Kunsill
tal-Unjoni Ewropea

Brussell, 10 ta' Lulju 2026
(OR. en)

11772/26
ADD 1

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

NOTA TA' TRAŻMISSJONI

minn:	Is-Segretarju Ġenerali tal-Kummissjoni Ewropea, iffirmata mis-Sa Martine DEPREZ, Direttur
data meta waslet:	1 ta' Lulju 2026
lil:	Is-Sa Thérèse BLANCHET, Segretarju Ġenerali tal-Kunsill tal-Unjoni Ewropea
Nru dok. Cion:	C(2026) 4534 annex
Suġġett:	ANNESSI tar- REGOLAMENT DELEGAT TAL-KUMMISSJONI (UE) .../... li jissupplimenta d-Direttiva (UE) 2024/2841 fir-rigward tal-istabbiliment tal-kodiċi QR dwar il-verżjoni fiżika tal-Kard Ewropea tad-Diżabilità u l-istabbiliment tal-kodiċi QR u l-istabbiliment ta' speċifikazzjonijiet tekniċi komuni li jiżguraw is-sigurtà tal-verżjoni fiżika tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità, kif ukoll kwistjonijiet ta' interoperabbiltà

IL-KUMMISSJONI
EWROPEA

Brussell, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ANNESSI

tar-

REGOLAMENT DELEGAT TAL-KUMMISSJONI (UE) .../...

li jissupplimenta d-Direttiva (UE) 2024/2841 fir-rigward tal-istabbiliment tal-kodiċi QR dwar il-verżjoni fiżika tal-Kard Ewropea tad-Diżabilità u l-istabbiliment tal-kodiċi QR u l-istabbiliment ta' speċifikazzjonijiet tekniċi komuni li jiżguraw is-sigurtà tal-verżjoni fiżika tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità, kif ukoll kwistjonijiet ta' interoperabbiltà

ANNESS I

SPEĊIFIKAZZJONIJIET TAL-KODIĊI QR GĦALL-VERŻJONI FIŻIKA TAL-KARD EWROPEA TAD-DIŻABILITÀ

1. **Format tal-Kodiċi QR għall-verżjoni fiżika tal-Kard Ewropea tad-Diżabilità (EDC)**

(a) **Format 2 tal-Mudell tal-kodiċi QR**, f'konformità mal-ispeċifikazzjonijiet internazzjonali tal-kodiċi QR ISO/IEC 18004: 2024 jew ekwivalenti.

(b) **Żball fil-Livell ta' Korrezzjoni M** (ridondanza ta' 15 %) li jiżgura reżiljenza għall-grif jew ħsara parzjali ta' kodiċi QR stampat.

(c) **Modalità ta' Kodifikazzjoni:** Il-payload (tagħbija utli) tal-QR għandha tikkonsisti mill-istruttura kkombinata tar-Rappreżentazzjoni tal-Oġġetti Binarji Konċiżi (CBOR, issuerSigned Concise Binary Object Representation) u mill-issuerAuth COSE_Sign1 korrispondenti kif definit fl-Iffirmar u fil-Kriptaġġ tal-Oġġett CBOR (COSE, RFC 9052 Taqsimiet 3.1, 4.2 u 4.4), skont il-mudell tad-data tal-mDOC għall-oġġetti issuerSigned, iżda adattat għall-użu statiku tal-kard fiżika. IssuerAuth għandu jkun oġġett COSE_Sign1 b'alg = ES256 u intestatura protetta li jkun fiha X5T (il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509 definit fl-RFC 9360 (it-Taqsima 2); għall-interoperabbiltà, l-algoritmu hash użat f'x5t għandu jkun SHA-256).

(d) Qabel il-kodifikazzjoni tal-kodiċi QR, l-oġġett CBOR/COSE kkombinat għandu jiġi **kkompressat bl-użu tal-format zlib** (RFC 1950, taqsima 2.2) **bl-algoritmu deflatat** (RFC 1951 taqsimiet 3.2 u 4). L-arranġament tal-byte kkompressat li jirriżulta għandu jiġi kkodifikat fil-**Modalità Byte tal-kodiċi QR**, filwaqt li jiġi żgurat appoġġ sħiħ għat-tagħbijiet utli binarji tas-CBOR/COSE u l-interoperabbiltà tal-iskener.

Għall-oqsma tat-test kollha inklużi fit-tagħbija utli tal-QR, l-emittenti għandhom jikkodifikaw il-karattri bħala Unicode UTF-8 fi ħdan is-sekwenzi tat-test tas-CBOR. It-trażlitterazzjoni ma għandhiex tiġi applikata għad-data tat-tagħbija ffirmata. Għall-finijiet tal-interoperabbiltà, l-emittenti għandhom japplikaw il-Formola C ta' Normalizzazzjoni tal-Unicode (NFC) għall-oqsma testwali kollha qabel ma jiffirmaw.

(e) **Prefiss:** Is-sekwenza QR tal-EDC għandha tibda b'"ED1: MDOC:". Dan jidentifika t-tip ta' kard u l-profil tal-ikkowdjar. Il-prefissi huma sensittivi għall-każ u jridu jkunu preżenti. Prefissi mhux magħrufa jew mhux appoġġati għandhom jikkawżaw rifjut. Il-prefiss u t-tagħbija utli kkompressata għandhom jiġu kkodifikati bħala segment wieħed tad-data tal-Modalità tal-Byte fil-kodiċi QR.

(f) **Daqs Minimu tal-Modulu ≥ 0,25 mm** biex tiġi żgurata l-leġġibbiltà fuq il-kards stampati.

(g) **Il-verżjoni Massima 20;** b'sa 97 × 97 moduli fuq kull naħa.

2. **Speċifikazzjonijiet tal-Ġenerazzjoni tal-Firma tal-EDC**

Is-siġill elettroniku kwalifikat (QSeal) użat biex jiġu ssiġillati l-kodiċijiet QR tal-EDC jiżgura li d-data kodifikata toriġina mill-awtorità emittenti awtorizzata u ma tkunx inbidlet.

(a) **Algoritmu tal-Firma:** L-algoritmu tal-firma għandu jkun ES256 (Algoritmu tal-Firma Diġitali b'Kurva Elliptika (ECDSA) bl-SHA-256 bl-użu tal-kurva P-256), kif definit fl-RFC 9053 (it-Taqsima 2.1); fis-COSE, l-algoritmu jiġi identifikat mill-parametru tal-intestatura tal-alg fl-RFC 9052 (it-Taqsima 3.1).

(b) **Kodiċi tal-Iffirmar:** Il-payload tal-QR għandha tiġi ffirmata bl-użu tal-kjavi privata li tikkorrispondi għal Ċertifikat Kwalifikat għas-Siġill Elettroniku (QSealC).

(c) **Struttura COSE:** Il-kontenitur tal-firma għandu jkun oġġett COSE_Sign1. L-intestatura protetta għandha tinkludi l-alg (ES256) u l-X5T (il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509 definit fl-RFC 9360 (it-Taqsima 2); għall-interoperabbiltà, l-algoritmu hash użat f'X5T għandu jkun SHA-256). Il-verifika għandha tiddependi fuq l-użu tal-valur X5T biex jiġi lokalizzat iċ-ċertifikat korrispondenti fil-ħanut fiduċjarju tal-verifikatur ikkwotat lokalment mibni mill-informazzjoni tal-Lista ta' Fiduċja u mbagħad għandha tivvalida l-katina taċ-ċertifikat u l-istatus taċ-ċertifikat f'konformità mal-qafas ta' fiduċja tal-eIDAS.

(d) **Standard tal-Iffirmar:** Il-payload tal-kodiċi QR għandha tiġi ffirmata bħala oġġett COSE_Sign1 f'konformità mal-RFC 9052 (it-taqsima 4), l-Iffirmar tal-Oġġett CBOR u l-Kriptaġġ. L-oġġett COSE_Sign1 għandu jinġarr f'issuerAuth u jiġi kkodifikat mingħajr it-tikketta CBOR għal COSE_Sign1. Il-kaxxa tat-tagħbija tal-oġġett COSE_Sign1 għandha tinqala' u tiġi kkodifikata bħala CBOR nulla. Għall-ġenerazzjoni u l-verifika tal-firem, it-tagħbija utli esterna għandha tkun l-istruttura kodifikata deterministic-CBOR li jkun fiha l-valur DOCTYPE u l-valur issuerSigned mill-mappa tas-CBOR tal-ogħla livell.

(e) **L-algoritmu Hash:** SHA-256 għandu jintuża bħala parti minn ES256 għall-ġenerazzjoni tal-firem u għall-verifika tal-integrità.

(f) **Kodifikazzjoni:** It-tagħbija utli għandha tiġi kkodifikata bl-użu tas-CBOR (RFC 8949, it-taqsima 4.2), kif meħtieġ mill-ispeċifikazzjonijiet tal-COSE u tal-mDOC, filwaqt li jiġu żgurati l-kodifikazzjoni u r-riproduċibbiltà tad-data ffirmata.

3. **Speċifikazzjonijiet tal-Istampar**

(a) **Żona Silenzjuża:** Għandu jkun hemm marġni ċar ta' **4 moduli** madwar il-kodiċi QR fuq in-naħat kollha, mingħajr ebda stampa, disinn jew sfond.

(b) **Kuntrast:** Il-kodiċi QR għandu jiġi stampat bil-blu skur fuq sfond abjad, bi proporzjon minimu ta' kuntrast ta' **4:1**, biex tiġi żgurata leġġibbiltà għolja f'kundizzjonijiet tad-dawl li jvarjaw.

(c) Il-kodiċi QR għandu jiġi stampat bl-użu tal-kulur definit fl-Anness I tad-Direttiva (UE) 2024/2841 li jiżgura kuntrast massimu.

(d) **Tqegħid u Daqs**: Il-kodiċi QR, inkluża ż-żona kwieta, għandu jkun ta' 26,25 mm × 26,25 mm,u jinsab fuq in-naħa ta' wara tal-kard fir-rokna ta' isfel tal-lemin. Il-kodiċi QR għandu jkun massimu tal-Verżjoni 20 (moduli 97 × 97), b'daqs tal-modulu ta' 0.25 mm jew akbar.

Il-kodiċi QR, inkluża ż-żona kwieta tiegħu, għandu jitqiegħed mill-inqas 5 mm mit-tarf tan-naħa tal-lemin u mill-inqas 5 mm mit-tarf ta' taħt tal-kard.

4. **Data fil-kodiċi QR tal-EDC**

Il-kodiċi QR għandu jkun fih sett tad-data minimu u verifikabbli offline f'konformità mal-prinċipju tal-minimizzazzjoni tad-data stabbilit fl-Artikolu 5(1), il-punt (c), tar-Regolament (UE) 2016/679. L-istruttura komuni għandha tkun kif ġej:

(a) L-attributi tal-kard huma kkodifikati f'CBOR f'oġġett issuerSigned.

(b) L-istruttura hija mgeżwra u ffirmata mill-QSeal tal-awtorità emittenti bħala issuerAuth (COSE_Sign1, ES256, inkluż x5t, il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509).

(c) L-oġġett CBOR/COSE li jirriżulta għandu jiġi kkompressat f'konformità mal-punt 1 (d) ta' dan l-Anness. It-tagħbija utli tal-kodiċi QR għandha tikkonsisti fil-prefiss "ED1: MDOC:", segwit mill-arranġament ta' bytes ikkumpressati li jirriżulta, u t-tagħbija utli sħiħa għandha tiġi kkodifikata bl-użu tal-Modalità Byte bħala segment uniku tad-data tal-kodiċi QR.

Il-kontenut tad-data għandu jikkonsisti f'subsett ta' data viżibbli mill-oqsma tal-kard ta' quddiem elenkati fl-Anness I tad-Direttiva (UE) 2024/2841 (l-isem, il-kunjom, in-numru tas-serje tal-kard, id-data tal-iskadenza), flimkien mal-identifikatur tar-revoka, il-firma elettronika, u l-informazzjoni tal-iskema.

Il-firma elettronika għandu jkun fiha:

(i) IssuerAuth - Oġġett COSE_Sign1 iffirmat bil-**kjavi privata QSealC** tal-awtorità emittenti.

(ii) Intestatura protetta li tinkludi alg = ES256 (algoritmu tal-firma) u X5T (il-parametru tal-hash header taċ-ċertifikat COSE X.509).

5. Data fakultattiva

L-ebda data fakultattiva ma għandha tiġi inkluża fil-kodiċi QR.

6. Identifikatur ta' Revoka (RID)

Minbarra n-numru tas-serje tal-kard viżibbli, il-kodiċi QR għandu jinkludi identifikatur iddedikat tar-revoka (RID).

L-RID għandu jintuża għad-determinazzjoni tal-istatus ta' revoka u għall-ġestjoni tal-lista ta' revoka. L-RID ma għandux jiġi stampat fuq il-kard u ma għandux jintwera lill-verifikaturi tal-kard.

6.1. *Rekwiżiti għall-RID*

L-RID:

(a) għandu jiġi inkluż fit-tagħbija utli tal-QR iffirmata;

(b) għandu jkun uniku mill-inqas fid-dominju tal-ħruġ tal-awtorità emittenti;

(c) ma għandux ikun stampat fuq il-kard u ma jkunx maħsub biex jinqara mill-bniedem;

(d) ma għandux jiżvela data personali u ma jkunx direttament sinifikanti;

(e) ma jistax jiġi derivat direttament min-numru tas-serje viżibbli tal-kard; kif ukoll

(f) għandu jkun marbua kriptografikament mat-tagħbija QR mis-siġill elettroniku kwalifikat.

6.2. *Il-format u d-daqs tal-RID*

L-RID għandu jiġi kkodifikat bħala sekwenza tal-bytes tas-CBOR (bstr). L-RID għandu jkun twil 16 byte (128 bits).

L-RID għandu jiġi ġġenerat mill-awtorità emittenti bl-użu ta' metodu taħt il-kontroll tagħha li jiżgura entropija suffiċjenti u reżistenza għall-qtugħ jew għall-enumerazzjoni.

6.3. *Listi ta' Revoka*

Il-listi ta' revoka ppubblikati għall-finijiet ta' verifika għandhom jirreferu biss għall-RID tal-kards revokati. In-numri tas-serje tal-kard ma għandhomx jiġu ppubblikati fil-listi ta' revoka.

7. Tagħbija utli tas-CBOR (fil-kodiċi QR) tal-EDC

Id-data li ġejja biss għandha tiġi inkluża fit-tagħbija tal-QR, b'mod konsistenti mal-kampijiet tad-data viżibbli tal-EDC stabbiliti fl-Anness I tad-Direttiva (UE) 2024/2841.

Kontenut tal-ogħla livell:

(a) DOCTYPE = "eu.edc"

(b) issuerSigned.nameSpaces. "eu.edc" bl-attributi murija fit-tabella ta' hawn taħt

(c) issuerAuth = COSE_Sign1 (QSial)

Kamp	**Path tal-mDOC**	**Tip/Format**
Verżjoni tal-iskema tad-data	issuerSigned.nameSpaces."eu.edc".ver	String (eż., "1.0")
Tip ta' Kard: ĊED	docType	Enum ("eu.edc")
Numru tas-Serje tal-Kard	issuerSigned.nameSpaces."eu.edc".sub	String
Identifikatur tar-Revoka	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bytes)
Isem id-detentur tal-kard	issuerSigned.nameSpaces."eu.edc".givenName	Sekwenza ta' test unicode (UTF-8)
Kunjom id-detentur tal-kard	issuerSigned.nameSpaces."eu.edc".familyName	Sekwenza ta' test unicode (UTF-8)
Id-data ta' skadenza tal-kard	issuerSigned.nameSpaces."eu.edc".exp	Tikketta CBOR 1004, kif definita fl-RFC 8943 (it-Taqsima 2.1), li

		fiha sekwenza ta' testi UTF-8 li tirrappreżenta data sħiħa tal-RFC 3339 Format SSSS-XX-JJ

Il-firma elettronika tingħarr f'issuerAuth (oġġett COSE_Sign1). Il-katina taċ-ċertifikat ma għandhiex tkun inkorporata fil-payload tal-kodiċi QR; minflok, l-intestatura protetta COSE għandha tinkludi x5t, l-intestatura protetta taċ-ċertifikat użata biex jiġi lokalizzat il-QSealC korrispondenti fil-maħżen fiduċjarju cached tal-verifikatur.

8. **Eżempju tal-payload tal-kodiċi QR tal-EPC: rappreżentazzjoni loġika tat-tip JavaScript Object Notation-style**

Dan l-eżempju huwa rappreżentazzjoni ta' JavaScript Object Notation (JSON) li tista' tinqara mill-bniedem ta' dehra loġika tal-EDC. Fil-prattika, din l-istruttura ma għandhiex tkun tista' tinqara mill-bniedem peress li għandha tkun:

(a) Ikkodifikat fis-CBOR (RFC 8949, it-Taqsima 3);

(b) Iffirmat bl-użu ta' struttura COSE_Sign1 mhux ittikkettata b'tagħbija utli maqlugħa (RFC 9052, it-taqsima 4.),

(c) tinkludi d-data ta' skadenza bħala tikketta tas-CBOR 1004 valur tad-data sħiħa f'konformità mal-RFC 8943 (it-taqsima 2.1);

(d) jinkludi l-parametru tal-intestatura protetta X5T f'konformità mal-RFC 9360, bl-użu ta' SHA-256 fuq l-entità finali kodifikata b'DER QSealC; kif ukoll

(e) ikkompressat u mwaħħal minn qabel bl-ispag ED1: MDOC: qabel ma tiġi kkodifikata fil-kodiċi QR.

```
{
 Dehra loġika biss tal-EDC tat-tip JSON, li tista' tinqara mill-bniedem.
 // Il-payload QR attwali hija CBOR deterministiku, mhux JSON.
 "docType": “eu.edc”,//Kredenzjal tal-EDC. Il-valur DOCTYPE huwa inkluż, flimkien ma'
  //issuerSigned, fit-tagħbija esterna ta' COSE_Sign1.

 "issuerSigned": {
  // Data protetta minn issuerAuth; użata bħala payload utli maqlugħ.
  Għall-ġenerazzjoni u l-verifika tal-firem, it-tagħbija utli esterna maqlugħa tkopri kemm
  it-tip ta' dokument u l-firmatarju tal-ħruġ.
  "nameSpaces": {
   “eu.edc”: {
    "ver": “1.0”,//verżjoni tal-profil/tal-iskema QR

    // Numru tas-Serje tal-Kard; definit mill-emittent, massimu ta' 24 karattru.
    "sub": "AB12345678901234567890CD",
```

```
    // Identifikatur tar-Revoka: bstr CBOR attwali, 16 bytes/128 bit.
    //Agħżel hawn bħala 32 karattri hex biex ikunu jistgħu jinqraw.
    "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

    “givenName”: “Ann”, // isem stampat fuq l-EDC
    “familyName”: “Oħrajn”, // kunjom stampat fuq l-EDC

    // Kodifikazzjoni tas-CBOR attwali tuża t-tikketta 1004 għad-data sħiħa tal-RFC 3339.
    "exp": "2030-12-31"
   }
  }
},

"issuerAuth": {
 // Forma attwali: COSE_Sign1 mhux oġġett JSON.
 “tip”: "COSE_Sign1",
 “ittikkettat”: false, //   ikkodifikat mingħajr tikketta CBOR COSE_Sign1
 "payload": “maqlugħa”,//L-attribut tat-tagħbija utli tal-COSE huwa CBOR null

 “intestatura Protetta”: {
  // alg: ES256; parametru tal-intestatura tas-COSE ekwivalenti 1 = -7.
  "alg": "ES256",

  // x5t: marka ta’ identifikazzjoni taċ-ċertifikat; parametru tal-intestatura tas-COSE 34.
  "x5t", {
   “hashAlg”: “SHA-256”,//valur tal-hash ekwivalenti għas-COSE -16
```

// SHA-256 hash tal-entità aħħarija QSealC ikkodifikata b’DER.

// 32 bytes irrappreżentati bħala karattri 64 hex.

“hashValue”:
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

“intestatura Mhux Protetta”: {}, // vojt f’dan l-eżempju

// Firma ta’//ES256 cose: // 64 bytes irrappreżentati bħala karattri 128 hex.

"firma":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Użu ta’ mekkaniżmi kriptografiċi

L-użu ta’ mekkaniżmi kriptografiċi fil-kuntest ta’ dan l-Anness għandu jkun f’konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà (ENISA).

ANNESS II

SPEĊIFIKAZZJONIJIET TAL-KODIĊI QR GĦALL-VERŻJONI FIŻIKA TAL-KARD EWROPEA GĦALL-PARKEĠĠ GĦALL-PERSUNI B'DIŻABILITÀ

1. **Format tal-kodiċi QR dwar il-verżjoni fiżika tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità (EPC)**

(a) **Format 2 tal-Mudell tal-kodiċi QR**, f'konformità mal-ispeċifikazzjonijiet internazzjonali tal-kodiċi QR ISO/IEC 18004: 2024 jew ekwivalenti.

(b) **Żball fil-Livell ta' Korrezzjoni M** (ridondanza ta' 15 %) li jiżgura reżiljenza għall-grif jew ħsara parzjali tal-kodiċi QR stampat.

(c) **Modalità ta' Kodifikazzjoni:** Il-payload (tagħbija utli) tal-QR għandha tikkonsisti mill-istruttura kkombinata tar-Rappreżentazzjoni tal-Oġġetti Binarji Konċiżi (CBOR, issuerSigned Concise Binary Object Representation) u mill-issuerAuth COSE_Sign1 korrispondenti kif definit fl-Iffirmar u fil-Kriptaġġ tal-Oġġett CBOR (COSE, RFC 9052 Taqsimiet 3.1, 4.2 u 4.4), skont il-mudell tad-data tal-mDOC għall-oġġetti issuerSigned, iżda adattat għall-użu statiku tal-kard fiżika. IssuerAuth għandu jkun oġġett COSE_Sign1 b'alg = ES256 u intestatura protetta li jkun fiha X5T (il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509 definit fl-RFC 9360 (it-Taqsima 2); għall-interoperabbiltà, l-algoritmu hash użat f'x5t għandu jkun SHA-256).

(d) Qabel il-kodifikazzjoni tal-kodiċi QR, l-oġġett CBOR/COSE kkombinat għandu jiġi **kkompressat bl-użu tal-format ZLIB (RFC 1950, it-taqsima 2.2)** bl-algoritmu deflatat (RFC 1951, it-taqsimiet 3.2 u 4). L-arranġament tal-byte kkompressat li jirriżulta għandu jiġi kkodifikat fil-**Modalità Byte tal-kodiċi QR**, filwaqt li jiġi żgurat appoġġ sħiħ għat-tagħbijiet utli binarji tas-CBOR/COSE u l-interoperabbiltà tal-iskener.

Għall-oqsma tat-test kollha inklużi fit-tagħbija utli tal-QR, l-emittenti għandhom jikkodifikaw il-karattri bħala Unicode UTF-8 fi ħdan is-sekwenzi tat-test tas-CBOR. It-trażlitterazzjoni ma għandhiex tiġi applikata għad-data tat-tagħbija ffirmata. Għall-finijiet tal-interoperabbiltà, l-emittenti għandhom japplikaw il-Formola C ta' Normalizzazzjoni tal-Unicode (NFC) għall-oqsma testwali kollha qabel ma jiffirmaw.

(e) **Prefiss:** Is-sekwenza QR tal-EPC għandha tibda b'"EP1:MDOC:". Dan jidentifika t-tip ta' kard u l-profil tal-ikkowdjar. Il-prefissi huma sensittivi għall-każ u jridu jkunu preżenti. Prefissi mhux magħrufa jew mhux appoġġati għandhom jikkawżaw rifjut. Il-prefiss u t-tagħbija utli kkompressata għandhom jiġu kkodifikati bħala segment wieħed tad-data tal-Modalità tal-Byte fil-kodiċi QR.

(f) **Daqs Minimu tal-Modulu ≥ 0.35 mm** biex tiġi żgurata l-leġġibbiltà fuq il-kards stampati.

(g) **Il-verżjoni Massima 20;** b'massimu ta' 97 x 97 moduli fuq kull naħa.

2. **Speċifikazzjonijiet tal-Ġenerazzjoni tal-Firma tal-EPC**

Is-siġill elettroniku kwalifikat (QSeal) użat biex jiġu ssiġillati l-kodiċijiet QR tal-EPC jiżgura li d-data kodifikata toriġina mill-awtorità emittenti awtorizzata u ma tkunx inbidlet.

(a) **Algoritmu tal-Firma:** L-algoritmu tal-firma għandu jkun ES256 (ECDSA b'SHA-256 bl-użu tal-kurva P-256), kif definit fl-RFC 9053 (it-Taqsima 2.1); fis-COSE, l-algoritmu jiġi identifikat mill-parametru tal-intestatura tal-alg fl-RFC 9052 (it-Taqsima 3.1).

(b) **Kodiċi tal-Iffirmar:** It-tagħbija QR għandha tiġi ffirmata bl-użu tal-kjavi privata li tikkorrispondi għal Ċertifikat Kwalifikat għas-Siġill Elettroniku (QSealC).

(c) **Struttura ta' Kju:** Il-kontenitur tal-firma għandu jkun oġġett COSE_Sign1. L-intestatura protetta għandha tinkludi l-alg (ES256) u l-X5T (il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509 definit fl-RFC 9360 (it-Taqsima 2); għall-interoperabbiltà, l-algoritmu hash użat f'X5T għandu jkun SHA-256). Il-verifika għandha tiddependi fuq l-użu tal-valur X5T biex jiġi lokalizzat iċ-ċertifikat korrispondenti fil-ħanut fiduċjarju tal-verifikatur ikkwotat lokalment mibni mill-informazzjoni tal-Lista ta' Fiduċja u mbagħad għandha tivvalida l-katina taċ-ċertifikat u l-istatus taċ-ċertifikat f'konformità mal-qafas ta' fiduċja tal-eIDAS.

(d) **Standard tal-Iffirmar:** Il-payload tal-kodiċi QR għandha tiġi ffirmata bħala oġġett COSE_Sign1 f'konformità mal-RFC 9052 (it-taqsima 4), l-Iffirmar tal-Oġġett CBOR u l-Kriptaġġ. L-oġġett COSE_Sign1 għandu jinġarr f'issuerAuth u jiġi kkodifikat mingħajr it-tikketta CBOR għal COSE_Sign1. Il-kaxxa tat-tagħbija tal-oġġett COSE_Sign1 għandha tinqala' u tiġi kkodifikata bħala CBOR nulla. Għall-ġenerazzjoni u l-verifika tal-firem, it-tagħbija utli esterna għandha tkun l-istruttura kodifikata deterministic-CBOR li jkun fiha l-valur DOCTYPE u l-valur issuerSigned mill-mappa tas-CBOR tal-ogħla livell.

(e) **L-algoritmu "hash":** SHA-256 jintuża bħala parti minn ES256 għall-ġenerazzjoni tal-firem u għall-verifika tal-integrità.

(f) **Kodifikazzjoni:** It-tagħbija utli għandha tiġi kkodifikata bl-użu tas-CBOR (RFC 8949, it-taqsima 4.2), kif meħtieġ mill-ispeċifikazzjonijiet tal-COSE u tal-mDOC, filwaqt li jiġu żgurati l-kodifikazzjoni u r-riproduċibbiltà tad-data ffirmata.

3. **Speċifikazzjonijiet tal-Istampar**

(a) **Żona silenzjuża:** Għandu jkun hemm marġni ċar ta' **4 moduli** madwar il-kodiċi QR fuq in-naħat kollha, mingħajr ebda stampa, disinn jew sfond.

(b) **Kuntrast:** Il-kodiċi QR għandu jiġi stampat bil-blu skur fuq sfond abjad, bi proporzjon minimu ta' kuntrast ta' **4:1**, biex tiġi żgurata leġġibbiltà għolja f'kundizzjonijiet tad-dawl li jvarjaw.

(c) Il-kodiċi QR għandu jiġi stampat bl-użu tal-kulur definit fl-Anness I tad-Direttiva (UE) 2024/2841 li jiżgura kuntrast massimu.

(d) **Tqegħid u Daqs:** Il-kodiċi QR, inkluża ż-żona kwieta, għandu jkun ta' **37 mm × 37 mm**, li jinsab fuq quddiem tal-kard, kemxejn' il barra miċ-ċentru lejn il-lemin, lejn it-tarf ta' taħt. Il-kodiċi QR għandu jkun il-verżjoni massima 20 (moduli 97 × 97), b'daqs tal-modulu ta' 0,35 mm jew akbar.

Il-kodiċi QR, inkluża ż-żona kwieta tiegħu, għandu jitqiegħed mill-inqas 5 mm mit-tarf ta' taħt tal-kard.

4. **Data fil-kodiċi QR tal-EPC**

Il-kodiċi QR għandu jkun fih sett tad-data minimu u verifikabbli offline f'konformità mal-prinċipju tal-minimizzazzjoni tad-data li jinsab fl-Artikolu 5(1), il-punt (c), tar-Regolament (UE) 2016/679. L-istruttura tal-gwida hija kif ġej:

(a) L-attributi tal-kard huma kkodifikati f'CBOR f'oġġett issuerSigned.

(b) Din l-istruttura hija mgeżwra u ffirmata mill-QSeal tal-awtorità emittenti bħala issuerAuth (COSE_Sign1, ES256, inkluż X5T, il-parametru tal-intestatura tal-hash taċ-ċertifikat COSE X.509).

(c) L-oġġett CBOR/COSE li jirriżulta għandu jiġi kkompressat f'konformità mal-punt 1 (d) ta' dan l-Anness. It-tagħbija utli tal-kodiċi QR għandha tikkonsisti fil-prefiss "EP1: MDOC:", segwit mill-arranġament ta' bytes ikkumpressati li jirriżulta, u t-tagħbija utli sħiħa għandha tiġi kkodifikata bl-użu tal-Modalità Byte bħala segment uniku tad-data tal-kodiċi QR.

Il-kontenut tad-data għandu jikkonsisti f'subsett ta' data viżibbli mill-oqsma tal-kard ta' quddiem elenkati fl-Anness II tad-Direttiva (UE) 2024/2841 (id-data tal-iskadenza, in-numru tas-serje tal-kard), flimkien mal-identifikatur tar-revoka, il-firma elettronika, u l-informazzjoni tal-iskema.

Il-firma elettronika għandu jkun fiha:

(i) IssuerAuth — Oġġett COSE_Sign1 iffirmat bil-**kjavi privata QSealC** tal-awtorità emittenti.

(ii) Intestatura protetta li tinkludi alg = ES256 (algoritmu tal-firma) u X5T (il-parametru tal-hash header taċ-ċertifikat COSE X.509).

5. Data fakultattiva

L-ebda data fakultattiva ma għandha tiġi inkluża fil-kodiċi QR.

6. Identifikatur ta' Revoka (RID)

L-identifikatur tar-Revoka tal-EPC għandu jikkonforma mal-punt 6 tal-Anness I.

Il-listi ta' revoka għall-EPCs revokati għandhom jirreferu biss għall-RID. In-numri tas-serje tal-kard ma għandhomx jiġu ppubblikati fil-listi ta' revoka.

7. Tagħbija utli tas-CBOR (fil-QR) tal-EPC

Id-data li ġejja biss għandha tiġi inkluża fit-tagħbija utli tal-QR, li hija konsistenti mal-oqsma viżibbli tal-kard tal-EPC stabbiliti fl-Anness II tad-Direttiva (UE) 2024/2841:

Kamp	**Path tal-mDOC**	**Tip/Format**
Verżjoni tal-iskema tad-data	issuerSigned.nameSpaces. "eu.epc".ver	String (eż., "1.0")
Tip ta' Kard: EPC	docType	Enum ("eu.epc")
Numru tas-Serje	issuerSigned.nameSpaces. "eu.epc".sub	String

tal-Kard		
identifikatur tar-Revoka	issuerSigned.nameSpaces. “eu.epc”.rid	CBOR bstr (16 bytes)
Id-data ta’ skadenza tal-kard:	issuerSigned.nameSpaces."eu.epc".exp	Tikketta CBOR 1004, kif definita fl-RFC 8943 (it-Taqsima 2.1), li fiha sekwenza ta’ testi UTF-8 li tirrappreżenta data sħiħa tal-RFC 3339 Format SSSS-XX-JJ

Il-firma elettronika għandha tinġarr f’issuerAuth (oġġett COSE_Sign1). Il-katina taċ-ċertifikat ma għandhiex tkun inkorporata fil-payload tal-kodiċi QR; minflok, l-intestatura protetta COSE għandha tinkludi x5t, l-intestatura protetta taċ-ċertifikat użata biex jiġi lokalizzat il-QSealC korrispondenti fil-maħżen fiduċjarju cached tal-verifikatur.

8. Eżempju tal-payload tal-kodiċi QR tal-EPC: rappreżentazzjoni loġika tat-tip JavaScript Object Notation-style

Dan l-eżempju huwa rappreżentazzjoni ta’ JavaScript Object Notation (JSON) li tista’ tinqara mill-bniedem ta’ dehra loġika tal-EDC. Fil-prattika, din l-istruttura ma għandhiex tkun tista’ tinqara mill-bniedem peress li għandha tkun:

(a) Ikkodifikat fis-CBOR (RFC 8949, it-Taqsima 3),

(b) Iffirmat bl-użu ta’ struttura COSE_Sign1 mhux ittikkettata b’tagħbija utli maqlugħa (RFC 9052, it-taqsima 4.),

(c) tinkludi d-data ta’ skadenza bħala tikketta tas-CBOR 1004 valur tad-data sħiħa f’konformità mal-RFC 8943 (it-taqsima 2.1);

(d) jinkludi l-parametru tal-intestatura protetta X5T f’konformità mal-RFC 9360, bl-użu ta’ SHA-256 fuq l-entità finali kodifikata b’DER QSealC; kif ukoll

(e) ikkompressat u mwaħħal minn qabel bl-ispag EP1: MDOC: qabel ma tiġi kkodifikata fil-kodiċi QR.

{

Dehra loġika biss tal-EDC tat-tip JSON, li tista’ tinqara mill-bniedem.

```
// Il-payload QR attwali hija CBOR deterministiku, mhux JSON.
"docType": “eu.epc”,//Kredenzjali tal-EPC. Il-valur DOCTYPE huwa inkluż, flimkien ma’
  //issuerSigned, fit-tagħbija esterna ta’ COSE_Sign1.

"issuerSigned": {
  // Data protetta minn issuerAuth; użata bħala payload utli maqlugħ.
Għall-ġenerazzjoni u l-verifika tal-firem, it-tagħbija utli esterna maqlugħa tkopri kemm
  it-tip ta’ dokument u l-firmatarju tal-ħruġ.
  "nameSpaces": {
    “eu.epc”: {
      "ver": “1.0”,//verżjoni tal-profil/tal-iskema QR

      // Numru tas-Serje tal-Kard; definit mill-emittent, massimu ta’ 24 karattru.
      "sub": "EF123456789012345678 90GH",

      // Identifikatur tar-Revoka: bstr CBOR attwali, 16 bytes/128 bit.
      //Agħżel hawn bħala 32 karattri hex biex ikunu jistgħu jinqraw.
      "rid": "4a8d9c112233445566778899aabbccdd",

      // Kodifikazzjoni tas-CBOR attwali tuża t-tikketta 1004 għad-data sħiħa tal-RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Forma attwali: COSE_Sign1 mhux oġġett JSON.
```

```
  “tip”: "COSE_Sign1",
  “ittikkettat”: false, //   ikkodifikat mingħajr tikketta CBOR COSE_Sign1
  "payload": “maqlugħa”,//L-attribut tat-tagħbija utli tal-COSE huwa CBOR null

  “intestatura Protetta”: {
    // alg: ES256; parametru tal-intestatura tas-COSE ekwivalenti 1 = -7.
    "alg": "ES256",

    // x5t: marka ta’ identifikazzjoni taċ-ċertifikat; parametru tal-intestatura tas-COSE 34.
    "x5t", {
      “hashAlg”: “SHA-256”,//valur tal-hash ekwivalenti għas-COSE -16

      // SHA-256 hash tal-entità aħħarija QSealC ikkodifikata b’DER.
      // 32 bytes irrappreżentati bħala karattri 64 hex.
      “hashValue”:
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  “intestatura Mhux Protetta”: {}, // vojt f’dan l-eżempju

  // Firma ta’//ES256 cose: // 64 bytes irrappreżentati bħala karattri 128 hex.
  "firma":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```


9. **Użu ta’ mekkaniżmi kriptografiċi**

L-użu ta’ mekkaniżmi kriptografiċi fil-kuntest ta’ dan l-Anness għandu jkun f’konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà (ENISA).

ANNESS III

NOTIFIKA TA' INFORMAZZJONI MSEMMIJA FL-ARTIKOLU 6(2)

1. L-Istati Membri għandhom jipprovdu l-informazzjoni li jmiss lill-Kummissjoni dwar kull awtorità jew korp kompetenti responsabbli għall-ħruġ tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għal persuni b'diżabilità:

   (a) L-isem tal-awtorità jew korp kompetenti responsabbli għall-ħruġ, it-tiġdid u l-irtirar tal-Kard Ewropea tad-Diżabilità u l-Kard Ewropea għall-Parkeġġ għal persuni b'diżabilità;

   (b) numru ta' reġistrazzjoni tal-awtorità jew korp kompetenti responsabbli għall-ħruġ, it-tiġdid u l-irtirar tal-Kard Ewropea tad-Diżabilità u l-Kard Ewropea għall-Parkeġġ għal persuni b'diżabilità;

   (c) L-email ta' kuntatt u n-numru ta' kuntatt tal-awtorità jew korp kompetenti responsabbli għall-ħruġ, it-tiġdid u l-irtirar tal-Kard Ewropea tad-Diżabilità u l-Kard Ewropea għall-Parkeġġ għal persuni b'diżabilità;

   (d) ċertifikat wieħed jew aktar li jistgħu jintużaw biex jiġi vverifikat is-siġill elettroniku maħluq mill-awtorità jew mill-korp kompetenti responsabbli għall-ħruġ tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità li toħroġ, u li għalihom id-data tal-identità ċċertifikata tinkludi l-isem, u n-numru tar-reġistrazzjoni tal-emittent, kif speċifikat fil-punti (a) u (b), rispettivament;

   (e) l-URL tal-post fejn l-emittent jippubblika l-istatus ta' validità tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità.

2. L-Istati Membri jistgħu jipprovdu l-informazzjoni li ġejja lill-Kummissjoni dwar kull awtorità jew korp kompetenti responsabbli għall-ħruġ tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità:

   (a) l-URL tal-paġna web li fiha l-politiki, it-termini u l-kundizzjonijiet tal-awtorità jew tal-korp kompetenti responsabbli għall-ħruġ tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità li japplikaw għall-forniment u l-użu tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità u l-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità li tipprovdi;

   (b) fejn applikabbli, l-URL tal-paġna web li fiha informazzjoni addizzjonali dwar l-awtorità jew il-korp kompetenti responsabbli għall-ħruġ tal-verżjonijiet fiżiċi tal-Kard Ewropea tad-Diżabilità jew tal-Kard Ewropea għall-Parkeġġ għall-persuni b'diżabilità.

ANNESS IV

SPEĊIFIKAZZJONIJIET TEKNIĊI GĦAL LISTA TA' REVOKA GĦALL-VERŻJONIJIET FIŻIĊI TAL-KARD EWROPEA TAD-DIŻABILITÀ JEW TAL-KARD EWROPEA GĦALL-PARKEĠĠ GĦALL-PERSUNI B'DIŻABILITÀ

1. Għall-finijiet ta' dan l-Anness, l-identifikatur għandu jikkorrispondi mal-identifikatur tar-revoka (RID) definit fil-punt 6 tal-Anness I u fil-punt 6 tal-Anness II.

2. Lista ta' revoka għandha tiġi implimentata bħala token tal-lista ta' identifikaturi fil-format CWT (RFC 8392, taqsima 7) f'konformità mal-Klawżola 5.2 tal-ispeċifikazzjoni tal-lista tal-istatus tat-token (draft-ietf-oauth-status-list-14) bl-emendi li ġejjin:

   (a) il-valur tat-talba tat-tip għandu jkun "application/identifierlist + cwt";

   (b) it-talba għal żmien ta' skadenza għandha tkun preżenti;

   (c) Il-pretensjoni StatusList ma għandhiex tkun preżenti fis-sett ta' pretensjonijiet tas-CWT;

   (d) l-istruttura tal-Lista ta' Identifikazzjoni definita fil-punt 3 għandha tkun preżenti bħala pretensjoni fil-pretensjonijiet tas-CWT stabbiliti bl-użu tal-kjavi 65530;

   (e) is-CWT għandu jkun oġġett COSE_Sign1 li, għall-kalkolu tal-firma, juża algoritmu tal-firma f'konformità mal-Mekkaniżmi Kriptografiċi Miftiehma approvati mill-Grupp Ewropew taċ-Ċertifikazzjoni taċ-Ċibersigurtà u ppubblikati mill-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà (ENISA);

   (f) is-CWT għandu jkun fih il-parametru x5chain kif definit fl-RFC 9360 (it-taqsima 2) fl-intestatura protetta li jkun fiha ċ-ċertifikat jew il-katina ta' ċertifikati biex tiġi vverifikata l-firma tal-lista ta' revoka;

   (g) l-OID tal-użu taċ-ċavetta estiża speċifikata fl-ispeċifikazzjoni tal-lista tal-istatus tat-token (draft-ietf-oauth-status-list-14) tista' tintuża għaċ-ċertifikat tal-iffirmar tal-lista ta' identifikaturi u huwa rrakkomandat li l-verifikaturi jappoġġaw l-OID tal-użu taċ-ċavetta estiża speċifikata fl-ispeċifikazzjoni tal-lista tal-istatus tat-token u li l-infrastrutturi tal-awtorità tal-emittent ma jagħmlux il-kamp tal-użu taċ-ċavetta estiża kritiku meta jużaw l-OID tal-użu taċ-ċavetta estiża speċifikata fl-ispeċifikazzjoni tal-lista tal-istatus tat-token.

3. L-istruttura tal-Lista ta' Identifikazzjoni għandha tkun struttura CBOR bil-Lingwa tad-Definizzjoni tad-Data Konċiża (CDDL) li ġejja:

```
Lista ta' Identifikaturi = {
 "identifikaturi": { * Identifier => IdentifierInfo },
   ? "aggregation_uri" : Aggregation_uri,
   * tstr => RFU
}

IdentifierInfo = {
```

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

Identifier = bstr

 Aggregation_uri = tstr
```