Europos Sąjungos Taryba

Briuselis, 2026 m. liepos 10 d.
(OR. en)

11772/26
ADD 1

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

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2026 m. liepos 1 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	C(2026) 4534 annex
Dalykas:	PRIEDAI prie KOMISIJOS DELEGUOTOJO REGLAMENTO (ES) .../... kuriuo Direktyva (ES) 2024/2841 papildoma nuostatomis dėl Europos asmens su negalia kortelės fizinės versijos QR kodo nustatymo, Europos asmens su negalia automobilio statymo kortelės fizinės versijos QR kodo ir jos saugumo užtikrinimo bendrųjų techninių specifikacijų nustatymo ir dėl sąveikumo dalykų

EUROPOS
KOMISIJA

Briuselis, 2026 07 01
C(2026) 4534 final

ANNEXES 1 to 4

PRIEDAI

prie

KOMISIJOS DELEGUOTOJO REGLAMENTO (ES) .../...

kuriuo Direktyva (ES) 2024/2841 papildoma nuostatomis dėl Europos asmens su negalia kortelės fizinės versijos QR kodo nustatymo, Europos asmens su negalia automobilio statymo kortelės fizinės versijos QR kodo ir jos saugumo užtikrinimo bendrųjų techninių specifikacijų nustatymo ir dėl sąveikumo dalykų

I PRIEDAS

EUROPOS ASMENS SU NEGALIA KORTELĖS FIZINEI VERSIJAI SKIRTO QR KODO SPECIFIKACIJOS

1. **Europos asmens su negalia kortelės fizinei versijai skirto QR kodo formatas**

(a) **QR kodo 2 modelio formatas** pagal tarptautines QR kodų specifikacijas ISO/IEC 18004:2024 arba lygiavertes specifikacijas.

(b) **Klaidų ištaisymo lygis M** (15 proc. perteklumas), užtikrinantis atspausdinto QR kodo atsparumą įbrėžimams ar daliniam sugadinimui.

(c) **Kodavimo režimas:** QR naudinguosius duomenis sudaro issuerSigned Concise Binary Object Representation (CBOR) struktūra ir atitinkamas issuerAuth COSE_Sign1 parašo objektas, kaip apibrėžta objekto pasirašymo ir šifravimo CBOR formatu protokole (COSE, standarto RFC 9052 3.1, 4.2 ir 4.4 skirsniuose), laikantis mDOC duomenų modelio issuerSigned objektams, bet pritaikant statiniam fiziniam kortelės naudojimui. issuerAuth yra COSE_Sign1 objektas, kurio alg yra ES256, o apsaugotoje antraštėje pateikiamas x5t (COSE X.509 sertifikato maišos antraštės parametras, apibrėžtas standarte RFC 9360 (2 skirsnis); sąveikai užtikrinti x5t naudojamas maišos algoritmas turi būti SHA-256).

(d) Prieš koduojant QR kodą, bendras CBOR/COSE objektas **glaudinamas naudojant zlib formatą** (standartas RFC 1950, 2.2 skirsnis) **ir „Deflate“** algoritmą (standartas RFC 1951, 3.2 ir 4 skirsniai). Gautas suglaudintas baitų masyvas užkoduojamas **QR kodu naudojant baitų režimą**, užtikrinant visišką dvinarių CBOR/COSE naudingųjų duomenų ir skenerių sąveikumo palaikymą.

Visuose į QR naudinguosius duomenis įtrauktuose teksto laukeliuose išdavėjai CBOR teksto eilutėse koduoja ženklus Unicode UTF-8 koduote. Transliteracija netaikoma pasirašytiems naudingiesiems duomenims. Sąveikumo tikslais išdavėjai visiems teksto laukams prieš pasirašydami taiko Unicode normalizavimo formą C (NFC).

(e) **Prefiksas:** Europos asmens su negalia kortelėje QR kodo eilutė prasideda kodu „ED1:MDOC:“. Jis nurodo kortelės rūšį ir kodavimo profilį. Prefikse skiriamos mažosios ir didžiosios raidės ir jis turi būti egzistuojantis. Jei prefiksas nežinomas arba nepalaikomas, prieiga prie informacijos negalima. Prefiksas ir suglaudinti naudingieji duomenys užkoduojami naudojant baitų režimą kaip vienas QR kodo duomenų segmentas.

(f) **Mažiausias modulio dydis yra ≥0,25 mm**, kad būtų užtikrintas kodo įskaitomumas ant spausdintų kortelių.

(g) **Didžiausia galima versija yra 20 versija;** iki 97 × 97 modulių kiekvienoje pusėje.

2. **Europos asmens su negalia kortelės parašo generavimo specifikacijos**

Kvalifikuotas elektroninis spaudas (QSeal), naudojamas Europos asmens su negalia kortelės QR kodams užantspauduoti, užtikrina, kad užkoduoti duomenys būtų gauti iš įgaliotos išduodančiosios institucijos ir nebūtų pakeisti.

(a) **Parašo algoritmas**. Parašo algoritmas turi būti ES256 (elipsinės kreivės skaitmeninio parašo algoritmas (ECDSA) kartu su algoritmu SHA-256, naudojant P-

256 kreivę), kaip apibrėžta standarte RFC 9053 (2.1 skirsnyje); COSE algoritmas identifikuojamas pagal antraštės parametrą alg standarte RFC 9052 (3.1 skirsnis).

(b) **Pasirašymo raktas**. QR naudingieji duomenys pasirašomi naudojant privatųjį raktą, atitinkantį kvalifikuotą elektroninio spaudo sertifikatą (QSealC).

(c) **COSE struktūra.** Parašo rinkmena turi būti COSE_Sign1 objektas. Apsaugotoje antraštėje yra alg (ES256) ir x5t (COSE X.509 sertifikato maišos antraštės parametras, apibrėžtas standarte RFC 9360 (2 skirsnis); sąveikai užtikrinti x5t naudojamas maišos algoritmas turi būti SHA-256). Atliekant patikrą remiamasi x5t verte, kad atitinkamas sertifikatas būtų rastas tikrintojo vietos lygmeniu podeliuojamoje patikimumo saugykloje, sukurtoje remiantis patikimo sąrašo informacija, o tada pagal eIDAS patikimumo sistemą patvirtinama sertifikato seka ir sertifikato statusas.

(d) **Parašo standartas**. QR kodo naudingieji duomenys pasirašomi kaip COSE_Sign1 objektas pagal standartą RFC 9052 (4 skirsnis), objekto pasirašymo ir šifravimo CBOR formatu protokolą. COSE_Sign1 objektas įtraukiamas į issuerAuth struktūrą ir užkoduojamas be CBOR žymens, skirto COSE_Sign1. Objekto COSE_Sign1 naudingosios apkrovos laukas atskiriamas ir užkoduojamas kaip negaliojantis CBOR. Parašo generavimo ir tikrinimo tikslais išoriniai naudingieji duomenys yra užkoduota deterministinė CBOR struktūra, kurioje yra vertės docType ir issuerSigned iš aukščiausio lygmens CBOR žemėlapio.

(e) **Maišos algoritmas**. Parašo generavimo ir vientisumo tikrinimo tikslais SHA-256 naudojamas kaip ES256 dalis.

(f) **Kodavimas**. Naudingieji duomenys koduojami naudojant CBOR (standartas RFC 8949, 4.2 skirsnis), kaip reikalaujama COSE ir mDOC specifikacijose, užtikrinant pasirašytų duomenų kodavimą ir atkuriamumą.

3. **Spausdinimo specifikacijos**

(a) **Tuščioji sritis**. Aplink QR kodą iš visų pusių turi būti aiški **4 modulių** dydžio sritis, be jokių atspaudų, raštų ar fono.

(b) **Kontrastas**. QR kodas spausdinamas baltame fone, o kontrasto santykis turi būti ne mažesnis kaip **4:1**, kad įvairiomis apšvietimo sąlygomis būtų užtikrintas geras įskaitomumas.

(c) QR kodas spausdinamas naudojant Direktyvos (ES) 2024/2841 I priede apibrėžtą spalvą, kuria užtikrinamas didžiausias kontrastas.

(d) **Išdėstymas ir dydis**. QR kodas, įskaitant tuščiąją sritį, turi būti 26,25 × 26,25 mm dydžio, patalpintas galinės kortelės pusės apatiniame dešiniajame kampe. QR kodas turi būti ne didesnis kaip 20 versija (97 × 97 moduliai), modulio dydis – 0,25 mm arba didesnis.

QR kodas, įskaitant jo tuščiąją sritį, turi būti ne mažiau kaip 5 mm nuo dešiniojo kortelės krašto ir ne mažiau kaip 5 mm nuo apatinio jos krašto.

4. **Europos asmens su negalia kortelės QR kodo duomenys**

QR kodas apima minimalų neinternetiniu būdu patikrinamą duomenų rinkinį, laikantis Reglamento (ES) 2016/679 5 straipsnio 1 dalies c punkte nustatyto duomenų kiekio mažinimo principo. Naudojama ši naudingųjų duomenų struktūra:

(a) kortelės savybės koduojamos CBOR formatu issuerSigned objekte;

(b) struktūra uždaroma ir pasirašoma išduodančiosios institucijos QSeal spaudu kaip issuerAuth (COSE_Sign1, ES256, kartu su x5t, COSE X.509 sertifikato maišos antraštės parametru);

(c) gautas CBOR/COSE objektas suglaudinamas pagal šio priedo 1 punkto d papunktį. QR kodo naudinguosius duomenis sudaro prefiksas „ED1:MDOC:“, po kurio pateikiamas suglaudintas baitų masyvas, o visi naudingieji duomenys užkoduojami naudojant baitų režimą kaip vienas QR kodo duomenų segmentas.

Duomenų turinį sudaro matomų duomenų poaibis iš priekinės kortelės pusės laukų, išvardytų Direktyvos (ES) 2024/2841 I priede (vardas, pavardė, kortelės serijos numeris, galiojimo pabaigos data), taip pat panaikinimo identifikatorius, elektroninis parašas ir schemos informacija.

Elektroninį parašą sudaro:

i) issuerAuth - A COSE_Sign1 objektas, pasirašytas išduodančiosios institucijos **QSealC privačiuoju raktu**;

ii) apsaugota antraštė, kurią sudaro alg = ES256 (parašo algoritmas) ir x5t (COSE X.509 sertifikato maišos antraštės parametras).

5. Neprivalomi duomenys

Į QR kodą neprivalomi duomenys neįtraukiami.

6. Panaikinimo identifikatorius

Be matomo kortelės serijos numerio, QR kode nurodomas kortelei skirtas panaikinimo identifikatorius.

Panaikinimo identifikatorius naudojamas panaikinimo statusui nustatyti ir panaikinimo sąrašui tvarkyti. Panaikinimo identifikatorius nespausdinamas ant kortelės ir nėra matomas kortelės tikrintojams.

6.1. *Panaikinimo identifikatoriui taikomi reikalavimai*

Panaikinimo identifikatorius:

(a) turi būti įtrauktas į pasirašytus QR naudinguosius duomenis;

(b) turi būti unikalus bent išduodančiosios institucijos išdavimo srityje;

(c) neturi būti atspausdintas ant kortelės ir negali būti žmogui suprantamas;

(d) neturi atskleisti asmens duomenų ir negali būti akivaizdžiai prasmingas;

(e) neturi būti tiesiogiai gaunamas iš matomo kortelės serijos numerio ir

(f) turi būti kvalifikuotu elektroniniu spaudu kriptografiškai susietas su QR naudingaisiais duomenimis.

6.2. *Panaikinimo identifikatoriaus formatas ir dydis*

Panaikinimo identifikatorius koduojamas kaip CBOR baitų eilutė (bstr). Panaikinimo identifikatorius turi būti 16 baitų (128 bitų) ilgio.

Išduodančioji institucija sugeneruoja panaikinimo identifikatorių taikydama metodą, kuris patenka į jos kontrolės sritį ir kuriuo užtikrinama pakankama entropija ir atsparumas spėliojimui ar išskaičiavimui.

6.3. *Panaikintų kortelių sąrašai*

Tikrinimo tikslais skelbiamuose panaikintų kortelių sąrašuose nurodomi tik panaikintų kortelių panaikinimo identifikatoriai. Kortelės serijos numeriai panaikintų kortelių sąrašuose neskelbiami.

7. Europos asmens su negalia kortelės CBOR naudingieji duomenys (QR kode)

Į QR naudinguosius duomenis įtraukiami tik toliau nurodomi duomenys, atitinkantys matomus Europos asmens su negalia kortelės duomenų laukus, nustatytus Direktyvos (ES) 2024/2841 I priede.

Svarbiausi duomenys:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces."eu.edc" su toliau pateiktoje lentelėje nurodytomis savybėmis

(c) issuerAuth = COSE_Sign1 (QSeal)

Laukas	**mDOC maršrutas**	**Tipas/formatas**
Duomenų schemos versija	issuerSigned.nameSpaces."eu.edc".ver	Eilutė (pvz., „1.0“)
Kortelės tipas: Europos asmens su negalia kortelė	docType	Enum ("eu.edc")
Kortelės serijos numeris	issuerSigned.nameSpaces."eu.edc".sub	Eilutė
Panaikinimo identifikatorius	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 baitų)
Kortelės turėtojo vardas	issuerSigned.nameSpaces."eu.edc".givenName	Unikodu koduoto teksto eilutė (UTF-8)
Kortelės turėtojo pavardė	issuerSigned.nameSpaces."eu.edc".familyName	Unikodu koduoto teksto eilutė (UTF-8)

Kortelės galiojimo pabaigos data	issuerSigned.nameSpaces."eu.edc".exp	CBOR žymuo 1004, kaip apibrėžta standarte RFC 8943 (2.1 skirsnis), su UTF-8 koduote teksto eilutėje, atitinkančioje tikslią datą pagal RFC 3339 naudojant formatą MMMM-MM-DD.

Elektroninis parašas įtraukiamas į issuerAuth struktūrą (COSE_Sign1 objektas). Sertifikato eilutė neturi būti įterpta į QR kodo naudinguosius duomenis; vietoj to apsaugotoje COSE antraštėje pateikiamas x5t – sertifikato nykščio atspaudas, kad atitinkamą QSealC būtų galima rasti tikrintojo podėliuojamoje patikimumo saugykloje.

8. **Europos asmens su negalia kortelės QR kodo naudingųjų duomenų pavyzdys aptartas JavaScript Object Notation-style loginis vaizdas**

Šis pavyzdys – žmonėms suprantamo JSON formato Europos asmens su negalia kortelės loginis vaizdas. Praktiškai ši struktūra neturi būti žmogui suprantama, nes ji turi būti:

(a) koduojama CBOR formatu (standartas RFC 8949, 3 skirsnis);

b) pasirašyta naudojant nežymėtą COSE_Sign1 struktūrą su atskirtais naudingaisiais duomenimis (RFC 9052, 4 skirsnis);

c) įtraukta galiojimo pabaigos data kaip CBOR žymens 1004 tikslios datos vertė pagal standartą RFC 8943 (2.1 skirsnis);

d) įtrauktas apsaugotos antraštės parametras x5t pagal standartą RFC 9360, taikant SHA-256 užuot naudojus DER užkoduoto galutinio subjekto QSealC; ir

e) suglaudintas, o prefiksas papildytas eilute ED1:MDOC: prieš koduojant QR kodu.

```
{
  // tik pateikiamas žmonėms suprantamas JSON formato Europos asmens su negalia kortelės loginis vaizdas.
  // Faktiniai QR naudingieji duomenys yra deterministinė CBOR struktūra, o ne JSON formatas.
  "docType": "eu.edc", // Europos asmens su negalia kortelės kredencialas. Vertė DocType įtraukiama kartu su
    //issuerSigned COSE_Sign1 išoriniuose naudinguosiuose duomenyse.

  "issuerSigned": {
    // issuerAuth apsaugoti duomenys; naudojama kaip atskirti naudingieji duomenys.
    // Parašo generavimo ir tikrinimo tikslais atskirti išoriniai naudingieji duomenys apima ir
    // docType, ir issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // QR profilio/schemos versija

        // Kortelės serijos numeris; išdavėjo nustatytas, ne daugiau kaip 24 ženklai.
        "sub": "AB123456789012345678 90CD",
```

```
      // Panaikinimo identifikatorius: faktinis CBOR bstr, 16 baitų/128 bitai.
      // Dėl aiškumo čia pateikiama kaip 32 bitai, užkoduoti šešioliktainiais ženklais.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ann",    // ant Europos asmens su negalia kortelės atspausdintas vardas
      "familyName": "Other", // ant Europos asmens su negalia kortelės atspausdinta pavardė

      // Atliekant faktinę CBOR koduotę tiksliai datai pagal RFC 3339 naudojamas žymuo 1004.
      "exp": "2030-12-31"
    }
   }
 },

 "issuerAuth": {
  // Faktinė forma: nežymėta COSE_Sign1, ne JSON objektas.
  "type": "COSE_Sign1",
  "tagged": klaidinga,       // koduojama be COSE_Sign1 CBOR žymens
  "payload": "detached", // COSE naudingųjų duomenų laukas yra negaliojantis CBOR

  "protectedHeader": {
   // alg: ES256; lygiavertis COSE antraštės parametras 1 = −7.
   "alg": "ES256",

   // x5t: sertifikato nykščio atspaudas; lygiavertis COSE antraštės parametras 34.
   "x5t": {
    "hashAlg": "SHA-256", // lygiavertė COSE maišos vertė −16
```

```
        // DER užkoduoto galutinio subjekto QSealC maiša SHA-256.
        // 32 baitai išreikšti kaip 64 bitai, užkoduoti šešioliktainiais ženklais.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // šiame pavyzdyje yra tuščia

    // ES256 COSE parašas: 64 baitai = 128 bitai, užkoduoti šešioliktainiais ženklais.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. Kriptografinių mechanizmų naudojimas

Įgyvendinant šį priedą naudojami kriptografiniai mechanizmai turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) paskelbtus suderintuosius kriptografinius mechanizmus.

II PRIEDAS

EUROPOS ASMENS SU NEGALIA AUTOMOBILIO STATYMO KORTELĖS FIZINEI VERSIJAI SKIRTO QR KODO SPECIFIKACIJOS

1. **Europos asmens su negalia automobilio statymo kortelės fizinei versijai skirto QR kodo formatas**

(a) **QR kodo 2 modelio formatas** pagal tarptautines QR kodų specifikacijas ISO/IEC 18004:2024 arba lygiavertes specifikacijas.

(b) **Klaidų ištaisymo lygis M** (15 proc. perteklumas), užtikrinantis atspausdinto QR kodo atsparumą įbrėžimams ar daliniam sugadinimui.

(c) **Kodavimo režimas:** QR naudinguosius duomenis sudaro issuerSigned Concise Binary Object Representation (CBOR) struktūra ir atitinkamas issuerAuth COSE_Sign1 parašo objektas, kaip apibrėžta objekto pasirašymo ir šifravimo CBOR formatu protokole (COSE, standarto RFC 9052 3.1, 4.2 ir 4.4 skirsniuose), laikantis mDOC duomenų modelio issuerSigned objektams, bet pritaikant statiniam fiziniam kortelės naudojimui. issuerAuth yra COSE_Sign1 objektas, kurio alg yra ES256, o apsaugotoje antraštėje pateikiamas x5t (COSE X.509 sertifikato maišos antraštės parametras, apibrėžtas standarte RFC 9360 (2 skirsnis); sąveikai užtikrinti x5t naudojamas maišos algoritmas turi būti SHA-256).

(d) Prieš koduojant QR kodą, bendras CBOR/COSE objektas **glaudinamas naudojant zlib formatą (standartas RFC 1950, 2.2 skirsnis) ir „Deflate“ algoritmą** (standartas RFC 1951, 3.2 ir 4 skirsniai). Gautas suglaudintas baitų masyvas užkoduojamas **QR kodu naudojant baitų režimą**, užtikrinant visišką dvinarių CBOR/COSE naudingųjų duomenų ir skenerių sąveikumo palaikymą.

Visuose į QR naudinguosius duomenis įtrauktuose teksto laukeliuose išdavėjai CBOR teksto eilutėse koduoja ženklus Unicode UTF-8 koduote. Transliteracija netaikoma pasirašytiems naudingiesiems duomenims. Sąveikumo tikslais išdavėjai prieš pasirašydami visiems teksto laukams taiko Unicode normalizavimo formą C (NFC).

(e) **Prefiksas**: Europos asmens su negalia automobilio statymo kortelėje QR kodo eilutė prasideda kodu „EP1:MDOC:“. Jie nurodo kortelės rūšį ir kodavimo profilį. Prefikse skiriamos mažosios ir didžiosios raidės ir jis turi būti egzistuojantis. Jei prefiksas nežinomas arba nepalaikomas, prieiga prie informacijos negalima. Prefiksas ir suglaudinti naudingieji duomenys užkoduojami naudojant baitų režimą kaip vienas QR kodo duomenų segmentas.

(f) **Mažiausias modulio dydis yra ≥0,35 mm**, kad būtų užtikrintas kodo įskaitomumas ant spausdintų kortelių.

(g) **Didžiausia galima versija yra 20 versija;** iki 97 × 97 modulių kiekvienoje pusėje.

2. **Europos asmens su negalia automobilio statymo kortelės parašo generavimo specifikacijos**

Kvalifikuotas elektroninis spaudas (QSeal), naudojamas Europos asmens su negalia automobilio statymo kortelės QR kodams užantspauduoti, užtikrina, kad užkoduoti duomenys būtų gauti iš įgaliotos išduodančiosios institucijos ir nebūtų pakeisti.

(a) **Parašo algoritmas**. Parašo algoritmas turi būti ES256 (ECDSA kartu su algoritmu SHA-256, naudojant P-256 kreivę), kaip apibrėžta standarte RFC 9053 (2.1 skirsnyje); COSE algoritmas identifikuojamas pagal antraštės parametrą alg standarte RFC 9052 (3.1 skirsnis).

(b) **Pasirašymo raktas**. QR naudingieji duomenys pasirašomi naudojant privatųjį raktą, atitinkantį kvalifikuotą elektroninio spaudo sertifikatą (QSealC).

(c) **COSE struktūra**. Parašo rinkmena turi būti COSE_Sign1 objektas. Apsaugotoje antraštėje pateikiamas alg (ES256) ir x5t (COSE X.509 sertifikato maišos antraštės parametras, apibrėžtas standarte RFC 9360 (2 skirsnis); sąveikai užtikrinti x5t naudojamas maišos algoritmas turi būti SHA-256). Atliekant patikrą remiamasi x5t verte, kad atitinkamas sertifikatas būtų rastas tikrintojo vietos lygmeniu podeliuojamoje patikimumo saugykloje, sukurtoje remiantis patikimo sąrašo informacija, o tada pagal eIDAS patikimumo sistemą patvirtinama sertifikato seka ir sertifikato statusas.

(d) **Parašo standartas**. QR kodo naudingieji duomenys pasirašomi kaip COSE_Sign1 objektas pagal standartą RFC 9052 (4 skirsnis), objekto pasirašymo ir šifravimo CBOR formatu protokolą. COSE_Sign1 objektas įtraukiamas į issuerAuth struktūrą ir užkoduojamas be CBOR žymens, skirto COSE_Sign1. Objekto COSE_Sign1 naudingosios apkrovos laukas atskiriamas ir užkoduojamas kaip negaliojantis CBOR. Parašo generavimo ir tikrinimo tikslais išoriniai naudingieji duomenys turi būti deterministinė CBOR koduota CBOR struktūra, kurioje yra docType vertė ir issuerSigned vertė iš aukščiausio lygio CBOR žemėlapio.

(e) **Maišos algoritmas**. Parašo generavimo ir vientisumo tikrinimo tikslais SHA-256 naudojamas kaip ES256 dalis.

(f) **Kodavimas**. Naudingieji duomenys koduojami naudojant CBOR (standartas RFC 8949, 4.2 skirsnis), kaip reikalaujama COSE ir mDOC specifikacijose, užtikrinant pasirašytų duomenų kodavimą ir atkuriamumą.

3. **Spausdinimo specifikacijos**

(a) **Tuščioji sritis**. Aplink QR kodą iš visų pusių turi būti aiški **4 modulių** dydžio sritis, be jokių atspaudų, raštų ar fono.

(b) **Kontrastas**. QR kodas spausdinamas baltame fone, o kontrasto santykis turi būti ne mažesnis kaip **4:1**, kad įvairiomis apšvietimo sąlygomis būtų užtikrintas geras įskaitomumas.

(c) QR kodas spausdinamas naudojant Direktyvos (ES) 2024/2841 II priede apibrėžtą spalvą, kuria užtikrinamas didžiausias kontrastas.

(d) **Išdėstymas ir dydis.** QR kodas, įskaitant tuščiąją sritį, turi būti **37 × 37 mm** dydžio, patalpintas priekinėje kortelės pusėje, šiek tiek į dešinę ir į apačią nuo kortelės vidurio. QR kodas turi būti ne didesnis kaip 20 versija (97 × 97 moduliai), modulio dydis – 0,35 mm arba didesnis.

QR kodas, įskaitant jo tyliąją zoną, turi būti bent 5 mm atstumu nuo kortelės apatinio krašto.

4. **Europos asmens su negalia automobilio statymo kortelės QR kodo duomenys**

QR kodas apima minimalų neinternetiniu būdu patikrinamą duomenų rinkinį, laikantis Reglamento (ES) 2016/679 5 straipsnio 1 dalies c punkte nustatyto duomenų kiekio mažinimo principo. Naudojama ši naudingųjų duomenų struktūra:

(a) kortelės savybės koduojamos CBOR formatu issuerSigned objekte;

(b) struktūra uždaroma ir pasirašoma išduodančiosios institucijos QSeal spaudu kaip issuerAuth (COSE_Sign1, ES256, kartu su x5t, COSE X.509 sertifikato maišos antraštės parametru);

(c) gautas CBOR/COSE objektas suglaudinamas pagal šio priedo 1 punkto d papunktį. QR kodo naudinguosius duomenis sudaro prefiksas „EP1:MDOC:“, po kurio pateikiamas suglaudintas baitų masyvas, o visi naudingieji duomenys užkoduojami naudojant baitų režimą kaip vienas QR kodo duomenų segmentas.

Duomenų turinį sudaro matomų duomenų poaibis iš priekinės kortelės pusės laukų, išvardytų Direktyvos (ES) 2024/2841 II priede (galiojimo pabaigos data, kortelės serijos numeris), taip pat panaikinimo identifikatorius, elektroninis parašas ir schemos informacija.

Elektroninį parašą sudaro:

i) issuerAuth - A COSE_Sign1 objektas, pasirašytas išduodančiosios institucijos **QSealC privačiuoju raktu**;

ii) apsaugota antraštė, kurią sudaro alg = ES256 (parašo algoritmas) ir x5t (COSE X.509 sertifikato maišos antraštės parametras).

5. Neprivalomi duomenys

Į QR kodą neprivalomi duomenys neįtraukiami.

6. Panaikinimo identifikatorius

Europos asmens su negalia automobilio statymo kortelės panaikinimo identifikatorius turi atitikti I priedo 6 punktą.

Panaikintų Europos asmens su negalia automobilio statymo kortelių sąrašuose nurodomi tik panaikinimo identifikatoriai. Kortelės serijos numeriai panaikintų kortelių sąrašuose neskelbiami.

7. Europos asmens su negalia automobilio statymo kortelės CBOR naudingieji duomenys (QR kode)

Į QR naudinguosius duomenis įtraukiami tik toliau nurodomi duomenys, atitinkantys matomus Europos asmens su negalia automobilio statymo kortelės duomenų laukus, nustatytus Direktyvos (ES) 2024/2841 II priede.

Laukas	**mDOC maršrutas**	**Tipas/formatas**
Duomenų schemos versija	issuerSigned.nameSpaces."eu.epc".ver	Eilutė (pvz., „1.0“)
Kortelės tipas: Europos asmens	docType	Enum ("eu.epc")

su negalia automobilio statymo kortelė		
Kortelės serijos numeris	issuerSigned.nameSpaces."eu.epc".sub	Eilutė
Panaikinimo identifikatorius	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 baitų)
Kortelės galiojimo pabaigos data	issuerSigned.nameSpaces."eu.epc".exp	CBOR žymuo 1004, kaip apibrėžta standarte RFC 8943 (2.1 skirsnis), su UTF-8 koduote teksto eilutėje, atitinkančioje tikslią datą pagal RFC 3339 naudojant formatą MMMM-MM-DD.

Elektroninis parašas įtraukiamas į issuerAuth struktūrą (COSE_Sign1 objektas). Sertifikato eilutė neturi būti įterpta į QR kodo naudinguosius duomenis; vietoj to apsaugotoje COSE antraštėje pateikiamas x5t – sertifikato nykščio atspaudas, kad atitinkamą QSealC būtų galima rasti tikrintojo podėliuojamoje patikimumo saugykloje.

8. Europos asmens su negalia automobilio statymo kortelės QR kodo naudingųjų duomenų pavyzdys aptartas JavaScript Object Notation-style loginis vaizdas

Šis pavyzdys – žmonėms suprantamo JSON formato Europos asmens su negalia automobilio statymo kortelės loginis vaizdas. Praktiškai ši struktūra neturi būti žmogui suprantama, nes ji turi būti:

(a) koduojama CBOR formatu (standartas RFC 8949, 3 skirsnis),

(b) pasirašyta naudojant nežymėtą COSE_Sign1 struktūrą su atskirtais naudingaisiais duomenimis (RFC 9052, 4 skirsnis);

(c) įtraukta galiojimo pabaigos data kaip CBOR žymens 1004 tikslios datos vertė pagal standartą RFC 8943 (2.1 skirsnis);

(d) įtrauktas apsaugotos antraštės parametras x5t pagal standartą RFC 9360, taikant SHA-256 užuot naudojus DER užkoduoto galutinio subjekto QSealC; ir

(e) suglaudintas, o prefiksas papildytas eilute EP1:MDOC: prieš koduojant QR kodu.

{

// tik pateikiamas žmonėms suprantamas JSON formato Europos asmens su negalia automobilio statymo kortelės loginis vaizdas.

// Faktiniai QR naudingieji duomenys yra deterministinė CBOR struktūra, o ne JSON formatas.

"docType": "eu.epc", // Europos asmens su negalia automobilio statymo kortelės kredencialas. Vertė DocType įtraukiama kartu su

//issuerSigned COSE_Sign1 išoriniuose naudinguosiuose duomenyse.

"issuerSigned": {

// issuerAuth apsaugoti duomenys; naudojama kaip atskirti naudingieji duomenys.

// Parašo generavimo ir tikrinimo tikslais atskirti išoriniai naudingieji duomenys apima ir

// docType, ir issuerSigned.

"nameSpaces": {

"eu.epc": {

"ver": "1.0", // QR profilio/schemos versija

// Kortelės serijos numeris; išdavėjo nustatytas, ne daugiau kaip 24 ženklai.

"sub": "EF123456789012345678 90GH",

// Panaikinimo identifikatorius: faktinis CBOR bstr, 16 baitų/128 bitai.

// Dėl aiškumo čia pateikiama kaip 32 bitai, užkoduoti šešioliktainiais ženklais.

"rid": "4a8d9c112233445566778899aabbccdd",

// Atliekant faktinę CBOR koduotę tiksliai datai pagal RFC 3339 naudojamas žymuo 1004.

"exp": "2030-12-31"

}

```
    }
  },

  "issuerAuth": {
    // Faktinė forma: nežymėta COSE_Sign1, ne JSON objektas.
    "type": "COSE_Sign1",
    "tagged": klaidinga,       // koduojama be COSE_Sign1 CBOR žymens
    "payload": "detached", // COSE naudingųjų duomenų laukas yra negaliojantis CBOR

    "protectedHeader": {
      // alg: ES256; lygiavertis COSE antraštės parametras 1 = −7.
      "alg": "ES256",

      // x5t: sertifikato nykščio atspaudas; lygiavertis COSE antraštės parametras 34.
      "x5t": {
        "hashAlg": "SHA-256", // lygiavertė COSE maišos vertė −16

        // DER užkoduoto galutinio subjekto QSealC maiša SHA-256.
        // 32 baitai išreikšti kaip 64 bitai, užkoduoti šešioliktainiais ženklais.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // šiame pavyzdyje yra tuščia

    // ES256 COSE parašas: 64 baitai = 128 bitai, užkoduoti šešioliktainiais ženklais.
```

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Kriptografinių mechanizmų naudojimas

Taikant šį priedą naudojami kriptografiniai mechanizmai turi atitikti Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) paskelbtus suderintuosius kriptografinius mechanizmus.

III PRIEDAS

6 STRAIPSNIO 2 DALYJE NURODYTOS INFORMACIJOS PATEIKIMAS

1. Valstybės narės apie kiekvieną kompetentingą instituciją ar įstaigą, atsakingą už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, Komisijai pateikia šią informaciją:

   (a) kompetentingos institucijos ar įstaigos, atsakingos už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, pavadinimą;

   (b) kompetentingos institucijos ar įstaigos, atsakingos už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, registracijos kodą;

   (c) kompetentingos institucijos ar įstaigos, atsakingos už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, kontaktinio el. pašto adresą ir telefono numerį;

   (d) vieną ar daugiau sertifikatų, kurie gali būti naudojami siekiant patikrinti kompetentingos institucijos ar įstaigos, atsakingos už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, sukurtą elektroninį spaudą ir į kurių patvirtintus tapatybės duomenis įtrauktas išdavėjo pavadinimas ir registracijos kodas, kaip nurodyta atitinkamai a ir b punktuose;

   (e) vietos, kurioje išdavėjas skelbia Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų galiojimo statusą, URL.

2. Valstybės narės apie kiekvieną kompetentingą instituciją ar įstaigą, atsakingą už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, Komisijai gali pateikti šią informaciją:

   (a) tinklalapio, kuriame pateikiama kompetentingos institucijos arba įstaigos, atsakingos už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, politika ir sąlygos, taikomos išduodant ir naudojant jos išduodamos Europos asmens su negalia kortelės ir Europos asmens su negalia automobilio statymo kortelės fizines versijas, URL;

   (b) kai taikytina, tinklalapio, kuriame pateikiama papildoma informacija apie kompetentingą instituciją ar įstaigą, atsakingą už Europos asmens su negalia kortelės arba Europos asmens su negalia automobilio statymo kortelės fizinių versijų išdavimą, URL.

IV PRIEDAS

PANAIKINTŲ EUROPOS ASMENS SU NEGALIA KORTELĖS ARBA EUROPOS ASMENS SU NEGALIA AUTOMOBILIO STATYMO KORTELĖS FIZINIŲ VERSIJŲ SĄRAŠO TECHNINĖS SPECIFIKACIJOS

1. Šiame priede identifikatorius reiškia panaikinimo identifikatorių, apibrėžtą I priedo 6 punkte ir II priedo 6 punkte.

2. Panaikintų kortelių sąrašas įgyvendinamas kaip CWT formato identifikatorių sąrašo raktas (standartas RFC 8392, 7 skirsnis), laikantis rakto statuso sąrašo specifikacijos 5.2 straipsnio (draft-ietf-oauth-status-list-14) su šiais pakeitimais:

   (a) tipo prašymo vertė yra „application/identifierlist+cwt“;

   (b) turi būti pateiktas galiojimo pabaigos termino prašymas;

   (c) StatusList prašymas neturi būti įtrauktas į CWT prašymų rinkinį;

   (d) 3 punkte apibrėžta IdentifierList struktūra CWT prašymų rinkinyje pateikiama kaip prašymas naudojant raktą 65530;

   (e) CWT yra COSE_Sign1 objektas, kuris apskaičiuoti parašui naudoja parašo algoritmą, atitinkantį Europos kibernetinio saugumo sertifikavimo grupės patvirtintus ir Europos Sąjungos kibernetinio saugumo agentūros (ENISA) paskelbtus suderintuosius kriptografinius mechanizmus;

   (f) CWT apsaugotoje antraštėje, kurioje yra sertifikatas arba sertifikatų grandinė, skirti panaikintų kortelių sąrašo parašui patikrinti, turi būti standarte RFC 9360 (2 skirsnis) apibrėžtas x5chain parametras;

   (g) identifikatorių sąrašo pasirašymo sertifikatui gali būti naudojamas išplėstinio rakto naudojimo OID, nurodytas rakto statuso sąrašo specifikacijoje (draft-ietf-oauth-status-list-14), ir rekomenduojama, kad tikrintojai galėtų naudoti išplėstinio rakto naudojimo OID, nurodytą rakto statuso sąrašo specifikacijoje, ir kad išdavėjo institucijos infrastruktūroje išplėstinio rakto naudojimo laukas netaptų itin svarbus naudojant išplėstinio rakto naudojimo OID, nurodytą rakto statuso sąrašo specifikacijoje.

3. IdentifierList struktūra yra CBOR struktūra, naudojant šią glaustą duomenų apibrėžimo kalbą (CDDL):

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

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

Identifier = bstr

Aggregation_uri = tstr