Official Journal
of the European Union

EN
L series

2026/1436

12.11.2026

COMMISSION DELEGATED REGULATION (EU) 2026/1436

of 1 July 2026

supplementing Directive (EU) 2024/2841 of the European Parliament and of the Council as regards setting the QR code on the physical version of the European Disability Card and setting the QR code and establishing common technical specifications that ensure the security of the physical version of the European Parking Card for persons with disabilities, as well as interoperability matters

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2024/2841 of the European Parliament and of the Council of 23 October 2024 establishing the European Disability Card and the European Parking Card for persons with disabilities ([1]), and in particular Article 7(7) and Article 8(7) thereof,

Whereas:

(1) Directive (EU) 2024/2841 lays down the rules governing the issuance of the European Disability Card and the European Parking Card for persons with disabilities and common templates for those cards. In accordance with Article 7(2) and Article 8(2) of Directive (EU) 2024/2841, European Disability Cards and European Parking Cards for persons with disabilities issued by Member States are to be mutually recognised in all Member States.

(2) The empowerments provided by Article 7(7) and Article 8(7) of Directive (EU) 2024/2841 have the same purpose, namely the prevention and combat of fraud, the security of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities, including through appropriate security measures for personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]), as well as ensuring interoperability. As the subject matter and objectives of the empowerments largely coincide, it is appropriate to lay down rules supplementing Directive (EU) 2024/2841 as regards those matters in a single delegated act.

(3) Directive (EU) 2024/2841 provides for the physical versions of the European Disability Card and the European Parking Card for persons with disabilities to contain a QR code as a state-of-the-art digital feature that uses electronic means to prevent and combat fraud. As such, QR codes are a mandatory digital feature to be printed on all physical cards. To ensure a uniform approach in the creation and use of the QR codes by the Member States, the Commission should adopt technical specifications to set the QR codes, including their content.

(4) The European Parking Card for persons with disabilities will replace all existing parking cards for persons with disabilities issued in accordance with Council Recommendation 98/376/EC ([3]). That Recommendation has not been updated to reflect technological and digitalisation developments and Member States have experienced problems with fraud and forgery. Therefore, it is necessary to establish the features that ensure the security of the physical version of the European Parking Card for persons with disabilities, which take into account its specificities such as the fact that it is usually behind the windscreen of the vehicle.

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

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Council Recommendation 98/376/EC of 4 June 1998 on a parking card for people with disabilities (OJ L 167, 12.6.1998, p. 25, ELI: http://data.europa.eu/eli/reco/1998/376/oj).

(5) Mandatory common technical specifications should be introduced to ensure the security of the physical version of the European Parking Card for persons with disabilities. Printing the card on an appropriate material, such as polycarbonate, using a diffractive optically variable image device would effectively protect against forgery and falsification. Anti-scan patterns would further increase security by making card duplication detectable, as they should contain a hidden text or a pattern, which would appear when the card is photocopied or scanned. Those features are to be applied without affecting the format of the physical version of the European Parking Card for persons with disabilities set out in Annex II to Directive (EU) 2024/2841, including the visual appearance of the card.

(6) In addition to the QR code and other mandatory technical specifications established by this Regulation, Member States should have the possibility to incorporate optional digital or physical security features, based on common technical specifications laid down in this Regulation, in the physical version of the European Parking Card for persons with disabilities to enhance its security. Where optional digital features contain more personal data than those provided for in the physical versions of the cards, in accordance with point 3(b) of Annex II to Directive (EU) 2024/2841 access to such data is to be limited to public authorities of the issuing Member States and only to authorised users. To maintain a harmonised framework for security features across Member States, the list of optional features should be exhaustive. Moreover, Member States should ensure that the integration of one or more of the optional digital or physical security features does not affect the recognition of valid cards from other Member States or compromise interoperability and the functionality of the mandatory technical specifications.

(7) The physical version of the European Parking Card for persons with disabilities may contain a radio-frequency identification (RFID) chip as an optional digital security feature. RFID makes use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it ([4]). RFID chips can strengthen protection against forgery and tampering through securely storing or transmitting card-related data. The physical version of the European Parking Card for persons with disabilities may also contain optically variable ink or colour-shifting ink. Such inks provide adequate protection against copying of and tampering with the card without requiring personalisation. To ensure that the card's data are properly secured against counterfeiting and falsification attempts, the text of the data fields may be integrated into the basic material of the card using laser-engraving technology. Physical security features, whether set as mandatory or optional in this Regulation, which are not visible or that become visible following certain manipulations do not contradict the format of the European Parking Card for persons with disabilities set out in Annex II to Directive (EU) 2024/2841.

(8) Technological advancements, parking verification systems and security risks are continuously evolving. The state of the art develops and the usage of the European Disability Card and the European Parking Card for persons with disabilities evolves, driven by both user feedback and technological progress, and so do techniques of fraud and forgery, leading to evolving security challenges. Therefore, new technological solutions, including those in parking verification, as well as security and anti-fraud prevention needs might necessitate changes in the security and anti-fraud architecture of the cards, including through updating the categorisation of digital features as either mandatory or optional. Depending on technological developments this may necessitate the update of this Regulation.

(9) To ensure that the physical versions of the European Disability Card and the European Parking Card for persons with disabilities can be used seamlessly across all Member States, it is necessary to guarantee interoperability of the digital features on the physical cards, in particular the QR codes. Interoperability should enable the verification of the authenticity and validity of the physical versions of the cards by card verifiers - any natural or legal person who verifies the validity and authenticity of the physical versions of the cards, for example by means of a verification application. To that end, it is necessary to lay down provisions on matters relating to interoperability so as to enable cross-border verifications of the physical versions of the cards to be performed in a consistent and reliable manner.

([4]) Commission Recommendation 2009/387/EC of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (OJ L 122, 16.5.2009, p. 47, ELI: http://data.europa.eu/eli/reco/2009/387/oj).

(10) To ensure the integrity and origin of the data contained in the QR codes on the physical versions of the European Disability Card and the European Parking Card for persons with disabilities, that data should be sealed with a qualified electronic seal as defined in Article 3, point (27), of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([5]). The QR code confirms the authenticity and validity of the physical card, when cross-checked against the verification parameters, and should not in itself attest the disability status or the entitlement to specific services based on a disability.

(11) In order to facilitate interoperability and the establishment of a trustworthy and secure verification system of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities across the Union, information notification and publication mechanisms should be established. In this regard, and in order to enable the verification that the physical versions of the cards are issued by a competent authority or body, Member States should provide the information necessary for the verification process, specifically the information required to verify the qualified electronic seal. Therefore, the Member States should be required to notify the Commission of the competent authorities or bodies responsible for issuing the physical versions of the cards (card issuers), as well as the relevant administrative and technical information relating to them. The information to be notified to the Commission should be limited to what is necessary to establish interoperable verification mechanisms for verifying the validity and authenticity of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities. The Commission should ensure public access to that information.

(12) Furthermore, in the event of card revocation, information about the revocation of the card should be promptly made available to enable card verifiers to verify the validity of the card. For this purpose, card issuers should maintain and publish in a timely manner lists containing information on the revocation status of all cards that they have revoked prior to their expiry dates (revocation lists). Such publication should respect the privacy and protect the personal data of the card holders. Moreover, revocation lists should not contain any personal data other than the unique revocation identifiers and should be published at a specific Uniform Resource Identifier (URI) in accordance with technical specifications to ensure interoperable verification.

(13) To read the QR code and verify the authenticity and validity of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities, customised verification applications at national level, may be used. The Commission can support this process by providing a common sample source code for the purpose of reading data contained in the QR codes, and for performing the main steps of the verification process, which can serve as a basis for the verification applications in Member States. All verification applications should perform the same trust-chain verification logic against the same trust infrastructure, thereby enabling the reading of data encoded in the cards by the issuing Member State. In addition, Annex I to Directive (EU) 2019/882 of the European Parliament and of the Council ([6]) sets out accessibility requirements to be complied with by Member States, where applicable.

(14) Recognising the dynamic nature of technological advancements and evolving cybersecurity threats, the Union is committed to ensuring that cryptographic mechanisms employed within its regulatory framework remain effective and secure. In light of this commitment, it is important to adopt cryptographic standards endorsed by the European Cybersecurity Certification Group and disseminated through the European Union Agency for Cybersecurity (ENISA).

(15) Regulation (EU) 2016/679 applies to the processing of personal data under this Regulation. In particular, the verification of the QR codes on the physical versions of the European Disability Card and the European Parking Card for persons with disabilities involves the processing of personal data. Therefore, appropriate data protection safeguards should be established to ensure the protection of personal data contained in the QR codes in compliance with Regulation (EU) 2016/679, where applicable. The general security measures provided in this Regulation should also ensure protection of personal data contained in the QR codes. In addition, the personal data contained in the QR codes should be limited to what is strictly necessary for the purpose of this Regulation. Moreover, retention of the data after the verification is completed should be prohibited. It is also necessary to ensure appropriate security of the revocation lists.

([5]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([6]) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

(16) In accordance with Article 14(4) of Directive (EU) 2024/2841, in the preparation of this Regulation the Commission consulted persons with disabilities and their representative organisations as well as experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([7]).

(17) The European Disability Card and the European Parking Card for persons with disabilities constitute a trans-European digital public service within the meaning of Regulation (EU) 2024/903 of the European Parliament and of the Council ([8]). Accordingly, an interoperability assessment has been carried out, and the resulting report is to be published on the Interoperable Europe Portal referred to in Article 8 of Regulation (EU) 2024/903.

(18) The European Data Protection Supervisor was consulted on this Regulation in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([9]) and it delivered an opinion on 12 May 2026,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

This Regulation lays down the rules supplementing Directive (EU) 2024/2841 as regards:

(a) setting the QR code for the physical versions of the European Disability Card and the European Parking Card for persons with disabilities, including appropriate security measures for personal data;

(b) establishing common mandatory and optional technical specifications that ensure the security of the physical version of the European Parking Card for persons with disabilities;

(c) setting interoperability requirements necessary to ensure that QR codes on the physical versions of the European Disability Card or the European Parking Card for persons with disabilities issued in one Member State can be reliably read and verified in another Member State.

Article 2

QR code on the physical version of the European Disability Card

The specifications for the QR code that is to appear on the physical version of the European Disability Card shall be those set out in Annex I.

Article 3

QR code on the physical version of the European Parking Card for persons with disabilities

The specifications for the QR code that is to appear on the physical version of the European Parking Card for persons with disabilities shall be those set out in Annex II.

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

([8]) Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([9]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Article 4

Mandatory common technical specifications for the European Parking Card for persons with disabilities

1. The physical versions of the European Parking Card for persons with disabilities shall comply with the following common technical specifications:

(a) they shall be made of a material which protects against delamination and is capable of complying with the requirements set out in Annex II to the Directive (EU) 2024/2841 and other mandatory common technical specifications set out in this Article;

(b) they shall contain a diffractive optically variable image device as an element of layered structure which becomes visible when the card is looked at from a certain angle;

(c) they shall be made using an anti-scan pattern which becomes visible when a card is photocopied or scanned.

2. The diffractive optically variable image device referred to in paragraph 1, point (b), shall appear on the front side of the physical version of the European Parking Card for persons with disabilities over one or more of the data fields on the left-hand side. It shall be approximately 20 mm in height and 20 mm in width. The image shown on the device shall consist of a stylised map of the issuing Member State or the distinguishing code of the issuing Member State surrounded by the circle of 12 stars symbolising the Union.

3. The anti-scan pattern referred to in paragraph 1, point (c), shall be located on the front side of the physical version of the European Parking Card for persons with disabilities above the data fields on the left-hand side and/or on the right-hand side outside the QR code and its quiet zone. It shall contain a hidden text or pattern, which would appear when the card is photocopied or scanned. Where the anti-scan pattern contains a hidden text, it shall consist of the words 'COPY' or 'VOID', and a translation thereof in one or more official languages of the issuing Member State. Where the anti-scan pattern contains a hidden pattern, it shall be composed of horizontal or vertical lines.

Article 5

Optional technical specifications and features for the security of the European Parking Card for persons with disabilities

1. In addition to the mandatory common technical specifications referred to in Article 4, Member States may apply only the optional technical specifications and features laid down in this Article.

2. Physical versions of the European Parking Card for persons with disabilities may contain a radio-frequency identification (RFID) chip. The RFID chip shall prevent and combat fraud through electronic means and serve as an additional means for verification of the authenticity and/or validity of a physical version of the European Parking Card for persons with disabilities at national level. The RFID chip shall not affect the functioning of the QR code on the card.

3. Any RFID chip referred to in paragraph 2 shall comply with the following specifications:

(a) it shall be passive;

(b) it shall be physically integrated into the body of the card on the front right-hand side;

(c) it shall be logically linked to the QR code record and shall contain the same revocation identifier (RID) as that encoded in the QR code;

(d) the RFID feature shall support reading at approximately 1 metre or more where required for operational use, but shall not be designed for reliable reading beyond 5 metres under reference test conditions;

(e) after issuance of the card, write access to the RFID chip, or to the relevant data area thereof, shall be prevented or otherwise controlled by the issuing authority;

(f) it shall be designed and configured so as to minimise the risk of cloning, substitution, unauthorised modification and unauthorised rewriting;

(g) it shall comply with the requirements of Directive 2014/53/EU of the European Parliament and of the Council ([10]);

(h) in addition to the RID referred to in point (c), the RFID chip may store only one or more of the following:

(i) data encoded in the QR code of the physical version of the European Parking Card for persons with disabilities;

(ii) vehicle plate number(s);

(iii) cryptographic verification data.

4. The front side of the physical versions of the European Parking Card for persons with disabilities may contain one or more of the following features:

(a) the wheelchair symbol on the left-hand side or the words European Parking Card for persons with disabilities in English and one or more official languages of the issuing Member State on the right-hand side, printed with optically variable ink or colour shifting ink, revealing changing colours when viewed from different angles;

(b) the use of laser-engraving technology that penetrates into the card layers to print the text in the data fields.

5. The introduction of optional technical specifications and features referred to in this Article shall not affect the recognition, in the Member State having introduced such features for the cards it issues, of valid cards issued in other Member States.

Article 6

Interoperability matters

1. The information included in the QR code shall be sealed with a qualified electronic seal within the meaning of Article 3, point (27), of Regulation (EU) No 910/2014.

2. Each Member State shall communicate to the Commission information about competent authorities or bodies responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities ("card issuers"), and any subsequent updates to that information in accordance with Annex III. The Commission shall ensure public access to that information.

3. Card issuers shall maintain and publish at a Uniform Resource Identifier that is notified to the Commission up-to-date revocation lists containing information on the revocation status of all cards that they have revoked in accordance with the technical specifications laid down in Annex IV. Information about the revocation shall be published within 24 hours of that revocation.

4. Member States may use verification applications to verify the authenticity and validity of the physical versions of the European Disability Card and European Parking Card for persons with disabilities.

5. Where Member States use verification applications to verify the authenticity and validity of the physical versions of the European Disability Card and European Parking Card for persons with disabilities, such applications shall be capable of verifying the authenticity and validity of a card by checking the electronic seal and the revocation status of the card. These verification applications shall read, and present a visual representation of, the personal data encoded in the QR code of the card, as set out in Annexes I and II, to allow for a comparison with the data visible in the corresponding data fields on the card, and an indication concerning the validity status of the card.

([10]) Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62, ELI: http://data.europa.eu/eli/dir/2014/53/oj).

Article 7

Security measures for the protection of personal data

1. The personal data contained in the QR codes on the physical versions of the European Disability Card and the European Parking Card for persons with disabilities shall be limited to what is strictly necessary to verify the authenticity and validity of the cards, as set out in Annexes I and II.

2. Following the completion of the verification of the authenticity and validity of a physical version of the European Disability Card or the European Parking Card for persons with disabilities by card verifiers, the data contained in the QR codes shall not be retained by the card verifiers.

3. The verification of a QR code on a physical version of the European Disability Card or the European Parking Card for persons with disabilities shall not result in the competent authority or body responsible for issuing the card being notified of that verification.

4. Information included in a revocation list published in accordance with Article 6(3) shall be limited to the revocation identifier of revoked cards.

5. The authority or body responsible for publishing the revocation lists in accordance with Article 6(3) shall ensure that appropriate technical and organisational security measures apply to the processing of personal data contained in revocation lists.

6. Where a Member State decides to incorporate an RFID chip in the physical version of the European Parking Card for persons with disabilities, paragraphs 2 to 3 shall apply to the processing of the personal data contained in that chip. The personal data contained in the RFID chip shall be limited to what is strictly necessary to verify the authenticity and/or validity of the cards, as set out in Article 5(3).

Where a Member State stores in the RFID chip personal data referred to in Article 5, which is not provided for in the physical version of the European Parking Card for persons with disabilities as set out in Annex II to Directive (EU) 2024/2841, access to such data shall be limited to public authorities of the issuing Member State and only to authorised users.

Article 8

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 1 July 2026.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

QR CODE SPECIFICATIONS FOR THE PHYSICAL VERSION OF THE EUROPEAN DISABILITY CARD

1. **Format of the QR code for the physical version of the European Disability Card (EDC)**

(a) **QR code Model 2 format**, in accordance with the international QR code specifications ISO/IEC 18004:2024 or equivalent.

(b) **Error Correction Level M** (15 % redundancy) ensuring resilience to scratches or partial damage of a printed QR code.

(c) **Encoding Mode**: The QR payload shall consist of the combined issuerSigned Concise Binary Object Representation (CBOR) structure and the corresponding issuerAuth COSE_Sign1 signature object as defined in CBOR Object Signing and Encryption (COSE, RFC 9052 Sections 3.1, 4.2 and 4.4), following the mDOC data-model pattern for issuerSigned items, but adapted for static physical-card use. The issuerAuth shall be a COSE_Sign1 object with alg = ES256 and a protected header containing x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256).

(d) Prior to QR code encoding, the combined CBOR/COSE object shall be **compressed using zlib format** (RFC 1950, section 2.2) **with the deflate** algorithm (RFC 1951 sections 3.2 and 4). The resulting compressed byte array shall be encoded in **QR code Byte Mode**, ensuring full support for binary CBOR/COSE payloads and scanner interoperability.

For all text fields included in the QR payload, issuers shall encode characters as Unicode UTF-8 within CBOR text strings. Transliteration shall not be applied to signed payload data. For interoperability purposes, issuers shall apply Unicode Normalisation Form C (NFC) to all textual fields before signing.

(e) **Prefix**: The EDC QR string shall begin with 'ED1:MDOC:'. This identifies card type and encoding profile. Prefixes are case-sensitive and must be present. Unknown or unsupported prefixes shall cause rejection. The prefix and the compressed payload shall be encoded as a single Byte Mode data segment in the QR code.

(f) **Minimum Module Size ≥ 0,25 mm** to ensure readability on printed cards.

(g) **Maximum Version 20**, with up to 97 × 97 modules on each side.

2. **EDC Signature Generation Specifications**

The qualified electronic seal (QSeal) used to seal EDC QR codes ensures that the encoded data originate from the authorised issuing authority and have not been altered.

(a) **Signature Algorithm**: The signature algorithm shall be ES256 (Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA-256 using the P-256 curve), as defined in RFC 9053 (section 2.1); in COSE, the algorithm is identified by the alg header parameter in RFC 9052 (section 3.1).

(b) **Signing Key**: The QR payload shall be signed using the private key corresponding to a Qualified Certificate for Electronic Seal (QSealC).

(c) **COSE Structure**: The signature container shall be a COSE_Sign1 object. The protected header shall include alg (ES256) and x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256). Verification shall rely on using the x5t value to locate the corresponding certificate in the verifier's locally cached trust store built from Trusted List information and shall then validate the certificate chain and certificate status in accordance with the eIDAS trust framework.

(d) **Signature Standard**: The QR code payload shall be signed as a COSE_Sign1 object in accordance with RFC 9052 (section 4), CBOR Object Signing and Encryption. The COSE_Sign1 object shall be carried in issuerAuth and encoded without the CBOR tag for COSE_Sign1. The payload field of the COSE_Sign1 object shall be detached and encoded as CBOR null. For signature generation and verification, the external payload shall be the deterministic-CBOR encoded structure containing the docType value and the issuerSigned value from the top-level CBOR map.

(e) **Hash Algorithm**: SHA-256 shall be used as part of ES256 for signature generation and integrity verification.

(f) **Encoding**: The payload shall be encoded using CBOR (RFC 8949, section 4.2), as required by the COSE and mDOC specifications, ensuring encoding and reproducibility of the signed data.

3. **Printing Specifications**

(a) **Quiet Zone**: A clear margin of **4 modules** shall surround the QR code on all sides, free of any print, pattern, or background.

(b) **Contrast**: QR code shall be printed on a white background, with a minimum contrast ratio of **4:1**, to ensure high readability under varying lighting conditions.

(c) The QR code shall be printed using the colour defined in Annex I to Directive (EU) 2024/2841 that ensures maximum contrast.

(d) **Placement and Size**: The QR code, including the quiet zone, shall be 26,25 mm × 26,25 mm, located on the reverse side of the card at the bottom-right corner. The QR code shall be maximum Version 20 (97 × 97 modules), with a module size of 0,25 mm or larger.

The QR code, including its quiet zone, shall be positioned at least 5 mm from the right-hand edge and at least 5 mm from the bottom edge of the card.

4. **Data in the EDC QR code**

The QR code shall contain a minimal, offline-verifiable dataset in compliance with the data minimisation principle laid down in Article 5(1), point (c), of Regulation (EU) 2016/679. The payload structure shall be as follows:

(a) Card attributes are encoded in CBOR within an issuerSigned object.

(b) The structure is wrapped and signed by the issuing authority's QSeal as an issuerAuth (COSE_Sign1, ES256, including x5t, the COSE X.509 certificate hash header parameter).

(c) The resulting CBOR / COSE object shall be compressed in accordance with point 1(d) of this Annex. The QR code payload shall consist of the prefix 'ED1:MDOC:', followed by the resulting compressed byte array, and the complete payload shall be encoded using Byte Mode as a single QR code data segment.

Data contents shall consist of a sub-set of visible data from the front card fields listed in Annex I to Directive (EU) 2024/2841 (name, surname, card serial number, expiry date), together with the revocation identifier, electronic signature, and schema information.

Electronic signature shall contain:

(i) issuerAuth – A COSE_Sign1 object signed with the issuing authority's **QSealC private key**.

(ii) protected header that includes alg = ES256 (signature algorithm) and x5t (the COSE X.509 certificate hash header parameter).

5. **Optional Data**

No optional data shall be included in the QR code.

6. **Revocation Identifier (RID)**

In addition to the visible card serial number the QR code shall include a dedicated revocation identifier (RID).

The RID shall be used for determining revocation status and for revocation list management. The RID shall not be printed on the card and it shall not be displayed to the card verifiers.

6.1. *Requirements for the RID*

The RID shall:

(a) be included in the signed QR payload;

(b) be unique at least within the issuing authority's issuance domain;

(c) not be printed on the card and not intended to be human readable;

(d) not reveal personal data and not be directly meaningful;

(e) not be directly derivable from the visible card serial number; and

(f) be cryptographically bound to the QR payload by the qualified electronic seal.

6.2. *RID format and size*

The RID shall be encoded as a CBOR byte string (bstr). The RID shall be 16 bytes (128 bits) in length.

The RID shall be generated by the issuing authority using a method under its control that ensures sufficient entropy and resistance to guessing or enumeration.

6.3. *Revocation Lists*

Revocation lists published for verification purposes shall reference only the RID of revoked cards. Card serial numbers shall not be published in revocation lists.

7. **CBOR payload (inside the QR code) of EDC**

Only the following data shall be included inside the QR payload, consistent with the visible EDC data fields laid down in Annex I to Directive (EU) 2024/2841.

Top level contents:

(a) docType = "eu.edc"

(b) issuerSigned.nameSpaces."eu.edc" with attributes shown in table below

(c) issuerAuth = COSE_Sign1 (QSeal)

Field	mDOC path	Type/Format
Data schema version	issuerSigned.nameSpaces."eu.edc".ver	String (e.g., "1.0")
Card type: EDC	docType	Enum ("eu.edc")
Card Serial Number	issuerSigned.nameSpaces."eu.edc".sub	String
Revocation Identifier	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 bytes)
First name of cardholder	issuerSigned.nameSpaces."eu.edc".givenName	Unicode text string (UTF-8)
Surname of cardholder	issuerSigned.nameSpaces."eu.edc".familyName	Unicode text string (UTF-8)
Expiry date of card	issuerSigned.nameSpaces."eu.edc".exp	CBOR tag 1004, as defined in RFC 8943 (section 2.1), containing a UTF-8 text string representing an RFC 3339 full-date in YYYY-MM-DD format.

The electronic signature is carried in issuerAuth (a COSE_Sign1 object). The certificate chain shall not be embedded in the QR code payload; instead, the protected COSE header shall include x5t, a certificate thumbprint used to locate the corresponding QSealC in the verifier's cached trust store.

8. **EDC QR code payload example: commented JavaScript Object Notation-style logical representation**

The following example is a human readable JavaScript Object Notation (JSON) representation of the EDC logical view. In practice, this structure shall not be human readable as it shall be:

(a) Encoded in CBOR (RFC 8949, section 3);

(b) Signed using untagged COSE_Sign1 structure with a detached payload (RFC 9052, section 4),

(c) include the expiry date as a CBOR tag 1004 full-date value in accordance with RFC 8943 (section 2.1);

(d) include the x5t protected-header parameter in accordance with RFC 9360, using SHA-256 over the DER-encoded end-entity QSealC; and

(e) compressed and prefixed with the string ED1:MDOC: before being encoded in the QR code.

```
{
  // JSON-style, human-readable EDC logical view only.
  // Actual QR payload is deterministic CBOR, not JSON.
  "docType": "eu.edc", // EDC credential. The docType value is included, together with
     //issuerSigned, in the COSE_Sign1 external payload.

  "issuerSigned": {
     // Data protected by issuerAuth; used as detached payload.
     // For signature generation and verification, the detached external payload covers both
     // docType and issuerSigned.
     "nameSpaces": {
       "eu.edc": {
         "ver": "1.0", // QR profile/schema version

         // Card serial number; issuer-defined, max. 24 characters.
         "sub": "AB123456789012345678 90CD",

         // Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
         // Shown here as 32 hex characters for readability.
         "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

         "givenName": "Ann", // first name printed on the EDC
         "familyName": "Other", // surname printed on the EDC

         // Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
         "exp": "2030-12-31"
       }
     }
   },

   "issuerAuth": {
     // Actual form: untagged COSE_Sign1, not a JSON object.
     "type": "COSE_Sign1",
```

```
    "tagged": false, // encoded without COSE_Sign1 CBOR tag
    "payload": "detached", // COSE payload field is CBOR null

    "protectedHeader": {
      // alg: ES256; equivalent COSE header parameter 1 = -7.
      "alg": "ES256",

      // x5t: certificate thumbprint; COSE header parameter 34.
      "x5t": {
        "hashAlg": "SHA-256", // equivalent COSE hash value -16

        // SHA-256 hash of DER-encoded end-entity QSealC.
        // 32 bytes represented as 64 hex characters.
        "hashValue":
        "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // empty in this example

    // ES256 COSE signature: 64 bytes = 128 hex characters.
    "signature":
    "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
    f0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```


9. **Use of cryptographic mechanisms**

The use of cryptographic mechanisms in the context of this Annex shall be in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA).

ANNEX II

QR CODE SPECIFICATIONS FOR THE PHYSICAL VERSION OF THE EUROPEAN PARKING CARD FOR PERSONS WITH DISABILITIES

1. **Format of the QR code on the physical version of the European Parking Card for persons with disabilities (EPC)**

(a) **QR code Model 2 format**, in accordance with the international QR code specifications ISO/IEC 18004:2024 or equivalent.

(b) **Error Correction Level M** (15 % redundancy) ensuring resilience to scratches or partial damage of printed QR code.

(c) **Encoding Mode**: The QR payload shall consist of the combined issuerSigned Concise Binary Object Representation (CBOR) structure and the corresponding issuerAuth COSE_Sign1 signature object as defined in CBOR Object Signing and Encryption (COSE, RFC 9052 Sections 3.1, 4.2 and 4.4), following the mDOC data-model pattern for issuerSigned items, but adapted for static physical-card use. The issuerAuth shall be a COSE_Sign1 object with alg = ES256 and a protected header containing x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256).

(d) Prior to QR code encoding, the combined CBOR/COSE object shall be **compressed using zlib format (RFC 1950, section 2.2) with the deflate** algorithm (RFC 1951, sections 3.2 and 4). The resulting compressed byte array shall be encoded in **QR code Byte Mode**, ensuring full support for binary CBOR/COSE payloads and scanner interoperability.

For all text fields included in the QR payload, issuers shall encode characters as Unicode UTF-8 within CBOR text strings. Transliteration shall not be applied to signed payload data. For interoperability purposes, issuers shall apply Unicode Normalisation Form C (NFC) to all textual fields before signing.

(e) **Prefix**: The EPC QR string shall begin with 'EP1:MDOC:'. This identifies card type and encoding profile. Prefixes are case-sensitive and must be present. Unknown or unsupported prefixes shall cause rejection. The prefix and the compressed payload shall be encoded as a single Byte Mode data segment in the QR code.

(f) **Minimum Module Size ≥ 0,35 mm** to ensure readability on printed cards.

(g) **Maximum Version 20**, with up to 97 × 97 modules on each side.

2. **EPC Signature Generation Specifications**

The qualified electronic seal (QSeal) used to seal EPC QR codes ensures that the encoded data originate from the authorised issuing authority and have not been altered.

(a) **Signature Algorithm**: The signature algorithm shall be ES256 (ECDSA with SHA-256 using the P-256 curve), as defined in RFC 9053 (section 2.1); in COSE, the algorithm is identified by the alg header parameter in RFC 9052 (section 3.1).

(b) **Signing Key**: The QR payload shall be signed using the private key corresponding to a Qualified Certificate for Electronic Seal (QSealC).

(c) **COSE Structure**: The signature container shall be a COSE_Sign1 object. The protected header shall include alg (ES256) and x5t (the COSE X.509 certificate hash header parameter defined in RFC 9360 (section 2); for interoperability, the hash algorithm used in x5t shall be SHA-256). Verification shall rely on using the x5t value to locate the corresponding certificate in the verifier's locally cached trust store built from Trusted List information and shall then validate the certificate chain and certificate status in accordance with the eIDAS trust framework.

(d) **Signature Standard**: The QR code payload shall be signed as a COSE_Sign1 object in accordance with RFC 9052 (section 4), CBOR Object Signing and Encryption. The COSE_Sign1 object shall be carried in issuerAuth and encoded without the CBOR tag for COSE_Sign1. The payload field of the COSE_Sign1 object shall be detached and encoded as CBOR null. For signature generation and verification, the external payload shall be deterministic-CBOR encoded CBOR structure containing the docType value and the issuerSigned value from the top-level CBOR map.

(e) **Hash Algorithm**: SHA-256 is used as part of ES256 for signature generation and integrity verification.

(f) **Encoding**: The payload shall be encoded using CBOR (RFC 8949, section 4.2), as required by the COSE and mDOC specifications, ensuring encoding and reproducibility of the signed data.

3. **Printing Specifications**

(a) **Quiet Zone**: A clear margin of **4 modules** shall surround the QR code on all sides, free of any print, pattern, or background.

(b) **Contrast**: QR code shall be printed on a white background, with a minimum contrast ratio of **4:1**, to ensure high readability under varying lighting conditions.

(c) The QR code shall be printed using the colour defined in Annex II to Directive (EU) 2024/2841 that ensures maximum contrast.

(d) **Placement and Size**: The QR code, including the quiet zone, shall be **37 mm × 37 mm**, located on the front of the card, slightly off-centre to the right, towards the bottom edge. The QR code shall be maximum version 20 (97 × 97 modules), with module size of 0,35 mm or larger.

The QR code, including its quiet zone, shall be positioned at least 5 mm from the bottom edge of the card.

4. **Data in EPC QR code**

The QR code shall contain a minimal, offline-verifiable dataset in compliance with the data minimisation principle contained in Article 5(1), point (c), of Regulation (EU) 2016/679. The payload structure is as follows:

(a) Card attributes are encoded in CBOR within an issuerSigned object.

(b) This structure is wrapped and signed by the issuing authority's QSeal as an issuerAuth (COSE_Sign1, ES256, including x5t, the COSE X.509 certificate hash header parameter).

(c) The resulting CBOR / COSE object shall be compressed in accordance with point 1(d) of this Annex. The QR code payload shall consist of the prefix 'EP1:MDOC:', followed by the resulting compressed byte array, and the complete payload shall be encoded using Byte Mode as a single QR code data segment.

Data contents shall consist of a sub-set of visible data from the front card fields listed in Annex II of Directive (EU) 2024/2841 (expiry date, card serial number), together with the revocation identifier, electronic signature, and schema information.

Electronic signature shall contain:

(i) issuerAuth – A COSE_Sign1 object signed with the issuing authority's **QSealC private key**.

(ii) Protected header that includes alg = ES256 (signature algorithm) and x5t (the COSE X.509 certificate hash header parameter).

5. **Optional Data**

No optional data shall be included in the QR code.

6. **Revocation Identifier (RID)**

The Revocation Identifier of the EPC shall comply with point 6 of Annex I.

Revocation lists for revoked EPCs shall reference only the RID. Card serial numbers shall not be published in revocation lists.

7. **CBOR payload (inside the QR) of EPC**

Only the following data shall be included inside the QR payload, which is consistent with the visible EPC card fields set out in Annex II to Directive (EU) 2024/2841:

Field	mDOC path	Type/Format
Data schema version	issuerSigned.nameSpaces."eu.epc".ver	String (e.g., "1.0")
Card type: EPC	docType	Enum ("eu.epc")
Card Serial Number	issuerSigned.nameSpaces."eu.epc".sub	String
Revocation Identifier	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 bytes)
Expiry date of card	issuerSigned.nameSpaces."eu.epc".exp	CBOR tag 1004, as defined in RFC 8943 (section 2.1), containing a UTF-8 text string representing an RFC 3339 full-date in YYYY-MM-DD format.

The electronic signature shall be carried in issuerAuth (a COSE_Sign1 object). The certificate chain shall not be embedded in the QR code payload; instead, the protected COSE header shall include x5t, a certificate thumbprint used to locate the corresponding QSealC in the verifier's cached trust store.

8. **EPC QR code payload example: commented JavaScript Object Notation-style logical representation**

The following example is a human readable JavaScript Object Notation (JSON) representation of the EPC logical view. In practice, this structure shall not be human readable as it shall be:

(a) Encoded in CBOR (RFC 8949, section 3);

(b) Signed using untagged COSE_Sign1 structure , with a detached payload (RFC 9052, section 4);

(c) include the expiry date as a CBOR tag 1004 full-date value in accordance with RFC 8943 (section 2.1);

(d) include the x5t protected-header parameter in accordance with RFC 9360, using SHA-256 over the DER-encoded end-entity QSealC; and

(e) compressed and prefixed with the string EP1:MDOC: before being encoded in the QR code.

```
{
  // JSON-style, human-readable EPC logical view only.
  // Actual QR payload is deterministic CBOR, not JSON.
  "docType": "eu.epc", // EPC credential. The docType value is included, together with
    //issuerSigned, in the COSE_Sign1 external payload.

  "issuerSigned": {
    // Data protected by issuerAuth; used as detached payload.
    // For signature generation and verification, the detached external payload covers both
```

```
  // docType and issuerSigned.
  "nameSpaces": {
    "eu.epc": {
      "ver": "1.0", // QR profile/schema version

      // Card serial number; issuer-defined, max. 24 characters.
      "sub": "EF12345678901234567890GH",

      // Revocation identifier: actual CBOR bstr, 16 bytes/128 bits.
      // Shown here as 32 hex characters for readability.
      "rid": "4a8d9c11223344556677889 9aabbccdd",

      // Actual CBOR encoding uses tag 1004 for RFC 3339 full-date.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Actual form: untagged COSE_Sign1, not a JSON object.
  "type": "COSE_Sign1",
  "tagged": false, // encoded without COSE_Sign1 CBOR tag
  "payload": "detached", // COSE payload field is CBOR null

  "protectedHeader": {
    // alg: ES256; equivalent COSE header parameter 1 = -7.
    "alg": "ES256",

    // x5t: certificate thumbprint; COSE header parameter 34.
    "x5t": {
      "hashAlg": "SHA-256", // equivalent COSE hash value -16

      // SHA-256 hash of DER-encoded end-entity QSealC.
      // 32 bytes represented as 64 hex characters.
      "hashValue":
      "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // empty in this example

  // ES256 COSE signature: 64 bytes = 128 hex characters.
  "signature":
  "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde-
  f0123456789abcdef0123456789abcdef0123456789abcdef"
}
}
```

9. **Use of cryptographic mechanisms**

The use of cryptographic mechanisms in the context of this Annex shall be in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA).

ANNEX III

NOTIFICATION OF INFORMATION REFERRED TO IN ARTICLE 6(2)

1. Member States shall provide the following information to the Commission on each competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities:

   (a) the name of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (b) a registration number of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (c) the contact email and contact phone number of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities;

   (d) one or more certificates that can be used to verify the electronic seal created by the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities it issues, and for which the certified identity data include the name, and the registration number of the issuer, as specified in points (a) and (b), respectively;

   (e) the URL of the location where the issuer publishes the validity status of the physical versions of the European Disability Card or the European Parking Card for persons with disabilities.

2. Member States may provide the following information to the Commission on each competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities:

   (a) the URL of the webpage that contains the policies, terms and conditions of the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities that apply to the provision and use of the physical versions of the European Disability Card and the European Parking Card for persons with disabilities it provides;

   (b) where applicable, the URL of the webpage that contains additional information about the competent authority or body responsible for issuing the physical versions of the European Disability Card or the European Parking Card for persons with disabilities.

ANNEX IV

TECHNICAL SPECIFICATIONS FOR A REVOCATION LIST FOR THE PHYSICAL VERSIONS OF THE EUROPEAN DISABILITY CARD OR THE EUROPEAN PARKING CARD FOR PERSONS WITH DISABILITIES

1. For the purposes of this Annex, the identifier shall correspond to the revocation identifier (RID) defined in point 6 of Annex I and point 6 of Annex II.

2. A revocation list shall be implemented as an identifier list token in CWT (RFC 8392, section 7) format in accordance with Clause 5.2 of the token status list specification (draft-ietf-oauth-status-list-14) with the following amendments:

   (a) the value of the type claim shall be 'application/identifierlist+cwt';

   (b) the expiration time claim shall be present;

   (c) The StatusList claim shall not be present in the CWT claims set;

   (d) the IdentifierList structure defined in point 3 shall be present as a claim in the CWT claims set using the key 65530;

   (e) the CWT shall be a COSE_Sign1 object using, for calculating the signature, a signature algorithm in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by the European Union Agency for Cybersecurity (ENISA);

   (f) the CWT shall contain the x5chain parameter as defined in RFC 9360 (section 2) in the protected header that contains the certificate or chain of certificates to verify the signature of the revocation list;

   (g) the extended key usage OID specified in the token status list specification (draft-ietf-oauth-status-list-14) may be used for the identifier list signing certificate and it is recommended that verifiers support the extended key usage OID specified in the token status list specification and that issuer authority infrastructures do not make the extended key usage field critical when using the extended key usage OID specified in the token status list specification.

3. The IdentifierList structure shall be a CBOR structure with the following Concise Data Definition Language (CDDL):

```
IdentifierList = {

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

  ? "aggregation_uri" : Aggregation_uri,

  * tstr => RFU

}

IdentifierInfo = {

  (tstr / int) => RFU

}

Identifier = bstr

Aggregation_uri = tstr
```