Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά L

2026/1731

22.7.2026

ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2026/1731 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 15ης Ιουλίου 2026

για την τροποποίηση των εκτελεστικών κανονισμών (ΕΕ) 2024/2977, (ΕΕ) 2024/2979, (ΕΕ) 2024/2980 και (ΕΕ) 2024/2982 όσον αφορά τα εφαρμοστέα πρότυπα και τις εφαρμοστέες προδιαγραφές

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ ([1]), και ιδίως το άρθρο 5α παράγραφος 23,

Εκτιμώντας τα ακόλουθα:

(1) Προκειμένου να διασφαλιστεί το υψηλότερο δυνατό επίπεδο εναρμόνισης μεταξύ των κρατών μελών για την ανάπτυξη των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, οι τεχνικές προδιαγραφές για τα πορτοφόλια βασίζονται στις εργασίες που πραγματοποιήθηκαν με βάση τη σύσταση (ΕΕ) 2021/946 της Επιτροπής ([2]), και ιδίως την αρχιτεκτονική και το πλαίσιο αναφοράς. Δεδομένου ότι η αρχιτεκτονική και το πλαίσιο αναφοράς έχουν εξελιχθεί σημαντικά μετά την έκδοση των εκτελεστικών κανονισμών (ΕΕ) 2024/2977 ([3]), (ΕΕ) 2024/2979 ([4]), (ΕΕ) 2024/2980 ([5]) και (ΕΕ) 2024/2982 της Επιτροπής ([6]), οι εν λόγω εκτελεστικοί κανονισμοί θα πρέπει να τροποποιηθούν ώστε να ευθυγραμμιστούν με τα νέα πρότυπα και τις νέες προδιαγραφές και διαδικασίες.

Σύμφωνα με τους στόχους του κανονισμού (ΕΕ) αριθ. 910/2014, επιλέχθηκαν ορισμένα πρότυπα για την εκπλήρωση των εν λόγω ειδικών απαιτήσεων. Τα πρότυπα αυτά θα πρέπει να αποτυπώνουν καθιερωμένες πρακτικές και να χαίρουν ευρείας αναγνώρισης στους σχετικούς τομείς. Για παράδειγμα, δεδομένου ότι ο μορφότυπος VCDM της W3C χρησιμοποιείται ως μορφότυπος αναφοράς για τις βεβαιώσεις, ιδίως στον εκπαιδευτικό τομέα, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει επίσης να υποστηρίζουν τον εν λόγω μορφότυπο μόλις τα νέα προφίλ καταστούν διαθέσιμα στον μορφότυπο VCDM της W3C. Εφόσον κρίνεται απαραίτητο, τα πρότυπα θα πρέπει να προσαρμόζονται ή να συμπληρώνονται προκειμένου να εξασφαλίζεται η ασφάλεια και η αξιοπιστία των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, ενώ παράλληλα θα πρέπει να διευκολύνεται η διασυνοριακή διαλειτουργικότητα και η αποτελεσματική λειτουργία της εσωτερικής αγοράς.

(2) Για κάθε χρήση του πορτοφολιού που απαιτεί παρουσίαση του πορτρέτου του χρήστη πορτοφολιού, οι υλοποιήσεις πορτοφολιού πρέπει να υποστηρίζουν τη λειτουργία της επιλεκτικής γνωστοποίησης και η γνωστοποίηση πρέπει να υπόκειται στον πλήρη έλεγχο του χρήστη. Για την προστασία της ικανότητας λήψης απόφασης σχετικά με τη γνωστοποίηση και για την προστασία του πορτρέτου από ακούσιο ή μη εγκεκριμένο αίτημα γνωστοποίησης, ο αρχιτεκτονικός σχεδιασμός των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας θα πρέπει να προβλέπει μηχανισμούς προειδοποίησης και καταγραφής όλων των συναλλαγών που σχετίζονται με τη χρήση του πορτρέτου. Προκειμένου να διασφαλιστεί ότι ο χρήστης πορτοφολιού έχει ενημερωθεί για την κοινοχρησία βιομετρικών δεδομένων, στις προειδοποιήσεις θα πρέπει να αναφέρεται

([1]) ΕΕ L 257 της 28.8.2014, σ. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Σύσταση (ΕΕ) 2021/946 της Επιτροπής, της 3ης Ιουνίου 2021, σχετικά με κοινή εργαλειοθήκη της Ένωσης για μια συντονισμένη προσέγγιση όσον αφορά το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα (ΕΕ L 210 της 14.6.2021, σ. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2977 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα δεδομένα ταυτοποίησης προσώπου και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται για τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας (ΕΕ L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2979 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την ακεραιότητα και τις βασικές λειτουργίες των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας (ΕΕ L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2980 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις κοινοποιήσεις προς την Επιτροπή σχετικά με το οικοσύστημα των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας (ΕΕ L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Εκτελεστικός κανονισμός (ΕΕ) 2024/2982 της Επιτροπής, της 28ης Νοεμβρίου 2024, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα πρωτόκολλα και τις διεπαφές που πρέπει να υποστηρίζονται από το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα (ΕΕ L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

ότι το αίτημα περιλαμβάνει κοινοχρησία βιομετρικών δεδομένων και ότι απαιτείται συγκεκριμένα από τον χρήστη να επιβεβαιώσει τη γνωστοποίηση. Όταν ένα βασιζόμενο μέρος επεξεργάζεται το πορτρέτο για τον σκοπό της αποκλειστικής ταυτοποίησης φυσικού προσώπου ή για την επιβεβαίωση της δηλωθείσας ταυτότητας του εν λόγω προσώπου, εφαρμόζονται τα άρθρα 6 και 9 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), καθώς και όλες οι άλλες απαιτήσεις του εν λόγω κανονισμού, συμπεριλαμβανομένης της απαίτησης ότι η επεξεργασία του πορτρέτου από τα βασιζόμενα μέρη θα πρέπει να περιορίζεται σε ό,τι είναι αναγκαίο για την προβλεπόμενη χρήση. Η προβλεπόμενη χρήση θα πρέπει να κοινοποιείται στον χρήστη πορτοφολιού, μαζί με το αίτημα γνωστοποίησης, με σαφή και κατανοητή διατύπωση. Για να ληφθεί δεόντως υπόψη η ευαισθησία των βιομετρικών δεδομένων, ο χρήστης πορτοφολιού θα πρέπει να επιβεβαιώνει ρητά και συγκεκριμένα τη γνωστοποίηση του πορτρέτου. Η σιωπή ή τα προσυμπληρωμένα τετραγωνίδια δεν θα πρέπει να θεωρούνται επιβεβαίωση από τον χρήστη πορτοφολιού. Η ρητή επιβεβαίωση του χρήστη πορτοφολιού θα πρέπει να αποτελεί τεχνική διασφάλιση και να μην παρέχει από μόνη της νομική βάση για την επεξεργασία. Όπως ορίζεται στο άρθρο 9 παράγραφος 4 του κανονισμού (ΕΕ) 2016/679, τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία.

(3) Προκειμένου να δοθεί στα κράτη μέλη επαρκής χρόνος για να προσαρμόσουν τις εθνικές τους διαδικασίες, το πορτρέτο του χρήστη πορτοφολιού μπορεί να αποτελεί μέρος των υποχρεωτικών δεδομένων ταυτοποίησης φυσικού προσώπου μόνο από τις 11 Αυγούστου 2028. Όταν οι εν λόγω εικόνες αντλούνται από υφιστάμενα έγγραφα ταυτότητας, όπως δελτία ταυτότητας ή διαβατήρια, ισχύουν οι σχετικές απαιτήσεις που ορίζονται στους κανονισμούς (ΕΕ) 2025/1208 ([8]) ή (ΕΚ) αριθ. 2252/2004 του Συμβουλίου ([9]), αντίστοιχα.

(4) Ο κανονισμός (ΕΕ) αριθ. 910/2014 ορίζει ότι τα πορτοφόλια είναι ικανά να επιδεικνύουν σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ ως επαληθεύσιμη, απλή και αναγνωρίσιμη ένδειξη ότι ένα πορτοφόλι έχει παρασχεθεί σύμφωνα με τον κανονισμό. Η χρήση του εν λόγω σήματος εμπιστοσύνης θα υποστηρίξει την αποτελεσματική λειτουργία της εσωτερικής αγοράς, θα διασφαλίσει τον θεμιτό ανταγωνισμό και θα προστατεύσει τα συμφέροντα των καταναλωτών. Για να είναι δυνατή η χρήση ενός τέτοιου σήματος εμπιστοσύνης, θα πρέπει να καθοριστούν τα οπτικά και τεχνικά χαρακτηριστικά του σήματος εμπιστοσύνης.

(5) Όπως ορίζεται στο άρθρο 12β του κανονισμού (ΕΕ) αριθ. 910/2014, οι πυλωροί πρέπει να παρέχουν στους παρόχους ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας και στους εκδότες κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης αποτελεσματική διαλειτουργικότητα με τα ίδια χαρακτηριστικά λειτουργικού συστήματος, υλισμικού ή λογισμικού και, για τους σκοπούς της διαλειτουργικότητας, πρόσβαση στα ίδια χαρακτηριστικά. Η αποτελεσματική διαλειτουργικότητα και πρόσβαση πρέπει να παρέχονται δωρεάν και ανεξάρτητα από το αν τα εν λόγω χαρακτηριστικά υλισμικού ή λογισμικού αποτελούν μέρος του λειτουργικού συστήματος, είναι διαθέσιμα στον εν λόγω πυλωρό ή χρησιμοποιούνται από αυτόν κατά την παροχή των εν λόγω υπηρεσιών. Δεδομένου ότι όλες οι υλοποιήσεις πορτοφολιού θα πρέπει να υποστηρίζουν ένα κοινό σύνολο πρωτοκόλλων και διεπαφών προκειμένου να διασφαλίζεται η χρηστικότητα, η ασφάλεια και η διαλειτουργικότητα σε όλα τα κράτη μέλη, οι πυλωροί θα πρέπει να επιτρέπουν τα χαρακτηριστικά λειτουργικού συστήματος, υλισμικού ή λογισμικού που απαιτούνται για την εφαρμογή των πρωτοκόλλων και των διεπαφών που ορίζονται στο παράρτημα XII του παρόντος κανονισμού. Στο πλαίσιο αυτό, στις επιγραμμικές ροές μεταξύ διατάξεων, τόσο για τον έλεγχο της φυσικής εγγύτητας όσο και για τη μεταφορά δεδομένων μεταξύ των δύο διατάξεων, οι πυλωροί θα πρέπει να προτιμούν έναν τοπικό δίαυλο επικοινωνίας, όπως προβλέπεται από την έκδοση 2.3 των προδιαγραφών του πρωτοκόλλου CTAP (Client To Authenticator Protocol) ([10]), αντί της χρήσης υπηρεσιών CTAP Hybrid Tunnel.

(6) Προκειμένου να δοθεί στα κράτη μέλη, στους παρόχους πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών και στους παρόχους πορτοφολιού επαρκής χρόνος ώστε οι μονάδες πορτοφολιού να είναι σε θέση να επαληθεύουν και να επικυρώνουν τα πιστοποιητικά καταχώρισης βασιζόμενων σε πορτοφόλι μερών, η απαίτηση αυτή θα πρέπει να εφαρμόζεται μόνο από τις 11 Αυγούστου 2028.

(7) Ο κανονισμός (ΕΕ) 2016/679 και, κατά περίπτωση, η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]) εφαρμόζονται σε όλες τις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του παρόντος κανονισμού.

([7]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Κανονισμός (ΕΕ) 2025/1208 του Συμβουλίου, της 12ης Ιουνίου 2025, για την ενίσχυση της ασφάλειας των δελτίων ταυτότητας των πολιτών της Ένωσης και των εγγράφων διαμονής που εκδίδονται για τους πολίτες της Ένωσης και τα μέλη των οικογενειών τους που ασκούν το δικαίωμα ελεύθερης κυκλοφορίας, (ΕΕ L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Κανονισμός (ΕΚ) αριθ. 2252/2004 του Συμβουλίου, της 13ης Δεκεμβρίου 2004, σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών (ΕΕ L 385 της 29.12.2004, σ. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Προτεινόμενο πρότυπο της Fido Alliance, Client to Authenticator Protocol (CTAP), 26 Φεβρουαρίου 2026.

([11]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([12]), ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ο οποίος γνωμοδότησε στις 17 Απριλίου 2026 ([13]).

(9) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 48 του κανονισμού (ΕΕ) αριθ. 910/2014,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Τροποποιήσεις του εκτελεστικού κανονισμού (ΕΕ) 2024/2977

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/2977 τροποποιείται ως εξής:

1) Παρεμβάλλεται το ακόλουθο άρθρο 3α:

«*Άρθρο 3α*

Προστασία του πορτρέτου

1. Πέρα από τις απαιτήσεις πληροφοριών σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, οι πάροχοι πορτοφολιών διασφαλίζουν ότι παρέχουν υλοποιήσεις πορτοφολιού που εκδίδουν προειδοποιήσεις στους χρήστες πορτοφολιού όταν τα βασιζόμενα σε πορτοφόλι μέρη ζητούν γνωστοποίηση του πορτρέτου, αναφέροντας ότι το αίτημα περιλαμβάνει κοινοχρησία βιομετρικών δεδομένων και ότι απαιτείται επιβεβαίωση για την επιλεκτική γνωστοποίηση του πορτρέτου.

2. Για την εφαρμογή της επιλεκτικής γνωστοποίησης του πορτρέτου σε βασιζόμενο σε πορτοφόλι μέρος, οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι υλοποιήσεις πορτοφολιού απαιτούν από τον χρήστη πορτοφολιού να επιβεβαιώσει ρητά και συγκεκριμένα την παρουσίαση του πορτρέτου.

3. Το πορτρέτο δεν διατηρείται από τα βασιζόμενα σε πορτοφόλι μέρη, εκτός εάν η επεξεργασία του είναι απαραίτητη για τους σκοπούς της ταυτοποίησης και της επαλήθευσης ταυτότητας σύμφωνα με το δίκαιο της Ένωσης για την προστασία των δεδομένων ή όταν αυτό προβλέπεται από το ενωσιακό ή το εθνικό δίκαιο, σε συμμόρφωση με το ενωσιακό δίκαιο για την προστασία των δεδομένων. Το πορτρέτο δεν διαβιβάζεται σε τρίτες χώρες ή διεθνείς οργανισμούς, εκτός εάν αυτό επιτρέπεται από το δίκαιο της Ένωσης για την προστασία των δεδομένων.»·

2) Στο άρθρο 4, η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Οι ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται προς μονάδες πορτοφολιού συμμορφώνονται με τουλάχιστον ένα από τα πρότυπα που ορίζονται στο παράρτημα ΙΙ του εκτελεστικού κανονισμού (ΕΕ) 2024/2979.»·

3) Το άρθρο 5 παράγραφος 4 στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) όταν έχει ανακληθεί η βεβαίωση μονάδας πορτοφολιού για την οποία εκδόθηκαν τα δεδομένα ταυτοποίησης προσώπου·»·

4) Το παράρτημα αντικαθίσταται από το κείμενο του παραρτήματος Ι του παρόντος κανονισμού.

([12]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | European Data Protection Supervisor (Επίσημες παρατηρήσεις του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σχετικά με το σχέδιο εκτελεστικού κανονισμού της Επιτροπής όσον αφορά τα εφαρμοστέα πρότυπα και τις εφαρμοστέες προδιαγραφές για την καταχώριση βασιζόμενων σε πορτοφόλι μερών | Ευρωπαίος Επόπτης Προστασίας Δεδομένων).

Άρθρο 2

Τροποποιήσεις του εκτελεστικού κανονισμού (ΕΕ) 2024/2979

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/2979 τροποποιείται ως εξής:

1) Στο άρθρο 3, η παράγραφος 2 απαλείφεται·

2) Στο άρθρο 5 παράγραφος 1, το στοιχείο α) αντικαθίσταται από το ακόλουθο κείμενο:

«α) εκτελούν κρυπτογραφικές λειτουργίες πορτοφολιού που αφορούν κρίσιμους πόρους, οι οποίοι αποθηκεύονται σε ασφαλή κρυπτογραφική διάταξη πορτοφολιού και δεν απαιτούνται για την επαλήθευση ταυτότητας του χρήστη πορτοφολιού, μόνο σε περιπτώσεις στις οποίες οι εν λόγω εφαρμογές έχουν επαληθεύσει επιτυχώς την ταυτότητα χρηστών πορτοφολιού·»·

3) Προστίθεται το ακόλουθο άρθρο 5α:

«*Άρθρο 5α*

Κρυπτογραφικοί μηχανισμοί

Για τους σκοπούς του άρθρου 4 παράγραφος 2, οι πάροχοι πορτοφολιών χρησιμοποιούν μόνο τους κρυπτογραφικούς μηχανισμούς που αναφέρονται στο παράρτημα Ια.»·

4) Το άρθρο 6 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Οι πάροχοι πορτοφολιών εκδίδουν βεβαιώσεις μονάδας πορτοφολιού για κάθε μονάδα πορτοφολιού. Οι πάροχοι πορτοφολιών υπογράφουν ή σφραγίζουν τις βεβαιώσεις μονάδας πορτοφολιού κατά τρόπο ώστε οι υπογραφές ή οι σφραγίδες να μπορούν να επικυρωθούν μέσω πιστοποιητικού που παρατίθεται στο παράρτημα ΙΙ τμήμα 2 σημείο 1 στοιχείο η) του εκτελεστικού κανονισμού (ΕΕ) 2024/2980.»·

β) η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι βεβαιώσεις μονάδας πορτοφολιού που αναφέρονται στην παράγραφο 1 πληρούν τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα Ιβ.»·

γ) στην παράγραφο 3, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) παρέχουν μηχανισμούς ασφαλούς ταυτοποίησης και επαλήθευσης ταυτότητας των χρηστών πορτοφολιού, οι οποίοι είναι ανεξάρτητοι από τις μονάδες πορτοφολιού»·

5) Στο άρθρο 9 παράγραφος 2, το στοιχείο β) αντικαθίσταται από το ακόλουθο κείμενο:

«β) το ονοματεπώνυμο, τα στοιχεία επικοινωνίας και τον μοναδικό αναγνωριστικό κωδικό του αντίστοιχου βασιζόμενου σε πορτοφόλι μέρους και το κράτος μέλος στο οποίο είναι εγκατεστημένο το εν λόγω βασιζόμενο σε πορτοφόλι μέρος·»·

6) Στο άρθρο 10, η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται σύμφωνα με τις ισχύουσες τεχνικές προδιαγραφές για τις κοινές ενσωματωμένες πολιτικές γνωστοποίησης που παρατίθενται στο παράρτημα ΙΙΙ μπορούν να υποβάλλονται σε επεξεργασία από τις μονάδες πορτοφολιού τις οποίες παρέχουν.»·

7) Το άρθρο 12 τροποποιείται ως εξής:

α) στην παράγραφο 2, το στοιχείο γ) αντικαθίσταται από το ακόλουθο κείμενο:

«γ) δημιουργία υπογραφών ή σφραγίδων σύμφωνα τουλάχιστον με τους υποχρεωτικούς μορφότυπους υπογραφής ή σφραγίδας που αναφέρονται στο παράρτημα IV·»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Οι εφαρμογές δημιουργίας υπογραφής μπορούν είτε να είναι ενσωματωμένες σε στιγμιότυπα πορτοφολιού είτε να είναι εξωτερικές.»·

γ) προστίθεται η ακόλουθη παράγραφος:

«4. Οι εφαρμογές δημιουργίας υπογραφής που χρησιμοποιούνται από μονάδες πορτοφολιού υποστηρίζουν τουλάχιστον τη διεπαφή προγραμματισμού εφαρμογών που αναφέρεται στο παράρτημα IV.»·

8) Στο άρθρο 14, η παράγραφος 1 απαλείφεται·

9) Παρεμβάλλεται το ακόλουθο άρθρο 14α:

«*Άρθρο 14α*

Σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ

1. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι μονάδες πορτοφολιού επιδεικνύουν το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ. Το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ έχει τη μορφή που ορίζεται στα παραρτήματα VI και VII.

2. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι μονάδες πορτοφολιού παρέχουν στους χρήστες πορτοφολιού τη δυνατότητα πρόσβασης σε πληροφορίες που τους επιτρέπουν να επαληθεύουν το καθεστώς πιστοποίησης της υλοποίησης πορτοφολιού. Για τον σκοπό αυτόν, οι πάροχοι πορτοφολιών διασφαλίζουν ότι, μετά την καταχώριση υλοποίησης πορτοφολιού, οι αντίστοιχες μονάδες πορτοφολιού περιλαμβάνουν τις διευθύνσεις URL που παρέχει η Ευρωπαϊκή Επιτροπή για την εν λόγω επαλήθευση. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι μονάδες πορτοφολιού τους έχουν πρόσβαση σε δεδομένα σήματος εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ τα οποία πληρούν τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα VIII.

3. Τα χρώματα αναφοράς του σήματος εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ είναι τα χρώματα Pantone αριθ. 661 και 116 ή το κυανό (100 % κυανό + 67 % ματζέντα + 0 % κίτρινο + 40 % μαύρο) και το κίτρινο (0 % κυανό + 20 % ματζέντα + 100 % κίτρινο + 0 % μαύρο), όταν χρησιμοποιείται τετραχρωμία· όταν χρησιμοποιούνται χρώματα RGB, τα χρώματα αναφοράς είναι το κυανό (0 κόκκινο + 51 πράσινο + 153 κυανό) και το κίτρινο (255 κόκκινο + 204 πράσινο + 0 κυανό).

4. Μόνο όταν η χρήση χρώματος δεν είναι εφικτή, το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ μπορεί να χρησιμοποιείται σε ασπρόμαυρη έκδοση, όπως ορίζεται στο παράρτημα VII.

5. Όταν το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ χρησιμοποιείται σε σκούρο φόντο, το λογότυπο μπορεί να χρησιμοποιηθεί σε αρνητικό με χρήση του ίδιου χρώματος φόντου. Όταν χρησιμοποιείται έγχρωμο σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ σε έγχρωμο φόντο που το καθιστά δυσδιάκριτο, μπορεί να χρησιμοποιείται περίγραμμα γύρω από το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ για τη βελτίωση της αντίθεσης με το φόντο.

6. Το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ έχει ελάχιστες διαστάσεις 64 × 85 pixels σε 150 dpi.

7. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ χρησιμοποιείται κατά τρόπο που προσδιορίζει σαφώς τη μονάδα πορτοφολιού την οποία αφορά το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ. Το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ μπορεί να συνδέεται με γραφικά στοιχεία ή στοιχεία κειμένου που προσδιορίζουν σαφώς τη μονάδα πορτοφολιού για την οποία χρησιμοποιείται, υπό την προϋπόθεση ότι δεν αλλάζουν την αναγνωρισιμότητά του ως σήματος εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ ούτε μεταβάλλουν τη σύνδεση με τον κατάλογο πιστοποιημένων ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας που αναφέρεται στο άρθρο 5δ του κανονισμού (ΕΕ) αριθ. 910/2014.

8. Εάν οι πάροχοι πορτοφολιών έχουν ανακαλέσει βεβαίωση μονάδας πορτοφολιού, μεριμνούν ώστε η αντίστοιχη μονάδα πορτοφολιού να μην επιδεικνύει πλέον το σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ.»·

10) Προστίθενται τα παραρτήματα Ια και Ιβ, όπως ορίζεται στο παράρτημα II και στο παράρτημα III του παρόντος κανονισμού·

11) Το παράρτημα II αντικαθίσταται από το παράρτημα IV του παρόντος κανονισμού·

12) Το παράρτημα III αντικαθίσταται από το παράρτημα V του παρόντος κανονισμού·

13) Το παράρτημα IV τροποποιείται σύμφωνα με το παράρτημα VI του παρόντος κανονισμού·

14) Το παράρτημα V απαλείφεται·

15) Το κείμενο που παρατίθεται στο παράρτημα VII του παρόντος κανονισμού προστίθεται ως παράρτημα VI·

16) Το κείμενο που παρατίθεται στο παράρτημα VIII του παρόντος κανονισμού προστίθεται ως παράρτημα VII·

17) Το κείμενο που παρατίθεται στο παράρτημα IX του παρόντος κανονισμού προστίθεται ως παράρτημα VIII.

Άρθρο 3

Τροποποιήσεις του εκτελεστικού κανονισμού (ΕΕ) 2024/2980

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/2980 τροποποιείται ως εξής:

1) Στο άρθρο 5, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2. Κατά περίπτωση, η Επιτροπή καταρτίζει, τηρεί και δημοσιεύει κατάλογο με τις πληροφορίες που κοινοποιούνται από τα κράτη μέλη σχετικά με τους παρόχους πορτοφολιών, τους παρόχους δεδομένων ταυτοποίησης προσώπου, τους παρόχους πιστοποιητικών πρόσβασης βασιζόμενων σε πορτοφόλι μερών και τους παρόχους πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών, όπως αναφέρεται στο παράρτημα ΙΙ τμήματα 2, 3, 4 και 5.»·

2) Το παράρτημα ΙΙ του εκτελεστικού κανονισμού (ΕΕ) 2024/2980 τροποποιείται σύμφωνα με το παράρτημα Χ του παρόντος κανονισμού.

Άρθρο 4

Τροποποιήσεις του εκτελεστικού κανονισμού (ΕΕ) 2024/2982

Ο εκτελεστικός κανονισμός (ΕΕ) 2024/2982 τροποποιείται ως εξής:

1) Στο άρθρο 1, η παράγραφος 2 αντικαθίσταται από το ακόλουθο κείμενο:

«2) την προσκόμιση των χαρακτηριστικών δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών σε βασιζόμενα σε πορτοφόλι μέρη·»·

2) Το άρθρο 3 τροποποιείται ως εξής:

α) η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1) επαληθεύουν και επικυρώνουν τα πιστοποιητικά πρόσβασης των βασιζόμενων σε πορτοφόλι μερών όταν αλληλεπιδρούν με βασιζόμενα σε πορτοφόλι μέρη, χωρίς να αναθέτουν την εκτέλεση των εν λόγω διαδικασιών σε φυλλομετρητή λειτουργικού συστήματος ή σε άλλη ενδιάμεση εφαρμογή·»·

β) η παράγραφος 2 απαλείφεται·

γ) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3) επαληθεύουν και επικυρώνουν αιτήματα που υποβάλλονται με τη χρήση πιστοποιητικών πρόσβασης βασιζόμενων σε πορτοφόλι μερών·»·

δ) η παράγραφος 4 αντικαθίσταται από το ακόλουθο κείμενο:

«4) επαληθεύουν και επικυρώνουν το πιστοποιητικό καταχώρισης του βασιζόμενου σε πορτοφόλι μέρους·»·

ε) η παράγραφος 5 αντικαθίσταται από το ακόλουθο κείμενο:

«5) παρουσιάζουν σε χρήστες πορτοφολιού τις πληροφορίες που περιέχονται στο πιστοποιητικό πρόσβασης βασιζόμενου σε πορτοφόλι μέρους·»·

στ) η παράγραφος 8 απαλείφεται·

ζ) η παράγραφος 9 αντικαθίσταται από το ακόλουθο κείμενο:

«9) δεν προσκομίζουν τυχόν ζητούμενα χαρακτηριστικά σε βασιζόμενα σε πορτοφόλι μέρη έως ότου ολοκληρωθούν τα ακόλουθα στάδια:

α) βεβαίωση ότι οι ενσωματωμένες πολιτικές γνωστοποίησης έχουν υποβληθεί σε επεξεργασία εντός της μονάδας πορτοφολιού σύμφωνα με το άρθρο 10 του εκτελεστικού κανονισμού (ΕΕ) 2024/2979·

β) βεβαίωση ότι οι χρήστες πορτοφολιού έχουν εγκρίνει εν μέρει ή πλήρως την προσκόμιση.»·

3) Στο άρθρο 4, η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι υλοποιήσεις πορτοφολιού υποστηρίζουν τα πρωτόκολλα και τις διεπαφές που παρατίθενται στο παράρτημα Ι για την έκδοση δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών προς μονάδες πορτοφολιού.»·

4) Το άρθρο 5 τροποποιείται ως εξής:

α) οι παράγραφοι 1 και 2 αντικαθίστανται από το ακόλουθο κείμενο:

«1. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι οι υλοποιήσεις πορτοφολιών υποστηρίζουν πρωτόκολλα και διεπαφές για την προσκόμιση χαρακτηριστικών σε βασιζόμενα σε πορτοφόλι μέρη, εξ αποστάσεως και, κατά περίπτωση, από κοντά, σύμφωνα με τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα ΙΙ.

2. Οι πάροχοι πορτοφολιών διασφαλίζουν ότι, κατόπιν αιτήματος των χρηστών, οι μονάδες πορτοφολιού ανταποκρίνονται σε επιτυχώς επαληθευμένα και επικυρωμένα αιτήματα από βασιζόμενα σε πορτοφόλι μέρη που αναφέρονται στο άρθρο 3, σύμφωνα με τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα ΙΙ.»·

β) η παράγραφος 5 απαλείφεται·

5) Το άρθρο 8 αντικαθίσταται από το ακόλουθο κείμενο:

«*Άρθρο 8*

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Το άρθρο 3 παράγραφος 4 εφαρμόζεται από τις 11 Αυγούστου 2028.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.»·

6) Το παράρτημα απαλείφεται·

7) Το κείμενο που παρατίθεται στο παράρτημα XI του παρόντος κανονισμού προστίθεται ως παράρτημα Ι·

8) Το κείμενο που παρατίθεται στο παράρτημα XII του παρόντος κανονισμού προστίθεται ως παράρτημα ΙΙ.

Άρθρο 5

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 15 Ιουλίου 2026.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ Ι

«ΠΑΡΑΡΤΗΜΑ

Τεχνικές προδιαγραφές για τα δεδομένα ταυτοποίησης προσώπου που αναφέρονται στο άρθρο 3 παράγραφος 3

1. Τμήμα 1: Σύνολο δεδομένων ταυτοποίησης φυσικού προσώπου

Πίνακας 1

Υποχρεωτικά στοιχεία ταυτοποίησης φυσικών προσώπων για επιλεκτική γνωστοποίηση

Αναγνωριστικό δεδομένων	Ορισμός
`family_name`	Τρέχον/-τα επώνυμο/-α του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`given_name`	Τρέχον/-τα όνομα/ονόματα, συμπεριλαμβανομένου του/των μεσαίου/-ων ονόματος/ονομάτων, κατά περίπτωση, του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`birth_date`	Ημέρα, μήνας και έτος γέννησης του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`birth_place`	Η χώρα ως κωδικός χώρας alpha-2, όπως ορίζεται στο πρότυπο ISO 3166-1, ή το κράτος, η επαρχία, η περιφέρεια ή η τοπική περιοχή ή ο δήμος, η πόλη, η κωμόπολη ή το χωριό όπου γεννήθηκε ο χρήστης τον οποίο αφορούν τα στοιχεία ταυτοποίησης προσώπου.
`nationality`	Ένας ή περισσότεροι κωδικοί χώρας alpha-2, όπως ορίζονται στο πρότυπο ISO 3166-1, οι οποίοι αντιπροσωπεύουν την ιθαγένεια του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`portrait`	Εκτός από τις περιπτώσεις κατά τις οποίες ο χρήστης επιλέγει ρητά να εξαιρεθεί, κατά περίπτωση, εικόνα προσώπου του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου σύμφωνα με τις απαιτήσεις ποιότητας για τύπο πλήρους κατά μέτωπο εικόνας, όπως ορίζεται στο πρότυπο ISO/IEC 39794-5, ή, για οπισθόδρομη συμβατότητα, όπως ορίζεται στο πρότυπο ISO/IEC 19794-5, σημεία 8.2, 8.3 και 8.4, υπό την προϋπόθεση ότι τα κωδικοποιημένα δεδομένα εικόνας χωρίς τις κεφαλίδες ή τις ενότητες όπως ορίζονται στο σημείο 5 του προτύπου ISO/IEC 19794-5, εξαιρουμένων των δεδομένων της ίδιας της εικόνας (JPEG), εφαρμόζονται από τις 11 Αυγούστου 2028.

— Τα κράτη μέλη μπορούν να προβλέπουν ότι ο χρήστης έχει τη δυνατότητα να αρνηθεί την προσθήκη του πορτρέτου στα δεδομένα ταυτοποίησης προσώπου.

— Τα κράτη μέλη διασφαλίζουν ότι η επιλεκτική γνωστοποίηση εφαρμόζεται σε κάθε αναγνωριστικό δεδομένων, συμπεριλαμβανομένου του πορτρέτου.

— Όταν δεν είναι γνωστή η ημερομηνία γέννησης του φυσικού προσώπου, τα κράτη μέλη επιλέγουν κατάλληλες τιμές οι οποίες πληρούν τις προδιαγραφές που ορίζονται στα τμήματα 4.1 ή 4.2 (κατά περίπτωση) του παρόντος παραρτήματος.

— Όταν δεν είναι γνωστή η ιθαγένεια του φυσικού προσώπου, τα κράτη μέλη χρησιμοποιούν την τιμή “QU”.

— Όταν δεν έχει ιθαγένεια το φυσικό πρόσωπο, τα κράτη μέλη χρησιμοποιούν την τιμή “QS”.

— Όταν ο χρήστης επιλέγει να εξαιρεθεί από την προσθήκη του πορτρέτου, τα κράτη μέλη αφήνουν την τιμή κενή.

Πίνακας 2

Προαιρετικά στοιχεία ταυτοποίησης φυσικών προσώπων για επιλεκτική γνωστοποίηση

Αναγνωριστικό δεδομένων	Ορισμός
`resident_address`	Η πλήρης διεύθυνση του τόπου τρέχουσας διαμονής ή του τόπου επικοινωνίας του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου (οδός, αριθμός οικίας, πόλη κ.λπ.).
`resident_country`	Η χώρα τρέχουσας διαμονής του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου, ως κωδικός χώρας alpha-2 που ορίζεται στο πρότυπο ISO 3166-1.
`resident_state`	Το κράτος, η επαρχία, η περιφέρεια ή η τοπική περιοχή όπου διαμένει επί του παρόντος ο χρήστης τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`resident_city`	Ο δήμος, η πόλη, η κωμόπολη ή το χωριό τρέχουσας διαμονής του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`resident_postal_code`	Ο ταχυδρομικός κώδικας του τόπου τρέχουσας διαμονής του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.
`resident_street`	Το όνομα της οδού τρέχουσας διαμονής του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου, συμπεριλαμβανομένων του αριθμού της οικίας και τυχόν προθήματος ή επιθήματος.
`personal_administrative_-number`	Τιμή που αποδίδεται στον χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου και είναι μοναδική μεταξύ όλων των προσωπικών διοικητικών αριθμών που εκδίδονται από τον πάροχο των δεδομένων ταυτοποίησης προσώπου. Όταν τα κράτη μέλη επιλέγουν να συμπεριλάβουν το χαρακτηριστικό αυτό, περιγράφουν στα οικεία συστήματα ηλεκτρονικής ταυτοποίησης, βάσει των οποίων εκδίδονται τα δεδομένα ταυτοποίησης προσώπου, την πολιτική που εφαρμόζουν στις τιμές του εν λόγω χαρακτηριστικού, συμπεριλαμβανομένων, κατά περίπτωση, ειδικών όρων για την επεξεργασία της συγκεκριμένης τιμής.
`family_name_birth`	Επώνυμο/-α του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου κατά τον χρόνο γέννησης.
`given_name_birth`	Όνομα/Ονόματα, συμπεριλαμβανομένου του/των μεσαίου/-ων ονόματος/ονομάτων του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου κατά τον χρόνο γέννησης.
`sex`	Οι τιμές είναι μία από τις ακόλουθες: 0 = άγνωστο· 1 = αρσενικό· 2 = θηλυκό· 3 = άλλο· 4 = ίντερσεξ· 5 = φυλοδιαφορετικό· 6 = ανοικτό· 9 = άνευ αντικειμένου. Για τις τιμές 0, 1, 2 και 9, εφαρμόζεται το πρότυπο ISO/IEC 5218.
`email_address`	Διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου [σύμφωνα με το RFC 5322 ([1])].

Αναγνωριστικό δεδομένων	Ορισμός
mobile_phone_number	Αριθμός κινητού τηλεφώνου του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου, ο οποίος ξεκινά με το σύμβολο «+» ως πρόθεμα διεθνούς κωδικού και τον κωδικό χώρας, ακολουθούμενο μόνο από αριθμούς.

([1]) P. Resnick, Ed., "Internet Message Format", RFC 5322, Οκτώβριος 2008.

2. Τμήμα 2: Σύνολο δεδομένων ταυτοποίησης για νομικά πρόσωπα

Πίνακας 3

Υποχρεωτικά στοιχεία ταυτοποίησης προσώπου για νομικά πρόσωπα

Αναγνωριστικό δεδομένων
τρέχουσα επωνυμία
μοναδικός αναγνωριστικός κωδικός, κατασκευασμένος από το αποστέλλον κράτος μέλος σύμφωνα με τις τεχνικές προδιαγραφές για τους σκοπούς της διασυνοριακής αναγνώρισης και ο οποίος είναι όσο το δυνατόν πιο ανθεκτικός στο χρόνο

— Όταν δεν είναι γνωστό ένα αναγνωριστικό δεδομένων για το πρόσωπο ή δεν μπορεί να εκδοθεί με άλλον τρόπο ως μέρος του συνόλου δεδομένων ταυτοποίησης προσώπου, τα κράτη μέλη χρησιμοποιούν τιμή χαρακτηριστικού η οποία είναι κατάλληλη για την περίπτωση.

Πίνακας 4

Προαιρετικά στοιχεία ταυτοποίησης προσώπου για νομικά πρόσωπα

Αναγνωριστικό δεδομένων
τρέχουσα διεύθυνση
αριθμός φορολογικού μητρώου ΦΠΑ
αριθμός φορολογικού μητρώου
ευρωπαϊκός μοναδικός αναγνωριστικός κωδικός που αναφέρεται στην οδηγία (ΕΕ) 2017/1132 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1])
αναγνωριστικός κωδικός νομικής οντότητας (LEI) που αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) αριθ. 2022/1860 της Επιτροπής ([2])
καταχώριση και αναγνώριση οικονομικών φορέων (EORI) που αναφέρεται στον εκτελεστικό κανονισμό (ΕΕ) αριθ. 1352/2013 της Επιτροπής ([3])
αριθμός ειδικού φόρου κατανάλωσης που προβλέπεται στο άρθρο 2 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 389/2012 του Συμβουλίου ([4])

([1]) Οδηγία (ΕΕ) 2017/1132 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Ιουνίου 2017, σχετικά με ορισμένες πτυχές του εταιρικού δίκαιου (ΕΕ L 169 της 30.6.2017, σ. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Εκτελεστικός κανονισμός (ΕΕ) 2022/1860 της Επιτροπής, της 10ης Ιουνίου 2022, για τον καθορισμό εκτελεστικών τεχνικών προτύπων για την εφαρμογή του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα πρότυπα, τους μορφότυπους, τη συχνότητα και τις μεθόδους και ρυθμίσεις για την υποβολή αναφορών (ΕΕ L 262 της 7.10.2022, σ. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Εκτελεστικός κανονισμός (ΕΕ) αριθ. 1352/2013 της Επιτροπής, της 4ης Δεκεμβρίου 2013, για την κατάρτιση των εντύπων που προβλέπονται στον κανονισμό (ΕΕ) αριθ. 608/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την τελωνειακή επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας (ΕΕ L 341 της 18.12.2013, σ. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Κανονισμός (ΕΕ) αριθ. 389/2012 του Συμβουλίου, της 2ας Μαΐου 2012 , για την διοικητική συνεργασία στον τομέα των ειδικών φόρων κατανάλωσης και την κατάργηση του κανονισμού (ΕΚ) αριθ. 2073/2004 (ΕΕ L 121 της 8.5.2012, σ. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3. Τμήμα 3: Σύνολο μεταδεδομένων σχετικά με τα δεδομένα ταυτοποίησης προσώπου

Πίνακας 5

Μεταδεδομένα σχετικά με τα δεδομένα ταυτοποίησης προσώπου

Αναγνωριστικό δεδομένων	Ορισμός	Παρουσία
`issuing_authority`	Ονομασία της διοικητικής αρχής που εξέδωσε τα δεδομένα ταυτοποίησης προσώπου ή κωδικός χώρας alpha-2, όπως ορίζεται στο πρότυπο ISO 3166, του αντίστοιχου κράτους μέλους, εάν δεν υπάρχει χωριστή αρχή εξουσιοδοτημένη να εκδίδει δεδομένα ταυτοποίησης προσώπου.	υποχρεωτική
`issuing_country`	Κωδικός χώρας alpha-2, όπως ορίζεται στο πρότυπο ISO 3166-1, της χώρας ή του εδάφους του παρόχου των δεδομένων ταυτοποίησης προσώπου.	υποχρεωτική
`expiry_date`	Ημερομηνία (και, εάν είναι δυνατόν, ώρα) κατά την οποία θα λήξει η περίοδος διοικητικής ισχύος των δεδομένων ταυτοποίησης προσώπου.	προαιρετική
`document_number`	Αριθμός για τα δεδομένα ταυτοποίησης προσώπου, ο οποίος χορηγείται από τον πάροχο των δεδομένων ταυτοποίησης προσώπου.	προαιρετική
`issuing_jurisdiction`	Κωδικός υποδιαίρεσης χώρας της δικαιοδοσίας που εξέδωσε τα δεδομένα ταυτοποίησης προσώπου, όπως ορίζεται στο πρότυπο ISO 3166-2:2020 σημείο 8. Το πρώτο μέρος του κωδικού είναι το ίδιο με την τιμή για τη χώρα έκδοσης.	προαιρετική
`issuance_date`	Ημερομηνία και, εάν είναι δυνατόν, ώρα έναρξης της περιόδου διοικητικής ισχύος των δεδομένων ταυτοποίησης προσώπου.	προαιρετική

4. Τμήμα 4: Κωδικοποίηση χαρακτηριστικών δεδομένων ταυτοποίησης φυσικού προσώπου

— Τα δεδομένα ταυτοποίησης φυσικού προσώπου εκδίδονται σύμφωνα με τα πρότυπα που ορίζονται στο παράρτημα ΙΙ του εκτελεστικού κανονισμού (ΕΕ) 2024/2979, σημεία 5 (μορφότυπος SD-JWT VC) και 6 (μορφότυπος ISO/IEC-mdoc), όπως εφαρμόζονται στις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών. Δεν εφαρμόζονται τα σημεία 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 και 6.2.5.

— Η κωδικοποίηση των δεδομένων ταυτοποίησης φυσικού προσώπου πληροί τις τεχνικές προδιαγραφές που περιλαμβάνονται στα τμήματα 4.1 και 4.2 του παρόντος παραρτήματος.

4.1 Κωδικοποίηση των δεδομένων ταυτοποίησης φυσικού προσώπου σε μορφότυπο ISO/IEC-mdoc

— Ο τύπος βεβαίωσης για τα δεδομένα ταυτοποίησης προσώπου σε μορφότυπο ISO/IEC mdoc είναι “eu.europa.ec.eudi.pid.1”. Το αναγνωριστικό του χώρου ονομάτων για τα χαρακτηριστικά δεδομένων ταυτοποίησης προσώπου που ορίζονται στο παρόν παράρτημα είναι “eu.europa.ec.eudi.pid.1”.

— Όταν τα δεδομένα ταυτοποίησης προσώπου περιλαμβάνουν δεδομένα για τα οποία δεν ορίζονται αναγνωριστικά δεδομένων στο παρόν παράρτημα, τα εν λόγω δεδομένα ορίζονται σε εγχώριο χώρο ονομάτων δεδομένων ταυτοποίησης προσώπου που χρησιμοποιεί τον γενικό μορφότυπο eu.europa.ec.eudi.pid.[κωδικός χώρας ISO 3166-1 alpha-2 ή κωδικός περιοχής ISO 3166-2], ακολουθούμενο προαιρετικά από τελεία και αριθμό έκδοσης.

— Όταν χρησιμοποιείται ο εγχώριος χώρος ονομάτων, το οικείο σύστημα, συμπεριλαμβανομένων όλων των αναγνωριστικών δεδομένων, των ορισμών, της παρουσίας και των μορφότυπων κωδικοποίησής τους, δημοσιεύεται σύμφωνα με το άρθρο 8 του εκτελεστικού κανονισμού (ΕΕ) 2025/1569 της Επιτροπής ([1]).

— Τα δεδομένα ταυτοποίησης προσώπου και τα μεταδεδομένα τους που ορίζονται στα τμήματα 1 και 3 του παρόντος παραρτήματος περιλαμβάνονται στα στοιχεία δεδομένων ταυτοποίησης προσώπου κατά την έννοια των προδιαγραφών του μορφότυπου ISO/IEC mdoc.

— Το μέλος deviceKey του μέλους deviceKeyInfo του στιγμιότυπου τύπου MobileSecurityObject περιλαμβάνει δημόσιο κλειδί.

— Το εν λόγω δημόσιο κλειδί αντιστοιχεί σε ιδιωτικό κλειδί που είναι αποθηκευμένο στην ασφαλή κρυπτογραφική διάταξη πορτοφολιού (στο εξής: WSCD) του χρήστη πορτοφολιού.

— Η προστατευόμενη κεφαλίδα της ψηφιακής υπογραφής CB-AdES για την υπογραφή των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο ISO/IEC-mdoc περιλαμβάνει τις παραμέτρους κεφαλίδας x5u και X5T, που ορίζονται αμφότερες στο RFC 9360 ([2]).

— Ο αλγόριθμος σύνοψης που χρησιμοποιείται στην παράμετρο κεφαλίδας x5t είναι SHA-256.

— Οι απαιτήσεις κωδικοποίησης των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο ISO/IEC-mdoc ορίζονται στον πίνακα 6:

Πίνακας 6

Απαιτήσεις κωδικοποίησης των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο ISO/IEC-mdoc

Αναγνωριστικό δεδομένων	Αναγνωριστικό χαρακτηριστικού	Μορφότυπος κωδικοποίησης
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Εκτελεστικός κανονισμός (ΕΕ) 2025/1569 της Επιτροπής, της 29ης Ιουλίου 2025, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τις εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που παρέχονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή (EE L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) J. Schaad, "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates" (https://datatracker.ietf.org/doc/rfc9360/).

Αναγνωριστικό δεδομένων	Αναγνωριστικό χαρακτηριστικού	Μορφότυπος κωδικοποίησης
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate ή full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate ή full-date

— Στη σημειογραφία του μορφότυπου κωδικοποίησης των χαρακτηριστικών που ορίζονται στον πίνακα 6 χρησιμοποιούνται τύποι αναπαράστασης όπως ορίζονται στο RFC 8610 ([3]), με τις ακόλουθες πρόσθετες απαιτήσεις:

α) το tstr κωδικοποιείται σε UTF-8·

β) το tstr υποστηρίζει το πλήρες εύρος Unicode·

γ) το tstr έχει μέγιστο μήκος 150 χαρακτήρων·

δ) η ημερομηνία κωδικοποιείται όπως ορίζεται στο RFC 8943 ([4])·

ε) η πλήρης ημερομηνία ερμηνεύεται ως #6.1004 (tstr), όπου το tag 1004 είναι όπως ορίζεται στο RFC 8943·

στ) το χαρακτηριστικό tdate περιέχει συμβολοσειρά ημερομηνίας-ώρας όπως ορίζεται στο RFC 3339 ([5])·

ζ) το χαρακτηριστικό full-date περιέχει συμβολοσειρά full-date, όπως ορίζεται στο RFC 3339, σύμφωνα με το RFC 8943·

η) εκτός εάν ορίζεται διαφορετικά, στην αναπαράσταση ημερομηνίας με χαρακτηριστικά:

— δεν χρησιμοποιούνται κλάσματα δευτερολέπτων,

— δεν χρησιμοποιείται τοπική διαφορά ώρας από την UTC και η διαφορά ώρας που ορίζεται στο RFC 3339 είναι “Z”·

θ) ο ακέραιος αριθμός με κύριες τιμές 0 και 1 είναι όσο το δυνατόν μικρότερος, όπως ορίζεται στο RFC 8949 ([6]) σημείο 4.2·

ι) το place_of_birth περιλαμβάνει τουλάχιστον ένα από τα ακόλουθα ζεύγη κλειδιού-τιμής: “country”, “region” ή “locality”·

ια) η αναφορά του μήκους σε bstr, tstr, πίνακα ή αντιστοίχιση είναι όσο το δυνατόν βραχύτερη, όπως ορίζεται στο RFC 8949 σημείο 4.2·

([3]) C. Vigano και H. Birkholz, “Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures”, RFC 8610, Ιούνιος 2019.
([4]) M. Jones, A. Nadalin and J. Richter, “Concise Binary Object Representation (CBOR) Tags for Date”, RFC 8943, Νοέμβριος 2020.
([5]) G. Klyne και C. Newman, “Date and Time on the Internet: Timestamps”, RFC 3339, Ιούλιος 2002.
([6]) C. Bormann και P. Hoffman, “Concise Binary Object Representation (CBOR)”, RFC 8949, Δεκέμβριος 2020.

ιβ) το χαρακτηριστικό ιθαγένειας κωδικοποιείται ως πίνακας κωδικών χώρας alpha-2, όπως ορίζεται στο πρότυπο ISO 3166-1. Όταν χρησιμοποιείται σημειογραφία CDDL όπως ορίζεται στο RFC 8610, η κωδικοποίηση του χαρακτηριστικού έχει ως εξής:

— nationalities = [+ CountryCode],

— CountryCode = tstr, κωδικός χώρας alpha-2 που ορίζεται στο πρότυπο ISO 3166-1,

— όταν ο χρήστης πορτοφολιού τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου έχει πολλαπλές ιθαγένειες και ο πάροχος δεδομένων ταυτοποίησης προσώπου βεβαιώνει τις εν λόγω πολλαπλές ιθαγένειες, ο πάροχος δεδομένων ταυτοποίησης προσώπου μπορεί να συμπεριλάβει όλες τις ιθαγένειες στα δεδομένα ταυτοποίησης προσώπου,

— το χαρακτηριστικό place_of_birth κωδικοποιείται ως τύπος place_of_birth. Όταν χρησιμοποιείται σημειογραφία CDDL όπως ορίζεται στο RFC 8610, η κωδικοποίηση του χαρακτηριστικού έχει ως εξής:

place_of_birth =

{

? 'country': tstr; μοναδικός κωδικός χώρας alpha-2, όπως ορίζεται στο ISO 3166-1

? 'region': tstr; το όνομα κράτους, επαρχίας, περιφέρειας ή τοπικής περιοχής

? 'locality':tstr; το όνομα δήμου, πόλης, κωμόπολης ή χωριού

}

4.2 Απαιτήσεις κωδικοποίησης των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο SD-JWT VC

— Τα δεδομένα ταυτοποίησης προσώπου και τα μεταδεδομένα τους που ορίζονται στο παρόν τμήμα περιλαμβάνονται στα δεδομένα ταυτοποίησης προσώπου ως δηλώσεις κατά την έννοια των προδιαγραφών του μορφότυπου SD-JWT VC.

— Όλες οι δηλώσεις που περιλαμβάνονται στα εκδοθέντα δεδομένα ταυτοποίησης προσώπου, όπως αναφέρονται στην προηγούμενη περίπτωση, είναι επιλεκτικά γνωστοποιήσιμες σε μεμονωμένη βάση, εξαιρουμένων των δηλώσεων που ορίζονται ως μη επιλεκτικά γνωστοποιήσιμες σε μορφότυπο SD-JWT VC.

— Στον πίνακα 7 ορίζεται η κωδικοποίηση των ονομάτων δηλώσεων που είναι δημόσια ονόματα.

— Στον πίνακα 8 ορίζεται η κωδικοποίηση των ονομάτων δηλώσεων που αφορούν ειδικά τα δεδομένα ταυτοποίησης προσώπου.

— Η συμβολοσειρά JSON που χρησιμοποιείται σε δεδομένα ταυτοποίησης προσώπου τα οποία κωδικοποιούνται σε μορφότυπο SD-JWT VC, κωδικοποιείται σε UTF-8 και υποστηρίζει το πλήρες εύρος Unicode, εκτός εάν ρητώς ορίζεται διαφορετικά στον πίνακα 8 κατωτέρω ή στις αναφορές που παρατίθενται σ' αυτόν.

— Οι δηλώσεις JWT nbf και exp, όπως ορίζονται στο RFC 7519 ([7]), χρησιμοποιούνται για να εκφράσουν την περίοδο τεχνικής ισχύος των δεδομένων ταυτοποίησης προσώπου σύμφωνα με τον μορφότυπο SD-JWT VC.

([7]) J. Jones et al., "JSON Web Token (JWT)", RFC 7519, Μάιος 2015.

— Τα δεδομένα ταυτοποίησης προσώπου ενσωματώνουν τη δήλωση cnf, όπως ορίζεται στο RFC 7800 ([8]), η οποία είναι δημόσιο κλειδί που δημιουργείται από ιδιωτικό κλειδί το οποίο είναι αποθηκευμένο στην WSCD της μονάδας πορτοφολιού του χρήστη πορτοφολιού.

— Η προστατευόμενη κεφαλίδα της ψηφιακής υπογραφής για την υπογραφή των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο SD-JWT VC περιλαμβάνει τις παραμέτρους κεφαλίδας x5u και x5t#S256, που ορίζονται στο RFC 7515 ([9]).

Πίνακας 7

Απαιτήσεις κωδικοποίησης των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο SD-JWT VC με τη χρήση δημόσιων ονομάτων

Αναγνωριστικό δεδομένων	Αναγνωριστικό χαρακτηριστικού	Μορφότυπος κωδικοποίησης
`family_name`	`family_name`	συμβολοσειρά
`given_name`	`given_name`	συμβολοσειρά
`birth_date`	`birthdate`	συμβολοσειρά, ISO 8601-1, μορφότυπος EEEE-MM-HH
`birth_place`	`place_of_birth`	δομή JSON
`nationality`	`nationalities`	πίνακας συμβολοσειρών
`resident_address`	`address.formatted`	συμβολοσειρά
`resident_country`	`address.country`	συμβολοσειρά
`resident_state`	`address.region`	συμβολοσειρά
`resident_city`	`address.locality`	συμβολοσειρά
`resident_postal_code`	`address.postal_code`	συμβολοσειρά
`resident_street`	`address.street_address`	συμβολοσειρά
`family_name_birth`	`birth_family_name`	συμβολοσειρά
`given_name_birth`	`birth_given_name`	συμβολοσειρά
`email_address`	`email`	συμβολοσειρά
`mobile_phone_number`	`phone_number`	συμβολοσειρά
`portrait`	`picture`	συμβολοσειρά· διεύθυνση URL δεδομένων που περιέχει πορτρέτο με κωδικοποίηση base64 σε μορφότυπο JPEG

([8]) M. Jones et al., "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, Απρίλιος 2016.
([9]) M. Jones et al., "JSON Web Signature (JWS)", RFC 7515, Μάιος 2015.

Πίνακας 8

Απαιτήσεις κωδικοποίησης των δεδομένων ταυτοποίησης προσώπου σε μορφότυπο SD-JWT VC με τη χρήση ιδιωτικών ονομάτων

Αναγνωριστικό δεδομένων	Αναγνωριστικό χαρακτηριστικού	Μορφότυπος κωδικοποίησης
`expiry_date`	`date_of_expiry`	συμβολοσειρά, ISO 8601-1, μορφότυπος EEEE-MM-HH
`issuance_date`	`date_of_issuance`	συμβολοσειρά, ISO 8601-1, μορφότυπος EEEE-MM-HH
`personal_administrative_-number`	`personal_administrati-ve_number`	συμβολοσειρά
`sex`	`sex`	αριθμός
`issuing_authority`	`issuing_authority`	συμβολοσειρά
`issuing_country`	`issuing_country`	συμβολοσειρά
`document_number`	`document_number`	συμβολοσειρά
`issuing_jurisdiction`	`issuing_jurisdiction`	συμβολοσειρά

— Ο βασικός τύπος δεδομένων ταυτοποίησης προσώπου είναι “urn:eudi:pid:1”, ο οποίος περιλαμβάνεται στη δήλωση vct. Όλα τα δεδομένα ταυτοποίησης προσώπου χρησιμοποιούν τύπους στον χώρο ονομάτων “urn:eudi:pid:”.

— Όταν τα δεδομένα ταυτοποίησης προσώπου περιλαμβάνουν χαρακτηριστικά που δεν ορίζονται στο παρόν παράρτημα, τα χαρακτηριστικά αυτά ορίζονται στο πλαίσιο εγχώριου τύπου.

— Όταν χρησιμοποιείται ο εγχώριος τύπος, το οικείο σύστημα, συμπεριλαμβανομένων όλων των αναγνωριστικών δεδομένων, των ορισμών, της παρουσίας και των μορφότυπων κωδικοποίησής τους, ορίζεται στο σύστημα που δημοσιεύεται σύμφωνα με το άρθρο 8 του εκτελεστικού κανονισμού (ΕΕ) 2025/1569.

5. Τμήμα 5: Στοιχεία υποδομής εμπιστοσύνης

Ο κατάλογος των παρόχων δεδομένων ταυτοποίησης προσώπου που διατίθενται από την Επιτροπή σύμφωνα με τον εκτελεστικό κανονισμό (ΕΕ) 2024/2980 καθιστά δυνατή την επαλήθευση των δεδομένων ταυτοποίησης προσώπου.».

ΠΑΡΑΡΤΗΜΑ ΙΙ

«ΠΑΡΑΡΤΗΜΑ Ια

Κρυπτογραφικοί μηχανισμοί που αναφέρονται στο άρθρο 5α

Ευρωπαϊκή ομάδα πιστοποίησης της κυβερνοασφάλειας, υποομάδα για την κρυπτογραφία: "Συμφωνημένοι κρυπτογραφικοί μηχανισμοί", που δημοσιεύτηκε από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) ([1]).»

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

ΠΑΡΑΡΤΗΜΑ III

«ΠΑΡΑΡΤΗΜΑ Ιβ

Τεχνικές προδιαγραφές για τις βεβαιώσεις μονάδας πορτοφολιού που αναφέρονται στο άρθρο 6 παράγραφος 2α

1) Η βεβαίωση μονάδας πορτοφολιού περιλαμβάνει μία ή περισσότερες βεβαιώσεις στιγμιότυπου πορτοφολιού και μία ή περισσότερες βεβαιώσεις κλειδιού.

2) Η βεβαίωση στιγμιότυπου πορτοφολιού και οι βεβαιώσεις κλειδιού πληρούν τις ακόλουθες απαιτήσεις:

α) Απαιτήσεις μορφότυπου

— FR-WIA-1: Η βεβαίωση στιγμιότυπου πορτοφολιού είναι JSON Web Token (JWT), όπως ορίζεται στο RFC 7519 ([1]), η οποία υπογράφεται ή σφραγίζεται από τον πάροχο πορτοφολιού με τη χρήση συνεπτυγμένης βασικής υπογραφής JAdES επιπέδου B.

— FR-WIA-1.1: Η βεβαίωση στιγμιότυπου πορτοφολιού είναι βεβαίωση πορτοφολιού, όπως ορίζεται στο προσάρτημα Ε του "OpenID for Verifiable Credential Issuance v1.0" ([2]) (στο εξής: OID4VCI), και επεκτείνεται όπως ορίζεται στα C-WIA-1 και C-WIA-2 κατωτέρω.

— FR-KA-1: Η βεβαίωση κλειδιού είναι JWT, όπως ορίζεται στο RFC 7519, η οποία υπογράφεται ή σφραγίζεται από τον πάροχο πορτοφολιού με τη χρήση συνεπτυγμένης βασικής υπογραφής JAdES επιπέδου B.

— FR_KA_1.1: Η βεβαίωση κλειδιού είναι βεβαίωση κλειδιού, όπως ορίζεται στο προσάρτημα Δ του OID4VCI, η οποία επεκτείνεται όπως ορίζεται στα C_KA-1 και C_KA-2 κατωτέρω.

β) Απαιτήσεις μεταφοράς

— TR-WIA-1: Η μονάδα πορτοφολιού χρησιμοποιεί βεβαίωση στιγμιότυπου πορτοφολιού κατά την έκδοση δεδομένων ταυτοποίησης προσώπου, εγκεκριμένων ή μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή.

— TR-WIA-2: Ο πάροχος πορτοφολιού επαληθεύει την ακεραιότητα του στιγμιότυπου πορτοφολιού και υπογράφει ή σφραγίζει τη βεβαίωση στιγμιότυπου πορτοφολιού.

— TR-WIA-2.1: Όταν ο πάροχος πορτοφολιού εκδίδει βεβαίωση στιγμιότυπου πορτοφολιού, η διαφορά μεταξύ της ώρας κατά την οποία ο πάροχος πορτοφολιού επαλήθευσε την ακεραιότητα του στιγμιότυπου πορτοφολιού και της ώρας που θα αναφέρει στην παράμετρο κεφαλίδας "exp" της εκδοθείσας βεβαίωσης στιγμιότυπου πορτοφολιού είναι μικρότερη από 24 ώρες.

— TR-WIA-2.2: Ο πάροχος πορτοφολιού διασφαλίζει ότι η μονάδα πορτοφολιού περιλαμβάνει βεβαιώσεις στιγμιότυπου πορτοφολιού, όπως απαιτείται για την έκδοση δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών.

— TR-WIA-3: Κατά την έκδοση, η μονάδα πορτοφολιού αποστέλλει βεβαίωση στιγμιότυπου πορτοφολιού στον εξυπηρετητή εξουσιοδότησης στο προωθούμενο αίτημα εξουσιοδότησης και στο αίτημα αδειοδοτικού, όπως ορίζεται στο OID4VCI.

— TR-WIA-3.1: Η μονάδα πορτοφολιού αποστέλλει τη βεβαίωση στιγμιότυπου πορτοφολιού μαζί με απόδειξη κατοχής (στο εξής: PoP), όπως ορίζεται στο προσάρτημα Ε του OID4VCI.

— TR-WIA-3.2: Η μονάδα πορτοφολιού αποστέλλει την ίδια βεβαίωση στιγμιότυπου πορτοφολιού σε έναν μόνο εξυπηρετητή εξουσιοδότησης.

([1]) RFC 7519: JSON Web Token (JWT), Μάιος 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Όταν ο πάροχος πορτοφολιού χρησιμοποιεί την επιλογή “per-issuer reuse” που ορίζεται στο R_WIA_1 κατωτέρω, μια μονάδα πορτοφολιού μπορεί να αποστείλει πολλές φορές βεβαίωση στιγμιότυπου πορτοφολιού στον ίδιο εξυπηρετητή εξουσιοδότησης.

— TR-WIA-3.2.2: Όταν ένας πάροχος πορτοφολιού δεν χρησιμοποιεί την επιλογή “per-issuer reuse”, η μονάδα πορτοφολιού χρησιμοποιεί βεβαίωση στιγμιότυπου πορτοφολιού το πολύ σε μία διαδικασία έκδοσης.

— TR-WIA-4: Όταν ένας εξυπηρετητής εξουσιοδότησης λαμβάνει βεβαίωση στιγμιότυπου πορτοφολιού, επαληθεύει την υπογραφή της βεβαίωσης στιγμιότυπου πορτοφολιού χρησιμοποιώντας το δημόσιο κλειδί στο πιστοποιητικό υπογραφής που περιλαμβάνεται στην παράμετρο “x5c” της κεφαλίδας JOSE της βεβαίωσης στιγμιότυπου πορτοφολιού.

— TR-WIA-4.1: Ο εξυπηρετητής εξουσιοδότησης επαληθεύει επίσης ότι το εν λόγω πιστοποιητικό υπογραφής μπορεί να επαληθευτεί με άγκυρα από τον κατάλογο των παρόχων πορτοφολιών που αναφέρονται στο άρθρο 5 του εκτελεστικού κανονισμού (ΕΕ) 2024/2980, χρησιμοποιώντας ενδεχομένως ενδιάμεσα πιστοποιητικά που περιλαμβάνονται στην παράμετρο x5c.

— TR-WIA-4.2: Ο εξυπηρετητής εξουσιοδότησης επαληθεύει ότι δεν έχει λήξει η βεβαίωση στιγμιότυπου πορτοφολιού.

— TR-WIA-4.3: Ο εξυπηρετητής εξουσιοδότησης επαληθεύει την υπογραφή της PoP βάσει του δημόσιου κλειδιού που εμφανίζεται στη δήλωση “cnf”.

— TR_KA-1: Η μονάδα πορτοφολιού χρησιμοποιεί βεβαίωση κλειδιού κατά την έκδοση δεδομένων ταυτοποίησης προσώπου και κατά την έκδοση εγκεκριμένων ή μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που συνδέονται με συγκεκριμένη διάταξη ή ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή.

— TR_KA-1.1: Η μονάδα πορτοφολιού δεν χρησιμοποιεί βεβαίωση κλειδιού κατά την έκδοση εγκεκριμένων ή μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που δεν συνδέονται με συγκεκριμένη διάταξη ή ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή.

— TR_KA-2: Ο πάροχος πορτοφολιού παρέχει μονάδα πορτοφολιού με διαφορετικές βεβαιώσεις κλειδιού για την WSCD της μονάδας πορτοφολιού και για καθέναν από τους οικείους χώρους αποθήκευσης κλειδιών.

— TR_KA-2.1: Ο πάροχος πορτοφολιού υπογράφει ή σφραγίζει βεβαίωση κλειδιού, αφού ο πάροχος πορτοφολιού επαληθεύσει ότι τα κλειδιά που βεβαιώνονται στη βεβαίωση κλειδιού είναι αποθηκευμένα στην WSCD της μονάδας πορτοφολιού ή στον χώρο αποθήκευσης κλειδιών που περιγράφεται στη βεβαίωση κλειδιού.

— TR_KA-2.2: Η βεβαίωση κλειδιού περιέχει τουλάχιστον ένα βεβαιωμένο δημόσιο κλειδί. Ο αριθμός κλειδιών της βεβαίωσης κλειδιού που αποστέλλεται σε εκδότη διαπιστευτηρίων δεν θα πρέπει να υπερβαίνει το μέγιστο μέγεθος παρτίδας που ορίζει ο εκδότης διαπιστευτηρίων στα οικεία μεταδεδομένα εκδότη διαπιστευτηρίων· βλ. ETSI TS 119 472-3 ([3]), παράμετρο “credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size”.

— TR_KA-2.3: Ο πάροχος πορτοφολιού συμπεριλαμβάνει δημόσιο κλειδί (το οποίο αντιστοιχεί σε ιδιωτικό κλειδί που είναι αποθηκευμένο στην WSCD ή στον χώρο αποθήκευσης κλειδιών της μονάδας πορτοφολιού) σε μία το πολύ βεβαίωση κλειδιού.

— TR_KA-2.4: Η μονάδα πορτοφολιού χρησιμοποιεί βεβαίωση κλειδιού κατά τη διάρκεια μίας το πολύ διαδικασίας έκδοσης ή επανέκδοσης διαπιστευτηρίων.

— TR_KA-2.5: Ο πάροχος πορτοφολιού διασφαλίζει ότι η μονάδα πορτοφολιού διαθέτει βεβαιώσεις κλειδιού, όπως απαιτείται για την έκδοση δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που συνδέονται με συγκεκριμένη διάταξη.

([3]) ETSI, “Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Ψηφιακές υπογραφές JAdES· Μέρος 3: Επίπεδα και βασικά προφίλ JAdES”, ETSI TS 119 472-3, V1.1.1, Μάρτιος 2026.

— TR_KA-3: Όταν κρίνεται αναγκαίο κατά την έκδοση, η μονάδα πορτοφολιού περιλαμβάνει βεβαίωση κλειδιού στο πεδίο “proofs” αιτήματος διαπιστευτηρίων που υποβάλλεται στον εκδότη διαπιστευτηρίων, όπως ορίζεται στο OID4VCI, σε μορφή απόδειξης είτε τύπου “jwt” είτε τύπου “attestation”.

— TR_KA_3.1: Όταν η μονάδα πορτοφολιού περιλαμβάνει βεβαίωση κλειδιού σε μορφή στοιχείου “jwt”, υπογράφει ή σφραγίζει τη βεβαίωση κλειδιού με τη χρήση του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί με δείκτη 0 από τον πίνακα “attested_keys” εντός του αντικειμένου “key_attestation”.

— TR_KA-4: Όταν ο εκδότης διαπιστευτηρίων εκδίδει διαπιστευτήρια που συνδέονται με συγκεκριμένη διάταξη, αναφέρει στην παράμετρο “proof_types_supported” των οικείων μεταδεδομένων εκδότη διαπιστευτηρίων — όπως ορίζεται στο σημείο 12.2.4 του OID4VCI— ότι υποστηρίζει αμφότερους τους τύπους απόδειξης “jwt” και “attestation” για τις βεβαιώσεις κλειδιού που περιλαμβάνουν το αντικείμενο “key_attestation_required”.

— TR_KA-4.1: Όταν ο εκδότης διαπιστευτηρίων εκδίδει διαπιστευτήρια που δεν συνδέονται με συγκεκριμένη διάταξη, παραλείπει τις παραμέτρους “proof_types_supported” και “cryptographic_binding_methods_supported” στα μεταδεδομένα εκδότη διαπιστευτηρίων.

— TR_KA-5: Όταν ο εκδότης διαπιστευτηρίων λαμβάνει βεβαίωση κλειδιού σε μορφή απόδειξης τύπου “jwt” ή “attestation”, επαληθεύει, αφενός, την υπογραφή της βεβαίωσης κλειδιού βάσει του δημόσιου κλειδιού στο πιστοποιητικό υπογραφής που περιλαμβάνεται στην παράμετρο “x5c” της κεφαλίδας JOSE της βεβαίωσης κλειδιού και, αφετέρου, ότι το εν λόγω πιστοποιητικό υπογραφής μπορεί να επαληθευτεί με άγκυρα εμπιστοσύνης από τον κατάλογο παρόχων πορτοφολιών που αναφέρεται στο άρθρο 5 του εκτελεστικού κανονισμού (ΕΕ) 2024/2980, ενδεχομένως με τη χρήση ενδιάμεσων πιστοποιητικών που περιλαμβάνονται στην παράμετρο “x5c”.

— TR_KA-6: Όταν ο εκδότης διαπιστευτηρίων λαμβάνει βεβαίωση κλειδιού σε μορφή απόδειξης τύπου “jwt”, επαληθεύει την υπογραφή του στοιχείου “jwt” βάσει του κλειδιού με δείκτη 0 από τον πίνακα “attested_keys” εντός του αντικειμένου “key_attestation” που περιλαμβάνεται στο στοιχείο “jwt”.

— TR_KA-6.1: Ο εκδότης διαπιστευτηρίων επαληθεύει ότι το πεδίο “nonce” του στοιχείου “jwt” περιλαμβάνει έγκυρο c_nonce από το οικείο nonce_endpoint, όπως ορίζεται στο OID4VC.

— TR_KA-7: Όταν ο εκδότης διαπιστευτηρίων λαμβάνει βεβαίωση κλειδιού σε μορφή απόδειξης τύπου “attestation”, επαληθεύει ότι το αντικείμενο “key_attestation” περιλαμβάνει έγκυρο c_nonce από το οικείο nonce_endpoint.

— TR_KA-8: Ο πάροχος δεδομένων ταυτοποίησης προσώπου διασφαλίζει ότι τα δεδομένα ταυτοποίησης προσώπου συνδέονται με δημόσιο κλειδί που προέρχεται από βεβαίωση κλειδιού στην οποία αναφέρεται WSCD.

γ) Απαιτήσεις περιεχομένου

— C_WIA-1: Στη βεβαίωση στιγμιότυπου πορτοφολιού περιλαμβάνονται τα ακόλουθα:

— Η δήλωση “wallet_name” που ορίζεται στο προσάρτημα Ε του OID4VCI, όπου η τιμή της είναι το αναγνωριστικό της υλοποίησης πορτοφολιού που είναι διαθέσιμο στον κατάλογο των παρόχων πορτοφολιών που αναφέρονται στο άρθρο 5 του εκτελεστικού κανονισμού (ΕΕ) 2024/2980.

— Δήλωση “wallet_version” ([4]), που αποτελεί συμβολοσειρά της οποίας η τιμή είναι η έκδοση της υλοποίησης πορτοφολιού.

— Δήλωση “wallet_solution_certification_information”, που είναι αντικείμενο JSON το οποίο περιέχει πληροφορίες σχετικά με τον οργανισμό αξιολόγησης της συμμόρφωσης που πιστοποίησε την υλοποίηση πορτοφολιού, τον αριθμό πιστοποίησης, κατά περίπτωση, και άλλα σχετικά στοιχεία όσον αφορά την πιστοποίηση.

([4]) Η δήλωση αυτή ορίζεται στο παρόν CIR, διότι δεν αποτελεί μέρος της προδιαγραφής OID4VCI.

— Δήλωση “client_status”, που περιλαμβάνει δύο υποπεδία:

— “status”: αναφορά καταλόγου καθεστώτος, όπως ορίζεται στο προσάρτημα Ε του OID4VCI, που αντιπροσωπεύει το καθεστώς ανάκλησης του στιγμιότυπου πορτοφολιού. Για λεπτομέρειες, βλ. στοιχείο ε) κατωτέρω,

— “exp”: NumericDate, όπως ορίζεται στο RFC 7519, που καθορίζει το χρονικό διάστημα κατά το οποίο ο πάροχος πορτοφολιού θα τηρήσει το καθεστώς ανάκλησης στον δείκτη καταλόγου καθεστώτος που αναφέρεται στο “status”.

— Δήλωση “exp” που ορίζεται στο προσάρτημα Ε του OID4VCI.

— *ΣΗΜΕΙΩΣΗ*: Η δήλωση “client_status.status” σε βεβαίωση στιγμιότυπου πορτοφολιού αντιπροσωπεύει το καθεστώς ανάκλησης του στιγμιότυπου πορτοφολιού και όχι το καθεστώς ανάκλησης της ίδιας της βεβαίωσης. Όπως περιγράφεται στο R_WIA-1 κατωτέρω, ο πάροχος πορτοφολιού μπορεί να αποφασίσει να εξετάσει κάθε βεβαίωση στιγμιότυπου πορτοφολιού σε συγκεκριμένο εξυπηρετητή εξουσιοδότησης με βάση το γεγονός ότι όλες οι βεβαιώσεις που απεστάλησαν στον εν λόγω εξυπηρετητή περιέχουν την ίδια τιμή δείκτη στην καταχώριση “client_status.status”.

— *ΣΗΜΕΙΩΣΗ*: Η τιμή “idx” στη δήλωση “status” μπορεί να χρησιμοποιηθεί ως (κατά ζεύγη) μοναδικό αναγνωριστικό του στιγμιότυπου πορτοφολιού και της μονάδας πορτοφολιού.

— C_WIA-2: Η βεβαίωση στιγμιότυπου πορτοφολιού θα πρέπει επίσης να περιλαμβάνει τη δήλωση “wallet_link” που ορίζεται στο προσάρτημα Ε του OID4VCI και η τιμή της δήλωσης αυτής είναι ένα URI από το οποίο μπορούν να ληφθούν περαιτέρω πληροφορίες σχετικά με την υλοποίηση πορτοφολιού.

— C_WIA-3: Ο εξυπηρετητής εξουσιοδότησης δεν ερμηνεύει την παράμετρο “exp” στο ανώτατο επίπεδο της βεβαίωσης στιγμιότυπου πορτοφολιού ως λήξη της περιόδου τήρησης της ανάκλησης του στιγμιότυπου πορτοφολιού.

— *ΣΗΜΕΙΩΣΗ*: Η παράμετρος “exp” στο ανώτατο επίπεδο βεβαίωσης στιγμιότυπου πορτοφολιού σημαίνει τη λήξη ισχύος της ίδιας της βεβαίωσης.

— C_KA-1: Στη βεβαίωση κλειδιού περιλαμβάνονται τα εξής:

— Οι δηλώσεις “key_storage” και “user_authentication” που ορίζονται στο προσάρτημα Δ του OID4VCI.

— Τα χαρακτηριστικά “key_storage” και “user_authentication” έχουν την τιμή “iso_18045_high” όταν στη βεβαίωση κλειδιού αναφέρεται WSCD.

— Η δήλωση “certification” η οποία ορίζεται στο προσάρτημα Δ του OID4VCI, που περιλαμβάνει διεύθυνση URL από όπου μπορούν να αντληθούν πληροφορίες σχετικά με την πιστοποίηση που έχει επιτευχθεί από την WSCD ή τον χώρο αποθήκευσης κλειδιών, ενδεικτικά το σύστημα όπως το Common Criteria ή το GlobalPlatform, οι αξιολογούμενες απαιτήσεις, όπως το εφαρμοστέο προφίλ προστασίας, και το επίπεδο αξιολόγησης.

— Από τις πληροφορίες αυτές είναι δυνατόν να προσδιοριστεί αν η αποθήκευση κλειδιών αποτελεί WSCD.

— Δήλωση “key_storage_status”, που περιλαμβάνει δύο υποπεδία:

— “status”: αναφορά καταλόγου καθεστώτος, όπως ορίζεται στο προσάρτημα Δ.1 του OID4VCI. Η τιμή αντιπροσωπεύει είτε το καθεστώς ανάκλησης του τύπου WSCD ή χώρου αποθήκευσης κλειδιών που χρησιμοποιείται για την αποθήκευση των βεβαιωμένων κλειδιών είτε —βάσει της επιλογής του δείκτη per-key-attestation— το καθεστώς ανάκλησης WSCD ή χώρου αποθήκευσης κλειδιών μεμονωμένης μονάδας πορτοφολιού. Για τις διαθέσιμες επιλογές απόδοσης δείκτη, βλ. R_KA_1 κατωτέρω,

— “exp”: NumericDate, όπως ορίζεται στο RFC 7519, που καθορίζει το χρονικό διάστημα κατά το οποίο ο πάροχος πορτοφολιού θα τηρήσει το καθεστώς ανάκλησης στον δείκτη καταλόγου καθεστώτος που αναφέρεται στο “status”.

— Δήλωση “exp” που ορίζεται στο προσάρτημα Δ του OID4VCI.

— *ΣΗΜΕΙΩΣΗ* σχετικά με την τιμή “idx” στη δήλωση “key_storage_status.status” που περιλαμβάνεται σε βεβαίωση κλειδιού: Όταν ο πάροχος πορτοφολιού χρησιμοποιεί την επιλογή “type-shared index” (βλ. R_KA_1 κατωτέρω), όλες οι βεβαιώσεις κλειδιού για τον ίδιο τύπο WSCD ή χώρου αποθήκευσης κλειδιών μοιράζονται τον ίδιο δείκτη καταλόγου καθεστώτος. Επομένως, η τιμή “idx” δεν είναι μοναδική ανά μονάδα πορτοφολιού. Αντιθέτως, όταν ο πάροχος πορτοφολιού χρησιμοποιεί την επιλογή “per-key-attestation index”, η τιμή “idx” είναι μοναδική για τη μονάδα πορτοφολιού (ή κατά ζεύγη μοναδική ανά εκδότη διαπιστευτηρίων). Σε κάθε περίπτωση, ωστόσο, ο εκδότης διαπιστευτηρίων δεν χρησιμοποιεί την τιμή “idx” σε βεβαίωση κλειδιού ως αναγνωριστικό μονάδας πορτοφολιού, αλλά χρησιμοποιεί την τιμή “idx” σε βεβαίωση στιγμιότυπου πορτοφολιού.

— C_KA-2: Όταν η βεβαίωση κλειδιού αποστέλλεται σε μορφή απόδειξης τύπου “attestation”, περιλαμβάνει επίσης έγκυρο c_nonce, όπως ορίζεται στο προσάρτημα ΣΤ.3 του OID4VCI.

— C_KA-3: Ο εκδότης διαπιστευτηρίων δεν ερμηνεύει την παράμετρο “exp” στο ανώτατο επίπεδο της βεβαίωσης κλειδιού ως λήξη της περιόδου τήρησης της ανάκλησης της WSCD ή του χώρου αποθήκευσης κλειδιών.

— *ΣΗΜΕΙΩΣΗ*: Η παράμετρος “exp” στο ανώτατο επίπεδο βεβαίωσης κλειδιού σημαίνει τη λήξη ισχύος της ίδιας της βεβαίωσης κλειδιού.

δ) Απαιτήσεις κύκλου ζωής

— Στο παρόν παράρτημα ορίζονται οι ακόλουθες παράμετροι μεταδεδομένων εκδότη διαπιστευτηρίων:

— “preferred_client_status_period”: OPTIONAL. Ακέραιος αριθμός ο οποίος ορίζει την προτιμώμενη εναπομένουσα περίοδο τήρησης του καθεστώτος της βεβαίωσης στιγμιότυπου πορτοφολιού που πρέπει να προσκομίσει η μονάδα πορτοφολιού κατά την έκδοση, σε δευτερόλεπτα. Η εναπομένουσα περίοδος τήρησης του καθεστώτος ορίζεται ως η τιμή “client_status.exp” στη βεβαίωση μείον τον χρόνο παραλαβής της βεβαίωσης.

— “preferred_key_storage_status_period”: OPTIONAL. Ακέραιος αριθμός ο οποίος ορίζει την προτιμώμενη εναπομένουσα περίοδο τήρησης του καθεστώτος της βεβαίωσης κλειδιού που πρέπει να προσκομίσει η μονάδα πορτοφολιού κατά την έκδοση, σε δευτερόλεπτα. Η εναπομένουσα περίοδος τήρησης του καθεστώτος ορίζεται ως η τιμή “key_storage_status.exp” στη βεβαίωση μείον τον χρόνο παραλαβής της βεβαίωσης.

— LC_WIA-1: Ο εξυπηρετητής εξουσιοδότησης μπορεί να κοινοποιεί τις προτιμήσεις του για την εναπομένουσα περίοδο τήρησης του καθεστώτος στις βεβαιώσεις στιγμιότυπου πορτοφολιού, συμπεριλαμβάνοντας την παράμετρο μεταδεδομένων “key_storage_status.exp” στο οικείο τελικό σημείο μεταδεδομένων εκδότη διαπιστευτηρίων, όπως ορίζεται στο σημείο 12.2.2 του OID4VCI.

— LC_WIA-1.1: Το πεδίο αυτό τοποθετείται στο ανώτατο επίπεδο των μεταδεδομένων εκδότη διαπιστευτηρίων.

— LC_WIA_2: Ο εξυπηρετητής εξουσιοδότησης δεν ερμηνεύει την παράμετρο “exp” στο ανώτατο επίπεδο της βεβαίωσης στιγμιότυπου πορτοφολιού ως λήξη της περιόδου τήρησης της ανάκλησης του στιγμιότυπου πορτοφολιού.

— LC_WIA_3: Όταν ο πάροχος πορτοφολιού υπογράφει ή σφραγίζει βεβαίωση στιγμιότυπου πορτοφολιού, τηρεί το καθεστώς ανάκλησης του σχετικού στιγμιότυπου πορτοφολιού έως ότου παρέλθει ο χρόνος “wallet_instance_status.exp” που αναφέρεται στην εν λόγω βεβαίωση στιγμιότυπου πορτοφολιού.

— LC_KA-1: Όταν απαιτείται βεβαίωση κλειδιού, ο εκδότης διαπιστευτηρίων μπορεί να κοινοποιεί τις προτιμήσεις του για την εναπομένουσα περίοδο τήρησης του καθεστώτος στις βεβαιώσεις κλειδιού, συμπεριλαμβάνοντας την παράμετρο μεταδεδομένων “preferred_key_storage_status_period” που αναφέρεται ανωτέρω στο οικείο τελικό σημείο μεταδεδομένων εκδότη διαπιστευτηρίων, όπως ορίζεται στο σημείο 12.2.2 του OID4VCI.

— LC_KA-1.1: Το πεδίο αυτό τοποθετείται εντός του αντικειμένου “key_attestations_required”, όπως ορίζεται στο σημείο 12.2.4 του OID4VCI.

— LC_KA-2: Ο πάροχος πορτοφολιού επιλέγει την περίοδο τεχνικής ισχύος των βεβαιώσεων κλειδιού που εκδίδει.

— LC_KA-3: Όταν ο πάροχος πορτοφολιού υπογράφει ή σφραγίζει βεβαίωση κλειδιού, τηρεί το καθεστώς ανάκλησης της σχετικής WSCD ή του σχετικού χώρου αποθήκευσης κλειδιών έως ότου παρέλθει ο χρόνος “key_storage_status.exp” που αναφέρεται στην εν λόγω βεβαίωση κλειδιού.

— LC_GEN-1: Ο πάροχος πορτοφολιού διασφαλίζει ότι η μονάδα πορτοφολιού μπορεί πάντοτε να προσκομίζει βεβαιώσεις μονάδας πορτοφολιού και βεβαιώσεις κλειδιού των οποίων οι τιμές “client_status.exp” και “key_storage_status.exp” (αντίστοιχα) είναι τουλάχιστον 31 ημέρες στο μέλλον κατά τον χρόνο προσκόμισης σε εξυπηρετητή εξουσιοδότησης ή σε εκδότη διαπιστευτηρίων.

— *ΣΗΜΕΙΩΣΗ*: Αυτό εγγυάται ότι οι πάροχοι δεδομένων ταυτοποίησης προσώπου μπορούν να βασίζονται σε αλυσιδωτές ανακλήσεις, χωρίς να αναγκάζονται να εκδίδουν δεδομένα ταυτοποίησης προσώπου βραχείας διάρκειας.

— LC_GEN-2: Ο πάροχος πορτοφολιού διασφαλίζει ότι η μονάδα πορτοφολιού παραλαμβάνει τα μεταδεδομένα εκδότη διαπιστευτηρίων κατά την έκδοση.

  — LC_GEN_2.1: Εάν στα μεταδεδομένα αυτά περιλαμβάνεται πεδίο “preferred_key_storage_status_period”, τότε η μονάδα πορτοφολιού αποστέλλει βεβαίωση κλειδιού με τιμή (“key_storage_status.exp” − τρέχουσα ώρα) − “preferred_key_storage_status_period” όσο το δυνατόν μικρότερη, αλλά όχι αρνητική. Εάν η μονάδα πορτοφολιού δεν διαθέτει τέτοια βεβαίωση κλειδιού, λαμβάνει από τον πάροχο πορτοφολιού νέα βεβαίωση κλειδιού, η οποία πληροί τον όρο “key_storage_status.exp” − τρέχουσα ώρα ≥ “preferred_key_storage_status_period”.

  — LC_GEN_2.2: Εάν στα μεταδεδομένα αυτά περιλαμβάνεται πεδίο “preferred_client_status_period”, τότε η μονάδα πορτοφολιού αποστέλλει βεβαίωση στιγμιότυπου πορτοφολιού με τιμή (“client_status.exp” − τρέχουσα ώρα) − “preferred_client_status_period” όσο το δυνατόν μικρότερη, αλλά όχι αρνητική. Εάν η μονάδα πορτοφολιού δεν διαθέτει τέτοια βεβαίωση στιγμιότυπου πορτοφολιού, ζητεί από τον πάροχο πορτοφολιού νέα βεβαίωση στιγμιότυπου πορτοφολιού, η οποία πληροί τον όρο “client_status.exp” − τρέχουσα ώρα ≥ “preferred_client_status_period”.

— LC_GEN-3: Η περίοδος τεχνικής ισχύος των δεδομένων ταυτοποίησης προσώπου λήγει πριν από την αποστολή του “client_status.exp” της βεβαίωσης στιγμιότυπου πορτοφολιού και του “key_storage_status.exp” της βεβαίωσης κλειδιού στον πάροχο δεδομένων ταυτοποίησης προσώπου κατά την έκδοση.

— LC_GEN-4: Ο πάροχος δεδομένων ταυτοποίησης προσώπου που διαθέτει περίοδο τεχνικής ισχύος άνω των 24 ωρών ελέγχει το καθεστώς ανάκλησης τόσο της βεβαίωσης στιγμιότυπου πορτοφολιού όσο και της βεβαίωσης κλειδιού που ελήφθησαν κατά την έκδοση τουλάχιστον μία φορά κάθε 24 ώρες, κατά τη διάρκεια της περιόδου τεχνικής ισχύος των δεδομένων ταυτοποίησης προσώπου. Σε περίπτωση ανάκλησης μίας εκ των δύο, ο πάροχος ανακαλεί τα δεδομένα ταυτοποίησης προσώπου.

ε) Απαιτήσεις ανάκλησης

— R_GEN-1: Ο πάροχος πορτοφολιού χρησιμοποιεί τους καταλόγους καθεστώτος αδειοδοτικού (που ορίζονται στον κατάλογο καθεστώτος αδειοδοτικού της IETF) ως μηχανισμό ανάκλησης τόσο για τις βεβαιώσεις κλειδιού όσο και για τις βεβαιώσεις στιγμιότυπου πορτοφολιού, όπως ορίζεται στα προσαρτήματα Δ και Ε του OID4VCI, αντίστοιχα.

— *ΣΗΜΕΙΩΣΗ*: Για τη βελτίωση της κλιμακοθετησιμότητας των καταλόγων καθεστώτος, ο πάροχος πορτοφολιών μπορεί να χρησιμοποιεί τις ακόλουθες βελτιστοποιήσεις:

  — Διαίρεση του καταλόγου καθεστώτος σε πολλαπλά τμήματα, όταν οι πάροχοι πορτοφολιών έχουν σημαντικό αριθμό χρηστών και εκδοθεισών βεβαιώσεων. Υπάρχουν πολλές στρατηγικές διαίρεσης σε τμήματα, π.χ. βάσει καθορισμένου μεγέθους ή κατά χρονική περίοδο. Η επιλογή της στρατηγικής διαίρεσης σε τμήματα επαφίεται στη διακριτική ευχέρεια του παρόχου πορτοφολιών. Σχετικές παράμετροι μπορούν να περιλαμβάνουν το μέγεθος ενός καταλόγου καθεστώτος για τηλεφόρτωση και την προστασία της ιδιωτικής ζωής του χρήστη.

  — Ύπαρξη πολλαπλών καταλόγων καθεστώτος.

  — Συμπίεση καταλόγου καθεστώτος με σκοπό τη μείωση του μεγέθους του.

— R_WIA-1: Ο πάροχος πορτοφολιού μπορεί να αποδίδει την ίδια τιμή στη δήλωση “idx” που περιλαμβάνεται στη δήλωση “client_status.status” σε όλες τις βεβαιώσεις στιγμιότυπου πορτοφολιού που προσκομίζει μια συγκεκριμένη μονάδα πορτοφολιού στον ίδιο εξυπηρετητή εξουσιοδότησης. Αυτό ονομάζεται επιλογή “per-issuer reuse”. Εάν γίνεται χρήση της συγκεκριμένης επιλογής:

  — R_WIA-1.1: Η μονάδα πορτοφολιού τηρεί το καθεστώς της τιμής δείκτη που χρησιμοποίησε για κάθε εξυπηρετητή εξουσιοδότησης με τον οποίο έχει αλληλεπιδράσει προηγουμένως και ζητεί βεβαίωση στιγμιότυπου πορτοφολιού που περιέχει την ίδια τιμή δείκτη όταν αλληλεπιδρά εκ νέου με τον ίδιο εξυπηρετητή εξουσιοδότησης.

  — R_WIA-1.2: Όταν ο πάροχος πορτοφολιού λαμβάνει αίτημα βεβαίωσης στιγμιότυπου πορτοφολιού που περιέχει συγκεκριμένη τιμή δείκτη, επαληθεύει ότι η αιτούσα μονάδα πορτοφολιού έχει λάβει προηγουμένως την εν λόγω τιμή δείκτη, πριν από την έκδοση νέας βεβαίωσης στιγμιότυπου πορτοφολιού με την εν λόγω τιμή δείκτη.

  — R_WIA-1.3: Η μονάδα πορτοφολιού δεν επαναχρησιμοποιεί την ίδια τιμή δείκτη για αλληλεπιδράσεις με διαφορετικούς εξυπηρετητές εξουσιοδότησης.

— *ΣΗΜΕΙΩΣΗ*: Εάν γίνεται χρήση της επιλογής “per-issuer reuse”, ο πάροχος πορτοφολιού θα έχει τη δυνατότητα να καθορίσει τον αριθμό των εξυπηρετητών εξουσιοδότησης με τους οποίους έχει αλληλεπιδράσει μια μονάδα πορτοφολιού, καθώς και τη συχνότητα αλληλεπίδρασής της με καθέναν από αυτούς.

— R_WIA-2: Στο πλαίσιο της οικείας πολιτικής για την προστασία της ιδιωτικής ζωής, ο πάροχος πορτοφολιού τεκμηριώνει αν κάνει χρήση της επιλογής “per-issuer reuse” για την ανάκληση στιγμιότυπου πορτοφολιού.

— R_WIA-3: Εάν ο πάροχος πορτοφολιού δεν κάνει χρήση της επιλογής “per-issuer reuse”, αποδίδει σε κάθε βεβαίωση στιγμιότυπου πορτοφολιού που εκδίδει νέα τιμή δείκτη, χωρίς δυνατότητα σύνδεσης.

— R_WIA-4: Όταν μια μονάδα πορτοφολιού πρέπει να ανακληθεί, ο πάροχος πορτοφολιού ανακαλεί τις τιμές δείκτη της δήλωσης “client_status.status” σε όλες τις βεβαιώσεις στιγμιότυπου πορτοφολιού που συνδέονται με την εν λόγω μονάδα πορτοφολιού.

— R_WIA-5: Ο πάροχος πορτοφολιού λαμβάνει υπόψη την κλίμακα εφαρμογής του και την υποκείμενη αρχιτεκτονική κατά τον καθορισμό του μεγέθους των οικείων καταλόγων καθεστώτος βεβαίωσης στιγμιότυπου πορτοφολιού, ώστε να διασφαλίζεται ότι οι εν λόγω κατάλογοι είναι αρκετά μεγάλοι για την αποτροπή συσχέτισης και την προστασία της ιδιωτικής ζωής του χρήστη. Κατ’ ελάχιστον, ο κατάλογος καθεστώτος πρέπει να αφορά, όπου είναι δυνατόν, τουλάχιστον 10 000 βεβαιώσεις.

— R_KA_1: Ο πάροχος πορτοφολιού κάνει χρήση μίας από τις ακόλουθες επιλογές απόδοσης δείκτη για τη δήλωση “key_storage_status.status” σε βεβαίωση κλειδιού:

  — Επιλογή 1, με την ονομασία “type-shared index”, στο πλαίσιο της οποίας όλες οι βεβαιώσεις κλειδιού που βεβαιώνουν κλειδιά που είναι αποθηκευμένα στον ίδιο τύπο WSCD ή χώρου αποθήκευσης κλειδιών περιλαμβάνουν την ίδια τιμή δείκτη στο “key_storage_status.status”.

  — Επιλογή 2, με την ονομασία “per-key-attestion index”, στο πλαίσιο της οποίας μια βεβαίωση κλειδιού που βεβαιώνει κλειδιά που είναι αποθηκευμένα σε μεμονωμένη WSCD ή σε μεμονωμένο χώρο αποθήκευσης κλειδιών περιλαμβάνει (κατά ζεύγη) μοναδική τιμή δείκτη στο “key_storage_status.status”.

— *ΣΗΜΕΙΩΣΗ*: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 1, μια ενιαία πράξη ανάκλησης ακυρώνει όλες τις βεβαιώσεις κλειδιού του επηρεαζόμενου τύπου σε όλες τις μονάδες πορτοφολιού. Επιπλέον, δεδομένου ότι όλες οι βεβαιώσεις κλειδιού για τον ίδιο τύπο WSCD ή χώρου αποθήκευσης κλειδιών μοιράζονται ενιαίο δείκτη καταλόγου καθεστώτος, ο αριθμός των καταχωρίσεων σε κατάλογο καθεστώτος βεβαίωσης κλειδιών αντικατοπτρίζει τον αριθμό των τύπων WSCD ή χώρου αποθήκευσης κλειδιών που υποστηρίζει ο πάροχος πορτοφολιού, και όχι τον αριθμό των χρησιμοποιούμενων μονάδων πορτοφολιού. Συνεπώς, οι παράμετροι προστασίας της ιδιωτικής ζωής που αιτιολογούν το ελάχιστο μέγεθος καταλόγου καθεστώτος για τους καταλόγους καθεστώτος στιγμιότυπου πορτοφολιού δεν ισχύουν για τους καταλόγους καθεστώτος βεβαίωσης κλειδιού βάσει της επιλογής 1, υπό την προϋπόθεση ότι υπάρχει αρκετά μεγάλος αριθμός μονάδων πορτοφολιού που χρησιμοποιούν τον ίδιο τύπο WSCD ή χώρου αποθήκευσης κλειδιών.

— *ΣΗΜΕΙΩΣΗ*: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 2, κάθε δείκτης αντιπροσωπεύει το καθεστώς ανάκλησης της συγκεκριμένης WSCD ή του συγκεκριμένου χώρου αποθήκευσης κλειδιών που βεβαιώνεται στην εν λόγω βεβαίωση κλειδιού.

— *ΣΗΜΕΙΩΣΗ*: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 2, η ανάκληση συγκεκριμένης WSCD ή συγκεκριμένου χώρου αποθήκευσης κλειδιών είναι επίσης δυνατή κατόπιν αιτήματος του χρήστη.

— R_KA-2: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 2, μπορεί προαιρετικά να κάνει χρήση της επιλογής “per-issuer reuse” που περιγράφεται στο R_WIA-1. Εάν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής αυτής, ισχύουν κατ’ αναλογία οι απαιτήσεις R_WIA-1 — R_WIA-3.

— R_KA-3: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 2, λαμβάνει υπόψη την κλίμακα εφαρμογής του και την υποκείμενη αρχιτεκτονική κατά τον καθορισμό του μεγέθους των οικείων καταλόγων καθεστώτος βεβαίωσης κλειδιού, ώστε να διασφαλίζεται ότι οι εν λόγω κατάλογοι είναι αρκετά μεγάλοι για την αποτροπή συσχέτισης και την προστασία της ιδιωτικής ζωής του χρήστη. Κατ’ ελάχιστον, ο κατάλογος καθεστώτος αφορά, όπου είναι δυνατόν, τουλάχιστον 10 000 βεβαιώσεις κλειδιού.

— R_KA-4: Όταν ο πάροχος πορτοφολιού κάνει χρήση της επιλογής 1 (“type-shared index”), ανακαλεί καταχώριση “key_storage_status.status” μόνο εάν ο τύπος WSCD ή χώρου αποθήκευσης κλειδιών παρουσιάζει ευπάθεια ασφάλειας.

στ) Απαιτήσεις σχετικά με τους αλγόριθμους υπογραφής

— SA-1: Για την υπογραφή βεβαιώσεων στιγμιότυπου πορτοφολιού, βεβαιώσεων κλειδιού, σχετικών καταλόγων απόδειξης κατοχής και καταλόγων καθεστώτος αδειοδοτικού, χρησιμοποιείται ένας από τους ακόλουθους αλγορίθμους:

  — ES256 (ECDSA με SHA-256 και P-256)

  — ES384 (ECDSA με SHA-384 και P-384)

  — ES512 (ECDSA με SHA-512 και P-521)

— SA-2: Ο πάροχος πορτοφολιού επιλέγει ποιον από τους αλγόριθμους που αναφέρονται στο SA-1 θα χρησιμοποιήσει.

— SA-3: Ο εξυπηρετητής εξουσιοδότησης ή ο εκδότης διαπιστευτηρίων (όπως ορίζεται στο OID4VCI) υποστηρίζει όλους τους αλγόριθμους που αναφέρονται στο SA-1.»

ΠΑΡΑΡΤΗΜΑ IV

«ΠΑΡΑΡΤΗΜΑ II

Κατάλογος προτύπων που αναφέρονται στο άρθρο 8

Ισχύουν οι τεχνικές προδιαγραφές που ορίζονται στα σημεία 2 έως 6 του ETSI TS 119 472-1 V1.2.1 (2026-02), οι οποίες διατυπώνονται με τις ακόλουθες προσαρμογές:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Ηλεκτρονικές υπογραφές και υποδομές (ESI)· Προφίλ πιστοποιητικών· Μέρος 1: Επισκόπηση και κοινές δομές δεδομένων".

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Ηλεκτρονικές υπογραφές και υποδομές εμπιστοσύνης (ESI)· Προφίλ πιστοποιητικών· Μέρος 6: Απαιτήσεις προφίλ πιστοποιητικών για τους παρόχους δεδομένων ταυτοποίησης προσώπου, πορτοφολιών, ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών από φορέα του δημόσιου τομέα υπεύθυνο για αυθεντική πηγή".

— [25] Κατάλογος καθεστώτος αδειοδοτικού της IETF (TSL), draft-ietf-oauth-status-list-20: "Κατάλογος καθεστώτος αδειοδοτικού", 20 Απριλίου 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: Όταν χρησιμοποιείται στοιχείο καθεστώτος για δεδομένα ταυτοποίησης προσώπου, εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών ή ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή, αναφέρει μόνο αν η βεβαίωση ανακαλείται ή όχι και δεν υποστηρίζει άλλες τιμές καθεστώτος, όπως η αναστολή.

— EAA-4.2.11.1-06.1: Όταν ανακαλείται βεβαίωση, η ανάκλησή της είναι μόνιμη.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Όταν εκδίδονται ηλεκτρονικές βεβαιώσεις χαρακτηριστικών βραχείας διάρκειας με περίοδο ισχύος 24 ωρών ή μικρότερη, δεν απαιτείται ανάκληση.

4) 4.6.3 Απαιτήσεις για την ηλεκτρονική βεβαίωση χαρακτηριστικών της ΕΕ εκδιδόμενη από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή (στο εξής: PuB-EAA)

— PuB-EAA-4.6.2-03: άκυρο.

— Pub-EAA-4.6.2-04: άκυρο.

— PuB-EAA-4.6.3-03: Η ψηφιακή υπογραφή PuB-EAA θα πρέπει να περιέχει το εγκεκριμένο πιστοποιητικό που υποστηρίζει την ψηφιακή υπογραφή PuB-EAA.

— PuB-EAA-4.6.3-04: Το εγκεκριμένο πιστοποιητικό που υποστηρίζει την ψηφιακή υπογραφή PuB-EAA πληροί τις απαιτήσεις του σημείου 8 του ETSI TS 119 412-6 v1.1.1 και περιέχει τη δήλωση QcType qcStatement, όπως ορίζεται στο ETSI EN 319 412-5 v2.5.1, με την τιμή id-etsi-qct-eidaspsbeaa να ορίζεται ως εξής:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Πιστοποιητικό που αναφέρεται στο άρθρο 45στ παράγραφος 1 στοιχείο β) το οποίο υποστηρίζει την εγκεκριμένη ηλεκτρονική υπογραφή ή την εγκεκριμένη ηλεκτρονική σφραγίδα του φορέα του δημόσιου τομέα που αναφέρεται στο άρθρο 3 σημείο 46) του κανονισμού (ΕΕ) αριθ. 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: άκυρο.

— EAA-5.2.10.1-05: άκυρο.

— EAA-5.2.10.1-06: Το μέλος καθεστώτος μπορεί να περιλαμβάνει το μέλος status_list, όπως ορίζεται στο σημείο 6.2 της IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: άκυρο.

— ΕΑΑ-5.2.10.1-08: άκυρο.

— ΕΑΑ-5.2.10.1-09: άκυρο.

— ΕΑΑ-5.2.10.1-10: άκυρο.

— ΕΑΑ-5.2.10.1-11: άκυρο.

— ΕΑΑ-5.2.10.1-12: άκυρο.

6) 6.2.10.1 General requirements

— ΕΑΑ-6.2.10.1-01: Όταν μια ηλεκτρονική βεβαίωση χαρακτηριστικών που συμμορφώνεται με τον μορφότυπο ISO/IEC mdoc χρησιμοποιεί τον μηχανισμό καταλόγου καθεστώτος βεβαίωσης, όπως ορίζεται στο ΕΑΑ-6.2.10.1-02.2, ή τον μηχανισμό καταλόγου ανάκλησης βεβαίωσης, όπως ορίζεται στο ΕΑΑ-6.2.10.1-02.3, το οικείο αντικείμενο κινητής ασφάλειας (στο εξής: MSO) περιέχει τη δομή καθεστώτος, όπως ορίζεται στο πρότυπο ΕΑΑ-6.2.10.1-17, που περιλαμβάνει πληροφορίες ανάκλησης MSO.

— ΕΑΑ-6.2.10.1-01.1: Κατά την εφαρμογή του μηχανισμού καταλόγου αναγνωριστικών, το στοιχείο καθεστώτος περιλαμβάνει το στοιχείο identifier_list, όπως ορίζεται στο ΕΑΑ-6.2.10.1-11.

— ΕΑΑ-6.2.10.1-01.2: Κατά την εφαρμογή του μηχανισμού καταλόγου καθεστώτος, το στοιχείο καθεστώτος περιλαμβάνει το στοιχείο status_list, όπως ορίζεται στο ΕΑΑ-6.2.10.1-13.

— *ΣΗΜΕΙΩΣΗ*:

  — Η δομή καθεστώτος περιλαμβάνει παραπομπή σε κατάλογο ανάκλησης MSO.

  — Ο κατάλογος ανάκλησης MSO είναι δομή COSE_Sign1, η οποία δηλώνει αν συγκεκριμένο MSO ανακαλείται ή όχι.

  — Η δομή καθεστώτος περιλαμβάνει όλες τις αναγκαίες πληροφορίες ώστε το βασιζόμενο σε πορτοφόλι μέρος να μπορεί να διαπιστώσει αν ο κατάλογος ανάκλησης MSO είναι αυθεντικός.

— ΕΑΑ-6.2.10.1-02: Ο πάροχος δεδομένων ταυτοποίησης προσώπου, ο πάροχος εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή ο πάροχος ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή χρησιμοποιεί μία από τις ακόλουθες μεθόδους για την ανάκληση δεδομένων ταυτοποίησης προσώπου, εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή.

— ΕΑΑ-6.2.10.1-02.1: Εάν εκδίδουν ηλεκτρονικές βεβαιώσεις χαρακτηριστικών βραχείας διάρκειας με περίοδο ισχύος ίση ή μικρότερη των 24 ωρών, τότε δεν απαιτείται ανάκληση.

— ΕΑΑ-6.2.10.1-02.2: Χρήση μηχανισμού καταλόγου καθεστώτος βεβαίωσης για την κωδικοποίηση των πληροφοριών ανάκλησης ως καταλόγου καθεστώτος.

— ΕΑΑ-6.2.10.1-02.2.1: Ο μηχανισμός καταλόγου καθεστώτος ανακαλεί MSO με βάση το αν το δυφίο της θέσης δυφίου που ορίζεται από τον εκδότη στο MSO είναι αληθές στον κατάλογο καθεστώτος.

— ΕΑΑ-6.2.10.1-02.2.2: Ο μηχανισμός καταλόγου καθεστώτος ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού (draft-ietf-oauth-status-list-20).

— ΕΑΑ-6.2.10.1-02.3: Χρήση μηχανισμού καταλόγου ανάκλησης βεβαίωσης για την κωδικοποίηση των πληροφοριών ανάκλησης ως καταλόγου αναγνωριστικών.

— ΕΑΑ-6.2.10.1-02.3.1: Ο μηχανισμός καταλόγου αναγνωριστικών ανακαλεί MSO με βάση το αν το αναγνωριστικό που ορίζεται από τον εκδότη στο MSO εμφανίζεται στον κατάλογο αναγνωριστικών.

— EAA-6.2.10.1-02.3.2: Τα EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 και EAA-6.2.10.1-11 ορίζουν τον μηχανισμό καταλόγου αναγνωριστικών, βάσει των απαιτήσεων από την προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού που περιλαμβάνουν την ομοιότητα μεταξύ του μηχανισμού καταλόγου καθεστώτος και του μηχανισμού καταλόγου αναγνωριστικών.

— EAA-6.2.10.1-03: Όταν χρησιμοποιείται στοιχείο καθεστώτος για δεδομένα ταυτοποίησης προσώπου, εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών ή ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή, χρησιμοποιείται αποκλειστικά το καθεστώς “ανακληθέν”.

— EAA-6.2.10.1-03.1: Για κατάλογο καθεστώτος, αυτό σημαίνει ότι χρησιμοποιούνται μόνο οι τιμές “valid” (έγκυρο) και “invalid” (μη έγκυρο), όπως ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού.

— EAA-6.2.10.1-03.2: Όσον αφορά τον κατάλογο αναγνωριστικών, περιλαμβάνονται μόνο ανακληθέντα MSO, και όχι MSO που έχουν ανασταλεί προσωρινά.

— EAA-6.2.10.1-04: Όταν ανακαλείται MSO, η ανάκλησή του είναι μόνιμη.

— EAA-6.2.10.1-05: Η επαλήθευση του καταλόγου ανάκλησης MSO είναι προαιρετική για το βασιζόμενο σε πορτοφόλι μέρος και, κατά περίπτωση, η επαλήθευση συμμορφώνεται τόσο με τις απαιτήσεις επαλήθευσης που ορίζονται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού όσο και με την προδιαγραφή δομής καθεστώτος που ορίζεται στο EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Όταν βασιζόμενο σε πορτοφόλι μέρος πρέπει να έχει τη δυνατότητα να επαληθεύσει το καθεστώς ανάκλησης δεδομένων ταυτοποίησης προσώπου ή ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, υποστηρίζει τόσο τον μηχανισμό καταλόγου καθεστώτος βεβαίωσης όσο και τον μηχανισμό καταλόγου ανάκλησης βεβαίωσης, όπως ορίζεται στο EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: Το identifier_list και το status_list στο MSO δύνανται να περιλαμβάνουν το στοιχείο πιστοποιητικού.

— EAA-6.2.10.1-06.1: Όταν υπάρχει το στοιχείο πιστοποιητικού, αυτό περιλαμβάνει πιστοποιητικό το οποίο περιέχει το δημόσιο κλειδί που υπέγραψε ή σφράγισε το πιστοποιητικό ανώτατου επιπέδου στο στοιχείο x5chain της δομής καταλόγου ανάκλησης MSO.

— EAA-6.2.10.1-06.1.1: Το στιγμιότυπο βασιζόμενου σε πορτοφόλι μέρους χρησιμοποιεί το εν λόγω πιστοποιητικό ως άγκυρα εμπιστοσύνης για την επαλήθευση του στοιχείου x5chain στη δομή καταλόγου ανάκλησης MSO.

— EAA-6.2.10.1-06.2: Όταν δεν υπάρχει το στοιχείο πιστοποιητικού, το πιστοποιητικό ανώτατου επιπέδου στο στοιχείο x5chain της δομής καταλόγου ανάκλησης MSO υπογράφεται ή σφραγίζεται από το πιστοποιητικό που χρησιμοποιείται για την υπογραφή του πιστοποιητικού στο στοιχείο x5chain του MSO.

— EAA-6.2.10.1-06.2.1: Το στιγμιότυπο βασιζόμενου σε πορτοφόλι μέρους χρησιμοποιεί το εν λόγω πιστοποιητικό ως άγκυρα εμπιστοσύνης για την επαλήθευση του στοιχείου x5chain στη δομή καταλόγου ανάκλησης MSO.

— EAA-6.2.10.1-07: Εφαρμόζεται κατάλογος ανάκλησης MSO σύμφωνα με την προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού σε μορφότυπο CWT.

— EAA-6.2.10.1-08: Για τον κατάλογο ανάκλησης MSO όσον αφορά τον μηχανισμό καταλόγου αναγνωριστικών και τον μηχανισμό καταλόγου καθεστώτος, ισχύουν οι ακόλουθες απαιτήσεις:

  — Εμφανίζεται η δήλωση exp.

  — Μπορεί να εμφανίζεται η δήλωση ttl.

  — Μπορεί να εμφανίζεται η δήλωση aggregation_uri στη δήλωση IdentifierList ή StatusList και ο πάροχος δεδομένων ταυτοποίησης προσώπου, ο πάροχος εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή ο πάροχος ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που παρέχονται από ή για λογαριασμό φορέα του

δημόσιου τομέα υπεύθυνου για αυθεντική πηγή μπορεί να χρησιμοποιεί τη δήλωση aggregation_uri για να δηλώσει ότι υποστηρίζει τον μηχανισμό συγκέντρωσης όπως ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού.

— Το CWT είναι αντικείμενο COSE_Sign1 που χρησιμοποιεί έναν από τους ακόλουθους αλγόριθμους υπογραφής για τον υπολογισμό της υπογραφής:

α) “ES256” (ECDSA με καμπύλη NIST P-256 και SHA-256)·

β) “ES384” (ECDSA με καμπύλη NIST P-384 και SHA-384)·

γ) “ES512” (ECDSA με καμπύλη NIST P-521 και SHA-512)·

δ) “ESB256” (ECDSA με καμπύλη brainpoolP256r1 και SHA-256)·

ε) “ESB384” (ECDSA με καμπύλη brainpoolP384r1 και SHA-384)·

στ) “ESB512” (ECDSA με καμπύλη brainpoolP512r1 και SHA-512)·

— Το CWT περιλαμβάνει το x5chain στην προστατευόμενη κεφαλίδα που περιέχει το πιστοποιητικό ή την αλυσίδα πιστοποιητικών για την επαλήθευση της υπογραφής του καταλόγου ανάκλησης MSO.

— Η εκτεταμένη χρήση κλειδιού του αναγνωριστικού αντικειμένου που ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού μπορεί να χρησιμοποιείται για το πιστοποιητικό υπογραφής του καταλόγου καθεστώτος και του καταλόγου αναγνωριστικών και τα στιγμιότυπα βασιζόμενου σε πορτοφόλι μέρους μπορούν να υποστηρίζουν την εκτεταμένη χρήση κλειδιού των αναγνωριστικών αντικειμένου που ορίζονται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού και για το αναγνωριστικό αντικειμένου, ο πάροχος εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή ο πάροχος ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που παρέχονται από φορέα του δημόσιου τομέα ή για λογαριασμό φορέα του δημόσιου τομέα δεν πρέπει να καθιστά κρίσιμο το πεδίο εκτεταμένης χρήσης κλειδιού κατά τη χρήση του OID εκτεταμένης χρήσης κλειδιού που ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού.

— EAA-6.2.10.1-09: Κατά παρέκκλιση από τις απαιτήσεις της προδιαγραφής του καταλόγου καθεστώτος αδειοδοτικού, για τον μηχανισμό καταλόγου αναγνωριστικών ισχύουν οι ακόλουθες απαιτήσεις:

— η τιμή της δήλωσης τύπου είναι “application/identifierlist+cwt”,

— η δήλωση StatusList δεν εμφανίζεται στο σύνολο των δηλώσεων CWT,

— η δομή IdentifierList που ορίζεται στο EAA-6.2.10.1-11 εμφανίζεται ως δήλωση στο σύνολο των δηλώσεων CWT που χρησιμοποιούν το κλειδί 65530.

— EAA-6.2.10.1-10: Η δομή IdentifierList είναι δομή CBOR με την ακόλουθη CDDL:

```
IdentifierList = {

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

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Όταν εμφανίζεται το αναγνωριστικό στο IdentifierList, ανακαλείται το MSO που περιλαμβάνει το αναγνωριστικό στο στοιχείο καθεστώτος.

— EAA-6.2.10.1-10.2: Η δήλωση Aggregation_uri ορίζεται στο σημείο 9.2 της προδιαγραφής του καταλόγου καθεστώτος αδειοδοτικού.

— EAA-6.2.10.1-10.3: Ο τύπος περιεχομένου του καταλόγου αναγνωριστικών είναι “application/identifierlist+cwt”, όπως ορίζεται στις απαιτήσεις του σημείου 8.2 της προδιαγραφής του καταλόγου καθεστώτος αδειοδοτικού.

— EAA-6.2.10.1-11: Για το στοιχείο identifier_list στο MSO ισχύουν οι απαιτήσεις που παρατίθενται κατωτέρω (βλ. EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Το στοιχείο IdentifierList είναι δομή CBOR με την ακόλουθη CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Για να αποτρέπεται η χρήση του αναγνωριστικού ως στοιχείου συσχέτισης μεταξύ προσκομίσεων, το αναγνωριστικό είναι μοναδικό ανά MSO.

— EAA-6.2.10.1-12: Για τον κατάλογο καθεστώτος ισχύουν οι ακόλουθες απαιτήσεις:

  — EAA-6.2.10.1-12.1: Το στοιχείο των δυφίων στη δομή StatusList ορίζεται στην τιμή 1.

— EAA-6.2.10.1-13: Για το στοιχείο status_list στο MSO ισχύουν οι ακόλουθες απαιτήσεις (βλ. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Το στοιχείο status_list πληροί τις απαιτήσεις για τη δομή StatusListInfo, όπως ορίζεται στην προδιαγραφή του καταλόγου καθεστώτος αδειοδοτικού, και προστίθεται το προαιρετικό στοιχείο πιστοποιητικού που ορίζεται στο EAA-6.2.10.1-06.

  — EAA-6.2.10.1-13.2: Για να αποτρέπεται η χρήση του δείκτη καθεστώτος ως στοιχείου συσχέτισης μεταξύ προσκομίσεων, ο συνδυασμός του δείκτη καθεστώτος και του URI είναι μοναδικός ανά MSO.

— EAA-6.2.10.1-14: Ο πάροχος πορτοφολιού χρησιμοποιεί τη δεύτερη (EAA-6.2.10.1-02.2) ή την τρίτη (EAA-6.2.10.1-02.3) από τις μεθόδους που ορίζονται στο EAA-6.2.10.1-02 για την ανάκληση βεβαίωσης μονάδας πορτοφολιού (WIA) και για την ανάκληση της βεβαίωσης κλειδιού (KA).

— EAA-6.2.10.1-15: Ο πάροχος πορτοφολιού εφαρμόζει τους μηχανισμούς ανάκλησης βεβαίωσης που ορίζονται στο EAA-6.2.10.1-02 στην οικεία υλοποίηση πορτοφολιού.

— EAA-6.2.10.1-16: Ο πάροχος δεδομένων ταυτοποίησης προσώπου και ο πάροχος ηλεκτρονικών βεβαιώσεων χαρακτηριστικών υποστηρίζουν τόσο τον μηχανισμό καταλόγου καθεστώτος βεβαίωσης όσο και τον μηχανισμό καταλόγου ανάκλησης βεβαίωσης, όπως ορίζεται στο EAA-6.2.10.1-02 για την επαλήθευση του καθεστώτος ανάκλησης βεβαίωσης μονάδας πορτοφολιού (WIA) και βεβαίωσης κλειδιού (KA).

— EAA-6.2.10.1-17: Η δομή καθεστώτος στο MSO είναι δομή CBOR με την ακόλουθη CDDL:

```
Status = {
? 'identifier_list' : IdentifierListInfo,
? 'status_list' : StatusListInfo,
* tstr => RFU
    }»
```

ΠΑΡΑΡΤΗΜΑ V

«ΠΑΡΑΡΤΗΜΑ III

Τεχνικές προδιαγραφές που αναφέρονται στο άρθρο 10

— Τεχνικές προδιαγραφές:

  — Σημείο 4.2.5 του ETSI TS 119 472-3 V1.1.1 (2026-03).»

ΠΑΡΑΡΤΗΜΑ VI

Το παράρτημα IV του εκτελεστικού κανονισμού (ΕΕ) 2024/2979 τροποποιείται ως εξής:

1. το σημείο 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Υποχρεωτικός μορφότυπος υπογραφής ή σφραγίδας:

α) PAdES (PDF Advanced Electronic Signature) όπως ορίζεται στο ETSI EN 319 142-1 V1.2.1 (2024-01)· Ηλεκτρονικές υπογραφές και υποδομές (ESI)· ψηφιακές υπογραφές PAdES· Μέρος 1: δομικά στοιχεία και βασικές υπογραφές PAdES.»·

2. το σημείο 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Διεπαφή προγραμματισμού εφαρμογών:
ETSI TS 119 432 v1.3.1 (2026-03) σημεία 6.4.3, A.6, A.7 και A.8.».

ΠΑΡΑΡΤΗΜΑ VII

«ΠΑΡΑΡΤΗΜΑ VI

Έγχρωμο σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ



»

ΠΑΡΑΡΤΗΜΑ VIII

«*ΠΑΡΑΡΤΗΜΑ VII*

Ασπρόμαυρο σήμα εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ



»

ΠΑΡΑΡΤΗΜΑ IX

«ΠΑΡΑΡΤΗΜΑ VIII

Δεδομένα του σήματος εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ

Δεδομένα	Περιγραφή	Κωδικοποίηση	Καθεστώς
TrustMarkResourceURL	Διεύθυνση URL των γραφικών του σήματος εμπιστοσύνης πορτοφολιού ψηφιακής ταυτότητας της ΕΕ και των πηγών πληροφοριών χρήστη στη διεπαφή χρήστη πορτοφολιού.	URL	υποχρεωτικό
ListOfCertifiedWalletsURL	Διεύθυνση URL του δημόσιου καταλόγου πιστοποιημένων υλοποιήσεων πορτοφολιού στην ΕΕ, όπως ορίζεται στον εκτελεστικό κανονισμό (ΕΕ) 2025/849 της Επιτροπής ([1]).	URL	υποχρεωτικό
ListOfCertifiedWalletsQRCode	QR Code που περιέχει τις πληροφορίες του ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	προαιρετικό
WalletSolutionInfoPageURL	Διεύθυνση URL προς τη σελίδα πληροφοριών της πιστοποιημένης υλοποίησης πορτοφολιού στον κατάλογο της σελίδας πιστοποιημένης υλοποίησης πορτοφολιού από τη διεύθυνση URL ListOfCertifiedWalletsURL με την προσθήκη συμβόλου "?" και του αναγνωριστικού WalletSolutionID της υλοποίησης πορτοφολιού.	URL	υποχρεωτικό
WalletSolutionInfoPageQRCode	QR Code που περιέχει τις πληροφορίες του WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	προαιρετικό
WalletVerifierToolURL*	Διεύθυνση URL προς το τελικό σημείο του εργαλείου επαλήθευσης πορτοφολιού */.well-known/openid-credential-issuer* που χρησιμοποιείται για την ανάκτηση των μεταδεδομένων του παρόχου βεβαίωσης.	URL	Προαιρετικό

([1]) Εκτελεστικός κανονισμός (ΕΕ) 2025/849 της Επιτροπής, της 6ης Μαΐου 2025, για τη θέσπιση κανόνων εφαρμογής του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την υποβολή πληροφοριών στην Επιτροπή και στην ομάδα συνεργασίας για τον κατάλογο πιστοποιημένων ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας (ΕΕ L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).»

ΠΑΡΑΡΤΗΜΑ Χ

Το παράρτημα ΙΙ του εκτελεστικού κανονισμού (ΕΕ) 2024/2980 τροποποιείται ως εξής:

1. Στο παράρτημα ΙΙ τμήμα 1 σημείο 1, το στοιχείο θ) αντικαθίσταται από το ακόλουθο κείμενο:

«θ) ένα ή περισσότερα πιστοποιητικά που συμμορφώνονται με το πρότυπο ETSI EN 319 412-2 V2.4.1 (2025-06) ή το πρότυπο ETSI EN 319 412-3 V1.3.1 (2023-09) και μπορούν να χρησιμοποιηθούν για την επαλήθευση της υπογραφής ή της σφραγίδας που δημιουργεί ο φορέας καταχώρισης στα δεδομένα του μητρώου, και για τα οποία τα πιστοποιημένα δεδομένα ταυτότητας περιλαμβάνουν την ονομασία του φορέα καταχώρισης και, κατά περίπτωση, τον αριθμό καταχώρισης του φορέα καταχώρισης, όπως προβλέπεται στα στοιχεία γ) και δ), αντίστοιχα.»·

2. Στο παράρτημα ΙΙ τμήμα 2 σημείο 1, το στοιχείο η) αντικαθίσταται από το ακόλουθο κείμενο:

«η) ένα ή περισσότερα πιστοποιητικά που συμμορφώνονται με το πρότυπο ETSI EN 319 412-2 V2.4.1 (2025-06) ή το πρότυπο ETSI EN 319 412-3 V1.3.1 (2023-09) και μπορούν να χρησιμοποιηθούν για την επαλήθευση και την επικύρωση των βεβαιώσεων μονάδας πορτοφολιού που έχει εκδώσει ο πάροχος πορτοφολιού, και για τα οποία τα πιστοποιημένα δεδομένα ταυτότητας περιλαμβάνουν την επωνυμία και, κατά περίπτωση, τον αριθμό καταχώρισης του παρόχου πορτοφολιού, όπως ορίζεται στα στοιχεία α) και β), αντίστοιχα.»·

3. Στο παράρτημα ΙΙ τμήμα 3 σημείο 1, το στοιχείο η) αντικαθίσταται από το ακόλουθο κείμενο:

«η) ένα ή περισσότερα πιστοποιητικά που συμμορφώνονται με το πρότυπο ETSI EN 319 412-2 V2.4.1 (2025-06) ή το πρότυπο ETSI EN 319 412-3 V1.3.1 (2023-09) και μπορούν να χρησιμοποιηθούν για την επαλήθευση της υπογραφής ή της σφραγίδας που δημιουργεί ο πάροχος δεδομένων ταυτοποίησης προσώπου στα δεδομένα ταυτοποίησης προσώπου που παρέχει, και για τα οποία τα πιστοποιημένα δεδομένα ταυτότητας περιλαμβάνουν την επωνυμία και, κατά περίπτωση, τον αριθμό καταχώρισης του παρόχου δεδομένων ταυτοποίησης προσώπου, όπως ορίζεται στα στοιχεία α) και β), αντίστοιχα.»·

4. Στο παράρτημα ΙΙ τμήμα 4 σημείο 1, το στοιχείο ζ) αντικαθίσταται από το ακόλουθο κείμενο:

«ζ) ένα ή περισσότερα πιστοποιητικά που συμμορφώνονται με το πρότυπο ETSI EN 319 412-2 V2.4.1 (2025-06) ή το πρότυπο ETSI EN 319 412-3 V1.3.1 (2023-09) και μπορούν να χρησιμοποιηθούν για την επαλήθευση της υπογραφής ή της σφραγίδας που δημιουργεί ο πάροχος πιστοποιητικών πρόσβασης βασιζόμενων σε πορτοφόλι μερών για τα πιστοποιητικά πρόσβασης τα οποία παρέχει σε βασιζόμενα σε πορτοφόλι μέρη, με, κατά περίπτωση, τις πληροφορίες που απαιτούνται για τη διάκριση των πιστοποιητικών πρόσβασης βασιζόμενων σε πορτοφόλι μερών από άλλα πιστοποιητικά.»·

5. Στο παράρτημα ΙΙ προστίθεται τμήμα 5 ως εξής:

«5. Κοινοποιήσεις πληροφοριών σχετικά με παρόχους πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών

1. Τα κράτη μέλη παρέχουν στην Επιτροπή τις ακόλουθες πληροφορίες σχετικά με τους παρόχους πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών:

α) την επωνυμία του παρόχου πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών·

β) κατά περίπτωση, αριθμό καταχώρισης του παρόχου πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών·

γ) το κράτος μέλος στο οποίο είναι εγκατεστημένος ο πάροχος πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών·

δ) την ηλεκτρονική διεύθυνση επικοινωνίας και τον αριθμό τηλεφώνου επικοινωνίας του παρόχου πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών, για θέματα που σχετίζονται με τα πιστοποιητικά καταχώρισης τα οποία παρέχει σε βασιζόμενα σε πορτοφόλι μέρη·

ε) κατά περίπτωση, τη διεύθυνση URL της ιστοσελίδας του παρόχου πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών η οποία περιέχει πρόσθετες πληροφορίες σχετικά με τον πάροχο και τα πιστοποιητικά καταχώρισης που παρέχει σε βασιζόμενα σε πορτοφόλι μέρη·

στ) τη διεύθυνση URL της ιστοσελίδας που περιέχει τις πολιτικές, τους όρους και τις προϋποθέσεις που ισχύουν για την παροχή και τη χρήση των πιστοποιητικών καταχώρισης τα οποία παρέχει σε βασιζόμενα σε πορτοφόλι μέρη·

ζ) ένα ή περισσότερα πιστοποιητικά που συμμορφώνονται με το πρότυπο ETSI EN 319 412-2 V2.4.1 (2025-06) ή το πρότυπο ETSI EN 319 412-3 V1.3.1 (2023-09) και μπορούν να χρησιμοποιηθούν για την επαλήθευση της υπογραφής ή της σφραγίδας που δημιουργεί ο πάροχος πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών για τα πιστοποιητικά καταχώρισης τα οποία παρέχει σε βασιζόμενα σε πορτοφόλι μέρη, με, κατά περίπτωση, τις πληροφορίες που απαιτούνται για τη διάκριση των πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών από άλλα πιστοποιητικά.

2. Οι πληροφορίες που αναφέρονται στο σημείο 1 παρέχονται ανά πάροχο πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών.».

ΠΑΡΑΡΤΗΜΑ XI

«ΠΑΡΑΡΤΗΜΑ I

Πρωτόκολλα και διεπαφές που αναφέρονται στο άρθρο 4

Ισχύει η τεχνική προδιαγραφή του ETSI TS 119 472-3 V1.1.1 (2026-03) με τις ακόλουθες προσαρμογές:

1) 4.1 General requirements

— GEN-REQ-4.1-05: άκυρο.

— ΣΗΜΕΙΩΣΗ: άκυρο.

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: Ένα από τα στοιχεία της παραμέτρου του πίνακα issuer_info περιέχει το πιστοποιητικό καταχώρισης του παρόχου PID/EAA.

— ISS-MDATA-REG_CERT-4.2.3-07: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-08: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-09: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-10: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-11: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-12: άκυρο

— ISS-MDATA-REG_CERT-4.2.3-13: άκυρο

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Όταν το μέλος id έχει την τιμή “arf_annex_ii” και ο πίνακας που αντιστοιχίζεται στην ετικέτα “details” περιέχει την τιμή “once_only” ή την τιμή “per-relying-party”, τότε το αντικείμενο JSON το οποίο περιέχει τον εν λόγω πίνακα που αντιστοιχίζεται στην ετικέτα “details” περιέχει επίσης έναν αριθμό JSON που αντιστοιχίζεται στην ετικέτα “reissue_trigger_unused”.

4) Το παράρτημα Α δεν εφαρμόζεται.»

ΠΑΡΑΡΤΗΜΑ XII

«ΠΑΡΑΡΤΗΜΑ II

Τεχνικές προδιαγραφές που αναφέρονται στο άρθρο 5

Ισχύει η τεχνική προδιαγραφή του παραρτήματος Γ του ISO/IEC 18013-7:2025.

Ισχύουν οι τεχνικές προδιαγραφές των σημείων 4.1, 4.2, 5, και 6 του ETSI TS 119 472-2 V1.2.1 (2026-03), με τις ακόλουθες προσαρμογές, συμπεριλαμβανομένης της προσθήκης νέου σημείου 4.3:

1) 1 Scope

— Το παρόν έγγραφο προσδιορίζει δύο προφίλ πρωτοκόλλων ώστε να επιτρέπεται, αφενός, στα βασιζόμενα μέρη (στο εξής: RP) να ζητούν δεδομένα παρόχων ηλεκτρονικής βεβαίωσης χαρακτηριστικών (στο εξής: EAAP) ή δεδομένα ταυτοποίησης προσώπου (στο εξής: PID) στο πορτοφόλι ψηφιακής ταυτότητας της ΕΕ και, αφετέρου, στο πορτοφόλι ψηφιακής ταυτότητας της ΕΕ να αποστέλλει τα ζητούμενα δεδομένα EAAP/PID στα RP. Καθένα από τα προφίλ υποστηρίζει δύο μηχανισμούς διαβίβασης, και συγκεκριμένα έναν μεσολαβούμενο από API (διεπαφή προγραμματισμού εφαρμογών) και έναν μη μεσολαβούμενο από API, όπως αναφέρεται κατωτέρω:

α) Ένα προφίλ βασίζεται στα εξής:

— ISO/IEC 18013-5 [10] μόνο για τον μη μεσολαβούμενο από API μηχανισμό διαβίβασης, και

— παράρτημα Γ του ISO/IEC 18013-7 [16], για τον μεσολαβούμενο από API μηχανισμό διαβίβασης.

Το προφίλ αυτό ονομάζεται προφίλ ISO/IEC-mdoc και ορίζεται στο σημείο 5 του παρόντος εγγράφου.

β) Ένα προφίλ βασίζεται στα εξής:

OpenID4VC-HAIP [11], τόσο για τον μεσολαβούμενο από API όσο και για τον μη μεσολαβούμενο από API μηχανισμό διαβίβασης, ως εξής:

— τμήματα 5, 5.1, 5.3, 7, και 8 του [11], για τη διαβίβαση μέσω Redirects ή για μη μεσολαβούμενο από API μηχανισμό διαβίβασης, και

— τμήματα 5, 5.2, 5.3, 7, και 8 του [11] για μη μεσολαβούμενο από API μηχανισμό διαβίβασης.

Το προφίλ αυτό ονομάζεται προφίλ OpenID4VC-HAIP και ορίζεται στο σημείο 6 του παρόντος εγγράφου.

2) 2.1 Normative references

— [15] ISO 639: 'Language code'.

— [16] ISO/IEC 18013-7:2025 “Ταυτοποίηση προσώπου — Συμβατή με τον ISO άδεια οδήγησης — Μέρος 7: Πρόσθετες λειτουργίες ψηφιακής άδειας οδήγησης (mDL)”.

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: άκυρο.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: άκυρο.

— *Note 2*: άκυρο.

— EAAP-ISO/IEC-mdoc-02: άκυρο.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: Το πορτοφόλι EUDI υποστηρίζει την API μεσολάβησης που υποστηρίζει και τα δύο πρωτόκολλα που ορίζονται στο σημείο 5.2 του [11] και στο παράρτημα Γ του [16].

— *ΣΗΜΕΙΩΣΗ*: Όταν η διάταξη στην οποία είναι εγκατεστημένο το πορτοφόλι EUDI δεν υποστηρίζει τα δύο πρωτόκολλα, η απαίτηση αυτή δεν μπορεί να εκπληρωθεί και προκύπτει μη συμμόρφωση επειδή τα υποκείμενα λειτουργικά συστήματα και οι φυλλομετρητές δεν εφαρμόζουν τα αναγκαία χαρακτηριστικά διαλειτουργικότητας.

— EAAP-API-GEN-02: Το πορτοφόλι EUDI υποστηρίζει την API μεσολάβησης τουλάχιστον για τους τύπους PID και EAA που είναι καταχωρισμένοι στον κατάλογο συστημάτων, όπως ορίζεται στον εκτελεστικό κανονισμό (ΕΕ) 2025/1569, και τουλάχιστον για όλους τους μορφότυπους που ορίζονται στο παράρτημα II του εκτελεστικού κανονισμού (ΕΕ) 2024/2979.

— *ΣΗΜΕΙΩΣΗ 1*: Όταν το υποκείμενο λειτουργικό σύστημα, ο φυλλομετρητής, οι διεπαφές προγραμματισμού εφαρμογών (API) μεσολάβησης ή οποιοδήποτε άλλο τεχνικό επίπεδο εκτός του ελέγχου του πορτοφολιού EUDI περιορίζει, φιλτράρει, προεπιλέγει ή επιβάλλει περιορισμό με άλλο τρόπο στους μορφότυπους διαπιστευτηρίων, καθώς και στους τύπους PID και EAA που είναι καταχωρισμένοι στον κατάλογο συστημάτων, η απαίτηση αυτή δεν μπορεί να εκπληρωθεί. Όταν ένας τέτοιος περιορισμός εμποδίζει το πορτοφόλι EUDI να υποστηρίξει έναν καταχωρισμένο τύπο ή μορφότυπο διαπιστευτηρίου, η προκύπτουσα μη συμμόρφωση οφείλεται στην αδυναμία των εν λόγω υποκείμενων λειτουργικών συστημάτων, φυλλομετρητών, API μεσολάβησης ή άλλου σχετικού τεχνικού επιπέδου να παράσχουν τα αναγκαία χαρακτηριστικά διαλειτουργικότητας.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: Το πορτοφόλι EUDI επικυρώνει το πιστοποιητικό καταχώρισης βασιζόμενου σε πορτοφόλι μέρους που λαμβάνεται στο αίτημα πριν από την προσκόμιση τυχόν ζητούμενου PID ή ηλεκτρονικής βεβαίωσης χαρακτηριστικών στον χρήστη πορτοφολιού προς έγκριση.

— WRP-VALIDATION-02: Όταν η επικύρωση του πιστοποιητικού καταχώρισης βασιζόμενου σε πορτοφόλι μέρους δεν είναι επιτυχής, μεταξύ άλλων στην περίπτωση που το πιστοποιητικό έχει λήξει, ανακληθεί, δεν έχει εκδοθεί από έγκυρο και αξιόπιστο πάροχο πιστοποιητικών καταχώρισης βασιζόμενων σε πορτοφόλι μερών, έχει αλλοιωθεί ή δεν μπορεί να επαληθευτεί κρυπτογραφικά, το πορτοφόλι EUDI προειδοποιεί τον χρήστη πορτοφολιού ότι το βασιζόμενο σε πορτοφόλι μέρος δεν μπόρεσε να επικυρωθεί και δεν παρουσιάζει το αίτημα ως επιτυχώς επικυρωμένο. Ο χρήστης πορτοφολιού εγκρίνει ρητά το αίτημα του βασιζόμενου μέρους. Η σιωπή ή τα προσυμπληρωμένα τετραγωνίδια δεν αρκούν για τη ρητή έγκριση.

— WRP-VALIDATION-03: Ο πάροχος πορτοφολιού προσδιορίζει, με βάση την ανάλυση κινδύνου και την πολιτική ασφάλειας που εφαρμόζει, αν και υπό ποιες προϋποθέσεις ο χρήστης πορτοφολιού μπορεί να παρακάμψει συγκεκριμένους αποτυχημένους ελέγχους επικύρωσης.

— WRP-OVERASKING-01: Το πορτοφόλι EUDI συγκρίνει τις βεβαιώσεις και τα χαρακτηριστικά που ζητούνται από το βασιζόμενο σε πορτοφόλι μέρος με τις καταχωρισμένες βεβαιώσεις και τα καταχωρισμένα χαρακτηριστικά στο πιστοποιητικό καταχώρισης βασιζόμενου σε πορτοφόλι μέρους.

— WRP-OVERASKING-02: Όταν το βασιζόμενο σε πορτοφόλι μέρος ζητεί PID ή ηλεκτρονικές βεβαιώσεις χαρακτηριστικών ή δηλώσεις που δεν καλύπτονται από το πιστοποιητικό καταχώρισης βασιζόμενου σε πορτοφόλι μέρους, το πορτοφόλι EUDI προειδοποιεί με σαφή τρόπο τον χρήστη πορτοφολιού πριν από οποιαδήποτε γνωστοποίηση. Στην προειδοποίηση αναφέρεται ότι το βασιζόμενο σε πορτοφόλι μέρος ζητεί περισσότερες πληροφορίες από όσες έχουν καταχωριστεί. Ο χρήστης πορτοφολιού εγκρίνει ρητά το αίτημα του βασιζόμενου μέρους. Η σιωπή ή τα προσυμπληρωμένα τετραγωνίδια δεν αρκούν για τη ρητή έγκριση.

— WRP-OVERASKING-03: Ο πάροχος πορτοφολιού προσδιορίζει, με βάση την ανάλυση κινδύνου, την πολιτική ασφάλειας και το εφαρμοστέο δίκαιο, αν ο χρήστης πορτοφολιού μπορεί να συνεχίσει παρά την εν λόγω προειδοποίηση, αν μπορεί να γνωστοποιηθεί μόνο το υποσύνολο των ζητούμενων δεδομένων που καλύπτονται από το πιστοποιητικό καταχώρισης ή αν το αίτημα απορρίπτεται.

7) 5.1 Introduction

— Το σημείο 5 και τα υποσημεία του ορίζουν προφίλ για ένα πρωτόκολλο το οποίο επιτρέπει, αφενός, σε RP να ζητούν δεδομένα EAAP ή PID στο πορτοφόλι ψηφιακής ταυτότητας της ΕΕ και, αφετέρου, στο πορτοφόλι ψηφιακής ταυτότητας της ΕΕ να αποστέλλει τα ζητούμενα δεδομένα EAAP/PID στα RP, με τη χρήση είτε μη μεσολαβούμενου από API μηχανισμού διαβίβασης, που βασίζεται στο ISO/IEC 18013-5 [10], είτε μη μεσολαβούμενου από API μηχανισμού διαβίβασης, που βασίζεται στο παράρτημα Γ του ISO/IEC 18013-7 [16], για τη διαβίβαση των δομών δεδομένων που ορίζονται στο ISO/IEC 18013-5 [10], σε κατάλληλη συμπυκνωμένη μορφή.

— Το υπόλοιπο περιεχόμενο του σημείου 5 οργανώνεται ως εξής:

— το σημείο 5.2 ορίζει απαιτήσεις σχετικά με την υποστήριξη του προφίλ και των μηχανισμών διαβίβασης από τα RP και το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ,

— το σημείο 5.3 καθορίζει απαιτήσεις που αφορούν ειδικά τον μη μεσολαβούμενο από API μηχανισμό διαβίβασης,

— το σημείο 5.4 και τα υποσημεία του ορίζουν απαιτήσεις που αφορούν ειδικά τον μεσολαβούμενο από API μηχανισμό διαβίβασης.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Οι μονάδες πορτοφολιού, οι πάροχοι PID, οι πάροχοι βεβαίωσης, οι πάροχοι πορτοφολιού και τα βασιζόμενα μέρη δεν υποστηρίζουν την ανάκτηση δεδομένων από εξυπηρετητή όπως ορίζεται στο ISO/IEC 18013-5 [10] για την υποβολή αιτήματος και προσκόμισης PID ή βεβαίωσης χαρακτηριστικών.

— ISO/IEC 18013-SUPPORT-02: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ πληροί τις απαιτήσεις που ορίζονται στα σημεία 5.3 και 5.4 του παρόντος εγγράφου.

— ISO/IEC 18013-SUPPORT-04: Κάθε βασιζόμενο μέρος θα πρέπει να εφαρμόζει το προφίλ που ορίζεται στο σημείο 5.4 του παρόντος εγγράφου.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Τα αιτήματα διάταξης που αποστέλλονται σε πορτοφόλια ψηφιακής ταυτότητας της ΕΕ περιλαμβάνουν το ζεύγος κλειδιού-τιμής “requestInfo” που ορίζεται στο σημείο 8.3.2.1.2.1 του [10]. Η τιμή αυτού του ζεύγους τιμών είναι του τύπου RequestInfo.

— ISO/IEC 18013-5-REQ-05: Ο τύπος RequestInfo ορίζεται σύμφωνα με τον ορισμό της CDDL που παρατίθεται κατωτέρω.

```
RequestInfo = {

    'euWrprc': bstr ; περιέχει πιστοποιητικό καταχώρισης (βλ. απαιτήσεις κατωτέρω)

}
```

— ISO/IEC 18013-5-REQ-06: Το αναφερόμενο μέλος requestInfo περιλαμβάνει ένα μέλος με την ένδειξη «euWrprc»

— ISO/IEC 18013-5-REQ-07: Η τιμή του “euWrprc” είναι πιστοποιητικό καταχώρισης με κωδικοποίηση CBOR.

— ISO/IEC 18013-5-REQ-08: άκυρο.

— *ΣΗΜΕΙΩΣΗ* 3: άκυρο.

— ISO/IEC 18013-5-REQ-09: άκυρο.

— ISO/IEC 18013-5-REQ-10: άκυρο.

— ISO/IEC 18013-5-REQ-11: άκυρο.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Το παρόν σημείο ορίζει τις απαιτήσεις για τον τύπο μηνύματος DeviceResponse, οι οποίες είναι κοινές για τους δύο τύπους μηχανισμών διαβίβασης (μεσολαβούμενος από API και μη μεσολαβούμενος από API).

— *ΣΗΜΕΙΩΣΗ 1*: Όταν χρησιμοποιείται μη μεσολαβούμενος από API μηχανισμός που βασίζεται στο πρότυπο ISO/IEC 18013-5 [10], η απόκριση EAAP αποτελεί επακριβώς στιγμιότυπο DeviceResponse, όπως περιγράφεται στο παρόν σημείο, ενώ όταν χρησιμοποιείται μεσολαβούμενος από API μηχανισμός που βασίζεται στο παράρτημα Γ του προτύπου ISO/IEC 18013-7 [16], το στιγμιότυπο DeviceRequest έχει συμπυκνωμένη μορφή, όπως ορίζεται στο παράρτημα Γ του [16].

— ISO/IEC 18013-5-RESP-02: Ο πάροχος δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών δεν περιλαμβάνει στοιχεία δεδομένων στην αντιστοίχιση KeyAuthorisations στο αντικείμενο κινητής ασφάλειας των δεδομένων ταυτοποίησης προσώπου και των ηλεκτρονικών βεβαιώσεων χαρακτηριστικών που εκδίδει, εξαιρουμένων των στοιχείων δεδομένων που παρέχονται από το βασιζόμενο σε πορτοφόλι μέρος στα δεδομένα συναλλαγών που περιλαμβάνονται στο αίτημα mdoc προς υπογραφή ή σφράγιση από τη μονάδα πορτοφολιού με τη χρήση του ιδιωτικού κλειδιού των δεδομένων ταυτοποίησης προσώπου ή των ηλεκτρονικών βεβαιώσεων χαρακτηριστικών.

— *ΣΗΜΕΙΩΣΗ 2*: Συνεπώς, οι μονάδες πορτοφολιού δεν μπορούν να προσκομίζουν σε βασιζόμενα σε πορτοφόλι μέρη στοιχεία δεδομένων που υπογράφονται από διάταξη, παρά μόνο να υπογράφουν δεδομένα που παρείχε το βασιζόμενο σε πορτοφόλι μέρος, π.χ. σε περιπτώσεις χρήσης για την ασφαλή επαλήθευση ταυτότητας χρήστη.

— *ΣΗΜΕΙΩΣΗ 3*: Το ISO/IEC 18013-5:2021 δεν ορίζει τον τρόπο με τον οποίο τα βασιζόμενα σε πορτοφόλι μέρη μπορούν να συμπεριλαμβάνουν δεδομένα συναλλαγών σε αίτημα mdoc. Η συμπερίληψη δεδομένων συναλλαγών σε αίτημα mdoc πραγματοποιείται με την προσθήκη τεχνικών προδιαγραφών.

— ISO/IEC 18013-5-RESP-03: Οι πάροχοι δεδομένων ταυτοποίησης προσώπου δεν επιτρέπουν στο ιδιωτικό κλειδί των δεδομένων ταυτοποίησης προσώπου να υπογράφει στοιχεία δεδομένων που παρέχονται από το βασιζόμενο σε πορτοφόλι μέρος στα δεδομένα συναλλαγών στο αίτημα mdoc.

11) 5.4 Requirements for API mediated mechanism (Απαιτήσεις για τον μεσολαβούμενο από API μηχανισμό)

5.4.1 ISO/IEC 18013-7-related requirements

Το παρόν σημείο ορίζει τις απαιτήσεις για τον μεσολαβούμενο από API μηχανισμό διαβίβασης οι οποίες συνδέονται με τις απαιτήσεις που ορίζονται στο παράρτημα Γ του [16].

— ISO/IEC 18013-7-API-01: Το προφίλ που υποστηρίζει προσκομίσεις μεσολαβούμενες από API συμμορφώνεται με τις απαιτήσεις του παραρτήματος Γ του ISO/IEC 18013-7 [16], όπως περιγράφεται αναλυτικότερα στα σημεία 5.3 και 5.4 του παρόντος εγγράφου.

— ISO/IEC 18013-7-API-02: Όλες οι υποχρεωτικές απαιτήσεις που ορίζονται στο παράρτημα Γ του [16] ισχύουν όπως περιγράφεται αναλυτικότερα στα σημεία 5.3 και 5.4 του παρόντος εγγράφου.

— ISO/IEC 18013-7-API-03: Όλες οι προαιρετικές απαιτήσεις που ορίζονται στο παράρτημα Γ του [16] παραμένουν προαιρετικές, εκτός εάν ορίζεται διαφορετικά στο παρόν έγγραφο.

12) 5.4.2 Additional requirements

— Το παρόν σημείο ορίζει τις πρόσθετες απαιτήσεις για τον μεσολαβούμενο από API μηχανισμό διαβίβασης.

— ISO/IEC 18013-ADD-API-01: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ γνωστοποιεί εξ ορισμού την παρουσία όλων των αποθηκευμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών στην API μεσολάβησης που λειτουργεί σύμφωνα με το παράρτημα Γ του [16], αλλά δεν γνωστοποιεί τα χαρακτηριστικά και τις τιμές τους στις εν λόγω ηλεκτρονικές βεβαιώσεις χαρακτηριστικών.

  — *ΣΗΜΕΙΩΣΗ 1*: Ο περιορισμός όσον αφορά την τιμή των χαρακτηριστικών ισχύει ακόμα και αν η εν λόγω γνωστοποίηση θα μπορούσε να βελτιώσει τις υπηρεσίες που παρέχονται από το λειτουργικό σύστημα στο πορτοφόλι ψηφιακής ταυτότητας της ΕΕ, όπως, π.χ., η επιλογή βεβαίωσης στο πλαίσιο της API μεσολάβησης.

— Υπάρχουν οι παράμετροι που συνδέονται με τα λειτουργικά συστήματα και τους φυλλομετρητές και δεν εμπίπτουν στον έλεγχο των εργαλείων εφαρμογής, οι οποίες είναι δυνατόν να λαμβάνονται υπόψη όπως αναφέρεται στις σημειώσεις 2 έως 4 που ακολουθούν:

  — *ΣΗΜΕΙΩΣΗ 2*: Αίτημα προσκόμισης από βασιζόμενο μέρος το οποίο υποστηρίζει το παράρτημα Γ του [16] μπορεί να υποβληθεί σε επεξεργασία από τον φυλλομετρητή και/ή το λειτουργικό σύστημα για την αναζήτηση διαθέσιμων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, για την πρόληψη περιπτώσεων απάτης που στοχεύουν τον χρήστη ή για σκοπούς αντιμετώπισης προβλημάτων.

  — *ΣΗΜΕΙΩΣΗ 3*: Αίτημα προσκόμισης από βασιζόμενο μέρος το οποίο υποστηρίζει το παράρτημα Γ του [16] αναμένεται να υποβληθεί σε επεξεργασία από τον φυλλομετρητή και/ή το λειτουργικό σύστημα για λόγους ασφάλειας των χρηστών.

— *ΣΗΜΕΙΩΣΗ 4*: Αίτημα προσκόμισης από βασιζόμενο μέρος το οποίο υποστηρίζει το παράρτημα Γ του [16] δεν αναμένεται να υποβληθεί σε επεξεργασία από τον φυλλομετρητή και/ή το λειτουργικό σύστημα για σκοπούς ανάλυσης της αγοράς (μεταξύ άλλων ούτε ως δευτερεύων σκοπός) ή για εσωτερικούς σκοπούς του φυλλομετρητή και/ή του λειτουργικού συστήματος.

— ISO/IEC 18013-ADD-API-02: Όταν το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ διαγράφει στο αίτημα του χρήστη PID ή EAA που είχε προηγουμένως γνωστοποιηθεί στην API μεσολάβησης, η οποία λειτουργεί σύμφωνα με το παράρτημα Γ του [16], το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ γνωστοποιεί το γεγονός ότι δεν αποθηκεύει πλέον τα εν λόγω PID ή την εν λόγω EAA στην API μεσολάβησης.

— ISO/IEC 18013-ADD-API-03: Εάν ο χρήστης προβεί σε απεγκατάσταση του πορτοφολιού ψηφιακής ταυτότητας της ΕΕ, το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ γνωστοποιεί το γεγονός ότι δεν αποθηκεύει πλέον τυχόν PID ή EAA που είχαν προηγουμένως γνωστοποιηθεί στην API μεσολάβησης, η οποία λειτουργεί σύμφωνα με το παράρτημα Γ του [16].

— ISO/IEC 18013-ADD-API-04: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ παρέχει καθολική ρύθμιση χρήστη για την απενεργοποίηση της γνωστοποίησης αποθηκευμένων EAA μέσω API μεσολάβησης η οποία λειτουργεί σύμφωνα με τις προδιαγραφές του ISO/IEC 18013-ADD-API-01. Όταν η ρύθμιση αυτή είναι απενεργοποιημένη, το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ δεν διαφημίζει ούτε αποκρίνεται σε αιτήματα προσκόμισης ή έκδοσης μεσολαβούμενης από API.

— ISO/IEC 18013-ADD-API-05: Τα πορτοφόλια EUDI επαληθεύουν σε ροές μεταξύ διατάξεων, χρησιμοποιώντας την API μεσολάβησης, ότι η αλληλεπιδρώσα διάταξη βρίσκεται σε στενή φυσική εγγύτητα με το πορτοφόλι EUDI με τη χρήση ασφαλούς, άμεσου και μεσολαβούμενου από τον χρήστη τοπικού διαύλου επικοινωνίας, όπως μια ασύρματη τεχνολογία επικοινωνίας μικρής εμβέλειας για τη διενέργεια του ελέγχου φυσικής εγγύτητας.

— *ΣΗΜΕΙΩΣΗ*: Η CTAP 2.3 επιτρέπει τη χρήση BLE για τη διενέργεια του ελέγχου στενής φυσικής εγγύτητας και, όταν εφαρμόζεται και από τις δύο διατάξεις, επιτρέπει επίσης τη μεταφορά των δεδομένων μεταξύ των διατάξεων μέσω τεχνολογιών μετάδοσης μικρής εμβέλειας. Η διενέργεια τόσο του ελέγχου φυσικής εγγύτητας όσο και της μεταφοράς δεδομένων μεταξύ των δύο διατάξεων με τη χρήση τοπικού διαύλου επικοινωνίας, όπως καθίσταται δυνατή από τη CTAP 2.3, θα πρέπει να προτιμάται από τα υποκείμενα λειτουργικά συστήματα, τους φυλλομετρητές, τις διεπαφές προγραμματισμού εφαρμογών (API) μεσολάβησης ή οποιοδήποτε άλλο τεχνικό επίπεδο εκτός του ελέγχου του πορτοφολιού EUDI έναντι της χρήσης υπηρεσιών CTAP Hybrid Tunnel.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ πληροί τις απαιτήσεις που ορίζονται στο σημείο 6.5 του παρόντος παραρτήματος.

— OIDFVP-HAIP-SUPPORT-03: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ δεν θα πρέπει να υποστηρίζει τον μηχανισμό βάσει Redirects που ορίζεται στο σημείο 6.4 για τις ροές προσκόμισης μεταξύ διατάξεων.

— *ΣΗΜΕΙΩΣΗ 3*: Η χρήση αυτού του μηχανισμού είναι ευάλωτη σε επιθέσεις, όπως δέσμευση της περιόδου λειτουργίας. Ο μετριασμός τέτοιων επιθέσεων είναι ευθύνη των βασιζόμενων μερών. Η εφαρμογή αυτού του μηχανισμού δεν θα πρέπει να οδηγεί σε μη συμμόρφωση.

— OIDFVP-HAIP-SUPPORT-05: Το βασιζόμενο μέρος πληροί τις απαιτήσεις που ορίζονται στο σημείο 6.5 του παρόντος παραρτήματος.

— *ΣΗΜΕΙΩΣΗ 5*: άκυρο.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Ισχύουν όλες οι υποχρεωτικές απαιτήσεις που ορίζονται στα σημεία 5, 5.3, 7 και 8 του HAIP [11].

— *ΣΗΜΕΙΩΣΗ 1*: Το "HAIP [11] Τμήμα 5" αναφέρεται μόνο στις απαιτήσεις που βρίσκονται ακριβώς κάτω από τον τίτλο του τμήματος 5. Δεν περιλαμβάνει τα τμήματα 5.1, 5.2 και 5.3.

— OIDFVP-HAIP-GEN-03: Εάν το παρόν παράρτημα τροποποιεί απαίτηση που περιλαμβάνεται στο OpenID4VC-HAIP [11], υπερισχύει η τροποποιημένη απαίτηση που ορίζεται στο παρόν παράρτημα.

— *ΣΗΜΕΙΩΣΗ 2*: Με τον τρόπο αυτόν θα είναι δυνατή, για παράδειγμα, η μετατροπή μιας προαιρετικής απαίτησης από το OpenID4VC-HAIP [11] σε υποχρεωτική ή η επέκταση των υποχρεωτικών απαιτήσεων.

— OIDFVP-HAIP-GEN-04: Όταν ο μορφότυπος της ζητούμενης βεβαίωσης συμμορφώνεται με το [10], τα βασιζόμενα μέρη και τα πορτοφόλια ψηφιακής ταυτότητας της ΕΕ συμμορφώνονται με το προφίλ "ISO mdocs" του [11] τμήμα 6.

— *ΣΗΜΕΙΩΣΗ 3*: Για λόγους σαφήνειας: από το "προφίλ ISO mdocs" του HAIP συνεπάγεται ότι τα βασιζόμενα μέρη και τα πορτοφόλια ψηφιακής ταυτότητας της ΕΕ πρέπει να πληρούν τις εφαρμοστέες απαιτήσεις του [7] παράρτημα B.2.

— OIDFVP-HAIP-GEN-05: Όταν ο μορφότυπος της ζητούμενης βεβαίωσης συμμορφώνεται με το [2], τα βασιζόμενα μέρη και τα πορτοφόλια ψηφιακής ταυτότητας της ΕΕ συμμορφώνονται με το προφίλ "IETF SD-JWT VCs" του [11] τμήμα 6.

— *ΣΗΜΕΙΩΣΗ 4*: Για λόγους σαφήνειας: από το "προφίλ IETF SD-JWT Vcs" συνεπάγεται ότι τα βασιζόμενα μέρη και τα πορτοφόλια ψηφιακής ταυτότητας της ΕΕ πρέπει να πληρούν τις απαιτήσεις του [7] παράρτημα B.3, καθώς και τις απαιτήσεις του [11] τμήμα 6.1.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: άκυρο.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-03: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-04: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-05: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-06: άκυρο.

— OIDFVP-HAIP-COMMON-REQ-RO-07: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-08: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-09: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-10: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-11: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-12: άκυρο

— *Σημείωση 2*: άκυρο

— OIDFVP-HAIP-COMMON-REQ-RO-13: Ένα από τα στοιχεία της παραμέτρου verifier_info περιλαμβάνει το πιστοποιητικό καταχώρισης.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Το πιστοποιητικό φύλλου που αναφέρεται στο OpenID4VP τμήμα 5.9.3 για χρήση με το x509_hash Client Identifier Prefix είναι πιστοποιητικό πρόσβασης RP σύμφωνα με τις προδιαγραφές του προτύπου ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: άκυρο.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: άκυρο.

— *ΣΗΜΕΙΩΣΗ*: άκυρο.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: Το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ γνωστοποιεί εξ ορισμού την παρουσία όλων των αποθηκευμένων τύπων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών στην API μεσολάβησης που λειτουργεί σύμφωνα με το σημείο 5.2 του [11], αλλά δεν γνωστοποιεί τα χαρακτηριστικά και τις τιμές τους στις εν λόγω ηλεκτρονικές βεβαιώσεις χαρακτηριστικών.

— OIDFVP-HAIP-ADD-API-04: Εάν το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ υποστηρίζει API μεσολάβησης η οποία λειτουργεί σύμφωνα με το OIDFVP-HAIP-ADD-API-01, παρέχει καθολική ρύθμιση χρήστη για την απενεργοποίηση της γνωστοποίησης αποθηκευμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών μέσω της API μεσολάβησης. Όταν η ρύθμιση αυτή έχει οριστεί στην απενεργοποιημένη γνωστοποίηση, το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ θα πρέπει στη συνέχεια να επιτρέπει στον χρήστη την επιλογή μεμονωμένων βεβαιώσεων προς γνωστοποίηση στην API μεσολάβησης.

— OIDFVP-HAIP-ADD-API-05: Τα πορτοφόλια EUDI επαληθεύουν σε ροές μεταξύ διατάξεων, χρησιμοποιώντας την API μεσολάβησης, ότι η αλληλεπιδρώσα διάταξη βρίσκεται σε στενή φυσική εγγύτητα με το πορτοφόλι EUDI με τη χρήση ασφαλούς, άμεσου και μεσολαβούμενου από τον χρήστη τοπικού διαύλου επικοινωνίας, όπως μια ασύρματη τεχνολογία επικοινωνίας μικρής εμβέλειας για τη διενέργεια του ελέγχου φυσικής εγγύτητας.

— *ΣΗΜΕΙΩΣΗ 5*: Η CTAP 2.3 επιτρέπει τη χρήση BLE για τη διενέργεια του ελέγχου στενής φυσικής εγγύτητας και, όταν εφαρμόζεται και από τις δύο διατάξεις, επιτρέπει επίσης τη μεταφορά των δεδομένων μεταξύ των διατάξεων μέσω τεχνολογιών μετάδοσης μικρής εμβέλειας. Η διενέργεια τόσο του ελέγχου φυσικής εγγύτητας όσο και της μεταφοράς δεδομένων μεταξύ των δύο διατάξεων με τη χρήση τοπικού διαύλου επικοινωνίας, όπως καθίσταται δυνατή από τη CTAP 2.3, θα πρέπει να προτιμάται από τα υποκείμενα λειτουργικά συστήματα, τους φυλλομετρητές, τις διεπαφές προγραμματισμού εφαρμογών (API) μεσολάβησης ή οποιοδήποτε άλλο τεχνικό επίπεδο εκτός του ελέγχου του πορτοφολιού EUDI έναντι της χρήσης υπηρεσιών CTAP Hybrid Tunnel.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Όλες οι απαιτήσεις που ορίζονται στο παρόν έγγραφο και ισχύουν για τις δομές αιτήματος διάταξης και απόκρισης διάταξης που ορίζονται στο ISO/IEC 18013-5 ισχύουν επίσης όταν το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ λαμβάνει αίτημα προσκόμισης ISO/IEC mdoc μέσω μεσολαβούμενου από API μηχανισμού διαβίβασης όπως ορίζεται στο σημείο Γ.1 του [16].»