Συμβούλιο της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 10 Ιουλίου 2026
(OR. en)

11772/26
ADD 1

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

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	1 Ιουλίου 2026
Αποδέκτης:	κα Thérèse BLANCHET, Γενική Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	C(2026) 4534 annex
Θέμα:	ΠΑΡΑΡΤΗΜΑΤΑ του ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) .../... ΤΗΣ ΕΠΙΤΡΟΠΗΣ για τη συμπλήρωση της οδηγίας (ΕΕ) 2024/2841 όσον αφορά τον καθορισμό του κωδικού QR στη φυσική έκδοση της ευρωπαϊκής κάρτας αναπηρίας και τον καθορισμό του κωδικού QR και τη θέσπιση κοινών τεχνικών προδιαγραφών που διασφαλίζουν την ασφάλεια της φυσικής έκδοσης της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία, καθώς και ζητήματα διαλειτουργικότητας

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 1.7.2026
C(2026) 4534 final

ANNEXES 1 to 4

ΠΑΡΑΡΤΗΜΑΤΑ

του

ΚΑΤ' ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) .../... ΤΗΣ ΕΠΙΤΡΟΠΗΣ

για τη συμπλήρωση της οδηγίας (ΕΕ) 2024/2841 όσον αφορά τον καθορισμό του κωδικού QR στη φυσική έκδοση της ευρωπαϊκής κάρτας αναπηρίας και τον καθορισμό του κωδικού QR και τη θέσπιση κοινών τεχνικών προδιαγραφών που διασφαλίζουν την ασφάλεια της φυσικής έκδοσης της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία, καθώς και ζητήματα διαλειτουργικότητας

ΠΑΡΑΡΤΗΜΑ Ι

ΠΡΟΔΙΑΓΡΑΦΕΣ ΚΩΔΙΚΟΥ QR ΓΙΑ ΤΗ ΦΥΣΙΚΗ ΕΚΔΟΣΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΑΡΤΑΣ ΑΝΑΠΗΡΙΑΣ

1. **Μορφότυπος του κωδικού QR για τη φυσική έκδοση της ευρωπαϊκής κάρτας αναπηρίας (ΕΚΑ)**

α) **Μορφότυπος κωδικού QR Model 2**, σύμφωνα με τις διεθνείς προδιαγραφές του κωδικού QR κατά ISO/IEC 18004:2024 ή ισοδύναμο πρότυπο.

β) **Επίπεδο διόρθωσης σφάλματος M** (πλεονασμός 15 %), ώστε να διασφαλίζεται η ανθεκτικότητα σε χαραγές ή μερική φθορά του εκτυπωμένου κωδικού QR.

γ) **Λειτουργία κωδικοποίησης:** Το ωφέλιμο φορτίο QR αποτελείται από τον συνδυασμό της δομής του μορφότυπου CBOR issuerSigned και του αντίστοιχου αντικειμένου υπογραφής issuerAuth COSE_Sign1, όπως ορίζεται στην υπογραφή και κρυπτογράφηση αντικειμένου με CBOR (COSE, RFC 9052 σημεία 3.1, 4.2 και 4.4), σύμφωνα με το σχήμα μοντέλου δεδομένων mDOC για τα στοιχεία issuerSigned, αλλά προσαρμοσμένα για τη χρήση στατικής φυσικής κάρτας. Το issuerAuth είναι αντικείμενο COSE_Sign1 με το στοιχείο alg = ES256 και προστατευόμενη κεφαλίδα που περιέχει την παράμετρο x5t [την παράμετρο κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509 που ορίζεται στο RFC 9360 (σημείο 2)· για τη διαλειτουργικότητα, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται στην παράμετρο x5t είναι ο SHA-256].

δ) Πριν από την κωδικοποίηση του κωδικού QR, ο συνδυασμός CBOR/αντικειμένου COSE **συμπιέζεται με τη χρήση του μορφότυπου zlib** (RFC 1950 σημείο 2.2) **με τον αλγόριθμο deflate** (RFC 1951 σημεία 3.2 και 4). Ο συμπιεσμένος πίνακας byte που προκύπτει κωδικοποιείται σε **λειτουργία Byte κωδικού QR**, ώστε να διασφαλίζεται πλήρης υποστήριξη για τα δυαδικά ωφέλιμα φορτία CBOR/COSE και τη διαλειτουργικότητα του σαρωτή.

Για όλα τα πεδία κειμένου που περιλαμβάνονται στο ωφέλιμο φορτίο QR, οι εκδότες κωδικοποιούν τους χαρακτήρες ως Unicode UTF-8 εντός των συμβολοσειρών κειμένου CBOR. Ο μεταγραμματισμός δεν εφαρμόζεται στα δεδομένα υπογεγραμμένου ωφέλιμου φορτίου. Για λόγους διαλειτουργικότητας, οι εκδότες εφαρμόζουν την κανονικοποιημένη μορφή «Unicode Normalisation Form C» (NFC) σε όλα τα πεδία κειμένου πριν από την υπογραφή.

ε) **Πρόθεμα:** Η συμβολοσειρά του QR της ΕΚΑ αρχίζει με την ένδειξη «ED1:MDOC:». Με αυτήν προσδιορίζονται ο τύπος της κάρτας και το προφίλ κωδικοποίησης. Τα προθέματα κάνουν τη διάκριση μεταξύ πεζών–κεφαλαίων και πρέπει να υπάρχουν. Άγνωστα ή μη υποστηριζόμενα προθέματα έχουν ως αποτέλεσμα την απόρριψη. Το πρόθεμα και το συμπιεσμένο ωφέλιμο φορτίο κωδικοποιούνται στον κωδικό QR ως ενιαίο τμήμα δεδομένων με λειτουργία Byte.

στ) **Ελάχιστο μέγεθος λειτουργικής μονάδας ≥ 0,25 mm**, ώστε να διασφαλίζεται η αναγνωσιμότητα στις εκτυπωμένες κάρτες.

ζ) **Μέγιστη έκδοση 20·** με έως και 97 × 97 λειτουργικές μονάδες σε κάθε όψη.

2. **Προδιαγραφές δημιουργίας υπογραφής της ΕΚΑ**

Με την εγκεκριμένη ηλεκτρονική σφραγίδα (QSeal) που χρησιμοποιείται για τη σφράγιση των κωδικών QR της ΕΚΑ διασφαλίζεται ότι τα κωδικοποιημένα δεδομένα προέρχονται από την εξουσιοδοτημένη αρχή έκδοσης και δεν έχουν αλλοιωθεί.

α) **Αλγόριθμος υπογραφής**: Ο αλγόριθμος υπογραφής είναι ο ES256 [αλγόριθμος ελλειπτικής καμπύλης ψηφιακής υπογραφής (ECDSA) με τον SHA-256 και τη χρήση της καμπύλης P-256], όπως ορίζεται στο RFC 9053 (σημείο 2.1)· στο COSE, ο αλγόριθμος προσδιορίζεται από τον αλγόριθμο της παραμέτρου κεφαλίδας στο RFC 9052 (σημείο 3.1).

β) **Κλειδί υπογραφής**: Το ωφέλιμο φορτίο QR υπογράφεται με τη χρήση του ιδιωτικού κλειδιού που αντιστοιχεί σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας (QSealC).

γ) **Δομή COSE:** Ο περιέκτης υπογραφής είναι αντικείμενο COSE_Sign1. Η προστατευόμενη κεφαλίδα περιλαμβάνει αλγόριθμο (ES256) και την παράμετρο x5t [την παράμετρο κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509 που ορίζεται στο RFC 9360 (σημείο 2)· για τη διαλειτουργικότητα, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται στην παράμετρο x5t είναι ο SHA-256]. Η επαλήθευση βασίζεται στη χρήση της τιμής x5t για τον εντοπισμό του αντίστοιχου πιστοποιητικού στον τοπικά αποθηκευμένο σε κρυφή μνήμη χώρο αποθήκευσης έμπιστων πιστοποιητικών του ελεγκτή, ο οποίος έχει δημιουργηθεί από πληροφορίες του καταλόγου εμπιστοσύνης, και στη συνέχεια για την επικύρωση της αλυσίδας πιστοποιητικών και της κατάστασης πιστοποιητικού σύμφωνα με το πλαίσιο εμπιστοσύνης eIDAS.

δ) **Πρότυπο υπογραφής**: Το ωφέλιμο φορτίο του κωδικού QR υπογράφεται ως αντικείμενο COSE_Sign1 σύμφωνα με το RFC 9052 (σημείο 4), υπογραφή και κρυπτογράφηση αντικειμένου με CBOR. Το αντικείμενο COSE_Sign1 περιέχεται στο issuerAuth και κωδικοποιείται χωρίς την ετικέτα CBOR για το COSE_Sign1. Το πεδίο ωφέλιμου φορτίου για το αντικείμενο COSE_Sign1 πρέπει να είναι αποσπασμένο και να κωδικοποιείται ως CBOR null. Για τη δημιουργία και την επαλήθευση της υπογραφής, το εξωτερικό ωφέλιμο φορτίο πρέπει να είναι μια δομή κωδικοποιημένη σε σταθερό CBOR, η οποία περιέχει την τιμή docType και την τιμή issuerSigned από το λεξικό CBOR ανώτατου επιπέδου.

ε) **Αλγόριθμος κατακερματισμού**: Ο SHA-256 χρησιμοποιείται ως μέρος του ES256 για τη δημιουργία υπογραφής και την επαλήθευση της ακεραιότητας.

στ) **Κωδικοποίηση**: Το ωφέλιμο φορτίο κωδικοποιείται με τη χρήση του μορφότυπου CBOR (RFC 8949 σημείο 4.2), όπως απαιτείται από τις προδιαγραφές COSE και mDOC, ώστε να διασφαλίζονται η κωδικοποίηση και η αναπαραγωγιμότητα των υπογεγραμμένων δεδομένων.

3. **Προδιαγραφές εκτύπωσης**

α) **Ήσυχη ζώνη**: Ο κωδικός QR περιβάλλεται, σε όλες τις πλευρές, από σαφές περιθώριο **4 λειτουργικών μονάδων**, χωρίς κανένα εκτύπωμα, σχέδιο ή φόντο.

β) **Αντίθεση**: Ο κωδικός QR εκτυπώνεται σε λευκό φόντο, με ελάχιστο λόγο αντίθεσης **4:1**, ώστε να διασφαλίζεται υψηλή αναγνωσιμότητα υπό μεταβαλλόμενες συνθήκες φωτισμού.

γ) Για την εκτύπωση του κωδικού QR χρησιμοποιείται το χρώμα που ορίζεται στο παράρτημα Ι της οδηγίας (ΕΕ) 2024/2841 ώστε να εξασφαλίζεται η μέγιστη αντίθεση.

δ) **Τοποθέτηση και διαστάσεις**: Ο κωδικός QR, συμπεριλαμβανομένης της ήσυχης ζώνης, έχει διαστάσεις 26,25 mm × 26,25 mm και βρίσκεται στην οπίσθια όψη της κάρτας, στην κάτω δεξιά γωνία. Η μέγιστη έκδοση του κωδικού QR είναι 20 (97 × 97 λειτουργικές μονάδες), με μέγεθος λειτουργικής μονάδας 0,25 mm ή μεγαλύτερο.

Ο κωδικός QR, καθώς και η ήσυχη ζώνη του, τοποθετούνται τουλάχιστον 5 mm από το άκρο στη δεξιά πλευρά και τουλάχιστον 5 mm από το κάτω άκρο της κάρτας.

4. **Δεδομένα στον κωδικό QR της ΕΚΑ**

Ο κωδικός QR περιέχει ένα ελάχιστο, επαληθεύσιμο εκτός διαδικτύου, σύνολο δεδομένων σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων που ορίζεται στο άρθρο 5 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679. Η δομή του ωφέλιμου φορτίου έχει ως εξής:

α) Τα χαρακτηριστικά της κάρτας κωδικοποιούνται σε μορφότυπο CBOR εντός αντικειμένου issuerSigned.

β) Η δομή περιτυλίγεται και υπογράφεται από την QSeal της αρχής έκδοσης ως issuerAuth (COSE_Sign1, ES256, συμπεριλαμβανομένης της παραμέτρου x5t, της παραμέτρου κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509).

γ) Το αντικείμενο CBOR/COSE που προκύπτει συμπιέζεται σύμφωνα με το σημείο 1 στοιχείο δ) του παρόντος παραρτήματος. Το ωφέλιμο φορτίο του κωδικού QR αποτελείται από το πρόθεμα «ED1:MDOC:», ακολουθούμενο από τον συμπιεσμένο πίνακα byte που προκύπτει, και το πλήρες ωφέλιμο φορτίο κωδικοποιείται με τη χρήση της λειτουργίας Byte ως ενιαίο τμήμα δεδομένων του κωδικού QR.

Το περιεχόμενο των δεδομένων αποτελείται από ένα υποσύνολο ορατών δεδομένων από τα πεδία της εμπρόσθιας όψης της κάρτας που παρατίθενται στο παράρτημα Ι της οδηγίας (ΕΕ) 2024/2841 (όνομα, επώνυμο, αριθμός σειράς κάρτας, ημερομηνία λήξης), μαζί με το αναγνωριστικό ανάκλησης, την ηλεκτρονική υπογραφή και τις πληροφορίες σχήματος.

Η **ηλεκτρονική υπογραφή** περιλαμβάνει τα εξής:

i) issuerAuth — αντικείμενο COSE_Sign1 που υπογράφεται με το **ιδιωτικό κλειδί QSealC** της αρχής έκδοσης·

ii) προστατευόμενη κεφαλίδα που περιλαμβάνει το στοιχείο alg = ES256 (αλγόριθμος υπογραφής) και την παράμετρο x5t (την παράμετρο κεφαλίδας κατακερματισμού του πιστοποιητικού COSE X.509).

5. **Προαιρετικά δεδομένα**

Στον κωδικό QR δεν περιλαμβάνονται προαιρετικά δεδομένα.

6. **Αναγνωριστικό ανάκλησης (RID)**

Επιπλέον του ορατού σειριακού αριθμού της κάρτας, ο κωδικός QR περιλαμβάνει ειδικό αναγνωριστικό ανάκλησης (στο εξής: RID).

Το RID χρησιμοποιείται για τον καθορισμό του καθεστώτος ανάκλησης και για τη διαχείριση του καταλόγου ανάκλησης. Το RID δεν εκτυπώνεται στην κάρτα και δεν εμφανίζεται στους ελεγκτές καρτών.

6.1. *Απαιτήσεις RID*

Το RID:

α) περιλαμβάνεται στο υπογεγραμμένο ωφέλιμο φορτίο QR·

β) είναι μοναδικό τουλάχιστον εντός του τομέα έκδοσης της αρχής έκδοσης·

γ) δεν εκτυπώνεται στην κάρτα και δεν προορίζεται να είναι αναγνώσιμο από άνθρωπο·

δ) δεν αποκαλύπτει δεδομένα προσωπικού χαρακτήρα και δεν έχει άμεσο νόημα·

ε) δεν μπορεί να συναχθεί απευθείας από τον ορατό σειριακό αριθμό της κάρτας· και

στ) συνδέεται κρυπτογραφικά με το ωφέλιμο φορτίο QR μέσω της εγκεκριμένης ηλεκτρονικής σφραγίδας.

6.2. *Μορφότυπος και μέγεθος RID*

Το RID κωδικοποιείται ως συμβολοσειρά byte CBOR (bstr). Το RID έχει μήκος 16 bytes (128 bits).

Το RID δημιουργείται από την αρχή έκδοσης με τη χρήση μεθόδου υπό τον έλεγχό της, η οποία εξασφαλίζει επαρκή εντροπία και αντοχή όσον αφορά απόπειρες πρόβλεψης συνθηματικών ή καταμέτρησης.

6.3. *Κατάλογοι ανάκλησης*

Στους καταλόγους ανάκλησης που δημοσιεύονται για σκοπούς επαλήθευσης αναφέρεται μόνο το RID των καρτών που έχουν ανακληθεί. Οι σειριακοί αριθμοί των καρτών δεν δημοσιεύονται στους καταλόγους ανάκλησης.

7. **Ωφέλιμο φορτίο CBOR (εντός του κωδικού QR) της ΕΚΑ**

Στο ωφέλιμο φορτίο QR περιλαμβάνονται μόνο τα δεδομένα που παρατίθενται κατωτέρω, τα οποία συνάδουν με τα ορατά πεδία δεδομένων της ΕΚΑ που καθορίζονται στο παράρτημα Ι της οδηγίας (ΕΕ) 2024/2841.

Περιεχόμενα ανώτατου επιπέδου:

α) docType = "eu.edc"

β) issuerSigned.nameSpaces."eu.edc" με τα χαρακτηριστικά που παρουσιάζονται στον πίνακα κατωτέρω

γ) issuerAuth = COSE_Sign1 (QSeal)

Πεδίο	**Διαδρομή mDOC**	**Τύπος/Μορφότυπος**
Έκδοση σχήματος δεδομένων	issuerSigned.nameSpaces."eu.edc".ver	Συμβολοσειρά (π.χ. «1.0»)
Τύπος κάρτας:	docType	Enum ("eu.edc")

ΕΚΑ		
Σειριακός αριθμός κάρτας	issuerSigned.nameSpaces."eu.edc".sub	Συμβολοσειρά
Αναγνωριστικό ανάκλησης	issuerSigned.nameSpaces."eu.edc".rid	bstr CBOR (16 bytes)
Όνομα κατόχου κάρτας	issuerSigned.nameSpaces."eu.edc".givenName	Συμβολοσειρά κειμένου Unicode (UTF-8)
Επώνυμο κατόχου κάρτας	issuerSigned.nameSpaces."eu.edc".familyName	Συμβολοσειρά κειμένου Unicode (UTF-8)
Ημερομηνία λήξης κάρτας	issuerSigned.nameSpaces."eu.edc".exp	Ετικέτα 1004 του CBOR, όπως ορίζεται στο RFC 8943 (σημείο 2.1), η οποία περιέχει συμβολοσειρά κειμένου UTF-8 η οποία αναπαριστά την πλήρη ημερομηνία σύμφωνα με το RFC 3339 στον μορφότυπο EEEE-MM-HH.

Η ηλεκτρονική υπογραφή περιέχεται στο issuerAuth (αντικείμενο COSE_Sign1). Η αλυσίδα πιστοποιητικών δεν είναι ενσωματωμένη·στο ωφέλιμο φορτίο κωδικού QR· αντ' αυτού, η προστατευόμενη κεφαλίδα COSE περιλαμβάνει αποτύπωμα πιστοποιητικού x5t που χρησιμοποιείται για τον εντοπισμό του αντίστοιχου QSealC στον αποθηκευμένο σε κρυφή μνήμη χώρο αποθήκευσης έμπιστων πιστοποιητικών του ελεγκτή.

8. **Παράδειγμα ωφέλιμου φορτίου κωδικού QR της ΕΚΑ: λογική αναπαράσταση τύπου σημειογραφίας αντικειμένων JavaScript με δυνατότητα σχολίων**

Το ακόλουθο παράδειγμα αποτελεί αναγνώσιμη από άνθρωπο αναπαράσταση σημειογραφίας αντικειμένων JavaScript (JSON) της λογικής όψης της ΕΚΑ. Στην πράξη, η δομή αυτή δεν είναι αναγνώσιμη από τον άνθρωπο διότι πρέπει:

α) να κωδικοποιείται σε CBOR (RFC 8949 σημείο 3)·

β) να υπογράφεται με τη χρήση της δομής COSE_Sign1 χωρίς ετικέτα με αποσπασμένο ωφέλιμο φορτίο (RFC 9052, σημείο 4.),

γ) να περιλαμβάνει την ημερομηνία λήξης ως ετικέτα CBOR 1004 σύμφωνα με το RFC 8943 (σημείο 2.1)·

δ) να περιλαμβάνει την παράμετρο προστατευόμενης κεφαλίδας x5t σύμφωνα με το RFC 9360, χρησιμοποιώντας τον SHA-256 στο QSealC της τελικής οντότητας, κωδικοποιημένο σε DER· και

ε) να συμπιέζεται και να περιέχει ως πρόθεμα τη συμβολοσειρά ED1:MDOC: πριν από την κωδικοποίησή της στον κωδικό QR.

```
{
 // Μόνο λογική όψη της ΕΚΑ, αναγνώσιμη από άνθρωπο, τύπου JSON.
 // Το πραγματικό ωφέλιμο φορτίο του κωδικού QR είναι σε σταθερό CBOR, όχι σε JSON.
 "docType": "eu.edc", // διαπιστευτήριο της ΕΚΑ. Η τιμή docType περιλαμβάνεται, σε συνδυασμό με το
  //issuerSigned, στο εξωτερικό ωφέλιμο φορτίο COSE_Sign1.

 "issuerSigned": {
  // Δεδομένα που προστατεύονται με issuerAuth· χρησιμοποιούνται ως αποσπασμένο ωφέλιμο φορτίο.
  // Για τη δημιουργία και την επαλήθευση της υπογραφής, το αποσπασμένο εξωτερικό ωφέλιμο φορτίο καλύπτει τόσο
  // το docType όσο και το issuerSigned.
  "nameSpaces": {
   "eu.edc": {
    "ver": "1.0", // έκδοση του προφίλ/σχήματος του κωδικού QR
```

// Σειριακός αριθμός κάρτας· αναγνωριστικό που ορίζεται από τον εκδότη, μέχρι 24 χαρακτήρες.

"sub": "AB1234567890123456789OCD",

// Αναγνωριστικό ανάκλησης: πραγματική συμβολοσειρά byte CBOR, 16 bytes/128 bits.

// Εμφανίζεται εδώ ως 32 δεξαεξαδικοί χαρακτήρες για ευκολία ανάγνωσης.

"rid": "9f8c4d3a7b1e2c0a55aa33ff8899ee11",

"givenName": "Ann", // όνομα που εκτυπώνεται στην ΕΚΑ

"familyName": "Other", // επώνυμο που εκτυπώνεται στην ΕΚΑ

// Η πραγματική κωδικοποίηση CBOR χρησιμοποιεί την ετικέτα 1004 για την πλήρη ημερομηνία σύμφωνα με το RFC 3339.

"exp": "2030-12-31"

}

}

},

"issuerAuth": {

// Πραγματική μορφή: COSE_Sign1 χωρίς ετικέτα, όχι αντικείμενο JSON.

"type": "COSE_Sign1",

"tagged": false, // κωδικοποιημένο χωρίς την ετικέτα COSE_Sign1 του CBOR

"payload": "detached", // το πεδίο ωφέλιμου φορτίου του COSE είναι CBOR null

"protectedHeader": {

// alg: ES256· αντίστοιχη παράμετρος κεφαλίδας COSE 1 = -7.

"alg": "ES256",

```
    // x5t: αποτύπωμα πιστοποιητικού· παράμετρος κεφαλίδας COSE 34.
    "x5t": {
      "hashAlg": "SHA-256", // αντίστοιχη τιμή κατακερματισμού COSE -16

      // κατακερματισμός SHA-256 του QSealC της τελικής οντότητας, κωδικοποιημένο σε DER.
      // 32 bytes που αναπαριστώνται ως 64 δεξαεξαδικοί χαρακτήρες.
      "hashValue": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
    }
  },

  "unprotectedHeader": {}, // κενό στο παρόν παράδειγμα

  // υπογραφή ES256 COSE: 64 bytes = 128 δεξαεξαδικοί χαρακτήρες.
  "signature": "0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"
 }
}
```

9. Χρήση κρυπτογραφικών μηχανισμών

Η χρήση κρυπτογραφικών μηχανισμών στο πλαίσιο του παρόντος παραρτήματος συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA).

ΠΑΡΑΡΤΗΜΑ ΙΙ

ΠΡΟΔΙΑΓΡΑΦΕΣ ΚΩΔΙΚΟΥ QR ΓΙΑ ΤΗ ΦΥΣΙΚΗ ΕΚΔΟΣΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΑΡΤΑΣ ΣΤΑΘΜΕΥΣΗΣ ΓΙΑ ΑΤΟΜΑ ΜΕ ΑΝΑΠΗΡΙΑ

1. **Μορφότυπος του κωδικού QR στη φυσική έκδοση της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία (ΕΚΣ)**

α) **Μορφότυπος κωδικού QR Model 2**, σύμφωνα με τις διεθνείς προδιαγραφές του κώδικα QR κατά ISO/IEC 18004:2024 ή ισοδύναμο πρότυπο.

β) **Επίπεδο διόρθωσης σφάλματος M** (πλεονασμός 15 %), ώστε να διασφαλίζεται η ανθεκτικότητα σε χαραγές ή μερική φθορά του εκτυπωμένου κωδικού QR.

γ) **Λειτουργία κωδικοποίησης:** Το ωφέλιμο φορτίο QR αποτελείται από τον συνδυασμό της δομής του μορφότυπου CBOR issuerSigned και του αντίστοιχου αντικειμένου υπογραφής issuerAuth COSE_Sign1, όπως ορίζεται στην υπογραφή και κρυπτογράφηση αντικειμένου με CBOR (COSE, RFC 9052 σημεία 3.1, 4.2 και 4.4), σύμφωνα με το σχήμα μοντέλου δεδομένων mDOC για τα στοιχεία issuerSigned, αλλά προσαρμοσμένα για τη χρήση στατικής φυσικής κάρτας. Το issuerAuth είναι αντικείμενο COSE_Sign1 με το στοιχείο alg = ES256 και προστατευόμενη κεφαλίδα που περιέχει την παράμετρο x5t [την παράμετρο κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509 που ορίζεται στο RFC 9360 (σημείο 2)· για τη διαλειτουργικότητα, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται στην παράμετρο x5t είναι ο SHA-256].

δ) Πριν από την κωδικοποίηση του κωδικού QR, ο συνδυασμός CBOR/αντικειμένου COSE **συμπιέζεται με τη χρήση του μορφότυπου zlib (RFC 1950 σημείο 2.2) με τον αλγόριθμο Deflate** (RFC 1951 σημεία 3.2 και 4). Ο συμπιεσμένος πίνακας byte που προκύπτει κωδικοποιείται σε **λειτουργία Byte κωδικού QR**, ώστε να διασφαλίζεται πλήρης υποστήριξη για τα δυαδικά ωφέλιμα φορτία CBOR/COSE και τη διαλειτουργικότητα του σαρωτή.

Για όλα τα πεδία κειμένου που περιλαμβάνονται στο ωφέλιμο φορτίο QR, οι εκδότες κωδικοποιούν τους χαρακτήρες ως Unicode UTF-8 εντός των συμβολοσειρών κειμένου CBOR. Ο μεταγραμματισμός δεν εφαρμόζεται στα δεδομένα υπογεγραμμένου ωφέλιμου φορτίου. Για λόγους διαλειτουργικότητας, οι εκδότες εφαρμόζουν την κανονικοποιημένη μορφή «Unicode Normalisation Form C» (NFC) σε όλα τα πεδία κειμένου πριν από την υπογραφή.

ε) **Πρόθεμα**: Η συμβολοσειρά του κωδικού QR της ΕΚΣ αρχίζει με το πρόθεμα «EP1:MDOC:». Με αυτό προσδιορίζονται ο τύπος της κάρτας και το προφίλ κωδικοποίησης. Τα προθέματα κάνουν τη διάκριση μεταξύ πεζών–κεφαλαίων και πρέπει να υπάρχουν. Άγνωστα ή μη υποστηριζόμενα προθέματα έχουν ως αποτέλεσμα την απόρριψη. Το πρόθεμα και το συμπιεσμένο ωφέλιμο φορτίο κωδικοποιούνται στον κωδικό QR ως ενιαίο τμήμα δεδομένων με λειτουργία Byte.

στ) **Ελάχιστο μέγεθος λειτουργικής μονάδας ≥ 0,35 mm**, ώστε να διασφαλίζεται η αναγνωσιμότητα στις εκτυπωμένες κάρτες.

ζ) **Μέγιστη έκδοση 20**· με έως και 97 × 97 λειτουργικές μονάδες σε κάθε όψη.

2. **Προδιαγραφές δημιουργίας υπογραφής της ΕΚΣ**

Με την εγκεκριμένη ηλεκτρονική σφραγίδα (QSeal) που χρησιμοποιείται για τη σφράγιση των κωδικών QR της ΕΚΣ διασφαλίζεται ότι τα κωδικοποιημένα δεδομένα προέρχονται από την εξουσιοδοτημένη αρχή έκδοσης και δεν έχουν αλλοιωθεί.

α) **Αλγόριθμος υπογραφής**: Ο αλγόριθμος υπογραφής είναι ο ES256 (ECDSA με τον SHA-256 και τη χρήση της καμπύλης P-256), όπως ορίζεται στο RFC 9053 (σημείο 2.1)· στο COSE, ο αλγόριθμος προσδιορίζεται από τον αλγόριθμο της παραμέτρου κεφαλίδας στο RFC 9052 (σημείο 3.1).

β) **Κλειδί υπογραφής**: Το ωφέλιμο φορτίο QR υπογράφεται με τη χρήση του ιδιωτικού κλειδιού που αντιστοιχεί σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας (QSealC).

γ) **Δομή COSE**: Ο περιέκτης υπογραφής είναι αντικείμενο COSE_Sign1. Η προστατευόμενη κεφαλίδα περιλαμβάνει αλγόριθμο (ES256) και την παράμετρο x5t [την παράμετρο κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509 που ορίζεται στο RFC 9360 (σημείο 2)· για τη διαλειτουργικότητα, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται στην παράμετρο x5t είναι ο SHA-256]. Η επαλήθευση βασίζεται στη χρήση της τιμής x5t για τον εντοπισμό του αντίστοιχου πιστοποιητικού στον τοπικά αποθηκευμένο σε κρυφή μνήμη χώρο αποθήκευσης έμπιστων πιστοποιητικών του ελεγκτή, ο οποίος έχει δημιουργηθεί από πληροφορίες του καταλόγου εμπιστοσύνης, και στη συνέχεια για την επικύρωση της αλυσίδας πιστοποιητικών και της κατάστασης πιστοποιητικού σύμφωνα με το πλαίσιο εμπιστοσύνης eIDAS.

δ) **Πρότυπο υπογραφής**: Το ωφέλιμο φορτίο του κωδικού QR υπογράφεται ως αντικείμενο COSE_Sign1 σύμφωνα με το RFC 9052 (σημείο 4), υπογραφή και κρυπτογράφηση αντικειμένου με CBOR. Το αντικείμενο COSE_Sign1 περιέχεται στο issuerAuth και κωδικοποιείται χωρίς την ετικέτα CBOR για το COSE_Sign1. Το πεδίο ωφέλιμου φορτίου για το αντικείμενο COSE_Sign1 πρέπει να είναι αποσπασμένο και να κωδικοποιείται ως CBOR null. Για τη δημιουργία και την επαλήθευση της υπογραφής, το εξωτερικό ωφέλιμο φορτίο πρέπει να είναι μια δομή CBOR κωδικοποιημένη σε σταθερό CBOR, η οποία περιέχει την τιμή docType και την τιμή issuerSigned από το λεξικό CBOR ανώτατου επιπέδου.

ε) **Αλγόριθμος κατακερματισμού**: Ο SHA-256 χρησιμοποιείται ως μέρος του ES256 για τη δημιουργία υπογραφής και την επαλήθευση της ακεραιότητας.

στ) **Κωδικοποίηση**: Το ωφέλιμο φορτίο κωδικοποιείται με τη χρήση του μορφότυπου CBOR (RFC 8949 σημείο 4.2), όπως απαιτείται από τις προδιαγραφές COSE και mDOC, ώστε να διασφαλίζονται η κωδικοποίηση και η αναπαραγωγιμότητα των υπογεγραμμένων δεδομένων.

3. **Προδιαγραφές εκτύπωσης**

α) **Ήσυχη ζώνη**: Ο κωδικός QR περιβάλλεται, σε όλες τις πλευρές, από σαφές περιθώριο **4 λειτουργικών μονάδων**, χωρίς κανένα εκτύπωμα, σχέδιο ή φόντο.

β) **Αντίθεση**: Ο κωδικός QR εκτυπώνεται σε λευκό φόντο, με ελάχιστο λόγο αντίθεσης **4:1**, ώστε να διασφαλίζεται υψηλή αναγνωσιμότητα υπό μεταβαλλόμενες συνθήκες φωτισμού.

γ) Για την εκτύπωση του κωδικού QR χρησιμοποιείται το χρώμα που ορίζεται στο παράρτημα II της οδηγίας (ΕΕ) 2024/2841 ώστε να εξασφαλίζεται η μέγιστη αντίθεση.

δ) **Τοποθέτηση και διαστάσεις:** Ο κωδικός QR, συμπεριλαμβανομένης της ήσυχης ζώνης, έχει διαστάσεις **37 mm × 37 mm** και βρίσκεται στην εμπρόσθια όψη της κάρτας, σε ελαφρώς έκκεντρη θέση προς τα δεξιά και προς το κάτω άκρο. Η μέγιστη έκδοση του κωδικού QR είναι 20 (97 × 97 λειτουργικές μονάδες), με μέγεθος λειτουργικής μονάδας 0,35 mm ή μεγαλύτερο.

Ο κωδικός QR, καθώς και η ήσυχη ζώνη του, τοποθετούνται τουλάχιστον 5 mm από το κάτω άκρο της κάρτας.

4. Δεδομένα στον κωδικό QR της ΕΚΣ

Ο κωδικός QR περιέχει ένα ελάχιστο, επαληθεύσιμο εκτός διαδικτύου, σύνολο δεδομένων σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων που περιλαμβάνεται στο άρθρο 5 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2016/679. Η δομή του ωφέλιμου φορτίου έχει ως εξής:

α) Τα χαρακτηριστικά της κάρτας κωδικοποιούνται σε μορφότυπο CBOR εντός αντικειμένου issuerSigned.

β) Η δομή αυτή περιτυλίγεται και υπογράφεται από την QSeal της αρχής έκδοσης ως issuerAuth (COSE_Sign1, ES256, συμπεριλαμβανομένης της παραμέτρου x5t, της παραμέτρου κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509).

γ) Το αντικείμενο CBOR/COSE που προκύπτει συμπιέζεται σύμφωνα με το σημείο 1 στοιχείο δ) του παρόντος παραρτήματος. Το ωφέλιμο φορτίο του κωδικού QR αποτελείται από το πρόθεμα «EP1:MDOC:», ακολουθούμενο από τον συμπιεσμένο πίνακα byte που προκύπτει, και το πλήρες ωφέλιμο φορτίο κωδικοποιείται με τη χρήση της λειτουργίας Byte ως ενιαίο τμήμα δεδομένων του κωδικού QR.

Το περιεχόμενο των δεδομένων αποτελείται από ένα υποσύνολο ορατών δεδομένων από τα πεδία της εμπρόσθιας όψης της κάρτας που παρατίθενται στο παράρτημα ΙΙ της οδηγίας (ΕΕ) 2024/2841 (ημερομηνία λήξης, σειριακός αριθμός κάρτας), μαζί με το αναγνωριστικό ανάκλησης, την ηλεκτρονική υπογραφή και τις πληροφορίες σχήματος.

Η **ηλεκτρονική υπογραφή** περιλαμβάνει τα εξής:

i) issuerAuth — αντικείμενο COSE_Sign1 που υπογράφεται με το **ιδιωτικό κλειδί QSealC** της αρχής έκδοσης·

ii) προστατευόμενη κεφαλίδα που περιλαμβάνει το στοιχείο alg = ES256 (αλγόριθμος υπογραφής) και την παράμετρο x5t (την παράμετρο κεφαλίδας κατακερματισμού πιστοποιητικού COSE X.509).

5. Προαιρετικά δεδομένα

Στον κωδικό QR δεν περιλαμβάνονται προαιρετικά δεδομένα.

6. Αναγνωριστικό ανάκλησης (RID)

Το αναγνωριστικό ανάκλησης της ΕΚΣ συμμορφώνεται με το σημείο 6 του παραρτήματος Ι.

Στους καταλόγους ανάκλησης για τις ΕΚΣ που έχουν ανακληθεί αναφέρεται μόνο το RID. Οι σειριακοί αριθμοί των καρτών δεν δημοσιεύονται στους καταλόγους ανάκλησης.

7. **Ωφέλιμο φορτίο CBOR (εντός του κωδικού QR) της ΕΚΣ**

Στο ωφέλιμο φορτίο QR περιλαμβάνονται μόνο τα ακόλουθα δεδομένα, τα οποία συνάδουν με τα ορατά πεδία δεδομένων της ΕΚΣ που καθορίζονται στο παράρτημα II της οδηγίας (ΕΕ) 2024/2841:

Πεδίο	**Διαδρομή mDOC**	**Τύπος/Μορφότυπος**
Έκδοση σχήματος δεδομένων	issuerSigned.nameSpaces."eu.epc".ver	Συμβολοσειρά (π.χ. «1.0»)
Τύπος κάρτας: ΕΚΣ	docType	Enum ("eu.epc")
Σειριακός αριθμός κάρτας	issuerSigned.nameSpaces."eu.epc".sub	Συμβολοσειρά
Αναγνωριστικό ανάκλησης	issuerSigned.nameSpaces."eu.epc".rid	bstr CBOR (16 bytes)
Ημερομηνία λήξης κάρτας	issuerSigned.nameSpaces."eu.epc".exp	Ετικέτα 1004 του CBOR, όπως ορίζεται στο RFC 8943 (σημείο 2.1), η οποία περιέχει συμβολοσειρά κειμένου UTF-8 η οποία αναπαριστά την πλήρη ημερομηνία σύμφωνα με το RFC 3339 στον μορφότυπο EEEE-MM-HH.

Η ηλεκτρονική υπογραφή περιέχεται στο issuerAuth (αντικείμενο COSE_Sign1). Η αλυσίδα πιστοποιητικών δεν είναι ενσωματωμένη·στο ωφέλιμο φορτίο κωδικού QR· αντ' αυτού, η προστατευόμενη κεφαλίδα COSE περιλαμβάνει αποτύπωμα πιστοποιητικού x5t που χρησιμοποιείται για τον εντοπισμό του αντίστοιχου QSealC στον αποθηκευμένο σε κρυφή μνήμη χώρο αποθήκευσης έμπιστων πιστοποιητικών του ελεγκτή.

8. **Παράδειγμα ωφέλιμου φορτίου κωδικού QR της ΕΚΣ: λογική αναπαράσταση τύπου σημειογραφίας αντικειμένων JavaScript με δυνατότητα σχολίων**

Το ακόλουθο παράδειγμα αποτελεί αναγνώσιμη από άνθρωπο αναπαράσταση σημειογραφίας αντικειμένων JavaScript (JSON) της λογικής όψης της ΕΚΣ. Στην πράξη, η δομή αυτή δεν είναι αναγνώσιμη από τον άνθρωπο διότι πρέπει:

α) να κωδικοποιείται σε CBOR (RFC 8949 σημείο 3)·

β) να υπογράφεται με τη χρήση της δομής COSE_Sign1 χωρίς ετικέτα με αποσπασμένο ωφέλιμο φορτίο (RFC 9052, σημείο 4.),

γ) να περιλαμβάνει την ημερομηνία λήξης ως ετικέτα CBOR 1004 σύμφωνα με το RFC 8943 (σημείο 2.1)·

δ) να περιλαμβάνει την παράμετρο προστατευόμενης κεφαλίδας x5t σύμφωνα με το RFC 9360, χρησιμοποιώντας τον SHA-256 στο QSealC της τελικής οντότητας, κωδικοποιημένο σε DER· και

ε) να συμπιέζεται και να περιέχει ως πρόθεμα τη συμβολοσειρά EP1:MDOC: πριν από την κωδικοποίησή της στον κωδικό QR.

```
{
  // Μόνο λογική όψη της ΕΚΣ, αναγνώσιμη από άνθρωπο, τύπου JSON.
  // Το πραγματικό ωφέλιμο φορτίο του κωδικού QR είναι σε σταθερό CBOR, όχι σε JSON.
  "docType": "eu.epc", // διαπιστευτήριο της ΕΚΣ. Η τιμή docType περιλαμβάνεται, σε συνδυασμό με το
    //issuerSigned, στο εξωτερικό ωφέλιμο φορτίο COSE_Sign1.

  "issuerSigned": {
    // Δεδομένα που προστατεύονται με issuerAuth· χρησιμοποιούνται ως αποσπασμένο ωφέλιμο φορτίο.
  // Για τη δημιουργία και την επαλήθευση της υπογραφής, το αποσπασμένο εξωτερικό ωφέλιμο φορτίο καλύπτει τόσο
    // το docType όσο και το issuerSigned.
    "nameSpaces": {
      "eu.epc": {
        "ver": "1.0", // έκδοση του προφίλ/σχήματος του κωδικού QR

        // Σειριακός αριθμός κάρτας· αναγνωριστικό που ορίζεται από τον εκδότη, μέχρι 24 χαρακτήρες.
        "sub": "EF123456789012345678 90GH",

        // Αναγνωριστικό ανάκλησης: πραγματική συμβολοσειρά byte CBOR, 16 bytes/128 bits.
```

```
      // Εμφανίζεται εδώ ως 32 δεξαεξαδικοί χαρακτήρες για ευκολία ανάγνωσης.
      "rid": "4a8d9c112233445566778899aabbccdd",

      // Η πραγματική κωδικοποίηση CBOR χρησιμοποιεί την ετικέτα 1004 για την πλήρη ημερομηνία σύμφωνα με το RFC 3339.
      "exp": "2030-12-31"
    }
  }
 },

 "issuerAuth": {
  // Πραγματική μορφή: COSE_Sign1 χωρίς ετικέτα, όχι αντικείμενο JSON.
  "type": "COSE_Sign1",
  "tagged": false,       // κωδικοποιημένο χωρίς την ετικέτα COSE_Sign1 του CBOR
  "payload": "detached", // το πεδίο ωφέλιμου φορτίου του COSE είναι CBOR null

  "protectedHeader": {
   // alg: ES256· αντίστοιχη παράμετρος κεφαλίδας COSE 1 = -7.
   "alg": "ES256",

   // x5t: αποτύπωμα πιστοποιητικού· παράμετρος κεφαλίδας COSE 34.
   "x5t": {
    "hashAlg": "SHA-256", // αντίστοιχη τιμή κατακερματισμού COSE -16

    // κατακερματισμός SHA-256 του QSealC της τελικής οντότητας, κωδικοποιημένο σε DER.
    // 32 bytes που αναπαριστώνται ως 64 δεξαεξαδικοί χαρακτήρες.
```

"hashValue":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef"

}

},

"unprotectedHeader": {}, // κενό στο παρόν παράδειγμα

// υπογραφή ES256 COSE: 64 bytes = 128 δεξαεξαδικοί χαρακτήρες.

"signature":
"0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789abc
def0123456789abcdef0123456789abcdef0123456789abcdef"

}

}

9. Χρήση κρυπτογραφικών μηχανισμών

Η χρήση κρυπτογραφικών μηχανισμών στο πλαίσιο του παρόντος παραρτήματος συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA).

ΠΑΡΑΡΤΗΜΑ ΙΙΙ

ΚΟΙΝΟΠΟΙΗΣΗ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΠΟΥ ΑΝΑΦΕΡΟΝΤΑΙ ΣΤΟ ΑΡΘΡΟ 6 ΠΑΡΑΓΡΑΦΟΣ 2

1. Τα κράτη μέλη παρέχουν στην Επιτροπή τις ακόλουθες πληροφορίες για κάθε αρμόδια αρχή ή αρμόδιο φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία:

   α) το όνομα της αρμόδιας αρχής ή του αρμόδιου φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία·

   β) αριθμό καταχώρισης της αρμόδιας αρχής ή του αρμόδιου φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία·

   γ) τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον αριθμό τηλεφώνου επικοινωνίας της αρμόδιας αρχής ή του αρμόδιου φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία·

   δ) ένα ή περισσότερα πιστοποιητικά τα οποία μπορούν να χρησιμοποιηθούν για την επαλήθευση της ηλεκτρονικής σφραγίδας που δημιουργεί η αρμόδια αρχή ή ο αρμόδιος φορέας που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία που εκδίδει, και για τα οποία τα πιστοποιημένα δεδομένα ταυτότητας περιλαμβάνουν το όνομα και τον αριθμό καταχώρισης του εκδότη, όπως ορίζεται στα στοιχεία α) και β), αντίστοιχα·

   ε) τη διεύθυνση URL της τοποθεσίας στην οποία ο εκδότης δημοσιεύει το καθεστώς ισχύος των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία.

2. Τα κράτη μέλη μπορούν να παρέχουν στην Επιτροπή τις ακόλουθες πληροφορίες για κάθε αρμόδια αρχή ή αρμόδιο φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία:

   α) τη διεύθυνση URL της ιστοσελίδας που περιέχει τις πολιτικές, τους όρους και τις προϋποθέσεις της αρμόδιας αρχής ή του αρμόδιου φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία και που ισχύουν για την παροχή και τη χρήση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας και της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία που παρέχουν η αρμόδια αρχή ή ο αρμόδιος φορέας·

   β) κατά περίπτωση, τη διεύθυνση URL της ιστοσελίδας που περιέχει πρόσθετες πληροφορίες σχετικά με την αρμόδια αρχή ή τον αρμόδιο φορέα που έχει την ευθύνη για την έκδοση των φυσικών εκδόσεων της ευρωπαϊκής κάρτας αναπηρίας ή της ευρωπαϊκής κάρτας στάθμευσης για άτομα με αναπηρία.

ΠΑΡΑΡΤΗΜΑ IV

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΑΝΑΚΛΗΣΗΣ ΓΙΑ ΤΙΣ ΦΥΣΙΚΕΣ ΕΚΔΟΣΕΙΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΑΡΤΑΣ ΑΝΑΠΗΡΙΑΣ Ή ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΑΡΤΑΣ ΣΤΑΘΜΕΥΣΗΣ ΓΙΑ ΑΤΟΜΑ ΜΕ ΑΝΑΠΗΡΙΑ

1. Για τους σκοπούς του παρόντος παραρτήματος, το αναγνωριστικό αντιστοιχεί στο αναγνωριστικό ανάκλησης (RID) που ορίζεται στο σημείο 6 του παραρτήματος I και στο σημείο 6 του παραρτήματος II.

2. Εφαρμόζεται κατάλογος ανάκλησης ως διακριτικό καταλόγου αναγνωριστικών σε μορφότυπο CWT (RFC 8392 σημείο 7), σύμφωνα με το σημείο 5.2 της προδιαγραφής καταλόγου κατάστασης διακριτικού (draft-ietf-oauth-status-list-14), με τις ακόλουθες τροποποιήσεις:

   α) η τιμή της δήλωσης τύπου είναι «application/identifierlist+cwt»·

   β) περιλαμβάνεται η δήλωση του χρόνου λήξης·

   γ) η δήλωση StatusList δεν περιλαμβάνεται στο σύνολο δηλώσεων CWT·

   δ) η δομή IdentifierList που ορίζεται στο σημείο 3 περιλαμβάνεται ως δήλωση στο σύνολο δηλώσεων CWT που χρησιμοποιούν το κλειδί 65530·

   ε) το CWT είναι αντικείμενο COSE_Sign1 το οποίο χρησιμοποιεί, για τον υπολογισμό της υπογραφής, αλγόριθμο υπογραφής που συμμορφώνεται με τους συμφωνημένους κρυπτογραφικούς μηχανισμούς που εγκρίνει η ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας και δημοσιεύει ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)·

   στ) το CWT περιέχει την παράμετρο x5chain, όπως ορίζεται στο RFC 9360 (σημείο 2), στην προστατευόμενη κεφαλίδα που περιέχει το πιστοποιητικό ή την αλυσίδα πιστοποιητικών για την επαλήθευση της υπογραφής του καταλόγου ανάκλησης·

   ζ) το αναγνωριστικό αντικειμένου εκτεταμένης χρήσης κλειδιού που ορίζεται στην προδιαγραφή καταλόγου κατάστασης διακριτικού (draft-ietf-oauth-status-list-14) μπορεί να χρησιμοποιηθεί για το πιστοποιητικό υπογραφής του καταλόγου αναγνωριστικών, και συνιστάται, αφενός, στους ελεγκτές να υποστηρίζουν το αναγνωριστικό αντικειμένου εκτεταμένης χρήσης κλειδιού που ορίζεται στην προδιαγραφή καταλόγου κατάστασης διακριτικού και, αφετέρου, στις υποδομές της αρχής έκδοσης να μην καθιστούν κρίσιμης σημασίας το πεδίο δεδομένων εκτεταμένης χρήσης κλειδιού κατά τη χρήση του αναγνωριστικού αντικειμένου εκτεταμένης χρήσης κλειδιού που ορίζεται στην προδιαγραφή καταλόγου κατάστασης διακριτικού.

3. Η δομή IdentifierList είναι δομή του μορφότυπου CBOR με την ακόλουθη συνοπτική γλώσσα ορισμού δεδομένων (CDDL):

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

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

Identifier = bstr

Aggregation_uri = tstr
```