Consiglio dell'Unione europea

Bruxelles, 10 luglio 2026
(OR. en)

11772/26
ADD 1

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

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	1º luglio 2026
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	C(2026) 4534 annex
Oggetto:	ALLEGATI del REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE che integra la direttiva (UE) 2024/2841 per quanto riguarda la definizione del codice QR sulla versione fisica della carta europea della disabilità, la definizione del codice QR e delle specifiche tecniche comuni che garantiscono la sicurezza della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità, nonché le questioni relative all'interoperabilità

COMMISSIONE
EUROPEA

Bruxelles, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ALLEGATI

del

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

che integra la direttiva (UE) 2024/2841 per quanto riguarda la definizione del codice QR sulla versione fisica della carta europea della disabilità, la definizione del codice QR e delle specifiche tecniche comuni che garantiscono la sicurezza della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità, nonché le questioni relative all'interoperabilità

ALLEGATO I

SPECIFICHE DEL CODICE QR PER LA VERSIONE FISICA DELLA CARTA EUROPEA DELLA DISABILITÀ

1. **Formato del codice QR per la versione fisica della carta europea della disabilità CED (European Disability Card - EDC)**

(a) **Formato del codice QR Modello 2**, conformemente alle specifiche internazionali del codice QR ISO/IEC 18004: 2024 o equivalente.

(b) **Livello di correzione di errore M** (ridondanza del 15 %) che garantisce la resilienza ai graffi o ai danni parziali di un codice QR stampato.

(c) **Modalità di codifica -** Il payload (carico utile) del QR è costituito dalla struttura combinata issuerSigned Concise Binary Object Representation (CBOR) e il corrispondente issuerAuth COSE_Sign1 signature object come definito in CBOR Object Signing and Encryption (COSE, RFC 9052 sezioni 3.1, 4.2 e 4.4), secondo il modello di dati mDOC per gli elementi issuerSigned, ma adattato per l'uso statico della carta fisica. L'issuerAuth è un oggetto COSE_Sign1 con alg = ES256 e un'intestazione protetta contenente x5t (il parametro di intestazione hash del certificato COSE X.509 definito in RFC 9360 (sezione 2); ai fini dell'interoperabilità, l'algoritmo hash utilizzato in x5t è SHA-256).

(d) Prima della codifica del codice QR, l'oggetto CBOR/COSE combinato deve essere **compresso utilizzando il formato zlib** (RFC 1950, sezione 2.2) **con** l'algoritmo **Deflate** (RFC 1951, sezioni 3.2 e 4). L'array di byte compresso risultante è codificato nella **modalità Byte del codice QR**, garantendo il pieno supporto per i payload binari CBOR/COSE e l'interoperabilità dello scanner.

Per tutti i campi di testo inclusi nel payload del QR gli emittenti codificano caratteri come Unicode UTF-8 nelle stringhe di testo CBOR. La traslitterazione non si applica ai dati di payload firmati. Ai fini dell'interoperabilità, gli emittenti applicano il modulo di normalizzazione Unicode C (NFC) a tutti i campi testuali prima della firma.

(e) **Prefisso -** La stringa del QR EDC inizia con "ED1: MDOC:", che identifica il tipo di carta e il profilo di codifica. I prefissi differenziano fra maiuscole e minuscole e devono essere presenti. Prefissi sconosciuti o non supportati comportano il rigetto. Il prefisso e il payload compresso sono codificati come segmento di dati singolo in modalità byte nel codice QR.

(f) **Dimensione minima del modulo ≥ 0,25 mm** per garantire la leggibilità sulle carte stampate.

(g) **Versione massima 20;** con un massimo di 97 × 97 moduli su ciascun lato.

2. **Specifiche di generazione della firma EDC**

Il sigillo elettronico qualificato (QSeal) utilizzato per sigillare i codici QR EDC garantisce che i dati codificati provengano dall'autorità emittente autorizzata e non siano stati alterati.

(a) **Algoritmo di firma**- L'algoritmo di firma è ES256 (algoritmo di firma digitale a curva ellittica (ECDSA) con SHA-256 e con uso della curva P-256), come definito in

RFC 9053 (sezione 2.1); in COSE, l'algoritmo è identificato dal parametro di intestazione alg in RFC 9052 (sezione 3.1).

(b) **Chiave di firma**- Il payload del QR è firmato utilizzando la chiave privata corrispondente a un certificato qualificato di sigillo elettronico (QSealC).

(c) **Struttura COSE-** Il contenitore di firma deve essere un oggetto COSE_Sign1. L'intestazione protetta comprende alg (ES256) e x5t (il parametro di intestazione hash del certificato COSE X.509 definito in RFC 9360 (sezione 2); ai fini dell'interoperabilità, l'algoritmo hash utilizzato in x5t è SHA-256). La verifica si basa sull'uso del valore x5t per localizzare il certificato corrispondente nel trust store nella cache locale del verificatore creato a partire dalle informazioni dell'elenco di fiducia, e convalida quindi la catena dei certificati e lo stato del certificato conformemente al quadro di fiducia eIDAS.

(d) **Norma della firma**- Il payload del codice QR è firmato come oggetto COSE_Sign1 conformemente all'RFC 9052 (sezione 4), CBOR Object Signing and Encryption. L'oggetto COSE_Sign1 è contenuto in issuerAuth e codificato senza il tag CBOR per COSE_Sign1. Il campo payload dell'oggetto COSE_Sign1 è separato e codificato come CBOR nullo. Per la generazione e la verifica della firma, il payload esterno è la struttura CBOR codificata in maniera deterministica contenente il valore docType e il valore issuerSigned della mappa CBOR di livello superiore.

(e) **Algoritmo hash**- SHA-256 è utilizzato nell'ambito di ES256 per la generazione della firma e la verifica dell'integrità.

(f) **Codifica**- Il payload è codificato utilizzando il CBOR (RFC 8949, sezione 4.2), come richiesto dalle specifiche COSE e mDOC, garantendo la codifica e la riproducibilità dei dati firmati.

3. **Specifiche di stampa**

(a) **Zona chiara**- Il codice QR è circondato da un chiaro margine di **4 moduli** su tutti i lati, privo di stampa, motivi o sfondo.

(b) **Contrasto**- Il codice QR è stampato su sfondo bianco, con un rapporto di contrasto minimo di **4:1**, per garantire un'elevata leggibilità in condizioni di illuminazione variabili.

(c) Il codice QR è stampato usando il colore definito nell'allegato I della direttiva (UE) 2024/2841 che garantisce il massimo contrasto.

(d) **Posizionamento e dimensioni**- Il codice QR, compresa la zona chiara, è di 26,25 mm × 26,25 mm, ed è situato sul verso della carta nell'angolo in basso a destra. Il codice QR deve essere al massimo la versione 20 (97 × 97 moduli), con una dimensione del modulo pari o superiore a 0,25 mm.

Il codice QR, compresa la zona chiara, è posizionato ad almeno 5 mm dal bordo destro e ad almeno 5 mm dal bordo inferiore della carta.

4. **Dati contenuti nel codice QR EDC**

Il codice QR contiene un insieme di dati minimo verificabile offline conformemente al principio di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679. La struttura del payload è la seguente:

(a) gli attributi della carta sono codificati in CBOR nell'ambito di un oggetto issuerSigned;

(b) la struttura è impacchettata e firmata dal QSeal dell'autorità emittente come issuerAuth (COSE_Sign1, ES256, incluso x5t, il parametro di intestazione hash del certificato COSE X.509);

(c) l'oggetto CBOR/COSE risultante è compresso conformemente al punto 1, lettera d), del presente allegato. Il payload del codice QR è composto dal prefisso "ED1:MDOC:" seguito dall'array di byte compresso risultante, e il payload completo è codificato usando la modalità byte come segmento di dati singolo del codice QR.

Il contenuto dei dati è costituito da un sottoinsieme di dati visibili dai campi del recto della carta elencati nell'allegato I della direttiva (UE) 2024/2841 (nome, cognome, numero di serie della carta, data di scadenza), insieme all'identificatore di revoca, alla firma elettronica e alle informazioni di schema.

La **firma elettronica** contiene:

i) issuerAuth - oggetto COSE_Sign1 firmato con la **chiave privata QSealC** dell'autorità emittente;

ii) un'intestazione protetta che comprende alg = ES256 (algoritmo di firma) e x5t (parametro di intestazione hash del certificato COSE X.509).

5. Dati facoltativi

Il codice QR non contiene dati facoltativi.

6. Identificatore di revoca (RID)

Oltre al numero di serie visibile della carta, il codice QR include un apposito identificatore di revoca (RID).

Il RID è utilizzato per determinare lo stato della revoca e per la gestione dell'elenco delle revoche. Il RID non è stampato sulla carta e i verificatori non possono visualizzarlo.

6.1. *Requisiti del RID*

Il RID:

(a) è incluso nel payload del QR firmato;

(b) è univoco almeno all'interno del dominio di emissione dell'autorità emittente;

(c) non è stampato sulla carta e non è destinato ad essere leggibile dall'uomo;

(d) non rivela dati personali e non ha un significato diretto;

(e) non si può dedurre direttamente dal numero di serie visibile della carta, e

(f) è associato crittograficamente al payload del QR dal sigillo elettronico qualificato.

6.2. *Formato e dimensioni del RID*

Il RID è codificato come una stringa di byte CBOR (bstr). Ha una lunghezza di 16 byte (128 bit).

Il RID è generato dall'autorità emittente utilizzando un metodo sotto il suo controllo che garantisca sufficiente entropia e resistenza all'indovinazione o all'enumerazione.

6.3. *Elenchi delle revoche*

Gli elenchi delle revoche pubblicati a fini di verifica menzionano solo il RID delle carte revocate. I numeri di serie delle carte non sono pubblicati negli elenchi delle revoche.

7. Payload CBOR (all'interno del codice QR) dell'EDC

Nel payload QR sono inclusi solo i seguenti dati, coerenti con i campi di dati EDC visibili di cui all'allegato I della direttiva (UE) 2024/2841.

Contenuti di primo livello:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces."eu.edc" con gli attributi figuranti nella tabella di cui sotto

(c) issuerAuth = COSE_Sign1 (QSeal)

Campo	**Percorso mDOC**	**Tipo/Formato**
Versione dello schema di dati	issuerSigned.nameSpaces."eu.edc".ver	Stringa (ad es., "1.0")
Tipo di carta: EDC	docType	Enum ("eu.edc")
Numero di serie della carta	issuerSigned.nameSpaces."eu.edc".sub	Stringa
Identificatore di revoca	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 byte)
Nome del titolare della carta	issuerSigned.nameSpaces."eu.edc".givenName	Stringa di testo Unicode (UTF-8)
Cognome del titolare della carta	issuerSigned.nameSpaces."eu.edc".familyName	Stringa di testo Unicode (UTF-8)
Data di scadenza della carta	issuerSigned.nameSpaces."eu.edc".exp	Tag CBOR 1004 come definito in RFC 8943 (sezione 2.1), contenente una stringa di testo UTF-8 che rappresenta una data completa secondo RFC

		3339 in formato AAAA-MM-GG.

La firma elettronica è contenuta in issuerAuth (oggetto COSE_Sign1). La catena dei certificati non è integrata nel payload del codice QR; l'intestazione protetta COSE deve invece includere x5t, un'identificazione personale (thumbprint) del certificato usata per localizzare il QSealC corrispondente nel trust store nella cache del verificatore.

8. Esempio di payload del codice QR dell'EDC: rappresentazione logica in stile notazione oggetti JavaScript commentata

L'esempio seguente è una rappresentazione tramite notazione oggetti JavaScript (JSON), leggibile dall'uomo, della vista logica dell'EDC. Nella pratica, questa struttura non è leggibile dall'uomo in quanto:

(a) è codificata in CBOR (RFC 8949, sezione 3);

(b) è firmata usando la struttura COSE_Sign1 senza tag con un payload separato (RFC 9052, sezione 4.),

(c) include la data di scadenza come tag CBOR 1004, valore di data completa, conformemente a RFC 8943 (sezione 2.1);

(d) include il parametro x5t d'intestazione protetta conformemente a RFC 9360, usando SHA-256 sull'entità finale QSealC codificata in DER, e

(e) è compressa e dotata della stringa ED1:MDOC: come prefisso prima di essere codificata nel codice QR.

```
{
 // Vista logica dell'EDC, leggibile dall'uomo, in stile JSON, unicamente.
 // Il payload effettivo del codice QR è in CBOR deterministico, non JSON.
 "docType": "eu.edc", // credenziale EDC. Il valore docType è incluso, insieme a
  //issuerSigned, nel payload esterno COSE_Sign1.

 "issuerSigned": {
  // Dati protetti da issuerAuth; usati come payload separato.
  // Per la generazione e la verifica della firma, il payload esterno separato copre sia
  // docType sia issuerSigned.
  "nameSpaces": {
```

```
    "eu.edc": {
      "ver": "1.0", // profilo QR/versione dello schema

      // Numero di serie della carta; definito dall'emittente, massimo 24 caratteri
      "sub": "AB123456789012345678 90CD",

      // Identificatore di revoca: CBOR bstr effettivo, 16 byte/128 bit.
      // Rappresentato qui come 32 caratteri esadecimali per una migliore leggibilità.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ann",    // nome stampato sull'EDC
      "familyName": "Other", // cognome stampato sull'EDC

      // La codifica CBOR effettiva utilizza il tag 1004 per la data completa conformemente a RFC 3339.
      "exp": "2030-12-31"
    }
  }
},

 "issuerAuth": {
  // Forma effettiva: COSE_Sign1 senza tag, non un oggetto JSON.
  "type": "COSE_Sign1",
  "tagged": falso,       // codificato senza il tag COSE_Sign1 CBOR
  "payload": "detached", // il campo payload COSE è CBOR nullo

  "protectedHeader": {
    // alg: ES256; parametro di intestazione COSE equivalente 1 = -7.
    "alg": "ES256",
```

```
    // x5t: identificazione personale (thumbprint) del certificato; parametro di intestazione COSE 34.

    "x5t": {

      "hashAlg": "SHA-256", // valore hash COSE equivalente -16


      // hash SHA-256 dell'entità finale QSealC codificata in DER.

      // 32 byte rappresentati come 64 caratteri esadecimali.

      "hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

    }

  },


  "unprotectedHeader": {}, // vuoto in questo esempio


  // firma COSE ES256: 64 byte = 128 caratteri esadecimali.

  "signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

 }

}
```

9. Uso di meccanismi crittografici

L'uso di meccanismi crittografici nel contesto del presente allegato è conforme agli Agreed Cryptographic Mechanisms ("Meccanismi crittografici concordati") approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

ALLEGATO II

SPECIFICHE DEL CODICE QR PER LA VERSIONE FISICA DEL CONTRASSEGNO EUROPEO DI PARCHEGGIO PER LE PERSONE CON DISABILITÀ

1. **Formato del codice QR per la versione fisica del contrassegno europeo di parcheggio per le persone con disabilità (European Parking Card - EPC)**

(a) **Formato del codice QR Modello 2**, conformemente alle specifiche internazionali del codice QR ISO/IEC 18004: 2024 o equivalente.

(b) **Livello di correzione di errore M** (ridondanza del 15 %) che garantisce la resilienza ai graffi o ai danni parziali di un codice QR stampato.

(c) **Modalità di codifica -** Il payload (carico utile) del QR è costituito dalla struttura combinata issuerSigned Concise Binary Object Representation (CBOR) e il corrispondente issuerAuth COSE_Sign1 signature object come definito in CBOR Object Signing and Encryption (COSE, RFC 9052 sezioni 3.1, 4.2 e 4.4), secondo il modello di dati mDOC per gli elementi issuerSigned, ma adattato per l'uso statico della carta fisica. L'issuerAuth è un oggetto COSE_Sign1 con alg = ES256 e un'intestazione protetta contenente x5t (il parametro di intestazione hash del certificato COSE X.509 definito in RFC 9360 (sezione 2); ai fini dell'interoperabilità, l'algoritmo hash utilizzato in x5t è SHA-256).

(d) Prima della codifica del codice QR, l'oggetto CBOR/COSE combinato deve essere **compresso utilizzando il formato zlib (RFC 1950, sezione 2.2) con** l'algoritmo **Deflate** (RFC 1951, sezioni 3.2 e 4). L'array di byte compresso risultante è codificato nella **modalità byte del codice QR**, garantendo il pieno supporto per i payload binari CBOR/COSE e l'interoperabilità dello scanner.

Per tutti i campi di testo inclusi nel payload del QR gli emittenti codificano caratteri come Unicode UTF-8 nelle stringhe di testo CBOR. La traslitterazione non si applica ai dati di payload firmati. Ai fini dell'interoperabilità, gli emittenti applicano il modulo di normalizzazione Unicode C (NFC) a tutti i campi testuali prima della firma.

(e) **Prefisso**- La stringa del QR EPC inizia con "EP1: MDOC:", che identifica il tipo di contrassegno e il profilo di codifica. I prefissi differenziano fra maiuscole e minuscole e devono essere presenti. Prefissi sconosciuti o non supportati comportano il rigetto. Il prefisso e il payload compresso sono codificati come segmento di dati singolo in modalità byte nel codice QR.

(f) **Dimensione minima del modulo ≥ 0,35 mm** per garantire la leggibilità sui contrassegni stampati.

(g) **Versione massima 20**; con un massimo di 97 × 97 moduli su ciascun lato.

2. **Specifiche di generazione della firma EPC**

Il sigillo elettronico qualificato (QSeal) utilizzato per sigillare i codici QR EPC garantisce che i dati codificati provengano dall'autorità emittente autorizzata e non siano stati alterati.

(a) **Algoritmo di firma**- L'algoritmo di firma è ES256 (ECDSA con SHA-256 e con uso della curva P-256), come definito in RFC 9053 (sezione 2.1); in COSE, l'algoritmo è identificato dal parametro di intestazione alg in RFC 9052 (sezione 3.1).

(b) **Chiave di firma**- Il payload del QR è firmato utilizzando la chiave privata corrispondente a un certificato qualificato di sigillo elettronico (QSealC).

(c) **Struttura COSE**- Il contenitore di firma deve essere un oggetto COSE_Sign1. L'intestazione protetta comprende alg (ES256) e x5t (il parametro di intestazione hash del certificato COSE X.509 definito in RFC 9360 (sezione 2); ai fini dell'interoperabilità, l'algoritmo hash utilizzato in x5t è SHA-256). La verifica si basa sull'uso del valore x5t per localizzare il certificato corrispondente nel trust store nella cache locale del verificatore creato a partire dalle informazioni dell'elenco di fiducia, e convalida quindi la catena dei certificati e lo stato del certificato conformemente al quadro di fiducia eIDAS.

(d) **Norma della firma**- Il payload del codice QR è firmato come oggetto COSE_Sign1 conformemente all'RFC 9052 (sezione 4), CBOR Object Signing and Encryption. L'oggetto COSE_Sign1 è contenuto in issuerAuth e codificato senza il tag CBOR per COSE_Sign1. Il campo payload dell'oggetto COSE_Sign1 è separato e codificato come CBOR nullo. Per la generazione e la verifica della firma, il payload esterno è la struttura CBOR codificata in maniera deterministica contenente il valore docType e il valore issuerSigned della mappa CBOR di livello superiore.

(e) **Algoritmo hash**- SHA-256 è utilizzato nell'ambito di ES256 per la generazione della firma e la verifica dell'integrità.

(f) **Codifica**- Il payload è codificato utilizzando il CBOR (RFC 8949, sezione 4.2), come richiesto dalle specifiche COSE e mDOC, garantendo la codifica e la riproducibilità dei dati firmati.

3. **Specifiche di stampa**

(a) **Zona chiara**- Il codice QR è circondato da un chiaro margine di **4 moduli** su tutti i lati, privo di stampa, motivi o sfondo.

(b) **Contrasto**- Il codice QR è stampato su sfondo bianco, con un rapporto di contrasto minimo di **4:1**, per garantire un'elevata leggibilità in condizioni di illuminazione variabili.

(c) Il codice QR è stampato usando il colore definito nell'allegato I della direttiva (UE) 2024/2841 che garantisce il massimo contrasto.

(d) **Posizionamento e dimensioni-** Il codice QR, compresa la zona chiara, è di **37 mm** × **37 mm**, ed è situato sul recto del contrassegno, leggermente a destra rispetto al centro, verso il bordo inferiore. Il codice QR deve essere al massimo la versione 20 (97 × 97 moduli), con una dimensione del modulo pari o superiore a 0,35 mm.

Il codice QR, compresa la zona chiara, è posizionato ad almeno 5 mm dal bordo inferiore della carta.

4. **Dati contenuti nel codice QR EPC**

Il codice QR contiene un insieme di dati minimo verificabile offline conformemente al principio di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679. La struttura del payload è la seguente:

(a) gli attributi del contrassegno sono codificati in CBOR nell'ambito di un oggetto issuerSigned;

(b) tale struttura è impacchettata e firmata dal QSeal dell'autorità emittente come issuerAuth (COSE_Sign1, ES256, incluso x5t, il parametro di intestazione hash del certificato COSE X.509);

(c) l'oggetto CBOR/COSE risultante è compresso conformemente al punto 1, lettera d), del presente allegato. Il payload del codice QR è composto dal prefisso "EP1:MDOC:" seguito dall'array di byte compresso risultante, e il payload completo è codificato usando la modalità byte come segmento di dati singolo del codice QR.

Il contenuto dei dati è costituito da un sottoinsieme di dati visibili dai campi del recto del contrassegno elencati nell'allegato II della direttiva (UE) 2024/2841 (data di scadenza, numero di serie del contrassegno), insieme all'identificatore di revoca, alla firma elettronica e alle informazioni di schema.

La **firma elettronica** contiene:

i) issuerAuth - oggetto COSE_Sign1 firmato con la **chiave privata QSealC** dell'autorità emittente;

ii) un'intestazione protetta che comprende alg = ES256 (algoritmo di firma) e x5t (parametro di intestazione hash del certificato COSE X.509).

5. Dati facoltativi

Il codice QR non contiene dati facoltativi.

6. Identificatore di revoca (RID)

L'identificatore di revoca dell'EPC è conforme all'allegato I, punto 6.

Gli elenchi delle revoche, per l'EPC, menzionano solo il RID. I numeri di serie dei contrassegni non sono pubblicati negli elenchi delle revoche.

7. Payload CBOR (all'interno del codice QR) dell'EPC

Nel payload QR sono inclusi solo i seguenti dati, coerenti con i campi del contrassegno EPC visibili di cui all'allegato II della direttiva (UE) 2024/2841.

Campo	**Percorso mDOC**	**Tipo/Formato**
Versione dello schema di dati	issuerSigned.nameSpaces."eu.epc".ver	Stringa (ad es., "1.0")
Tipo di contrassegno: EPC	docType	Enum ("eu.epc")
Numero di serie del contrassegno	issuerSigned.nameSpaces."eu.epc".sub	Stringa
Identificatore di revoca	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 byte)

Data di scadenza del contrassegno	issuerSigned.nameSpaces."eu.epc".exp	Tag CBOR 1004 come definito in RFC 8943 (sezione 2.1), contenente una stringa di testo UTF-8 che rappresenta una data completa secondo RFC 3339 in formato AAAA-MM-GG.

La firma elettronica è contenuta in issuerAuth (oggetto COSE_Sign1). La catena dei certificati non è integrata nel payload del codice QR; l'intestazione protetta COSE deve invece includere x5t, un'identificazione personale (thumbprint) del certificato usata per localizzare il QSealC corrispondente nel trust store nella cache del verificatore.

8. Esempio di payload del codice QR dell'EPC: rappresentazione logica in stile notazione oggetti JavaScript commentata

L'esempio seguente è una rappresentazione tramite notazione oggetti JavaScript (JSON), leggibile dall'uomo, della vista logica dell'EPC. Nella pratica, questa struttura non è leggibile dall'uomo in quanto è:

(a) codificata in CBOR (RFC 8949, sezione 3);

(b) è firmata usando la struttura COSE_Sign1 senza tag con un payload separato (RFC 9052, sezione 4.),

(c) include la data di scadenza come tag CBOR 1004, valore di data completa, conformemente a RFC 8943 (sezione 2.1);

(d) include il parametro x5t d'intestazione protetta conformemente a RFC 9360, usando SHA-256 sull'entità finale QSealC codificata in DER, e

(e) è compressa e dotata della stringa EP1:MDOC: come prefisso prima di essere codificata nel codice QR.

```
{
 // Vista logica dell'EDC, leggibile dall'uomo, in stile JSON, unicamente.
 // Il payload effettivo del codice QR è in CBOR deterministico, non JSON.
```

```
 "docType": "eu.epc", // credenziale EPC. Il valore docType è incluso, insieme a
   //issuerSigned, nel payload esterno COSE_Sign1.

 "issuerSigned": {
   // Dati protetti da issuerAuth; usati come payload separato.
// Per la generazione e la verifica della firma, il payload esterno separato copre sia
   // docType sia issuerSigned.
   "nameSpaces": {
     "eu.epc": {
       "ver": "1.0", // profilo QR/versione dello schema

       // Numero di serie della carta; definito dall'emittente, massimo 24 caratteri
       "sub": "EF123456789012345678 90GH",

       // Identificatore di revoca: CBOR bstr effettivo, 16 byte/128 bit.
       // Rappresentato qui come 32 caratteri esadecimali per una migliore leggibilità.
       "rid": "4a8d9c112233445566778899aabbccdd",

       // La codifica CBOR effettiva utilizza il tag 1004 per la data completa conformemente a
RFC 3339.
       "exp": "2030-12-31"
     }
   }
 },

 "issuerAuth": {
   // Forma effettiva: COSE_Sign1 senza tag, non un oggetto JSON.
   "type": "COSE_Sign1",
```

```
  "tagged": falso,       // codificato senza il tag COSE_Sign1 CBOR
  "payload": "detached", // il campo payload COSE è CBOR nullo

  "protectedHeader": {
    // alg: ES256; parametro di intestazione COSE equivalente 1 = -7.
    "alg": "ES256",

    // x5t: identificazione personale (thumbprint) del certificato; parametro di intestazione COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // valore hash COSE equivalente -16

      // hash SHA-256 dell'entità finale QSealC codificata in DER.
      // 32 byte rappresentati come 64 caratteri esadecimali.
      "hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // vuoto in questo esempio

  // firma COSE ES256: 64 byte = 128 caratteri esadecimali.
  "signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Uso di meccanismi crittografici

L'uso di meccanismi crittografici nel contesto del presente allegato è conforme agli Agreed Cryptographic Mechanisms ("Meccanismi crittografici concordati") approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

ALLEGATO III

NOTIFICA DELLE INFORMAZIONI DI CUI ALL'ARTICOLO 6, PARAGRAFO 2

1. Gli Stati membri forniscono alla Commissione le informazioni seguenti su ciascuna autorità o ciascun organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità:

   (a) il nome dell'autorità o dell'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità;

   (b) un numero di registrazione dell'autorità o dell'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità;

   (c) l'indirizzo di posta elettronica di contatto e il numero di telefono di contatto dell'autorità o dell'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità;

   (d) uno o più certificati che possono essere utilizzati per verificare il sigillo elettronico creato dall'autorità o dall'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità, e per i quali i dati di identità certificati comprendono il nome e il numero di registrazione dell'emittente, come specificato rispettivamente alle lettere a) e b);

   (e) l'ubicazione URL in cui l'emittente pubblica lo stato di validità delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità.

2. Gli Stati membri possono fornire alla Commissione le informazioni seguenti su ciascuna autorità o ciascun organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità:

   (a) l'URL della pagina web contenente le politiche, i termini e le condizioni dell'autorità o dell'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità, che si applicano alla fornitura e all'uso delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità che essi emettono;

   (b) se del caso, l'URL della pagina web contenente informazioni aggiuntive sull'autorità o sull'organismo competente responsabile del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità.

ALLEGATO IV

SPECIFICHE TECNICHE DI UN ELENCO DELLE REVOCHE PER LE VERSIONI FISICHE DELLA CARTA EUROPEA DELLA DISABILITÀ O DEL CONTRASSEGNO EUROPEO DI PARCHEGGIO PER LE PERSONE CON DISABILITÀ

1. Ai fini del presente allegato, l'identificatore corrisponde all'identificatore di revoca (RID) di cui all'allegato I, punto 6, e all'allegato II, punto 6.

2. È implementato un elenco delle revoche come token dell'elenco degli identificatori in formato CWT (RFC 8392, sezione 7) conformemente alla clausola 5.2 della specifica relativa all'elenco degli stati del token (draft-ietf-oauth-status-list-14) con le seguenti modifiche:

   (a) il valore della dichiarazione "type" [tipo] è "application/identifierlist+cwt";

   (b) la dichiarazione della data di scadenza deve essere presente;

   (c) la dichiarazione StatusList non deve essere presente nella serie di dichiarazioni CWT;

   (d) la struttura di IdentifierList definita al punto 3 deve essere presente come dichiarazione nella serie di dichiarazioni CWT, con l'utilizzo della chiave 65530;

   (e) il CWT deve essere un oggetto COSE_Sign1 che utilizza, per calcolare la firma, un algoritmo di firma conforme agli Agreed Cryptographic Mechanisms ("Meccanismi crittografici concordati") approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA);

   (f) nel CWT deve figurare il parametro x5chain quale definito in RFC 9360 (sezione 2) nell'intestazione protetta che contiene il certificato o la catena di certificati ai fini della verifica della firma dell'elenco delle revoche;

   (g) l'utilizzo esteso della chiave OID di cui alla specifica relativa all'elenco degli stati dei token (draft-ietf-oauth-status-list-14) può essere impiegato per il certificato di firma dell'elenco degli identificatori e si raccomanda che i verificatori supportino l'utilizzo esteso della chiave OID di cui alla specifica relativa all'elenco degli stati dei token e che le infrastrutture dell'autorità emittente non rendano critico il campo relativo all'utilizzo esteso della chiave quando si ricorre all'OID per l'utilizzo esteso della chiave di cui alla specifica relativa all'elenco degli stati dei token.

3. La struttura di IdentifierList è una struttura CBOR con il seguente linguaggio di definizione dei dati conciso (Concise Data Definition Language - CDDL):

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

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

Identifier = bstr

Aggregation_uri = tstr
```