Gazzetta ufficiale
dell'Unione europea

IT
Serie L

2026/1436

12.11.2026

REGOLAMENTO DELEGATO (UE) 2026/1436 DELLA COMMISSIONE

del 1º luglio 2026

che integra la direttiva (UE) 2024/2841 del Parlamento europeo e del Consiglio 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

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2024/2841 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, che istituisce la carta europea della disabilità e il contrassegno europeo di parcheggio per le persone con disabilità ([1]), in particolare l'articolo 7, paragrafo 7, e l'articolo 8, paragrafo 7,

considerando quanto segue:

(1) La direttiva (UE) 2024/2841 stabilisce le norme che disciplinano il rilascio della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità e i modelli comuni per tale carta e tale contrassegno. Conformemente all'articolo 7, paragrafo 2, e all'articolo 8, paragrafo 2, della direttiva (UE) 2024/2841, le carte europee della disabilità e i contrassegni europei di parcheggio per le persone con disabilità rilasciati dagli Stati membri devono essere reciprocamente riconosciuti in tutti gli Stati membri.

(2) I conferimenti di poteri di cui all'articolo 7, paragrafo 7, e all'articolo 8, paragrafo 7, della direttiva (UE) 2024/2841 hanno la stessa finalità, vale a dire prevenire e combattere le frodi, garantire la sicurezza delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità, anche attraverso misure di sicurezza appropriate per i dati personali in conformità del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]), nonché garantire l'interoperabilità. Poiché l'oggetto e gli obiettivi dei conferimenti di poteri in larga misura coincidono, è opportuno stabilire norme che integrino la direttiva (UE) 2024/2841 per quanto riguarda tali materie in un unico atto delegato.

(3) La direttiva (UE) 2024/2841 prevede che le versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità contengano un codice QR quale caratteristica digitale all'avanguardia che utilizza mezzi elettronici per scongiurare e combattere le frodi. In quanto tali, i codici QR sono una caratteristica digitale obbligatoria da stampare su ogni carta e contrassegno fisici. Per garantire un approccio uniforme nella creazione e nell'uso dei codici QR da parte degli Stati membri, la Commissione dovrebbe adottare specifiche tecniche per la loro definizione, compreso il loro contenuto.

(4) Il contrassegno europeo di parcheggio per le persone con disabilità sostituirà tutti gli attuali contrassegni di parcheggio per i disabili rilasciati conformemente alla raccomandazione 98/376/CE del Consiglio ([3]). Tale raccomandazione non è stata aggiornata in modo da tenere conto degli sviluppi tecnologici e della digitalizzazione e gli Stati membri hanno riscontrato problemi di frode e falsificazione. È pertanto necessario stabilire le caratteristiche che garantiscano la sicurezza della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità e che tengano conto delle sue specificità, come il fatto che solitamente si trova dietro il parabrezza del veicolo.

([1]) GU L, 2024/2841,14.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2841/oj.

([2]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Raccomandazione 98/376/CE del Consiglio, del 4 giugno 1998, su un contrassegno di parcheggio per disabili (GU L 167 del 12.6.1998, pag. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Dovrebbero essere stabilite specifiche tecniche comuni obbligatorie per garantire la sicurezza della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità. Stampare la carta su un materiale appropriato, come il policarbonato, utilizzando un elemento diffrattivo otticamente variabile dell'immagine, proteggerebbe efficacemente da falsificazioni e da contraffazioni. I motivi antiscansione aumenterebbero ulteriormente la sicurezza rendendo individuabile la duplicazione della carta, poiché dovrebbero contenere un testo o un motivo nascosto che apparirebbe quando la carta viene fotocopiata o scansionata. Tali caratteristiche devono essere applicate senza pregiudicare il formato della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità di cui all'allegato II della direttiva (UE) 2024/2841, compreso l'aspetto visivo del contrassegno.

(6) Oltre al codice QR e ad altre specifiche tecniche obbligatorie stabilite dal presente regolamento gli Stati membri, al fine di rafforzare la sicurezza del contrassegno europeo di parcheggio per le persone con disabilità, dovrebbero avere la possibilità di integrare nella sua versione fisica caratteristiche di sicurezza digitali o fisiche facoltative, basate sulle specifiche tecniche comuni stabilite nel presente regolamento. Qualora le caratteristiche digitali facoltative contengano un numero di dati personali superiore a quello previsto nelle versioni fisiche dei contrassegni, conformemente all'allegato II, punto 3, lettera b), della direttiva (UE) 2024/2841 l'accesso a tali dati deve essere limitato alle autorità pubbliche degli Stati membri di rilascio e ai soli utenti autorizzati. Per mantenere un quadro armonizzato per le caratteristiche di sicurezza in tutti gli Stati membri, l'elenco delle caratteristiche facoltative dovrebbe essere esaustivo. Gli Stati membri dovrebbero inoltre garantire che l'integrazione di una o più caratteristiche di sicurezza digitali o fisiche facoltative non pregiudichi il riconoscimento di contrassegni validi di altri Stati membri né comprometta l'interoperabilità e la funzionalità delle specifiche tecniche obbligatorie.

(7) La versione fisica del contrassegno europeo di parcheggio per le persone con disabilità può contenere un chip di identificazione a radiofrequenza (*radio-frequency identification chip* - RFID) come caratteristica di sicurezza digitale facoltativa. L'RFID si avvale di onde elettromagnetiche o dell'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da o verso un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati ([4]). I chip RFID possono rafforzare la protezione contro la falsificazione e la manomissione stoccando o trasmettendo in modo sicuro i dati relativi al contrassegno. La versione fisica del contrassegno europeo di parcheggio per le persone con disabilità può contenere anche inchiostro otticamente variabile o inchiostro cangiante. Tali inchiostri offrono una protezione adeguata contro la copiatura e la manomissione del contrassegno senza necessità di personalizzazione. Per garantire che i dati del contrassegno siano adeguatamente protetti contro tentativi di contraffazione e falsificazione, il testo dei campi di dati può essere integrato nel materiale di base del contrassegno utilizzando la tecnica di incisione laser. Le caratteristiche di sicurezza fisiche, siano esse obbligatorie o facoltative ai sensi del presente regolamento, che non sono visibili o che diventano visibili a seguito di determinate manipolazioni, non confliggono con il formato del contrassegno europeo di parcheggio per le persone con disabilità di cui all'allegato II della direttiva (UE) 2024/2841.

(8) I progressi tecnologici, i sistemi di verifica dei parcheggi e i rischi per la sicurezza sono in continua evoluzione. I livelli tecnologici sono in costante avanzamento e l'uso della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità evolve, sulla base sia dei riscontri degli utenti che del progresso tecnologico, così come evolvono le tecniche di frode e falsificazione, portando a un continuo mutamento delle sfide in materia di sicurezza. Pertanto, le nuove soluzioni tecnologiche, comprese quelle relative alla verifica dei parcheggi, come pure le esigenze di sicurezza e di prevenzione antifrode potrebbero richiedere modifiche nell'architettura di sicurezza e antifrode delle carte e dei contrassegni, anche attraverso l'aggiornamento della categorizzazione delle caratteristiche digitali come obbligatorie o facoltative. A seconda degli sviluppi tecnologici, potrebbe rendersi necessario l'aggiornamento del presente regolamento.

(9) Per garantire che le versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità possano essere utilizzate senza soluzione di continuità in tutti gli Stati membri, è necessario garantire l'interoperabilità delle caratteristiche digitali delle carte e dei contrassegni fisici, in particolare i codici QR. L'interoperabilità dovrebbe consentire la verifica dell'autenticità e della validità delle versioni fisiche delle carte e dei contrassegni da parte dei verificatori - vale a dire da parte di qualsiasi persona fisica o giuridica incaricata di controllare la validità e l'autenticità delle versioni fisiche delle carte e dei contrassegni, ad esempio mediante un'applicazione di verifica. A tal fine è necessario stabilire disposizioni sulle questioni relative all'interoperabilità in modo da consentire che le verifiche transfrontaliere delle versioni fisiche delle carte e dei contrassegni siano effettuate in modo coerente e affidabile.

([4]) Raccomandazione 2009/387/CE della Commissione, del 12 maggio 2009, sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza (GU L 122 del 16.5.2009, pag. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) Al fine di garantire l'integrità e l'origine dei dati contenuti nei codici QR nelle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità, tali dati dovrebbero essere sigillati con un sigillo elettronico qualificato quale definito all'articolo 3, punto 27), del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([5]). Il codice QR conferma l'autenticità e la validità della carta o del contrassegno fisici quando viene controllato rispetto ai parametri di verifica, e non dovrebbe di per sé attestare la condizione di disabilità o il diritto a servizi specifici sulla base di una disabilità.

(11) Al fine di agevolare l'interoperabilità e l'istituzione di un sistema affidabile e sicuro di verifica delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità in tutta l'Unione, è opportuno istituire meccanismi di notifica e pubblicazione delle informazioni. A tale riguardo, e al fine di poter verificare che le versioni fisiche della carta e del contrassegno siano rilasciate da un'autorità o da un organismo competente, gli Stati membri dovrebbero fornire le informazioni necessarie per il processo di verifica, in particolare le informazioni richieste per verificare il sigillo elettronico qualificato. Pertanto, gli Stati membri dovrebbero essere tenuti a notificare alla Commissione le autorità o gli organismi competenti responsabili del rilascio delle versioni fisiche della carta e del contrassegno («emittenti»), nonché le relative informazioni amministrative e tecniche pertinenti. Le informazioni da notificare alla Commissione dovrebbero essere limitate a quanto necessario per istituire meccanismi di verifica interoperabile della validità e dell'autenticità delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità. La Commissione dovrebbe garantire l'accesso del pubblico a tali informazioni.

(12) Inoltre, in caso di revoca della carta o del contrassegno, le informazioni sulla revoca dovrebbero essere immediatamente rese disponibili per consentire ai verificatori di controllare la validità della carta o del contrassegno. A tal fine, gli emittenti dovrebbero tenere aggiornati e pubblicare tempestivamente elenchi contenenti informazioni sullo stato della revoca di ogni carta e contrassegno oggetto di tale procedimento prima della loro data di scadenza («elenchi delle revoche»). Tale pubblicazione dovrebbe rispettare la vita privata e proteggere i dati personali dei titolari della carta o del contrassegno. Gli elenchi delle revoche non dovrebbero inoltre contenere altri dati personali oltre agli identificatori di revoca unici, e dovrebbero essere pubblicati presso uno specifico identificatore uniforme di risorsa (*Uniform Resource Identifier* - URI) conformemente alle specifiche tecniche per garantire una verifica interoperabile.

(13) Per leggere il codice QR e verificare l'autenticità e la validità delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità, possono essere utilizzate applicazioni di verifica ad hoc a livello nazionale. La Commissione può sostenere tale processo fornendo un campione di codice sorgente comune ai fini della lettura dei dati contenuti nei codici QR e dell'esecuzione delle fasi principali del processo di verifica, che può fungere da base per le applicazioni di verifica negli Stati membri. Tutte le applicazioni di verifica dovrebbero applicare la stessa logica di verifica della catena di fiducia rispetto alla stessa infrastruttura di fiducia, consentendo in tal modo la lettura dei dati codificati nelle carte e nei contrassegni da parte dello Stato membro di rilascio. L'allegato I della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio ([6]) stabilisce inoltre i requisiti di accessibilità che gli Stati membri devono se del caso rispettare.

(14) Consapevole della natura dinamica dei progressi tecnologici e dell'evoluzione delle minacce relative alla cibersicurezza, l'Unione si impegna a garantire che i meccanismi crittografici utilizzati nell'ambito del suo quadro normativo rimangano efficaci e sicuri. Alla luce di tale impegno, è importante adottare norme crittografiche approvate dal Gruppo europeo per la certificazione della cibersicurezza e diffuse attraverso l'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

(15) Al trattamento dei dati personali effettuato a norma del presente regolamento si applica il regolamento (UE) 2016/679. La verifica dei codici QR sulle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità comporta il trattamento di dati personali. È pertanto opportuno, se del caso, stabilire adeguate garanzie per assicurare la protezione dei dati personali contenuti nei codici QR in conformità del regolamento (UE) 2016/679. La protezione dei dati personali contenuti nei codici QR dovrebbe essere garantita anche dalle misure generali di sicurezza di cui al presente regolamento. I dati personali contenuti nei codici QR dovrebbero inoltre essere limitati a quanto strettamente necessario ai fini del presente regolamento. Dovrebbe essere altresì vietata la conservazione dei dati dopo la fine della verifica. È inoltre necessario garantire un'adeguata sicurezza degli elenchi delle revoche.

([5]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Direttiva (UE) 2019/882 del Parlamento e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi (GU L 151 del 7.6.2019, pag. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) Ai sensi dell'articolo 14, paragrafo 4, della direttiva (UE) 2024/2841, ai fini dell'elaborazione del presente regolamento la Commissione ha consultato le persone con disabilità e le organizzazioni che le rappresentano, nonché gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016 ([7]).

(17) La carta europea della disabilità e il contrassegno europeo di parcheggio per le persone con disabilità costituiscono un servizio pubblico digitale transeuropeo ai sensi del regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio ([8]). È stata effettuata di conseguenza una valutazione dell'interoperabilità e la relazione risultante deve essere pubblicata sul portale «Europa interoperabile» di cui all'articolo 8 dello stesso regolamento.

(18) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([9]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 12 maggio 2026,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto e ambito di applicazione

Il presente regolamento stabilisce norme che integrano la direttiva (UE) 2024/2841 per quanto riguarda:

(a) la definizione dei codici QR per le versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità, comprese le misure di sicurezza appropriate per i dati personali;

(b) la definizione di specifiche tecniche comuni obbligatorie e facoltative per garantire la sicurezza della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità;

(c) la definizione dei requisiti di interoperabilità necessari per garantire che i codici QR sulle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità rilasciati in uno Stato membro possano essere letti e verificati in modo affidabile in un altro Stato membro.

Articolo 2

Codice QR sulla versione fisica della carta europea della disabilità

Le specifiche del codice QR che deve figurare sulla versione fisica della carta europea della disabilità sono indicate nell'allegato I.

Articolo 3

Codice QR sulla versione fisica del contrassegno europeo di parcheggio per le persone con disabilità

Le specifiche del codice QR che deve figurare sulla versione fisica del contrassegno europeo di parcheggio per le persone con disabilità sono indicate nell'allegato II.

([7]) GU L 123 del 12.5.2016, pag. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([8]) Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio, del 13 marzo 2024, che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile) (GU L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Articolo 4

Specifiche tecniche comuni obbligatorie del contrassegno europeo di parcheggio per le persone con disabilità

1. Le versioni fisiche del contrassegno europeo di parcheggio per le persone con disabilità sono conformi alle seguenti specifiche tecniche comuni:

(a) sono costituite da un materiale che protegga dalla delaminazione e che soddisfi i requisiti di cui all'allegato II della direttiva (UE) 2024/2841 e le altre specifiche tecniche comuni obbligatorie di cui al presente articolo;

(b) contengono un elemento diffrattivo otticamente variabile dell'immagine come elemento di struttura a strati, che diventa visibile quando il contrassegno è osservato da una certa angolazione;

(c) sono realizzati con un motivo antiscansione che diventa visibile quando un contrassegno è fotocopiato o scansionato.

2. L'elemento diffrattivo otticamente variabile dell'immagine di cui al paragrafo 1, lettera b), figura sul recto della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità, sopra uno o più dei campi di dati situati sulla parte sinistra. Misura circa 20 mm di altezza e 20 mm di larghezza. L'immagine che figura sull'elemento ottico è costituita da una cartina geografica stilizzata dello Stato membro di rilascio o dal codice distintivo dello Stato membro di rilascio circondato dal cerchio di 12 stelle che simboleggia l'Unione.

3. Il motivo antiscansione di cui al paragrafo 1, lettera c), è collocato sul recto della versione fisica del contrassegno europeo di parcheggio per le persone con disabilità al di sopra dei campi di dati situati sulla parte sinistra e/o sulla parte destra al di fuori del codice QR e della sua zona chiara. Esso contiene un testo o un motivo nascosto, che appare quando il contrassegno è fotocopiato o scansionato. Nel caso in cui il motivo antiscansione contenga un testo nascosto, tale testo è costituito dai termini «COPY» («COPIA») oppure «VOID» («NON VALIDO»), e da una traduzione di tali termini in una o più lingue ufficiali dello Stato membro di rilascio. Nel caso in cui il motivo antiscansione contenga un motivo nascosto, tale motivo è costituito da linee orizzontali o verticali.

Articolo 5

Specifiche tecniche e caratteristiche facoltative per la sicurezza del contrassegno europeo di parcheggio per le persone con disabilità

1. Oltre alle specifiche tecniche comuni obbligatorie di cui all'articolo 4, gli Stati membri possono applicare solo le specifiche tecniche e caratteristiche facoltative stabilite nel presente articolo.

2. Le versioni fisiche del contrassegno europeo di parcheggio per le persone con disabilità possono contenere un chip di identificazione a radiofrequenza (*radio-frequency identification chip* - RFID). Il chip RFID serve a scongiurare e a combattere le frodi grazie a mezzi elettronici e funge da strumento supplementare a livello nazionale per la verifica dell'autenticità e/o della validità di una versione fisica del contrassegno europeo di parcheggio per le persone con disabilità. Il chip RFID non influisce sul funzionamento del codice QR sul contrassegno.

3. Il chip RFID di cui al paragrafo 2 è conforme alle seguenti specifiche:

(a) è passivo;

(b) è fisicamente integrato nel corpo del contrassegno, sulla parte destra del recto;

(c) è collegato logicamente al record del codice QR e contiene lo stesso identificatore di revoca (RID) codificato nel codice QR;

(d) la caratteristica RFID supporta la lettura a circa 1 metro o più ove richiesto per usi operativi, ma non è progettata per una lettura affidabile oltre i 5 metri in condizioni di test di riferimento;

(e) dopo l'emissione del contrassegno, l'autorità emittente impedisce o controlla in altro modo l'accesso in scrittura al chip RFID o alla relativa area dati;

(f) è progettato e configurato in modo da ridurre al minimo il rischio di clonazione, sostituzione, modifica non autorizzata e riscrittura non autorizzata;

(g) è conforme ai requisiti della direttiva 2014/53/UE del Parlamento europeo e del Consiglio ([10]);

(h) oltre al RID di cui alla lettera c), può stoccare solo uno o più dei seguenti elementi:

i) i dati codificati nel codice QR sulla versione fisica del contrassegno europeo di parcheggio per le persone con disabilità;

ii) il numero o i numeri di targa dei veicoli;

iii) i dati crittografici di verifica.

4. Il recto delle versioni fisiche del contrassegno europeo di parcheggio per le persone con disabilità può contenere una o più delle seguenti caratteristiche:

(a) il simbolo della sedia a rotelle sulla parte sinistra o, sulla parte destra, la dicitura «European Parking Card for persons with disabilities» («Contrassegno europeo di parcheggio per le persone con disabilità») in inglese e in una o più lingue ufficiali dello Stato membro di rilascio, a stampa con inchiostro otticamente variabile o con inchiostro cangiante, che cambia colore a seconda dell'angolo di osservazione;

(b) la stampa del testo nei campi di dati per mezzo della tecnica di incisione laser che penetra negli strati del contrassegno.

5. L'introduzione delle specifiche tecniche e caratteristiche facoltative di cui al presente articolo non pregiudica il riconoscimento, nello Stato membro che ha introdotto tali caratteristiche per i contrassegni che rilascia, dei contrassegni validi rilasciati in altri Stati membri.

Articolo 6

Questioni relative all'interoperabilità

1. Le informazioni contenute nel codice QR sono sigillate con un sigillo elettronico qualificato ai sensi dell'articolo 3, punto 27), del regolamento (UE) n. 910/2014.

2. Ciascuno Stato membro comunica alla Commissione informazioni sulle autorità o sugli organismi competenti responsabili del rilascio delle versioni fisiche della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità («emittenti»), e qualsiasi successivo aggiornamento di tali informazioni conformemente all'allegato III. La Commissione garantisce l'accesso del pubblico a tali informazioni.

3. Gli emittenti tengono aggiornati e pubblicano, presso un identificatore uniforme di risorsa notificato alla Commissione, gli elenchi delle revoche contenenti le informazioni sullo stato della revoca di ogni carta e contrassegno oggetto di tale procedimento conformemente alle specifiche tecniche di cui all'allegato IV. Le informazioni sulla revoca sono pubblicate entro 24 ore dalla revoca stessa.

4. Gli Stati membri possono utilizzare applicazioni di verifica per verificare l'autenticità e la validità delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità.

5. Qualora gli Stati membri utilizzino applicazioni di verifica per verificare l'autenticità e la validità delle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità, tali applicazioni sono in grado di verificare l'autenticità e la validità di una carta o di un contrassegno controllandone il sigillo elettronico e lo stato della revoca. Tali applicazioni di verifica leggono e propongono una rappresentazione visiva dei dati personali codificati nel codice QR della carta o del contrassegno, come indicato agli allegati I e II, per consentire un confronto con i dati visibili nei corrispondenti campi di dati della carta o del contrassegno, e un'indicazione relativa allo stato di validità della carta.

([10]) Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Articolo 7

Misure di sicurezza per la protezione dei dati personali

1. I dati personali contenuti nei codici QR sulle versioni fisiche della carta europea della disabilità e del contrassegno europeo di parcheggio per le persone con disabilità sono limitati a quanto strettamente necessario ai fini della verifica dell'autenticità e della validità delle carte e dei contrassegni, come indicato agli allegati I e II.

2. Una volta ultimata la verifica dell'autenticità e della validità di una versione fisica della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità, i verificatori non conservano i dati contenuti nei codici QR.

3. Non occorre che all'autorità o all'organismo competente responsabile del rilascio della carta europea della disabilità o del contrassegno europeo di parcheggio per le persone con disabilità sia notificata la verifica di un codice QR su una versione fisica di tale carta o contrassegno.

4. Le informazioni incluse in un elenco delle revoche pubblicato a norma dell'articolo 6, paragrafo 3, sono limitate all'identificatore di revoca della carta o del contrassegno revocati.

5. L'autorità o l'organismo responsabile della pubblicazione degli elenchi delle revoche a norma dell'articolo 6, paragrafo 3, provvede affinché al trattamento dei dati personali contenuti negli elenchi delle revoche siano applicate appropriate misure di sicurezza tecniche e organizzative.

6. Qualora uno Stato membro decida di incorporare un chip RFID nella versione fisica del contrassegno europeo di parcheggio per le persone con disabilità, al trattamento dei dati personali contenuti in tale chip si applicano i paragrafi da 2 a 3. I dati personali contenuti nel chip RFID sono limitati a quanto strettamente necessario ai fini della verifica dell'autenticità e/o della validità dei contrassegni, come stabilito all'articolo 5, paragrafo 3.

Qualora uno Stato membro registri nel chip RFID dati personali di cui all'articolo 5 che non sono previsti nella versione fisica del contrassegno europeo di parcheggio per le persone con disabilità secondo quanto indicato all'allegato II della direttiva (UE) 2024/2841, l'accesso a tali dati è limitato alle autorità pubbliche dello Stato membro di rilascio e solo agli utenti autorizzati.

Articolo 8

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 1º luglio 2026

Per la Commissione
La presidente
Ursula VON DER LEYEN

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":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
    f0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```


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": "EF12345678901234567890GH",

      // Identificatore di revoca: CBOR bstr effettivo, 16 byte/128 bit.
      // Rappresentato qui come 32 caratteri esadecimali per una migliore leggibilità.
      "rid": "4a8d9c11223344556677889 9aabbccdd",

      // 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":
  "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

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
```