2026/1436

12.11.2026

KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2026/1436

af 1. juli 2026

om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2024/2841 for så vidt angår QR-koden på den fysiske udgave af EU-handicapkortet og QR-koden på og de fælles tekniske specifikationer til sikring af den fysiske udgave af EU-parkeringskortet for personer med handicap samt interoperabilitetsaspekter

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv (EU) 2024/2841 af 23. oktober 2024 om indførelse af det europæiske handicapkort og det europæiske parkeringskort for personer med handicap ([1]), særlig artikel 7, stk. 7, og artikel 8, stk. 7, og

ud fra følgende betragtninger:

(1) I direktiv (EU) 2024/2841 fastsættes reglerne for udstedelse af EU-handicapkortet og EU-parkeringskortet for personer med handicap og fælles modeller for disse kort. I henhold til artikel 7, stk. 2, og artikel 8, stk. 2, i direktiv (EU) 2024/2841 skal EU-handicapkort og EU-parkeringskort for personer med handicap, der udstedes af medlemsstaterne, anerkendes gensidigt i alle medlemsstaterne.

(2) De beføjelser, der er fastsat i henholdsvis artikel 7, stk. 7, og artikel 8, stk. 7, i direktiv (EU) 2024/2841, har samme formål, nemlig at forebygge og bekæmpe svig, at garantere sikkerheden af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, herunder ved hjælp af passende sikkerhedsforanstaltninger til beskyttelse af personoplysninger i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([2]), samt at sikre interoperabilitet. Da genstanden for og formålene med beføjelserne i vid udstrækning er sammenfaldende, bør reglerne til supplering af direktiv (EU) 2024/2841 for så vidt angår disse spørgsmål fastsættes i én enkelt delegeret retsakt.

(3) I henhold til direktiv (EU) 2024/2841 skal de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap indeholde en digital funktion på det aktuelle tekniske niveau i form af en QR-kode, der anvender elektroniske midler til at forebygge og bekæmpe svig. QR-koder er således en obligatorisk digital funktion, der skal trykkes på alle fysiske kort. For at sikre en ensartet tilgang til medlemsstaternes oprettelse og anvendelse af QR-koderne bør Kommissionen vedtage tekniske specifikationer for disse QR-koder, herunder deres indhold.

(4) EU-parkeringskortet for personer med handicap skal erstatte alle eksisterende parkeringskort for personer med handicap, der er udstedt i overensstemmelse med Rådets henstilling 98/376/EF ([3]). Nævnte henstilling er ikke blevet ajourført for at afspejle den teknologiske udvikling og digitaliseringen, og medlemsstaterne har oplevet problemer med svig og forfalskning. Det er derfor nødvendigt at fastsætte de elementer, der skal indføres for at garantere sikkerheden af den fysiske udgave af EU-parkeringskortet for personer med handicap, og som tager hensyn til dets særlige karakteristika såsom det forhold, at det normalt befinder sig bag køretøjets forrude.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Rådets henstilling 98/376/EF af 4. juni 1998 om parkeringskort for mennesker med handicap (EFT L 167 af 12.6.1998, s. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Der bør indføres obligatoriske fælles tekniske specifikationer for at garantere sikkerheden af den fysiske udgave af EU-parkeringskortet for personer med handicap. Hvis kortet trykkes på et egnet materiale, f.eks. polycarbonat, og der anvendes et diffraktivt optisk variabelt billede, vil det være muligt at beskytte det effektivt mod forfalskning. Antiscanningsmønstre vil øge sikkerheden yderligere ved at gøre det muligt at spore kopiering af kort, da de skal indeholde en skjult tekst eller et mønster, der bliver synligt, når kortet fotokopieres eller scannes. Nævnte elementer skal anvendes, uden at det har indflydelse på det format for den fysiske udgave af EU-parkeringskortet for personer med handicap, der er fastsat i bilag II til direktiv (EU) 2024/2841, herunder kortets udseende.

(6) Ud over QR-koden og de andre obligatoriske tekniske specifikationer, der fastsættes ved denne forordning, bør medlemsstaterne have mulighed for at indarbejde valgfrie digitale sikkerhedsfunktioner eller fysiske sikkerhedselementer baseret på de fælles tekniske specifikationer, der er fastsat i denne forordning, i den fysiske udgave af EU-parkeringskortet for personer med handicap, med det formål at gøre kortet mere sikkert. Hvis de valgfrie digitale funktioner indeholder flere personoplysninger end dem, der er angivet på de fysiske udgaver af kortene, skal adgangen til sådanne oplysninger i overensstemmelse med punkt 3, litra b), i bilag II til direktiv (EU) 2024/2841 begrænses til offentlige myndigheder i de udstedende medlemsstater og udelukkende til autoriserede brugere. For at opretholde en harmoniseret ramme for sikkerhedselementerne i alle medlemsstaterne bør listen over valgfrie elementer være udtømmende. Desuden bør medlemsstaterne sikre, at indarbejdelsen af en eller flere af de valgfrie digitale funktioner eller fysiske sikkerhedselementer ikke har konsekvenser for anerkendelsen af gyldige kort fra andre medlemsstater eller kompromitterer interoperabiliteten og funktionaliteten af de obligatoriske tekniske specifikationer.

(7) Den fysiske udgave af EU-parkeringskortet for personer med handicap kan indeholde en chip til radiofrekvensidentifikation (RFID) som en valgfri digital sikkerhedsfunktion. RFID bruger elektromagnetiske bølger eller induktiv kobling i radiofrekvensdelen af det elektromagnetiske spektrum til at kommunikere til eller fra et RFID-tag ved hjælp af forskellige modulations- og kodningssystemer, således at RFID-taggets identitet eller andre data, der er lagret i den, kan læses entydigt ([4]). RFID-chips kan styrke beskyttelsen mod forfalskning og manipulation ved hjælp af sikker opbevaring eller overførsel af kortrelaterede data. Den fysiske udgave af EU-parkeringskortet for personer med handicap kan også indeholde optisk variable trykfarver eller trykfarver, hvor farven er afhængig af synsvinklen. Sådanne trykfarver giver tilstrækkelig beskyttelse mod kopiering og manipulation af kortet, uden at der kræves personalisering. For at sikre, at kortets data er ordentligt sikret mod forsøg på efterligning og forfalskning, kan teksten i datafelterne integreres i kortets grundmateriale ved hjælp af lasergraveringsteknologi. Fysiske sikkerhedselementer, uanset om de er obligatoriske eller valgfrie i henhold til denne forordning, der ikke er synlige, eller som bliver synlige efter visse manipulationer, er ikke i strid med formatet for EU-parkeringskortet for personer med handicap som fastsat i bilag II til direktiv (EU) 2024/2841.

(8) Der gøres løbende teknologiske fremskridt, og systemerne for parkeringskontrol og sikkerhedsrisiciene udvikler sig løbende. Det aktuelle tekniske niveau udvikler sig, og anvendelsen af EU-handicapkortet og EU-parkeringskortet for personer med handicap udvikler sig, idet denne udvikling er drevet af både brugerfeedback og teknologiske fremskridt, og det samme gælder de teknikker, der bruges til svig og forfalskning, hvilket fører til nye sikkerhedsudfordringer. Nye teknologiske løsninger, herunder i forbindelse med parkeringskontrol, samt behovet for sikkerhed og forebyggelse af svig kan derfor nødvendiggøre ændringer i den udformning af kortene, der skal garantere sikkerheden og bekæmpelsen af svig, herunder ved at ajourføre kategoriseringen af digitale funktioner som enten obligatoriske eller valgfrie. Afhængigt af den teknologiske udvikling kan dette gøre det nødvendigt at ajourføre denne forordning.

(9) For at sikre, at den fysiske udgave af EU-handicapkortet og EU-parkeringskortet for personer med handicap kan anvendes problemfrit i alle medlemsstaterne, er det nødvendigt at sikre interoperabilitet mellem de digitale funktioner på de fysiske kort, navnlig QR-koderne. Formålet med interoperabilitet er at gøre det muligt for kortkontrollører, dvs. enhver fysisk eller juridisk person, der kontrollerer gyldigheden og ægtheden af de fysiske udgaver af kortene, at kontrollere ægtheden og gyldigheden af de fysiske udgaver af kortene, f.eks. ved hjælp af en kontrolapplikation. Med henblik herpå er det nødvendigt at fastsætte bestemmelser om interoperabilitet for at gøre det muligt at foretage en konsekvent og pålidelig kontrol på tværs af grænserne af de fysiske udgaver af kortene.

([4]) Kommissionens henstilling 2009/387/EF af 12. maj 2009 om gennemførelse af principperne om beskyttelse af personoplysninger og privatlivets fred i forbindelse med anvendelse af radiofrekvensbaseret identifikation (meddelt under nummer K(2009) 3200) (EUT L 122 af 16.5.2009, s. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) For at sikre integriteten og oprindelsen af de data, der er indeholdt i QR-koderne på de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, bør disse data forsegles med et kvalificeret elektronisk segl som defineret i artikel 3, nr. 27), i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([5]). QR-koden bekræfter ægtheden og gyldigheden af det fysiske kort, når det krydstjekkes med kontrolparametrene, og bør ikke i sig selv attestere handicapstatus eller retten til specifikke tjenester på grund af et handicap.

(11) For at fremme interoperabiliteten og oprettelsen af et pålideligt og sikkert system for kontrol af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap i hele Unionen bør der indføres mekanismer til meddelelse og offentliggørelse af oplysninger. Med henblik herpå og for at gøre det muligt at kontrollere, at de fysiske udgaver af kortene er udstedt af en kompetent myndighed eller et kompetent organ, bør medlemsstaterne give de oplysninger, der er nødvendige for kontrolprocessen, navnlig de oplysninger, der er nødvendige for at kontrollere det kvalificerede elektroniske segl. Medlemsstaterne bør derfor forpligtes til at underrette Kommissionen om de kompetente myndigheder eller organer, der er ansvarlige for at udstede de fysiske udgaver af kortene (kortudstederne), samt de relevante administrative og tekniske oplysninger, der vedrører dem. De oplysninger, der skal meddeles Kommissionen, bør begrænses til, hvad der er nødvendigt for at etablere interoperable mekanismer til kontrol af gyldigheden og ægtheden af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap. Kommissionen bør sikre, at der er offentlig adgang til disse oplysninger.

(12) I tilfælde af inddragelse af kort bør oplysningerne om inddragelsen af kortet desuden straks stilles til rådighed, således at kortkontrollørerne kan kontrollere kortets gyldighed. Med henblik herpå bør kortudstedere føre og rettidigt offentliggøre lister med oplysninger om inddragelsesstatus for alle kort, som de har inddraget inden deres udløbsdato (lister over inddragne kort). En sådan offentliggørelse bør respektere privatlivets fred og beskytte kortindehavernes personoplysninger. Desuden bør listerne over inddragne kort ikke indeholde andre personoplysninger end de entydige inddragelsesidentifikatorer, og for at sikre interoperabel kontrol bør de offentliggøres ved hjælp af en specifik Uniform Resource Identifier (URI) i overensstemmelse med tekniske specifikationer.

(13) Med henblik på at læse QR-koden og kontrollere ægtheden og gyldigheden af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap kan der anvendes skræddersyede kontrolapplikationer på nationalt plan. Kommissionen kan støtte denne proces ved at stille en fælles kildekode til stikprøver til rådighed med henblik på læsning af data i QR-koderne og udførelse af de vigtigste trin i kontrolprocessen, som kan danne grundlag for kontrolapplikationerne i medlemsstaterne. Alle kontrolapplikationer bør følge den samme logik for kontrol af tillidskæden ved hjælp af den samme tillidsinfrastruktur og dermed gøre det muligt for den udstedende medlemsstat at læse de data, der er indkodet i kortene. Desuden er der i bilag I til Europa-Parlamentets og Rådets direktiv (EU) 2019/882 ([6]) fastsat tilgængelighedskrav, som medlemsstaterne skal efterleve, hvis relevant.

(14) I erkendelse af den dynamiske karakter af teknologiske fremskridt og nye cybersikkerhedstrusler er Unionen fast besluttet på at sikre, at de kryptografiske mekanismer, der anvendes inden for dens lovgivningsmæssige rammer, forbliver effektive og sikre. I lyset heraf er det derfor vigtigt at vedtage kryptografiske standarder, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og formidlet gennem Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

(15) Forordning (EU) 2016/679 finder anvendelse på behandlingen af personoplysninger i henhold til nærværende forordning. Kontrol af QR-koder på de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap indebærer navnlig behandling af personoplysninger. Der bør derfor fastsættes passende databeskyttelsesgarantier for at sikre beskyttelsen af personoplysninger i QR-koder i overensstemmelse med forordning (EU) 2016/679, hvor det er relevant. De generelle sikkerhedsforanstaltninger i denne forordning bør også sikre beskyttelsen af de personoplysninger, der er indeholdt i QR-koderne. Desuden bør personoplysningerne i QR-koderne begrænses til, hvad der er strengt nødvendigt med henblik på denne forordning. Det bør desuden være forbudt at lagre data, efter at kontrollen er afsluttet. Det er også nødvendigt at sikre, at listerne over inddragne kort er tilstrækkeligt sikre.

([5]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Europa-Parlamentets og Rådets direktiv (EU) 2019/882 af 17. april 2019 om tilgængelighedskrav for produkter og tjenester (EUT L 151 af 7.6.2019, s. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) Kommissionen har i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([7]) som led i udarbejdelsen af denne forordning hørt personer med handicap og de organisationer, der repræsenterer dem, samt eksperter, der er udpeget af hver enkelt medlemsstat, jf. artikel 14, stk. 4, i direktiv (EU) 2024/2841.

(17) EU-handicapkortet og EU-parkeringskortet for personer med handicap udgør en transeuropæisk digital offentlig tjeneste som omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2024/903 ([8]). Der er derfor foretaget en interoperabilitetsvurdering, og den deraf følgende rapport skal offentliggøres på portalen for et interoperabelt Europa, jf. artikel 8 i forordning (EU) 2024/903.

(18) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt om nærværende forordning i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([9]) og afgav udtalelse den 12. maj 2026 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand og anvendelsesområde

Ved denne forordning fastsættes regler til supplering af direktiv (EU) 2024/2841 for så vidt angår:

a) fastsættelsen af bestemmelser om den QR-kode, der skal forefindes på de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, herunder passende sikkerhedsforanstaltninger for personoplysninger

b) fastsættelse af fælles obligatoriske og valgfrie tekniske specifikationer, der garanterer sikkerheden ved den fysiske udgave af EU-parkeringskortet for personer med handicap

c) fastsættelse af de interoperabilitetskrav, der er nødvendige for at sikre, at QR-koderne på de fysiske udgaver af EU-handicapkortet eller EU-parkeringskortet for personer med handicap, der er udstedt i én medlemsstat, kan læses og kontrolleres pålideligt i en anden medlemsstat.

Artikel 2

QR-koden på den fysiske udgave af EU-handicapkortet

Specifikationerne for den QR-kode, der skal forefindes på den fysiske udgave af EU-handicapkortet, er fastsat i bilag I.

Artikel 3

QR-koden på den fysiske udgave af EU-parkeringskort for personer med handicap

Specifikationerne for den QR-kode, der skal forefindes på den fysiske udgave af EU-parkeringskortet for personer med handicap, er fastsat i bilag II.

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

([8]) Europa-Parlamentets og Rådets forordning (EU) 2024/903 af 13. marts 2024 om foranstaltninger til sikring af et højt niveau af interoperabilitet i den offentlige sektor i hele Unionen (forordningen om et interoperabelt Europa) (EUT L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 4

Obligatoriske fælles tekniske specifikationer for EU-parkeringskortet for personer med handicap

1. De fysiske udgaver af EU-parkeringskortet for personer med handicap skal opfylde følgende fælles tekniske specifikationer:

a) de skal være fremstillet af et materiale, der beskytter mod delaminering og opfylder kravene i bilag II til direktiv (EU) 2024/2841 og andre obligatoriske fælles tekniske specifikationer, der er fastsat i denne artikel

b) de skal indeholde et diffraktivt optisk variabelt billede som et element i en lagdelt struktur, der bliver synligt, når kortet ses fra en bestemt vinkel

c) de skal fremstilles med et antiscanningsmønster, der bliver synligt ved fotokopiering eller scanning af kortet.

2. Det diffraktive optisk variable billede, der er omhandlet i stk. 1, litra b), skal være anbragt på forsiden af den fysiske udgave af EU-parkeringskortet for personer med handicap hen over et eller flere datafelter i venstre side. Det skal være ca. 20 mm højt og 20 mm bredt. Billedet skal bestå af et stiliseret kort over den udstedende medlemsstat eller den udstedende medlemsstats kendingskode omgivet af en cirkel med 12 stjerner, der symboliserer Unionen.

3. Det antiscanningsmønster, der er omhandlet i stk. 1, litra c), skal være anbragt på forsiden af den fysiske udgave af EU-parkeringskortet for personer med handicap oven over datafelterne i venstre side og/eller i højre side uden for QR-koden og det tomme område omkring koden. Det skal indeholde en skjult tekst eller et skjult mønster, der bliver synligt ved fotokopiering eller scanning af kortet. Hvis antiscanningsmønsteret indeholder en skjult tekst, skal den bestå ordene »COPY« (»KOPI«) eller »VOID« (»UGYLDIGT«) og en oversættelse heraf til et eller flere af den udstedende medlemsstats officielle sprog. Hvis antiscanningsmønsteret indeholder et skjult mønster, skal det bestå af vandrette eller lodrette linjer.

Artikel 5

Valgfrie tekniske specifikationer for og sikkerhedselementer i EU-parkeringskortet for personer med handicap

1. Ud over de obligatoriske fælles tekniske specifikationer, der er omhandlet i artikel 4, må medlemsstaterne kun anvende de valgfrie tekniske specifikationer og elementer, der er fastsat i nærværende artikel.

2. De fysiske udgaver af EU-parkeringskortet for personer med handicap kan indeholde en chip til radiofrekvensidentifikation (RFID). RFID-chippen skal forebygge og bekæmpe svig ved hjælp af elektroniske midler og fungere som et yderligere middel til kontrol på nationalt plan af ægtheden og/eller gyldigheden af en fysisk udgave af EU-parkeringskortet for personer med handicap. RFID-chippen må ikke påvirke QR-kodens funktion på kortet.

3. En RFID-chip som omhandlet i stk. 2 skal opfylde følgende specifikationer:

a) Den skal være passiv

b) Den skal være fysisk integreret i kortets materiale på højre forside

c) Den skal være logisk knyttet til QR-koderegistreringen og indeholde den samme inddragelsesidentifikator (RID) som den, der er indkodet i QR-koden

d) RFID-funktionen skal understøtte aflæsning i en afstand af ca. én meter eller mere, når det kræves til operationelt brug, men må ikke være konstrueret til pålidelig aflæsning i en afstand på over fem meter under referenceprøvningsforhold.

e) Efter udstedelsen af kortet må der ikke være skriveadgang til RFID-chippen eller til det relevante dataområde deri, medmindre den udstedende myndighed fører kontrol hermed

f) Den skal udformes og konfigureres på en sådan måde, at risikoen for kloning, substitution, uautoriseret ændring og uautoriseret omskrivning minimeres

g) Den skal opfylde kravene i Europa-Parlamentets og Rådets direktiv 2014/53/EU ([10])

h) Ud over den RID, der er omhandlet i litra c), må RFID-chippen kun lagre en eller flere af følgende oplysninger:

i) data, der er indkodet i QR-koden på den fysiske udgave af EU-parkeringskortet for personer med handicap

ii) køretøjets nummerplade(r)

iii) kryptografiske kontroldata.

4. Forsiden af de fysiske udgaver af EU-parkeringskortet for personer med handicap kan indeholde et eller flere af følgende elementer:

a) kørestolssymbolet i venstre side eller ordene »European Parking Card for persons with disabilities« på engelsk og på et eller flere af den udstedende medlemsstats officielle sprog i højre side trykt med optisk variabel trykfarve eller trykfarve, der skifter farve, når kortet ses fra forskellige vinkler

b) brugen af lasergravering, der trænger ind i kortlagene, til at skrive teksten i datafelterne.

5. Indførelsen af valgfrie tekniske specifikationer og elementer som omhandlet i denne artikel berører ikke anerkendelsen i den medlemsstat, der har indført sådanne elementer for de kort, den udsteder, af gyldige kort, der er udstedt i andre medlemsstater.

Artikel 6

Interoperabilitet

1. Oplysningerne i QR-koden forsegles med et kvalificeret elektronisk segl som omhandlet i artikel 3, nr. 27), i forordning (EU) nr. 910/2014.

2. Hver medlemsstat meddeler Kommissionen oplysninger om de kompetente myndigheder eller organer, der er ansvarlige for at udstede de fysiske udgaver af EU-handicapkortet eller EU-parkeringskortet for personer med handicap (»kortudstedere«), og eventuelle efterfølgende ajourføringer af disse oplysninger i overensstemmelse med bilag III. Kommissionen skal sikre, at der er offentlig adgang til disse oplysninger.

3. Kortudstedere skal ved hjælp af en Uniform Resource Identifier, som meddeles Kommissionen, føre og offentliggøre ajourførte lister over inddragne kort med oplysninger om inddragelsesstatus for alle kort, som de har inddraget, jf. de tekniske specifikationer i bilag IV. Oplysninger om inddragelse offentliggøres senest 24 timer efter inddragelsen.

4. Medlemsstaterne kan anvende kontrolapplikationer til at kontrollere ægtheden og gyldigheden af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap.

5. Hvis medlemsstaterne anvender kontrolapplikationer til at kontrollere ægtheden og gyldigheden af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, skal sådanne applikationer være i stand til at kontrollere et korts ægthed og gyldighed ved at kontrollere kortets elektroniske segl og inddragelsesstatus. Kontrolapplikationerne skal læse og vise en visuel præsentation af de personoplysninger, der er indkodet i kortets QR-kode, jf. bilag I og II, for at muliggøre en sammenligning med de data, der er synlige i de tilsvarende datafelter på kortet, og en angivelse af kortets gyldighedsstatus.

([10]) Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF (EUT L 153 af 22.5.2014, s. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Artikel 7

Sikkerhedsforanstaltninger til beskyttelse af personoplysninger

1. Personoplysningerne i QR-koderne på de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap begrænses til, hvad der er strengt nødvendigt for kontrollen af kortenes ægthed og gyldighed, jf. bilag I og II.

2. Når kortkontrollørerne har afsluttet kontrollen af ægtheden og gyldigheden af en fysisk udgave af EU-handicapkortet eller EU-parkeringskortet for personer med handicap, må de ikke opbevare de data, der er indeholdt i QR-koderne.

3. Kontrollen af en QR-kode på en fysisk udgave af EU-handicapkortet eller EU-parkeringskortet for personer med handicap må ikke føre til, at den kompetente myndighed eller det kompetente organ, der har ansvaret for udstedelsen af kortet, underrettes om kontrollen.

4. Oplysningerne i lister over inddragne kort, der offentliggøres i overensstemmelse med artikel 6, stk. 3, begrænses til inddragelsesidentifikatoren for inddragne kort.

5. Den myndighed eller det organ, der har ansvaret for at offentliggøre listerne over inddragne kort i henhold til artikel 6, stk. 3, sikrer, at der anvendes passende tekniske og organisatoriske sikkerhedsforanstaltninger på behandlingen af personoplysninger i listerne over inddragne kort.

6. Hvis en medlemsstat beslutter at indarbejde en RFID-chip i den fysiske udgave af EU-parkeringskortet for personer med handicap, finder stk. 2 og 3 anvendelse på behandlingen af de personoplysninger, der er indeholdt i nævnte chip. Personoplysningerne i RFID-chippen begrænses til, hvad der er strengt nødvendigt for kontrollen af kortenes ægthed og/eller gyldighed, jf. artikel 5, stk. 3.

Hvis en medlemsstat lagrer personoplysninger i den i artikel 5 omhandlede RFID-chip, som ikke fremgår af den fysiske udgave af EU-parkeringskortet for personer med handicap, jf. bilag II til direktiv (EU) 2024/2841, er adgangen til sådanne oplysninger begrænset til offentlige myndigheder i den udstedende medlemsstat og kun til autoriserede brugere.

Artikel 8

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 1. juli 2026.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

SPECIFIKATIONER FOR QR-KODEN PÅ DEN FYSISKE UDGAVE AF EU-HANDICAPKORTET

1. **Formatet for QR-koden på den fysiske udgave af EU-handicapkortet**

a) **Formatet for en QR-kode af Model 2** skal være i overensstemmelse med de internationale QR-kodespecifikationer ISO/IEC 18004: 2024 eller tilsvarende.

b) Der kræves **Error Correction Level M** (fejl ved korrektionsniveau M) (15 % redundans), hvilket sikrer modstandsdygtighed over for ridser eller delvis beskadigelse af en trykt QR-kode.

c) **Encoding Mode (indkodningsmodus)**: QR payload'en (QR-informationsfeltet) skal bestå af den kombinerede struktur issuerSigned Concise Binary Object Representation (CBOR) og det tilsvarende issuerAuth COSE_Sign1-signatur-objekt som defineret i CBOR Object Signing and Encryption (COSE, RFC 9052, afdeling 3.1, 4.2 og 4.4), der følger mDOC data-modelmønstret for issuerSigned-elementer, men er tilpasset statisk brug af fysiske kort. IssuerAuth skal være et COSE_Sign1-objekt med alg = ES256 og en beskyttet header, der indeholder x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256).

d) Inden indkodning af QR-koden **komprimeres det kombinerede CBOR/COSE-objekt ved hjælp af zlib-formatet** (RFC 1950, afdeling 2.2) **med deflatoralgoritmen** (RFC 1951, afdeling 3.2 og 4). Den komprimerede byte-array skal indkodes i **QR code Byte Mode**, hvilket sikrer fuld støtte til de binære CBOR/COSE-informationsfelter og scannerinteroperabilitet.

Udstederne skal for alle tekstfelter i QR-informationsfeltet indkode tegn som Unicode UTF-8 i CBOR-tekststrenge. Der må ikke anvendes translitteration på underskrevne data i informationsfelterne. Af hensyn til interoperabiliteten skal udstederne anvende Unicode Normalisation Form C (NFC) på alle tekstfelter, inden de underskriver.

e) **Præfiks:** QR-strengen for EU-handicapkort begynder med »ED1: MDOC:«. Dette identificerer korttype og indkodningsprofil. I præfikserne skelnes der mellem store og små skrifttegn, og de skal angives. Ukendte eller ikke-understøttede præfikser skal medføre afvisning. Præfikset og det komprimerede informationsfelt skal indkodes i QR-koden som ét enkelt Byte Mode-datasegment.

f) Den **mindste modulstørrelse er ≥ 0,25 mm** for at sikre læsbarheden på trykte kort.

g) **Maksimumversion 20** med op til 97 × 97 moduler på hver side.

2. **Specifikationer for generering af underskrift på EU-handicapkort**

Det kvalificerede elektroniske segl (QSeal), der anvendes til at forsegle QR-koder i EU-handicapkort, sikrer, at de indkodede data stammer fra den godkendte udstedende myndighed og ikke er blevet ændret.

a) **Underskriftsalgoritme**: Underskriftsalgoritmen skal være ES256 (Elliptic Curve Digital Signature Algorithm (ECDSA) (digital underskriftsalgoritme med elliptisk kurve (ECDSA)) med SHA-256 ved hjælp af P-256-kurven som defineret i RFC 9053 (afdeling 2.1); i COSE identificeres algoritmen ved algheaderparameteren i RFC 9052 (afdeling 3.1).

b) **Signing Key** (signeringsnøgle): QR-informationsfeltet skal underskrives ved hjælp af den private nøgle, der svarer til et kvalificeret certifikat for elektronisk segl (QSealC).

c) **COSE-struktur**: Signaturcontaineren skal være et objekt af typen COSE_Sign1. Den beskyttede header skal omfatte en alg (ES256) og x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256). Kontrollen skal baseres på anvendelsen af x5t-værdien til at lokalisere det tilsvarende certifikat i kontrollørens lokalt cachede tillidslager (trust store), der består af oplysninger fra positivlisten, hvorefter certifikatkæden og certifikatstatus skal valideres i overensstemmelse med eIDAS-tillidsrammen.

d) **Underskrift - standard**: QR-kodens informationsfelt skal underskrives som et COSE_Sign1-objekt i overensstemmelse med RFC 9052 (afdeling 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet skal forefindes i issuerAuth og indkodes uden et CBOR-tag til COSE_Sign1. COSE_Sign1-objektets informationsfelt skal være særskilt og indkodes som CBOR null. Det eksterne informationsfelt skal med henblik på generering og kontrol af underskrift være den deterministiske CBOR-indkodede struktur, der indeholder docType-værdien og issuerSigned-værdien fra topniveau-CBOR-map-strukturen.

e) **Hashalgoritme**: SHA-256 anvendes som en del af ES256 til generering af underskrifter og integritetskontrol.

f) **Indkodning**: Informationsfeltet skal indkodes ved hjælp af CBOR (RFC 8949, afdeling 4.2) som krævet i COSE- og mDOC-specifikationerne, hvilket sikrer indkodning og reproducerbarhed af de underskrevne data.

3. **Trykningsspecifikationer**

a) **Quiet Zone** (tomt område): QR-koden skal være omgivet af en tom margen på **4 moduler** på alle sider uden tryk, mønster eller baggrund.

b) **Kontrast**: QR-koden skal trykkes på hvid baggrund med et kontrastforhold på mindst **4:1** for at sikre høj læsbarhed under forskellige lysforhold.

c) QR-koden skal trykkes i den farve, der er defineret i bilag I til direktiv (EU) 2024/2841, og som sikrer størst mulig kontrast.

d) **Placering og størrelse**: QR-koden, inklusive det tomme område, skal være 26,25 mm × 26,25 mm og skal forefindes på bagsiden af kortet i nederste højre hjørne. QR-koden må højst være version 20 (97 × 97 moduler) med en modulstørrelse på 0,25 mm eller derover.

QR-koden, inklusive det tomme område, skal forefindes mindst 5 mm fra kortets højre kant og mindst 5 mm fra kortets nederste kant.

4. **Data i QR-koden på EU-handicapkort**

QR-koden skal indeholde et minimumsdatasæt, der kan kontrolleres offline, jf. princippet om dataminimering som fastsat i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679. Strukturen for informationsfeltet skal være som følger:

a) Kortattributter indkodes i CBOR i et issuerSigned-objekt.

b) Strukturen indpakkes og underskrives ved hjælp af den udstedende myndigheds QSeal i form af en issuerAuth (COSE_Sign1, ES256, herunder x5t, COSE X.509-certifikatets hashheaderparameter).

c) Det deraf følgende CBOR/COSE-objekt skal komprimeres i overensstemmelse med dette bilags punkt 1, litra d). QR-kodens informationsfelt skal bestå af præfikset »ED1:MDOC:« efterfulgt af den deraf følgende komprimerede byte-array, og det komplette informationsfelt skal indkodes ved brug af Byte Mode som ét enkelt QR-kodedatasegment.

Dataindholdet skal bestå af en undergruppe af synlige data fra de felter på kortets forside, der er opført i bilag I til direktiv (EU) 2024/2841 (fornavn, efternavn, kortets serienummer, udløbsdato), sammen med inddragelsesidentifikatoren, den elektroniske underskrift og skemaoplysningerne.

Den **elektroniske underskrift** skal indeholde:

i) et issuerAuth – Et COSE_Sign1-objekt, der er underskrevet med den udstedende myndigheds QSeal-privatnøgle (**QSealC private key**)

ii) en beskyttet header, der omfatter en alg = ES256 (signaturalgoritme) og x5t (COSE X.509-certifikatets hashheaderparameter).

5. **Valgfrie data**

QR-koden må ikke indeholde valgfrie data.

6. **Inddragelsesidentifikator (Revocation Identifier – RID)**

Ud over kortets synlige serienummer skal QR-koden indeholde en særlig inddragelsesidentifikator (RID).

RID'en anvendes til at fastslå inddragelsesstatus og til forvaltning af listen over inddragne kort. RID'en må ikke trykkes på kortet og må ikke være synlig for kortkontrollørerne.

6.1. *Krav til RID'en*

RID'en:

a) skal indgå i det underskrevne QR-informationsfelt

b) skal være entydig, som minimum inden for den udstedende myndigheds udstedelsesdomæne

c) må ikke trykkes på kortet og ikke være beregnet til at være menneskeligt læsbar

d) må ikke afsløre personoplysninger og må ikke være umiddelbart forståelig

e) må ikke kunne udledes direkte af kortets synlige serienummer og

f) skal være kryptografisk knyttet til QR-informationsfeltet ved hjælp af det kvalificerede elektroniske segl.

6.2. *RID'ens format og størrelse*

RID'en skal indkodes som en CBOR-byte-streng (bstr). RID'en skal være 16 byte (128 bit) lang.

RID'en skal genereres af den udstedende myndighed ved hjælp af en metode, som denne har kontrol over, og som sikrer tilstrækkelig entropi og modstandsdygtighed over for gætteri eller optælling.

6.3. *Lister over inddragne kort*

I de lister over inddragne kort, der offentliggøres med henblik på kontrol, må der kun henvises til RID'en for inddragne kort. Kortenes serienumre må ikke offentliggøres i lister over inddragne kort.

7. **CBOR-informationsfeltet (inden for QR-koden) på EU-handicapkort**

Alene følgende data må medtages i QR-informationsfeltet i overensstemmelse med EU-handicapkortets synlige datafelter som fastsat i bilag I til direktiv (EU) 2024/2841.

Indhold på øverste niveau:

a) docType = »eu.edc«

b) issuerSigned.nameSpaces.»eu.edc« med attributter som vist i tabellen nedenfor

c) issuerAuth = COSE_Sign1 (QSeal)

Felt	mDOC path	Type/format
Dataskemaversion	issuerSigned.nameSpaces.»eu.edc«.ver	Streng (f.eks. »1.0«)
Korttype: EDC (EU-handicapkort)	docType	Enum (»eu.edc«)
Kortets serienummer	issuerSigned.nameSpaces.»eu.edc«.sub	Streng
Inddragelsesidentifikator	issuerSigned.nameSpaces.»eu.edc«.rid	CBOR bstr (16 byte)
Kortindehaverens fornavn	issuerSigned.nameSpaces.»eu.edc«.givenName	Unicode-tekststreng (UTF-8)
Kortindehaverens efternavn	issuerSigned.nameSpaces.»eu.edc«.familyName	Unicode-tekststreng (UTF-8)
Kortets udløbsdato	issuerSigned.nameSpaces.»eu.edc«.exp	CBOR-tag af typen 1004 som defineret i RFC 8943 (afdeling 2.1), der indeholder en UTF-8-tekststreng, der repræsenterer en fuldstændig RFC 3339-dato (full-date) angivet i formatet ÅÅÅÅ-MM-DD.

Den elektroniske signatur forefindes i issuerAuth (et COSE_Sign1-objekt). Certifikatkæden må ikke være indlejret i QR-kodens informationsfelt; i stedet skal den beskyttede COSE-header indeholde x5t, et certifikat med thumbprint, der bruges til at lokalisere det dertil svarende QSealC i kontrollørens trustlager i cachen.

8. **Eksempel på QR-kodens informationsfelt på EU-parkeringskort: logisk præsentation i JavaScript Object Notation-stil med kommentarer**

Følgende eksempel er en menneskeligt læsbar JavaScript Object Notation (JSON)-gengivelse af den logiske præsentation af EU-handicapkortet. I praksis må denne struktur ikke være menneskeligt læsbar, da den skal:

a) være indkodet i CBOR (RFC 8949, afdeling 3)

b) være underskrevet ved hjælp af en COSE_Sign1-struktur uden tag med et særskilt informationsfelt (RFC 9052, afdeling 4.)

c) indeholde udløbsdatoen som et CBOR-tag af typen 1004 med full-date-værdi i overensstemmelse med RFC 8943 (afdeling 2.1)

d) indeholde den x5t-beskyttede headerparameter i overensstemmelse med RFC 9360, idet der bruges SHA-256 hen over det DER-indkodede end-entity QSealC og

e) være komprimeret og forsynet med præfiksstrengen ED1:MDOC: før den indkodes i QR-koden.

```
{
  // JSON-style, kun menneskeligt læsbar logisk præsentation af EU-handicapkortet.
  // Det faktiske QR-informationsfelt er en deterministisk simulation af CBOR, ikke JSON.
  »docType«: »eu.edc«, // EU-handicapkort-credential. DocType-værdien er sammen med
     //issuerSigned indeholdt i det eksterne COSE_Sign1-informationsfelt.

  »issuerSigned«: {
     // Data, der er beskyttet af issuerAuth; bruges som et særskilt informationsfelt.
     // Det særskilte eksterne informationsfelt dækker både generering og kontrol af underskrift
     // docType og issuerSigned.
     »nameSpaces«: {
       »eu.edc«: {
         »ver«: »1.0«, // QR-profil/skemaversion

         // Kortets serienummer, issuer-defined, maks. 24 tegn.
         »sub«: »AB123456789012345678 90CD«,

         // Inddragelsesidentifikator: faktisk CBOR bstr, 16 byte/128 bit.
         // Vist her som 32 hex-tegn af hensyn til læsbarheden.
         »rid«: »9f8c4d3a7b1e2c0a55aa33ff8899ee11«,

         »givenName«: »Jens«, // det fornavn, der er trykt på EU-handicapkortet
         »familyName«: »Jensen«, // det efternavn, der er trykt på EU-handicapkortet

         // Ved den faktiske CBOR-indkodning bruges tagget af typen 1004 med henblik på angivelse af en fuldstændig RFC 3339-dato (full date).
         »exp«: »2030-12-31«
       }
     }
  },

  »issuerAuth«: {
    // Faktisk format: COSE_Sign1 uden tag, ikke et JSON-objekt.
    »type«: »COSE_Sign1«,
```

```
    »tagged«: falsk, // indkodet uden COSE_Sign1 CBOR-tag
    »payload«: »detached«, // COSE-informationsfeltet er CBOR null

    »protectedHeader«: {
      // alg: ES256; tilsvarende COSE-headerparameter 1 = -7.
      »alg«: »ES256«,

      // x5t: certifkat-thumbprint; COSE-headerparameter 34.
      »x5t«: {
        »hashAlg«: »SHA-256«, // tilsvarende COSE-hashværdi -16

        // SHA-256-hashfunktionen af det DER-indkodede end-entity QSealC.
        // 32 byte, der repræsenteres ved 64 hex-tegn.
        »hashValue«:
        »0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef«
      }
    },

    »unprotectedHeader«: {}, // tom i dette eksempel

    // ES256 COSE-signatur: 64 byte = 128 hex-tegn.
    »signature«:
    »0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
    f0123456789abcdef0123456789abcdef0123456789abcdef«
  }
}
```

9. **Brug af kryptografiske mekanismer**

Anvendelsen af kryptografiske mekanismer i forbindelse med dette bilag skal ske i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

BILAG II

SPECIFIKATIONER FOR QR-KODEN PÅ DEN FYSISKE UDGAVE AF EU-PARKERINGSKORTET FOR PERSONER MED HANDICAP

1. **Formatet for QR-koden på den fysiske udgave af EU-parkeringskort for personer med handicap**

a) **Formatet for en QR-kode af Model 2** skal være i overensstemmelse med de internationale QR-kodespecifikationer ISO/IEC 18004: 2024 eller tilsvarende.

b) Der kræves **Error Correction Level M** (fejl ved korrektionsniveau M) (15 % redundans), hvilket sikrer modstandsdygtighed over for ridser eller delvis beskadigelse af en trykt QR-kode.

c) **Encoding Mode (indkodningsmodus)**: QR payload'en (QR-informationsfeltet) skal bestå af den kombinerede struktur issuerSigned Concise Binary Object Representation (CBOR) og det tilsvarende issuerAuth COSE_Sign1-signatur-objekt som defineret i CBOR Object Signing and Encryption (COSE, RFC 9052, afdeling 3.1, 4.2 og 4.4), der følger mDOC data-modelmønstret for issuerSigned-elementer, men er tilpasset statisk brug af fysiske kort. IssuerAuth skal være et COSE_Sign1-objekt med alg = ES256 og en beskyttet header, der indeholder x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256).

d) Inden indkodning af QR-koden **komprimeres det kombinerede CBOR/COSE-objekt ved hjælp af zlib-formatet (RFC 1950, afdeling 2.2) med deflatoralgoritmen** (RFC 1951, afdeling 3.2 og 4). Den således komprimerede byte-array skal indkodes i **QR code Byte Mode**, hvilket sikrer fuld støtte til de binære CBOR/COSE-informationsfelter og scannerinteroperabilitet.

Udstederne skal for alle tekstfelter i QR-informationsfeltet indkode tegn som Unicode UTF-8 i CBOR-tekststrenge. Der må ikke anvendes translitteration på underskrevne data i informationsfelterne. Af hensyn til interoperabiliteten skal udstederne anvende Unicode Normalisation Form C (NFC) på alle tekstfelter, inden de underskriver.

e) **Præfiks**: QR-strengen for EU-parkeringskort begynder med »EP1:MDOC:«. Dette identificerer korttype og indkodningsprofil. I præfikserne skelnes der mellem store og små skrifttegn, og de skal angives. Ukendte eller ikke-understøttede præfikser skal medføre afvisning. Præfikset og det komprimerede informationsfelt skal indkodes i QR-koden som ét enkelt Byte Mode-datasegment.

f) Den **mindste modulstørrelse er ≥ 0,35 mm** for at sikre læsbarheden på trykte kort.

g) **Maximumversion 20** med op til 97 × 97 moduler på hver side.

2. **Specifikationer for generering af underskrift på EU-parkeringskort**

Det kvalificerede elektroniske segl (QSeal), der anvendes til at forsegle QR-koder i EU-parkeringskort, sikrer, at de indkodede data stammer fra den godkendte udstedende myndighed og ikke er blevet ændret.

a) **Underskriftsalgoritme**: Underskriftsalgoritmen skal være ES256 (ECDSA med SHA-256 ved hjælp af P-256-kurven) som defineret i RFC 9053 (afdeling 2.1); i COSE identificeres algoritmen ved algheaderparameteren i RFC 9052 (afdeling 3.1).

b) **Signing Key** (signeringsnøgle): QR-informationsfeltet skal underskrives ved hjælp af den private nøgle, der svarer til et kvalificeret certifikat for elektronisk segl (QSealC).

c) **COSE-struktur**: Signaturcontaineren skal være et objekt af typen COSE_Sign1. Den beskyttede header skal omfatte en alg (ES256) og x5t (COSE X.509-certifikatets hashheaderparameter som defineret i RFC 9360 (afdeling 2); af hensyn til interoperabiliteten skal den hashalgoritme, der anvendes i x5t, være SHA-256). Kontrollen skal baseres på anvendelsen af x5t-værdien til at lokalisere det tilsvarende certifikat i kontrollørens lokalt cachede tillidslager (trust store), der består af oplysninger fra positivlisten, hvorefter certifikatkæden og certifikatstatus skal valideres i overensstemmelse med eIDAS-tillidsrammen.

d) **Underskrift - standard**: QR-kodens informationsfelt skal underskrives som et COSE_Sign1-objekt i overensstemmelse med RFC 9052 (afdeling 4), CBOR Object Signing and Encryption. COSE_Sign1-objektet skal forefindes i issuerAuth og indkodes uden et CBOR-tag til COSE_Sign1. COSE_Sign1-objektets informationsfelt skal være særskilt og indkodes som CBOR null. Det eksterne informationsfelt skal med henblik på generering og kontrol af underskrift være den deterministiske CBOR-indkodede CBOR-struktur, der indeholder docType-værdien og issuerSigned-værdien fra topniveau-CBOR-map-strukturen.

e) **Hashalgoritme**: SHA-256 anvendes som en del af ES256 til generering af underskrifter og integritetskontrol.

f) **Indkodning**: Informationsfeltet skal indkodes ved hjælp af CBOR (RFC 8949, afdeling 4.2) som krævet i COSE- og mDOC-specifikationerne, hvilket sikrer indkodning og reproducerbarhed af de underskrevne data.

3. **Trykningsspecifikationer**

a) **Quiet Zone** (tomt område): QR-koden skal være omgivet af en tom margen på **4 moduler** på alle sider uden tryk, mønster eller baggrund.

b) **Kontrast**: QR-koden skal trykkes på hvid baggrund med et kontrastforhold på mindst **4:1** for at sikre høj læsbarhed under forskellige lysforhold.

c) QR-koden skal trykkes i den farve, der er defineret i bilag II til direktiv (EU) 2024/2841, og som sikrer størst mulig kontrast.

d) **Placering og størrelse**: QR-koden, inklusive det tomme område, skal være **37 mm × 37 mm** og skal forefindes på forsiden af kortet, lidt til højre for midten, nederst på kortet. QR-koden må højst være version 20 (97 × 97 moduler) med en modulstørrelse på 0,35 mm eller derover.

QR-koden, inklusive det tomme område, skal forefindes mindst 5 mm fra kortets nederste kant.

4. **Data i QR-koden på EU-parkeringskort**

QR-koden skal indeholde et minimumsdatasæt, der kan kontrolleres offline, jf. princippet om dataminimering som fastsat i artikel 5, stk. 1, litra c), i forordning (EU) 2016/679. Informationsfeltets struktur er som følger:

a) Kortattributter indkodes i CBOR i et issuerSigned-objekt.

b) Strukturen indpakkes og underskrives ved hjælp af den udstedende myndigheds QSeal i form af en issuerAuth (COSE_Sign1, ES256, herunder x5t, COSE X.509-certifikatets hashheaderparameter).

c) Det deraf følgende CBOR/COSE-objekt skal komprimeres i overensstemmelse med dette bilags punkt 1, litra d). QR-kodens informationsfelt skal bestå af præfikset »EP1:MDOC:« efterfulgt af den deraf følgende komprimerede byte-array, og det komplette informationsfelt skal indkodes ved brug af Byte Mode som ét enkelt QR-kodedatasegment.

Dataindholdet skal bestå af en undergruppe af synlige data fra de felter på kortets forside, der er opført i bilag II til direktiv (EU) 2024/2841 (udløbsdato, kortets serienummer), sammen med inddragelsesidentifikatoren, den elektroniske underskrift og skemaoplysningerne.

Den **elektroniske underskrift** skal indeholde:

i) et issuerAuth – Et COSE_Sign1-objekt, der er underskrevet med den udstedende myndigheds QSeal-privatnøgle (**QSealC private key**)

ii) En beskyttet header, der omfatter en alg = ES256 (signaturalgoritme) og x5t (COSE X.509-certifikatets hashheaderparameter).

5. **Valgfrie data**

QR-koden må ikke indeholde valgfrie data.

6. **Inddragelsesidentifikator (Revocation Identifier – RID)**

Inddragelsesidentifikatoren i EU-parkeringskortet skal være i overensstemmelse med bilag I, punkt 6.

I listerne over inddragne EU-parkeringskort må der kun henvises til RID'en. Kortenes serienumre må ikke offentliggøres i lister over inddragne kort.

7. **CBOR-informationsfeltet (inden for QR-koden) på EU-parkeringskort**

Alene følgende data må medtages i QR-informationsfeltet, hvilket er i overensstemmelse med EU-handicapkortets synlige datafelter som fastsat i bilag II til direktiv (EU) 2024/2841:

Felt	mDOC path	Type/format
Dataskemaversion	issuerSigned.nameSpaces.»eu.epc«.ver	Streng (f.eks. »1.0«)
Korttype: EPC (EU-parkeringskort)	docType	Enum (»eu.epc«)
Kortets serienummer	issuerSigned.nameSpaces.»eu.epc«.sub	Streng
Inddragelsesidentifikator	issuerSigned.nameSpaces.»eu.epc«.rid	CBOR bstr (16 byte)
Kortets udløbsdato	issuerSigned.nameSpaces.»eu.epc«.exp	CBOR-tag af typen 1004 som defineret i RFC 8943 (afdeling 2.1), der indeholder en UTF-8-tekststreng, der repræsenterer en fuldstændig RFC 3339-dato (full-date) angivet i formatet ÅÅÅÅ-MM-DD.

Den elektroniske signatur skal forefindes i issuerAuth (et COSE_Sign1-objekt). Certifikatkæden må ikke være indlejret i QR-kodens informationsfelt; i stedet skal den beskyttede COSE-header indeholde x5t, et certifikat med thumbprint, der bruges til at lokalisere det dertil svarende QSealC i kontrollørens trustlager i cachen.

8. **Eksempel på QR-kodens informationsfelt på EU-parkeringskort: logisk præsentation i JavaScript Object Notation-stil med kommentarer**

Følgende eksempel er en menneskeligt læsbar JavaScript Object Notation (JSON)-gengivelse af den logiske præsentation af EU-parkeringskortet. I praksis må denne struktur ikke være menneskeligt læsbar, da den skal:

a) være indkodet i CBOR (RFC 8949, afdeling 3)

b) være underskrevet ved hjælp af en COSE_Sign1-struktur uden tag med et særskilt informationsfelt (RFC 9052, afdeling 4.)

c) indeholde udløbsdatoen som et CBOR-tag af typen 1004 med full-date-værdi i overensstemmelse med RFC 8943 (afdeling 2.1)

d) indeholde den x5t-beskyttede headerparameter i overensstemmelse med RFC 9360, idet der bruges SHA-256 hen over det DER-indkodede end-entity QSealC og

e) være komprimeret og forsynet med præfiksstrengen EP1:MDOC: før den indkodes i QR-koden.

```
{
  // JSON-style, kun menneskeligt læsbar logisk præsentation af EU-parkeringskortet.
  // Det faktiske QR-informationsfelt er en deterministisk simulation af CBOR, ikke JSON.
  »docType«: »eu.epc«, // EU-parkeringskort-credential. DocType-værdien er sammen med
    //issuerSigned indeholdt i det eksterne COSE_Sign1-informationsfelt.

  »issuerSigned«: {
    // Data, der er beskyttet af issuerAuth; bruges som et særskilt informationsfelt.
    // Det særskilte eksterne informationsfelt dækker både generering og kontrol af underskrift
```

```
  // docType og issuerSigned.
  »nameSpaces«: {
    »eu.epc«: {
      »ver«: »1.0«, // QR-profil/skemaversion

      // Kortets serienummer, issuer-defined, maks. 24 tegn.
      »sub«: »EF123456789012345678 90GH«,

      // Inddragelsesidentifikator: faktisk CBOR bstr, 16 byte/128 bit.
      // Vist her som 32 hex-tegn af hensyn til læsbarheden.
      »rid«: »4a8d9c112233445566778899aabbccdd«,

      // Ved den faktiske CBOR-indkodning bruges tagget af typen 1004 med henblik på angivelse af en fuldstændig RFC 3339-dato (full date).
      »exp«: »2030-12-31«
    }
  }
},

»issuerAuth«: {
  // Faktisk format: COSE_Sign1 uden tag, ikke et JSON-objekt.
  »type«: »COSE_Sign1«,
  »tagged«: falsk, // indkodet uden COSE_Sign1 CBOR-tag
  »payload«: »detached«, // COSE-informationsfeltet er CBOR null

  »protectedHeader«: {
    // alg: ES256; tilsvarende COSE-headerparameter 1 = -7.
    »alg«: »ES256«,

    // x5t: certifkat-thumbprint; COSE-headerparameter 34.
    »x5t«: {
      »hashAlg«: »SHA-256«, // tilsvarende COSE-hashværdi -16

      // SHA-256-hashfunktionen af det DER-indkodede end-entity QSealC.
      // 32 byte, der repræsenteres ved 64 hex-tegn.
      »hashValue«:
      »0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef«
    }
  },

  »unprotectedHeader«: {}, // tom i dette eksempel

  // ES256 COSE-signatur: 64 byte = 128 hex-tegn.
  »signature«:
  »0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef«
}
}
```

9. **Brug af kryptografiske mekanismer**

Anvendelsen af kryptografiske mekanismer i forbindelse med dette bilag skal ske i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

BILAG III

MEDDELELSE AF DE OPLYSNINGER, DER ER OMHANDLET I ARTIKEL 6, STK. 2

1. Medlemsstaterne meddeler Kommissionen følgende oplysninger om hver af de kompetente myndigheder eller organer, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap:

   a) navnet på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   b) registreringsnummeret på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   c) e-mailadressen og telefonnummeret på den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap

   d) et eller flere certifikater, der kan anvendes til at kontrollere det elektroniske segl, der er genereret af den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet eller EU-parkeringskortet for personer med handicap, og for hvilke de certificerede identitetsdata omfatter udstederens navn og registreringsnummer, jf. henholdsvis litra a) og b)

   e) den URL, hvor udstederen offentliggør oplysninger om gyldighedsstatus for de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap.

2. Medlemsstaterne kan meddele Kommissionen følgende oplysninger om hver af de kompetente myndigheder eller hvert af de kompetente organer, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap:

   a) URL'en på den webside, der indeholder de politikker, vilkår og betingelser, der finder anvendelse på leveringen og brugen af de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap, som udstedes af den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af disse kort

   b) hvis det er relevant, URL'en på den webside, der indeholder yderligere oplysninger om den kompetente myndighed eller det kompetente organ, der har ansvaret for at udstede de fysiske udgaver af EU-handicapkortet og EU-parkeringskortet for personer med handicap.

BILAG IV

TEKNISKE SPECIFIKATIONER FOR INDDRAGELSESLISTEN OVER DE FYSISKE UDGAVER AF EU-HANDICAPKORTET ELLER EU-PARKERINGSKORTET FOR PERSONER MED HANDICAP

1. Med henblik på dette bilag skal identifikatoren svare til den inddragelsesidentifikator (RID), der er defineret i bilag I, punkt 6, og bilag II, punkt 6.

2. Der opstilles en liste over inddragne kort i form af en identifikatorliste-token (identifier list token) i CWT-format (RFC 8392, afdeling 7) i overensstemmelse med punkt 5.2 i »token status list specification« (draft-ietf-oauth-status-list-14) med følgende ændringer:

   a) Værdien af typekravet skal være »application/identifierlist+cwt«

   b) Kravet »udløbstidspunkt« (expiration time claim) skal forefindes

   c) Der må ikke forefindes et StatusListe-krav i CWT-kravene

   d) Identikatorliste-strukturen, der er defineret i punkt 3, skal være til stede som et krav i de CWT-krav, der er fastsat ved hjælp af 65530-nøglen

   e) CWT'en skal være et COSE_Sign1-objekt, der med henblik på beregning af underskriften bruger en underskrift-salgoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)

   f) CWT'en skal med henblik på kontrol af underskriften på listen over inddragne kort indeholde den x5chain-parameter, der er defineret i RFC 9360 (afdeling 2), i den beskyttede header, der indeholder certifikatet eller kæden af certifikater

   g) den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten (draft-ietf-oauth-status-list-14), kan anvendes til certifikatet til underskrivelse af identifikatorlisten, og det anbefales, at kontrollørerne understøtter den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten, og at den udstedende myndigheds infrastrukturer ikke sætter feltet for den udvidede nøgleanvendelses til kritisk, når de anvender den udvidede nøgleanvendelse OID, der er fastsat i specifikationen for tokenstatuslisten.

3. Identifikatorlistens struktur skal være en CBOR-struktur med følgende Concise Data Definition Language (CDDL):

```
IdentifierList = {

  »identifiers« : { * Identifier => IdentifierInfo },

  ? »aggregation_uri« : Aggregation_uri,

  * tstr => RFU

}

IdentifierInfo = {

  (tstr / int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```