Conselho
da União Europeia

**Bruxelas, 10 de julho de 2026**
**(OR. en)**

**11772/26**
**ADD 1**

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

**NOTA DE ENVIO**

| | |
|---|---|
| de: | Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora |
| data de receção: | 1 de julho de 2026 |
| para: | Thérèse BLANCHET, secretária-geral do Conselho da União Europeia |
| n.° doc. Com.: | C(2026) 4534 annex |
| Assunto: | ANEXOS<br>do<br>REGULAMENTO DELEGADO (UE) .../... DA COMISSÃO<br>que complementa a Diretiva (UE) 2024/2841 no respeitante à definição do código QR na versão física do cartão europeu de deficiência e à definição do código QR e de especificações técnicas comuns que garantam a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência, bem como a questões relativas à interoperabilidade |

COMISSÃO
EUROPEIA

Bruxelas, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

**ANEXOS**

**do**

**REGULAMENTO DELEGADO (UE) .../... DA COMISSÃO**

**que complementa a Diretiva (UE) 2024/2841 no respeitante à definição do código QR na versão física do cartão europeu de deficiência e à definição do código QR e de especificações técnicas comuns que garantam a segurança da versão física do cartão europeu de estacionamento para pessoas com deficiência, bem como a questões relativas à interoperabilidade**

# ANEXO I

## ESPECIFICAÇÕES DO CÓDIGO QR PARA A VERSÃO FÍSICA DO CARTÃO EUROPEU DE DEFICIÊNCIA

1. **Formato do código QR para a versão física do cartão europeu de deficiência**

a) **Formato do código QR Modelo 2**, em conformidade com as especificações internacionais do código QR ISO/IEC 18004:2024 ou equivalentes.

b) **Nível de correção de erro M** (redundância de 15 %) que assegura a proteção contra riscos ou danos parciais de um código QR impresso.

c) **Modo de codificação:** A carga útil do QR é constituída pela estrutura combinada issuerSigned Concise Binary Object Representation (representação concisa de objetos binários) (CBOR) e pelo correspondente objeto de assinatura issuerAuth COSE_Sign1, conforme definido em CBOR Object Signing and Encryption (*assinatura e codificação de objetos*) (COSE, RFC 9052, secções 3.1, 4.2 e 4.4), segundo o padrão de modelo de dados mDOC para os elementos issuerSigned, mas adaptado para utilização estática num cartão físico. O issuerAuth deve ser um objeto COSE_Sign1 com alg = ES256 e um cabeçalho protegido que contenha um valor x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256].

d) Antes da codificação do código QR, o objeto combinado CBOR/COSE deve ser **comprimido utilizando o formato zlib** (RFC 1950, secção 2.2) **com o algoritmo deflate** (RFC 1951, secções 3.2 e 4). A matriz de bytes (byte array) comprimida resultante deve ser codificada **sob a forma de bytes para código QR**, para assegurar a total compatibilidade com cargas úteis binárias CBOR/COSE e a interoperabilidade do digitalizador.

Para todos os campos de texto incluídos na carga útil do código QR, os emitentes devem introduzir carateres com codificação Unicode UTF-8 nas cadeias de texto CBOR. A transliteração não pode ser aplicada aos dados de carga útil assinados. Para efeitos de interoperabilidade, os emitentes devem aplicar a Forma de Normalização Unicode C (NFC) a todos os campos textuais antes de assinar.

e) **Prefixo:** A cadeia de carateres do código QR para o cartão europeu de deficiência começa por «ED1: MDOC:». Isto identifica o tipo de cartão e o perfil de codificação. Os prefixos são sensíveis às maiúsculas e minúsculas e devem estar presentes. Os prefixos desconhecidos ou não suportados serão causa de rejeição. O prefixo e a carga útil comprimida devem ser codificados no código QR como um único segmento de dados sob a forma de bytes.

f) **Dimensão mínima do módulo ≥ 0,25 mm** para garantir a legibilidade nos cartões impressos.

g) **Versão 20, no máximo;** com até 97 × 97 módulos de cada lado.

2. **Especificações para gerar assinaturas para o cartão europeu de deficiência**

O selo eletrónico qualificado (QSeal) utilizado para selar os códigos QR do cartão europeu de deficiência garante que os dados codificados provêm da autoridade emissora autorizada e que não foram alterados.

a) **Algoritmo de assinatura**: O algoritmo de assinatura deve ser ES256 [algoritmo de assinatura digital de curva elíptica (ECDSA) com SHA-256 e utilizando a curva P-256], conforme definido no RFC 9053 (secção 2.1); no COSE, o algoritmo é identificado pelo parâmetro do cabeçalho «alg» no RFC 9052 (secção 3.1).

b) **Chave de assinatura**: A carga útil do código QR deve ser assinada utilizando a chave privada correspondente a um certificado qualificado de selo eletrónico (QSealC).

c) **Estrutura COSE:** O contentor da assinatura deve ser um objeto COSE_Sign1. O cabeçalho protegido deve incluir os valores alg (ES256) e x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256]. A verificação deve basear-se na utilização do valor x5t para localizar o certificado correspondente na lista de certificados de confiança armazenada na memória cache local do verificador, construída a partir de informações da Lista de Confiança e, em seguida, validar a cadeia de certificados e o estado do certificado em conformidade com o quadro de confiança eIDAS.

d) **Norma de assinatura**: A assinatura da carga útil do código QR deve ser um objeto COSE_Sign1, em conformidade com o RFC 9052 (secção 4), CBOR Object Signing and Encryption (*assinatura e codificação de objetos*). O objeto COSE_Sign1 deve ser transportado pelo issuerAuth e codificado sem a etiqueta CBOR para COSE_Sign1. O campo da carga útil do objeto COSE_Sign1 deve ser separado e codificado com um valor CBOR nulo. Para a criação e verificação da assinatura, a carga útil externa deve consistir na estrutura CBOR determinística que contém os valores docType e issuerSigned do mapa CBOR de nível superior.

e) **Algoritmo de dispersão (Hash)**: O SHA-256 deve ser utilizado como parte do ES256 para gerar assinaturas e verificação da integridade.

f) **Codificação**: A carga útil deve ser codificada utilizando o CBOR (RFC 8949, secção 4.2), conforme exigido pelas especificações COSE e mDOC, para assegurar a codificação e a reprodutibilidade dos dados assinados.

3. **Especificações de impressão:**

a) **Zona em branco**: O código QR deve ser contornado, em todos os lados, por uma margem vazia de **quatro módulos** sem qualquer impressão, padrão ou fundo.

b) **Contraste**: O código QR deve ser impresso sobre um fundo branco, com uma relação de contraste mínima de **4:1**, a fim de assegurar uma elevada legibilidade em condições de iluminação variáveis.

c) O código QR deve ser impresso utilizando a cor definida no anexo I da Diretiva (UE) 2024/2841 que garanta o máximo contraste.

d) **Colocação e dimensão**: O código QR, incluindo a zona em branco, deve ser de 26,25 mm × 26,25 mm, no verso do cartão, no canto inferior direito. O código QR deve ser, no máximo, a versão 20 (97 × 97 módulos), com um módulo de dimensão igual ou superior a 0,25 mm.

O código QR, incluindo a zona em branco, deve estar posicionado a, pelo menos, 5 mm da margem direita e a, pelo menos, 5 mm da margem inferior do cartão.

## 4. Dados no código QR do cartão europeu de deficiência

O código QR deve conter um conjunto de dados mínimo verificável fora de linha, em conformidade com o princípio da minimização dos dados consagrado pelo artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679. A estrutura da carga útil é a seguinte:

a) Os atributos do cartão são codificados no CBOR num objeto issuerSigned.

b) A estrutura é encapsulada e assinada pelo QSeal da autoridade emissora como issuerAuth (COSE_Sign1, ES256, incluindo um valor x5t, o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

c) O objeto CBOR/COSE resultante deve ser comprimido de acordo com o ponto 1, alínea d) do presente anexo. A carga útil do código QR deve consistir no prefixo «ED1:MDOC:», seguido da matriz de bytes comprimida resultante, e a carga útil completa deve ser codificada utilizando o formato binário como um único segmento de dados do código QR.

O conteúdo dos dados deve consistir num subconjunto de dados visíveis que figurem nos campos da parte da frente do cartão enumerados no anexo I da Diretiva (UE) 2024/2841 (nome, apelido, número de série do cartão, data de expiração), juntamente com o identificador de revogação, a assinatura eletrónica e as informações sobre o esquema.

**A assinatura eletrónica** deve conter:

i) issuerAuth — objeto COSE_Sign1 assinado com a **chave privada QSealC** da autoridade emissora.

ii) cabeçalho protegido que inclui os valores alg = ES256 (algoritmo de assinatura) e x5t (o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

## 5. Dados facultativos

Não devem ser incluídos dados facultativos no código QR.

## 6. Identificador de revogação

Para além do número de série visível do cartão, o código QR deve incluir um identificador de revogação específico.

O identificador de revogação deve ser utilizado para determinar o estado de revogação e para a gestão da lista de revogação. O identificador de revogação não pode ser impresso no cartão nem apresentado aos verificadores de cartões.

### 6.1. *Obrigações do identificador de revogação*

O identificador de revogação:

a) Deve ser incluído na carga útil assinada do QR;

b) Deve ser único, pelo menos, no domínio de emissão da autoridade emissora;

c) Não pode ser impresso no cartão nem destinar-se a ser compreendida por humanos;

d) Não pode revelar dados pessoais nem ter um significado diretamente identificável;

e) Não pode ser dedutível diretamente a partir do número de série visível do cartão; e

f) Deve estar criptograficamente ligado à carga útil do código QR pelo selo eletrónico qualificado.

6.2. *Formato e dimensão do identificador de revogação*

O identificador de revogação deve ser codificado como uma cadeia de bytes CBOR (bstr). O identificador de revogação deve ter um comprimento de16 bytes (128 bits).

O identificador de revogação deve ser gerado pela autoridade emissora utilizando um método sob o seu controlo que garanta entropia e resistência suficientes contra tentativas de decifração ou enumeração.

6.3. *Listas de revogação*

As listas de revogação publicadas para efeitos de verificação devem fazer referência apenas ao identificador de revogação dos cartões revogados. Os números de série dos cartões não podem ser publicados nas listas de revogação.

## 7. Carga útil CBOR (dentro do código QR) do cartão europeu de deficiência

Apenas os seguintes dados devem ser incluídos na carga útil do código QR, em consonância com os campos de dados visíveis do cartão europeu de deficiência estabelecidos no anexo I da Diretiva (UE) 2024/2841.

Conteúdos de nível superior:

a) docType = "eu.edc"

b) issuerSigned.nameSpaces."eu.edc" com os atributos indicados no quadro abaixo

c) issuerAuth = COSE_Sign1 (QSeal)

| **Campo** | **caminho de acesso mDOC** | **Tipo/Formato** |
|---|---|---|
| Versão do esquema de dados | issuerSigned.nameSpaces."eu.edc".ver | Cadeia de carateres alfanuméricos (p. ex., "1.0") |
| Tipo de cartão: cartão europeu de deficiência | docType | Enum ("eu.edc") |
| Número de série do cartão | issuerSigned.nameSpaces."eu.edc".sub | Cadeia de carateres alfanuméricos |
| Identificador de revogação | issuerSigned.nameSpaces."eu.edc".rid | CBOR bstr (16 bytes) |

| | | |
|---|---|---|
| Nome próprio do titular do cartão | issuerSigned.nameSpaces."eu.edc".givenName | Cadeia de texto Unicode (UTF-8) |
| Apelido do titular do cartão | issuerSigned.nameSpaces."eu.edc".familyName | Cadeia de texto Unicode (UTF-8) |
| Data de validade do cartão | issuerSigned.nameSpaces."eu.edc".exp | Etiqueta CBOR 1004, conforme definida no RFC 8943 (secção 2.1), que contém uma cadeia de carateres de texto com codificação UTF-8 que representa uma data completa RFC 3339 no formato AAAA-MM-DD |

A assinatura eletrónica é transportada pelo issuerAuth (um objeto COSE_Sign1). A cadeia de certificados não pode ser incorporada na carga útil do código QR; em vez disso, o cabeçalho protegido COSE deve incluir um valor x5t, um código de identificação digital do certificado utilizado para localizar o QSealC correspondente na lista de certificados de confiança armazenada na memória cache do verificador.

8. **Exemplo de carga útil do código QR do cartão europeu de deficiência: representação lógica comentada no estilo de notação de objetos JavaScript**

O exemplo que se segue é uma representação do esquema lógico do cartão europeu de deficiência em notação JSON que pode ser compreendida por humanos. Na prática, esta estrutura não pode ser compreendida por humanos, uma vez que:

a) É codificada no CBOR (RFC 8949, secção 3);

b) É assinada utilizando uma estrutura COSE_Sign1 sem etiqueta com uma carga útil separada (RFC 9052, secção 4);

c) Incluirá uma etiqueta CBOR 1004 com a data de expiração no formato de valor de data completa, de acordo com o RFC 8943 (secção 2.1);

d) Incluirá o parâmetro de cabeçalho protegido x5t, em conformidade com o RFC 9360, utilizando o SHA-256 sobre o QSealC de entidade final codificado em DER; e

e) É comprimida e pré-fixada com a cadeia de carateres ED1:MDOC: antes de ser codificada no código QR.

```
{
  // Apenas esquema lógico do cartão europeu de deficiência, em formato JSON legível por humanos.
  // A carga útil real do código QR é CBOR determinístico e não JSON.
  "docType": "eu.edc", // credencial do cartão europeu de deficiência. O valor docType está incluído, juntamente com
    // issuerSigned, na carga útil externa COSE_Sign1.

  "issuerSigned": {
    // Dados protegidos por issuerAuth; utilizado como carga útil separada.
    // Para a criação e verificação da assinatura, a carga útil externa separada abrange
    // docType e issuerSigned.
    "nameSpaces": {
      "eu.edc": {
        "ver": "1.0", // perfil QR/versão do esquema

        // Número de série do cartão; definido pelo emitente, máx. 24 carateres.
        "sub": "AB123456789012345678 90CD",
```

```
    // Identificador de revogação: CBOR bstr real, 16 bytes/128 bits.
    // Apresentado aqui como 32 carateres hexadecimais para legibilidade.
    "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

    "givenName": "Ann",    // nome próprio impresso no cartão europeu de deficiência
    "familyName": "Other", // apelido impresso no cartão europeu de deficiência

    // A codificação CBOR real utiliza a etiqueta 1004 para a data completa RFC 3339.
    "exp": "2030-12-31"
   }
  }
},

"issuerAuth": {
 // Formulário efetivo: COSE_Sign1 sem etiqueta, não um objeto JSON.
 "type": "COSE_Sign1",
 "tagged": falso,       // codificado sem etiqueta CBOR COSE_Sign1
 "payload": "detached", // O campo da carga útil COSE é CBOR nulo.

 "protectedHeader": {
  // alg: ES256; parâmetro de cabeçalho COSE equivalente 1 = -7.
  "alg": "ES256",

  // x5t: código de identificação digital do certificado; parâmetro de cabeçalho COSE 34.
  "x5t": {
   "hashAlg": "SHA-256", valor de dispersão equivalente COSE -16
```

```
        // Valor de dispersão SHA-256 do QSealC de entidade final codificado em DER.
        // 32 bytes representados por 64 carateres hexadecimais.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // em branco neste exemplo

    // Assinatura ES256 COSE: 64 bytes = 128 carateres hexadecimais.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

## 9. Utilização de mecanismos criptográficos

A utilização de mecanismos criptográficos no contexto do presente anexo deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA).

## ANEXO II

## ESPECIFICAÇÕES DO CÓDIGO QR PARA A VERSÃO FÍSICA DO CARTÃO EUROPEU DE ESTACIONAMENTO PARA PESSOAS COM DEFICIÊNCIA

1. **Formato do código QR na versão física do cartão europeu de estacionamento para pessoas com deficiência**

a) **Formato do código QR Modelo 2**, em conformidade com as especificações internacionais do código QR ISO/IEC 18004:2024 ou equivalentes.

b) **Nível de correção de erro M** (redundância de 15 %) que assegura a proteção contra riscos ou danos parciais de um código QR impresso.

c) **Modo de codificação:** A carga útil do QR é constituída pela estrutura combinada issuerSigned Concise Binary Object Representation (representação concisa de objetos binários) (CBOR) e pelo correspondente objeto de assinatura issuerAuth COSE_Sign1, conforme definido em CBOR Object Signing and Encryption (*assinatura e codificação de objetos*) (COSE, RFC 9052, secções 3.1, 4.2 e 4.4), segundo o padrão de modelo de dados mDOC para os elementos issuerSigned, mas adaptado para utilização estática num cartão físico. O issuerAuth deve ser um objeto COSE_Sign1 com alg = ES256 e um cabeçalho protegido que contenha um valor x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256].

d) Antes da codificação do código QR, o objeto combinado CBOR/COSE deve ser **comprimido utilizando o formato zlib (RFC 1950, secção 2.2) com o algoritmo deflate** (RFC 1951, secções 3.2 e 4). A matriz de bytes (byte array) comprimida resultante deve ser codificada **sob a forma de bytes para código QR**, para assegurar a total compatibilidade com cargas úteis binárias CBOR/COSE e a interoperabilidade do digitalizador.

Para todos os campos de texto incluídos na carga útil do código QR, os emitentes devem introduzir carateres com codificação Unicode UTF-8 nas cadeias de texto CBOR. A transliteração não pode ser aplicada aos dados de carga útil assinados. Para efeitos de interoperabilidade, os emitentes devem aplicar a Forma de Normalização Unicode C (NFC) a todos os campos textuais antes de assinar.

e) **Prefixo**: A cadeia de carateres do código QR para o cartão europeu de estacionamento para pessoas com deficiência começa por «EP1:MDOC:». Isto identifica o tipo de cartão e o perfil de codificação. Os prefixos são sensíveis às maiúsculas e minúsculas e devem estar presentes. Os prefixos desconhecidos ou não suportados serão causa de rejeição. O prefixo e a carga útil comprimida devem ser codificados no código QR como um único segmento de dados sob a forma de bytes.

f) **Dimensão mínima do módulo ≥ 0,35 mm** para garantir a legibilidade nos cartões impressos.

g) **Versão 20, no máximo**; com até 97 × 97 módulos de cada lado.

2. **Especificações para gerar assinaturas para o cartão europeu de estacionamento para pessoas com deficiência**

O selo eletrónico qualificado (QSeal) utilizado para selar os códigos QR do cartão europeu de estacionamento para pessoas com deficiência garante que os dados codificados provêm da autoridade emissora autorizada e que não foram alterados.

a) **Algoritmo de assinatura**: O algoritmo de assinatura deve ser ES256 (ECDSA com SHA-256 e utilizando a curva P-256), conforme definido no RFC 9053 (secção 2.1); no COSE, o algoritmo é identificado pelo parâmetro do cabeçalho «alg» no RFC 9052 (secção 3.1).

b) **Chave de assinatura**: A carga útil do código QR deve ser assinada utilizando a chave privada correspondente a um certificado qualificado de selo eletrónico (QSealC).

c) **Estrutura COSE**: O contentor da assinatura deve ser um objeto COSE_Sign1. O cabeçalho protegido deve incluir os valores alg (ES256) e x5t [o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509 definido no RFC 9360 (secção 2); para efeitos de interoperabilidade, o algoritmo de dispersão utilizado no valor x5t deve ser SHA-256]. A verificação deve basear-se na utilização do valor x5t para localizar o certificado correspondente na lista de certificados de confiança armazenada na memória cache local do verificador, construída a partir de informações da Lista de Confiança e, em seguida, validar a cadeia de certificados e o estado do certificado em conformidade com o quadro de confiança eIDAS.

d) **Norma de assinatura**: A assinatura da carga útil do código QR deve ser um objeto COSE_Sign1, em conformidade com o RFC 9052 (secção 4), CBOR Object Signing and Encryption (*assinatura e codificação de objetos*). O objeto COSE_Sign1 deve ser transportado pelo issuerAuth e codificado sem a etiqueta CBOR para COSE_Sign1. O campo da carga útil do objeto COSE_Sign1 deve ser separado e codificado com um valor CBOR nulo. Para a criação e verificação da assinatura, a carga útil externa deve consistir na estrutura CBOR determinística que contém os valores docType e issuerSigned do mapa CBOR de nível superior.

e) **Algoritmo de dispersão (Hash)**: O SHA-256 é utilizado como parte do ES256 para gerar assinaturas e verificação da integridade.

f) **Codificação**: A carga útil deve ser codificada utilizando o CBOR (RFC 8949, secção 4.2), conforme exigido pelas especificações COSE e mDOC, para assegurar a codificação e a reprodutibilidade dos dados assinados.

3. **Especificações de impressão:**

a) **Zona em branco**: O código QR deve ser contornado, em todos os lados, por uma margem vazia de **quatro módulos** sem qualquer impressão, padrão ou fundo.

b) **Contraste**: O código QR deve ser impresso sobre um fundo branco, com uma relação de contraste mínima de **4:1**, a fim de assegurar uma elevada legibilidade em condições de iluminação variáveis.

c) O código QR deve ser impresso utilizando a cor definida no anexo II da Diretiva (UE) 2024/2841 que garanta o máximo contraste.

d) **Colocação e dimensão:** O código QR, incluindo a zona em branco, deve ser de **37 mm × 37 mm**, na parte da frente do cartão, ligeiramente à direita do centro, em direção à margem inferior. O código QR deve ser, no máximo, a versão 20 (97 × 97 módulos), com um módulo de dimensão igual ou superior a 0,35 mm.

O código QR, incluindo a sua zona em branco, deve estar posicionado a, pelo menos, 5 mm da margem inferior do cartão.

## 4. Dados no código QR do cartão europeu de estacionamento para pessoas com deficiência

O código QR deve conter um conjunto de dados mínimo verificável fora de linha, em conformidade com o princípio da minimização dos dados consagrado pelo artigo 5.º, n.º 1, alínea c), do Regulamento (UE) 2016/679. A estrutura da carga útil é a seguinte:

a) Os atributos do cartão são codificados no CBOR num objeto issuerSigned.

b) Esta estrutura é encapsulada e assinada pelo QSeal da autoridade emissora como emissorAuth (COSE_Sign1, ES256, incluindo um valor x5t, o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

c) O objeto CBOR/COSE resultante deve ser comprimido de acordo com o ponto 1, alínea d) do presente anexo. A carga útil do código QR deve consistir no prefixo «EP1:MDOC:», seguido da matriz de bytes comprimida resultante, e a carga útil completa deve ser codificada utilizando o formato binário como um único segmento de dados do código QR.

O conteúdo dos dados deve consistir num subconjunto de dados visíveis que figurem nos campos da parte da frente do cartão enumerados no anexo II da Diretiva (UE) 2024/2841 (data de expiração, número de série do cartão), juntamente com o identificador de revogação, a assinatura eletrónica e as informações sobre o esquema.

**A assinatura eletrónica** deve conter:

i) issuerAuth — objeto COSE_Sign1 assinado com a **chave privada QSealC** da autoridade emissora.

ii) cabeçalho protegido que inclui os valores alg = ES256 (algoritmo de assinatura) e x5t (o parâmetro de cabeçalho com o valor de dispersão do certificado COSE X.509).

## 5. Dados facultativos

Não devem ser incluídos dados facultativos no código QR.

## 6. Identificador de revogação

O identificador de revogação do cartão europeu de estacionamento para pessoas com deficiência deve cumprir o disposto no anexo I, ponto 6.

As listas para cartões europeus de estacionamento para pessoas com deficiência revogados devem fazer referência apenas ao identificador de revogação. Os números de série dos cartões não podem ser publicados nas listas de revogação.

## 7. Carga útil CBOR (dentro do QR) do cartão europeu de estacionamento para pessoas com deficiência

Apenas os seguintes dados devem ser incluídos na carga útil do QR, em consonância com os campos visíveis do cartão europeu de estacionamento para pessoas com deficiência estabelecidos no anexo II da Diretiva (UE) 2024/2841:

| **Campo** | **caminho de acesso mDOC** | **Tipo/Formato** |
|---|---|---|
| Versão do esquema de dados | issuerSigned.nameSpaces."eu.epc".ver | Cadeia de carateres alfanuméricos (p. ex., "1.0") |
| Tipo de cartão: cartão europeu de estacionamento para pessoas com deficiência | docType | Enum («eu.epc») |
| Número de série do cartão | issuerSigned.nameSpaces."eu.epc".sub | Cadeia de carateres alfanuméricos |
| Identificador de revogação | issuerSigned.nameSpaces."eu.epc".rid | CBOR bstr (16 bytes) |
| Data de validade do cartão | issuerSigned.nameSpaces."eu.epc".exp | Etiqueta CBOR 1004, conforme definida no RFC 8943 (secção 2.1), que contém uma cadeia de carateres de texto com codificação UTF-8 que representa uma data completa RFC 3339 no formato AAAA-MM-DD |

A assinatura eletrónica é transportada pelo issuerAuth (um objeto COSE_Sign1). A cadeia de certificados não pode ser incorporada na carga útil do código QR; em vez disso, o cabeçalho protegido COSE deve incluir um valor x5t, um código de identificação digital do certificado utilizado para localizar o QSealC correspondente na lista de certificados de confiança armazenada na memória cache do verificador.

8. **Exemplo de carga útil do código QR do cartão europeu de estacionamento para pessoas com deficiência: representação lógica comentada no estilo de notação de objetos JavaScript**

O exemplo que se segue é uma representação do esquema lógico do cartão europeu de deficiência em notação JSON que pode ser compreendida por humanos. Na prática, esta estrutura não pode ser compreendida por humanos, uma vez que:

a) É codificada no CBOR (RFC 8949, secção 3);

b) É assinada utilizando uma estrutura COSE_Sign1 sem etiqueta com uma carga útil separada (RFC 9052, secção 4);

c) Incluirá uma etiqueta CBOR 1004 com a data de expiração no formato de valor de data completa, de acordo com o RFC 8943 (secção 2.1);

d) Incluirá o parâmetro de cabeçalho protegido x5t, em conformidade com o RFC 9360, utilizando o SHA-256 sobre o QSealC de entidade final codificado em DER; e

e) É comprimida e pré-fixada com a cadeia de carateres EP1:MDOC: antes de ser codificada no código QR.

```
{
  // Apenas esquema lógico do cartão europeu de estacionamento para pessoas com deficiência, em formato JSON legível por humanos.
  // A carga útil real do código QR é CBOR determinístico e não JSON.
  "docType": "eu.epc", // credencial do cartão europeu de estacionamento para pessoas com deficiência. O valor docType está incluído, juntamente com
    // issuerSigned, na carga útil externa COSE_Sign1.

  "issuerSigned": {
    // Dados protegidos por issuerAuth; utilizado como carga útil separada.
 // Para a criação e verificação da assinatura, a carga útil externa separada abrange
    // docType e issuerSigned.
    "nameSpaces": {
      "eu.epc": {
        "ver": "1.0", // perfil QR/versão do esquema

        // Número de série do cartão; definido pelo emitente, máx. 24 carateres.
```

```
    "sub": "EF123456789012345678900GH",

    // Identificador de revogação: CBOR bstr real, 16 bytes/128 bits.
    // Apresentado aqui como 32 carateres hexadecimais para legibilidade.
    "rid": "4a8d9c112233445566778899aabbccdd",

    // A codificação CBOR real utiliza a etiqueta 1004 para a data completa RFC 3339.
    "exp": "2030-12-31"
   }
  }
},

"issuerAuth": {
 // Formulário efetivo: COSE_Sign1 sem etiqueta, não um objeto JSON.
 "type": "COSE_Sign1",
 "tagged": falso,       // codificado sem etiqueta CBOR COSE_Sign1
 "payload": "detached", // O campo da carga útil COSE é CBOR nulo.

 "protectedHeader": {
  // alg: ES256; parâmetro de cabeçalho COSE equivalente 1 = -7.
  "alg": "ES256",

  // x5t: código de identificação digital do certificado; parâmetro de cabeçalho COSE 34.
  "x5t": {
   "hashAlg": "SHA-256", valor de dispersão equivalente COSE -16

   // Valor de dispersão SHA-256 do QSealC de entidade final codificado em DER.
```

```
        // 32 bytes representados por 64 carateres hexadecimais.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // em branco neste exemplo

    // Assinatura ES256 COSE: 64 bytes = 128 carateres hexadecimais.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

## 9. Utilização de mecanismos criptográficos

A utilização de mecanismos criptográficos no contexto do presente anexo deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA).

## ANEXO III

## NOTIFICAÇÃO DAS INFORMAÇÕES A QUE SE REFERE O ARTIGO 6.º, n.º 2,

1. Os Estados-Membros devem fornecer à Comissão as seguintes informações sobre cada autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência:

   a) O nome da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   b) Um número de registo da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   c) Um endereço de correio eletrónico e número de telefone de contacto da autoridade ou do organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência;

   d) Um ou mais certificados que possam ser utilizados para verificar o selo eletrónico criado pela autoridade ou pelo organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência que a autoridade ou organismo emite, e relativamente aos quais os dados de identificação certificados incluam o nome e o número de registo do emitente, conforme especificado nas alíneas a) e b), respetivamente;

   e) o URL da localização onde o emitente publica o estado de validade das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência.

2. Os Estados-Membros podem fornecer à Comissão as seguintes informações sobre cada autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência:

   a) O URL da página Web em que se apresentam as políticas e as condições da autoridade ou organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência aplicáveis à disponibilização e utilização das versões físicas do cartão europeu de deficiência e do cartão europeu de estacionamento para pessoas com deficiência que a autoridade ou organismo disponibiliza;

   b) Se for caso disso, o URL da página Web em que se apresentam informações adicionais sobre a autoridade ou o organismo competente responsável pela emissão das versões físicas do cartão europeu de deficiência ou do cartão europeu de estacionamento para pessoas com deficiência.

## ANEXO IV

## ESPECIFICAÇÕES TÉCNICAS PARA UMA LISTA DE REVOGAÇÃO DAS VERSÕES FÍSICAS DO CARTÃO EUROPEU DE DEFICIÊNCIA OU DO CARTÃO EUROPEU DE ESTACIONAMENTO PARA PESSOAS COM DEFICIÊNCIA

1. Para efeitos do presente anexo, o identificador deve corresponder ao identificador de revogação definido no anexo I, ponto 6, e no anexo II, ponto 6.

2. Deve ser implementada uma lista de revogação sob a forma de um *token* da lista de identificadores no formato CWT (RFC 8392, secção 7), em conformidade com a cláusula 5.2 da especificação relativa à lista de estado do *token* (draft-ietf-oauth-status-list-14), com as seguintes alterações:

   a) O valor do atributo-tipo deve ser “application/identifierlist+cwt”;

   b) O atributo do prazo de validade deve estar respeitado;

   c) O atributo StatusList não deve estar presente no conjunto de atributos CWT;

   d) A estrutura IdentifierList definida no ponto 3 deve estar presente como um atributo no conjunto de atributos CWT estabelecidos que utilizem a chave 65530;

   e) O CWT deve ser um objeto COSE_Sign1 que utiliza, para o cálculo da assinatura, um algoritmo de assinatura em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela Agência da União Europeia para a Cibersegurança (ENISA);

   f) O CWT deve conter o parâmetro da cadeia x5, conforme definido no RFC 9360 (secção 2), no cabeçalho protegido que contém o certificado ou a cadeia de certificados para verificar a assinatura da lista de revogação;

   g) O OID de utilização alargada da chave indicado na especificação da lista de estado do *token* (draft-ietf-oauth-status-list-14) pode ser utilizado para o certificado de assinatura da lista de identificadores e recomenda-se que os verificadores apoiem o OID de utilização alargada da chave indicado na especificação da lista de estado do *token* e que as infraestruturas da autoridade emissora não tornem crítico o campo de utilização alargada da chave quando utilizam o OID de utilização alargada da chave indicado na especificação da lista de estado do *token*.

3. A estrutura IdentifierList deve ser uma estrutura CBOR com a Concise Data Definition Language (CDDL) seguinte:

```
IdentifierList = {
 "identifiers": { * Identifier => IdentifierInfo },
   ? "aggregation_uri": Aggregation_uri,
   * Tstr = > RFU
}

IdentifierInfo = {
```

```
    (tstr / int) => RFU
}

Identifier = bstr

Aggregation_uri = tstr
```