ΠΑΡΑΡΤΗΜΑ ΙΙΙ

Ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών και επιχειρήσεων σε ψηφιακές υπηρεσίες του δημόσιου τομέα.

1. Ταυτοποίηση και αυθεντικοποίηση

Η ταυτοποίηση και η αυθεντικοποίηση για την πρόσβαση σε ψηφιακές δημόσιες υπηρεσίες αποσκοπούν στην ενίσχυση της ασφάλειας και της εμπιστοσύνης των πολιτών στο ψηφιακό κράτος. Οι διαδικασίες αυτές περιλαμβάνουν τη χρήση συστημάτων ηλεκτρονικής ταυτοποίησης, που διασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε δεδομένα και υπηρεσίες, όταν υπάρχει απαίτηση εξουσιοδοτημένης πρόσβασης. Οι νόμοι και οι κανονισμοί που διέπουν την ψηφιακή διακυβέρνηση υποστηρίζουν τη λειτουργία αυτών των διαδικασιών, προκειμένου να διασφαλιστεί η προστασία των προσωπικών πληροφοριών, των πληροφοριών που χρήζουν προστασίας και η συμμόρφωση με διεθνείς προδιαγραφές ασφάλειας.

Η παροχή ψηφιακών δημοσίων υπηρεσιών και η ανταπόκριση σε αιτήματα φυσικών ή νομικών προσώπων ή νομικών οντοτήτων που περιλαμβάνει:

- διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ φορέων του δημόσιου τομέα,
- διασύνδεση ηλεκτρονικών αρχείων ή βάσεων δεδομένων με προστατευμένα δεδομένα, που τηρούνται από φορείς του δημόσιου τομέα,
- πλήρως αυτοματοποιημένο τρόπο επεξεργασίας με την υποστήριξη πληροφοριακών συστημάτων και βάσεων δεδομένων,

πραγματοποιείται με τήρηση των προϋποθέσεων και εγγυήσεων των κατωτέρω:

του Κανονισμού (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),

του ν. 4624/2019 (Α΄ 137) «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.»,

του ν. 4727/2020 (Α' 184) «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.» και

του άρθρου 11 «Τεχνικά μέτρα προστασίας σχετικά με τη μη εγκεκριμένη χρήση ή κοινολόγηση δεδομένων» του Κανονισμού (ΕΕ) 2023/2854[1] για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους και για

[1] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L_202302854

την τροποποίηση του Κανονισμού (ΕΕ) 2017/2394[2] και της Οδηγίας (ΕΕ) 2020/1828[3] (Κανονισμός για τα δεδομένα).

Κατά την ανταλλαγή επίσημων πληροφοριών από δημόσιους φορείς, τα δεδομένα θα πρέπει να διακινούνται μέσω ασφαλών και ελεγχόμενων καναλιών επικοινωνίας τα οποία, κατά περίπτωση, εξασφαλίζουν τα ακόλουθα:

- ότι οι συμμετέχοντες έχουν ταυτοποιηθεί και ότι έχει επαληθευτεί η ταυτότητά τους με τη χρήση συμφωνημένων διαδικασιών και μηχανισμών,
- ότι τα δεδομένα είναι κρυπτογραφημένα, ώστε να διασφαλίζεται, όπου αυτό κρίνεται απαραίτητο από τη διαβάθμισή τους ή από την κείμενη νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα, η εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται,
- ότι η ακεραιότητα και η πηγή των δεδομένων ελέγχονται για επιθέσεις προσπάθειας αλλοίωσης των πληροφοριών,
- ότι οι ενέργειες καταγράφονται, εξασφαλίζοντας έτσι τη δυνατότητα διενέργειας ελέγχων.

Για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας, της μη αποποίησης συμμετοχής σε συναλλαγές, και της εξακρίβωσης της ταυτότητας της πηγής αρχείων, θα πρέπει να γίνεται χρήση εγκεκριμένων υπηρεσιών εμπιστοσύνης, σύμφωνα με τον Ευρωπαϊκό Κανονισμό για την ηλεκτρονική ταυτοποίηση και την κείμενη νομοθεσία[4].

Η ταυτοποίηση και αυθεντικοποίηση (έλεγχος της ταυτότητας) των συναλλασσόμενων πολιτών και επιχειρήσεων αποτελούν βασικές προϋποθέσεις για την εξυπηρέτησή τους στα πλαίσια μιας ηλεκτρονικής συναλλαγής. Για τη διασφάλιση της ασφαλούς πρόσβασης σε υπηρεσίες και δεδομένα, απαιτείται η αξιοποίηση υπηρεσιών επιβεβαίωσης της ταυτότητας των συναλλασσόμενων με ψηφιακά μέσα. Στόχος του συγκεκριμένου δομικού στοιχείου διαλειτουργικότητας, που αφορά στην ταυτοποίηση χρηστών και υλοποιείται από το Κέντρο Ταυτοποίησης του Κέντρου Διαλειτουργικότητας (ΚΕΔ), είναι η αξιοποίηση των υποδομών του δημόσιου και ιδιωτικού τομέα για την παροχή κοινόχρηστων υπηρεσιών ηλεκτρονικής ταυτοποίησης, μέσα από ένα ενιαίο πλαίσιο προδιαγραφών ασφάλειας.

Σύμφωνα με τη **Βίβλο Ψηφιακού Μετασχηματισμού 2020-2025**[5] το δομικό στοιχείο της ηλεκτρονικής ταυτοποίησης του ΚΕΔ θα αξιοποιείται από την Ενιαία Ψηφιακή Πύλη-gov.gr και από το Κέντρο Ειδοποιήσεων, παρέχοντας υπηρεσία μοναδικού σημείου ταυτοποίησης (Single Sign-On) σε όλες τις ψηφιακές υπηρεσίες που διατίθενται μέσω του gov.gr. Παράλληλα πρέπει να προβλέπεται να διαμορφωθεί πλαίσιο αξιοποίησης των σχετικών υπηρεσιών ταυτοποίησης και από συστήματα του ιδιωτικού τομέα.

Σε ό,τι αφορά στα Νομικά Πρόσωπα Ιδιωτικού και Δημοσίου Δικαίου, η ιδιαιτερότητά τους έγκειται στο γεγονός ότι δεν έχουν φυσική υπόσταση και όλες τους οι συναλλαγές πραγματοποιούνται μέσω νομίμως εξουσιοδοτημένων εκπροσώπων και ειδικών κωδικών που αποδίδονται μέσα από ενέργειες του νόμιμου ή εξουσιοδοτημένου εκπροσώπου του Νομικού Προσώπου[6]. Στις ηλεκτρονικά προσφερόμενες υπηρεσίες, η ταυτοποίηση των Νομικών Προσώπων γίνεται μέσω των νομίμως εξουσιοδοτημένων εκπροσώπων, οι οποίοι ενεργούν για

[2] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32017R2394
[3] https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:32020L1828
[4] ΚΑΝΟΝΙΣΜΌΣ (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 (όπως ισχύει) ΚΕΦΑΛΑΙΟ Θ΄ ΥΠΗΡΕΣΙΕΣ ΕΜΠΙΣΤΟΣΥΝΗΣ Ν.4727/2020
[5] https://digitalstrategy.gov.gr/
[6] https://www.aade.gr/sites/default/files/2024-10/manual_afm_kleidarithmos_v.2.pdf

λογαριασμό του φορέα.

[Κ.1] Σε εθνικό επίπεδο, όταν οι υπηρεσίες απαιτούν εξουσιοδοτημένη πρόσβαση, οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ ταυτοποιούν τους χρήστες με έναν από τους ακόλουθους τρόπους[7]:

1. Με τη χρήση των κωδικών-διαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, όπως περιγράφεται στο άρθρο 84, παρ.1 του ν. 4727/2020.
2. Με τη χρήση των κωδικών-διαπιστευτηρίων των συστημάτων ηλεκτρονικής τραπεζικής (e-banking) των πιστωτικών ιδρυμάτων όπως ορίζονται στο στοιχείο 1 της παρ. 1 του άρθρου 4 του Κανονισμού (ΕΕ) 2013/575 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 (ΕΕ L 176), περιλαμβανομένων των υποκαταστημάτων τους, όπως ορίζονται στο στοιχείο 17 της παρ. 1 του άρθρου 4 του εν λόγω Κανονισμού, όταν τα υποκαταστήματα αυτά βρίσκονται στην Ελλάδα είτε η έδρα τους βρίσκεται εντός της Ευρωπαϊκής Ένωσης, είτε σύμφωνα με το άρθρο 36 του ν. 4261/2014 (Α΄ 107) σε τρίτη χώρα, του Ταμείου Παρακαταθηκών και Δανείων, καθώς και των ιδρυμάτων ηλεκτρονικού χρήματος και των ιδρυμάτων πληρωμών όπως ορίζονται στο άρθρο 1 του ν. 4537/2018 (Α΄ 84).
3. Με τη χρήση εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής[8].

Οι δημόσιοι φορείς για τον σκοπό αυτό ΠΡΕΠΕΙ ΝΑ εφαρμόζουν:

α) την Υ.Α. 10238 ΕΞ2020 «Αυθεντικοποίηση Χρηστών για τη χρήση των ηλεκτρονικών υπηρεσιών της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης είτε μέσω των διαπιστευτηρίων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων της Δημόσιας Διοίκησης είτε μέσω των διαπιστευτηρίων των Πιστωτικών Ιδρυμάτων» (Β΄ 1611),
β) την Υ.Α. 29810 ΕΞ2020 «Διαδικασία αυθεντικοποίησης υπαλλήλων του δημόσιου τομέα σε ψηφιακές δημόσιες υπηρεσίες» (Β' 4798)

2. Ταυτοποίηση και αυθεντικοποίηση σε διασυνοριακό επίπεδο

Η διασυνοριακή ταυτοποίηση των χρηστών πρέπει να εξασφαλίζεται με πρότυπα διαλειτουργικότητας, όπως αυτά έχουν καθοριστεί στον Ευρωπαϊκό Κανονισμό για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης (ΕΕ) 2014/910 και ιδίως:

α) τον Εκτελεστικό κανονισμό της επιτροπής (ΕΕ) 2015/1501 για το πλαίσιο διαλειτουργικότητας σύμφωνα με το άρθρο 12 παράγραφος 8 του Κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.

β) την τροποποίησή του Κανονισμού (ΕΕ) 2014/910, όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα από τον (ΕΕ) 2024/1183 και

[7] άρθρο 24 Ν. 4727/2020.
[8] Ν. 4727/2020 ΚΕΦΑΛΑΙΟ Θ΄ ΥΠΗΡΕΣΙΕΣ ΕΜΠΙΣΤΟΣΥΝΗΣ

γ) τον Κανονισμό (ΕΕ) 2018/1724 (Single Digital Gateway-SDG)[9] και ειδικότερα τον Εκτελεστικό Κανονισμό (ΕΕ) 2022/1463 για τον καθορισμό των τεχνικών και λειτουργικών προδιαγραφών του τεχνικού συστήματος διασυνοριακής αυτοματοποιημένης ανταλλαγής δικαιολογητικών και την εφαρμογή της αρχής «μόνον άπαξ».

Τα επίπεδα διασφάλισης θα πρέπει να χαρακτηρίζουν τον βαθμό εμπιστοσύνης ενός μέσου ηλεκτρονικής ταυτοποίησης, όσον αφορά την εξακρίβωση της ταυτότητας ενός προσώπου, βεβαιώνοντας με τον τρόπο αυτόν ότι το πρόσωπο που επικαλείται συγκεκριμένη ταυτότητα είναι στην πραγματικότητα το πρόσωπο στο οποίο έχει αποδοθεί η ταυτότητα αυτή. Το επίπεδο διασφάλισης εξαρτάται από τον βαθμό εμπιστοσύνης που παρέχει το μέσο ηλεκτρονικής ταυτοποίησης όσον αφορά στην ταυτότητα την οποία επικαλείται ή δηλώνει ένα πρόσωπο, λαμβανομένων υπόψη των διαδικασιών (για παράδειγμα, απόδειξη ταυτότητας και εξακρίβωση και επαλήθευση ταυτότητας), των δραστηριοτήτων διαχείρισης (για παράδειγμα, την οντότητα που εκδίδει τα μέσα ηλεκτρονικής ταυτοποίησης και τη διαδικασία έκδοσης των μέσων αυτών) και των πραγματοποιούμενων τεχνικών ελέγχων.

Σύμφωνα με τον Εκτελεστικό Κανονισμό (ΕΕ) 2015/1502[10] της Επιτροπής (8-9-2015) τα επίπεδα διασφάλισης (Levels of Assurance) των μέσων ηλεκτρονικής ταυτοποίησης είναι:

i. Χαμηλό (Low)
ii. Βασικό (Substantial)
iii. Υψηλό (High)

Οι ελάχιστες τεχνικές προδιαγραφές και διαδικασίες για τα ανωτέρω επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης καθορίζονται στο Παράρτημα του Εκτελεστικού Κανονισμού (ΕΕ) 2015/1502 της Επιτροπής, της 8ης Σεπτεμβρίου 2015, σχετικά με τη θέσπιση ελάχιστων τεχνικών προδιαγραφών και διαδικασιών για τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης σύμφωνα με το άρθρο 8 παράγραφος 3 του Κανονισμού (ΕΕ) αριθ. 2014/910 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.

Κάθε φορέας πάροχος υπηρεσιών Δημοσίου, θα πρέπει να προσδιορίσει για κάθε παρεχόμενη υπηρεσία και πρόσβαση σε δεδομένα, το κατάλληλο επίπεδο διασφάλισης των αποδεκτών μέσων ηλεκτρονικής ταυτοποίησης. Στα στοιχεία που πρέπει να ληφθούν υπόψη για την επιλογή του κατάλληλου επιπέδου διασφάλισης περιλαμβάνεται και το είδος των δεδομένων στα οποία αφορά η παρεχόμενη υπηρεσία στην οποία παρέχεται πρόσβαση και η απαίτηση προστασίας των δεδομένων, σύμφωνα με την κείμενη εθνική και ευρωπαϊκή νομοθεσία.
Για τον προσδιορισμό του επιπέδου διασφάλισης, ο φορέας θα πρέπει να προσδιορίσει τα δεδομένα που επεξεργάζεται η υπηρεσία και να τα κατατάξει σε μια από τις παρακάτω κατηγορίες εμπιστοσύνης:

- Επίπεδο εμπιστοσύνης υψηλό, όπως αυτά που αφορούν σε εμπορικό απόρρητο, επιχειρηματικό, επαγγελματικό και εταιρικό απόρρητο, στατιστικό απόρρητο, δικαιώματα διανοητικής ιδιοκτησίας τρίτων, ευαίσθητα προσωπικά δεδομένα (όπως για παράδειγμα στοιχεία που αφορούν το ποινικό μητρώο ενός χρήστη ή δεδομένα υγείας) κλπ. – προβλέπονται ρητά από τη νομοθεσία), τα οποία εντάσσονται στο υψηλό επίπεδο διασφάλισης

[9] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32018R1724
[10] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015R1502

- Επίπεδο εμπιστοσύνης μέτριο, που αφορά κυρίως προσωπικά δεδομένα, που δεν είναι χαρακτηρισμένα ως ευαίσθητα βάσει του ν. 4624/2019, τα οποία προστατεύονται (κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως σε όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου) και εντάσσονται στο βασικό επίπεδο διασφάλισης

- Επίπεδο εμπιστοσύνης μέτριο όπως π.χ. τα οικονομικά δεδομένα (που αφορούν σε συναλλαγές, σε φορολογικό απόρρητο ή σε στοιχεία φορολογούμενου κλπ), τα οποία εντάσσονται είτε στο υψηλό επίπεδο διασφάλισης, είτε στο βασικό, ανάλογα με το άν προστατεύονται από συγκεκριμένο νομοθέτημα ή προσδιορίζεται σημαντική επίπτωση από ενδεχόμενο περιστατικό ασφαλείας ή όχι

- Απλά – (δεδομένα που δεν εμπίπτουν σε κάποια από τις παραπάνω κατηγορίες ή δεν προστατεύονται με κάποια άλλη διάταξη), τα οποία μπορούν να ενταχθούν στο χαμηλό επίπεδο διασφάλισης.

Το επίπεδο διασφάλισης για την πρόσβαση σε κάποια υπηρεσία είναι το υψηλότερο επίπεδο των εμπλεκόμενων δεδομένων ή υπηρεσιών, σύμφωνα με τη ροή της διαδικασίας για την παροχή της εν λόγω υπηρεσίας. Για παράδειγμα εάν για την ολοκληρωμένη παροχή μιας υπηρεσίας διακινούνται δεδομένα που εντάσσονται στο υψηλό επίπεδο διασφάλισης ή καλούνται (καταναλώνονται) υπηρεσίες που απαιτούν υψηλό επίπεδο διασφάλισης, τότε και η εν λόγω υπηρεσία εντάσσεται στο υψηλό επίπεδο διασφάλισης, ως προς την πρόσβασή της.

[Κ.2]	Όταν οι υπηρεσίες απαιτούν εξουσιοδοτημένη πρόσβαση, οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ αποφασίζουν και να κοινοποιούν το ελάχιστο επίπεδο διασφάλισης ήτοι α) Χαμηλό (Low), β) Βασικό (Substantial), γ)Υψηλό (High) που απαιτείται για την πρόσβαση και την παροχή της υπηρεσίας, σύμφωνα με τις απαιτήσεις του νομοθετικού πλαισίου και το είδος των δεδομένων που χειρίζονται.

[Κ.3]	Για τις διασυνοριακές συναλλαγές, όταν οι υπηρεσίες απαιτούν εξουσιοδοτημένη πρόσβαση, οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ ελέγχουν ότι οι χρήστες χρησιμοποιούν κοινοποιημένα μέσα ηλεκτρονικής ταυτοποίησης που καλύπτουν το ελάχιστο επίπεδο διασφάλισης που έχουν αποφασίσει για την πρόσβαση στην υπηρεσία και εκδίδονται στο πλαίσιο των κοινοποιημένων σχεδίων ηλεκτρονικής ταυτοποίησης, σύμφωνα με το άρθρο 8 του κανονισμού (ΕΕ) αριθ. 910/2014.

Για την επιλογή του επιπέδου διασφάλισης για την πρόσβαση σε υπηρεσία και δεδομένα, λαμβάνεται υπόψη και η ανάλυση κινδύνου σχετικά με τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των δεδομένων. Εκπονείται ως τμήμα της συνολικής ανάλυσης κινδύνου που οφείλει να εκπονεί κάθε δημόσιος οργανισμός, στο πλαίσιο της συνολικής οργανωσιακής προσέγγισης διαχείρισης του κινδύνου που σχετίζεται με τη λειτουργία και τη χρήση πληροφοριακών συστημάτων. Αναλυτικά τα θέματα ανάλυσης και διαχείρισης κινδύνου παρουσιάζονται στο Εγχειρίδιο Κυβερνοασφάλειας[11], που εκπονήθηκε από την Εθνική Αρχή Κυβερνοασφάλειας. Ειδικότερα, στην ενότητα 5 του Εγχειριδίου Κυβερνοασφάλειας, παρουσιάζονται τα ζητήματα αυθεντικοποίησης χρηστών και τα προτεινόμενα μέτρα

[11] https://cyber.gov.gr/wp-content/uploads/2024/12/Εγχειρίδιο-Κυβερνοασφάλειας-Ελληνική-έκδοση.pdf

προστασίας, όπως η εφαρμογή αυθεντικοποίησης δύο παραγόντων (2-factor authentication) για κάθε χρήστη που επιθυμεί πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα και η χρήση υποδομής δημόσιου κλειδιού για τη διενέργεια αυθεντικοποίησης χρηστών με τη χρήση ψηφιακού πιστοποιητικού.

Κατά την επιλογή της αυθεντικοποίησης δύο παραγόντων θα πρέπει να ληφθεί υπόψη ότι η αποστολή κειμένου μέσω SMS είναι πλέον ευπαθής σε διάφορα είδη επιθέσεων, με πιο γνωστή τη μέθοδο SIM swapping. Πολύ πιο ασφαλής είναι η χρήση εφαρμογής για κινητές συσκευές, που δημιουργεί κωδικούς μιας χρήσης (one-time passwords) στη συσκευή του χρήστη, χωρίς δηλαδή ο κωδικός να μεταδίδεται μέσω δικτύου και με ό,τι κινδύνους αυτό συνεπάγεται. Γνωστά παραδείγματα τέτοιων εφαρμογών αποτελούν το Google Authenticator, Microsoft Authenticator, Aegis Authenticator, LastPass, Authy κ.α.

Ως **«Κόμβος»**[12] ορίζεται το σημείο σύνδεσης που αποτελεί μέρος της αρχιτεκτονικής της διαλειτουργικότητας της ηλεκτρονικής ταυτοποίησης και σχετίζεται με τη διασυνοριακή επαλήθευση της ταυτότητας προσώπων και το οποίο έχει την ικανότητα να αναγνωρίζει και να επεξεργάζεται ή να διαβιβάζει στοιχεία σε κόμβους άλλων χωρών, επιτρέποντας οι εθνικές υποδομές ηλεκτρονικής ταυτοποίησης ενός κράτους μέλους να διασυνδέονται με τις εθνικές υποδομές ηλεκτρονικής ταυτοποίησης άλλων κρατών μελών. Ένας κόμβος σε ένα κράτος μέλος είναι σε θέση να συνδέεται με τους κόμβους των άλλων κρατών μελών. Επίσης ως «φορέας εκμετάλλευσης κόμβου» ορίζεται ο φορέας που είναι υπεύθυνος να διασφαλίζει ότι ο κόμβος εκτελεί ορθά και αξιόπιστα τις λειτουργίες του, ως σημείου σύνδεσης, και για την περίπτωση της Ελλάδας είναι η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης.

Όταν, σύμφωνα με την εθνική νομοθεσία ή την εθνική διοικητική πρακτική, απαιτούνται ηλεκτρονική ταυτοποίηση με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης και επαλήθευση της ταυτότητας για την απόκτηση πρόσβασης σε υπηρεσία, η οποία παρέχεται επιγραμμικά από φορέα του δημόσιου τομέα σε ορισμένο κράτος μέλος, ισχύει η αρχή της αμοιβαίας αναγνώρισης, όταν το μέσο ηλεκτρονικής ταυτοποίησης το οποίο έχει εκδοθεί σε άλλο κράτος μέλος πληροί τους όρους της κοινοποίησης και η κοινοποίηση έχει δημοσιευθεί στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Μολαταύτα, η αρχή της αμοιβαίας αναγνώρισης θα πρέπει να αφορά μόνο την επαλήθευση ταυτότητας σε επιγραμμική υπηρεσία. Η υποχρέωση αναγνώρισης μέσων ηλεκτρονικής ταυτοποίησης θα πρέπει να σχετίζεται μόνο με εκείνα τα συστήματα, των οποίων το επίπεδο ασφαλούς ταυτοποίησης αντιστοιχεί ή υπερβαίνει το επίπεδο που απαιτείται για την εν λόγω επιγραμμική υπηρεσία. Επιπροσθέτως, η υποχρέωση αυτή θα πρέπει να εφαρμόζεται μόνο εφόσον ο εν λόγω φορέας του δημόσιου τομέα χρησιμοποιεί **το βασικό ή το υψηλό επίπεδο διασφάλισης** για την πρόσβαση σε αυτή την επιγραμμική υπηρεσία.

Το **δίκτυο eIDAS**[13] αποτελείται από έναν αριθμό διασυνδεδεμένων κόμβων eIDAS, ενός ανά συμμετέχουσα χώρα, οι οποίοι μπορούν είτε να ζητούν είτε να παρέχουν διασυνοριακή επαλήθευση ταυτότητας. Οι κόμβοι χρησιμοποιούν για τη σύνταξη κοινά μορφότυπα μηνυμάτων με βάση τα πρότυπα που έχουν ήδη εφαρμοστεί περισσότερες από μία φορές μεταξύ κρατών μελών, και έχει αποδειχθεί ότι λειτουργούν σε επιχειρησιακό περιβάλλον. Η σύνταξη επιτρέπει: α) ορθή επεξεργασία του ελάχιστου συνόλου δεδομένων ταυτοποίησης προσώπου που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο· β) ορθή επεξεργασία του επιπέδου διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης· γ)

[12] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015R1501

[13] https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts

διάκριση μεταξύ φορέων του δημόσιου τομέα και άλλων συμβαλλόμενων μερών· δ) ευελιξία, ώστε να καλύπτονται οι ανάγκες πρόσθετων χαρακτηριστικών που σχετίζονται με την ταυτοποίηση.

Τα βήματα μιας διαδικασίας ταυτοποίησης με χρήση του δικτύου eIDAS για την πρόσβαση σε διαδικτυακή υπηρεσία, σε υψηλό επίπεδο, είναι τα ακόλουθα[14]:

1. Ένας πολίτης ζητάει μια διαδικτυακή υπηρεσία σε ένα κράτος μέλος
2. Ο πολίτης καλείται να πιστοποιήσει την ταυτότητά του μέσω της διαδικτυακής υπηρεσίας
3. Στο στάδιο πιστοποίησης, καθίσταται σαφές ότι ο πολίτης διαθέτει eID από άλλο κράτος μέλος
4. Το αίτημα πιστοποίησης αποστέλλεται στη χώρα του πολίτη για πιστοποίηση, μέσω της λύσης eID, και συγκεκριμένα στον πάροχο ταυτότητας (IdP) του πολίτη, όπου πραγματοποιείται η πιστοποίηση
5. Το αποτέλεσμα της πιστοποίησης επιστρέφεται στον πάροχο υπηρεσιών
6. Η πιστοποίηση ολοκληρώνεται και ο πολίτης μπορεί να προχωρήσει στην πρόσβαση στην υπηρεσία.

Στοιχεία για τους διασυνδεδεμένους κόμβους στο δίκτυο κόμβων eIDAS δίνονται στο eIDAS Dashboard με ευθύνη των κρατών μελών.

[K.4]	Ο ελληνικός κόμβος eIDAS, με βάση τον εκτελεστικό κανονισμό (ΕΕ) 2015/1501 (κόμβος eIDAS), ΠΡΕΠΕΙ ΝΑ συνδέεται με τους αντίστοιχους κόμβους όλων των άλλων Κρατών Μελών.

[K.5]	Ο ελληνικός κόμβος eIDAS, με βάση τον εκτελεστικό κανονισμό (ΕΕ) 2015/1501 (κόμβος eIDAS), ΠΡΕΠΕΙ ΝΑ διασφαλίζει την ακεραιότητα και τη γνησιότητα των δεδομένων, για να εξασφαλίζεται ότι όλα τα αιτήματα και οι απαντήσεις είναι γνήσια και δεν έχουν παραποιηθεί.

[K.6]	Ο ελληνικός κόμβος eIDAS, με βάση τον εκτελεστικό κανονισμό (ΕΕ) 2015/1501 (κόμβος eIDAS), ΠΡΕΠΕΙ ΝΑ χρησιμοποιεί για τη σύνταξη κοινά μορφότυπα μηνυμάτων, με βάση τα πρότυπα που έχουν ήδη εφαρμοστεί περισσότερες από μία φορές μεταξύ κρατών μελών, και έχει αποδειχθεί ότι λειτουργούν σε επιχειρησιακό περιβάλλον. Η σύνταξη επιτρέπει: α) ορθή επεξεργασία του ελάχιστου συνόλου δεδομένων ταυτοποίησης προσώπου, που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο· β) ορθή επεξεργασία του επιπέδου διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης· γ) διάκριση μεταξύ φορέων του δημόσιου τομέα και άλλων συμβαλλόμενων μερών·

[14] https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109866/How+does+it+work

	δ) ευελιξία, ώστε να καλύπτονται οι ανάγκες πρόσθετων χαρακτηριστικών που σχετίζονται με την ταυτοποίηση.

[Κ.7]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, ως φορέας εκμετάλλευσης του κόμβου eIDAS, ΠΡΕΠΕΙ ΝΑ κοινοποιεί τα μεταδεδομένα της διαχείρισης του κόμβου με τυποποιημένο, μηχανικά επεξεργάσιμο τρόπο και με ασφαλή και αξιόπιστα μέσα.

[Κ.8]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, ως φορέας εκμετάλλευσης του κόμβου eIDAS, ΠΡΕΠΕΙ ΝΑ αποθηκεύει δεδομένα τα οποία, σε περίπτωση συμβάντος, επιτρέπουν την ανασυγκρότηση της ακολουθίας της ανταλλαγής μηνυμάτων για την επιβεβαίωση του τόπου και της φύσης του συμβάντος. Τα δεδομένα αποθηκεύονται για ένα χρονικό διάστημα σύμφωνα με τις εθνικές απαιτήσεις και αποτελούνται τουλάχιστον από τα ακόλουθα στοιχεία: α) ταυτοποίηση κόμβου β) ταυτοποίηση μηνύματος γ) ημερομηνία και ώρα μηνύματος.

[Κ.9]	Οι κόμβοι eIDAS, που παρέχουν επαλήθευση της ταυτότητας και συμμετέχουν στο πλαίσιο διαλειτουργικότητας, ΠΡΕΠΕΙ ΝΑ πληρούν αποδεδειγμένα τις απαιτήσεις του προτύπου ISO/IEC 27001 μέσω πιστοποίησης, ή μέσω ισοδύναμων μεθόδων αξιολόγησης, ή μέσω της συμμόρφωσης με την εθνική νομοθεσία.

Στοιχεία σχετικά με τον ελληνικό κόμβο eIDAS είναι, επίσης, διαθέσιμα στην ιστοσελίδα eIDAS Dashboard, με επιλεγμένη χώρα την Ελλάδα.

Στη συγκεκριμένη σελίδα δημοσιεύονται μεταξύ άλλων και τα μεταδεδομένα επικοινωνίας κάθε κόμβου eIDAS, ώστε κάθε δημόσιος φορέας που επιθυμεί τη διασυνοριακή παροχή υπηρεσίας, να επικοινωνεί, καταρχήν, με τον διαχειριστή του ελληνικού κόμβου eIDAS, ώστε να διασυνδεθεί με αυτόν.

Στην ενότητα «Operational eID connections» παρουσιάζονται οι διαθέσιμες διασυνδέσεις κάθε χώρας στο δίκτυο κόμβων eIDAS και στοιχεία για τις κατηγορίες και τα συγκεκριμένα δεδομένα που αποδέχεται και ανταλλάσει κάθε χώρα, μέσω του eIDAS κόμβου της.

Για την παροχή διασυνοριακής υπηρεσίας, ο δημόσιος φορέας θα πρέπει να ακολουθήσει την προβλεπόμενη διαδικασία, όπως θα του υποδειχθεί από τον διαχειριστή του κόμβου eIDAS, για τη διασύνδεσή του με τον ελληνικό κόμβο eIDAS, ώστε να μπορεί να αποδέχεται αιτήματα παροχής υπηρεσιών από ευρωπαίους πολίτες. Η ταυτοποίηση των ευρωπαίων πολιτών δεν θα γίνεται μέσω των διαπιστευτηρίων που προβλέπονται για την παροχή υπηρεσίας σε εθνικό επίπεδο (άρθρο 24 του ν.4727/2000), αλλά μέσω των υποχρεωτικών δεδομένων που ταυτοποιούν φυσικό ή νομικό πρόσωπο μέσω του δικτύου κόμβων eIDAS. Η διαδικασία περιλαμβάνει τη συμπλήρωση σχετικής αίτησης, η οποία θα πρέπει αρχικά να εγκριθεί από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του

Υπουργείου Ψηφιακής Διακυβέρνησης, και στη συνέχεια ρυθμίζονται τα επόμενα βήματα για την τεχνική διασύνδεση του φορέα με τον ελληνικό κόμβο eIDAS.

[Κ.10]	Οι δημόσιοι φορείς για τις ψηφιακές υπηρεσίες που έχουν χρήστες ευρωπαίους πολίτες ΠΡΕΠΕΙ ΝΑ συνδέονται στον ελληνικό κόμβο eIDAS με βάση τον Εκτελεστικό Κανονισμό (ΕΕ) 2015/1501.

[Κ.11]	Οι δημόσιοι φορείς για τις ψηφιακές υπηρεσίες που έχουν χρήστες ευρωπαίους πολίτες ΠΡΕΠΕΙ ΝΑ τις προσαρμόσουν έτσι, ώστε να είναι εφικτή η πρόσβαση σε αυτές μόνο με τα ελάχιστα στοιχεία ταυτοποίησης φυσικών και νομικών προσώπων, όπως αυτά ορίζονται στο παράρτημα του Εκτελεστικού Κανονισμού (ΕΕ) 2015/1501.

[Κ.12]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, για τις περιπτώσεις της διασυνοριακής αναγνώρισης, σύμφωνα με τα οριζόμενα στο άρθρο 11 του Εκτελεστικού Κανονισμού (ΕΕ) 2015/1502, στο ελάχιστο σύνολο δεδομένων που παρέχει για φυσικό πρόσωπο ΠΡΕΠΕΙ ΝΑ περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά: α) σημερινό/-ά επώνυμο/-α· β) σημερινό/-ά όνομα/-τα· γ) ημερομηνία γέννησης· δ) ένα μοναδικό αναγνωριστικό κωδικό κατασκευασμένο 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 στον χρόνο.

[Κ.13]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, για τις περιπτώσεις της διασυνοριακής αναγνώρισης, σύμφωνα με τα οριζόμενα στο άρθρο 11 του Εκτελεστικού Κανονισμού (ΕΕ) 2015/1502, στο ελάχιστο σύνολο δεδομένων που παρέχει για νομικό πρόσωπο ΠΡΕΠΕΙ ΝΑ περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά: α) σημερινή επωνυμία· β) ένα μοναδικό αναγνωριστικό κωδικό κατασκευασμένο 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 στον χρόνο.

[Κ.14]	Σε περίπτωση προσφυγής σε κοινοποιημένο σύστημα ηλεκτρονικής ταυτοποίησης, κατά τη διασυνοριακή αντιστοίχιση ταυτότητας φυσικών προσώπων, οι πληροφορίες που ΠΡΕΠΕΙ ΝΑ χρησιμοποιούνται για την αδιαμφισβήτητη αντιστοίχιση ταυτότητας είναι τα υποχρεωτικά χαρακτηριστικά του ελάχιστου συνόλου δεδομένων για φυσικό πρόσωπο που ορίζεται στο τμήμα 1 του παραρτήματος του Εκτελεστικού Κανονισμού (ΕΕ) 2015/1501, όπως αυτό

	ισχύει συμπεριλαμβανομένων, κατά περίπτωση, τυχόν πρόσθετων πληροφοριών ή συμπληρωματικών διαδικασιών.

3. Ταυτοποίηση και αυθεντικοποίηση με βάση το ευρωπαϊκό πλαίσιο για την ψηφιακή ταυτότητα

Ο **Κανονισμός (ΕΕ) 2024/1183**[15] αφορά στην τροποποίηση του Κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά στη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα και στη δημιουργία του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας. Σύμφωνα με τα οριζόμενα σε αυτόν, όλα τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει να δίνουν στους χρήστες τη δυνατότητα ηλεκτρονικής ταυτοποίησής τους και επαλήθευσης ταυτότητας τόσο εντός διαδικτύου, όσο και σε λειτουργία εκτός διαδικτύου σε διασυνοριακό επίπεδο για την πρόσβαση σε ευρύ φάσμα δημόσιων και ιδιωτικών υπηρεσιών. Ως **"ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας"** νοείται το μέσο ηλεκτρονικής ταυτοποίησης που επιτρέπει στον χρήστη να αποθηκεύει, να διαχειρίζεται και να επικυρώνει με ασφάλεια δεδομένα ταυτοποίησης προσώπου και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών, με σκοπό την παροχή τους σε βασιζόμενα μέρη και σε άλλους χρήστες ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, και να υπογράφει μέσω εγκεκριμένων ηλεκτρονικών υπογραφών ή να σφραγίζει μέσω εγκεκριμένων ηλεκτρονικών σφραγίδων. Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας παρέχονται στο πλαίσιο συστήματος ηλεκτρονικής ταυτοποίησης **με υψηλό επίπεδο διασφάλισης**.

[Κ.15]	Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας σύμφωνα με τον Κανονισμό (ΕΕ) 2024/1183 ΠΡΕΠΕΙ ΝΑ παρέχονται στο πλαίσιο συστήματος ηλεκτρονικής ταυτοποίησης με υψηλό επίπεδο διασφάλισης.

Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει να διαθέτουν λειτουργία με κοινό πίνακα εργαλείων, ενσωματωμένο στον σχεδιασμό, προκειμένου να διασφαλίζεται υψηλότερος βαθμός διαφάνειας, προστασίας της ιδιωτικής ζωής και ελέγχου από τους χρήστες των οικείων δεδομένων προσωπικού χαρακτήρα. Η εν λόγω λειτουργία θα πρέπει να παρέχει μια εύκολη και φιλική προς τον χρήστη διεπαφή με επισκόπηση όλων των βασιζόμενων μερών στα οποία ο χρήστης κοινοποιεί δεδομένα, συμπεριλαμβανομένων χαρακτηριστικών, καθώς και του είδους των δεδομένων που έχουν κοινοποιηθεί σε κάθε βασιζόμενο μέρος. Η λειτουργία αυτή θα πρέπει να επιτρέπει στους χρήστες να παρακολουθούν όλες τις συναλλαγές που εκτελούνται μέσω του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας, παρέχοντας τουλάχιστον τα ακόλουθα δεδομένα: ώρα και ημερομηνία της συναλλαγής, ταυτότητα αντισυμβαλλομένου, δεδομένα προσωπικού χαρακτήρα που ζητήθηκαν και δεδομένα που κοινοποιήθηκαν. Οι πληροφορίες αυτές θα πρέπει να αποθηκεύονται ακόμη και αν η συναλλαγή δεν ολοκληρώθηκε.

Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας πρέπει να είναι τεχνικώς ικανά να λαμβάνουν και να προσκομίζουν δεδομένα ταυτοποίησης προσώπου και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών σε διασυνοριακά σενάρια, χωρίς να θίγεται η διαλειτουργικότητα, και θα πρέπει να υποστηρίζουν προκαθορισμένους τύπους μορφοτύπων δεδομένων και επιλεκτική γνωστοποίηση, σύμφωνα με τα πρότυπα που αναφέρονται στα

[15] https://eur-lex.europa.eu/eli/reg/2024/1183/oj?locale=el

παραρτήματα του Εκτελεστικού Κανονισμού (ΕΕ) 2924/2979[16]. Όπως ορίζεται στον Κανονισμό (ΕΕ) αριθ. 910/2014, ως επιλεκτική γνωστοποίηση νοείται η παροχή στον ιδιοκτήτη των δεδομένων του δικαιώματος να γνωστοποιεί μόνον ορισμένα τμήματα ευρύτερου συνόλου δεδομένων, προκειμένου η λαμβάνουσα οντότητα να λαμβάνει μόνον τις αναγκαίες πληροφορίες για την παροχή υπηρεσίας που ζητεί ο χρήστης. Τα δεδομένα ταυτοποίησης προσώπου εκδίδονται σε δύο μορφότυπους:

1) μορφότυπος που καθορίζεται στο ISO/IEC 18013-5:2021·
2) «Verifiable Credentials Data Model 1.1.», σύσταση W3C, της 3ης Μαρτίου 2022.

[Κ.16]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, ως πάροχος δεδομένων ταυτοποίησης προσώπου, ΠΡΕΠΕΙ ΝΑ διασφαλίζει ότι τα δεδομένα ταυτοποίησης προσώπου παρέχονται με βάση τα πρότυπα του Εκτελεστικού Κανονισμού (ΕΕ) 2024/2979, και ιδίως με βάση τα: α) ISO/IEC 18013-5:2021, β) «Verifiable Credentials Data Model 1.1.», σύσταση W3C, της 3ης Μαρτίου 2022.

[Κ.17]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν σε ενέργειες προσαρμογής των ψηφιακών υπηρεσιών, προκειμένου να είναι σε θέση αυτές να ταυτοποιήσουν τους χρήστες με τη χρήση Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, για την, κατά περίπτωση, αποθήκευση δεδομένων ταυτότητας, διαπιστευτηρίων, επίσημων ψηφιακών εγγράφων και χαρακτηριστικών που συνδέονται με την ταυτότητα των συναλλασσόμενων, σαν ένα ξεχωριστό σχήμα ταυτοποίησης.

[Κ.18]	Δεδομένου ότι η χρήση του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας είναι προαιρετική για τους χρήστες, οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ παρέχουν στους χρήστες εναλλακτικές μεθόδους ταυτοποίησης, ώστε αυτοί να αποκτούν πρόσβαση στις υπηρεσίες που παρέχουν οι δημόσιοι φορείς, σύμφωνα με τον Εκτελεστικό Κανονισμό (ΕΕ) 2025/846 για τη διασυνοριακή αντιστοίχιση ταυτότητας φυσικών προσώπων.

[Κ.19]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, ως πάροχος δεδομένων ταυτοποίησης προσώπου, στην περίπτωση της διασυνοριακής αναγνώρισης με χρήση Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, σύμφωνα με τα οριζόμενα στο Παράρτημα «Τεχνικές προδιαγραφές για τα δεδομένα ταυτοποίησης προσώπου που αναφέρονται στο άρθρο 3 παράγραφο 3» του Εκτελεστικού Κανονισμού (ΕΕ) 2024/2977, στο ελάχιστο σύνολο δεδομένων για φυσικό πρόσωπο που παρέχει ΠΡΕΠΕΙ ΝΑ περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά: Α) επώνυμο: Τρέχον/-τα επώνυμο/-α του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου.

[16] Εκτελεστικός κανονισμός - ΕΕ - 2024/2979 - EN - EUR-Lex

	Β) όνομα: Τρέχον/-τα όνομα/-τα, συμπεριλαμβανομένου του/των μεσαίου/-ων ονόματος/-ων, κατά περίπτωση, του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου. Γ) ημερομηνία γέννησης: Ημέρα, μήνας και έτος γέννησης του χρήστη τον οποίο αφορούν τα δεδομένα ταυτοποίησης προσώπου. Δ) τόπος γέννησης: 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. Ε) ιθαγένεια: 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. Όταν μια τιμή χαρακτηριστικού δεν είναι γνωστή για το πρόσωπο ή δεν μπορεί να εκδοθεί με άλλο τρόπο ως μέρος του συνόλου δεδομένων ταυτοποίησης προσώπου, τα κράτη μέλη χρησιμοποιούν αντ' αυτής τιμή χαρακτηριστικού η οποία είναι κατάλληλη για την περίπτωση.
[Κ.20]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης, ως πάροχος δεδομένων ταυτοποίησης προσώπου, στην περίπτωση της διασυνοριακής αναγνώρισης με χρήση Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, σύμφωνα με τα οριζόμενα στο Παράρτημα «Τεχνικές προδιαγραφές για τα δεδομένα ταυτοποίησης προσώπου που αναφέρονται στο άρθρο 3 παράγραφο 3» του Εκτελεστικού Κανονισμού (ΕΕ) 2024/2977, στο ελάχιστο σύνολο δεδομένων για νομικό πρόσωπο που παρέχει ΠΡΕΠΕΙ ΝΑ περιλαμβάνει όλα τα ακόλουθα υποχρεωτικά χαρακτηριστικά: Α) σημερινή επωνυμία· Β) 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 στον χρόνο Όταν ένα στοιχείο δεδομένων δεν είναι γνωστό για το πρόσωπο ή δεν μπορεί να εκδοθεί με άλλο τρόπο ως μέρος του συνόλου δεδομένων ταυτοποίησης προσώπου, τα κράτη μέλη χρησιμοποιούν αντ' αυτής τιμή χαρακτηριστικού η οποία είναι κατάλληλη για την περίπτωση.
[Κ.21]	Σε περίπτωση προσφυγής σε Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας, κατά τη διασυνοριακή αντιστοίχιση ταυτότητας φυσικών προσώπων, οι πληροφορίες που ΠΡΕΠΕΙ ΝΑ χρησιμοποιούνται από τους δημόσιους φορείς για την αδιαμφισβήτητη αντιστοίχιση ταυτότητας είναι τα υποχρεωτικά δεδομένα ταυτοποίησης προσώπου, που ορίζονται στο τμήμα 1 του Παραρτήματος του Εκτελεστικού Κανονισμού (ΕΕ) 2024/2977, όπως αυτός ισχύει, μαζί με τυχόν προαιρετικά δεδομένα που απαιτούνται, προκειμένου να διασφαλιστεί ότι το σύνολο δεδομένων που παρουσιάζεται είναι μοναδικό, συμπεριλαμβανομένων, κατά περίπτωση, πρόσθετων πληροφοριών ή συμπληρωματικών διαδικασιών.

Η δημιουργία ειδικών ψευδωνύμων για τα βασιζόμενα στα ευρωπαϊκά ψηφιακά πορτοφόλια μέρη, θα πρέπει να παρέχει στους χρήστες του πορτοφολιού τη δυνατότητα να ταυτοποιούνται χωρίς να παρέχουν περιττές πληροφορίες στα βασιζόμενα στο ευρωπαϊκό ψηφιακό πορτοφόλι μέρη. Όπως ορίζεται στον Κανονισμό (ΕΕ) αριθ. 910/2014, οι χρήστες ευρωπαϊκών ψηφιακών πορτοφολιών δεν πρέπει να παρεμποδίζονται από την πρόσβαση σε υπηρεσίες με ψευδώνυμο, όταν δεν υπάρχει νομική απαίτηση νομικής ταυτότητας για επαλήθευση ταυτότητας. Ως εκ τούτου, αυτά πρέπει να περιλαμβάνουν μια λειτουργία για τη δημιουργία ψευδωνύμων που επιλέγονται και τελούν υπό τη διαχείριση του χρήστη, για την επαλήθευση ταυτότητας κατά την πρόσβαση σε επιγραμμικές υπηρεσίες.

Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει να είναι ασφαλή εκ σχεδιασμού και να εφαρμόζουν προηγμένα χαρακτηριστικά ασφάλειας για την προστασία από την κλοπή ταυτότητας και άλλων δεδομένων, την άρνηση υπηρεσίας και κάθε άλλη κυβερνοαπειλή. Η ασφάλεια αυτή θα πρέπει να περιλαμβάνει προηγμένες μεθόδους κρυπτογράφησης και αποθήκευσης που είναι προσβάσιμες και μπορούν να αποκρυπτογραφηθούν μόνον από τον χρήστη και βασίζονται σε διατερματικά κρυπτογραφημένη επικοινωνία με άλλα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας και βασιζόμενα μέρη. Επιπλέον, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει να απαιτούν ασφαλή, ρητή και ενεργό επιβεβαίωση των χρηστών για τις λειτουργίες που εκτελούνται μέσω αυτών.

Κάθε κράτος μέλος θα πρέπει να παρέχει τουλάχιστον ένα Ψηφιακό Πορτοφόλι εντός 24 μηνών από την έναρξη ισχύος των εκτελεστικών πράξεων του Κανονισμού (ΕΕ) 2024/1183.
Ως "βασιζόμενο μέρος" νοείται κάθε φυσικό ή νομικό πρόσωπο που βασίζεται σε ηλεκτρονική ταυτοποίηση, ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας ή άλλα μέσα ηλεκτρονικής ταυτοποίησης, ή σε υπηρεσία εμπιστοσύνης. Κάθε αίτημα από το βασιζόμενο μέρος προς χρήστη ευρωπαϊκού πορτοφολιού ψηφιακής ταυτοποίησης για παροχή πληροφοριών θα πρέπει να είναι αναγκαίο και αναλογικό προς την προβλεπόμενη χρήση σε κάθε δεδομένη περίπτωση, θα πρέπει να συνάδει με την αρχή της ελαχιστοποίησης των δεδομένων και θα πρέπει να διασφαλίζει τη διαφάνεια όσον αφορά στα δεδομένα που ανταλλάσσονται και τους σκοπούς για τους οποίους ανταλλάσσονται. Όταν ένα βασιζόμενο μέρος προτίθεται να βασίζεται σε ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας για την παροχή δημόσιων ή ιδιωτικών υπηρεσιών μέσω ψηφιακής αλληλεπίδρασης, το βασιζόμενο μέρος καταχωρίζεται στο κράτος μέλος στο οποίο είναι εγκατεστημένο, ακολουθώντας την προβλεπόμενη στο άρθρο 5β του Κανονισμού (ΕΕ) 2024/1183, διαδικασία.

[K.22]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν σε ενέργειες για την καταχώρησή τους σε ένα Εθνικό Μητρώο Βασιζόμενων σε πορτοφόλι μερών, σύμφωνα με τις απαιτήσεις του Εκτελεστικού Κανονισμού (ΕΕ) 2025/848[17]. Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ πραγματοποιούν ενημέρωση, χωρίς καθυστέρηση, σχετικά με τυχόν αλλαγές στις πληροφορίες που παρέχονται στην καταχώρηση.

Τα κράτη μέλη, όταν ενεργούν ως βασιζόμενα μέρη για διασυνοριακές υπηρεσίες, εξασφαλίζουν αδιαμφισβήτητη αντιστοίχιση ταυτότητας για τα φυσικά πρόσωπα που χρησιμοποιούν κοινοποιημένα μέσα ηλεκτρονικής ταυτοποίησης ή ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας. Επίσης, προβλέπουν τεχνικά και οργανωτικά μέτρα για τη διασφάλιση υψηλού επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται για την αντιστοίχιση ταυτότητας, και για την πρόληψη της κατάρτισης προφίλ των χρηστών.

[17] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=OJ:L_202500848

Όταν η ηλεκτρονική ταυτοποίηση με τη χρήση μέσου ηλεκτρονικής ταυτοποίησης και επαλήθευσης ταυτότητας απαιτείται βάσει του εθνικού δικαίου για την πρόσβαση σε επιγραμμική υπηρεσία που παρέχεται από φορέα του δημόσιου τομέα, τα δεδομένα ταυτοποίησης προσώπου στην ηλεκτρονική βεβαίωση χαρακτηριστικών δεν υποκαθιστούν την ηλεκτρονική ταυτοποίηση με τη χρήση μέσου ηλεκτρονικής ταυτοποίησης και την επαλήθευση ταυτότητας για την ηλεκτρονική ταυτοποίηση, εκτός εάν αυτό επιτρέπεται ρητά από το κράτος μέλος. Στην περίπτωση αυτή, γίνεται, επίσης, δεκτή εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών από άλλα κράτη μέλη. Ως "ηλεκτρονική βεβαίωση χαρακτηριστικών" νοείται η βεβαίωση σε ηλεκτρονική μορφή που επιτρέπει την επαλήθευση της γνησιότητας των χαρακτηριστικών, σύμφωνα με τα οριζόμενα στον Κανονισμό (ΕΕ) 2024/1183. Οι τεχνικές προδιαγραφές για την υλοποίηση του Κανονισμού αποτυπώνονται στο Αρχιτεκτονικό Πλαίσιο Αναφοράς (Architecture Reference Framework - ARF), και συνοδεύονται από μία υλοποίηση αναφοράς (Reference Implementation).Επίσης, οι Εκτελεστικοί Κανονισμοί (Implementation Acts (IAs)) ορίζουν τις νομικές απαιτήσεις για τις βασικές λειτουργίες του πορτοφολιού EUDI (https://github.com/eu-digital-identity-wallet).

[K.23]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν σε ενέργειες προσαρμογής των ψηφιακών υπηρεσιών, προκειμένου αυτές να είναι σε θέση να ταυτοποιήσουν τους χρήστες με τη χρήση Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, με βάση τον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2977, όσον αφορά τα δεδομένα ταυτοποίησης προσώπου και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών και του Εκτελεστικού Κανονισμού (ΕΕ) 2025/846, όσον αφορά τη διασυνοριακή αντιστοίχιση ταυτότητας φυσικών προσώπων.

Ακολούθως αναφέρονται επιγραμματικά οι ρόλοι του οικοσυστήματος του Ευρωπαϊκού Ψηφιακού Πορτοφολιού, με τους όρους που χρησιμοποιούνται στον Κανονισμό (ως Πορτοφόλι, νοείται το Ευρωπαϊκό Ψηφιακό Πορτοφόλι):

1. Χρήστες Μονάδων Πορτοφολιού (Users of Wallet Units)[18]

Οι χρήστες του Ευρωπαϊκού Ψηφιακού Πορτοφολιού χρησιμοποιούν τη Μονάδα Πορτοφολιού για να λαμβάνουν, να αποθηκεύουν και να παρουσιάζουν δεδομένα ταυτοποίησης προσώπου (PID), εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (QEAA), δημόσιες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (PuB-EAA), ή μη εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (EAA) στα βασιζόμενα μέρη.

2. Πάροχοι Πορτοφολιού (Wallet Providers)[19]

Πάροχοι Πορτοφολιού είναι κράτη μέλη ή οργανισμοί και παρέχουν Λύσεις Πορτοφολιού στους Χρήστες. Όλες οι Λύσεις Πορτοφολιού πρέπει να είναι πιστοποιημένες. Ένας Πάροχος Πορτοφολιού διαθέτει έναν συνδυασμό διαφόρων προϊόντων και Υπηρεσιών Εμπιστοσύνης σε έναν Χρήστη, οι οποίες παρέχουν στον Χρήστη τον αποκλειστικό έλεγχο της χρήσης των δεδομένων ταυτοποίησης προσώπου (PID) και των Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών (QEAA, PuB-EAA ή EAA), καθώς και οποιονδήποτε άλλων προσωπικών δεδομένων εντός της Μονάδας Πορτοφολιού του Χρήστη.

[18] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#32-users-of-wallet-units

[19] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#33-wallet-providers

Οι Πάροχοι Πορτοφολιού είναι υπεύθυνοι για τη διασφάλιση της συμμόρφωσης με τις απαιτήσεις του Κανονισμού για τις Λύσεις Πορτοφολιού και, από την άποψη των άλλων παραγόντων στο οικοσύστημα Πορτοφολιών EUDI, είναι υπεύθυνοι για όλα τα στοιχεία της Μονάδας Πορτοφολιού.

[K.24]	Οι πάροχοι ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας ΠΡΕΠΕΙ ΝΑ μεριμνούν ώστε αυτά να είναι τεχνικώς ικανά να λαμβάνουν και να προσκομίζουν δεδομένα ταυτοποίησης προσώπου και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών σε διασυνοριακά σενάρια χωρίς να θίγεται η διαλειτουργικότητα και θα ΠΡΕΠΕΙ ΝΑ υποστηρίζουν προκαθορισμένους τύπους μορφοτύπων δεδομένων και επιλεκτική γνωστοποίηση.

[K.25]	Οι πάροχοι ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας ΠΡΕΠΕΙ ΝΑ μεριμνούν ώστε τα πρωτόκολλα επικοινωνίας και οι τεχνικές προδιαγραφές να συμβαδίζουν με τον Κανονισμό (ΕΕ) 2024/1183[20] και τα σχετικά προβλεπόμενα και εγκεκριμένα στο Αρχιτεκτονικό Πλαίσιο Αναφοράς (ARF), στην υλοποίηση αναφοράς, καθώς, επίσης, και με τους σχετικούς Εκτελεστικούς Κανονισμούς (Implementation Acts (IAs)) που ορίζουν τις νομικές απαιτήσεις για τις βασικές λειτουργίες του πορτοφολιού EUDI (https://github.com/eu-digital-identity-wallet) και κάθε μεταγενέστερη επικαιροποίησή τους.

3. Πάροχοι Δεδομένων Ταυτοποίησης Προσώπου (Person Identification Data (PID) Providers)[21]

Οι Πάροχοι Δεδομένων Ταυτοποίησης Προσώπου (PID) είναι αξιόπιστες οντότητες που είναι υπεύθυνες για την επαλήθευση της ταυτότητας του Χρήστη, σύμφωνα με τις απαιτήσεις του υψηλού επιπέδου διασφάλισης, την έκδοση Δεδομένων Ταυτοποίησης Προσώπου (PID) στη Μονάδα Πορτοφολιού και τη διάθεση, με τρόπο που να διασφαλίζει την ιδιωτικότητα, πληροφοριών στα Βασιζόμενα Μέρη, για την επαλήθευση της εγκυρότητας των Δεδομένων Ταυτοποίησης Προσώπου. Οι όροι και οι προϋποθέσεις αυτών των υπηρεσιών καθορίζονται από κάθε Κράτος Μέλος. Οι Πάροχοι Δεδομένων Ταυτοποίησης Προσώπου μπορεί να είναι οι ίδιοι οργανισμοί που σήμερα εκδίδουν επίσημα έγγραφα ταυτότητας, ηλεκτρονικά μέσα ταυτότητας κ.λπ.

4. Πάροχοι Καταλόγου Παρόχων Εμπιστοσύνης (Trusted List Providers (TLP))[22]

Οι Πάροχοι Καταλόγου Εμπιστοσύνης είναι φορείς υπεύθυνοι για τη διατήρηση, τη διαχείριση και τη δημοσίευση καταλόγων εμπιστοσύνης. Εντός του οικοσυστήματος του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, υπάρχουν Λίστες Αξιόπιστης Πιστοποίησης για οντότητες όπως: Πάροχοι Πορτοφολιού, Πάροχοι Δεδομένων Ταυτοποίησης Προσώπου, Αρχές Πιστοποίησης Πρόσβασης κ.ά.

[20] https://www.european-digital-identity-regulation.com/
[21] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#34-person-identification-data-pid-providers
[22] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#35-trusted-list-provider

[K.26]	Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ΠΡΕΠΕΙ ΝΑ διαχειρίζεται και να δημοσιεύει τους Καταλόγους Παρόχων Εμπιστοσύνης σύμφωνα με τις απαιτήσεις του Κανονισμού (ΕΕ) 2024/1183 και του Εκτελεστικού Κανονισμού (ΕΕ) 2025/1572 της Επιτροπής, όσον αφορά τον μορφότυπο και τις διαδικασίες κοινοποίησης πρόθεσης και επαλήθευσης, σε σχέση με την έναρξη εγκεκριμένων υπηρεσιών εμπιστοσύνης.

5. Πάροχοι εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (Qualified Electronic Attestation of Attributes (QEAA) Providers)[23]

Οι Πάροχοι εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, διατηρούν μία διεπαφή με Μονάδες Πορτοφολιού και παρέχουν εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών κατόπιν αιτήματος. Επιπλέον, μπορούν δυνητικά να διατηρούν μία διεπαφή με αυθεντικές πηγές προς επιβεβαίωση χαρακτηριστικών.

[K.27]	Οι δημόσιοι φορείς ΣΥΝΙΣΤΑΤΑΙ ΝΑ προβούν σε ενέργειες προσαρμογής των ψηφιακών υπηρεσιών προκειμένου να παρέχουν εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (QEAA) και την επαλήθευση της αυθεντικότητας των παραπάνω χαρακτηριστικών, σύμφωνα με τις απαιτήσεις του Εκτελεστικού Κανονισμού (ΕΕ) 2025/1569.

6. Πάροχοι ηλεκτρονικής βεβαίωσης χαρακτηριστικών που εκδίδεται από ή για λογαριασμό δημόσιου φορέα υπεύθυνου για αυθεντική πηγή (Electronic Attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source (PuB-EAA) Providers)[24]

Όπως ορίζεται στον Κανονισμό για την Ευρωπαϊκή Ψηφιακή Ταυτότητα, μια βεβαίωση μπορεί να εκδοθεί από ή για λογαριασμό ενός φορέα του δημόσιου τομέα που είναι υπεύθυνος για μια Αυθεντική Πηγή. Ένας φορέας του δημόσιου τομέα είναι κυρίως μια κρατική, περιφερειακή ή τοπική αρχή ή ένας φορέας που διέπεται από το δημόσιο δίκαιο.

7. Πάροχοι μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (Non-qualified Electronic Attestation of Attributes (EAA) Providers)[25]

Μη εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (EAA) μπορούν να παρέχονται από οποιονδήποτε (μη πιστοποιημένο) Πάροχο Υπηρεσιών Εμπιστοσύνης. Ενώ θα εποπτεύονται βάσει του [Ευρωπαϊκού Κανονισμού για την Ψηφιακή Ταυτότητα], μπορεί να υποτεθεί ότι άλλα νομικά ή συμβατικά πλαίσια θα διέπουν ως επί το πλείστον τους κανόνες για την παροχή, τη χρήση και την αναγνώριση των EAA. Αυτά τα άλλα πλαίσια μπορούν να καλύπτουν τομείς πολιτικής, όπως τα εκπαιδευτικά πιστοποιητικά, οι ψηφιακές πληρωμές, αν

[23] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#36-qualified-electronic-attestation-of-attributes-qeaa-providers

[24] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#37-eaa-issued-by-or-on-behalf-of-a-public-sector-body-responsible-for-an-authentic-source-pub-eaa-providers

[25] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#38-non-qualified-electronic-attestation-of-attributes-eaa-providers

και μπορούν επίσης να βασίζονται σε Πιστοποιημένους Παρόχους Ηλεκτρονικής Βεβαίωσης Χαρακτηριστικών. Για τη χρήση μη πιστοποιημένων ΕΑΑ, οι Πάροχοι ΕΑΑ προσφέρουν στους Χρήστες έναν τρόπο να ζητούν και να λαμβάνουν αυτές τις ΕΑΑ. Αυτό σημαίνει ότι αυτοί οι μη πιστοποιημένοι Πάροχοι ΕΑΑ συμμορφώνονται με τις προδιαγραφές διεπαφής της Μονάδας Πορτοφολιού. Οι όροι και οι προϋποθέσεις έκδοσης ΕΑΑ και συναφών υπηρεσιών υπόκεινται σε τομεακούς κανόνες.

[K.28]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν σε ενέργειες προσαρμογής των ψηφιακών υπηρεσιών προκειμένου να παρέχουν δημόσιες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (PuB-EAA) και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (EAA) και την επαλήθευση της αυθεντικότητας των παραπάνω χαρακτηριστικών.

8. Πάροχοι Απομακρυσμένης Δημιουργίας Εγκεκριμένων Ηλεκτρονικών Υπογραφών (Qualified Electronic Signature Remote Creation Providers (QESRC))[26]

Η Μονάδα Πορτοφολιού θα επιτρέπει στον Χρήστη να χρησιμοποιεί εγκεκριμένες ηλεκτρονικές υπογραφές ή σφραγίδες σε οποιαδήποτε δεδομένα. Αυτό θα ενισχύσει, επίσης, τη χρήση της Μονάδας Πορτοφολιού για υπογραφή, με φυσικό και βολικό τρόπο.

9. Αυθεντικές πηγές (Authentic Sources)[27]

Οι Αυθεντικές Πηγές είναι δημόσια ή ιδιωτικά αποθετήρια ή συστήματα, αναγνωρισμένα ή απαιτούμενα από τον νόμο, που περιέχουν χαρακτηριστικά σχετικά με φυσικά ή νομικά πρόσωπα. Οι Αυθεντικές Πηγές είναι πηγές για χαρακτηριστικά, για παράδειγμα, διεύθυνση, ηλικία, φύλο, οικογενειακή κατάσταση, σύνθεση οικογένειας, ιθαγένεια, τίτλους και άδειες εκπαίδευσης και κατάρτισης, τίτλους και άδειες επαγγελματικών προσόντων, οικονομικά και εταιρικά δεδομένα κλπ. Οι Αυθεντικές Πηγές υποχρεούνται να παρέχουν μια διεπαφή στους Παρόχους εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (QEAA) για την επαλήθευση της αυθεντικότητας των παραπάνω χαρακτηριστικών, είτε άμεσα, είτε μέσω καθορισμένων μεσαζόντων που αναγνωρίζονται σε εθνικό επίπεδο.

[K.29]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν σε ενέργειες προσαρμογής των ψηφιακών υπηρεσιών και των αυθεντικών πηγών για τις οποίες είναι υπεύθυνοι, προκειμένου να παρέχουν μια διεπαφή στους Παρόχους εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (QEAA) για την επαλήθευση της αυθεντικότητας των παραπάνω χαρακτηριστικών, είτε άμεσα, είτε μέσω καθορισμένων μεσαζόντων που αναγνωρίζονται σε εθνικό επίπεδο.

10. Βασιζόμενα Μέρη και Διαμεσολαβητές (Relying Parties and intermediaries)[28]

Εντός του πεδίου εφαρμογής του αναφερόμενου Αρχιτεκτονικού Πλαισίου Αναφοράς (ARF), Βασιζόμενο Μέρος είναι ένας πάροχος υπηρεσιών που ζητά χαρακτηριστικά που περιέχονται σε ένα PID, QEAA, PuB-EAA ή EAA από τη Μονάδα Πορτοφολιού, υπό την επιφύλαξη της

[26] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#39-qualified-electronic-signature-remote-creation-qesrc-providers
[27] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#310-authentic-sources
[28] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#311-relying-parties-and-intermediaries

έγκρισης του Χρήστη και εντός των ορίων της ισχύουσας νομοθεσίας και των σχετικών κανόνων. Αποσαφηνίζεται ότι ο όρος «Βασιζόμενο Μέρος» χρησιμοποιείται σε όλα τα μέρη του ARF αποκλειστικά για να σημαίνει έναν πάροχο υπηρεσιών, που αλληλεπιδρά με μια Μονάδα Πορτοφολιού για να ζητήσει και να λάβει χαρακτηριστικά από μια βεβαίωση. Ο λόγος για τον οποίο ένα Βασιζόμενο Μέρος βασίζεται στη Μονάδα Πορτοφολιού μπορεί να είναι μια νομική απαίτηση, μια συμβατική συμφωνία ή η δική του απόφαση.

Οι λεγόμενοι «Διαμεσολαβητές» (intermediaries) αποτελούν μια ειδική κατηγορία Βασιζόμενων Μερών. Το άρθρο 5β (10) του Ευρωπαϊκού Κανονισμού Ψηφιακής Ταυτότητας ορίζει ότι «Οι Διαμεσολαβητές που ενεργούν για λογαριασμό των Βασιζόμενων Μερών θεωρούνται Βασιζόμενα Μέρη και δεν αποθηκεύουν δεδομένα σχετικά με το περιεχόμενο της συναλλαγής.». Ένας τέτοιος Διαμεσολαβητής είναι ένα μέρος που προσφέρει υπηρεσίες σε Βασιζόμενα Μέρη για να συνδεθεί, εκ μέρους τους, με Μονάδες Πορτοφολιού και να ζητήσει τα χαρακτηριστικά Χρήστη που χρειάζονται τα συγκεκριμένα Βασιζόμενα Μέρη. Στη συνέχεια, ο Διαμεσολαβητής αποστέλλει τα χαρακτηριστικά που παρουσιάζονται στο Βασιζόμενο Μέρος, για το οποίο διαμεσολάβησε. Αυτό υπονοεί ότι ένας Διαμεσολαβητής εκτελεί όλα όσα προβλέπονται στο ARF για τα Βασιζόμενα Μέρη, εκ μέρους του Βασιζόμενου Μέρους για το οποίο διαμεσολαβεί.

11. Οργανισμός Αξιολόγησης της Συμμόρφωσης (Conformity Assessment Bodies (CAB))[29]

Οι Οργανισμοί Αξιολόγησης της Συμμόρφωσης είναι δημόσιοι ή ιδιωτικοί φορείς που είναι διαπιστευμένοι από έναν εθνικό φορέα πιστοποίησης, ο οποίος ορίζεται από τα κράτη μέλη. Συγκεκριμένα, οι Οργανισμοί Αξιολόγησης της Συμμόρφωσης είναι διαπιστευμένοι για να διενεργούν αξιολογήσεις, στις οποίες θα βασίζονται τα κράτη μέλη πριν εκδώσουν μια Λύση Πορτοφολιού ή πριν παράσχουν την ιδιότητα του καταλλήλου σε έναν Πάροχο Υπηρεσιών Εμπιστοσύνης. Οι Λύσεις Πορτοφολιού θα πιστοποιούνται από τους Οργανισμούς Αξιολόγησης της Συμμόρφωσης.

[K.30]	Ο αρμόδιοι φορείς ΠΡΕΠΕΙ ΝΑ προβούν στην έκδοση Εθνικού Σχήματος Πιστοποίησης λύσεων Ευρωπαϊκών Πορτοφολιών Ψηφιακής Ταυτότητας με βάση α) τον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2981 όσον αφορά την πιστοποίηση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, β) το Ευρωπαϊκό σχήμα πιστοποίησης για Κυβερνοασφάλεια βασισμένο στα κοινά κριτήρια, γ) απαιτήσεις του ΓΚΠΔ.

[K.31]	Οι Οργανισμοί Αξιολόγησης της Συμμόρφωσης ΠΡΕΠΕΙ ΝΑ πιστοποιούν τις λύσεις Ευρωπαϊκών Πορτοφολιών Ψηφιακής Ταυτότητας με βάση το Εθνικό ή το Ευρωπαϊκό σχήμα πιστοποίησης.

12. Εποπτικές αρχές (Supervisory Bodies)[30]

Οι εποπτικές αρχές εξετάζουν την ορθή λειτουργία των Παρόχων Πορτοφολιών και άλλων φορέων στο οικοσύστημα του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας. Οι εποπτικές

[29] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reeeference-framework-main/#312-conformity-assessment-bodies-cab

[30] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#313-supervisory-bodies

αρχές θα δημιουργηθούν, θα διοριστούν και θα κοινοποιηθούν στην Ευρωπαϊκή Επιτροπή από τα κράτη μέλη.

[K.32]	Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ΠΡΕΠΕΙ ΝΑ λειτουργήσει ως Εποπτική αρχή σύμφωνα με τις απαιτήσεις του Κανονισμού (ΕΕ) 2024/1183.

13. Κατασκευαστές συσκευών και πάροχοι σχετικών υποσυστημάτων (Device Manufacturers and Related Subsystems Providers)[31]

Στο οικοσύστημα του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, παράγοντες της αγοράς, όπως οι κατασκευαστές συσκευών και οι πάροχοι σχετικών υποσυστημάτων, εκπληρώνουν τον σημαντικό ρόλο της διασφάλισης ότι μια Μονάδα Πορτοφολιού λειτουργεί ομαλά και με ασφάλεια. Οι κατασκευαστές συσκευών και οι πάροχοι σχετικών υποσυστημάτων παρέχουν μια πλατφόρμα πάνω στην οποία μπορεί να κατασκευαστεί μια Μονάδα Πορτοφολιού. Οι Πάροχοι Πορτοφολιού διασφαλίζουν ότι οι Μονάδες Πορτοφολιού τους χρησιμοποιούν αυτήν την πλατφόρμα για να διασφαλίσουν τη χρηστικότητα, την ασφάλεια, τη σταθερότητα και τη συνδεσιμότητα.

14. Πάροχοι Σχημάτων Χαρακτηριστικών (Attribute Schema Providers for QEAA, PuB-EAA and EAA) [32]

Οι Πάροχοι Σχημάτων Χαρακτηριστικών δημοσιεύουν σχήματα χαρακτηριστικών που περιγράφουν τη δομή των εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (QEAAs), των δημόσιων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (PuB-EAA) και των ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (μη εγκεκριμένων) (EAAs), συμπεριλαμβανομένων του αναγνωριστικού, της σημασιολογίας και της κωδικοποίησης όλων των χαρακτηριστικών. Αυτά τα σχήματα χαρακτηριστικών δημοσιεύονται στα Κανονιστικά Πλαίσια των Βεβαιώσεων (Attestation Rulebooks).

[K.33]	Οι δημόσιοι φορείς ΠΡΕΠΕΙ ΝΑ περιγράφουν τη δομή των δημόσιων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (PuB-EAA) και των ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (μη εγκεκριμένων) (EAAs) και να δημοσιεύουν τα Κανονιστικά Πλαίσια των Βεβαιώσεων (Attestation Rulebooks).

15. Εθνικοί Φορείς Διαπίστευσης (National Accreditation Bodies) [33]

Οι Εθνικοί Φορείς Διαπίστευσης, είναι οι φορείς των κρατών-μελών,που εκτελούν διαπίστευση με εξουσιοδότηση που προέρχεται από το κράτος μέλος. Οι Εθνικοί Φορείς Διαπίστευσης διαπιστεύουν τους Οργανισμούς Αξιολόγησης της Συμμόρφωσης ως αρμόδιους, ανεξάρτητους και εποπτευόμενους επαγγελματικούς φορείς πιστοποίησης, που είναι

[31] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#314-device-manufacturers-and-related-subsystems-providers
[32] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#315-attribute-schema-providers-for-qeaa-pub-eaa-and-eaa
[33] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#316-national-accreditation-bodies

υπεύθυνοι για την πιστοποίηση των Λύσεων Πορτοφολιού, βάσει κανονιστικών εγγράφων που καθορίζουν τις σχετικές απαιτήσεις.

16. Αρχές Πιστοποίησης Πρόσβασης (Access Certificate Authorities)[34]

Οι Αρχές Πιστοποίησης Πρόσβασης εκδίδουν πιστοποιητικό πρόσβασης σε όλους τους Παρόχους Δεδομένων Ταυτοποίησης Προσώπου (PID), τους Παρόχους Εγκεκριμένων Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών (QEAA), τους Παρόχους Δημοσίων Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών (PuB-EAA), τους Παρόχους Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών (μη εγκεκριμένων) (EAA) και στα Βασιζόμενα Μέρη, στο οικοσύστημα των Ευρωπαϊκών Πορτοφολιών Ψηφιακής Ταυτότητας (EUDI).

[K.34]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης ΠΡΕΠΕΙ ΝΑ αναπτύξει και λειτουργήσει ως Αρχή Πιστοποίησης Πρόσβασης σύμφωνα με τις απαιτήσεις του Εκτελεστικού Κανονισμού (ΕΕ) 2025/848.

Η επισκόπηση της αρχιτεκτονικής του οικοσυστήματος EUDI Wallet και των στοιχείων του παρουσιάζεται στο Αρχιτεκτονικό Πλαίσιο Αναφοράς (ARF)[35]. Οι βασικές οντότητες και οι σχέσεις στο μοντέλο εμπιστοσύνης του οικοσυστήματος EUDI Wallet παρουσιάζονται επίσης στο Αρχιτεκτονικό Πλαίσιο Αναφοράς[36].

Στον πυρήνα βρίσκεται η **Μονάδα Πορτοφολιού**, η οποία αλληλεπιδρά με διάφορες οντότητες καθ' όλη τη διάρκεια του κύκλου ζωής της. Ο κύκλος ζωής της Μονάδας Πορτοφολιού περιλαμβάνει την εγκατάσταση, την ενεργοποίηση, τη διαχείριση και την απεγκατάσταση. Κάθε Μονάδα Πορτοφολιού είναι μια διαμόρφωση μιας **Λύσης Πορτοφολιού**, που περιλαμβάνει ένα **Στιγμιότυπο Πορτοφολιού** και ένα ή περισσότερα WSCA (Wallet Secure Cryptographic Device) / WSCD (Wallet Secure Cryptographic Application), που παρέχονται από έναν **Πάροχο Πορτοφολιού**. Ο Πάροχος Πορτοφολιού επιβλέπει αυτά τα στοιχεία και διαχειρίζεται την εγγραφή, την ανάκληση ή την αναστολή τους. Ο Πάροχος Πορτοφολιού διασφαλίζει ότι μια έγκυρη Μονάδα Πορτοφολιού διαθέτει τουλάχιστον μία **Βεβαίωση Μονάδας Πορτοφολιού** (WUA), για να επιτρέψει σε άλλες οντότητες να επαληθεύσουν την ταυτότητα της Μονάδας Πορτοφολιού. Ο Πάροχος Πορτοφολιού μπορεί να ανακαλέσει τις Μονάδες Πορτοφολιού, εάν χρειαστεί.

Η Μονάδα Πορτοφολιού χειρίζεται τα Δεδομένα Ταυτοποίησης Προσώπου (PID) και τις Ηλεκτρονικές Βεβαιώσεις Χαρακτηριστικών (QEAA, PuB-EAA και μη εγκεκριμένες EAA). Τα PID εκδίδονται από τους Παρόχους PID και οι βεβαιώσεις από τους Παρόχους Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών. Πριν από την αλληλεπίδραση με μια Μονάδα Πορτοφολιού, οι Πάροχοι πρέπει να είναι εγγεγραμμένοι σε έναν Κατάλογο Παρόχων PID (**PID Provider Registrar)** ή σε ένα Κατάλογο Παρόχων Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών (**Attestation Provider Registrar)**. Κατά την εγγραφή, λαμβάνουν ένα

[34] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/#317-access-certificate-authorities
[35] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/media/Figure_2_High-Level_Architecture.jpg
[36] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/media/Figure_11_Trust_Model.jpeg

πιστοποιητικό πρόσβασης από μια Αρχή Πιστοποίησης Πρόσβασης Παρόχου PID ή μια Αρχή Πιστοποίησης Πρόσβασης Παρόχου Ηλεκτρονικών Βεβαιώσεων Χαρακτηριστικών.
Μόλις μια Μονάδα Πορτοφολιού λάβει ένα PID ή μια Ηλεκτρονική Βεβαίωση Χαρακτηριστικού, μπορεί να παρουσιάσει στοιχεία (attributes) του Χρήστη σε Στιγμιότυπο ενός Βασιζόμενου Μέρους (δεξιά πλευρά του παραπάνω σχήματος). Αυτά τα στιγμιότυπα είναι ρυθμίσεις υλικού/λογισμικού που επιτρέπουν στα Βασιζόμενα Μέρη να αλληλεπιδρούν με Μονάδες Πορτοφολιού. Τα Βασιζόμενα Μέρη εγγράφονται σε έναν Καταχωρητή και λαμβάνουν ένα πιστοποιητικό πρόσβασης για κάθε Στιγμιότυπο Βασιζόμενου Μέρους. Ένα Βασιζόμενο Μέρος μπορεί προαιρετικά να λάβει ένα ή περισσότερα πιστοποιητικά εγγραφής Βασιζόμενου Μέρους από τον Καταχωρητή.

[K.35]	Η Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης ΠΡΕΠΕΙ ΝΑ αναπτύξει και να λειτουργήσει ένα Εθνικό Μητρώο Βασιζόμενων σε πορτοφόλι μερών, σύμφωνα με τις απαιτήσεις του Εκτελεστικού Κανονισμού (ΕΕ) 2025/848.

4. Οδηγίες και κανόνες, βασισμένοι στο ισχύον νομικό – κανονιστικό πλαίσιο για την ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών και επιχειρήσεων σε ψηφιακές υπηρεσίες του δημόσιου τομέα

[K.36]	Οι δημόσιοι φορείς θα ΠΡΕΠΕΙ ΝΑ διασφαλίζουν την προστασία των συναλλαγών και των πληροφοριών με κατάλληλες συμφωνίες και με τη χρήση υπηρεσιών που παρέχονται από εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης.

[K.37]	Η διαχείριση των δεδομένων ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τον ΓΚΠΔ, και να διασφαλίζει ότι η πρόσβαση είναι περιορισμένη.

[K.38]	Η ταυτοποίηση και αυθεντικοποίηση των πολιτών από παρόχους ταυτότητας, μέσω ενιαίου κέντρου, ΠΡΕΠΕΙ ΝΑ εξασφαλίζει την εφαρμογή ενιαίου πλαισίου προδιαγραφών ασφαλείας σε εθνικό και ευρωπαϊκό επίπεδο.

[K.39]	Όλα τα δεδομένα ταυτοποίησης ΠΡΕΠΕΙ ΝΑ κρυπτογραφούνται, τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά.

[K.40]	Όλα τα αιτήματα ταυτοποίησης μεταξύ συστημάτων ΠΡΕΠΕΙ ΝΑ καταγράφονται με τρόπο που να επιτρέπει διαφάνεια και ανασκόπηση σε περίπτωση ελέγχου. Οι εξουσιοδοτημένοι υπάλληλοι και οι αρμόδιοι φορείς μπορούν να έχουν πρόσβαση σε ιστορικό ταυτοποιήσεων για λόγους διαφάνειας και ασφάλειας.

[K.41]	Στο πλαίσιο λειτουργίας του Κανονισμού (ΕΕ) 2018/1724[37] για την Ενιαία Ψηφιακή Θύρα ΠΡΕΠΕΙ ΝΑ διασφαλίζεται ότι οι διασυνοριακοί χρήστες είναι σε

[37] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R1724

	θέση να ταυτοποιούνται και να επαληθεύουν την ταυτότητά τους, να υπογράφουν ή να σφραγίζουν έγγραφα ηλεκτρονικά, όπως προβλέπεται στον Κανονισμό (ΕΕ) αριθ. 910/2014, σε όλες τις περιπτώσεις όπου αυτό είναι δυνατόν και για τους μη διασυνοριακούς χρήστες.

[K.42]	Στο πλαίσιο λειτουργίας του Κανονισμού (ΕΕ) 2018/1724[38] για την Ενιαία Ψηφιακή Θύρα, όταν η διαδικασία δεν απαιτεί ηλεκτρονική ταυτοποίηση ή εξακρίβωση ταυτότητας και όταν οι αρμόδιες αρχές μπορούν, δυνάμει του ισχύοντος νόμου ή των ισχυόντων διοικητικών πρακτικών, να κάνουν δεκτά ψηφιοποιημένα αντίγραφα μη ηλεκτρονικών αποδεικτικών στοιχείων ταυτότητας –όπως δελτίων ταυτότητας ή διαβατηρίων–, όσον αφορά τους μη διασυνοριακούς χρήστες, οι εν λόγω αρχές ΠΡΕΠΕΙ ΝΑ κάνουν, επίσης, δεκτά τα αντίστοιχα ψηφιοποιημένα αντίγραφα, όσον αφορά τους διασυνοριακούς χρήστες.

[K.43]	Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας ΠΡΕΠΕΙ ΝΑ είναι τεχνικώς ικανά να λαμβάνουν και να προσκομίζουν δεδομένα ταυτοποίησης προσώπου και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών σε διασυνοριακά σενάρια, χωρίς να θίγεται η διαλειτουργικότητα, και θα ΠΡΕΠΕΙ ΝΑ υποστηρίζουν προκαθορισμένους τύπους μορφοτύπων δεδομένων και επιλεκτική γνωστοποίηση.

[K.44]	Τα πρωτόκολλα επικοινωνίας και οι τεχνικές προδιαγραφές για τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας ΠΡΕΠΕΙ ΝΑ συμβαδίζουν με τον Κανονισμό (ΕΕ) 2024/1183[39] και με τα σχετικά προβλεπόμενα και εγκεκριμένα στο Αρχιτεκτονικό Πλαίσιο Αναφοράς (Architecture Reference Framework (ARF)), τον Κώδικα Αναφοράς (Reference Implementation Code (Baseline)), καθώς επίσης και με τους Εκτελεστικούς Κανονισμούς (Implementation Acts - IAs), που ορίζουν τις νομικές απαιτήσεις για τις βασικές λειτουργίες του πορτοφολιού EUDI (https://github.com/eu-digital-identity-wallet) και με κάθε μεταγενέστερη επικαιροποίησή τους.

[K.45]	Οι πάροχοι δεδομένων ταυτοποίησης προσώπου ΠΡΕΠΕΙ ΝΑ διασφαλίζουν ότι τα δεδομένα ταυτοποίησης προσώπου που εκδίδονται προς τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας περιέχουν τις πληροφορίες που απαιτούνται για την επαλήθευση και την επικύρωση των δεδομένων ταυτοποίησης προσώπου.

[K.46]	Οι πάροχοι δεδομένων ταυτοποίησης προσώπου ΠΡΕΠΕΙ ΝΑ διασφαλίζουν ότι τα δεδομένα ταυτοποίησης προσώπου που εκδίδονται προς τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας είναι σύμφωνα με τα οριζόμενα στον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2977 για τα δεδομένα ταυτοποίησης προσώπου και τις ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται για τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας.

[38] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R1724

[39] https://www.european-digital-identity-regulation.com/

[K.47]	Οι πάροχοι ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ΠΡΕΠΕΙ ΝΑ διασφαλίζουν ότι οι ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται προς μονάδες ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας περιέχουν τις πληροφορίες που απαιτούνται για την επαλήθευση και την επικύρωση των εν λόγω ηλεκτρονικών βεβαιώσεων χαρακτηριστικών.

[K.48]	Οι πάροχοι ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ΠΡΕΠΕΙ ΝΑ τηρούν τα σχετικά οριζόμενα στον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2977 και τα σχετικά προβλεπόμενα και εγκεκριμένα στο Αρχιτεκτονικό Πλαίσιο Αναφοράς (Architecture Reference Framework - ARF).
[K.49]	Οι πάροχοι δεδομένων ταυτοποίησης προσώπου που εκδίδονται προς μονάδα πορτοφολιού, ΠΡΕΠΕΙ ΝΑ διαθέτουν γραπτές και προσβάσιμες στο κοινό πολιτικές σχετικά με τη διαχείριση του καθεστώτος ισχύος, συμπεριλαμβανομένων, κατά περίπτωση, των όρων υπό τους οποίους τα εν λόγω δεδομένα ταυτοποίησης προσώπου μπορούν να ανακληθούν χωρίς καθυστέρηση.

[K.50]	Οι πάροχοι δεδομένων ταυτοποίησης προσώπου που εκδίδονται προς μονάδα πορτοφολιού ΠΡΕΠΕΙ ΝΑ ακολουθούν τα οριζόμενα στον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2977 σχετικά με την ανάκληση δεδομένων ταυτοποίησης προσώπου.

[K.51]	Η διαδικασία αυθεντικοποίησης και ταυτοποίησης ΠΡΕΠΕΙ ΝΑ προσαρμόζεται σε νέες τεχνολογίες και απαιτήσεις ασφάλειας, παραμένοντας ταυτόχρονα συμβατή με τις προβλέψεις του Κανονισμού (ΕΕ) 2014/1183, όπως ισχύει.

[K.52]	Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα που διενεργείται από τα κράτη μέλη ή για λογαριασμό τους από φορείς ή μέρη υπεύθυνα για την παροχή των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, ως μέσων ηλεκτρονικής ταυτοποίησης, ΠΡΕΠΕΙ ΝΑ διενεργείται σύμφωνα με κατάλληλα και αποτελεσματικά μέτρα προστασίας δεδομένων. Η συμμόρφωση της εν λόγω επεξεργασίας με τον Κανονισμό (ΕΕ) 2016/679 ΠΡΕΠΕΙ ΝΑ αποδεικνύεται.

[K.53]	Οποιαδήποτε νέα πρόβλεψη ή τεχνολογική αναβάθμιση θα ΠΡΕΠΕΙ ΝΑ ενσωματώνεται χωρίς να επηρεάζεται η λειτουργικότητα και η ασφάλεια των υπηρεσιών.

[K.54]	Οι υπηρεσίες ταυτοποίησης, για τα νέα συστήματα που υλοποιούνται και για τα υφιστάμενα που αναβαθμίζονται, ΠΡΕΠΕΙ ΝΑ συνδυαστούν με τη χρήση Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας[40], για την, κατά περίπτωση, αποθήκευση δεδομένων ταυτότητας, διαπιστευτηρίων, επίσημων ψηφιακών εγγράφων και χαρακτηριστικών που συνδέονται με την ταυτότητα των συναλλασσόμενων, σαν ένα ξεχωριστό σχήμα ταυτοποίησης.

[40] https://eur-lex.europa.eu/eli/reg/2024/1183/oj?locale=el

[K.55]	Οι υπηρεσίες ταυτοποίησης μέσω Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας ΠΡΕΠΕΙ ΝΑ είναι συμβατές και να ανταποκρίνονται στις απαιτήσεις ασφάλειας, προστασίας δεδομένων και διαλειτουργικότητας του Κανονισμού (ΕΕ) 1183/2024 και του Εκτελεστικού Κανονισμού (ΕΕ) 2025/846, όπως αυτοί θα οριστούν και θα ισχύσουν.

[K.56]	ΠΡΕΠΕΙ ΝΑ παρέχεται η δυνατότητα στους χρήστες να χρησιμοποιούν τοπικά αποθηκευμένα ψευδώνυμα μέσω του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας, για υπηρεσίες που δεν απαιτούν την πλήρη γνώση των προσωπικών στοιχείων του χρήστη[41].

[41] Δικαίωμα ψευδωνυμίας (άρθρο 5 του Κανονισμού (ΕΕ) 2024/1183)