Eiropas Savienības Padome

Briselē, 2026. gada 10. jūlijā
(OR. en)

11772/26
ADD 1

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

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2026. gada 1. jūlijs
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	C(2026) 4534 annex
Temats:	PIELIKUMI dokumentam KOMISIJAS DELEĢĒTĀ REGULA (ES) .../..., ar ko Direktīvu (ES) 2024/2841 papildina saistībā ar kvadrātkoda noteikšanu Eiropas invaliditātes kartes fiziskai versijai un kvadrātkoda noteikšanu un tādu kopīgu tehnisko specifikāciju izveidi, kas nodrošina Eiropas stāvvietu kartes personām ar invaliditāti fiziskās versijas drošību, kā arī saistībā ar sadarbspējas jautājumiem

EIROPAS
KOMISIJA

Briselē, 1.7.2026.
C(2026) 4534 final

ANNEXES 1 to 4

PIELIKUMI

dokumentam

KOMISIJAS DELEĢĒTĀ REGULA (ES) .../...,

ar ko Direktīvu (ES) 2024/2841 papildina saistībā ar kvadrātkoda noteikšanu Eiropas invaliditātes kartes fiziskai versijai un kvadrātkoda noteikšanu un tādu kopīgu tehnisko specifikāciju izveidi, kas nodrošina Eiropas stāvvietu kartes personām ar invaliditāti fiziskās versijas drošību, kā arī saistībā ar sadarbspējas jautājumiem

I PIELIKUMS

EIROPAS INVALIDITĀTES KARTES FIZISKAJĀ VERSIJĀ IEKĻAUJAMĀ KVADRĀTKODA SPECIFIKĀCIJAS

1. **Eiropas invaliditātes kartes (*EDC*) fiziskajā versijā iekļaujamā kvadrātkoda formāts**

(a) **Kvadrātkoda 2. parauga formāts** saskaņā ar starptautiskajām kvadrātkoda specifikācijām ISO/IEC 18004:2024 vai līdzvērtīgām specifikācijām.

(b) **Kļūdu korekcijas līmenis M** (15 % redundance), kas nodrošina noturību pret iespiesta kvadrātkoda skrāpējumiem vai daļējiem bojājumiem.

(c) **Kodēšanas režīms:** kvadrātkoda vērtums sastāv no apvienotās issuerSigned īsā binārā objekta attēlojuma (*Concise Binary Object Representation* (*CBOR*)) struktūras un atbilstoša issuerAuth COSE_Sign1 paraksta objekta, kā definēts *CBOR* objekta parakstīšanā un šifrēšanā (*COSE*, RFC 9052 3.1., 4.2. un 4.4. iedaļa), ievērojot mDOC datu modeļa rakstu attiecībā uz issuerSigned vienumiem, bet pielāgojot statiskam fiziskās kartes lietojumam. IssuerAuth ir COSE_Sign1 objekts ar alg = ES256 un aizsargātu galveni, kas satur x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametrs, kas definēts RFC 9360 (2. iedaļa); sadarbspējas nodrošināšanai x5t izmantotais jaucējalgoritms ir SHA-256).

(d) Pirms kvadrātkoda kodēšanas apvienoto *CBOR/COSE* objektu **saspiež, izmantojot zlib formātu** (RFC 1950, 2.2. iedaļa) **ar *deflate*** algoritmu (RFC 1951, 3.2. un 4. iedaļa). Iegūto saspiesto baitu masīvu kodē **kvadrātkodā baitu režīmā**, nodrošinot pilnīgu atbalstu bināro *CBOR/COSE* vērtumu un skeneru sadarbspējai.

Attiecībā uz visiem teksta laukiem, kas iekļauti kvadrātkoda vērtumā, karšu izdevēji *CBOR* teksta virknēs kodē rakstzīmes kā *Unicode UTF-8*. Transliterāciju nepiemēro parakstītiem vērtuma datiem. Sadarbspējas nolūkā karšu izdevēji pirms parakstīšanas visiem teksta laukiem piemēro *Unicode Normalisation Form C* (*NFC*).

(e) **Prefikss:** *EDC* kvadrātkoda virkne sākas ar "ED1:MDOC:". Tas identificē kartes veidu un kodēšanas profilu. Prefiksi ir reģistrjutīgi, un tiem ir jābūt. Nezināmi vai nepamatoti prefiksi izraisa noraidījumu. Prefiksu un saspiesto vērtumu kodē kvadrātkodā kā vienu baita režīma datu segmentu.

(f) **Moduļa minimālais izmērs ≥ 0,25 mm**, lai nodrošinātu lasāmību uz drukātām kartēm.

(g) **Maksimālā versija ir versija 20,** ar līdz 97 × 97 moduļiem katrā pusē.

2. ***EDC* paraksta ģenerēšanas specifikācijas**

Kvalificētais elektroniskais zīmogs (*QSeal*), ko izmanto *EDC* kvadrātkodu apzīmogošanai, nodrošina, ka kodētie dati nāk no pilnvarotās izdevējiestādes un nav mainīti.

(a) **Paraksta algoritms**: paraksta algoritms ir ES256 (elliptiskās līknes digitālā paraksta algoritms (*ECDSA*) ar SHA-256, izmantojot P-256 līkni), kā definēts RFC 9053 (2.1. iedaļa); *COSE* algoritmu identificē ar alg galvenes parametru RFC 9052 (3.1. iedaļa).

(b) **Parakstīšanas atslēga**: kvadrātkoda vērtumu paraksta, izmantojot privāto atslēgu, kas atbilst kvalificētam elektroniskā zīmoga sertifikātam (*QSealC*).

(c) ***COSE* struktūra:** paraksta konteiners ir COSE_Sign1 objekts. Aizsargātā galvene ietver alg (ES256) un x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametru, kas definēts RFC 9360 (2. iedaļa); sadarbspējas nodrošināšanai x5t izmantotais jaucējalgoritms ir SHA-256). Verifikācija balstās uz x5t vērtības izmantošanu, lai atrastu attiecīgo sertifikātu verificētāja vietējā kešatmiņā saglabātajā uzticamības krātuvē, kas izveidota no uzticamā saraksta informācijas, un pēc tam tā validē sertifikāta ķēdi un sertifikāta statusu saskaņā ar *eIDAS* uzticamības satvaru.

(d) **Paraksta standarts**: kvadrātkoda vērtumu paraksta kā COSE_Sign1 objektu saskaņā ar RFC 9052 (4. iedaļa) "*CBOR* objekta parakstīšana un šifrēšana". Objektu COSE_Sign1 iekļauj *issuerAuth* un kodē bez COSE_Sign1 CBOR birkas. COSE_Sign1 objekta vērtuma lauklu atdala un kodē kā CBOR nulli. Paraksta ģenerēšanai un verifikācijai ārējais vērtums ir determinēta CBOR kodēta struktūra, kas satur docType vērtību un issuerSigned vērtību no augstākā līmeņa CBOR kartes.

(e) **Jaucējalgoritms**: SHA-256 izmanto kā daļu no ES256 parakstu ģenerēšanai un integritātes verifikācijai.

(f) **Kodēšana**: vērtumu kodē, izmantojot *CBOR* (RFC 8949, 4.2. iedaļa), kā noteikts *COSE* un mDOC specifikācijās, nodrošinot parakstīto datu kodēšanu un reproducējamību.

3. **Drukāšanas specifikācijas**

(a) **Tukšā zona**: kvadrātkodu no visām pusēm aptver skaidra **četru moduļu** piemale bez drukājuma, raksta vai fona.

(b) **Kontrasts**: kvadrātkodu drukā uz balta fona ar minimālo kontrasta attiecību **4:1**, lai nodrošinātu augstu nolasāmību dažādos apgaismojuma apstākļos.

(c) Kvadrātkodu drukā, izmantojot Direktīvas (ES) 2024/2841 I pielikumā noteikto krāsu, kas nodrošina maksimālu kontrastu.

(d) **Izvietojums un izmērs**: kvadrātkods, ieskaitot tukšo zonu, ir 26,25 mm × 26,25 mm, un tas atrodas kartes aizmugurē apakšējā labajā stūrī. Kvadrātkoda maksimālā versija ir 20. versija (97 × 97 moduļi) ar moduļa izmēru 0,25 mm vai lielāku.

Kvadrātkodu, ieskaitot tukšo zonu, novieto vismaz 5 mm attālumā no kartes labās puses malas un vismaz 5 mm attālumā no kartes apakšējās malas.

4. ***EDC* kvadrātkodā ietvertie dati**

Kvadrātkods ietver minimālu bezsaistē verificējamu datu kopu saskaņā ar Regulas (ES) 2016/679 5. panta 1. punkta c) apakšpunktā noteikto datu minimizēšanas principu. Vērtuma struktūra ir šāda:

(a) kartes atribūti ir kodēti *CBOR* issuerSigned objektā;

(b) struktūra ir aplauzta un parakstīta ar izdevējiestādes *QSeal* kā issuerAuth (COSE_Sign1, ES256, ietverot x5t, *COSE* X.509 sertifikāta jaucējkoda galvenes parametru);

(c) Iegūto CBOR/COSE objektu saspiež saskaņā ar šā pielikuma 1. punkta d) apakšpunktu. Kvadrātkoda vērtumu veido prefikss "ED1:MDOC:", kam seko iegūtais saspiesto baitu masīvs, un visu vērtumu kodē, izmantojot baitu režīmu kā vienu kvadrātkoda datu segmentu.

Datu saturs ietver tādu redzamo datu apakškopu, kas ir kartes priekšpuses laukos, kuri uzskaitīti Direktīvas (ES) 2024/2841 I pielikumā (vārds, uzvārds, kartes sērijas numurs, derīguma termiņa beigu datums), kā arī atsaukšanas identifikatoru, elektronisko parakstu un shēmas informāciju.

Elektroniskais paraksts ietver:

i) issuerAuth – COSE_Sign1 objektu, kas parakstīts ar izdevējiestādes ***QSealC*** **privāto atslēgu**;

ii) aizsargātu galveni, kas ietver alg = ES256 (paraksta algoritms) un x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametrs).

5. Fakultatīvie dati

Kvadrātkodā neiekļauj fakultatīvos datus.

6. Atcelšanas identifikators (*RID*)

Papildus redzamajam kartes sērijas numuram kvadrātkodā iekļauj īpašu atsaukšanas identifikatoru (*RID*).

RID izmanto atsaukšanas statusa noteikšanai un atsaukšanas saraksta pārvaldībai. *RID* nedrukā uz kartes, un to nerāda kartes verificētājiem.

6.1. *Prasības attiecībā uz* RID

RID:

(a) jāiekļauj parakstītajā kvadrātkoda vērtumā;

(b) ir unikāls vismaz izdevējiestādes izdošanas domēnā;

(c) nav uzdrukāts uz kartes, un tas nav paredzēts tā, lai būtu cilvēklasāms;

(d) neatklāj personas datus un nav tieši jēgpilns;

(e) nav tieši atvasināms no redzamā kartes sērijas numura un

(f) kvalificēts elektroniskais zīmogs to kriptogrāfiski saista ar kvadrātkoda vērtumu.

6.2. RID *formāts un lielums*

RID kodē kā *CBOR* baitu virkni (bstr). *RID* ir 16 baitu (128 bitu) garumā.

RID ģenerē izdevējiestāde, izmantojot tās kontrolē esošu metodi, kas nodrošina pietiekamu entropiju un izturību pret uzminēšanu vai uzskaitīšanu.

6.3. *Atsaukšanas saraksti*

Pārbaudes vajadzībām publicētajos atsaukšanas sarakstos norāda tikai atsaukto karšu *RID*. Karšu sērijas numurus atsaukšanas sarakstos nepublicē.

7. ***EDC CBOR*** **vērtums (kvadrātkodā)**

Kvadrātkoda vērtumā iekļauj tikai šādus datus, kas atbilst redzamajiem *EDC* datu laukiem, kuri noteikti Direktīvas (ES) 2024/2841 I pielikumā.

Augšējā līmeņa saturs:

(a) docType = “eu.edc”

(b) issuerSigned.nameSpaces.“eu.edc” ar atribūtiem, kas norādīti turpmāk tabulā

(c) issuerAuth = COSE_Sign1 (*QSeal*)

Lauks	**mDOC ceļš**	**Veids/formāts**
Datu shēmas versija	issuerSigned.nameSpaces.“eu.edc”.ver	Virkne (piemēram, “1.0”)
Kartes veids: *EDC*	docType	Enum (“eu.edc”)
Kartes sērijas numurs	issuerSigned.nameSpaces.“eu.edc”sub	Virkne
Atcelšanas identifikators	issuerSigned.nameSpaces.“eu.edc.”rid	*CBOR* bstr (16 baiti)
Kartes turētāja vārds	issuerSigned.nameSpaces.“eu.edc.”givenName	*Unicode* teksta virkne (*UTF-8*)
Kartes turētāja uzvārds	issuerSigned.nameSpaces.“eu.edc”.familyName	*Unicode* teksta virkne (*UTF-8*)
Kartes derīguma termiņa beigu datums	issuerSigned.nameSpaces.“eu.edc”.exp	CBOR birka 1004, kā definēts RFC 8943 (2.1. iedaļa), kurā ir UTF-8 teksta virkne, kas reprezentē RFC 3339 pilnu datumu GGGG-MM-DD formātā.

Elektronisko parakstu iekļauj issuerAuth (COSE_Sign1 objekts). Sertifikātu ķēde nav iegulta kvadrātkoda vērtumā; tās vietā aizsargātajā *COSE* galvenē iekļauj x5t, sertifikāta nospiedumu, ko izmanto, lai attiecīgo *QSealC* varētu atrast verificētāja kešatmiņā saglabātajā uzticamības krātuvē.

8. **EDC kvadrātkoda vērtuma piemērs: “JavaScript Object Notation” veida loģisks attēlojums ar komentāriem**

Šis piemērs ir cilvēklasāms *JavaScript Object Notation* (*JSON*) EDC loģiskā pārskata attēlojums. Praksē šī struktūra nav cilvēklasāma, jo tā:

(a) ir kodēta *CBOR* (RFC 8949, 3. iedaļa);

b) ir parakstīta, izmantojot nemarķētu COSE_Sign1 struktūru ar atdalītu vērtumu (RFC 9052, 4. iedaļa),

c) ietver beigu datumu kā CBOR birkas 1004 pilna datuma vērtību saskaņā ar RFC 8943 (2.1. iedaļa);

d) ietver x5t aizsargātās galvenes parametru saskaņā ar RFC 9360, izmanotojot SHA-256 DER kodētajā gala vienībā QSealC, un

e) ir saspiesta un tai pievienots prefikss ar virkni ED1:MDOC: pirms kodēšanas kvadrātkodā.

```
{
 //JSON stilā, tikai cilvēklasāms EDC loģiskā pārskata attēlojums.
 //Faktiskais kvadrātkoda vērtums ir determinēts CBOR, nevis JSON.
 “docType”: “eu.edc”,//EDC apliecinājuma dokuments. Ir iekļauta docType vērtība kopā ar
  //issuerSigned, izmantojot COSE_Sign1 ārējo vērtumu.

 “issuerSigned”: {
  // issuerAuth aizsargāti dati; izmanto kā atdalītu vērtumu.
  //Paraksta ģenerēšanai un verifikācijai atdalītais ārējais vērtums aptver gan
  //docType un issuerSigned.
  “nameSpaces”: {
   “eu.edc”: {
    “ver”: “1.0”,//kvadrātkoda profils/shēmas versija

    // Kartes sērijas numurs; kartes izdevēja definēts, ne vairāk kā 24 rakstzīmes.
    “sub”: "AB1234567890123456789OCD",

    // Atcelšanas identifikators: faktiskais CBOR bstr, 16 baiti/128 biti.
```

```
      //Šeit attālotas kā 32 heksadecimālās rakstzīmes salasāmības nolūkā.
      “rid”: "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      “givenName”: “Ann”//uz EDC uzdrukātais vārds
      “familyName”: “Other”//uz EDC uzdrukātais uzvārds

      //Faktiskajā CBOR kodēšanā izmanto birku 1004 RFC 3339 pilnam datumam.
      “exp”: "2030-12-31"
    }
  }
},

“issuerAuth”: {
  // Faktiskā veidlapa: nemarķēts COSE_Sign1, nav JSON objekts.
  “tips”: "COSE_Sign1",
  “marķēts”: nepareizi          // kodēti bez COSE_Sign1 CBOR birkas
  “vērtums”: “atdalīts”,//COSE vērtuma lauks ir “CBOR null”

  “aizsargāts galvene”: {
    //alg: ES256; ekvivalentais COSE galvenes parametrs 1 = -7.
    "alg": "ES256",

    // x5t: sertifikāta nospiedums; COSE galvenes parametrs 34.
    "x5t": {
      "hashAlg": “SHA-256”//ekvivalenta COSE jaucējkoda vērtība -16

      // DER kodētas gala viernības QSealC SHA-256 jaucējkods.
```

//32 baiti, kas atveidoti kā 64 heksadecimālās rakstzīmes.

“jaucējkoda vērtība”:
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

“neaizsargāta galvene”: {},//tukša šajā piemērā

//ES256 COSE paraksts: 64 baiti = 128 heksadecimālās rakstzīmes.

“paraksts”
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Kriptogrāfijas mehānismu izmantošana

Šā pielikuma kontekstā kriptogrāfijas mehānismus izmanto saskaņā ar saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*).

II PIELIKUMS

EIROPAS STĀVVIETU KARTES PERSONĀM AR INVALIDITĀTI FIZISKAJĀ VERSIJĀ IEKĻAUJAMĀ KVADRĀTKODA SPECIFIKĀCIJAS

1. **Eiropas stāvvietu kartes personām ar invaliditāti (*EPC*) fiziskajā versijā iekļaujamā kvadrātkoda formāts**

(a) **Kvadrātkoda 2. parauga formāts** saskaņā ar starptautiskajām kvadrātkoda specifikācijām ISO/IEC 18004:2024 vai līdzvērtīgām specifikācijām.

(b) **Kļūdu korekcijas līmenis M** (15 % redundance), kas nodrošina noturību pret iespiesta kvadrātkoda skrāpējumiem vai daļējiem bojājumiem.

(c) **Kodēšanas režīms:** kvadrātkoda vērtums sastāv no apvienotās issuerSigned īsā binārā objekta attēlojuma (Concise Binary Object Representation (CBOR)) struktūras un atbilstoša issuerAuth COSE_Sign1 paraksta objekta, kā definēts CBOR objekta parakstīšanā un šifrēšanā (COSE, RFC 9052 3.1., 4.2. un 4.4. iedaļa), ievērojot mDOC datu modeļa rakstu attiecībā uz issuerSigned vienumiem, bet pielāgojot statiskam fiziskās kartes lietojumam. IssuerAuth ir COSE_Sign1 objekts ar alg = ES256 un aizsargātu galveni, kas satur x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametrs, kas definēts RFC 9360 (2. iedaļa); sadarbspējas nodrošināšanai x5t izmantotais jaucējalgoritms ir SHA-256).

(d) Pirms kvadrātkoda kodēšanas apvienoto *CBOR/COSE* objektu **saspiež, izmantojot zlib formātu (RFC 1950, 2.2. iedaļa) ar *deflate*** algoritmu (RFC 1951, 3.2. un 4. iedaļa). Iegūto saspiesto baitu masīvu kodē **kvadrātkodā baitu režīmā**, nodrošinot pilnīgu atbalstu bināro *CBOR/COSE* vērtumu un skeneru sadarbspējai.

Attiecībā uz visiem teksta laukiem, kas iekļauti kvadrātkoda vērtumā, karšu izdevēji *CBOR* teksta virknēs kodē rakstzīmes kā *Unicode UTF-8*. Transliterāciju nepiemēro parakstītiem vērtuma datiem. Sadarbspējas nolūkā karšu izdevēji pirms parakstīšanas visiem teksta laukiem piemēro *Unicode Normalisation Form C* (*NFC*).

(e) **Prefikss**: *EPC* kvadrātkoda virkne sākas ar "EP1:MDOC:". Tas identificē kartes veidu un kodēšanas profilu. Prefiksi ir reģistrjutīgi, un tiem ir jābūt. Nezināmi vai nepamatoti prefiksi izraisa noraidījumu. Prefiksu un saspiesto vērtumu kodē kvadrātkodā kā vienu baita režīma datu segmentu.

(f) **Moduļa minimālais izmērs ≥ 0,35 mm**, lai nodrošinātu lasāmību uz drukātām kartēm.

(g) **Maksimālā versija ir versija 20**, ar līdz 97 x 97 moduļiem katrā pusē.

2. ***EPC* paraksta ģenerēšanas specifikācijas**

Kvalificētais elektroniskais zīmogs (*QSeal*), ko izmanto *EPC* kvadrātkodu apzīmogošanai, nodrošina, ka kodētie dati nāk no pilnvarotās izdevējiestādes un nav mainīti.

(a) **Paraksta algoritms**: paraksta algoritms ir ES256 (*ECDSA* ar SHA-256, izmantojot P-256 līkni), kā definēts RFC 9053 (2.1. iedaļa); *COSE* algoritmu identificē ar alg galvenes parametru RFC 9052 (3.1. iedaļa).

(b) **Parakstīšanas atslēga**: kvadrātkoda vērtumu paraksta, izmantojot privāto atslēgu, kas atbilst kvalificētam elektroniskā zīmoga sertifikātam (*QSealC*).

(c) ***COSE* struktūra**: paraksta konteiners ir COSE_Sign1 objekts. Aizsargātā galvene ietver alg (ES256) un x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametrs, kas definēts RFC 9360 (2. iedaļa); sadarbspējas nodrošināšanai x5t izmantotais jaucējalgoritms ir SHA-256). Verifikācija balstās uz x5t vērtības izmantošanu, lai atrastu attiecīgo sertifikātu verificētāja vietējā kešatmiņā saglabātajā uzticamības krātuvē, kas izveidota no uzticamā saraksta informācijas, un pēc tam tā validē sertifikāta ķēdi un sertifikāta statusu saskaņā ar *eIDAS* uzticamības satvaru.

(d) **Paraksta standarts**: kvadrātkoda vērtumu paraksta kā COSE_Sign1 objektu saskaņā ar RFC 9052 (4. iedaļa) "*CBOR* objekta parakstīšana un šifrēšana". Objektu COSE_Sign1 iekļauj *issuerAuth* un kodē bez COSE_Sign1 CBOR birkas. COSE_Sign1 objekta vērtuma lauklu atdala un kodē kā CBOR nulli. Paraksta ģenerēšanai un verifikācijai ārējais vērtums ir determinēta CBOR kodēta struktūra, kas satur docType vērtību un issuerSigned vērtību no augstākā līmeņa CBOR kartes.

(e) **Jaucējalgoritms**: SHA-256 izmanto kā daļu no ES256 parakstu ģenerēšanai un integritātes verifikācijai.

(f) **Kodēšana**: vērtumu kodē, izmantojot *CBOR* (RFC 8949, 4.2. iedaļa), kā noteikts *COSE* un mDOC specifikācijās, nodrošinot parakstīto datu kodēšanu un reproducējamību.

3. **Drukāšanas specifikācijas**

(a) **Tukšā zona**: kvadrātkodu no visām pusēm aptver skaidra **četru moduļu** piemale bez drukājuma, raksta vai fona.

(b) **Kontrasts**: kvadrātkodu drukā uz balta fona ar minimālo kontrasta attiecību **4:1**, lai nodrošinātu augstu nolasāmību dažādos apgaismojuma apstākļos.

(c) Kvadrātkodu drukā, izmantojot Direktīvas (ES) 2024/2841 II pielikumā noteikto krāsu, kas nodrošina maksimālu kontrastu.

(d) **Izvietojums un izmērs:** kvadrātkods, ieskaitot tukšo zonu, ir **37 mm × 37 mm**, un tas atrodas kartes priekšpusē, nedaudz novirzīts no centra uz labo pusi un tuvāk apakšējai malai. Kvadrātkoda maksimālā versija ir 20. versija (97 × 97 moduļi) ar moduļa izmēru 0,35 mm vai lielāku.

Kvadrātkodu, ieskaitot tukšo zonu, novieto vismaz 5 mm attālumā no kartes apakšējās malas.

4. ***EPC* kvadrātkodā ietvertie dati**

Kvadrātkods ietver minimālu bezsaistē verificējamu datu kopu saskaņā ar Regulas (ES) 2016/679 5. panta 1. punkta c) apakšpunktā noteikto datu minimizēšanas principu. Vērtuma struktūra ir šāda:

(a) kartes atribūti ir kodēti *CBOR* issuerSigned objektā;

(b) struktūra ir aplauzta un parakstīta ar izdevējiestādes *QSeal* kā issuerAuth (COSE_Sign1, ES256, ietverot x5t, *COSE* X.509 sertifikāta jaucējkoda galvenes parametru);

(c) Iegūto CBOR/COSE objektu saspiež saskaņā ar šā pielikuma 1. punkta d) apakšpunktu. Kvadrātkoda vērtumu veido prefikss "EP1:MDOC:", kam seko iegūtais

saspiesto baitu masīvs, un visu vērtumu kodē, izmantojot baitu režīmu kā vienu kvadrātkoda datu segmentu.

Datu saturs ietver tādu redzamo datu apakškopu, kas ir kartes priekšpuses laukos, kuri uzskaitīti Direktīvas (ES) 2024/2841 II pielikumā (derīguma termiņa beigu datums, kartes sērijas numurs), kā arī atsaukšanas identifikatoru, elektronisko parakstu un shēmas informāciju.

Elektroniskais paraksts ietver:

i) issuerAuth – COSE_Sign1 objektu, kas parakstīts ar izdevējiestādes ***QSealC* privāto atslēgu**;

ii) aizsargātu galveni, kas ietver alg = ES256 (paraksta algoritms) un x5t (*COSE* X.509 sertifikāta jaucējkoda galvenes parametrs).

5. Fakultatīvie dati

Kvadrātkodā neiekļauj fakultatīvos datus.

6. Atcelšanas identifikators (*RID*)

EPC atcelšanas identifikators atbilst I pielikuma 6. punkta prasībām.

Atsaukšanas sarakstos atsauktajām *EPC* norāda tikai *RID*. Karšu sērijas numurus atsaukšanas sarakstos nepublicē.

7. *EPC CBOR* vērtums (kvadrātkodā)

Kvadrātkoda vērtumā iekļauj tikai šādus datus, kas atbilst redzamajiem *EPC* datu laukiem, kuri noteikti Direktīvas (ES) 2024/2841 II pielikumā.

Lauks	**mDOC ceļš**	**Veids/formāts**
Datu shēmas versija	issuerSigned.nameSpaces.“eu.epc”.ver	Virkne (piemēram, “1.0”)
Kartes veids: *EPC*	docType	Enum (“eu.epc”)
Kartes sērijas numurs	issuerSigned.nameSpaces.“eu.epc”sub	Virkne
Atcelšanas identifikators	issuerSigned.nameSpaces.“eu.epc”.rid	*CBOR* bstr (16 baiti)
Kartes derīguma termiņa beigu datums	issuerSigned.nameSpaces.“eu.epc”.exp	CBOR birka 1004, kā definēts RFC 8943 (2.1. iedaļa), kurā ir UTF-8 teksta

		virkne, kas reprezentē RFC 3339 pilnu datumu GGGG-MM-DD formātā.

Elektronisko parakstu iekļauj issuerAuth (COSE_Sign1 objekts). Sertifikātu ķēde nav iegulta kvadrātkoda vērtumā; tās vietā aizsargātajā *COSE* galvenē iekļauj x5t, sertifikāta nospiedumu, ko izmanto, lai attiecīgo *QSealC* varētu atrast verificētāja kešatmiņā saglabātajā uzticamības krātuvē.

8. EPC kvadrātkoda vērtuma piemērs: "JavaScript Object Notation" veida loģisks attēlojums ar komentāriem

Šis piemērs ir cilvēklasāms *JavaScript Object Notation* (*JSON*) EPC loģiskā pārskata attēlojums. Praksē šī struktūra nav cilvēklasāma, jo tā:

(a) kodēta *CBOR* (RFC 8949, 3. iedaļa);

(b) ir parakstīta, izmantojot nemarķētu COSE_Sign1 struktūru ar atdalītu vērtumu (RFC 9052, 4. iedaļa),

(c) ietver beigu datumu kā CBOR birkas 1004 pilna datuma vērtību saskaņā ar RFC 8943 (2.1. iedaļa);

(d) ietver x5t aizsargātās galvenes parametru saskaņā ar RFC 9360, izmanotojot SHA-256 DER kodētajā gala vienībā QSealC, un

(e) ir saspiesta un tai pievienots prefikss ar virkni EP1:MDOC: pirms kodēšanas kvadrātkodā.

```
{
 //JSON stilā, tikai cilvēklasāms EPC loģiskā pārskata attēlojums.
 //Faktiskais kvadrātkoda vērtums ir determinēts CBOR, nevis JSON.
 "docType": "eu.epc"//EPC apliecinājuma dokuments. Ir iekļauta docType vērtība kopā ar
  //issuerSigned, izmantojot COSE_Sign1 ārējo vērtumu.

 "issuerSigned": {
  // issuerAuth aizsargāti dati; izmanto kā atdalītu vērtumu.
//Paraksta ģenerēšanai un verifikācijai atdalītais ārējais vērtums aptver gan
```

```
//docType un issuerSigned.
“nameSpaces”: {
  “eu.epc”: {
    “ver”: “1.0”,//kvadrātkoda profils/shēmas versija

    // Kartes sērijas numurs; kartes izdevēja definēts, ne vairāk kā 24 rakstzīmes.
    “sub”: "EF12345678901234567890GH",

    // Atcelšanas identifikators: faktiskais CBOR bstr, 16 baiti/128 biti.
    //Šeit attālotas kā 32 heksadecimālās rakstzīmes salasāmības nolūkā.
    “rid”: "4a8d9c11223344556677889 9aabbccdd",

    //Faktiskajā CBOR kodēšanā izmanto birku 1004 RFC 3339 pilnam datumam.
    “exp”: "2030-12-31"
  }
 }
},

“issuerAuth”: {
 // Faktiskā veidlapa: nemarķēts COSE_Sign1, nav JSON objekts.
 “tips”: "COSE_Sign1",
 “marķēts”: nepareizi        // kodēti bez COSE_Sign1 CBOR birkas
 “vērtums”: “atdalīts”,//COSE vērtuma lauks ir “CBOR null”

 “aizsargāts galvene”: {
  //alg: ES256; ekvivalentais COSE galvenes parametrs 1 = -7.
  "alg": "ES256",
```

```
    // x5t: sertifikāta nospiedums; COSE galvenes parametrs 34.
    "x5t": {
      "hashAlg": “SHA-256”//ekvivalenta COSE jaucējkoda vērtība -16

      // DER kodētas gala viernības QSealC SHA-256 jaucējkods.
      //32 baiti, kas atveidoti kā 64 heksadecimālās rakstzīmes.
      “jaucējkoda vērtība”:
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  “neaizsargāta galvene”: {},//tukša šajā piemērā

  //ES256 COSE paraksts: 64 baiti = 128 heksadecimālās rakstzīmes.
  “paraksts”
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Kriptogrāfijas mehānismu izmantošana

Šā pielikuma kontekstā kriptogrāfijas mehānismus izmanto saskaņā ar saskaņotajiem kriptogrāfijas mehānismiem, ko apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*).

III PIELIKUMS

REGULAS 6. PANTA 2. PUNKTĀ MINĒTAIS INFORMĀCIJAS PAZIŅOJUMS

1. Dalībvalstis par katru kompetento iestādi vai struktūru, kas atbildīga par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu, sniedz Komisijai šādu informāciju:

   (a) par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu atbildīgās kompetentās iestādes vai struktūras nosaukumu;

   (b) par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu atbildīgās kompetentās iestādes vai struktūras reģistrācijas numuru;

   (c) par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu atbildīgās kompetentās iestādes vai struktūras e-pasta adresi un tālruņa numuru, ko izmanto saziņai;

   (d) vienu vai vairākus sertifikātus, kurus var izmantot, lai verificētu elektronisko zīmogu, ko izveidojusi par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu atbildīgā kompetentā iestāde vai struktūra, un kuriem sertificētie identitātes dati ietver izdevēja nosaukumu un reģistrācijas numuru, kā norādīts attiecīgi a) un b) apakšpunktā;

   (e) tās vietas URL, kurā izdevējs publicē Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju derīguma statusu.

2. Dalībvalstis par katru kompetento iestādi vai struktūru, kas atbildīga par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu, var sniegt Komisijai šādu informāciju:

   (a) tās tīmekļa vietnes URL, kurā norādīta par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu atbildīgās kompetentās iestādes vai struktūras politika, noteikumi un nosacījumi, kas attiecas uz Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju nodrošināšanu un izmantošanu;

   (b) attiecīgā gadījumā tās tīmekļa vietnes URL, kurā ir papildu informācija par kompetento iestādi vai struktūru, kas atbildīga par Eiropas invaliditātes kartes vai Eiropas stāvvietu kartes personām ar invaliditāti fizisko versiju izdošanu.

IV PIELIKUMS

TEHNISKĀS SPECIFIKĀCIJAS EIROPAS INVALIDITĀTES KARTES VAI EIROPAS STĀVVIETU KARTES PERSONĀM AR INVALIDITĀTI FIZISKO VERSIJU ATSAUKŠANAS SARAKSTAM

1. Šī pielikuma vajadzībām identifikators atbilst atsaukšanas identifikatoram (*RID*), kas noteikts I pielikuma 6. punktā un II pielikuma 6.punktā.

2. Atsaukšanas sarakstu ievieš kā identifikatora saraksta marķieri *CWT* (RFC 8392, 7. iedaļa) formātā, kas ir saskaņā ar marķieru statusu saraksta specifikācijas 5.2. punktu (draft-ietf-oauth-status-list-14), ņemot vērā šādus grozījumus:

   (a) tipa pieprasījuma vērtība ir “application/identifierlist+cwt”;

   (b) jābūt derīguma termiņa beigu pieprasījumam;

   (c) StatusList pieprasījums nav iekļauts *CWT* pieprasījumu kopā;

   (d) IdentifierList struktūru, kas noteikta 3. punktā, *CWT* pieprasījumu kopā uzrāda kā pieprasījumu, izmantojot atslēgu 65530;

   (e) *CWT* ir COSE_Sign1 objekts, kas paraksta izskaitļošanai izmanto paraksta algoritmu saskaņā ar saskaņotajiem kriptogrāfijas mehānismiem, kurus apstiprinājusi Eiropas Kiberdrošības sertifikācijas grupa un publicējusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*);

   (f) aizsargātajā galvenē, kurā ir sertifikāts vai sertifikātu ķēde atsaukšanas saraksta paraksta verificēšanai, *CWT* ietver x5chain parametru, kas noteikts RFC 9360 (2. iedaļa);

   (g) marķieru statusu saraksta specifikācijā (draft-ietf-oauth-status-list-14) norādīto paplašinātā atslēgas lietojuma *OID* var izmantot identifikatoru saraksta parakstīšanas sertifikātam, un ir ieteicams, lai verificētāji atbalstītu marķieru statusu saraksta specifikācijā norādīto paplašinātā atslēgas lietojuma *OID* un lai izdevējiestādes infrastruktūra nepadarītu paplašinātā atslēgas lietojuma lauku par kritisku, kad tiek izmantots marķieru statusu saraksta specifikācijā norādītais paplašinātā atslēgas lietojuma *OID*.

3. IdentifierList struktūra ir *CBOR* struktūra ar šādu īso datu definēšanas valodu (*CDDL*):

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

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

Identifier = bstr

Aggregation_uri = tstr