Amtsblatt
der Europäischen Union

DE
Reihe L

2026/1436

12.11.2026

DELEGIERTE VERORDNUNG (EU) 2026/1436 DER KOMMISSION

vom 1. Juli 2026

zur Ergänzung der Richtlinie (EU) 2024/2841des Europäischen Parlaments und des Rates im Hinblick auf die Festlegung des QR-Codes für die physische Version des Europäischen Behindertenausweises sowie die Festlegung des QR-Codes und gemeinsamer technischer Spezifikationen, mit denen die Sicherheit der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen gewährleistet wird, und Interoperabilitätsfragen

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2024/2841 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 zur Einführung des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen ([1]), insbesondere auf Artikel 7 Absatz 7 und Artikel 8 Absatz 7,

in Erwägung nachstehender Gründe:

(1) In der Richtlinie (EU) 2024/2841 sind die Vorschriften für die Ausstellung des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen sowie gemeinsame Mustervorlagen für diese Ausweise festgelegt. Gemäß Artikel 7 Absatz 2 und Artikel 8 Absatz 2 der Richtlinie (EU) 2024/2841 müssen die von einem Mitgliedstaat ausgestellten Europäischen Behindertenausweise und Europäischen Parkausweise für Menschen mit Behinderungen in allen anderen Mitgliedstaaten anerkannt werden.

(2) Die in Artikel 7 Absatz 7 und Artikel 8 Absatz 7 der Richtlinie (EU) 2024/2841 festgelegten Befugnisse dienen demselben Zweck, nämlich der Prävention und Bekämpfung von Betrug, der Sicherheit der physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen, auch durch geeignete Vorkehrungen zum Schutz personenbezogener Daten gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]), sowie der Gewährleistung der Interoperabilität. Da der Gegenstand und die Ziele der Befugnisübertragungen weitgehend übereinstimmen, ist es sinnvoll, Vorschriften zur Ergänzung der Richtlinie (EU) 2024/2841 in Bezug auf diese Aspekte in einem einzigen delegierten Rechtsakt festzulegen.

(3) Gemäß der Richtlinie (EU) 2024/2841 sollen die physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen einen QR-Code als ein auf dem Stand der Technik befindliches digitales Merkmal enthalten, das elektronische Mittel zur Prävention und Bekämpfung von Betrug verwendet. QR-Codes sind daher ein verbindliches digitales Merkmal, das auf alle physischen Ausweise aufgedruckt werden muss. Um für ein einheitliches Vorgehen bei der Erstellung und Verwendung der QR-Codes durch die Mitgliedstaaten zu sorgen, sollte die Kommission technische Spezifikationen für die QR-Codes, einschließlich ihres Inhalts, festlegen.

(4) Der Europäische Parkausweis für Menschen mit Behinderungen wird alle bisherigen Parkausweise für Menschen mit Behinderungen ersetzen, die gemäß der Empfehlung 98/376/EG des Rates ([3]) ausgestellt wurden. Die vorgenannte Empfehlung wurde nicht an die technologischen und digitalen Entwicklungen angepasst, und in den Mitgliedstaaten traten Probleme mit Betrug und Fälschung auf. Daher ist es notwendig, die Merkmale festzulegen, mit denen die Sicherheit der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen gewährleistet wird, wobei die Besonderheiten des Ausweises, wie die Tatsache, dass er in der Regel hinter der Windschutzscheibe des Fahrzeugs angebracht ist, zu berücksichtigen sind.

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

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Empfehlung 98/376/EG des Rates vom 4. Juni 1998 betreffend einen Parkausweis für Behinderte (ABl. L 167 vom 12.6.1998, S. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Es sollten verbindliche gemeinsame technische Spezifikationen eingeführt werden, um die Sicherheit der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen zu gewährleisten. Der Druck des Ausweises auf einem geeigneten Material, z. B. Polycarbonat, und die Verwendung eines beugungsoptisch variablen Bildelements würden einen wirksamen Schutz vor Fälschung und Verfälschung bieten. Kopierschutzelemente würden die Sicherheit weiter erhöhen, da sie die Erkennung von Ausweisduplikaten ermöglichen, indem sie verborgene Texte oder Muster enthalten, die auf einer Fotokopie oder einem Scan des Ausweises sichtbar werden. Diese Merkmale sind zu verwenden, ohne das Format der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen gemäß Anhang II der Richtlinie (EU) 2024/2841, einschließlich des optischen Erscheinungsbildes des Ausweises, zu verändern.

(6) Zusätzlich zu dem QR-Code und anderen verbindlichen technischen Spezifikationen, die in dieser Verordnung festgelegt sind, sollten die Mitgliedstaaten die Möglichkeit haben, optionale digitale oder physische Sicherheitsmerkmale auf der Grundlage gemeinsamer technischer Spezifikationen, die in dieser Verordnung festgelegt sind, in die physische Version des Europäischen Parkausweises für Menschen mit Behinderungen aufzunehmen, um dessen Sicherheit zu erhöhen. Enthalten optionale digitale Merkmale mehr personenbezogene Daten als in den physischen Versionen der Ausweise vorgesehen, so ist der Zugang zu diesen Daten gemäß Anhang II Nummer 3 Buchstabe b der Richtlinie (EU) 2024/2841 auf die Behörden der ausstellenden Mitgliedstaaten und nur auf befugte Nutzer zu beschränken. Um einen harmonisierten Rahmen für Sicherheitsmerkmale in allen Mitgliedstaaten aufrechtzuerhalten, sollte die Liste der optionalen Merkmale abschließend sein. Ferner sollten die Mitgliedstaaten sicherstellen, dass die Integration eines oder mehrerer optionaler digitaler oder physischer Sicherheitsmerkmale weder die Anerkennung gültiger Ausweise aus anderen Mitgliedstaaten noch die Interoperabilität und Funktionalität der verbindlichen technischen Spezifikationen beeinträchtigt.

(7) Die physische Version des Europäischen Parkausweises für Menschen mit Behinderungen kann als optionales digitales Sicherheitsmerkmal einen Chip zur Funkwellenidentifikation (RFID) enthalten. Bei RFID werden elektromagnetische Wellen oder die elektromagnetische Nachfeldkopplung im Funkbereich des Frequenzspektrums für die Kommunikation von oder zu einem RFID-Tag mithilfe verschiedener Modulations- oder Kodierungstechniken oder nur für das Auslesen der Kennung eines RFID-Tags oder anderer darin gespeicherter Daten genutzt ([4]). RFID-Chips können den Schutz vor Fälschung und Manipulation erhöhen, indem sie ausweisbezogene Daten sicher speichern oder übermitteln. Die physische Version des Europäischen Parkausweises für Menschen mit Behinderungen kann auch optisch variable Farbe oder vom Blickwinkel abhängige Farbe enthalten. Diese Farben bieten einen ausreichenden Schutz gegen Kopieren und Manipulation des Ausweises, ohne dass eine Personalisierung erforderlich ist. Zum Schutz der Ausweisdaten vor Fälschungs- und Verfälschungsversuchen kann der Text der Datenfelder mittels Lasergravurtechnik in das Grundmaterial des Ausweises eingearbeitet werden. Physische Sicherheitsmerkmale, unabhängig davon, ob sie in dieser Verordnung als verbindlich oder optional festgelegt sind, die nicht sichtbar sind oder nach bestimmten Manipulationen sichtbar werden, stehen nicht im Widerspruch zu dem in Anhang II der Richtlinie (EU) 2024/2841 festgelegten Format des Europäischen Parkausweises für Menschen mit Behinderungen.

(8) Technologische Fortschritte, Parkraumüberwachungssysteme und Sicherheitsrisiken entwickeln sich ständig weiter. Der Stand der Technik und die Verwendung des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen entwickeln sich weiter, was sowohl auf die Rückmeldungen der Nutzer als auch auf den technologischen Fortschritt zurückzuführen ist; dies gilt auch für Betrugs- und Fälschungstechniken, was zu immer neuen Sicherheitsherausforderungen führt. Daher könnten neue technologische Lösungen, darunter solche, die in Parkraumüberwachungssystemen eingesetzt werden, sowie Sicherheits- und Betrugsbekämpfungserfordernisse Änderungen an der Sicherheits- und Betrugsbekämpfungsarchitektur der Ausweise erforderlich machen, unter anderem durch eine Aktualisierung der Kategorisierung der digitalen Merkmale als verbindlich oder optional. Je nach technologischer Entwicklung kann es notwendig werden, diese Verordnung zu aktualisieren.

(9) Um sicherzustellen, dass die physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen in allen Mitgliedstaaten nahtlos verwendet werden können, muss die Interoperabilität der digitalen Merkmale auf den physischen Ausweisen, insbesondere der QR-Codes, gewährleistet werden. Die Interoperabilität sollte die Überprüfung der Echtheit und Gültigkeit der physischen Versionen der Ausweise durch Prüfstellen ermöglichen, d. h. durch jede natürliche oder juristische Person, die die Gültigkeit und Echtheit der physischen Versionen der Ausweise überprüft, z. B. mittels einer Überprüfungssoftware. Zu diesem Zweck müssen Bestimmungen über die Interoperabilität festgelegt werden, damit grenzüberschreitende Überprüfungen der physischen Versionen der Ausweise in kohärenter und verlässlicher Weise durchgeführt werden können.

([4]) Empfehlung 2009/387/EG der Kommission vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen (ABl. L 122 vom 16.5.2009, S. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) Zur Sicherstellung der Integrität und der Herkunft der Daten in den QR-Codes auf den physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen sollten diese Daten mit einem qualifizierten elektronischen Siegel im Sinne von Artikel 3 Nummer 27 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([5]) besiegelt werden. Mit dem QR-Code wird die Echtheit und Gültigkeit des physischen Ausweises bestätigt, wenn er mit den Überprüfungsparametern abgeglichen wird; der QR-Code an sich sollte nicht den Behindertenstatus oder den Anspruch auf bestimmte Dienstleistungen aufgrund einer Behinderung bescheinigen.

(11) Zur Erleichterung der Interoperabilität und der Einrichtung eines vertrauenswürdigen und sicheren Überprüfungssystems für die physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen in der gesamten Union sollten Verfahren für die Meldung und Veröffentlichung von Informationen eingerichtet werden. Diesbezüglich und um die Überprüfung zu ermöglichen, ob die physischen Versionen der Ausweise von einer zuständigen Behörde oder Stelle ausgestellt wurden, sollten die Mitgliedstaaten die für den Überprüfungsprozess erforderlichen Informationen bereitstellen, insbesondere die Informationen, die zur Überprüfung des qualifizierten elektronischen Siegels erforderlich sind. Daher sollten die Mitgliedstaaten verpflichtet werden, der Kommission die für die Ausstellung der physischen Versionen der Ausweise zuständigen Behörden oder Stellen (Aussteller der Ausweise) sowie die einschlägigen administrativen und technischen Informationen zu diesen Ausweisen mitzuteilen. Die der Kommission mitzuteilenden Informationen sollten sich auf die Informationen beschränken, die für die Einrichtung interoperabler Mechanismen zur Überprüfung der Gültigkeit und Echtheit der physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen erforderlich sind. Die Kommission sollte den Zugang der Öffentlichkeit zu diesen Informationen sicherstellen.

(12) Ferner sollten im Falle eines Widerrufs des Ausweises die Informationen über den Widerruf des Ausweises unverzüglich zur Verfügung gestellt werden, damit die Prüfstellen die Gültigkeit des Ausweises überprüfen können. Zu diesem Zweck sollten die Aussteller der Ausweise Listen mit Informationen über den Widerrufsstatus aller Ausweise, die sie vor ihrem Ablaufdatum widerrufen haben (Widerrufslisten), führen und zeitnah veröffentlichen. Bei einer solchen Veröffentlichung sollte die Privatsphäre gewahrt werden und sollten die personenbezogenen Daten der Ausweisinhaber geschützt werden. Darüber hinaus sollten Widerrufslisten keine anderen personenbezogenen Daten als die eindeutigen Widerrufskennungen enthalten und gemäß den technischen Spezifikationen unter einem spezifischen Uniform Resource Identifier (URI) veröffentlicht werden, damit eine interoperable Überprüfung sichergestellt werden kann.

(13) Um den QR-Code zu lesen und die Echtheit und Gültigkeit der physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen zu überprüfen, kann auf nationaler Ebene individuell angepasste Überprüfungssoftware verwendet werden. Die Kommission kann dieses Verfahren unterstützen, indem sie einen gemeinsamen Beispiel-Quellcode zum Auslesen der in den QR-Codes enthaltenen Daten sowie zur Durchführung der wichtigsten Schritte des Überprüfungsverfahrens bereitstellt, der als Grundlage für die Überprüfungssoftware in den Mitgliedstaaten dienen kann. Bei jeder Überprüfungssoftware sollte dieselbe Logik zur Überprüfung der Vertrauenskette anhand derselben Vertrauensinfrastruktur angewendet werden, wodurch das Auslesen der vom ausstellenden Mitgliedstaat in den Ausweisen kodierten Daten ermöglicht wird. Überdies sind in Anhang I der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates ([6]) die Barrierefreiheitsanforderungen festgelegt, denen die Mitgliedstaaten gegebenenfalls entsprechen müssen.

(14) Die Union ist sich der Dynamik des technologischen Fortschritts und der sich entwickelnden Cybersicherheitsbedrohungen bewusst und hat sich verpflichtet, dafür zu sorgen, dass die in ihrem Rechtsrahmen eingesetzten kryptografischen Mechanismen wirksam und sicher bleiben. Angesichts dieser Verpflichtung ist es wichtig, kryptografische Standards zu übernehmen, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung befürwortet und über die Agentur der Europäischen Union für Cybersicherheit (ENISA) verbreitet werden.

(15) Für die Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung gilt die Verordnung (EU) 2016/679. Insbesondere ist die Überprüfung der QR-Codes auf den physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen mit der Verarbeitung personenbezogener Daten verbunden. Daher sollten gegebenenfalls geeignete Datenschutzgarantien festgelegt werden, um den Schutz der in den QR-Codes enthaltenen personenbezogenen Daten gemäß der Verordnung (EU) 2016/679 sicherzustellen. Durch die in dieser Verordnung vorgesehenen allgemeinen Sicherheitsvorkehrungen sollte auch der Schutz der in den QR-Codes enthaltenen personenbezogenen Daten sichergestellt werden. Darüber hinaus sollten die in den QR-Codes enthaltenen personenbezogenen Daten auf das für die Zwecke dieser Verordnung unbedingt notwendige Maß beschränkt werden. Zudem sollte die Speicherung der Daten nach Abschluss der Überprüfung verboten werden. Außerdem muss für eine angemessene Sicherheit der Widerrufslisten gesorgt werden.

([5]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151 vom 7.6.2019, S. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) Die Kommission hat im Rahmen der Ausarbeitung dieser Verordnung gemäß Artikel 14 Absatz 4 der Richtlinie (EU) 2024/2841 im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([7]) enthaltenen Grundsätzen Menschen mit Behinderungen und ihre Vertretungsorganisationen sowie die von den einzelnen Mitgliedstaaten benannten Sachverständigen konsultiert.

(17) Der Europäische Behindertenausweis und der Europäische Parkausweis für Menschen mit Behinderungen stellen einen transeuropäischen digitalen öffentlichen Dienst im Sinne der Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates ([8]) dar. Dementsprechend wurde eine Interoperabilitätsbewertung durchgeführt, deren Ergebnis auf dem in Artikel 8 der Verordnung (EU) 2024/903 genannten Portal für ein interoperables Europa zu veröffentlichen ist.

(18) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([9]) zu dieser Verordnung konsultiert und hat am 12. Mai 2026 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand und Anwendungsbereich

Diese Verordnung enthält Bestimmungen zur Ergänzung der Richtlinie (EU) 2024/2841 in Bezug auf:

a) die Festlegung des QR-Codes für die physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen, einschließlich geeigneter Vorkehrungen zum Schutz personenbezogener Daten;

b) die Festlegung gemeinsamer verbindlicher und optionaler technischer Spezifikationen, mit denen die Sicherheit der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen gewährleistet wird;

c) die Festlegung von Interoperabilitätsanforderungen, um sicherzustellen, dass QR-Codes auf den physischen Versionen von in einem Mitgliedstaat ausgestellten Europäischen Behindertenausweisen oder Europäischen Parkausweisen für Menschen mit Behinderungen in einem anderen Mitgliedstaat zuverlässig gelesen und überprüft werden können.

Artikel 2

QR-Code auf der physischen Version des Europäischen Behindertenausweises

Die Spezifikationen für den auf der physischen Version des Europäischen Behindertenausweises anzubringenden QR-Code sind in Anhang I festgelegt.

Artikel 3

QR-Code auf der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen

Die Spezifikationen für den auf der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen anzubringenden QR-Code sind in Anhang II festgelegt.

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

([8]) Verordnung (EU) 2024/903 des Europäischen Parlaments und des Rates vom 13. März 2024 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Verordnung für ein interoperables Europa) (ABl. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 4

Verbindliche gemeinsame technische Spezifikationen für den Europäischen Parkausweis für Menschen mit Behinderungen

(1) Die physischen Versionen des Europäischen Parkausweises für Menschen mit Behinderungen müssen den folgenden gemeinsamen technischen Spezifikationen entsprechen:

a) Sie bestehen aus einem Material, das vor Delamination schützt und geeignet ist, die in Anhang II der Richtlinie (EU) 2024/2841 festgelegten Anforderungen sowie andere in diesem Artikel aufgeführte verbindliche gemeinsame technische Spezifikationen zu erfüllen.

b) Im Schichtenaufbau der physischen Versionen ist ein beugungsoptisch variables Bildelement enthalten, das bei Betrachtung des Ausweises aus einem bestimmten Winkel sichtbar wird.

c) Sie enthalten ein Kopierschutzelement, das auf einer Fotokopie oder einem Scan des Ausweises sichtbar wird.

(2) Das in Absatz 1 Buchstabe b genannte beugungsoptisch variable Bildelement ist auf der Vorderseite der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen über einem oder mehreren der Datenfelder auf der linken Seite anzubringen. Es muss etwa 20 mm hoch und 20 mm breit sein. Das auf dem Element abgebildete Bild enthält eine stilisierte Landkarte des ausstellenden Mitgliedstaats oder die Kennbuchstaben des ausstellenden Mitgliedstaats, umrahmt von einem Kreis von zwölf Sternen, der die Union symbolisiert.

(3) Das in Absatz 1 Buchstabe c genannte Kopierschutzelement ist auf der Vorderseite der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen oberhalb der Datenfelder links oder rechts außerhalb des QR-Codes und seiner Ruhezone anzubringen. Es enthält verborgene Texte oder Muster, die auf einer Fotokopie oder einem Scan des Ausweises sichtbar werden. Enthält das Kopierschutzelement einen verborgenen Text, so besteht dieser aus den Worten „COPY“ („KOPIE“) oder „VOID“ („UNGÜLTIG“) und einer Übersetzung davon in eine oder mehrere Amtssprachen des ausstellenden Mitgliedstaats. Enthält das Kopierschutzelement ein verborgenes Muster, so besteht dieses aus horizontalen oder vertikalen Linien.

Artikel 5

Optionale technische Spezifikationen und Merkmale für die Sicherheit des Europäischen Parkausweises für Menschen mit Behinderungen

(1) Zusätzlich zu den verbindlichen gemeinsamen technischen Spezifikationen nach Artikel 4 dürfen die Mitgliedstaaten nur die in diesem Artikel festgelegten optionalen technischen Spezifikationen und Merkmale verwenden.

(2) Physische Versionen des Europäischen Parkausweises für Menschen mit Behinderungen können einen Chip zur Funkwellenidentifikation (RFID) enthalten. Der RFID-Chip ist ein elektronisches Mittel zur Prävention und Bekämpfung von Betrug und dient als zusätzliches Mittel zur Überprüfung der Echtheit und/oder Gültigkeit einer physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen auf nationaler Ebene. Durch den RFID-Chip darf die Funktion des QR-Codes auf dem Ausweis nicht beeinträchtigt werden.

(3) Jeder RFID-Chip nach Absatz 2 muss den folgenden Spezifikationen entsprechen:

a) Er ist passiv.

b) Er ist auf der Vorderseite rechts physisch in die Struktur des Ausweises integriert.

c) Er ist logisch mit dem QR-Code-Datensatz verknüpft und enthält dieselbe Widerrufskennung (RID), die im QR-Code kodiert ist.

d) Das RFID-Merkmal unterstützt das Ablesen in einem Abstand von etwa 1 Meter oder mehr, wenn dies für den Wirkbetrieb erforderlich ist, es ist jedoch nicht für ein zuverlässiges Ablesen in einem Abstand von mehr als 5 Metern unter Referenzprüfbedingungen ausgelegt.

e) Nach Ausstellung des Ausweises wird der Schreibzugriff auf den RFID-Chip oder auf den entsprechenden Datenbereich verhindert oder von der ausstellenden Behörde anderweitig kontrolliert.

f) Er ist so konzipiert und konfiguriert, dass das Risiko des Klonens, des Austauschs, der unbefugten Veränderung und des unbefugten Überschreibens so gering wie möglich gehalten wird.

g) Er entspricht den Anforderungen der Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates ([10]).

h) Zusätzlich zu der in Buchstabe c genannten RID können auf dem RFID-Chip auch nur eines oder mehrere der folgenden Elemente gespeichert werden:

i) Daten, die im QR-Code der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen kodiert sind;

ii) amtliches Kennzeichen des Fahrzeugs;

iii) kryptografische Überprüfungsdaten.

(4) Die Vorderseite der physischen Versionen des Europäischen Parkausweises für Menschen mit Behinderungen kann eines oder mehrere der folgenden Merkmale enthalten:

a) das Rollstuhlsymbol auf der linken Seite oder die Aufschrift „Europäischer Parkausweis für Menschen mit Behinderungen“ in Englisch und einer oder mehreren Amtssprachen des ausstellenden Mitgliedstaats auf der rechten Seite, gedruckt mit optisch variabler Farbe oder vom Blickwinkel abhängiger Farbe, die bei Betrachtung aus verschiedenen Winkeln wechselnde Farben erkennen lässt;

b) Lasergravurtechnik, bei deren Verwendung der Laser in die Schichten des Ausweises eindringt, um den Text in die Datenfelder zu drucken.

(5) Die Einführung der in diesem Artikel genannten optionalen technischen Spezifikationen und Merkmale berührt nicht die Anerkennung der in anderen Mitgliedstaaten ausgestellten gültigen Ausweise in dem Mitgliedstaat, der diese Merkmale für die von ihm ausgestellten Ausweise eingeführt hat.

Artikel 6

Interoperabilitätsfragen

(1) Die im QR-Code enthaltenen Informationen werden mit einem qualifizierten elektronischen Siegel im Sinne von Artikel 3 Nummer 27 der Verordnung (EU) Nr. 910/2014 besiegelt.

(2) Jeder Mitgliedstaat übermittelt der Kommission Informationen über die für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörden oder Stellen (im Folgenden „Aussteller der Ausweise“) sowie alle späteren Aktualisierungen dieser Informationen gemäß Anhang III. Die Kommission stellt den Zugang der Öffentlichkeit zu diesen Informationen sicher.

(3) Die Aussteller der Ausweise führen und veröffentlichen unter einem Uniform Resource Identifier (URI), der der Kommission mitgeteilt wird, aktuelle Widerrufslisten mit Informationen über den Widerrufsstatus aller Ausweise, die sie gemäß den technischen Spezifikationen in Anhang IV widerrufen haben. Informationen über den Widerruf werden innerhalb von 24 Stunden nach dem Widerruf veröffentlicht.

(4) Die Mitgliedstaaten können Überprüfungssoftware einsetzen, um die Echtheit und Gültigkeit der physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen zu überprüfen.

(5) Verwenden die Mitgliedstaaten Überprüfungssoftware zur Überprüfung der Echtheit und Gültigkeit der physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen, so muss diese Software geeignet sein, die Echtheit und Gültigkeit eines Ausweises durch Überprüfung des elektronischen Siegels und des Widerrufsstatus des Ausweises zu überprüfen. Diese Überprüfungssoftware liest die im QR-Code des Ausweises kodierten personenbezogenen Daten gemäß den Anhängen I und II und stellt sie visuell dar, um einen Vergleich mit den in den entsprechenden Datenfeldern des Ausweises sichtbaren Daten zu ermöglichen und einen Hinweis auf den Gültigkeitsstatus des Ausweises zu geben.

([10]) Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Artikel 7

Sicherheitsvorkehrungen zum Schutz personenbezogener Daten

(1) Die in den QR-Codes auf den physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen enthaltenen personenbezogenen Daten sind auf das für die Überprüfung der Echtheit und Gültigkeit der Ausweise unbedingt notwendige Maß gemäß den Anhängen I und II beschränkt.

(2) Nach Abschluss der Überprüfung der Echtheit und Gültigkeit einer physischen Version des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen durch die Prüfstellen dürfen die in den QR-Codes enthaltenen Daten von den Prüfstellen nicht gespeichert werden.

(3) Die Überprüfung eines QR-Codes auf einer physischen Version des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen darf nicht dazu führen, dass die für die Ausstellung des Ausweises zuständige Behörde oder Stelle über diese Überprüfung informiert wird.

(4) Die in einer nach Artikel 6 Absatz 3 veröffentlichten Widerrufsliste enthaltenen Informationen beschränken sich auf die Widerrufskennung der widerrufenen Ausweise.

(5) Die für die Veröffentlichung der Widerrufslisten gemäß Artikel 6 Absatz 3 zuständige Behörde oder Stelle stellt sicher, dass bei der Verarbeitung der in den Widerrufslisten enthaltenen personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewendet werden.

(6) Beschließt ein Mitgliedstaat, in die physische Version des Europäischen Parkausweises für Menschen mit Behinderungen einen RFID-Chip aufzunehmen, finden für die Verarbeitung der in diesem Chip enthaltenen personenbezogenen Daten die Absätze 2 bis 3 Anwendung. Die auf dem RFID-Chip gespeicherten personenbezogenen Daten sind auf das für die Überprüfung der Echtheit und/oder Gültigkeit der Ausweise unbedingt notwendige Maß nach Artikel 5 Absatz 3 beschränkt.

Werden in einem Mitgliedstaat auf dem RFID-Chip personenbezogene Daten im Sinne von Artikel 5 gespeichert, die in der physischen Version des Europäischen Parkausweises für Menschen mit Behinderungen gemäß Anhang II der Richtlinie (EU) 2024/2841 nicht vorgesehen sind, so ist der Zugang zu diesen Daten auf die Behörden des ausstellenden Mitgliedstaats und nur auf befugte Nutzer beschränkt.

Artikel 8

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 1. Juli 2026

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

QR-CODE-SPEZIFIKATIONEN FÜR DIE PHYSISCHE VERSION DES EUROPÄISCHEN BEHINDERTE-NAUSWEISES

1. **Format des QR-Codes für die physische Version des Europäischen Behindertenausweises**

a) **Format QR-Code Modell 2**, gemäß den internationalen QR-Code-Spezifikationen ISO/IEC 18004:2024 oder gleichwertig.

b) **Fehlerkorrektur-Level M** (15 % Redundanz), wodurch sichergestellt wird, dass ein gedruckter QR-Code unempfindlich gegenüber Kratzern oder teilweisen Beschädigungen ist.

c) **Kodierungsmodus**: Die QR-Nutzdaten müssen aus der kombinierten issuerSigned Concise Binary Object Representation (CBOR)-Struktur und dem entsprechenden issuerAuth COSE_Sign1-Signaturobjekt, wie in der CBOR-Objektsignatur und -verschlüsselung (COSE, RFC 9052 Abschnitte 3.1, 4.2 und 4.4) definiert, bestehen und dem mDOC-Datenmodellmuster für issuerSigned-Elemente entsprechen, jedoch angepasst für die Verwendung auf statischen physischen Ausweisen. Der issuerAuth muss ein COSE_Sign1-Objekt mit alg = ES256 und einem geschützten Header sein, der x5t (den in RFC 9360 (Abschnitt 2) definierten Hash-Header-Parameter des COSE X.509-Zertifikats; aus Gründen der Interoperabilität muss der in x5t verwendete Hash-Algorithmus SHA-256 sein) enthält.

d) Vor der Kodierung des QR-Codes ist das kombinierte CBOR/COSE-Objekt **im ZLIB-Format** (RFC 1950 Abschnitt 2.2) **mit dem Deflate**-Algorithmus (RFC 1951 Abschnitte 3.2 und 4) **zu komprimieren**. Das resultierende komprimierte Byte-Array muss im **QR-Code-Byte-Modus** kodiert werden, um sicherzustellen, dass die binären CBOR/COSE-Nutzdaten und die Interoperabilität der Scanner in vollem Umfang unterstützt werden.

Für alle in den QR-Nutzdaten enthaltenen Textfelder müssen die Aussteller die Zeichen innerhalb des CBOR-Text-Strings als Unicode UTF-8 verschlüsseln. Auf signierte Nutzdaten darf keine Transliteration angewendet werden. Aus Gründen der Interoperabilität müssen Aussteller vor der Signatur auf alle Textfelder die Unicode-Normalisierungsform C (NFC) anwenden.

e) **Präfix**: Der QR-String des Europäischen Behindertenausweises muss mit „ED1:MDOC:“ beginnen. Damit werden die Art des Ausweises und das Kodierungsprofil identifiziert. Bei den Präfixen wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen vorhanden sein. Unbekannte oder nicht unterstützte Präfixe führen zur Ablehnung. Das Präfix und die komprimierten Nutzdaten sind als ein einzelnes Byte-Modus-Datensegment im QR-Code zu kodieren.

f) **Die Größe des Moduls muss mindestens 0,25 mm betragen**, um die Lesbarkeit auf gedruckten Ausweisen sicherzustellen.

g) Es darf sich **höchstens um Version 20 handeln**; mit bis zu 97 × 97 Modulen je Seite.

2. **Spezifikationen für die Generierung von Signaturen des Europäischen Behindertenausweises**

Mit dem qualifizierten elektronischen Siegel (QSeal), das zum Besiegeln von QR-Codes des Europäischen Behindertenausweises verwendet wird, wird sichergestellt, dass die kodierten Daten von der autorisierten ausstellenden Behörde stammen und nicht verändert wurden.

a) **Signaturalgorithmus**: Der Signaturalgorithmus ist ES256 (Elliptic Curve Digital Signature Algorithm (ECDSA) mit SHA-256 unter Verwendung der P-256-Kurve), wie in RFC 9053 (Abschnitt 2.1) definiert; in COSE wird der Algorithmus durch den Header-Parameter „alg“ in RFC 9052 (Abschnitt 3.1) identifiziert.

b) **Signierschlüssel**: Die QR-Nutzdaten müssen mit dem privaten Schlüssel signiert werden, der einem qualifizierten Zertifikat für elektronische Siegel (QSealC) entspricht.

c) **COSE-Struktur**: Der Signaturcontainer muss ein COSE_Sign1-Objekt sein. Der geschützte Header muss alg (ES256) und x5t (den in RFC 9360 (Abschnitt 2) definierten Hash-Header-Parameter des COSE X.509-Zertifikats; aus Gründen der Interoperabilität muss der in x5t verwendete Hash-Algorithmus SHA-256 sein) enthalten. Die Überprüfung erfolgt anhand des x5t-Werts, um das entsprechende Zertifikat im lokal zwischengespeicherten Truststore der Prüfstelle zu lokalisieren, der auf der Grundlage der Informationen aus der Vertrauensliste erstellt wurde; anschließend werden die Zertifikatskette und der Zertifikatsstatus gemäß dem eIDAS-Vertrauensrahmen überprüft.

d) **Signaturstandard**: Die QR-Code-Nutzdaten müssen als COSE_Sign1-Objekt gemäß RFC 9052 (Abschnitt 4), CBOR-Objektsignatur und -verschlüsselung, signiert werden. Das COSE_Sign1-Objekt muss in issuerAuth enthalten sein und ohne CBOR-Tag für COSE_Sign1 kodiert werden. Das Nutzdatenfeld des COSE_Sign1-Objekts ist abzutrennen und als CBOR null zu kodieren. Für die Erstellung und Überprüfung von Signaturen bestehen die externen Nutzdaten aus der deterministischen CBOR-kodierten Struktur, die den docType-Wert und den issuerSigned-Wert aus der CBOR-Map der obersten Ebene enthält.

e) **Hash-Algorithmus**: SHA-256 muss als Teil von ES256 für die Erstellung von Signaturen und die Überprüfung der Integrität verwendet werden.

f) **Kodierung**: Die Nutzdaten müssen gemäß den COSE- und mDOC-Spezifikationen mit CBOR (RFC 8949 Abschnitt 4.2) kodiert werden, um die Kodierung und Reproduzierbarkeit der signierten Daten sicherzustellen.

3. **Druckspezifikationen**

a) **Ruhezone**: Der QR-Code muss von allen Seiten mit einem deutlichen Abstand von **vier Modulen** umgeben sein, ohne jegliche Bedruckung, Muster oder Hintergründe.

b) **Kontrast**: Der QR-Code muss auf weißem Hintergrund gedruckt werden und ein Kontrastverhältnis von mindestens **4:1** aufweisen, um eine gute Lesbarkeit bei unterschiedlichen Lichtverhältnissen sicherzustellen.

c) Der QR-Code ist unter Verwendung der in Anhang I der Richtlinie (EU) 2024/2841 festgelegten Farbe zu drucken, die einen maximalen Kontrast gewährleistet.

d) **Platzierung und Größe**: Der QR-Code einschließlich der Ruhezone muss 26,25 mm × 26,25 mm groß sein und sich auf der Rückseite des Ausweises in der rechten unteren Ecke befinden. Der QR-Code darf höchstens der Version 20 (97 × 97 Module) entsprechen und muss eine Modulgröße von mindestens 0,25 mm aufweisen.

Der QR-Code einschließlich der Ruhezone ist mindestens 5 mm von der rechten Kante und mindestens 5 mm von der Unterkante der Karte entfernt anzubringen.

4. **Daten im QR-Code des Europäischen Behindertenausweises**

Der QR-Code muss einen minimalen, offline überprüfbaren Datensatz enthalten, der dem in Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 festgelegten Grundsatz der Datenminimierung entspricht. Die Nutzdaten müssen wie folgt strukturiert sein:

a) Die Attribute der Ausweise werden in CBOR innerhalb eines issuerSigned-Objekts kodiert.

b) Die Struktur wird vom QSeal der ausstellenden Behörde als issuerAuth (COSE_Sign1, ES256, einschließlich x5t, dem Hash-Header-Parameter des COSE X.509-Zertifikats) verpackt und signiert.

c) Das resultierende CBOR/COSE-Objekt wird gemäß Nummer 1 Buchstabe d dieses Anhangs komprimiert. Die QR-Code-Nutzdaten bestehen aus dem Präfix „ED1:MDOC:“, gefolgt von dem resultierenden komprimierten Byte-Array, und die vollständigen Nutzdaten werden unter Verwendung des Byte-Modus als ein einziges QR-Code-Datensegment kodiert.

Der Dateninhalt besteht aus einer Teilmenge der sichtbaren Daten aus den in Anhang I der Richtlinie (EU) 2024/2841 aufgeführten Feldern auf der Vorderseite des Ausweises (Vor- und Nachname, Seriennummer des Ausweises, Ablaufdatum) sowie der Widerrufskennung, der elektronischen Signatur und den Schema-Informationen.

Die **elektronische Signatur** muss Folgendes enthalten:

i) issuerAuth – ein COSE_Sign1-Objekt, das mit dem **privaten QSealC-Schlüssel** der ausstellenden Behörde signiert ist,

ii) den geschützten Header mit alg = ES256 (Signaturalgorithmus) und x5t (Hash-Header-Parameter des COSE X.509-Zertifikats).

5. **Optionale Daten**

Der QR-Code darf keine optionalen Daten enthalten.

6. **Widerrufskennung (RID)**

Zusätzlich zur sichtbaren Seriennummer des Ausweises muss der QR-Code eine spezielle Widerrufskennung (RID) enthalten.

Die RID wird zur Bestimmung des Widerrufsstatus und zur Verwaltung der Widerrufsliste verwendet. Die RID darf nicht auf den Ausweis gedruckt werden und den Prüfstellen nicht angezeigt werden.

6.1. *Anforderungen an die RID*

Die RID

a) muss in den signierten QR-Nutzdaten enthalten sein;

b) muss zumindest innerhalb des Ausstellungsbereichs der ausstellenden Behörde eindeutig sein;

c) darf nicht auf dem Ausweis aufgedruckt und nicht dazu bestimmt sein, vom Menschen lesbar zu sein;

d) darf keine personenbezogenen Daten offenlegen und nicht direkt aussagekräftig sein;

e) darf sich nicht direkt aus der sichtbaren Seriennummer des Ausweises ableiten lassen und

f) muss durch das qualifizierte elektronische Siegel kryptografisch mit den QR-Nutzdaten verbunden sein.

6.2. *RID-Format und -Größe*

Die RID ist als CBOR-Byte-String (bstr) zu kodieren. Die RID ist 16 Byte (128 Bit) lang.

Die RID wird von der ausstellenden Behörde nach einer unter ihrer Kontrolle stehenden Methode generiert, die eine ausreichende Entropie und Beständigkeit gegen Erraten oder Berechnung gewährleistet.

6.3. *Widerrufslisten*

In den zu Überprüfungszwecken veröffentlichten Widerrufslisten darf nur auf die RID der widerrufenen Ausweise verwiesen werden. Die Seriennummern der Ausweise werden nicht in den Widerrufslisten veröffentlicht.

7. **CBOR-Nutzdaten (innerhalb des QR-Codes) des Europäischen Behindertenausweises**

In die QR-Nutzdaten dürfen nur die folgenden Daten aufgenommen werden, die mit den in Anhang I der Richtlinie (EU) 2024/2841 festgelegten sichtbaren Datenfeldern des Europäischen Behindertenausweises übereinstimmen.

Inhalt der obersten Ebene:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" mit den in der nachstehenden Tabelle aufgeführten Attributen

c) issuerAuth = COSE_Sign1 (QSeal)

Feld	mDOC-Pfad	Art/Format
Version des Datenschemas	issuerSigned.nameSpaces."eu.edc".ver	String (z. B. "1.0")
Ausweisart: Europäischer Behindertenausweis	docType	Enum ("eu.edc")
Seriennummer des Ausweises	issuerSigned.nameSpaces."eu.edc".sub	String
Widerrufskennung	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 Byte)
Vorname des Ausweisinhabers	issuerSigned.nameSpaces."eu.edc".givenName	Unicode-Text-String (UTF-8)
Nachname des Ausweisinhabers	issuerSigned.nameSpaces."eu.edc".familyName	Unicode-Text-String (UTF-8)
Ablaufdatum des Ausweises	issuerSigned.nameSpaces."eu.edc".exp	CBOR-Tag 1004 nach RFC 8943 (Abschnitt 2.1), das eine UTF-8-Zeichenkette enthält, die ein vollständiges Datum im Format JJJJ-MM-TT nach RFC 3339 darstellt.

Die elektronische Signatur ist in issuerAuth (einem COSE_Sign1-Objekt) enthalten. Die Zertifikatkette darf nicht in die QR-Code-Nutzdaten eingebettet sein; stattdessen muss der geschützte COSE-Header x5t enthalten, einen Zertifikatsfingerabdruck, der zur Lokalisierung des entsprechenden QSealC im zwischengespeicherten Truststore der Prüfstelle verwendet wird.

8. **Beispiel für die Nutzdaten eines QR-Codes eines Europäischen Behindertenausweises: kommentierte logische JavaScript Object Notation-Darstellung**

Bei dem nachstehenden Beispiel handelt es sich um eine vom Menschen lesbare JavaScript Object Notation (JSON)-Darstellung der logischen Ansicht des Europäischen Behindertenausweises. In der Praxis ist diese Struktur nicht vom Menschen lesbar, da sie

a) in CBOR kodiert ist (RFC 8949, Abschnitt 3);

b) unter Verwendung der nicht markierten COSE_Sign1-Struktur signiert ist, mit abgetrennten Nutzdaten (RFC 9052, Abschnitt 4);

c) das Ablaufdatum als CBOR-Tag 1004 – vollständiges Datum nach RFC 8943 – enthält (Abschnitt 2.1);

d) den x5t-Parameter des geschützten Headers nach RFC 9360 enthält, unter Verwendung von SHA-256 der DER-kodierten End-Dateneinheit QSealC; und

e) komprimiert und mit der Zeichenfolge ED1:MDOC: als Präfix versehen ist, bevor die Kodierung im QR-Code erfolgt.

```
{
  // nur JSON-ähnliche, vom Menschen lesbare logische Ansicht des Europäischen Behindertenausweises.
  // Die tatsächliche QR-Nutzdaten sind deterministisches CBOR, nicht JSON.
  "docType": "eu.edc", // Zertifikat des Europäischen Behindertenausweises. Der docType-Wert ist, zusammen mit
     //issuerSigned, in den externen COSE_Sign1-Nutzdaten enthalten.

  "issuerSigned": {
     // Daten geschützt durch issuerAuth; verwendet als abgetrennte Nutzdaten.
     // Für die Erstellung und Überprüfung von Signaturen umfassen die abgetrennten externen Nutzdaten sowohl
     // docType als auch issuerSigned.
     "nameSpaces": {
       "eu.edc": {
         "ver": „1.0“,//QR-Profil-/Schemaversion

         // Seriennummer des Ausweises; vom Aussteller festgelegt, höchstens 24 Zeichen.
         "sub": "AB123456789012345678 90CD",

         // Widerrufskennung: tatsächlicher CBOR-Byte-String, 16 Byte/128 Bit.
         // Zwecks Lesbarkeit hier als 32-stelliger Hex-String angezeigt.
         "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

         "givenName": "Ann", ....// auf dem Europäischen Behindertenausweis aufgedruckter Vorname
         "familyName": "Other", // auf dem Europäischen Behindertenausweis aufgedruckter Nachname

         // Bei der tatsächlichen CBOR-Kodierung wird Tag 1004 für die Formatierung als vollständiges Datum nach
         RFC 3339 verwendet.
         "exp": "2030-12-31"
       }
     }
  },

  "issuerAuth": {
    // Tatsächliche Form: nicht markiertes COSE_Sign1, nicht ein JSON-Objekt.
    "type": "COSE_Sign1",
```

```
"tagged": falsch, //ohne CBOR-Tag für COSE_Sign1 kodiert
"payload": "detached" ,// COSE-Nutzdatenfeld ist CBOR null

"protectedHeader": {
  // Alg.: ES256; äquivalenter COSE-Headerparameter 1 = -7.
  "alg": "ES256",

  "x5t": Fingerabdruck des Zertifikats; COSE-Headerparameter 1 = 34.
  "x5t": {
    "hashAlg": "SHA-256", // äquivalenter COSE-Hashwert -16

    // Hash SHA-256 der DER-kodierten End-Dateneinheit QSealC.
    // 32 Byte, dargestellt als 64-stelliger Hex-String.
    "hashValue":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
  }
},

"unprotectedHeader": {}, // in diesem Beispiel leer

// COSE-Signatur ES256: // 64 Byte = 128-stelliger Hex-String.
"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
f0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. **Verwendung kryptografischer Mechanismen**

Die Verwendung kryptografischer Mechanismen im Rahmen dieses Anhangs muss den Vereinbarten kryptografischen Mechanismen (Agreed Cryptographic Mechanisms) entsprechen, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligt und von der Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlicht wurden.

ANHANG II

QR-CODE-SPEZIFIKATIONEN FÜR DIE PHYSISCHE VERSION DES EUROPÄISCHEN PARKAUSWEISES FÜR MENSCHEN MIT BEHINDERUNG

1. **Format des QR-Codes auf der physischen Version des Europäischen Parkausweises für Menschen mit Behinderung**

   a) **Format QR-Code Modell 2**, gemäß den internationalen QR-Code-Spezifikationen ISO/IEC 18004:2024 oder gleichwertig.

   b) **Fehlerkorrektur-Level M** (15 % Redundanz), wodurch sichergestellt wird, dass ein gedruckter QR-Code unempfindlich gegenüber Kratzern oder teilweisen Beschädigungen ist.

   c) **Kodierungsmodus**: Die QR-Nutzdaten müssen aus der kombinierten issuerSigned Concise Binary Object Representation (CBOR)-Struktur und dem entsprechenden issuerAuth COSE_Sign1-Signaturobjekt, wie in der CBOR-Objektsignatur und -verschlüsselung (COSE, RFC 9052 Abschnitte 3.1, 4.2 und 4.4) definiert, bestehen und dem mDOC-Datenmodellmuster für issuerSigned-Elemente entsprechen, jedoch angepasst für die Verwendung auf statischen physischen Ausweisen. Der issuerAuth muss ein COSE_Sign1-Objekt mit alg = ES256 und einem geschützten Header sein, der x5t (den in RFC 9360 (Abschnitt 2) definierten Hash-Header-Parameter des COSE X.509-Zertifikats; aus Gründen der Interoperabilität muss der in x5t verwendete Hash-Algorithmus SHA-256 sein) enthält.

   d) Vor der Kodierung des QR-Codes ist das kombinierte CBOR/COSE-Objekt **im ZLIB-Format (RFC 1950 Abschnitt 2.2) mit dem Deflate**-Algorithmus (RFC 1951 Abschnitte 3.2 und 4) **zu komprimieren**. Das resultierende komprimierte Byte-Array muss im **QR-Code-Byte-Modus** kodiert werden, um sicherzustellen, dass die binären CBOR/COSE-Nutzdaten und die Interoperabilität der Scanner in vollem Umfang unterstützt werden.

   Für alle in den QR-Nutzdaten enthaltenen Textfelder müssen die Aussteller die Zeichen innerhalb des CBOR-Text-Strings als Unicode UTF-8 verschlüsseln. Auf signierte Nutzdaten darf keine Transliteration angewendet werden. Aus Gründen der Interoperabilität müssen Aussteller vor der Signatur auf alle Textfelder die Unicode-Normalisierungsform C (NFC) anwenden.

   e) **Präfix**: Der QR-String des Europäischen Parkausweises für Menschen mit Behinderung muss mit „EP1:MDOC:“ beginnen. Damit werden die Art des Ausweises und das Kodierungsprofil identifiziert. Bei den Präfixen wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen vorhanden sein. Unbekannte oder nicht unterstützte Präfixe führen zur Ablehnung. Das Präfix und die komprimierten Nutzdaten sind als ein einzelnes Byte-Modus-Datensegment im QR-Code zu kodieren.

   f) **Die Größe des Moduls muss mindestens 0,35 mm betragen**, um die Lesbarkeit auf gedruckten Ausweisen sicherzustellen.

   g) Es darf sich **höchstens um Version 20 handeln**; mit bis zu 97 × 97 Modulen je Seite.

2. **Spezifikationen für die Generierung von Signaturen des Europäischen Parkausweises für Menschen mit Behinderung**

   Mit dem qualifizierten elektronischen Siegel (QSeal), das zum Besiegeln von QR-Codes des Europäischen Parkausweises für Menschen mit Behinderung verwendet wird, wird sichergestellt, dass die kodierten Daten von der autorisierten ausstellenden Behörde stammen und nicht verändert wurden.

   a) **Signaturalgorithmus**: Der Signaturalgorithmus ist ES256 (ECDSA mit SHA-256 unter Verwendung der P-256-Kurve), wie in RFC 9053 (Abschnitt 2.1) definiert; in COSE wird der Algorithmus durch den Header-Parameter „alg“ in RFC 9052 (Abschnitt 3.1) identifiziert.

   b) **Signierschlüssel**: Die QR-Nutzdaten müssen mit dem privaten Schlüssel signiert werden, der einem qualifizierten Zertifikat für elektronische Siegel (QSealC) entspricht.

   c) **COSE-Struktur**: Der Signaturcontainer muss ein COSE_Sign1-Objekt sein. Der geschützte Header muss alg (ES256) und x5t (den Hash-Header-Parameter des COSE X.509-Zertifikats gemäß RFC 9360 (Abschnitt 2); aus Gründen der Interoperabilität muss der in x5t verwendete Hash-Algorithmus SHA-256 sein) enthalten. Die Überprüfung erfolgt anhand des x5t-Werts, um das entsprechende Zertifikat im lokal zwischengespeicherten Truststore der Prüfstelle zu lokalisieren, der auf der Grundlage der Informationen aus der Vertrauensliste erstellt wurde; anschließend werden die Zertifikatskette und der Zertifikatsstatus gemäß dem eIDAS-Vertrauensrahmen überprüft.

   d) **Signaturstandard**: Die QR-Code-Nutzdaten müssen als COSE_Sign1-Objekt gemäß RFC 9052 (Abschnitt 4), CBOR-Objektsignatur und -verschlüsselung, signiert werden. Das COSE_Sign1-Objekt muss in issuerAuth enthalten sein und ohne CBOR-Tag für COSE_Sign1 kodiert werden. Das Nutzdatenfeld des COSE_Sign1-Objekts ist abzutrennen und als CBOR null zu kodieren. Für die Erstellung und Überprüfung von Signaturen bestehen die externen Nutzdaten aus der deterministischen CBOR-kodierten CBOR-Struktur, die den docType-Wert und den issuerSigned-Wert aus der CBOR-Map der obersten Ebene enthält.

e) **Hash-Algorithmus**: SHA-256 ist als Teil von ES256 für die Erstellung von Signaturen und die Überprüfung der Integrität zu verwenden.

f) **Kodierung**: Die Nutzdaten müssen gemäß den COSE- und mDOC-Spezifikationen mit CBOR (RFC 8949 Abschnitt 4.2) kodiert werden, um die Kodierung und Reproduzierbarkeit der signierten Daten sicherzustellen.

3. **Druckspezifikationen**

a) **Ruhezone**: Der QR-Code muss von allen Seiten mit einem deutlichen Abstand von **vier Modulen** umgeben sein, ohne jegliche Bedruckung, Muster oder Hintergründe.

b) **Kontrast**: Der QR-Code muss auf weißem Hintergrund gedruckt werden und ein Kontrastverhältnis von mindestens **4:1** aufweisen, um eine gute Lesbarkeit bei unterschiedlichen Lichtverhältnissen sicherzustellen.

c) Der QR-Code ist unter Verwendung der in Anhang I der Richtlinie (EU) 2024/2841 festgelegten Farbe zu drucken, die einen maximalen Kontrast gewährleistet.

d) **Platzierung und Größe**: Die Größe des QR-Codes, einschließlich der Ruhezone, muss **37 mm × 37 mm** betragen, und er muss sich auf der Vorderseite des Ausweises leicht rechts von der Mitte in Richtung des unteren Randes befinden. Der QR-Code darf höchstens der Version 20 (97 × 97 Module) entsprechen und muss eine Modulgröße von mindestens 0,35 mm aufweisen.

Der QR-Code einschließlich der Ruhezone ist mindestens 5 mm von der Unterkante der Karte entfernt anzubringen.

4. **Daten im QR-Code des Europäischen Parkausweises für Menschen mit Behinderung**

Der QR-Code muss einen minimalen, offline überprüfbaren Datensatz enthalten, der dem in Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 vorgesehenen Grundsatz der Datenminimierung entspricht. Die Nutzdaten sind wie folgt strukturiert:

a) Die Attribute der Ausweise werden in CBOR innerhalb eines issuerSigned-Objekts kodiert.

b) Die Struktur wird vom QSeal der ausstellenden Behörde als issuerAuth (COSE_Sign1, ES256, einschließlich x5t, dem Hash-Header-Parameter des COSE X.509-Zertifikats) verpackt und signiert.

c) Das resultierende CBOR/COSE-Objekt wird gemäß Nummer 1 Buchstabe d dieses Anhangs komprimiert. Die QR-Code-Nutzdaten bestehen aus dem Präfix „EP1:MDOC:“, gefolgt von dem resultierenden komprimierten Byte-Array, und die vollständigen Nutzdaten werden unter Verwendung des Byte-Modus als ein einziges QR-Code-Datensegment kodiert.

Der Dateninhalt besteht aus einer Teilmenge der sichtbaren Daten aus den in Anhang II der Richtlinie (EU) 2024/2841 aufgeführten Feldern auf der Vorderseite des Ausweises (Ablaufdatum, Seriennummer des Ausweises) sowie der Widerrufskennung, der elektronischen Signatur und den Schema-Informationen.

Die **elektronische Signatur** muss Folgendes enthalten:

i) issuerAuth – ein COSE_Sign1-Objekt, das mit dem **privaten QSealC-Schlüssel** der ausstellenden Behörde signiert ist,

ii) den geschützten Header mit alg = ES256 (Signaturalgorithmus) und x5t (dem Hash-Header-Parameter des COSE X.509-Zertifikats).

5. **Optionale Daten**

Der QR-Code darf keine optionalen Daten enthalten.

6. **Widerrufskennung (RID)**

Die Widerrufskennung des Europäischen Parkausweises für Menschen mit Behinderung muss Anhang I Nummer 6 entsprechen.

In den Widerrufslisten für widerrufene Europäische Parkausweise für Menschen mit Behinderung darf nur auf die RID verwiesen werden. Die Seriennummern der Ausweise werden nicht in den Widerrufslisten veröffentlicht.

7. **CBOR-Nutzdaten (innerhalb des QR-Codes) des Europäischen Parkausweises für Menschen mit Behinderung**

In die QR-Nutzdaten dürfen nur die folgenden Daten aufgenommen werden, die mit den in Anhang II der Richtlinie (EU) 2024/2841 aufgeführten sichtbaren Feldern des Europäischen Parkausweises für Menschen mit Behinderung übereinstimmen:

Feld	mDOC-Pfad	Art/Format
Version des Datenschemas	issuerSigned.nameSpaces."eu.epc".ver	String (z. B. "1.0")
Ausweisart: Europäischer Parkausweis für Menschen mit Behinderung	docType	Enum ("eu.epc")
Seriennummer des Ausweises	issuerSigned.nameSpaces."eu.epc".sub	String
Widerrufskennung	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 Byte)
Ablaufdatum des Ausweises	issuerSigned.nameSpaces."eu.epc".exp	CBOR-Tag 1004 nach RFC 8943 (Abschnitt 2.1), das eine UTF-8-Zeichenkette enthält, die ein vollständiges Datum im Format JJJJ-MM-TT nach RFC 3339 darstellt.

Die elektronische Signatur muss in issuerAuth (einem COSE_Sign1-Objekt) enthalten sein. Die Zertifikatkette darf nicht in die QR-Code-Nutzdaten eingebettet sein; stattdessen muss der geschützte COSE-Header x5t enthalten, einen Zertifikatsfingerabdruck, der zur Lokalisierung des entsprechenden QSealC im zwischengespeicherten Truststore der Prüfstelle verwendet wird.

8. **Beispiel für die Nutzdaten eines QR-Codes eines Europäischen Parkausweises für Menschen mit Behinderungen: kommentierte logische JavaScript Object Notation-Darstellung**

Bei dem nachstehenden Beispiel handelt es sich um eine vom Menschen lesbare JavaScript Object Notation (JSON)-Darstellung der logischen Ansicht des Europäischen Parkausweises für Menschen mit Behinderungen. In der Praxis ist diese Struktur nicht vom Menschen lesbar, da sie

a) in CBOR kodiert ist (RFC 8949 Abschnitt 3);

b) unter Verwendung der nicht markierten COSE_Sign1-Struktur signiert ist, mit abgetrennten Nutzdaten (RFC 9052, Abschnitt 4);

c) das Ablaufdatum als CBOR-Tag 1004 – vollständiges Datum nach RFC 8943 – enthält (Abschnitt 2.1);

d) den x5t-Parameter des geschützten Headers nach RFC 9360 enthält, unter Verwendung von SHA-256 der DER-kodierten End-Dateneinheit QSealC; und

e) komprimiert und mit der Zeichenfolge EP1:MDOC: als Präfix versehen ist, bevor die Kodierung im QR-Code erfolgt.

```
{
  // nur JSON-ähnliche, vom Menschen lesbare logische Ansicht des Europäischen Parkausweises für Menschen mit Behinderungen.
  // Die tatsächliche QR-Nutzdaten sind deterministisches CBOR, nicht JSON.
  "docType": "eu.epc", // Zertifikat des Europäischen Parkausweises für Menschen mit Behinderungen. Der docType-Wert ist, zusammen mit
    //issuerSigned, in den externen COSE_Sign1-Nutzdaten enthalten.

  "issuerSigned": {
    // Daten geschützt durch issuerAuth; verwendet als abgetrennte Nutzdaten.
    // Für die Erstellung und Überprüfung von Signaturen umfassen die abgetrennten externen Nutzdaten sowohl
```

```
  // docType als auch issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0",//QR-Profil-/Schemaversion

      // Seriennummer des Ausweises; vom Aussteller festgelegt, höchstens 24 Zeichen.
      "sub": "EF123456789012345678 90GH",

      // Widerrufskennung: tatsächlicher CBOR-Byte-String, 16 Byte/128 Bit.
      // Zwecks Lesbarkeit hier als 32-stelliger Hex-String angezeigt.
      "rid": "4a8d9c112233445566778899aabbccdd",

      // Bei der tatsächlichen CBOR-Kodierung wird Tag 1004 für die Formatierung als vollständiges Datum nach RFC 3339 verwendet.
      "exp": "2030-12-31"
    }
  }
 },

 "issuerAuth": {
  // Tatsächliche Form: nicht markiertes COSE_Sign1, nicht ein JSON-Objekt.
  "type": "COSE_Sign1",
  "tagged": falsch, //ohne CBOR-Tag für COSE_Sign1 kodiert
  "payload": "detached",// COSE-Nutzdatenfeld ist CBOR null

  "protectedHeader": {
   // Alg.: ES256; äquivalenter COSE-Headerparameter 1 = -7.
   "alg": "ES256",

   "x5t": Fingerabdruck des Zertifikats; COSE-Headerparameter 1 = 34.
   "x5t": {
    "hashAlg": "SHA-256", // äquivalenter COSE-Hashwert -16

    // Hash SHA-256 der DER-kodierten End-Dateneinheit QSealC.
    // 32 Byte, dargestellt als 64-stelliger Hex-String.
    "hashValue":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
   }
  },

  "unprotectedHeader": {}, // in diesem Beispiel leer

  // COSE-Signatur ES256: // 64 Byte = 128-stelliger Hex-String.
  "signature":
  "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. **Verwendung kryptografischer Mechanismen**

Die Verwendung kryptografischer Mechanismen im Rahmen dieses Anhangs muss den Vereinbarten kryptografischen Mechanismen (Agreed Cryptographic Mechanisms) entsprechen, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligt und von der Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlicht wurden.

ANHANG III

MELDUNG VON INFORMATIONEN GEMÄß ARTIKEL 6 ABSATZ 2

1. Die Mitgliedstaaten übermitteln der Kommission zu jeder für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle folgende Informationen:

   a) den Namen der für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle;

   b) eine Registrierungsnummer der für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle;

   c) eine E-Mail-Adresse und Telefonnummer für die Kontaktaufnahme mit der für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle;

   d) ein oder mehrere Zertifikate, die zur Überprüfung des elektronischen Siegels, das von der für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle erstellt wurde, verwendet werden können und deren zertifizierte Identitätsdaten den Namen und gegebenenfalls die Registrierungsnummer des Ausstellers gemäß den Buchstaben a und b enthalten;

   e) die Internetadresse, unter der der Aussteller den Gültigkeitsstatus der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen veröffentlicht.

2. Die Mitgliedstaaten können der Kommission zu jeder für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle folgende Informationen übermitteln:

   a) die Internetadresse der Webseite, die die Regelungen und Nutzungsbedingungen der für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständigen Behörde oder Stelle enthält, die für die Bereitstellung und Nutzung der von dieser Behörde oder Stelle ausgegebenen physischen Versionen des Europäischen Behindertenausweises und des Europäischen Parkausweises für Menschen mit Behinderungen gelten;

   b) gegebenenfalls die Internetadresse der Webseite, die zusätzliche Informationen über die für die Ausstellung der physischen Versionen des Europäischen Behindertenausweises oder des Europäischen Parkausweises für Menschen mit Behinderungen zuständige Behörde oder Stelle enthält.

ANHANG IV

TECHNISCHE SPEZIFIKATIONEN FÜR EINE WIDERRUFSLISTE FÜR DIE PHYSISCHEN VERSIONEN DES EUROPÄISCHEN BEHINDERTENAUSWEISES ODER DES EUROPÄISCHEN PARKAUSWEISES FÜR PERSONEN MIT BEHINDERUNGEN

1. Für die Zwecke dieses Anhangs entspricht die Kennung der in Anhang I Nummer 6 und Anhang II Nummer 6 definierten Widerrufskennung (RID).

2. Eine Widerrufsliste wird als Kennungslisten-Token im CWT-Format (RFC 8392 Abschnitt 7) gemäß Klausel 5.2 der Spezifikation der Token-Statusliste (draft-ietf-oauth-status-list-14) mit den folgenden Änderungen implementiert:

   a) Der Wert des Type-Claims lautet „application/identifierlist+cwt“;

   b) die Angabe der Ablaufzeit muss vorhanden sein;

   c) der StatusList-Claim darf nicht im CWT-ClaimSet enthalten sein;

   d) die in Nummer 3 definierte IdentifierList-Struktur muss als Claim im CWT-ClaimSet unter Verwendung des Schlüssels 65530 vorhanden sein;

   e) der CWT muss ein COSE_Sign1-Objekt sein, das für die Berechnung der Signatur einen Signaturalgorithmus verwendet, der den Vereinbarten kryptografischen Mechanismen (Agreed Cryptographic Mechanisms) entspricht, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligt und von der Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlicht wurden;

   f) der CWT muss den in RFC 9360 (Abschnitt 2) definierten x5chain-Parameter im geschützten Header enthalten, der das Zertifikat oder die Kette von Zertifikaten zur Überprüfung der Signatur der Widerrufsliste enthält;

   g) die in der Spezifikation für die Token-Statusliste (draft-ietf-oauth-status-list-14) angegebene erweiterte OID für die Schlüsselverwendung kann für das Signierzertifikat der Kennungsliste verwendet werden, und es wird empfohlen, dass die Prüfstellen die in der Spezifikation für die Token-Statusliste angegebene erweiterte OID für die Schlüsselverwendung unterstützen und dass die Infrastrukturen der ausstellenden Behörde das Feld für die erweiterte Schlüsselverwendung nicht als zwingend erforderlich festlegen, wenn sie die in der Spezifikation für die Token-Statusliste angegebene erweiterte OID für die Schlüsselverwendung verwenden.

3. Die IdentifierList-Struktur ist eine CBOR-Struktur mit der folgenden Concise Data Definition Language (CDDL):

```
IdentifierList = {

  "identifiers" : { * Identifier => IdentifierInfo },

  ? "aggregation_uri" : Aggregation_uri,

  * tstr => RFU

}

IdentifierInfo = {

  (tstr/int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```