Rat der
Europäischen Union

Brüssel, den 10. Juli 2026
(OR. en)

11772/26
ADD 1

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

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	1. Juli 2026
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	C(2026) 4534 annex
Betr.:	ANHÄNGE der DELEGIERTEN VERORDNUNG (EU) .../... DER KOMMISSION zur Ergänzung der Richtlinie (EU) 2024/2841 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

EUROPÄISCHE
KOMMISSION

Brüssel, den 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ANHÄNGE

der

DELEGIERTEN VERORDNUNG (EU) .../... DER KOMMISSION

zur Ergänzung der Richtlinie (EU) 2024/2841 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

ANHANG I

QR-CODE-SPEZIFIKATIONEN FÜR DIE PHYSISCHE VERSION DES EUROPÄISCHEN BEHINDERTENAUSWEISES

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 x 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“:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef“

}

}

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 x 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“:
„0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef“

}

}

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
```