REGULAMENTUL DELEGAT (UE) 2026/1436 AL COMISIEI

din 1 iulie 2026

de completare a Directivei (UE) 2024/2841 a Parlamentului European și a Consiliului în ceea ce privește stabilirea codului QR de pe versiunea fizică a cardului european pentru dizabilitate și stabilirea codului QR și a unor specificații tehnice comune care să asigure securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, precum și a aspectelor legate de interoperabilitate

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva (UE) 2024/2841 a Parlamentului European și a Consiliului din 23 octombrie 2024 de instituire a cardului european pentru dizabilitate și a cardului european de parcare pentru persoanele cu dizabilități ([1]), în special articolul 7 alineatul (7) și articolul 8 alineatul (7),

întrucât:

(1) Directiva (UE) 2024/2841 stabilește normele care reglementează emiterea cardului european pentru dizabilitate și a cardului european de parcare pentru persoanele cu dizabilități, precum și modelele comune pentru aceste carduri. În conformitate cu articolul 7 alineatul (2) și cu articolul 8 alineatul (2) din Directiva (UE) 2024/2841, cardurile europene pentru dizabilitate și cardurile europene de parcare pentru persoanele cu dizabilități emise de statele membre trebuie să fie recunoscute reciproc în toate statele membre.

(2) Delegările de competență prevăzute la articolul 7 alineatul (7) și la articolul 8 alineatul (7) din Directiva (UE) 2024/2841 au același scop, și anume prevenirea și combaterea fraudei, securitatea versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități, inclusiv prin măsuri de securitate adecvate pentru datele cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([2]), precum și asigurarea interoperabilității. Întrucât obiectul și obiectivele delegărilor de competență coincid în mare măsură, este oportun să se stabilească norme de completare a Directivei (UE) 2024/2841 în ceea ce privește aspectele respective într-un singur act delegat.

(3) Directiva (UE) 2024/2841 prevede ca versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități să conțină un cod QR, ca o caracteristică digitală de ultimă generație care utilizează mijloace electronice pentru a preveni și a combate frauda. Ca atare, codurile QR sunt o caracteristică digitală obligatorie care trebuie imprimată pe toate cardurile fizice. Pentru a asigura o abordare uniformă în ceea ce privește crearea și utilizarea codurilor QR de către statele membre, Comisia ar trebui să adopte specificații tehnice pentru stabilirea codurilor QR, inclusiv a conținutului acestora.

(4) Cardul european de parcare pentru persoanele cu dizabilități va înlocui toate cardurile de parcare existente pentru persoanele cu dizabilități emise în conformitate cu Recomandarea 98/376/CE a Consiliului ([3]). Recomandarea respectivă nu a fost actualizată pentru a reflecta evoluțiile în domeniul tehnologiei și al digitalizării, iar statele membre s-au confruntat cu probleme legate de fraudă și falsificare. Prin urmare, este necesar să se stabilească funcționalitățile care asigură securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, care să țină seama de particularitățile acestuia, cum ar fi faptul că se află de obicei în spatele parbrizului vehiculului.

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

([2]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Recomandarea 98/376/CE a Consiliului din 4 iunie 1998 privind un permis de parcare pentru persoane cu handicap (JO L 167, 12.6.1998, p. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Ar trebui introduse specificații tehnice comune obligatorii pentru a asigura securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități. Imprimarea cardului pe un material adecvat, cum ar fi policarbonatul, cu ajutorul unui element de difracție cu imagine optic variabilă, ar proteja în mod eficient împotriva falsificării și a fraudei. Modelele anti-scanare ar spori și mai mult securitatea, permițând detectarea duplicării cardului, deoarece acestea ar trebui să conțină un text ascuns sau un model care ar apărea atunci când cardul este fotocopiat sau scanat. Aceste caracteristici trebuie aplicate fără a afecta formatul versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități prevăzut în anexa II la Directiva (UE) 2024/2841, inclusiv aspectul vizual al cardului.

(6) Pe lângă codul QR și alte specificații tehnice obligatorii stabilite prin prezentul regulament, statele membre ar trebui să aibă posibilitatea de a integra elemente de securitate digitale sau fizice opționale pe baza specificațiilor tehnice comune prevăzute în prezentul regulament, în versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități, în vederea sporirii securității acestuia. În cazul în care caracteristicile digitale opționale conțin mai multe date cu caracter personal decât cele prevăzute în versiunile fizice ale cardurilor, în conformitate cu punctul 3 litera (b) din anexa II la Directiva (UE) 2024/2841, accesul la astfel de date trebuie limitat la autoritățile publice ale statelor membre emitente și numai la utilizatorii autorizați. Pentru a menține un cadru armonizat pentru elementele de securitate în toate statele membre, lista elementelor opționale ar trebui să fie exhaustivă. În plus, statele membre ar trebui să se asigure că integrarea unuia sau mai multor elemente de securitate digitale sau fizice opționale nu afectează recunoașterea cardurilor valabile din alte state membre și nu compromite interoperabilitatea și funcționalitatea specificațiilor tehnice obligatorii.

(7) Versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități poate conține un cip de identificare prin radiofrecvență (RFID) ca element de securitate digital opțional. RFID utilizează unde electromagnetice sau un cuplaj de câmp reactiv în porțiunea de frecvențe radio a spectrului pentru comunicarea bidirecțională cu o etichetă printr-o serie de dispozitive de modulare și codare pentru a citi în mod univoc identitatea unei etichete de radiofrecvență sau alte date stocate pe etichetă ([4]). Cipurile RFID pot consolida protecția împotriva falsificării și a manipulării frauduloase prin stocarea sau transmiterea în condiții de siguranță a datelor referitoare la card. Versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități poate conține, de asemenea, cerneală optic variabilă sau cerneală în culori schimbătoare. Aceste tipuri de cerneală oferă o protecție adecvată împotriva copierii și a manipulării frauduloase a cardului fără a fi necesară personalizarea. Pentru a se asigura că datele cardului sunt securizate în mod corespunzător împotriva tentativelor de contrafacere și falsificare, textul câmpurilor de date poate fi integrat în materialul de bază al cardului utilizând tehnologia de gravare cu laser. Elementele de securitate fizice, indiferent dacă sunt stabilite ca obligatorii sau opționale în prezentul regulament, care nu sunt vizibile sau care devin vizibile în urma anumitor manipulări, nu contravin formatului cardului european de parcare pentru persoanele cu dizabilități prevăzut în anexa II la Directiva (UE) 2024/2841.

(8) Progresele tehnologice, sistemele de verificare a parcărilor și riscurile de securitate evoluează în permanență. Tehnologia de ultimă generație se dezvoltă, iar utilizarea cardului european pentru dizabilitate și a cardului european de parcare pentru persoanele cu dizabilități evoluează, fiind determinată atât de feedbackul din partea utilizatorilor, cât și de progresul tehnologic, la fel ca și tehnicile de fraudă și falsificare, ceea ce duce la apariția unor noi provocări în materie de securitate. Prin urmare, noile soluții tehnologice, inclusiv cele legate de verificarea parcărilor, precum și nevoile în materie de securitate și de prevenire a fraudei ar putea necesita modificări ale arhitecturii de securitate și antifraudă a cardurilor, inclusiv prin actualizarea clasificării caracteristicilor digitale ca fiind obligatorii sau opționale. În funcție de evoluțiile tehnologice, acest lucru ar putea necesita actualizarea prezentului regulament.

(9) Pentru a se asigura că versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități pot fi utilizate fără sincope în toate statele membre, este necesar să se garanteze interoperabilitatea caracteristicilor digitale de pe cardurile fizice, în special a codurilor QR. Interoperabilitatea ar trebui să permită verificarea autenticității și a valabilității versiunilor fizice ale cardurilor de către verificatorii de carduri – orice persoană fizică sau juridică ce verifică valabilitatea și autenticitatea versiunilor fizice ale cardurilor, de exemplu prin intermediul unei aplicații de verificare. În acest scop, este necesar să se stabilească dispoziții privind aspectele legate de interoperabilitate, astfel încât să se permită efectuarea în mod coerent și fiabil a verificărilor transfrontaliere ale versiunilor fizice ale cardurilor.

([4]) Recomandarea 2009/387/CE a Comisiei din 12 mai 2009 privind aplicarea principiilor de respectare a vieții private și protecție a datelor în aplicațiile bazate pe identificarea prin radiofrecvență (JO L 122, 16.5.2009, p. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) Pentru a asigura integritatea și originea datelor conținute în codurile QR de pe versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități, datele respective ar trebui sigilate cu un sigiliu electronic calificat, astfel cum este definit la articolul 3 punctul 27 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([5]). Codul QR confirmă autenticitatea și valabilitatea cardului fizic, atunci când este verificat prin comparație cu parametrii de verificare, și nu ar trebui să ateste în sine statutul de persoană cu dizabilități sau dreptul la servicii specifice bazate pe o dizabilitate.

(11) Pentru a facilita interoperabilitatea și instituirea unui sistem fiabil și securizat de verificare a versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități în întreaga Uniune, ar trebui instituite mecanisme de notificare și publicare a informațiilor. În acest sens și pentru a permite verificarea faptului că versiunile fizice ale cardurilor sunt emise de o autoritate competentă sau de un organism competent, statele membre ar trebui să furnizeze informațiile necesare pentru procesul de verificare, în special informațiile necesare pentru verificarea sigiliului electronic calificat. Prin urmare, statele membre ar trebui să aibă obligația de a notifica Comisiei autoritățile sau organismele competente responsabile cu emiterea versiunilor fizice ale cardurilor (emitenții de carduri), precum și informațiile administrative și tehnice relevante referitoare la acestea. Informațiile care trebuie notificate Comisiei ar trebui să se limiteze la ceea ce este necesar pentru a institui mecanisme interoperabile de verificare a valabilității și autenticității versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități. Comisia ar trebui să asigure accesul publicului la aceste informații.

(12) În plus, în cazul revocării cardului, informațiile cu privire la revocarea cardului ar trebui să fie puse la dispoziție cu promptitudine pentru a permite verificatorilor de carduri să verifice valabilitatea cardului. În acest scop, emitenții de carduri ar trebui să mențină și să publice în timp util liste care să conțină informații privind statutul de revocat al tuturor cardurilor pe care le-au revocat înainte de datele lor de expirare (liste de revocare). O astfel de publicare ar trebui să respecte viața privată și să protejeze datele cu caracter personal ale titularilor de carduri. În plus, listele de revocare nu ar trebui să conțină alte date cu caracter personal decât identificatorii unici de revocare și ar trebui să fie publicate la un identificator uniform de resurse (URI) specific, în conformitate cu specificațiile tehnice, pentru a asigura verificarea interoperabilă.

(13) Pentru a citi codul QR și a verifica autenticitatea și valabilitatea versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități, pot fi utilizate aplicații de verificare personalizate la nivel național. Comisia poate sprijini acest proces prin furnizarea unui cod sursă comun de referință în scopul citirii datelor conținute în codurile QR și pentru efectuarea principalelor etape ale procesului de verificare, care poate servi drept bază pentru aplicațiile de verificare din statele membre. Toate aplicațiile de verificare ar trebui să aplice aceeași logică de verificare a lanțului de încredere în raport cu aceeași infrastructură de asigurare a încrederii, permițând astfel citirea datelor codificate în carduri de către statul membru emitent. În plus, anexa I la Directiva (UE) 2019/882 a Parlamentului European și a Consiliului ([6]) stabilește cerințele de accesibilitate care trebuie respectate de statele membre, după caz.

(14) Recunoscând caracterul dinamic al progreselor tehnologice și al amenințărilor cibernetice în continuă evoluție, Uniunea se angajează să se asigure că mecanismele criptografice utilizate în cadrul său de reglementare rămân eficace și sigure. Având în vedere acest angajament, este important să se adopte standarde criptografice aprobate de Grupul european pentru certificarea securității cibernetice și diseminate prin intermediul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA).

(15) Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal în temeiul prezentului regulament. În special, verificarea codurilor QR de pe versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități implică prelucrarea datelor cu caracter personal. Prin urmare, ar trebui stabilite garanții adecvate în materie de protecție a datelor pentru a asigura protecția datelor cu caracter personal conținute în codurile QR în conformitate cu Regulamentul (UE) 2016/679, după caz. Măsurile generale de securitate prevăzute în prezentul regulament ar trebui, de asemenea, să asigure protecția datelor cu caracter personal conținute în codurile QR. În plus, datele cu caracter personal conținute în codurile QR ar trebui să se limiteze la ceea ce este strict necesar în sensul prezentului regulament. Mai mult, păstrarea datelor după finalizarea verificării ar trebui interzisă. De asemenea, este necesar să se asigure securitatea adecvată a listelor de revocare.

([5]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Directiva (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor (JO L 151, 7.6.2019, p. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) În conformitate cu articolul 14 alineatul (4) din Directiva (UE) 2024/2841, la pregătirea prezentului regulament, Comisia a consultat persoane cu dizabilități și organizațiile reprezentative ale acestora, precum și experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([7]).

(17) Cardul european pentru dizabilitate și cardul european de parcare pentru persoanele cu dizabilități constituie un serviciu public digital transeuropean în sensul Regulamentului (UE) 2024/903 al Parlamentului European și al Consiliului ([8]). În consecință, a fost efectuată o evaluare a interoperabilității, iar raportul rezultat urmează să fie publicat pe portalul Europa interoperabilă menționat la articolul 8 din Regulamentul (UE) 2024/903.

(18) Autoritatea Europeană pentru Protecția Datelor a fost consultată cu privire la prezentul regulament în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([9]) și a emis un aviz la 12 mai 2026,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect și domeniu de aplicare

Prezentul regulament stabilește normele de completare a Directivei (UE) 2024/2841 în ceea ce privește:

(a) stabilirea codului QR pentru versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități, inclusiv a unor măsuri de securitate adecvate pentru datele cu caracter personal;

(b) stabilirea unor specificații tehnice comune obligatorii și opționale care să asigure securitatea versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități;

(c) stabilirea cerințelor de interoperabilitate necesare pentru a se asigura că codurile QR de pe versiunile fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități, emise într-un stat membru, pot fi citite și verificate în mod fiabil într-un alt stat membru.

Articolul 2

Codul QR de pe versiunea fizică a cardului european pentru dizabilitate

Specificațiile pentru codul QR care trebuie să apară pe versiunea fizică a cardului european pentru dizabilitate sunt cele prevăzute în anexa I.

Articolul 3

Codul QR de pe versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități

Specificațiile pentru codul QR care trebuie să apară pe versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități sunt cele prevăzute în anexa II.

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

([8]) Regulamentul (UE) 2024/903 al Parlamentului European și al Consiliului din 13 martie 2024 de stabilire a unor măsuri pentru un nivel ridicat de interoperabilitate a sectorului public în întreaga Uniune (Regulamentul privind Europa interoperabilă) (JO L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Articolul 4

Specificații tehnice comune obligatorii pentru cardul european de parcare pentru persoanele cu dizabilități

(1) Versiunile fizice ale cardului european de parcare pentru persoanele cu dizabilități respectă următoarele specificații tehnice comune:

(a) sunt fabricate dintr-un material care protejează împotriva delaminării și care are capacitatea de a respecta cerințele prevăzute în anexa II la Directiva (UE) 2024/2841 și alte specificații tehnice comune obligatorii prevăzute la prezentul articol;

(b) conțin un element de difracție cu imagine optic variabilă, ca element al unei structuri stratificate, care devine vizibil atunci când cardul este privit dintr-un anumit unghi;

(c) sunt realizate utilizând un model anti-scanare care devine vizibil atunci când un card este fotocopiat sau scanat.

(2) Elementul de difracție cu imagine optic variabilă menționat la alineatul (1) litera (b) apare pe partea din față a versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, deasupra unuia sau mai multor câmpuri de date din partea stângă. El are o înălțime de aproximativ 20 mm și o lățime de aproximativ 20 mm. Imaginea afișată pe element constă într-o hartă stilizată a statului membru emitent sau codul distinctiv al statului membru emitent, înconjurat de cercul de 12 stele care simbolizează Uniunea.

(3) Modelul anti-scanare menționat la alineatul (1) litera (c) se amplasează pe partea din față a versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități, deasupra câmpurilor de date din partea stângă și/sau din partea dreaptă, în afara codului QR și a zonei sale liniștite. El conține un text sau un model ascuns, care apare atunci când cardul este fotocopiat sau scanat. În cazul în care modelul anti-scanare conține un text ascuns, acesta constă în cuvintele „COPY” (copie) sau „VOID” (nul) și o traducere a acestora în una sau mai multe limbi oficiale ale statului membru emitent. În cazul în care modelul anti-scanare conține un model ascuns, acesta este compus din linii orizontale sau verticale.

Articolul 5

Specificații și caracteristici tehnice opționale pentru securitatea cardului european de parcare pentru persoanele cu dizabilități

(1) Pe lângă specificațiile tehnice comune obligatorii menționate la articolul 4, statele membre pot aplica numai specificațiile și caracteristicile tehnice opționale prevăzute la prezentul articol.

(2) Versiunile fizice ale cardului european de parcare pentru persoanele cu dizabilități pot conține un cip de identificare prin radiofrecvență (RFID). Cipul RFID previne și combate frauda prin mijloace electronice și servește drept mijloc suplimentar de verificare a autenticității și/sau a valabilității unei versiuni fizice a cardului european de parcare pentru persoanele cu dizabilități la nivel național. Cipul RFID nu afectează funcționarea codului QR de pe card.

(3) Orice cip RFID menționat la alineatul (2) respectă următoarele specificații:

(a) este pasiv;

(b) este integrat fizic în corpul cardului, în partea dreaptă de pe fața cardului;

(c) este asociat logic cu înregistrarea codului QR și conține același identificator de revocare (RID) ca cel codificat în codul QR;

(d) caracteristica RFID trebuie să permită citirea la aproximativ un metru sau mai mult atunci când este necesară pentru utilizarea operațională, dar nu trebuie să fie proiectată pentru citirea fiabilă la peste cinci metri în condițiile de încercare de referință;

(e) după emiterea cardului, accesul pentru scriere la cipul RFID sau la zona de date relevantă a acestuia este împiedicat sau controlat în alt mod de către autoritatea emitentă;

(f) este proiectat și configurat astfel încât să se reducă la minimum riscul clonării, al substituirii, al modificării neautorizate și al rescrierii neautorizate;

(g) respectă cerințele Directivei 2014/53/UE a Parlamentului European și a Consiliului ([10]);

(h) pe lângă RID menționat la litera (c), cipul RFID poate stoca numai unul sau mai multe dintre următoarele elemente:

(i) date codificate în codul QR al versiunii fizice a cardului european de parcare pentru persoanele cu dizabilități;

(ii) numărul (numerele) de înmatriculare al(e) vehiculului;

(iii) date de verificare criptografică.

(4) Partea din față a versiunilor fizice ale cardului european de parcare pentru persoanele cu dizabilități poate conține una sau mai multe dintre următoarele caracteristici:

(a) simbolul scaunului cu rotile în partea stângă sau cuvintele „European Parking Card for persons with disabilities” în limba engleză și în una sau mai multe limbi oficiale ale statului membru emitent în partea dreaptă, imprimate cu cerneală optic variabilă sau cu cerneală în culori schimbătoare, care prezintă culori diferite atunci când este privită din unghiuri diferite;

(b) utilizarea tehnologiei de gravare cu laser care pătrunde în straturile cardului pentru a imprima textul în câmpurile de date.

(5) Introducerea specificațiilor și caracteristicilor tehnice opționale menționate la prezentul articol nu afectează recunoașterea, în statul membru care a introdus astfel de caracteristici pentru cardurile pe care le emite, a cardurilor valabile emise în alte state membre.

Articolul 6

Aspecte legate de interoperabilitate

(1) Informațiile incluse în codul QR se sigilează cu un sigiliu electronic calificat în sensul articolului 3 punctul 27 din Regulamentul (UE) nr. 910/2014.

(2) Fiecare stat membru comunică Comisiei informații cu privire la autoritățile sau organismele competente responsabile cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități („emitenții de carduri”), precum și toate actualizările ulterioare ale informațiilor respective în conformitate cu anexa III. Comisia asigură accesul publicului la aceste informații.

(3) Emitenții de carduri mențin și publică la un identificator uniform de resurse care este notificat Comisiei liste de revocare actualizate care conțin informații privind statutul de revocat al tuturor cardurilor pe care le-au revocat în conformitate cu specificațiile tehnice prevăzute în anexa IV. Informațiile privind revocarea se publică în termen de 24 de ore de la revocarea respectivă.

(4) Statele membre pot utiliza aplicații de verificare pentru a verifica autenticitatea și valabilitatea versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități.

(5) În cazul în care statele membre utilizează aplicații de verificare pentru a verifica autenticitatea și valabilitatea versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități, aceste aplicații trebuie să poată verifica autenticitatea și valabilitatea unui card prin verificarea sigiliului electronic și a statutului de revocat al cardului. Aceste aplicații de verificare citesc și prezintă o reprezentare vizuală a datelor cu caracter personal codificate în codul QR al cardului, astfel cum se prevede în anexele I și II, pentru a permite o comparație cu datele vizibile în câmpurile de date corespunzătoare de pe card, precum și o indicație privind statutul valabilității cardului.

([10]) Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Articolul 7

Măsuri de securitate pentru protecția datelor cu caracter personal

(1) Datele cu caracter personal conținute în codurile QR de pe versiunile fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități se limitează la ceea ce este strict necesar pentru a verifica autenticitatea și valabilitatea cardurilor, astfel cum se prevede în anexele I și II.

(2) După finalizarea verificării autenticității și a valabilității unei versiuni fizice a cardului european pentru dizabilitate sau a cardului european de parcare pentru persoanele cu dizabilități de către verificatorii de carduri, datele conținute în codurile QR nu sunt păstrate de verificatorii de carduri.

(3) Verificarea unui cod QR de pe o versiune fizică a cardului european pentru dizabilitate sau a cardului european de parcare pentru persoanele cu dizabilități nu are ca rezultat notificarea autorității competente sau a organismului responsabil cu emiterea cardului cu privire la verificarea respectivă.

(4) Informațiile incluse într-o listă de revocare publicată în conformitate cu articolul 6 alineatul (3) se limitează la identificatorul de revocare al cardurilor revocate.

(5) Autoritatea sau organismul responsabil cu publicarea listelor de revocare în conformitate cu articolul 6 alineatul (3) se asigură că se aplică măsuri de securitate tehnice și organizatorice adecvate pentru prelucrarea datelor cu caracter personal conținute în listele de revocare.

(6) În cazul în care un stat membru decide să integreze un cip RFID în versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități, alineatele (2)-(3) se aplică prelucrării datelor cu caracter personal conținute în cipul respectiv. Datele cu caracter personal conținute în cipul RFID se limitează la ceea ce este strict necesar pentru a verifica autenticitatea și/sau valabilitatea cardurilor, astfel cum se prevede la articolul 5 alineatul (3).

În cazul în care un stat membru stochează în cipul RFID datele cu caracter personal menționate la articolul 5 care nu sunt prevăzute în versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități, astfel cum se prevede în anexa II la Directiva (UE) 2024/2841, accesul la aceste date este limitat la autoritățile publice ale statului membru emitent și numai la utilizatorii autorizați.

Articolul 8

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 1 iulie 2026.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

SPECIFICAȚIILE CODULUI QR PENTRU VERSIUNEA FIZICĂ A CARDULUI EUROPEAN PENTRU DIZABILITATE

1. **Formatul codului QR pentru versiunea fizică a cardului european pentru dizabilitate (EDC)**

(a) **Formatul Modelului 2 al codului QR**, în conformitate cu specificațiile internaționale ale codului QR ISO/IEC 18004:2024 sau echivalent.

(b) **Nivelul M de corectare a erorilor** (redundanță 15 %) care asigură rezistența la zgârieturi sau la deteriorarea parțială a unui cod QR imprimat.

(c) **Mod de codificare**: Sarcina utilă QR constă în structura combinată issuerSigned Concise Binary Object Representation (reprezentare concisă a obiectelor binare – CBOR) și obiectul de semnătură issuerAuth COSE_Sign1 corespunzător, astfel cum este definit în CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR) (COSE, RFC 9052 secțiunile 3.1, 4.2 și 4.4), urmând modelul de date mDOC pentru elementele issuerSigned, dar adaptat pentru utilizarea statică a cardului fizic. IssuerAuth este un obiect COSE_Sign1 cu alg = ES256 și un antet protejat care conține x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256].

(d) Înainte de codificarea codului QR, obiectul CBOR/COSE combinat se **comprimă utilizând formatul zlib** (RFC 1950, secțiunea 2.2) cu algoritmul de **deflatare** (RFC 1951 secțiunile 3.2 și 4). Seria de octeți comprimați rezultată se codifică în **modul de octeți cu cod QR**, asigurând sprijin deplin pentru sarcinile utile binare CBOR/COSE și interoperabilitatea scanerului.

Pentru toate câmpurile de text incluse în sarcina utilă QR, emitenții trebuie să codifice caracterele ca Unicode UTF-8 în șirurile de text CBOR. Transliterația nu se aplică datelor privind sarcina utilă semnate. Din motive de interoperabilitate, emitenții aplică formularul de normalizare Unicode C (NFC) tuturor câmpurilor textuale înainte de a semna.

(e) **Prefix:** Șirul QR al EDC începe cu „ED1:MDOC:”. Această formulă identifică tipul cardului și profilul de codificare. Prefixele respectă regimul de litere mici și mari și trebuie să fie prezente. Prefixele necunoscute sau neacceptate conduc la respingere. Prefixul și sarcina utilă comprimată se codifică sub forma unui singur segment de date în modul de octeți în codul QR.

(f) **Dimensiunea minimă a modulului ≥ 0,25 mm** pentru a asigura lizibilitatea pe cardurile imprimate.

(g) **Versiunea maximă 20**; cu până la 97 × 97 de pe fiecare parte.

2. **Specificații privind generarea semnăturii EDC**

Sigiliul electronic calificat (QSeal) utilizat pentru sigilarea codurilor QR ale EDC asigură faptul că datele codificate provin de la autoritatea emitentă autorizată și nu au fost modificate.

(a) **Algoritmul de semnătură**: Algoritmul semnăturii este ES256 [algoritmul de semnătură digitală bazat pe curbe eliptice (*Elliptic Curve Digital Signature Algorithm* – ECDSA) cu SHA-256 utilizând curba P-256], astfel cum este definit în RFC 9053 (secțiunea 2.1); în COSE, algoritmul este identificat prin parametrul antetului alg din RFC 9052 (secțiunea 3.1).

(b) **Cheia de semnătură**: Sarcina utilă a codului QR se semnează utilizând cheia privată corespunzătoare unui certificat calificat pentru semnături electronice (QSealC).

(c) **Structura COSE**: Containerul cu semnătură este un obiect COSE_Sign1. Antetul protejat include alg (ES256) și x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256]. Verificarea se bazează pe utilizarea valorii x5t pentru a localiza certificatul corespunzător în registrul de încredere stocat local în memoria cache a verificatorului, creat pe baza informațiilor din lista sigură, și apoi validează lanțul de certificate și statutul certificatului în conformitate cu cadrul de încredere eIDAS.

(d) **Standardul de semnătură**: Sarcina utilă a codului QR se semnează ca obiect COSE_Sign1 în conformitate cu RFC 9052 (secțiunea 4), CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR). Obiectul COSE_Sign1 se stochează în issuerAuth și se codifică fără eticheta CBOR pentru COSE_Sign1. Câmpul sarcinii utile al obiectului COSE_Sign1 se detașează și se codifică drept CBOR null. Pentru generarea și verificarea semnăturii, sarcina utilă externă este structura CBOR codificată determinist, care conține valoarea docType și valoarea issuerSigned din harta CBOR de prim nivel.

(e) **Algoritmul hash**: SHA-256 se utilizează ca parte a ES256 pentru generarea semnăturii și verificarea integrității.

(f) **Codificare**: Sarcina utilă se codifică utilizând CBOR (RFC 8949, secțiunea 4.2), astfel cum se prevede în specificațiile COSE și mDOC, asigurând codificarea și reproductibilitatea datelor semnate.

3. **Specificații de imprimare**

(a) **Zonă liniștită**: O margine liberă de **4 module** trebuie să înconjoare codul QR pe toate laturile, fără niciun fel de text imprimat, model sau fundal.

(b) **Contrast**: Codul QR se imprimă pe fond alb, cu un raport de contrast de cel puțin **4:1**, pentru a asigura o lizibilitate ridicată în condiții de iluminare variabile.

(c) Codul QR se imprimă utilizând culoarea definită în anexa I la Directiva (UE) 2024/2841 care asigură contrastul maxim.

(d) **Amplasare și dimensiune**: Codul QR, inclusiv zona liniștită, este de 26,25 mm × 26,25 mm, amplasat pe versoul cardului, în colțul din dreapta-jos. Codul QR este versiunea maximă 20 (97 × 97 de module), cu o dimensiune a modulului de 0,25 mm sau mai mare.

Codul QR, inclusiv zona sa liniștită, este amplasat la cel puțin 5 mm față de marginea din dreapta și la cel puțin 5 mm față de marginea inferioară a cardului.

4. **Datele din codul QR al EDC**

Codul QR conține un set de date minim, verificabil offline, în conformitate cu principiul reducerii la minimum a datelor prevăzut la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Structura sarcinii utile este următoarea:

(a) Atributele cardului sunt codificate în CBOR în cadrul unui obiect issuerSigned.

(b) Structura este sigilată și semnată de QSeal al autorității emitente ca issuerAuth (COSE_Sign1, ES256, inclusiv x5t, parametrul antetului hash al certificatului COSE X.509).

(c) Obiectul CBOR/COSE rezultat se comprimă în conformitate cu punctul 1 litera (d) din prezenta anexă. Sarcina utilă a codului QR constă în prefixul „ED1:MDOC:", urmat de seria de octeți comprimați rezultată, iar sarcina utilă completă se codifică utilizând modul de octeți sub forma unui singur segment de date în codul QR.

Conținutul datelor constă într-un subset de date vizibile din câmpurile de pe fața cardului enumerate în anexa I la Directiva (UE) 2024/2841 (nume, prenume, numărul de serie al cardului, data expirării), împreună cu identificatorul de revocare, semnătura electronică și informații privind schema.

Semnătura electronică conține:

(i) issuerAuth – un obiect COSE_Sign1 semnat cu **cheia privată QSealC** a autorității emitente;

(ii) antet protejat care include alg = ES256 (algoritm de semnătură) și x5t (parametrul antetului hash al certificatului COSE X.509).

5. **Date opționale**

În codul QR nu se includ date opționale.

6. **Identificatorul de revocare (RID)**

Pe lângă numărul de serie vizibil al cardului, codul QR include un identificator de revocare dedicat (RID).

RID se utilizează pentru determinarea statutului de revocat și pentru gestionarea listei de revocare. RID nu se imprimă pe card și nu se afișează pentru verificatorii de carduri.

6.1. *Cerințe aplicabile RID*

RID:

(a) se include în sarcina utilă QR semnată;

(b) este unic cel puțin în cadrul domeniului de emitere al autorității emitente;

(c) nu se imprimă pe card și nu este destinat să fie lizibil pentru om;

(d) nu dezvăluie date cu caracter personal și nu are o semnificație directă;

(e) nu se poate deduce direct din numărul de serie vizibil al cardului; și

(f) este legat criptografic de sarcina utilă QR prin sigiliul electronic calificat.

6.2. *Formatul și dimensiunea RID*

RID se codifică sub formă de șir de octeți CBOR (bstr). RID are o lungime de 16 octeți (128 de biți).

RID se generează de autoritatea emitentă utilizând o metodă aflată sub controlul său care asigură o entropie și o rezistență suficiente la ghicire sau enumerare.

6.3. *Liste de revocare*

Listele de revocare publicate în scopul verificării fac trimitere numai la RID-ul cardurilor revocate. Numerele de serie ale cardurilor nu se publică în listele de revocare.

7. **Sarcina utilă CBOR (în interiorul codului QR) a EDC**

Numai următoarele date se includ în sarcina utilă QR, în concordanță cu câmpurile de date ale EDC vizibile prevăzute în anexa I la Directiva (UE) 2024/2841.

Conținuturile de nivel superior:

(a) docType = „eu.edc”

(b) issuerSigned.nameSpaces.„eu.edc” cu atributele prezentate în tabelul de mai jos

(c) issuerAuth = COSE_Sign1 (QSeal)

Câmp	Calea mDOC	Tip/Format
Versiunea schemei de date	issuerSigned.nameSpaces.„eu.edc”.ver	Șir (de exemplu, „1.0”)
Tipul cardului: EDC	docType	Enum („eu.edc”)
Numărul de serie al cardului	issuerSigned.nameSpaces.„eu.edc”.sub	Șir
Identificator de revocare	issuerSigned.nameSpaces.„eu.edc”.rid	CBOR bstr (16 octeți)
Prenumele titularului cardului	issuerSigned.nameSpaces.„eu.edc”.givenName	Șir de text Unicode (UTF-8)
Numele titularului cardului	issuerSigned.nameSpaces.„eu.edc”.familyName	Șir de text Unicode (UTF-8)
Data expirării cardului	issuerSigned.nameSpaces.„eu.edc”.exp	Eticheta CBOR 1004, astfel cum este definită în RFC 8943 (secțiunea 2.1), conținând un șir de text UTF-8 care reprezintă o dată completă conform RFC 3339 în format AAAA-LL-ZZ.

Semnătura electronică este stocată în issuerAuth (un obiect COSE_Sign1). Lanțul de certificate nu se integrează în sarcina utilă a codului QR; în schimb, antetul protejat COSE include x5t, o amprentă a certificatului utilizată pentru a localiza QSealC corespunzător în registrul de încredere stocat în memoria cache a verificatorului.

8. **Exemplu de sarcină utilă a codului QR al EDC: reprezentare logică comentată de tipul JavaScript Object Notation**

Următorul exemplu este o reprezentare JavaScript Object Notation (JSON – notarea obiectelor în JavaScript) lizibilă pentru om a vizualizării logice a EDC. În practică, această structură nu trebuie să fie lizibilă pentru om, deoarece:

(a) este codificată în CBOR (RFC 8949, secțiunea 3);

(b) este semnată utilizând structura COSE_Sign1 neetichetată cu o sarcină utilă detașată (RFC 9052, secțiunea 4.),

(c) include data expirării ca etichetă CBOR 1004, valoarea datei complete, în conformitate cu RFC 8943 (secțiunea 2.1);

(d) include parametrul antetului protejat x5t în conformitate cu RFC 9360, utilizând SHA-256 pe entitatea finală QSealC codificată în DER; și

(e) este comprimată și prefixată cu șirul ED1:MDOC: înainte de a fi codificată în codul QR.

```
{
  // Numai vizualizare logică lizibilă pentru om a EDC, de tip JSON.
  // Sarcina utilă efectivă a codului QR este în format CBOR determinist, nu JSON.
  „docType”: „eu.edc”, // acreditare EDC. Valoarea docType este inclusă, împreună cu
     //issuerSigned, în sarcina utilă externă COSE_Sign1.

  „issuerSigned”: {
     // Date protejate de issuerAuth; utilizate ca sarcină utilă detașată.
     // Pentru generarea și verificarea semnăturii, sarcina utilă externă detașată acoperă atât
     // docType, cât și issuerSigned.
     „nameSpaces”: {
       „eu.edc”: {
         „ver”: „1.0”, // versiunea profilului/schemei codului QR

         // Numărul de serie al cardului; definit de emitent, maximum 24 de caractere.
         „sub”: „AB1234567890123456789OCD”,

         // Identificator de revocare: CBOR bstr efectiv, 16 octeți/128 de biți.
         // reprezentat aici sub formă de 32 de caractere hexadecimale pentru lizibilitate.
         „rid”: „9f8c4d3a7b1e2c0a55aa33ff8899ee11”,

         „givenName”: „Ann”, // prenumele imprimat pe EDC
         „familyName”: „Other”, // numele de familie imprimat pe EDC

         // Codificarea CBOR efectivă utilizează eticheta 1004 pentru data completă conform RFC 3339.
         „exp”: „31-12-2030”
       }
     }
  },

  „issuerAuth”: {
    // Forma efectivă: COSE_Sign1 neetichetată, nu un obiect JSON.
    „type”: „COSE_Sign1”,
```

„tagged”: fals, // codificat fără eticheta CBOR COSE_Sign1
„payload”: „detached”, // câmpul sarcinii utile COSE este CBOR null

„protectedHeader”: {
// alg: ES256; parametrul antetului COSE echivalent 1 = -7.
„alg”: „ES256”,

// x5t: amprenta certificatului; parametrul antetului COSE 34.
„x5t”: {
„hashAlg”: „SHA-256”, // valoarea hash COSE echivalentă -16

// hash SHA-256 al entității finale QSealC codificate în DER.
// 32 de octeți reprezentați de 64 de caractere hexadecimale.
„hashValue”:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”
}
},

„unprotectedHeader”: {}, // gol în acest exemplu

// semnătură COSE ES256: 64 de octeți = 128 de caractere hexadecimale.
„signature”:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
f0123456789abcdef0123456789abcdef0123456789abcdef”
}
}

9. **Utilizarea mecanismelor criptografice**

Utilizarea mecanismelor criptografice în contextul prezentei anexe este în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

ANEXA II

SPECIFICAȚIILE CODULUI QR PENTRU VERSIUNEA FIZICĂ A CARDULUI EUROPEAN DE PARCARE PENTRU PERSOANELE CU DIZABILITĂȚI

1. **Formatul codului QR de pe versiunea fizică a cardului european de parcare pentru persoanele cu dizabilități (EPC)**

   (a) **Formatul Modelului 2 al codului QR**, în conformitate cu specificațiile internaționale ale codului QR ISO/IEC 18004:2024 sau echivalent.

   (b) **Nivelul M de corectare a erorilor** (redundanță 15 %) care asigură rezistența la zgârieturi sau la deteriorarea parțială a codului QR imprimat.

   (c) **Mod de codificare** :Sarcina utilă QR constă în structura combinată issuerSigned Concise Binary Object Representation (reprezentare concisă a obiectelor binare – CBOR) și obiectul de semnătură issuerAuth COSE_Sign1 corespunzător, astfel cum este definit în CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR) (COSE, RFC 9052 secțiunile 3.1, 4.2 și 4.4), urmând modelul de date mDOC pentru elementele issuerSigned, dar adaptat pentru utilizarea statică a cardului fizic. IssuerAuth este un obiect COSE_Sign1 cu alg = ES256 și un antet protejat care conține x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256].

   (d) Înainte de codificarea codului QR, obiectul CBOR/COSE combinat **se comprimă utilizând formatul zlib (RFC 1950, secțiunea 2.2) cu algoritmul de deflatare** (RFC 1951, secțiunile 3.2 și 4). Seria de octeți comprimați rezultată se codifică în **modul de octeți cu cod QR**, asigurând sprijin deplin pentru sarcinile utile binare CBOR/COSE și interoperabilitatea scanerului.

   Pentru toate câmpurile de text incluse în sarcina utilă QR, emitenții trebuie să codifice caracterele ca Unicode UTF-8 în șirurile de text CBOR. Transliterația nu se aplică datelor privind sarcina utilă semnate. Din motive de interoperabilitate, emitenții aplică formularul de normalizare Unicode C (NFC) tuturor câmpurilor textuale înainte de a semna.

   (e) **Prefix**: Șirul QR al EDC începe cu „EP1:MDOC:". Această formulă identifică tipul cardului și profilul de codificare. Prefixele respectă regimul de litere mici și mari și trebuie să fie prezente. Prefixele necunoscute sau neacceptate conduc la respingere. Prefixul și sarcina utilă comprimată se codifică sub forma unui singur segment de date în modul de octeți în codul QR.

   (f) **Dimensiunea minimă a modulului ≥ 0,35 mm** pentru a asigura lizibilitatea pe cardurile imprimate.

   (g) **Versiunea maximă 20**; cu până la 97 × 97 de module pe fiecare parte.

2. **Specificații privind generarea semnăturii EPC**

   Sigiliul electronic calificat (QSeal) utilizat pentru sigilarea codurilor QR ale EPC asigură faptul că datele codificate provin de la autoritatea emitentă autorizată și nu au fost modificate.

   (a) **Algoritmul de semnătură**: Algoritmul semnăturii este ES256 [ECDSA cu SHA-256 utilizând curba P-256], astfel cum este definit în RFC 9053 (secțiunea 2.1); în COSE, algoritmul este identificat prin parametrul antetului alg din RFC 9052 (secțiunea 3.1).

   (b) **Cheia de semnătură**: Sarcina utilă a codului QR se semnează utilizând cheia privată corespunzătoare unui certificat calificat pentru semnături electronice (QSealC).

   (c) **Structura COSE**: Containerul cu semnătură este un obiect COSE_Sign1. Antetul protejat include alg (ES256) și x5t [parametrul antetului hash al certificatului COSE X.509 definit în RFC 9360 (secțiunea 2); pentru interoperabilitate, algoritmul hash utilizat în x5t este SHA-256]. Verificarea se bazează pe utilizarea valorii x5t pentru a localiza certificatul corespunzător în registrul de încredere stocat local în memoria cache a verificatorului, creat pe baza informațiilor din lista sigură, și apoi validează lanțul de certificate și statutul certificatului în conformitate cu cadrul de încredere eIDAS.

   (d) **Standardul de semnătură**: Sarcina utilă a codului QR se semnează ca obiect COSE_Sign1 în conformitate cu RFC 9052 (secțiunea 4), CBOR Object Signing and Encryption (semnare și criptare de obiecte utilizând CBOR). Obiectul COSE_Sign1 se stochează în issuerAuth și se codifică fără eticheta CBOR pentru COSE_Sign1. Câmpul sarcinii utile al obiectului COSE_Sign1 se detașează și se codifică drept CBOR null. Pentru generarea și verificarea semnăturii, sarcina utilă externă este structura CBOR codificată în CBOR determinist, care conține valoarea docType și valoarea issuerSigned din harta CBOR de prim nivel.

(e) **Algoritmul hash**: SHA-256 se utilizează ca parte a ES256 pentru generarea semnăturii și verificarea integrității.

(f) **Codificare**: Sarcina utilă se codifică utilizând CBOR (RFC 8949, secțiunea 4.2), astfel cum se prevede în specificațiile COSE și mDOC, asigurând codificarea și reproductibilitatea datelor semnate.

3. **Specificații de imprimare**

(a) **Zonă liniștită**: O margine liberă de **4 module** trebuie să înconjoare codul QR pe toate laturile, fără niciun fel de text imprimat, model sau fundal.

(b) **Contrast**: Codul QR se imprimă pe fond alb, cu un raport de contrast de cel puțin **4:1**, pentru a asigura o lizibilitate ridicată în condiții de iluminare variabile.

(c) Codul QR se imprimă utilizând culoarea definită în anexa II la Directiva (UE) 2024/2841 care asigură contrastul maxim.

(d) **Amplasare și dimensiune**: Codul QR, inclusiv zona liniștită, este de **37 mm × 37 mm**, amplasat pe fața cardului, ușor în afara centrului către dreapta, spre marginea inferioară. Codul QR este versiunea maximă 20 (97 × 97 module), cu o dimensiune a modulului de 0,35 mm sau mai mare.

Codul QR, inclusiv zona sa liniștită, este amplasat la cel puțin 5 mm față de marginea inferioară a cardului.

4. **Datele din codul QR al EPC**

Codul QR conține un set de date minim, verificabil offline, în conformitate cu principiul reducerii la minimum a datelor cuprins la articolul 5 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Structura sarcinii utile este următoarea:

(a) Atributele cardului sunt codificate în CBOR în cadrul unui obiect issuerSigned.

(b) Această structură este sigilată și semnată de QSeal al autorității emitente ca issuerAuth (COSE_Sign1, ES256, inclusiv x5t, parametrul antetului hash al certificatului COSE X.509).

(c) Obiectul CBOR/COSE rezultat se comprimă în conformitate cu punctul 1 litera (d) din prezenta anexă. Sarcina utilă a codului QR constă în prefixul „EP1:MDOC:”, urmat de seria de octeți comprimați rezultată, iar sarcina utilă completă se codifică utilizând modul de octeți sub forma unui singur segment de date în codul QR.

Conținutul datelor constă într-un subset de date vizibile din câmpurile de pe fața cardului enumerate în anexa II la Directiva (UE) 2024/2841 (data expirării, numărul de serie al cardului), împreună cu identificatorul de revocare, semnătura electronică și informații privind schema.

Semnătura electronică conține:

(i) issuerAuth – un obiect COSE_Sign1 semnat cu **cheia privată QSealC** a autorității emitente;

(ii) antet protejat care include alg = ES256 (algoritm de semnătură) și x5t (parametrul antetului hash al certificatului COSE X.509).

5. **Date opționale**

În codul QR nu se includ date opționale.

6. **Identificatorul de revocare (RID)**

Identificatorul de revocare al EPC este conform cu punctul 6 din anexa I.

Listele de revocare pentru EPC-urile revocate fac trimitere numai la RID. Numerele de serie ale cardurilor nu se publică în listele de revocare.

7. **Sarcina utilă CBOR (în interiorul codului QR) a EPC**

În sarcina utilă QR se includ numai următoarele date, care sunt în concordanță cu câmpurile cardului EPC vizibile prevăzute în anexa II la Directiva (UE) 2024/2841:

Câmp	Calea mDOC	Tip/Format
Versiunea schemei de date	issuerSigned.nameSpaces.„eu.epc”.ver	Șir (de exemplu, „1.0”)
Tipul cardului: EPC	docType	Enum („eu.epc”)
Numărul de serie al cardului	issuerSigned.nameSpaces.„eu.epc”.sub	Șir
Identificator de revocare	issuerSigned.nameSpaces.„eu.epc”.rid	CBOR bstr (16 octeți)
Data expirării cardului	issuerSigned.nameSpaces.„eu.epc”.exp	Eticheta CBOR 1004, astfel cum este definită în RFC 8943 (secțiunea 2.1), conținând un șir de text UTF-8 care reprezintă o dată completă conform RFC 3339 în format AAAA-LL-ZZ.

Semnătura electronică se stochează în issuerAuth (un obiect COSE_Sign1). Lanțul de certificate nu se integrează în sarcina utilă a codului QR; în schimb, antetul protejat COSE include x5t, o amprentă a certificatului utilizată pentru a localiza QSealC corespunzător în registrul de încredere stocat în memoria cache a verificatorului.

8. **Exemplu de sarcină utilă a codului QR al EPC: reprezentare logică comentată de tipul JavaScript Object Notation**

Următorul exemplu este o reprezentare JavaScript Object Notation (JSON – notarea obiectelor în JavaScript) lizibilă pentru om a vizualizării logice a EPC. În practică, această structură nu trebuie să fie lizibilă pentru om, deoarece este:

(a) codificată în CBOR (RFC 8949, secțiunea 3);

(b) este semnată utilizând structura COSE_Sign1 neetichetată, cu o sarcină utilă detașată (RFC 9052, secțiunea 4.);

(c) include data expirării ca etichetă CBOR 1004, valoarea datei complete, în conformitate cu RFC 8943 (secțiunea 2.1);

(d) include parametrul antetului protejat x5t în conformitate cu RFC 9360, utilizând SHA-256 pe entitatea finală QSealC codificată în DER; și

(e) este comprimată și prefixată cu șirul EP1:MDOC: înainte de a fi codificată în codul QR.

```
{
  // Numai vizualizare logică lizibilă pentru om a EPC, de tip JSON.
  // Sarcina utilă efectivă a codului QR este în format CBOR determinist, nu JSON.
  „docType”: „eu.epc”, // acreditare EPC. Valoarea docType este inclusă, împreună cu
    //issuerSigned, în sarcina utilă externă COSE_Sign1.

  „issuerSigned”: {
    // Date protejate de issuerAuth; utilizate ca sarcină utilă detașată.
    // Pentru generarea și verificarea semnăturii, sarcina utilă externă detașată acoperă atât
```

```
  // docType, cât și issuerSigned.
  „nameSpaces”: {
    „eu.epc”: {
      „ver”: „1.0”, // versiunea profilului/schemei codului QR

      // Numărul de serie al cardului; definit de emitent, maximum 24 de caractere.
      „sub”: „EF123456789012345678 90GH”,

      // Identificator de revocare: CBOR bstr efectiv, 16 octeți/128 de biți.
      // reprezentat aici sub formă de 32 de caractere hexadecimale pentru lizibilitate.
      „rid”: „4a8d9c112233445566778899aabbccdd”,

      // Codificarea CBOR efectivă utilizează eticheta 1004 pentru data completă conform RFC 3339.
      „exp”: „31-12-2030”
    }
  }
},

„issuerAuth”: {
  // Forma efectivă: COSE_Sign1 neetichetată, nu un obiect JSON.
  „type”: „COSE_Sign1”,
  „tagged”: fals, // codificat fără eticheta CBOR COSE_Sign1
  „payload”: „detached”, // câmpul sarcinii utile COSE este CBOR null

  „protectedHeader”: {
    // alg: ES256; parametrul antetului COSE echivalent 1 = -7.
    „alg”: „ES256”,

    // x5t: amprenta certificatului; parametrul antetului COSE 34.
    „x5t”: {
      „hashAlg”: „SHA-256”, // valoarea hash COSE echivalentă -16

      // hash SHA-256 al entității finale QSealC codificate în DER.
      // 32 de octeți reprezentați de 64 de caractere hexadecimale.
      „hashValue”:
      „0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef”
    }
  },

  „unprotectedHeader”: {}, // gol în acest exemplu

  // semnătură COSE ES256: 64 de octeți = 128 de caractere hexadecimale.
  „signature”:
  „0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef”
}
}
```

9. **Utilizarea mecanismelor criptografice**

Utilizarea mecanismelor criptografice în contextul prezentei anexe este în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

ANEXA III

NOTIFICAREA INFORMAȚIILOR MENȚIONATE LA ARTICOLUL 6 ALINEATUL (2)

1. Statele membre furnizează Comisiei următoarele informații cu privire la fiecare autoritate sau organism competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități:

   (a) denumirea autorității sau a organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (b) numărul de înregistrare al autorității sau al organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (c) adresa de e-mail și numărul de telefon de contact ale autorității sau ale organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități;

   (d) unul sau mai multe certificate care pot fi utilizate pentru a verifica sigiliul electronic creat de autoritatea sau organismul competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități pe care le emite și pentru care datele de identitate certificate includ numele și numărul de înregistrare al emitentului, astfel cum se precizează la litera (a) și, respectiv, la litera (b);

   (e) adresa URL a site-ului pe care emitentul publică statutul valabilității versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități.

2. Statele membre pot furniza Comisiei următoarele informații cu privire la fiecare autoritate sau organism competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități:

   (a) adresa URL a paginii web care conține politicile și condițiile autorității sau ale organismului competent(e) responsabil(e) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități care se aplică furnizării și utilizării versiunilor fizice ale cardului european pentru dizabilitate și ale cardului european de parcare pentru persoanele cu dizabilități pe care le furnizează;

   (b) după caz, adresa URL a paginii web care conține informații suplimentare cu privire la autoritatea sau organismul competent(ă) responsabil(ă) cu emiterea versiunilor fizice ale cardului european pentru dizabilitate sau ale cardului european de parcare pentru persoanele cu dizabilități.

ANEXA IV

SPECIFICAȚII TEHNICE PRIVIND LISTA DE REVOCARE PENTRU VERSIUNILE FIZICE ALE CARDULUI EUROPEAN PENTRU DIZABILITATE SAU ALE CARDULUI EUROPEAN DE PARCARE PENTRU PERSOANELE CU DIZABILITĂȚI

1. În sensul prezentei anexe, identificatorul corespunde identificatorului de revocare (RID) definit la punctul 6 din anexa I și la punctul 6 din anexa II.

2. O listă de revocare se implementează sub forma unui token de tip „listă de identificatori” în format CWT (RFC 8392, secțiunea 7), în conformitate cu clauza 5.2 din specificația listei privind statutul tokenurilor (draft-ietf-oauth-status-list-14), cu următoarele modificări:

   (a) valoarea revendicării de tip este „application/identifierlist+cwt”;

   (b) este prezentă revendicarea privind termenul de expirare;

   (c) revendicarea StatusList nu este prezentă în setul de revendicări CWT;

   (d) structura IdentifierList definită la punctul 3 este prezentă ca revendicare în setul de revendicări CWT, utilizând cheia 65530;

   (e) CWT este un obiect COSE_Sign1 care utilizează, pentru calcularea semnăturii, un algoritm de semnătură în conformitate cu mecanismele criptografice convenite, aprobate de Grupul european pentru certificarea securității cibernetice și publicate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA);

   (f) CWT conține parametrul x5chain, astfel cum este definit în RFC 9360 (secțiunea 2), în antetul protejat care conține certificatul sau lanțul de certificate pentru a verifica semnătura listei de revocare;

   (g) OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor (draft-ietf-oauth-status-list-14) poate fi utilizat pentru certificatul de semnare a listei de identificatori și se recomandă ca verificatorii să accepte OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor și ca infrastructurile autorităților emitente să nu considere câmpul de utilizare extinsă a cheii ca fiind critic atunci când utilizează OID-ul de utilizare extinsă a cheii specificat în specificația listei privind statutul tokenurilor.

3. Structura IdentifierList este o structură CBOR cu următorul limbaj de definire a datelor concise (*Concise Data Definition Language* – CDDL):

```
IdentifierList = {

  „identifiers”: { * Identifier => IdentifierInfo },

  ? „aggregation_uri”: Aggregation_uri,

  * tstr => RFU

}

IdentifierInfo = {

  (tstr/int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```