetta 1004 RFC 3339:n mukaisessa full-date-arvossa.
        "exp": "2030-12-31"
      }
    }
  },

  "issuerAuth": {
    // Todellinen muoto: tunnisteeton COSE_Sign1, ei JSON-objekti.
```

```
  "type": "COSE_Sign1",
  "tagged": false, // koodattu ilman COSE_Sign1 CBOR -tunnistetta
  "payload": "detached", // COSE-hyötykuormakenttä on CBOR ”null”

  "protectedHeader": {
   // alg: ES256; vastaava COSE-otsikkoparametri 1 = -7.
   "alg": "ES256",

   // x5t: varmenteen sormenjälki; COSE-otsikkoparametri 34.
   "x5t": {
    "hashAlg": "SHA-256", // vastaava COSE:n hash-arvo -16

    // DER-koodatun loppukäyttäjän QSealC-varmenteen SHA-256-hash.
    // 32 tavua esitettynä 64:na hex-merkkinä.
    "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // tyhjä tässä esimerkissä

  // ES256 COSE-allekirjoitus: 64 tavua = 128 hex-merkkiä.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. **Salausmekanismien käyttö**

Jos tämän liitteen yhteydessä käytetään salausmekanismeja, siinä on noudatettava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymiä ja Euroopan unionin kyberturvallisuusviraston (ENISA) julkaisemia sovittuja salausmekanismeja.

LIITE II

EUROOPPALAISEN VAMMAISTEN HENKILÖIDEN PYSÄKÖINTILUVAN FYYSISESSÄ VERSIOSSA OLEVAN QR-KOODIN ERITELMÄT

1. **Eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisessä versiossa olevan QR-koodin muoto**

a) **QR-koodin Model 2 -muoto** QR-koodin kansainvälisen eritelmän ISO/IEC 18004:2024 tai vastaavan mukaisesti.

b) **Virheenkorjaustaso M** (15 %:n redundanssi), jolla varmistetaan, että painettu QR-koodi kestää naarmuja tai osittaista vahingoittumista.

c) **Koodaustila:** QR-hyötykuorma koostuu yhdistetystä issuerSigned Concise Binary Object Representation (CBOR) -rakenteesta ja vastaavasta issuerAuth COSE_Sign1 -allekirjoitusobjektista, sellaisina kuin ne on määritelty CBOR Object Signing and Encryption -standardissa (COSE, RFC 9052, kohdat 3.1, 4.2 ja 4.4). IssuerSigned-elementeissä noudatetaan mDOC-datamallinnusmallia, mutta mukautettuna fyysisen kortin staattiseen käyttöön. IssuerAuth on COSE_Sign1-objekti, jonka alg = ES256 ja jossa on suojattu otsikko, joka sisältää x5t:n (COSE X.509 -varmenteen hash-otsikkoparametri, joka on määritelty standardissa RFC 9360 (2 jakso); yhteentoimivuuden vuoksi x5t:ssä käytettävän hajautusalgoritmin on oltava SHA-256).

d) Ennen QR-koodin koodausta yhdistetty CBOR/COSE-objekti on **pakattava käyttäen zlib-muotoa (RFC 1950, kohta 2.2) ja Deflate-algoritmia** (RFC 1951, kohdat 3.2 ja 4). Tuloksena saatu tiivistetty tavutaulukko on koodattava **QR-koodin tavutilassa**, jotta varmistetaan täysi tuki binäärisille CBOR/COSE-hyötykuormille ja skannereiden yhteentoimivuudelle.

Myöntäjien on kaikissa QR-hyötykuormaan sisältyvissä tekstikentissä koodattava merkit Unicode UTF-8 -merkkeinä CBOR-tekstijonoissa. Allekirjoitettuihin hyötykuormatietoihin ei saa soveltaa translitterointia. Yhteentoimivuuden vuoksi myöntäjien on ennen allekirjoittamista sovellettava kaikkiin tekstikenttiin Unicode-normalisointimuotoa C (NFC).

e) **Etuliite**: Eurooppalaisen vammaisten henkilöiden pysäköintiluvan QR-jonon alussa on oltava ”EP1:MDOC:”. Tämä yksilöi kortin tyypin ja koodausprofiilin. Etuliitteet ovat aakkoskoosta riippuvaisia, ja ne on esitettävä. Tuntemattomat tai tukemattomat etuliitteet aiheuttavat hylkäämisen. Etuliite ja tiivistetty hyötykuorma on koodattava QR-koodiin yhtenä tavutilan datasegmenttinä.

f) **Moduulin vähimmäiskoko ≥ 0,35 mm** luettavuuden varmistamiseksi painetussa kortissa.

g) **Enintään versio 20**; enintään 97 × 97 moduulia kummallakin sivulla.

2. **Eurooppalaisen vammaisten henkilöiden pysäköintiluvan allekirjoituksen luomista koskevat eritelmät**

Eurooppalaisen vammaisten henkilöiden pysäköintiluvan QR-koodien leimaamiseen käytettävällä hyväksytyllä sähköisellä leimalla (Qseal) varmistetaan, että koodatut tiedot ovat peräisin valtuutetulta myöntävältä viranomaiselta eikä niitä ole muutettu.

a) **Allekirjoitusalgoritmi**: Allekirjoitusalgoritmin on oltava ES256 (ECDSA, SHA-256-hajautusalgoritmilla käyttäen P-256-käyrää), sellaisena kuin se on määritelty standardissa RFC 9053 (2.1 kohta); COSE:ssa algoritmi yksilöidään RFC 9052:n alg-otsikkoparametrilla (3.1 kohta).

b) **Allekirjoitusavain**: QR-hyötykuorma on allekirjoitettava käyttäen sähköisen leiman hyväksyttyä varmennetta (QSealC) vastaavaa yksityistä avainta.

c) **COSE-rakenne**: Allekirjoitussäilön on oltava COSE_Sign1-objekti. Suojatun otsikon on sisällettävä alg (ES256) ja x5t (COSE X.509 -varmenteen hash-otsikkoparametri, joka on määritelty standardissa RFC 9360 (2 jakso); yhteentoimivuuden vuoksi x5t:ssä käytettävän hajautusalgoritmin on oltava SHA-256). Todentamisessa käytetään x5t-arvoa vastaavan varmenteen paikantamiseksi tarkastajan paikallisesti välimuistiin tallentamassa luotettujen varmenteiden säilössä, joka on rakennettu luotetun luettelon tiedoista, ja sen jälkeen varmenneketjun ja varmenteen tilan validoimiseksi eIDAS-luottamuskehyksen mukaisesti.

d) **Allekirjoitusstandardi**: QR-koodin hyötykuorma on allekirjoitettava COSE_Sign1-objektina standardin RFC 9052 (4 jakso), ”CBOR Object Signing and Encryption” mukaisesti. COSE_Sign1-objektin on oltava mukana issuerAuth-objektissa ja se on koodattava ilman CBOR-tunnistetta COSE_Sign1-rakennetta varten. COSE_Sign1-objektin hyötykuormakenttä on irrotettava ja koodattava CBOR-arvoksi ”null”. Allekirjoituksen luomisessa ja todentamisessa käytetty ulkoinen hyötykuorma on deterministinen CBOR-koodattu rakenne, joka sisältää docType-arvon ja issuerSigned-arvon ylätason CBOR-kartasta.

e) **Hajautusalgoritmi**: SHA-256:ta on käytettävä osana ES256:ta allekirjoituksen luomisessa ja eheyden todentamisessa.

f) **Koodaus**: Hyötykuorma on koodattava käyttäen CBOR:ta (RFC 8949, 4.2 kohta), kuten COSE- ja mDOC-eritelmissä edellytetään, jotta varmistetaan allekirjoitettujen tietojen koodaus ja toistettavuus.

3. **Painamista koskevat eritelmät**

a) **Tyhjä tila**: QR-koodin kaikilla sivuilla on oltava selkeä **neljän moduulin** levyinen marginaali, jossa ei ole painatusta, kuviota tai taustaa.

b) **Kontrasti**: QR-koodi on painettava valkoiselle taustalle siten, että kontrastisuhde on vähintään **4:1**, jotta varmistetaan hyvä luettavuus erilaisissa valaistusolosuhteissa.

c) QR-koodi on painettava käyttäen direktiivin (EU) 2024/2841 liitteessä II määriteltyä väriä, jolla varmistetaan mahdollisimman suuri kontrasti.

d) **Sijainti ja koko:** QR-koodin, tyhjä tila mukaan luettuna, koon on oltava **37 mm** × **37 mm**, ja sen on sijaittava kortin etupuolella alareunassa hieman kortin keskilinjan oikealla puolella. QR-koodi saa olla enintään versio 20 (97 × 97 moduulia), ja moduulin koon on oltava vähintään 0,35 mm.

QR-koodi, tyhjä tila mukaan luettuna, on sijoitettava vähintään 5 mm:n etäisyydelle kortin alareunasta.

4. **Eurooppalaisen vammaisten henkilöiden pysäköintiluvan QR-koodissa olevat tiedot**

QR-koodin on sisällettävä vähimmäismäärä verkon ulkopuolella todennettavia tietoja asetuksen (EU) 2016/679 5 artiklan 1 kohdan c alakohdassa säädetyn tietojen minimoinnin periaatteen mukaisesti. Hyötykuorman rakenne on seuraava:

a) Kortin attribuutit koodataan CBOR-rakenteena issuerSigned-objektiin.

b) Rakenne kääritään ja allekirjoitetaan myöntävän viranomaisen Qseal-leimalla issuerAuth-objektina (COSE_Sign1, ES256, mukaan lukien x5t, COSE X.509 -varmenteen hash-otsikkoparametri).

c) Tuloksena saatu CBOR/COSE-objekti on pakattava tämän liitteen 1 kohdan d alakohdan mukaisesti. QR-koodin hyötykuorma koostuu etuliitteestä ”EP1:MDOC:”, jota seuraa tuloksena saatu tiivistetty tavutaulukko, ja koko hyötykuorma koodataan tavutilaa käyttäen yhtenä QR-koodin datasegmenttinä.

Tietosisältö koostuu direktiivin (EU) 2024/2841 liitteessä II lueteltujen kortin etupuolen kenttien näkyvien tietojen osajoukosta (viimeinen voimassaolopäivä, kortin sarjanumero) sekä peruuttamistunnisteesta, sähköisestä allekirjoituksesta ja skeematiedoista.

Sähköisen allekirjoituksen on sisällettävä

i) issuerAuth - COSE_Sign1-objekti, joka on allekirjoitettu myöntävän viranomaisen **QSealC-yksityisavaimella**.

ii) suojattu otsikko, johon sisältyy alg = ES256 (allekirjoitusalgoritmi) ja x5t (COSE X.509-varmenteen hash-otsikkoparametri).

5. **Valinnaiset tiedot**

QR-koodi ei saa sisältää valinnaisia tietoja.

6. **Peruuttamistunniste (RID)**

Eurooppalaisen vammaisten henkilöiden pysäköintiluvan peruuttamistunnisteen on oltava liitteessä I olevan 6 kohdan mukainen.

Peruutettujen eurooppalaisten vammaisten henkilöiden pysäköintilupien peruuttamisluetteloissa on viitattava ainoastaan peruuttamistunnisteeseen. Korttien sarjanumeroita ei saa julkaista peruuttamisluetteloissa.

7. **Eurooppalaisen vammaisten henkilöiden pysäköintiluvan CBOR-hyötykuorma (QR-koodin sisällä)**

QR-hyötykuormaan on sisällytettävä ainoastaan seuraavat tiedot direktiivin (EU) 2024/2841 liitteessä II vahvistettujen eurooppalaisen vammaisten henkilöiden pysäköintiluvan (EPC) näkyvien tietokenttien mukaisesti.

Kenttä	**mDOC-polku**	**Tyyppi/muoto**
Tietoskeeman versio	issuerSigned.nameSpaces."eu.epc".ver	Merkkijono (esim. ”1.0”)

Korttityyppi: EPC	docType	Enum ("eu.epc")
Kortin sarjanumero	issuerSigned.nameSpaces."eu.epc".sub	Merkkijono
Peruuttamistunniste	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 tavua)
Kortin viimeinen voimassaolopäivä	issuerSigned.nameSpaces."eu.epc".exp	CBOR-tunniste 1004, sellaisena kuin se on määriteltynä standardissa RFC 8943 (2.1 kohta), joka sisältää UTF-8-tekstijonon, joka edustaa RFC 3339:n mukaista full-date-arvoa muodossa VVVV-KK-PP.

Sähköinen allekirjoitus on mukana issuerAuth-objektissa (COSE_Sign1-objekti). Varmenneketjua ei saa upottaa QR-koodin hyötykuormaan; sen sijaan suojatun COSE-otsikon on sisällettävä x5t, varmenteen sormenjälki, jota käytetään vastaavan QSealC-varmenteen paikantamiseen tarkastajan välimuistissa olevassa luotettujen varmenteiden säilössä.

8. Esimerkki eurooppalaisen vammaisten henkilöiden pysäköintiluvan QR-koodin hyötykuormasta: kommentoitu JavaScript Object Notation -tyylinen looginen esitys

Seuraava esimerkki on ihmisen luettavissa oleva JavaScript Object Notation (JSON) -esitys eurooppalaisen vammaisten henkilöiden pysäköintiluvan loogisesta näkymästä. Käytännössä tämä rakenne ei ole ihmisen luettavissa, koska sen on

a) oltava koodattu CBOR-rakenteena (RFC 8949, 3 jakso);

b) oltava allekirjoitettu käyttäen tunnisteetonta COSE_Sign1-rakennetta, jossa hyötykuorma on irrotettu (RFC 9052, 4 jakso);

c) sisällettävä voimassaolon päättymispäivä CBOR-tunnisteen 1004 full-date-arvona RFC 8943:n mukaisesti (2.1 kohta);

d) sisällettävä RFC 9360:n mukainen suojattu x5t-otsikkoparametri käyttäen SHA-256:ta DER-koodatussa loppukäyttäjän QSealC-varmenteessa; ja

e) oltava pakattu ja sen etuliitteenä on oltava merkkijono EP1:MDOC: ennen kuin se koodataan QR-koodiin.

{

// Vain JSON-tyylinen, ihmisen luettavissa oleva eurooppalaisen vammaisten henkilöiden pysäköintiluvan looginen näkymä.

// Todellinen QR-hyötykuorma on deterministinen CBOR, ei JSON.

"docType": "eu.epc", // eurooppalaisen vammaisten henkilöiden pysäköintiluvan valtuustieto. Sisältää docType-arvon sekä

// issuerSigned-objektin, COSE_Sign1-muotoisen ulkoisen hyötykuorman.

"issuerSigned": {

// IssuerAuth-objektilla suojatut tiedot; käytetään irrotettuna hyötykuormana.

// Allekirjoituksen luomisen ja todentamisen osalta irrotettu ulkoinen hyötykuorma kattaa sekä

// docType:n että issuerSigned:n.

"nameSpaces": {

"eu.epc": {

"ver": "1.0", // QR-profiilin/skeeman versio

// Kortin sarjanumero; myöntäjän määrittelemä, enintään 24 merkkiä.

"sub": "EF1234567890123456789OGH",

// Peruuttamistunniste: tosiasiallisesti CBOR bstr, 16 tavua/128 bittiä.

// Näytetään tässä 32:na hex-merkkinä luettavuuden vuoksi.

"rid": "4a8d9c112233445566778899aabbccdd",

// Tosiasiallisessa CBOR-koodauksessa käytetään tunnistetta 1004 RFC 3339:n mukaisessa full-date-arvossa.

```
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Todellinen muoto: tunnisteeton COSE_Sign1, ei JSON-objekti.
  "type": "COSE_Sign1",
  "tagged": false, // koodattu ilman COSE_Sign1 CBOR -tunnistetta
  "payload": "detached", // COSE-hyötykuormakenttä on CBOR ”null”

  "protectedHeader": {
    // alg: ES256; vastaava COSE-otsikkoparametri 1 = -7.
    "alg": "ES256",

    // x5t: varmenteen sormenjälki; COSE-otsikkoparametri 34.
    "x5t": {
      "hashAlg": "SHA-256", // vastaava COSE:n hash-arvo -16

      // DER-koodatun loppukäyttäjän QSealC-varmenteen SHA-256-hash.
      // 32 tavua esitettynä 64:na hex-merkkinä.
      "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // tyhjä tässä esimerkissä
```

// ES256 COSE-allekirjoitus: 64 tavua = 128 hex-merkkiä.

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Salausmekanismien käyttö

Jos tämän liitteen yhteydessä käytetään salausmekanismeja, siinä on noudatettava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymiä ja Euroopan unionin kyberturvallisuusviraston (ENISA) julkaisemia sovittuja salausmekanismeja.

LIITE III

6 ARTIKLAN 2 KOHDASSA TARKOITETTUJEN TIETOJEN ILMOITTAMINEN

1. Jäsenvaltioiden on annettava komissiolle seuraavat tiedot kustakin toimivaltaisesta viranomaisesta tai elimestä, joka vastaa eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä:

   a) eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavan toimivaltaisen viranomaisen tai elimen nimi;

   b) eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavan toimivaltaisen viranomaisen tai elimen rekisterinumero;

   c) eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavan toimivaltaisen viranomaisen tai elimen sähköpostiosoite ja puhelinnumero;

   d) yksi tai useampi varmenne, jota voidaan käyttää eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavan toimivaltaisen viranomaisen tai elimen luoman sähköisen leiman todentamiseen ja jonka osalta varmennettuihin henkilöllisyystietoihin sisältyvät a ja b alakohdassa täsmennetyt myöntäjän nimi ja rekisterinumero;

   e) sen paikan URL-osoite, jossa myöntäjä julkaisee tiedon eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden voimassaolotilasta.

2. Jäsenvaltiot voivat antaa komissiolle seuraavat tiedot kustakin toimivaltaisesta viranomaisesta tai elimestä, joka vastaa eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä:

   a) sen verkkosivun URL-osoite, joka sisältää eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavan toimivaltaisen viranomaisen tai elimen toimintaperiaatteet ja ehdot, joita sovelletaan eurooppalaisen vammaiskortin ja eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden tarjoamiseen ja käyttöön;

   b) tarvittaessa sen verkkosivun URL-osoite, joka sisältää lisätietoja eurooppalaisen vammaiskortin tai eurooppalaisen vammaisten henkilöiden pysäköintiluvan fyysisten versioiden myöntämisestä vastaavasta toimivaltaisesta viranomaisesta tai elimestä.

LIITE IV

EUROOPPALAISEN VAMMAISKORTIN TAI EUROOPPALAISEN VAMMAISTEN HENKILÖIDEN PYSÄKÖINTILUVAN FYYSISTEN VERSIOIDEN PERUUTTAMISLUETTELON TEKNISET ERITELMÄT

1. Tätä liitettä sovellettaessa tunnisteen on vastattava liitteessä I olevassa 6 kohdassa ja liitteessä II olevassa 6 kohdassa määriteltyä peruuttamistunnistetta (RID).

2. Peruuttamisluettelo on toteutettava tunnisteluettelotokenina CWT-muodossa (RFC 8392, 7 jakso) token-statusluetteloa koskevan eritelmän 5.2 kohdan (draft-ietf-oauth-status-list-14) mukaisesti seuraavin muutoksin:

   a) tyyppiä koskevan väitteen arvon on oltava ”application/identifierlist+cwt”;

   b) voimassaolon päättymisajankohtaa koskeva väite on esitettävä;

   c) CWT-väitteiden joukossa ei saa olla StatusList-väitettä;

   d) jäljempänä 3 kohdassa määritelty IdentifierList-rakenne on esitettävä väitteenä CWT-väitejoukossa käyttäen avainta 65530;

   e) CWT:n on oltava COSE_Sign1-objekti, jossa allekirjoituksen laskentaan käytetään Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymien ja Euroopan unionin kyberturvallisuusviraston (ENISA) julkaisemien sovittujen salausmekanismien mukaista allekirjoitusalgoritmia;

   f) CWT:ssä on oltava x5chain-parametri, sellaisena kuin se on määritelty standardissa RFC 9360 (2 jakso), suojatussa otsikossa, joka sisältää varmenteen tai varmenneketjun peruuttamisluettelon allekirjoituksen todentamiseksi;

   g) tunnisteluettelon allekirjoitusvarmenteessa voidaan käyttää token-statusluettelon eritelmässä (draft-ietf-oauth-status-list-14) määriteltyä avaimen laajennetun käytön objektitunnistetta, ja on suositeltavaa, että tarkastajat tukevat token-statusluettelon eritelmässä määriteltyä avaimen laajennetun käytön objektitunnistetta ja että myöntäjäviranomaisen infrastruktuurit eivät tee avaimen laajennettua käyttöä koskevasta kentästä kriittistä, kun käytetään token-statusluettelon eritelmässä määriteltyä avaimen laajennetun käytön objektitunnistetta.

3. IdentifierList-rakenteen on oltava CBOR-rakenne, jossa on seuraava CDDL (Concise Data Definition Language):

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

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

Identifier = bstr

Aggregation_uri = tstr