Euroopa Liidu
Nõukogu

Brüssel, 10. juuli 2026
(OR. en)

11772/26
ADD 1

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

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	1. juuli 2026
Saaja:	Thérèse BLANCHET, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	C(2026) 4534 annex
Teema:	LISAD järgmise dokumendi juurde: KOMISJONI DELEGEERITUD MÄÄRUS (EL) .../..., millega täiendatakse direktiivi (EL) 2024/2841 seoses Euroopa puudega inimese kaardi füüsilise versiooni ruutkoodi kindlaksmääramisega, Euroopa puudega inimese parkimiskaardi füüsilise versiooni ruutkoodi kindlaksmääramisega ja selle füüsilise versiooni turvalisust tagava ühtse tehnilise kirjelduse kehtestamisega ning koostalitlusvõime küsimustega

EUROOPA
KOMISJON

Brüssel, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

LISAD

järgmise dokumendi juurde:

KOMISJONI DELEGEERITUD MÄÄRUS (EL) .../...,

millega täiendatakse direktiivi (EL) 2024/2841 seoses Euroopa puudega inimese kaardi füüsilise versiooni ruutkoodi kindlaksmääramisega, Euroopa puudega inimese parkimiskaardi füüsilise versiooni ruutkoodi kindlaksmääramisega ja selle füüsilise versiooni turvalisust tagava ühtse tehnilise kirjelduse kehtestamisega ning koostalitlusvõime küsimustega

I LISA

EUROOPA PUUDEGA INIMESE KAARDI FÜÜSILISE VERSIOONI RUUTKOODI TEHNILINE KIRJELDUS

1. **Euroopa puudega inimese kaardi (EDC) füüsilise versiooni ruutkoodi vorming**

a) **Ruutkoodi mudeli 2 vorming** kooskõlas ruutkoodi rahvusvahelise tehnilise kirjeldusega ISO/IEC 18004:2024 või samaväärsete standarditega.

b) **Veaparandustase M** (taastab 15 %), mis tagab prinditud ruutkoodi vastupidavuse kriimustustele või osalistele kahjustustele.

c) **Kodeerimisrežiim:** ruutkoodi andmelast peab koosnema kombineeritud CBORi (issuerSigned Concise Binary Object Representation ehk väljaandja allkirjastatud kompaktne kahendobjektide esitus) struktuurist ja vastavast väljaandja autenditud allkirjaobjektist issuerAuth COSE_Sign1, nagu on määratletud dokumendis „CBOR Object Signing and Encryption“ (CBOR objektide allkirjastamine ja krüpteerimine) (COSE, RFC 9052, jaotised 3.1, 4.2 ja 4.4), järgides andmemudeli mDOC mustrit issuerSigned-elementide jaoks, kuid kohandatuna staatilise füüsilise kaardi kasutamiseks. issuerAuth peab olema COSE_Sign1 objekt, milles alg = ES256 ja mille kaitstud päis sisaldab parameetrit x5t (COSE X.509 sertifikaadi räsipäise parameeter, mis on määratletud dokumendis RFC 9360 (jaotis 2); koostalitlusvõime tagamiseks peab x5t-s kasutatav räsialgoritm olema SHA-256).

d) Enne ruutkoodi kodeerimist tuleb kombineeritud CBOR/COSE-objekt **pakkida zlib-vormingus** (RFC 1950, jaotis 2.2), **kasutades deflate-algoritmi** (RFC 1951, jaotised 3.2 ja 4). Saadud pakitud baitide massiiv tuleb kodeerida **ruutkoodi baidirežiimis** (Byte Mode), tagades täieliku toetuse binaarsetele CBOR/COSE-andmelastidele ja erinevate skännerite kasutamise võimaluse.

Kõigi ruutkoodi andmelastis sisalduvate tekstiväljade puhul peavad väljaandjad kodeerima CBOR-tekstistringide tähemärgid Unicode UTF-8-na. Allkirjastatud andmelastile ei tohi kohaldada transliteratsiooni. Koostalitlusvõime tagamiseks peavad väljaandjad enne allkirjastamist kohaldama kõigile tekstiväljadele Unicode’i normaliseerimisvormi C (NFC).

e) **Eesliide:** Euroopa puudega inimese kaardi ruutkoodi string peab algama „ED1:MDOC:“. See tuvastab kaarditüübi ja kodeerimisprofiili. Eesliited on tõstutundlikud ja peavad olemas olema. Tundmatud või mittetoetatavad eesliited põhjustavad tagasilükkamise. Eesliide ja pakitud andmelast tuleb ruutkoodis kodeerida ühe baidirežiimi andmesegmendina.

f) **Minimaalne mooduli suurus ≥ 0,25 mm**, et tagada prinditud kaartidel loetavus.

g) **Maksimaalne versioon 20;** küljepikkusega kuni 97 × 97 moodulit.

2. **Euroopa puudega inimese kaardi allkirja genereerimise tehniline kirjeldus**

Kvalifitseeritud e-tempel (QSeal), mida kasutatakse Euroopa puudega inimese kaardi ruutkoodide pitseerimiseks, tagab, et kodeeritud andmed pärinevad volitatud väljaandjalt ja neid ei ole muudetud.

a) **Allkirja algoritm**: allkirja algoritm peab olema ES256 (elliptilise kõveraga digitaalallkirja algoritm (ECDSA) koos SHA-256-ga, kasutades P-256 kõverat), nagu

on määratletud dokumendis RFC 9053 (jaotis 2.1); COSEs tuvastatakse algoritm alg-päise parameetriga, nagu on määratletud dokumendis RFC 9052 (jaotis 3.1).

b) **Allkirjastamisvõti**: ruutkoodi andmelast tuleb allkirjastada, kasutades privaatvõtit, mis vastab kvalifitseeritud e-templi sertifikaadile (QSealC).

c) **COSE struktuur:** allkirja konteiner peab olema COSE_Sign1 objekt. Kaitstud päises peavad olema alg (ES256) ja x5t (COSE X.509 sertifikaadi räsipäise parameeter, mis on määratletud dokumendis RFC 9360 (jaotis 2); koostalitlusvõime tagamiseks peab x5t-s kasutatav räsialgoritm olema SHA-256). Kinnitamine peab tuginema x5t väärtuse kasutamisele, et leida vastav sertifikaat kontrollija kohalikust vahemällu salvestatud usaldushoidlast, mis on koostatud usaldusnimekirja põhjal, ning seejärel tuleb sertifikaadiahel ja sertifikaadi staatus kooskõlas eIDASi usaldusraamistikuga valideerida.

d) **Allkirjastamisstandard**: ruutkoodi andmelast tuleb allkirjastada COSE_Sign1 objektina kooskõlas RFC 9052-ga (jaotis 4) „CBOR objektide allkirjastamine ja krüpteerimine“. COSE_Sign1 objekt asub issuerAuth-is ja kodeeritakse ilma CBOR-sildita COSE_Sign1 jaoks. COSE_Sign1 objekti andmelasti väli eraldatakse ja kodeeritakse kui CBOR null. Allkirja genereerimiseks ja kontrollimiseks kasutatud välisandmelast on deterministlik CBOR kodeeritud struktuur, mis sisaldab docType-väärtust ja issuerSigned-väärtust kõrgeima taseme CBOR kaardilt.

e) **Räsialgoritm**: allkirja genereerimiseks ja terviklikkuse kontrollimiseks tuleb kasutada SHA-256-t osana ES256-st.

f) **Kodeerimine**: andmelast tuleb kodeerida CBORi abil (RFC 8949, jaotis 4.2), nagu on nõutud COSE ja mDOCi tehnilistes kirjeldustes, tagades allkirjastatud andmete kodeerimise ja taasesitatavuse.

3. **Printimise tehniline kirjeldus**

a) **Vaikne ala**: ruutkoodi peab igast küljest ümbritsema **4 mooduli** laiune vaikne ala, millel ei tohi olla trükist, mustrit ega tausta.

b) **Kontrast**: ruutkood tuleb printida valgele taustale, minimaalse kontrastisuhtega **4:1**, et tagada erinevates valgustingimustes hea loetavus.

c) Ruutkood prinditakse direktiivi (EL) 2024/2841 I lisas määratletud värviga, mis tagab maksimaalse kontrastsuse.

d) **Paigutus ja suurus**: Ruutkood, vaikne ala kaasa arvatud, peab olema suurusega 26,25 mm × 26,25 mm ja asuma kaardi tagaküljel paremas alumises nurgas. Ruutkood peab olema maksimaalselt versioon 20 (97 × 97 moodulit), kusjuures mooduli suurus on 0,25 mm või rohkem.

Ruutkood, vaikne ala kaasa arvatud, tuleb paigutada vähemalt 5 mm kaugusele kaardi paremast servast ja vähemalt 5 mm kaugusele selle alumisest servast.

4. **Andmed Euroopa puudega inimese kaardi ruutkoodis**

Kooskõlas määruse (EL) 2016/679 artikli 5 lõike 1 punktis c sätestatud võimalikult väheste andmete kogumise põhimõttega peab ruutkood sisaldama minimaalset võrguühenduseta kontrollitavat andmekogumit. Andmelasti struktuur peab olema järgmine:

a) kaardi atribuudid on kodeeritud CBORis issuerSigned-objekti sees;

b) struktuur on pakitud ja allkirjastatud väljaandva asutuse QSeal-iga kui issuerAuth (COSE_Sign1, ES256, kaasa arvatud x5t, COSE X.509 sertifikaadi räsipäise parameeter);

c) Saadud CBOR/COSE-objekt tuleb pakkida kooskõlas käesoleva lisa punkti 1 alapunktiga d. Ruutkoodi andmelast koosneb eesliitest „ED1:MDOC:“, millele järgneb saadud pakitud baitide massiiv, ning kogu andmelast kodeeritakse baidirežiimis ühe ruutkoodi andmesegmendina.

Andmekogum peab koosnema direktiivi (EL) 2024/2841 I lisas loetletud kaardi esikülje väljade nähtavatest andmetest (eesnimi, perekonnanimi, kaardi seerianumber, kehtivusaeg) koos kehtetuks tunnistamise identifikaatori, elektroonilise allkirja ja skeemiteabega.

Elektrooniline allkiri peab sisaldama järgmist:

i) issuerAuth – COSE_Sign1 objekt, mis on allkirjastatud väljaandva asutuse **QSealC privaatvõtmega**;

ii) kaitstud päis, milles sisaldub alg = ES256 (allkirja algoritm) ja x5t (COSE X.509 sertifikaadi räsipäise parameeter).

5. Valikulised andmed

Ruutkoodi ei tohi lisada valikulisi andmeid.

6. Kehtetuks tunnistamise identifikaator (RID)

Lisaks nähtavale kaardi seerianumbrile peab ruutkood sisaldama spetsiaalset kehtetuks tunnistamise identifikaatorit (RID).

RID-d kasutatakse kehtetuks tunnistamise staatuse kindlaksmääramiseks ja kehtetuks tunnistatud kaartide loendi haldamiseks. RID-d ei tohi printida kaardile ega kuvada kaardi kontrollijatele.

6.1. *RID nõuded*

RID:

a) peab olema lisatud allkirjastatud ruutkoodi andmelasti;

b) peab olema vähemalt väljaandva asutuse väljastamisdomeenis kordumatu;

c) ei tohi olla kaardile prinditud ega olla inimloetav;

d) ei tohi paljastada isikuandmeid ega olla otseselt tähenduslik;

e) ei tohi olla otseselt kaardi nähtavast seerianumbrist tuletatav ja

f) peab olema kvalifitseeritud e-templi kaudu ruutkoodi andmelastiga krüptograafiliselt seotud.

6.2. *RID vorming ja suurus*

RID tuleb kodeerida CBOR-baidijadana (bstr). RID pikkus peab olema 16 baiti (128 bitti).

RID-i peab genereerima väljaandev asutus, kasutades tema kontrolli all olevat meetodit, mis tagab piisava entroopia ja vastupidavuse äraarvamisel või loendamisel põhinevatele manipulatsioonidele.

6.3. *Kehtetuks tunnistatud kaartide loendid*

Kontrollimise jaoks avaldatud kehtetuks tunnistatud kaartide loendid peavad viitama ainult kehtetuks tunnistatud kaartide RID-le. Kaartide seerianumbreid ei tohi kehtetuks tunnistatud kaartide loendites avaldada.

7. Euroopa puudega inimese kaardi CBOR-andmelast (ruutkoodi sees)

Ruutkoodi andmelast peab sisaldama ainult järgmisi andmeid, mis on kooskõlas direktiivi (EL) 2024/2841 I lisas sätestatud Euroopa puudega inimese kaardi nähtavate andmeväljadega.

Ülemise taseme sisu:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" koos allpool tabelis esitatud atribuutidega

c) issuerAuth = COSE_Sign1 (QSeal)

Väli	**mDOC tee**	**Tüüp/vorming**
Andmeskeemi versioon	issuerSigned.nameSpaces."eu.edc".ver	String (nt "1.0")
Kaardi tüüp: EDC	docType	Enum ("eu.edc")
Kaardi seerianumber	issuerSigned.nameSpaces."eu.edc".sub	String
Kehtetuks tunnistamise identifikaator	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 baiti)
Kaardiomaja eesnimi	issuerSigned.nameSpaces."eu.edc".givenName	Unicode-tekstistring (UTF-8)
Kaardiomaja perekonnanimi	issuerSigned.nameSpaces."eu.edc".familyName	Unicode-tekstistring (UTF-8)
Kaardi kehtivusaeg	issuerSigned.nameSpaces."eu.edc".exp	CBOR-silt 1004, nagu on määratletud dokumendis RFC 8943 (jaotis 2.1), mis sisaldab UTF-8 tekstistringi, mis tähistab

		RFC 3339 kohast full-date-väärtust vormingus AAAA-KK-PP

Elektrooniline allkiri asub issuerAuth-is (COSE_Sign1 objekt). Sertifikaadiahelat ei tohi ruutkoodi andmelasti integreerida; selle asemel peab kaitstud COSE päis sisaldama x5t-d, sertifikaadi sõrmejälge, mida kasutatakse vastava QSealC leidmiseks kontrollija vahemällu salvestatud usaldushoidlast.

8. **Euroopa puudega inimese kaardi ruutkoodi andmelasti näide: kommenteeritud JavaScript Object Notation-vormingus loogiline esitus**

Järgmine näide on Euroopa puudega inimese kaardi loogilise vaate inimloetav JavaScript Object Notation- (JSON-) vormingus esitus. Praktikas ei tohi see struktuur olla inimloetav, kuna see peab olema

a) kodeeritud CBORis (RFC 8949, jaotis 3);

b) allkirjastatud, kasutades sildita COSE_Sign1 struktuuri, kus andmelast on eraldatud (RFC 9052, jaotis 4);

c) sisaldab aegumiskuupäeva CBOR-sildi 1004 full-date-väärtusena kooskõlas RFC 8943-ga (jaotis 2.1);

d) sisaldab x5t kaitstud päise parameetrit kooskõlas RFC 9360-ga, kasutades SHA-256-d DER-kodeeritud lõppkasutaja QSealC-s; ja

e) pakitud ja eesliidetud stringiga ED1:MDOC: enne kui see kodeeritakse ruutkoodi.

```
{
 // JSON-vormingus, ainult inimloetav Euroopa puudega inimese kaardi loogiline vaade.
 // Tegelik ruutkoodi andmelast on deterministlik CBOR, mitte JSON.
 "docType": „eu.edc“,// Euroopa puudega inimese kaardi mandaat. Sisaldab docType-väärtust koos
  //issuerSignediga, COSE_Sign1 välisandmelastis.

 "issuerSigned": {
  // Andmed kaitstud issuerAuth-ga; kasutatakse eraldatud andmelastina.
  // Allkirja genereerimiseks ja kontrollimiseks hõlmab eraldatud välisandmelast mõlemat:
  //docType’i ja issuerSigned’.
  "nameSpaces": {
   "eu.edc": {
    "ver": „1.0“,// Ruutkoodi profiil/skeemi versioon

    // Kaardi seerianumber; väljaandja määratud, kuni 24 märki.
    "sub": "AB12345678901234567890CD",
```

```
      // Kehtetuks tunnistamise identifikaator: tegelik CBOR bstr, 16 baiti/128 bitti.
      // Siin loetavuse huvides näidatud 32 kuueteistkümnendmärgina.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ann",    // Euroopa puudega inimese kaardile prinditud eesnimi
      "familyName": "Other", // Euroopa puudega inimese kaardile prinditud perekonnanimi

      // Tegelikul CBOR-kodeerimisel kasutatakse RFC 3339 full-date-väärtuse silti 1004.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Tegelik vorm: sildita COSE_Sign1, mitte JSON-objekt.
  "type": "COSE_Sign1",
  "tagged": false,       // kodeeritud ilma COSE_Sign1 CBOR-sildita
  "payload": "detached", // COSE-andmelasti väli on CBOR null

  "protectedHeader": {
    // alg: ES256; samaväärne COSE päise parameeter 1 = -7.
    "alg": "ES256",

    // x5t: sertifikaadi sõrmejälg; COSE päise parameeter 34.
    "x5t": {
      "hashAlg": „SHA-256“ // samaväärne COSE räsiväärtus -16
```

```
        // DER-kodeeritud lõppkasutaja QSealC SHA-256 räsi
        // 32 baiti, esitatud 64 kuueteistkümnendmärgina.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // siin näites tühi

    // ES256 COSE allkiri: 64 baiti = 128 kuueteistkümnendmärki.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. Krüptograafiliste mehhanismide kasutamine

Käesoleva lisa kontekstis peab krüptograafiliste mehhanismide kasutamine olema kooskõlas Euroopa küberjulgeoleku sertifitseerimise rühma poolt heaks kiidetud ja Euroopa Liidu Küberturvalisuse Ameti (ENISA) poolt avaldatud kokkulepitud krüptograafiliste mehhanismidega.

II LISA

EUROOPA PUUDEGA INIMESE PARKIMISKAARDI FÜÜSILISE VERSIOONI RUUTKOODI TEHNILINE KIRJELDUS

1. **Euroopa puudega inimese parkimiskaardi (EPC) füüsilise versiooni ruutkoodi vorming**

a) **Ruutkoodi mudeli 2 vorming** kooskõlas ruutkoodi rahvusvahelise tehnilise kirjeldusega ISO/IEC 18004:2024 või samaväärsete standarditega.

b) **Veaparandustase M** (taastab 15 %), mis tagab prinditud ruutkoodi vastupidavuse kriimustustele või osalistele kahjustustele.

c) **Kodeerimisrežiim:** ruutkoodi andmelast peab koosnema kombineeritud CBORi (issuerSigned Concise Binary Object Representation ehk väljaandja allkirjastatud kompaktne kahendobjektide esitus) struktuurist ja vastavast väljaandja autenditud allkirjaobjektist issuerAuth COSE_Sign1, nagu on määratletud dokumendis „CBOR Object Signing and Encryption“ (CBOR objektide allkirjastamine ja krüpteerimine) (COSE, RFC 9052, jaotised 3.1, 4.2 ja 4.4), järgides andmemudeli mDOC mustrit issuerSigned-elementide jaoks, kuid kohandatuna staatilise füüsilise kaardi kasutamiseks. issuerAuth peab olema COSE_Sign1 objekt, milles alg = ES256 ja mille kaitstud päis sisaldab parameetrit x5t (COSE X.509 sertifikaadi räsipäise parameeter, mis on määratletud dokumendis RFC 9360 (jaotis 2); koostalitlusvõime tagamiseks peab x5t-s kasutatav räsialgoritm olema SHA-256).

d) Enne ruutkoodi kodeerimist tuleb kombineeritud CBOR/COSE-objekt **pakkida zlib-vormingus (RFC 1950, jaotis 2.2), kasutades deflate-algoritmi** (RFC 1951, jaotised 3.2 ja 4). Saadud pakitud baitide massiiv tuleb kodeerida **ruutkoodi baidirežiimis** (Byte Mode), tagades täieliku toetuse binaarsetele CBOR/COSE-andmelastidele ja erinevate skännerite kasutamise võimaluse.

Kõigi ruutkoodi andmelastis sisalduvate tekstiväljade puhul peavad väljaandjad kodeerima CBOR-tekstistringide tähemärgid Unicode UTF-8-na. Allkirjastatud andmelastile ei tohi kohaldada transliteratsiooni. Koostalitlusvõime tagamiseks peavad väljaandjad enne allkirjastamist kohaldama kõigile tekstiväljadele Unicode’i normaliseerimisvormi C (NFC).

e) **Eesliide**: Euroopa puudega inimese parkimiskaardi ruutkoodi string peab algama „EP1:MDOC:“-ga. See tuvastab kaarditüübi ja kodeerimisprofiili. Eesliited on tõstutundlikud ja peavad olemas olema. Tundmatud või mittetoetatavad eesliited põhjustavad tagasilükkamise. Eesliide ja pakitud andmelast tuleb ruutkoodis kodeerida ühe baidirežiimi andmesegmendina.

f) **Minimaalne mooduli suurus ≥ 0,35 mm**, et tagada prinditud kaartidel loetavus.

g) **Maksimaalne versioon 20**; küljepikkusega kuni 97 × 97 moodulit.

2. **Euroopa puudega inimese parkimiskaardi allkirja genereerimise tehniline kirjeldus**

Kvalifitseeritud e-tempel (QSeal), mida kasutatakse Euroopa puudega inimese parkimiskaardi ruutkoodide pitseerimiseks, tagab, et kodeeritud andmed pärinevad volitatud väljaandjalt ja neid ei ole muudetud.

a) **Allkirja algoritm**: allkirja algoritm peab olema ES256 (ECDSA koos SHA-256-ga, kasutades P-256 kõverat), nagu on määratletud dokumendis RFC 9053 (jaotis 2.1); COSEs tuvastatakse algoritm alg-päise parameetriga, nagu on määratletud dokumendis RFC 9052 (jaotis 3.1).

b) **Allkirjastamisvõti**: ruutkoodi andmelast tuleb allkirjastada, kasutades privaatvõtit, mis vastab kvalifitseeritud e-templi sertifikaadile (QSealC).

c) **COSE struktuur**: allkirja konteiner peab olema COSE_Sign1 objekt. Kaitstud päises peavad olema alg (ES256) ja x5t (COSE X.509 sertifikaadi räsipäise parameeter, mis on määratletud dokumendis RFC 9360 (jaotis 2); koostalitlusvõime tagamiseks peab x5t-s kasutatav räsialgoritm olema SHA-256). Kinnitamine peab tuginema x5t väärtuse kasutamisele, et leida vastav sertifikaat kontrollija kohalikust vahemällu salvestatud usaldushoidlast, mis on koostatud usaldusnimekirja põhjal, ning seejärel tuleb sertifikaadiahel ja sertifikaadi staatus kooskõlas eIDASi usaldusraamistikuga valideerida.

d) **Allkirjastamisstandard**: ruutkoodi andmelast tuleb allkirjastada COSE_Sign1 objektina kooskõlas RFC 9052-ga (jaotis 4) „CBOR objektide allkirjastamine ja krüpteerimine“. COSE_Sign1 objekt asub issuerAuth-is ja kodeeritakse ilma CBOR-sildita COSE_Sign1 jaoks. COSE_Sign1 objekti andmelasti väli eraldatakse ja kodeeritakse kui CBOR null. Allkirja genereerimiseks ja kontrollimiseks kasutatud välisandmelast on deterministlik CBOR kodeeritud struktuur, mis sisaldab docType-väärtust ja issuerSigned-väärtust kõrgeima taseme CBOR-kaardilt.

e) **Räsialgoritm**: allkirja genereerimiseks ja terviklikkuse kontrollimiseks tuleb kasutada SHA-256-t osana ES256-st.

f) **Kodeerimine**: andmelast tuleb kodeerida CBORi abil (RFC 8949, jaotis 4.2), nagu on nõutud COSE ja mDOCi tehnilistes kirjeldustes, tagades allkirjastatud andmete kodeerimise ja taasesitatavuse.

3. **Printimise tehniline kirjeldus**

a) **Vaikne ala**: ruutkoodi peab igast küljest ümbritsema **4 mooduli** laiune vaikne ala, millel ei tohi olla trükist, mustrit ega tausta.

b) **Kontrast**: ruutkood tuleb printida valgele taustale, minimaalse kontrastisuhtega **4:1**, et tagada erinevates valgustingimustes hea loetavus.

c) Ruutkood prinditakse direktiivi (EL) 2024/2841 II lisas määratletud värviga, mis tagab maksimaalse kontrastsuse.

d) **Paigutus ja suurus:** ruutkood, vaikne ala kaasa arvatud, peab olema suurusega **37 mm × 37 mm** ja asuma kaardi esiküljel alumises servas keskkohast veidi paremal. Ruutkood peab olema maksimaalselt versioon 20 (97 × 97 moodulit), kusjuures mooduli suurus on 0,35 mm või rohkem.

Ruutkood, vaikne ala kaasa arvatud, tuleb paigutada vähemalt 5 mm kaugusele kaardi alumisest servast.

4. **Andmed Euroopa puudega inimese parkimiskaardi ruutkoodis**

Kooskõlas määruse (EL) 2016/679 artikli 5 lõike 1 punktis c sätestatud võimalikult väheste andmete kogumise põhimõttega peab ruutkood sisaldama minimaalset võrguühenduseta kontrollitavat andmekogumit. Andmelasti struktuur on järgmine:

a) kaardi atribuudid on kodeeritud CBORis issuerSigned-objekti sees;

b) see struktuur on pakitud ja allkirjastatud väljaandva asutuse QSeal-iga kui issuerAuth (COSE_Sign1, ES256, kaasa arvatud x5t, COSE X.509 sertifikaadi räsipäise parameeter);

c) Saadud CBOR/COSE-objekt tuleb pakkida kooskõlas käesoleva lisa punkti 1 alapunktiga d. Ruutkoodi andmelast koosneb eesliitest „EP1:MDOC:“, millele järgneb saadud pakitud baitide massiiv, ning kogu andmelast kodeeritakse baidirežiimis ühe ruutkoodi andmesegmendina.

Andmekogum peab koosnema direktiivi (EL) 2024/2841 II lisas loetletud kaardi esikülje väljade nähtavatest andmetest (kehtivusaeg, kaardi seerianumber) koos kehtetuks tunnistamise identifikaatori, elektroonilise allkirja ja skeemiteabega.

Elektrooniline allkiri peab sisaldama järgmist:

i) issuerAuth – COSE_Sign1 objekt, mis on allkirjastatud väljaandva asutuse **QSealC privaatvõtmega**;

ii) kaitstud päis, milles sisaldub alg = ES256 (allkirja algoritm) ja x5t (COSE X.509 sertifikaadi räsipäise parameeter).

5. Valikulised andmed

Ruutkoodi ei tohi lisada valikulisi andmeid.

6. Kehtetuks tunnistamise identifikaator (RID)

Euroopa puudega inimese parkimiskaardi kehtetuks tunnistamise identifikaator peab vastama I lisa punktile 6.

Kehtetuks tunnistatud Euroopa puudega inimese parkimiskaartide loendid peavad viitama ainult RID-le. Kaartide seerianumbreid ei tohi kehtetuks tunnistatud kaartide loendites avaldada.

7. Euroopa puudega inimese parkimiskaardi CBOR-andmelast (ruutkoodi sees)

Ruutkoodi andmelast peab sisaldama ainult järgmisi andmeid, mis on kooskõlas direktiivi (EL) 2024/2841 II lisas sätestatud Euroopa puudega inimese parkimiskaardi nähtavate väljadega.

Väli	**mDOC tee**	**Tüüp/vorming**
Andmeskeemi versioon	issuerSigned.nameSpaces."eu.epc".ver	String (nt "1.0")
Kaardi tüüp: EPC	docType	Enum ("eu.epc")

Kaardi seerianumber	issuerSigned.nameSpaces."eu.epc".sub	String
Kehtetuks tunnistamise identifikaator	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 baiti)
Kaardi kehtivusaeg	issuerSigned.nameSpaces."eu.epc".exp	CBOR-silt 1004, nagu on määratletud dokumendis RFC 8943 (jaotis 2.1), mis sisaldab UTF-8 tekstistringi, mis tähistab RFC 3339 kohast full-date-väärtust vormingus AAAA-KK-PP

Elektrooniline allkiri peab asuma issuerAuth-is (COSE_Sign1 objekt). Sertifikaadiahelat ei tohi ruutkoodi andmelasti integreerida; selle asemel peab kaitstud COSE päis sisaldama x5t-d, sertifikaadi sõrmejälge, mida kasutatakse vastava QSealC leidmiseks kontrollija vahemällu salvestatud usaldushoidlast.

8. Euroopa puudega inimese parkimiskaardi ruutkoodi andmelasti näide: kommenteeritud JavaScript Object Notation-vormingus loogiline esitus

Järgmine näide on Euroopa puudega inimese parkimiskaardi loogilise vaate inimloetav JavaScript Object Notation- (JSON-) vormingus esitus. Praktikas ei tohi see struktuur olla inimloetav, kuna see peab olema

a) kodeeritud CBORis (RFC 8949, jaotis 3),

b) allkirjastatud, kasutades sildita COSE_Sign1 struktuuri eraldatud andmelastiga (RFC 9052, jaotis 4);

c) sisaldab aegumiskuupäeva CBOR-sildi 1004 full-date-väärtusena kooskõlas RFC 8943-ga (jaotis 2.1);

d) sisaldab x5t kaitstud päise parameetrit kooskõlas RFC 9360-ga, kasutades SHA-256-d DER-kodeeritud lõppkasutaja QSealC-s; ja

e) pakitud ja eesliidetud stringiga EP1:MDOC: enne kui see kodeeritakse ruutkoodi.

```
{
  // JSON-vormingus, ainult inimloetav Euroopa puude inimese parkimiskaardi loogiline vaade.
  // Tegelik ruutkoodi andmelast on deterministlik CBOR, mitte JSON.
  "docType": „eu.epc“,//Euroopa puude inimese parkimiskaardi mandaat. Sisaldab docType-väärtust koos
    //issuerSignediga, COSE_Sign1 välisandmelastis.

  "issuerSigned": {
    // Andmed kaitstud issuerAuth-ga; kasutatakse eraldatud andmelastina.
    // Allkirja genereerimiseks ja kontrollimiseks hõlmab eraldatud välisandmelast mõlemat:
    //docType’i ja issuerSigned’.
    "nameSpaces": {
      "eu.epc": {
        "ver": „1.0“,// Ruutkoodi profiil/skeemi versioon

        // Kaardi seerianumber; väljaandja määratud, kuni 24 märki.
        "sub": "EF123456789012345678 90GH",

        // Kehtetuks tunnistamise identifikaator: tegelik CBOR bstr, 16 baiti/128 bitti.
        // Siin loetavuse huvides näidatud 32 kuueteistkümnendmärgina.
        "rid": "4a8d9c112233445566778899aabbccdd",

        // Tegelikul CBOR-kodeerimisel kasutatakse RFC 3339 full-date-väärtuse silti 1004.
        "exp": "2030-12-31"
      }
    }
  },
```

```
 "issuerAuth": {
  // Tegelik vorm: sildita COSE_Sign1, mitte JSON-objekt.
  "type": "COSE_Sign1",
  "tagged": false,       // kodeeritud ilma COSE_Sign1 CBOR-sildita
  "payload": "detached", // COSE-andmelasti väli on CBOR null

  "protectedHeader": {
   // alg: ES256; samaväärne COSE päise parameeter 1 = -7.
   "alg": "ES256",

   // x5t: sertifikaadi sõrmejälg; COSE päise parameeter 34.
   "x5t": {
    "hashAlg": „SHA-256“ // samaväärne COSE räsiväärtus -16

    // DER-kodeeritud lõppkasutaja QSealC SHA-256 räsi
    // 32 baiti, esitatud 64 kuueteistkümnendmärgina.
    "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // siin näites tühi

  // ES256 COSE allkiri: 64 baiti = 128 kuueteistkümnendmärki.
  "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
```

}

}

9. Krüptograafiliste mehhanismide kasutamine

Käesoleva lisa kontekstis peab krüptograafiliste mehhanismide kasutamine olema kooskõlas Euroopa küberjulgeoleku sertifitseerimise rühma poolt heaks kiidetud ja Euroopa Liidu Küberturvalisuse Ameti (ENISA) poolt avaldatud kokkulepitud krüptograafiliste mehhanismidega.

III LISA

ARTIKLI 6 LÕIKES 2 OSUTATUD TEABEST TEATAMINE

1. Liikmesriigid esitavad komisjonile järgmise teabe iga pädeva asutuse või organi kohta, kes vastutab Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest:

   a) Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest vastutava pädeva asutuse või organi nimi;

   b) Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest vastutava pädeva asutuse või organi registreerimisnumber;

   c) Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest vastutava pädeva asutuse või organi e-posti aadress ja telefoninumber;

   d) üks või mitu sertifikaati, mida saab kasutada selle pädeva asutuse või organi loodud e-templi kontrollimiseks, kes vastutab enda väljaantavate Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest, ning mille sertifitseeritud isikuandmed sisaldavad vastavalt punktides a ja b nimetatud väljaandja nime ja registreerimisnumbrit;

   e) selle koha URL-aadress, kus väljaandja avaldab Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide kehtivuse staatuse.

2. Liikmesriigid võivad esitada komisjonile järgmise teabe iga pädeva asutuse või organi kohta, kes vastutab Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest:

   a) selle veebilehe URL-aadress, mis sisaldab Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest vastutava pädeva asutuse või organi põhimõtteid, tingimusi ja norme, mida kohaldatakse tema poolt väljaantava Euroopa puudega inimese kaardi ja Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise ja kasutamise suhtes;

   b) vajaduse korral selle veebilehe URL-aadress, mis sisaldab Euroopa puudega inimese kaardi või Euroopa puudega inimese parkimiskaardi füüsiliste versioonide väljaandmise eest vastutava pädeva asutuse või organi kohta lisateavet.

IV LISA

KEHTETUKS TUNNISTATUD EUROOPA PUUDEGA INIMESE KAARDI VÕI EUROOPA PUUDEGA INIMESE PARKIMISKAARDI FÜÜSILISTE VERSIOONIDE LOENDI TEHNILINE KIRJELDUS

1. Käesolevas lisas käsitletav identifikaator vastab I lisa punktis 6 ja II lisa punktis 6 määratletud kehtetuks tunnistamise identifikaatorile (RID).

2. Kehtetuks tunnistatud kaartide loend koostatakse identifikaatorite loendi tõendina CWT-vormingus (RFC 8392, jaotis 7) kooskõlas tõendite oleku loendi kirjelduse (draft-ietf-oauth-status-list-14) punktiga 5.2, võttes arvesse järgmisi muudatusi:

   a) tüübiväite väärtus on „application/identifierlist+cwt“;

   b) kehtivusaja väide peab olema olemas;

   c) StatusList-väidet ei tohi CWT väidete kogumis olla;

   d) punktis 3 määratletud IdentifierList-struktuur peab CWT väidete kogumis väitena olemas olema, kasutades võtit 65530;

   e) CWT peab olema COSE_Sign1 objekt, mis kasutab allkirja arvutamiseks allkirja algoritmi, mis on kooskõlas Euroopa küberjulgeoleku sertifitseerimise rühma poolt heaks kiidetud ja Euroopa Liidu Küberturvalisuse Ameti (ENISA) poolt avaldatud kokkulepitud krüptograafiliste mehhanismidega;

   f) CWT peab sisaldama dokumendis RFC 9360 (jaotis 2) määratletud x5chain-parameetrit kaitstud päises, mis sisaldab sertifikaati või sertifikaatide ahelat kehtetuks tunnistamise loendi allkirja kontrollimiseks;

   g) identifikaatorite loendi allkirjastamise sertifikaadi jaoks võib kasutada tõendite oleku loendi kirjelduses (draft-ietf-oauth-status-list-14) määratletud võtmekasutuslaiendi objektiidentifikaatorit ning soovitatav on, et kontrollijad toetaksid tõendite oleku loendi kirjelduses määratletud võtmekasutuslaiendi objektiidentifikaatorit ja et väljaandvate asutuste taristud ei muudaks võtmekasutuslaiendi välja kriitiliseks, kui kasutatakse tõendite oleku loendi kirjelduses määratletud võtmekasutuslaiendi objektiidentifikaatorit.

3. IdentifierList struktuur peab olema CBOR-struktuur, millel on järgmine CDDL (Concise Data Definition Language):

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

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

Identifier = bstr

Aggregation_uri = tstr