Съвет на
Европейския съюз

Брюксел, 10 юли 2026 г.
(OR. en)

11772/26
ADD 1

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

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	1 юли 2026 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	C(2026) 4534 annex
Относно:	ПРИЛОЖЕНИЯ към ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА за допълнение на Директива (ЕС) 2024/2841 по отношение на задаването на QR кода върху физическата версия на европейската карта за хора с увреждания и задаването на QR кода и установяването на общи технически спецификации, с които се гарантира сигурността на физическата версия на европейската карта за паркиране за хора с увреждания, както и на въпроси, свързани с оперативната съвместимост

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 1.7.2026 г.
C(2026) 4534 final

ANNEXES 1 to 4

ПРИЛОЖЕНИЯ

към

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА

за допълнение на Директива (ЕС) 2024/2841 по отношение на задаването на QR кода върху физическата версия на европейската карта за хора с увреждания и задаването на QR кода и установяването на общи технически спецификации, с които се гарантира сигурността на физическата версия на европейската карта за паркиране за хора с увреждания, както и на въпроси, свързани с оперативната съвместимост

ПРИЛОЖЕНИЕ I

СПЕЦИФИКАЦИИ НА QR КОДА ЗА ФИЗИЧЕСКАТА ВЕРСИЯ НА ЕВРОПЕЙСКАТА КАРТА ЗА ХОРА С УВРЕЖДАНИЯ

1. **Формат на QR кода за физическата версия на европейската карта за хора с увреждания (EDC)**

а) **Формат на QR кода „Модел 2“** в съответствие с международните спецификации за QR кодове ISO/IEC 18004:2024 или еквивалентни.

б) **Ниво на корекция на грешки M** (15 % дублиране), осигуряващо издръжливост при надраскване или при частично повреждане на отпечатан QR код.

в) **Режим на кодиране:** полезният товар на QR кода се състои от комбинирана структура issuerSigned Concise Binary Object Representation (CBOR) и съответния обект за подпис issuerAuth COSE_Sign1, както е определено в CBOR Object Signing and Encryption (COSE, RFC 9052, раздели 3.1, 4.2 и 4.4), като се следва моделът на данните mDOC за елементи issuerSigned, но адаптиран за използване със статична физическа карта. Елементът issuerAuth е обект COSE_Sign1 с алгоритъм alg = ES256 и защитен заглавен блок, съдържащ x5t (параметърът за хеш на заглавния блок на сертификата COSE X.509, определен в RFC 9360 (раздел 2); за целите на оперативната съвместимост хеширащият алгоритъм, използван в x5t, е SHA-256).

г) Преди кодирането на QR кода комбинираният обект CBOR/COSE се **компресира във формат zlib** (RFC 1950, раздел 2.2) **с алгоритъма deflate** (RFC 1951, раздели 3.2 и 4). Полученият компресиран масив от байтове се кодира в **QR код с байтов режим**, като се гарантира пълна поддръжка на двоични полезни товари CBOR/COSE и оперативна съвместимост със сканиращите устройства.

За всички текстови полета, включени в полезния товар на QR кода, издателите кодират символите като Unicode UTF-8 в текстови низове CBOR. Не се прилага транслитерация за подписания полезен товар от данни. С цел осигуряване на оперативна съвместимост издателите прилагат форма C за нормализация на Unicode (NFC) към всички текстови полета преди подписването.

д) **Префикс:** низът на QR кода на EDC започва с „ED1:MDOC:“. Това определя типа на картата и профила на кодиране. Префиксите са задължителни и в тях е от значение дали се използват малки или големи букви. Неизвестните или неподдържаните префикси водят до отхвърляне. Префиксът и компресираният полезен товар се кодират в QR кода като един сегмент от данни с байтов режим.

е) **Минимален размер на модула ≥ 0,25 mm**, за да се гарантира четливостта върху отпечатаните карти.

ж) **Максимална версия 20;** с до 97 × 97 модула от всяка страна.

2. **Спецификации за генерирането на подпис на EDC**

Квалифицираният електронен печат (QSeal), използван за подпечатване на QR кодовете на EDC, гарантира, че кодираните данни произхождат от издаващия орган и не са били променяни.

а) **Алгоритъм за електронни подписи**: алгоритъмът за електронни подписи е ES256 (алгоритъм за електронни подписи по елиптична крива (ECDSA) с SHA-256, използващ кривата P-256), както е определено в RFC 9053 (раздел 2.1); в COSE алгоритъмът се идентифицира чрез параметъра alg header в RFC 9052 (раздел 3.1).

б) **Ключ за подписване**: полезният товар на QR кода се подписва с частния ключ, съответстващ на квалифицирано удостоверение за електронен печат (QSealC).

в) **Структура на COSE:** контейнерът за подпис е обект COSE_Sign1. Защитеният заглавен блок включва alg (ES256) и x5t (параметъра за хеширане на заглавния блок на сертификата COSE X.509, определен в RFC 9360 (раздел 2); за целите на оперативната съвместимост хеширащият алгоритъм, използван в x5t, е SHA-256). Проверката се основава на използването на стойността x5t за локализиране на съответния сертификат в локално кешираното доверително хранилище на проверяващия орган, създадено въз основа на информацията от доверителния списък, след което веригата на сертифициране и статусът на сертификата се валидират в съответствие с рамката за доверие на eIDAS.

г) **Стандарт на подписа**: полезният товар на QR кода се подписва като обект COSE_Sign1 в съответствие с RFC 9052 (раздел 4), CBOR Object Signing and Encryption. Обектът COSE_Sign1 се съдържа в issuerAuth и се кодира без тага за CBOR за COSE_Sign1. Полето за полезния товар в обекта COSE_Sign1 е отделено и кодирано като CBOR null. За генерирането и проверката на подписи външният полезен товар е детерминистичната CBOR кодирана структура, съдържаща стойността docType и стойността issuerSigned от картата на CBOR от първо ниво.

д) **Хеширащ алгоритъм**: SHA-256 се използва като част от ES256 за генериране на подписи и проверка на целостността.

е) **Кодиране**: полезният товар се кодира чрез CBOR (RFC 8949, раздел 4.2), както се изисква от спецификациите COSE и mDOC, като се гарантират кодирането и възпроизводимостта на подписаните данни.

3. **Спецификации за отпечатването**

а) **Тиха зона**: от всички страни на QR кода се оставя свободно пространство от **4 модула**, без никакви печатни елементи, шарки или фон.

б) **Контраст**: QR кодът се отпечатва върху бял фон, с минимално съотношение на контраста **4:1**, за да се гарантира висока степен на четливост при различни условия на светлина.

в) QR кодът се отпечатва, като се използва цветът, определен в приложение I към Директива (ЕС) 2024/2841, който гарантира максимален контраст.

г) **Разположение и размери**: QR кодът, включително тихата зона, е с размери 26,25 mm × 26,25 mm и се намира на гърба на картата, в долния десен ъгъл. QR кодът е най-много версия 20 (97 × 97 модула), като размерът на модулите е 0,25 mm или по-голям.

QR кодът, включително тихата му зона, се разполага най-малко на 5 mm от десния край и най-малко на 5 mm от долния край на картата.

4. Данните в QR кода на EDC

QR кодът съдържа минимален набор от данни, който може да бъде проверен офлайн, в съответствие с принципа за свеждане на данните до минимум, установен в член 5, параграф 1, буква в) от Регламент (ЕС) 2016/679. Структурата на полезния товар от данни е, както следва:

а) атрибутите на картата се кодират в CBOR в рамките на обект от типа issuerSigned;

б) структурата е обгърната и подписана с QSeal на издаващия орган като issuerAuth (COSE_Sign1, ES256, включително x5t — параметърът за хеширане на заглавния блок на сертификата COSE X.509);

в) Полученият обект CBOR/COSE се компресира в съответствие с точка 1, буква г) от настоящото приложение. Полезният товар на QR кода се състои от префикса „ED1:MDOC:“, последван от получения компресиран масив от байтове, като целият полезен товар се кодира с използване на байтов режим като един сегмент от данни в QR кода.

Съдържанието на данните се състои от подмножество на видимите данни от полетата на лицевата страна на картата, изброени в приложение I към Директива (ЕС) 2024/2841 (собствено и фамилно име, сериен номер на картата, срок на валидност), заедно с идентификатора за отмяна, електронния подпис и информацията за схемата.

Електронният подпис съдържа:

i) issuerAuth — обект COSE_Sign1, подписан с **частния ключ QSealC** на издаващия орган;

ii) защитен заглавен блок, който включва alg = ES256 (алгоритъм за електронни подписи) и x5t (параметърът за хеширане на заглавния блок на сертификата COSE X.509).

5. Незадължителни данни

В QR кода не се включват никакви допълнителни данни.

6. Идентификатор за отмяна (RID)

Освен видимия сериен номер на картата, QR кодът съдържа специален идентификатор за отмяна (RID).

RID се използва за определяне на статуса на отмяната и за управление на списъка с отменени карти. RID не се отпечатва върху картата и не се показва на проверяващите картата органи.

6.1. *Изисквания по отношение на RID*

Идентификаторът за отмяна (RID)

а) се включва в полезния товар на подписания QR код;

б) е уникален поне в рамките на домейна на издаващия орган;

в) не е отпечатан върху картата и не е предназначен за четене от човек;

г) не разкрива лични данни и няма непосредствено значение;

д) не може да бъде изведен пряко от серийния номер, който се вижда на картата; и

е) е криптографски свързан с полезния товар на QR кода чрез квалифициран електронен печат.

6.2. *Формат и размер на RID*

RID се кодира като байтов низ (bstr) CBOR. Дължината на RID е 16 байта (128 бита).

RID се генерира от издаващия орган чрез контролиран от него метод, с който се гарантират достатъчна информационна ентропия и устойчивост на отгатване или изброяване.

6.3. *Списъци с отменени карти*

Списъците с отменени карти, публикувани за целите на проверката, съдържат само RID кода на отменените карти. Серийните номера на картите не се публикуват в списъците с отменени карти.

7. Полезен товар CBOR (вътре в QR кода) на EDC

В полезния товар на QR кода се включват само следните данни, в съответствие с видимите полета с данни на EDC, определени в приложение I към Директива (ЕС) 2024/2841.

Съдържание на най-високо ниво:

а) docType = "eu.edc"

б) issuerSigned.nameSpaces."eu.edc" с атрибутите, показани в таблицата по-долу;

в) issuerAuth = COSE_Sign1 (QSeal).

Поле	**Път към mDOC**	**Тип/Формат**
Версия на схемата на данните	issuerSigned.nameSpaces."eu.edc".ver	Низ (например "1.0")
Тип карта: EDC	docType	Enum („eu.edc“)
Сериен номер на картата	issuerSigned.nameSpaces."eu.edc".sub	Низ
Идентификатор за отмяна	issuerSigned.nameSpaces."eu.edc".rid	CBOR bstr (16 байта)
Собствено име на титуляра на	issuerSigned.nameSpaces."eu.edc".givenName	Текстов низ в Unicode (UTF-

картата		8)
Фамилно име на титуляра на картата	issuerSigned.nameSpaces."eu.edc".familyName	Текстов низ в Unicode (UTF-8)
Срок на валидност на картата	issuerSigned.nameSpaces."eu.edc".exp	Таг CBOR 1004, както е определен в RFC 8943 (раздел 2.1), съдържащ текстови низ UTF-8, представляваща RFC 3339 full-date (пълна дата) във формат ГГГГ-ММ-ДД.

Електронният подпис се съдържа в issuerAuth (обект COSE_Sign1). Веригата на сертифициране не се вграждда в полезния товар на QR кода; вместо това защитеният заглавен блок COSE съдържа x5t — отпечатък на сертификата, използван за локализиране на съответстващия QSealC в кешираното доверително хранилище на проверяващия орган.

8. **Пример за полезен товар на QR код на EDC: коментирано JavaScript Object Notation-style логическо представяне**

Следният пример е човекочетимо представяне с JavaScript Object Notation (JSON) на логическия изглед на EDC. На практика тази структура няма да бъде човекочетима, тъй като е:

а) кодирана в CBOR (RFC 8949, раздел 3);

б) подписана, като се използва структура COSE_Sign1 без тагове с отделен полезен товар (RFC 9052, раздел 4);

в) включва срока на валидност като таг за пълна дата CBOR tag 1004 full-date в съответствие с RFC 8943 (раздел 2.1);

г) включва параметъра защитена заглавна част x5t в съответствие с RFC 9360, като използва SHA-256 върху DER-encoded end-entity QSealC; и

д) е компресиран и префиксирана с низ ED1: MDOC: преди да бъде въведена в QR кода.

```
{
 //JSON-style, само човекочетим логически изглед на EDC.
 //Действителният полезен товар на QR кода е детерминистичен CBOR, а не JSON.
 "docType": "eu.edc", // акредитив на EDC. Стойността docTyp е включена заедно с
  //issuerSigned във външния полезен товар COSE_Sign1.

 "issuerSigned": {
  //Данни, защитени с issuerAuth; използва се като отделен полезен товар.
  //За генерирането и проверката на подписи отделеният външен полезен товар обхваща и двете
  // docType и issuerSigned.
  "nameSpaces": {
   "eu.edc": {
    "ver": "1.0", // версия на QR профила/схемата

    // Сериен номер на картата; определен от издателя, максимум 24 символа.
    "sub": "AB12345678901234567890CD",
```

```
      // Идентификатор за отмяна: действителен CBOR bstr, 16 байта /128 бита.
      // Показан тук като 32 hex символа за четливост.
      "rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

      "givenName": "Ана",    // собствено име, отпечатано на EDC
      "familyName": "Друго",// фамилно име, отпечатано на EDC

      // Действителното кодиране CBOR използва таг 1004 за пълна дата RFC 3339 full-date.
      "exp": "2030-12-31"
    }
  }
},

"issuerAuth": {
  // Действителна форма: COSE_Sign1 без тагове, не е JSON обект.
  "type": "COSE_Sign1",
  "tagged": false,       // кодирано без таг COSE_Sign1 CBOR
  "payload": "detached", // полето за полезен товар COSE е CBOR null

  "protectedHeader": {
    // alg: ES256; еквивалентен параметър на заглавната част COSE 1 = -7.
    "alg": "ES256",

    // x5t: отпечатък на сертификата; параметър на заглавната част COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // еквивалентна COSE хеш стойност -16
```

```
        // SHA-256 хеш на DER-encoded end-entity QSealC.
        // 32 байта, представени като 64 hex символа.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // празен в този пример

    // ES256 COSE signature: 64 байта = 128 hex символа.
    "signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"
  }
}
```

9. Използване на криптографски механизми

Използването на криптографски механизми в контекста на настоящото приложение е в съответствие с договорените криптографски механизми, утвърдени от Европейската група за сертифициране на киберсигурността и публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA).

ПРИЛОЖЕНИЕ II

СПЕЦИФИКАЦИИ НА QR КОДА ЗА ФИЗИЧЕСКАТА ВЕРСИЯ НА ЕВРОПЕЙСКАТА КАРТА ЗА ПАРКИРАНЕ ЗА ХОРА С УВРЕЖДАНИЯ

1. **Формат на QR кода върху физическата версия на европейската карта за паркиране за хора с увреждания (EPC)**

а) **Формат на QR кода „Модел 2“** в съответствие с международните спецификации за QR кодове ISO/IEC 18004:2024 или еквивалентни.

б) **Ниво на корекция на грешки M** (15 % дублиране), осигуряващо издръжливост при надраскване или частично повреждане на отпечатан QR код.

в) **Режим на кодиране:** полезният товар на QR кода се състои от комбинирана структура issuerSigned Concise Binary Object Representation (CBOR) и съответния обект за подпис issuerAuth COSE_Sign1, както е определено в CBOR Object Signing and Encryption (COSE, RFC 9052, раздели 3.1, 4.2 и 4.4), като се следва моделът на данните mDOC за елементи issuerSigned, но адаптиран за използване със статична физическа карта. Елементът issuerAuth е обект COSE_Sign1 с алгоритъм alg = ES256 и защитен заглавен блок, съдържащ x5t (параметърът за хеш на заглавния блок на сертификата COSE X.509, определен в RFC 9360 (раздел 2); за целите на оперативната съвместимост хеширащият алгоритъм, използван в x5t, е SHA-256).

г) Преди кодирането на QR кода комбинираният обект CBOR/COSE се **компресиран във формат zlib (RFC 1950, раздел 2.2) с алгоритъма deflate** (RFC 1951, раздели 3.2 и 4). Полученият компресиран масив от байтове се кодира в **QR код с байтов режим**, като се гарантира пълна поддръжка на двоични полезни товари CBOR/COSE и оперативна съвместимост със сканиращите устройства.

За всички текстови полета, включени в полезния товар на QR кода, издателите кодират символите като Unicode UTF-8 в текстови низове CBOR. Не се прилага транслитерация за подписания полезен товар от данни. С цел осигуряване на оперативна съвместимост издателите прилагат форма C за нормализация на Unicode (NFC) към всички текстови полета преди подписването.

д) **Префикс**: низът на QR кода на EPC започва с „EP1:MDOC:“. Това определя типа на картата и профила на кодиране. Префиксите са задължителни и в тях е от значение дали се използват малки или големи букви. Неизвестните или неподдържаните префикси водят до отхвърляне. Префиксът и компресираният полезен товар се кодират в QR кода като един сегмент от данни с байтов режим.

е) **Минимален размер на модула ≥ 0,35 mm**, за да се гарантира четливостта върху отпечатаните карти.

ж) **Максимална версия 20**; с до 97 × 97 модула от всяка страна.

2. **Спецификации за генерирането на подпис на EPC**

Квалифицираният електронен печат (QSeal), използван за подпечатване на QR кодовете на EPC, гарантира, че кодираните данни произхождат от издаващия орган и не са били променяни.

а) **Алгоритъм за електронни подписи**: алгоритъмът за електронни подписи е ES256 (ECDSA с SHA-256, използващ кривата P-256), както е определено в RFC 9053 (раздел 2.1); в COSE алгоритъмът се идентифицира чрез параметъра alg header в RFC 9052 (раздел 3.1).

б) **Ключ за подписване**: полезният товар на QR кода се подписва с частния ключ, съответстващ на квалифицирано удостоверение за електронен печат (QSealC).

в) **Структура на COSE**: контейнерът за подпис е обект COSE_Sign1. Защитеният заглавен блок включва alg (ES256) и x5t (параметърът за хеширане на заглавния блок на сертификата COSE X.509, определен в RFC 9360 (раздел 2); за целите на оперативната съвместимост хеширащият алгоритъм, използван в x5t, е SHA-256). Проверката се основава на използването на стойността x5t за локализиране на съответния сертификат в локално кешираното доверително хранилище на проверяващия орган, създадено въз основа на информацията от доверителния списък, след което веригата на сертифициране и статусът на сертификата се валидират в съответствие с рамката за доверие на eIDAS.

г) **Стандарт на подписа**: полезният товар на QR кода се подписва като обект COSE_Sign1 в съответствие с RFC 9052 (раздел 4), CBOR Object Signing and Encryption. Обектът COSE_Sign1 се съдържа в issuerAuth и се кодира без тага за CBOR за COSE_Sign1. Полето за полезния товар в обекта COSE_Sign1 е отделено и кодирано като CBOR null. За генерирането и проверката на подписи външният полезен товар е детерминистичната CBOR кодирана структура, съдържаща стойността docType и стойността issuerSigned от картата на CBOR от първо ниво.

д) **Хеширащ алгоритъм**: SHA-256 се използва като част от ES256 за генериране на подписи и проверка на целостността.

е) **Кодиране**: полезният товар се кодира чрез CBOR (RFC 8949, раздел 4.2), както се изисква от спецификациите COSE и mDOC, като се гарантират кодирането и възпроизводимостта на подписаните данни.

3. **Спецификации за отпечатването**

а) **Тиха зона**: от всички страни на QR кода се оставя свободно пространство от **4 модула**, без никакви печатни елементи, шарки или фон.

б) **Контраст**: QR кодът се отпечатва върху бял фон, с минимално съотношение на контраста **4:1**, за да се гарантира висока степен на четливост при различни условия на светлина.

в) QR кодът се отпечатва, като се използва цветът, определен в приложение I към Директива (ЕС) 2024/2841, който гарантира максимален контраст.

г) **Разположение и размери:** QR кодът, включително тихата зона, е с размери **37 mm × 37 mm** и да разположен на лицевата страна на картата, леко изместен надясно от центъра, към долния край. QR кодът е най-много версия 20 (97 × 97 модула), като размерът на модулите е 0,35 mm или повече.

QR кодът, включително тихата му зона, се разполага най-малко на 5 mm от долния край на картата.

4. **Данните в QR кода на EPC**

QR кодът съдържа минимален набор от данни, който може да бъде проверен офлайн, в съответствие с принципа за свеждане на данните до минимум, посочен в член 5, параграф 1, буква в) от Регламент (ЕС) 2016/679. Структурата на полезния товар е както следва:

а) атрибутите на картата се кодират в CBOR в рамките на обект issuerSigned;

б) тази структура е обгърната и подписана с QSeal на издаващия орган като issuerAuth (COSE_Sign1, ES256, включително x5t — параметърът за хеширане на заглавния блок на сертификата COSE X.509);

в) Полученият обект CBOR/COSE се компресира в съответствие с точка 1, буква г) от настоящото приложение. Полезният товар на QR кода се състои от префикса „EP1:MDOC:“, последван от получения компресиран масив от байтове, като целият полезен товар се кодира с използване на байтов режим като един сегмент от данни в QR кода.

Съдържанието на данните се състои от подмножество на видимите данни от полетата на лицевата страна на картата, изброени в приложение II към Директива (ЕС) 2024/2841 (срок на валидност, сериен номер на картата), заедно с идентификатора за отмяна, електронния подпис и информацията за схемата.

Електронният подпис съдържа:

i) issuerAuth — обект COSE_Sign1, подписан с **частния ключ QSealC** на издаващия орган;

ii) защитен заглавен блок, който включва alg = ES256 (алгоритъм за електронни подписи) и x5t (параметърът за хеширане на заглавния блок на сертификата COSE X.509).

5. **Незадължителни данни**

В QR кода не се включват никакви допълнителни данни.

6. **Идентификатор за отмяна (RID)**

Идентификаторът за отмяна на EPC отговаря на точка 6 от приложение I.

Списъците с отменени карти съдържат само RID. Серийните номера на картите не се публикуват в списъците с отменени карти.

7. **Полезен товар CBOR (вътре в QR кода) на EPC**

В полезния товар на QR кода се включват само следните данни, които са в съответствие с видимите полета за данни на EPC, определени в приложение I към Директива (ЕС) 2024/2841:

Поле	**Път към mDOC**	**Тип/Формат**
Версия на схемата на	issuerSigned.nameSpaces."eu.epc".ver	Низ (например "1.0")

данните		
Тип карта: EPC	docType	Enum ("eu.epc")
Сериен номер на картата	issuerSigned.nameSpaces."eu.epc".sub	Низ
Идентификатор за отмяна	issuerSigned.nameSpaces."eu.epc".rid	CBOR bstr (16 байта)
Срок на валидност на картата	issuerSigned.nameSpaces."eu.epc".exp	Таг CBOR 1004, както е определен в RFC 8943 (раздел 2.1), съдържащ текстови низ UTF-8, представляваща RFC 3339 full-date (пълна дата) във формат ГГГГ-ММ-ДД.

Електронният подпис се съдържа в issuerAuth (обект COSE_Sign1). Веригата на сертифициране не се вграждда в полезния товар на QR кода; вместо това защитеният заглавен блок COSE съдържа x5t — отпечатък на сертификата, използван за локализиране на съответстващия QSealC в кешираното доверително хранилище на проверяващия орган.

8. Пример за полезен товар на QR код на EPC: коментирано JavaScript Object Notation-style логическо представяне

Следният пример е човекочетимо представяне с JavaScript Object Notation (JSON) на логическия изглед на EPC. На практика тази структура няма да бъде човекочетима, тъй като е:

а) кодирана в CBOR (RFC 8949, раздел 3),

б) подписана, като се използва структура COSE_Sign1 без тагове с отделен полезен товар (RFC 9052, раздел 4);

в) включва срока на валидност като таг за пълна дата CBOR tag 1004 full-date в съответствие с RFC 8943 (раздел 2.1);

г) включва параметъра защитена заглавна част x5t в съответствие с RFC 9360, като използва SHA-256 върху DER-encoded end-entity QSealC; и

д) е компресиран и префиксирана с низ EP1: MDOC: преди да бъде въведена в QR кода.

```
{
 //JSON-style, само човекочетим логически изглед на EPC.
 //Действителният полезен товар на QR кода е детерминистичен CBOR, а не JSON.
 "docType": "eu.epc", // акредитив на EPC. Стойността docTyp е включена заедно с
  //issuerSigned във външния полезен товар COSE_Sign1.

 "issuerSigned": {
  //Данни, защитени с issuerAuth; използва се като отделен полезен товар.
 //За генерирането и проверката на подписи отделеният външен полезен товар обхваща и двете
  // docType и issuerSigned.
  "nameSpaces": {
   "eu.epc": {
    "ver": "1.0", // версия на QR профила/схемата

    // Сериен номер на картата; определен от издателя, максимум 24 символа.
    "sub": "EF123456789012345678 90GH",

    // Идентификатор за отмяна: действителен CBOR bstr, 16 байта /128 бита.
    // Показан тук като 32 hex символа за четливост.
    "rid": "4a8d9c11223344556677 8899aabbccdd",

    // Действителното кодиране CBOR използва таг 1004 за пълна дата RFC 3339 full-date.
    "exp": "2030-12-31"
   }
  }
```

```
  },

  "issuerAuth": {
    // Действителна форма: COSE_Sign1 без тагове, не е JSON обект.
    "type": "COSE_Sign1",
    "tagged": false,       // кодирано без таг COSE_Sign1 CBOR
    "payload": "detached", // полето за полезен товар COSE е CBOR null

    "protectedHeader": {
      // alg: ES256; еквивалентен параметър на заглавната част COSE 1 = -7.
      "alg": "ES256",

      // x5t: отпечатък на сертификата; параметър на заглавната част COSE 34.
      "x5t": {
        "hashAlg": "SHA-256", // еквивалентна COSE хеш стойност -16

        // SHA-256 хеш на DER-encoded end-entity QSealC.
        // 32 байта, представени като 64 hex символа.
        "hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
      }
    },

    "unprotectedHeader": {}, // празен в този пример

    // ES256 COSE signature: 64 байта = 128 hex символа.
```

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Използване на криптографски механизми

Използването на криптографски механизми в контекста на настоящото приложение е в съответствие с договорените криптографски механизми, утвърдени от Европейската група за сертифициране на киберсигурността и публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA).

ПРИЛОЖЕНИЕ III

НОТИФИЦИРАНЕ НА ИНФОРМАЦИЯТА, ПОСОЧЕНА В ЧЛЕН 6, ПАРАГРАФ 2

1. Държавите членки предоставят на Комисията следната информация за всеки компетентен орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания:

   а) наименованието на компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания;

   б) регистрационен номер на компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания;

   в) електронния адрес и телефонния номер за връзка на компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания;

   г) един или няколко сертификата, които могат да се използват за удостоверяване на електронния печат, създаден от компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания, които те издават, и за които сертифицираните данни за самоличността включват наименованието и регистрационния номер на издателя, както е посочено съответно в букви а) и б);

   д) URL адреса на мястото, където издателят публикува статуса на валидност на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания.

2. Държавите членки могат да предоставят на Комисията следната информация за всеки компетентен орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания:

   а) URL адреса на уебстраницата, съдържаща политиките, правилата и условията на компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания, които се прилагат за предоставянето и използването на физическите версии на европейската карта за хора с увреждания и на европейската карта за паркиране за хора с увреждания, които те издават;

   б) когато е приложимо, URL адреса на уебстраницата, съдържаща допълнителна информация за компетентния орган или служба, отговарящи за издаването на физическите версии на европейската карта за хора с увреждания или на европейската карта за паркиране за хора с увреждания.

ПРИЛОЖЕНИЕ IV

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ ЗА СПИСЪК С ОТМЕНЕНИ ФИЗИЧЕСКИ ВЕРСИИ НА ЕВРОПЕЙСКАТА КАРТА ЗА ХОРА С УВРЕЖДАНИЯ ИЛИ НА ЕВРОПЕЙСКАТА КАРТА ЗА ПАРКИРАНЕ ЗА ХОРА С УВРЕЖДАНИЯ

1. За целите на настоящото приложение идентификаторът съответства на идентификатора за отмяна (RID), определен в точка 6 от приложение I и точка 6 от приложение II.

2. Списък с отменени карти се въвежда като identifier list token във формат CWT (RFC 8392, раздел 7) в съответствие с точка 5.2 от спецификацията за token status list (draft-ietf-oauth-status-list-14), като се прилагат следните изменения:

   а) типът на заявката е „application/identifierlist+cwt“;

   б) посочва се срокът на валидност;

   в) заявката StatusList не присъства в набора от заявки за CWT;

   г) структурата IdentifierList, определена в точка 3, присъства като заявка в набора от заявки за CWT, като се използва ключ 65530;

   д) CWT е обект COSE_Sign1, който използва за изчисляване на подписа алгоритъм за подписване, съответстващ на договорените криптографски механизми, одобрени от Европейската група за сертифициране на киберсигурността и публикувани от Агенцията на Европейския съюз за киберсигурност (ENISA);

   е) CWT съдържа параметъра x5chain, както е определен в RFC 9360 (раздел 2), в защитения заглавен блок, който съдържа сертификата или веригата на сертифициране за проверка на подписа на списъка с отменени карти;

   ж) OID за разширено използване на ключа, посочен в спецификацията за token status list (draft-ietf-oauth-status-list-14), може да се използва за сертификата за подписване на списъка с идентификатори; препоръчва се проверяващите органи да поддържат OID за разширено използване на ключа, посочен в спецификацията за token status list, а инфраструктурите на издаващите органи да не определят полето за разширено използване на ключа като задължително при използване на OID за разширено използване на ключа, посочен в спецификацията за token status list.

3. Структурата IdentifierList е структура CBOR със следния Concise Data Definition Language (CDDL):

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

IdentifierInfo = {
```

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

Identifier = bstr

Aggregation_uri = tstr
```