ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Από το eIDAS στο eIDAS 2.0 και το ψηφιακό πορτοφόλι

Σοφία Άννα Π. Μιχαηλίδου

Επιβλέπων Καθηγητής:
Παναγιώτης Ριζομυλιώτης, αναπληρωτής καθηγητής

ΠΕΙΡΑΙΑΣ

ΟΚΤΩΒΡΙΟΣ 2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΤΙΚΗ ΕΡΓΑΣΙΑ

Από το eIDAS στο eIDAS 2.0 και το ψηφιακό πορτοφόλι

Σοφία Άννα Μιχαηλίδου

Α.Μ.: ΜΤΕ2214

ΠΕΡΙΛΗΨΗ

Η μετάβαση από τις παραδοσιακές ταυτότητες στις ψηφιακές και η υιοθέτηση κανονισμού για την ρύθμιση της λειτουργίας τους αποτελεί ένα σημαντικό βήμα της ψηφιακής εποχής. Αρχικά, οι ταυτότητες ήταν φυσικά έγγραφα που χρησιμοποιούνταν για την επαλήθευση της ταυτότητας ενός ατόμου. Με την πρόοδο της τεχνολογίας και την ανάγκη για ασφαλείς ηλεκτρονικές συναλλαγές, η Ευρωπαϊκή Ένωση εισήγαγε το 2014 τον κανονισμό eIDAS. Το eIDAS (Electronic Identification, Authentication and Trust Services) καθιέρωσε ένα ενιαίο νομικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης. Το 2024, το eIDAS 2.0 τέθηκε σε ισχύ για να αντιμετωπίσει τα κενά της προηγούμενη έκδοσής του, τις νέες ανάγκες της αγοράς και να βελτιώσει περαιτέρω την ασφάλεια και την εμπειρία πολιτών και επιχειρήσεων. Με τον νέο κανονισμό εισήχθη και η έννοια του του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας (EUDI Wallet), το οποίο επιτρέπει την αποθήκευση και διαχείριση διαπιστευτηρίων και άλλων χαρακτηριστικών, μαζί με άλλες λειτουργίες όπως η χρήση ψηφιακών υπογραφών με κύριους γνώμονες την ασφάλεια, την ιδιωτικότητα και την διαλειτουργικότητα.

Αντικείμενο της διπλωματικής εργασίας αποτελεί ο κανονισμός eIDAS και ιδίως το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας. Ο σκοπός της παρούσας διπλωματικής είναι διττός. Παρέχεται στους αναγνώστες μία ολοκληρωμένη και αναλυτική παρουσίαση βασικών στοιχείων των δύο εκδόσεων του κανονισμού για τις ηλεκτρονικές ταυτότητες και τις υπηρεσίες εμπιστοσύνης. Επιπροσθέτως παρουσιάζεται σε βάθος το ψηφιακό πορτοφόλι με έμφαση στην αρχιτεκτονική, τον τρόπο λειτουργίας καθώς επίσης και τα ανοιχτά θέματα που σχετίζονται με την υλοποίηση του οικοσυστήματος αυτού.

Στο Κεφάλαιο 1 γίνεται ανάλυση του κανονισμού eIDAS (910/2014), του δικτύου για την ηλεκτρονική ταυτοποίηση και παρουσιάζονται τα στατιστικά από την υιοθέτηση του κανονισμού καθώς και από την αξιολόγησή του. Στο Κεφάλαιο 2 γίνεται μία ολοκληρωμένη περιγραφή του αναθεωρημένου κανονισμού eIDAS 2.0 (2024/1183) με έμφαση στις αλλαγές και τα αναμενόμενα οφέλη, ενώ στο Κεφάλαιο 3 εξηγείται αναλυτικά η έννοια του ψηφιακού πορτοφολιού, παρουσιάζονται στοιχεία της αρχιτεκτονικής του οικοσυστήματος καθώς και των διαφόρων αλληλεπιδράσεων ανάμεσα στις οντότητές του. Τέλος, στο Κεφάλαιο 4 καταγράφονται οι κυριότεροι προβληματισμοί και τα ανοιχτά θέματα που έχουν εντοπιστεί ως σήμερα σχετικά με το ψηφιακό πορτοφόλι καθώς και τα συμπεράσματα της εργασίας.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ηλεκτρονική ταυτοποίηση και ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας, ηλεκτρονική ταυτοποίηση, επαλήθευση ταυτότητας, υπηρεσία εμπιστοσύνης

ABSTRACT

The transition from traditional identities to digital ones and the adoption of a regulation to better manage their operation is an important step towards the digital age. Originally, IDs were physical documents used to verify a person's identity. With the progress of technology and the need for secure electronic transactions, the European Union introduced in 2014 the eIDAS Regulation. eIDAS (Electronic Identification, Authentication and Trust Services) established a single legal framework for electronic identification and trust services. In 2024, eIDAS 2.0 entered into force, aiming to address the gaps of its previous version, new market needs and further improve the security and experience of citizens and businesses. The new regulation also introduced the concept of the European Digital Identity Wallet (EUDI Wallet), which allows the storage and management of credentials and attributes along with other features such as the use of digital signatures, while providing security, privacy and interoperability.

The subject of this diploma thesis is the eIDAS Regulation, and particularly the European Digital Identity Wallet. The purpose of this thesis is twofold. Readers are provided with a comprehensive and detailed presentation of key elements of the two versions of the regulation on electronic identities and trust services. Additionally, the digital wallet is presented in depth, emphasizing on its architecture, functionalities as well as the open issues examined regarding the practical implementation of this ecosystem.

In Chapter 1 the eIDAS regulation (910/2014) is analyzed, as well as the network for electronic identification. Also, the statistics from the adoption of the regulation and its evaluation are presented. Chapter 2 provides a comprehensive description of the revised eIDAS 2.0 Regulation (2024/1183) with emphasis on the changes and the expected benefits, while Chapter 3 explains in detail the concept of the digital wallet. The elements of the ecosystem’s architecture as well as the various interactions between entities are presented. Finally, in Chapter 4, the main concerns and open issues regarding the digital wallet that have been identified so far are described, as well as the conclusions of this thesis.

SUBJECT AREA: Electronic identification and the European Digital Identity Wallet

KEY WORDS: European digital identity wallet, electronic identification, authentication, trust service

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. Ο ΚΑΝΟΝΙΣΜΟΣ EIDAS

1.1 Εισαγωγή

Ιστορική Αναδρομή

Η έννοια της ταυτότητας και η πράξη της ταυτοποίησης εντοπίζεται από την προϊστορία, όπου με διάφορους τρόπους οι άνθρωποι προσπαθούσαν να αποδώσουν την ατομικότητά τους για να αναγνωρίζονται μεταξύ τους, να αναπτύσσουν σχέσεις εμπιστοσύνης αλλά και να απολαμβάνουν διάφορες «υπηρεσίες» με την ευρεία έννοια του όρου. Η αναγνώριση ενός ατόμου από την εμφάνισή του, τον τρόπο κίνησης και τους ήχους που έκανε φαίνεται να είναι η πρώτη μορφή ταυτότητας που χρησιμοποιήθηκε, με τις πρώτες συναλλαγές να λαμβάνουν χώρα μεταξύ ατόμων που ανήκουν στην ίδια γειτονιά. Περίπου το 3000 π.Χ. υπάρχουν στοιχεία για την πρώτη χρήση ονομάτων, ενώ τα επώνυμα εμφανίζονται πρώτα στην Κίνα, με τη Δύση να ακολουθεί αρκετούς αιώνες αργότερα, κατά τη διάρκεια της Ρωμαϊκής Αυτοκρατορίας.

Πιο κοντά στη σημερινή χρήση του όρου, η έννοια της ταυτότητας συναντάται από τις αρχές του 19ου αιώνα, όπου ξεκινά η χρήση διαβατηρίων ακολουθούμενη από άλλα έγγραφα ταυτότητας που περιλάμβαναν μεταξύ άλλων άδειες και αριθμούς κοινωνικής ασφάλισης για την ταυτοποίηση των ατόμων. Ακολούθως, η εξέλιξη της τεχνολογίας οδήγησε στην εμφάνιση των ψηφιακών ταυτοτήτων (digital identities) με τις πρώτες εκδοχές τους να είναι το δίπτυχο ονόματος χρήστη και κωδικού που επέτρεπε την πρόσβαση σε μεμονωμένες υπηρεσίες, ενώ αργότερα με τη χρήση των ίδιου ζεύγους στοιχείων άρχισε να παρέχεται πρόσβαση σε διαφορετικές υπηρεσίες ή ιστοσελίδες. Η εμφάνιση και η ανάπτυξη του διαδικτύου αλλά και των ψηφιακών υπηρεσιών έπαιξε καθοριστικό ρόλο στον πολλαπλασιασμό των ψηφιακών ταυτοτήτων.

Φυσικά, η ραγδαία άνοδος των κοινωνικών δικτύων έχει και αυτή ένα πολύ σημαντικό ρόλο στον τρόπο χρήσης και στην εξέλιξη των ταυτοτήτων, τόσο λόγω της δημιουργίας δισεκατομμυρίων προφίλ χρηστών αλλά και της δυνατότητας αξιοποίησης αυτών για την απόλαυση άλλων υπηρεσιών όπως η επαλήθευση ταυτότητας και η πρόσβαση σε τρίτες ιστοσελίδες.

Μέσα από τη σύντομη αναδρομή καθίσταται σαφές ότι τόσο η έννοια της ταυτότητας όσο και ο ρόλος της είναι σύνθετος, ενώ διαμορφώνεται και εξελίσσεται παράλληλα με την ανάπτυξη των κοινωνιών και της τεχνολογίας. [1] [2] [3] [4]

Η έννοια της ταυτότητας

Ο όρος «ταυτότητα» μπορεί να αποδοθεί ποικιλοτρόπως. Αν αναζητηθεί σε ένα λεξικό, όπως αυτό του κ. Τριανταφυλλίδη, η πρώτη ερμηνεία του όρου που συναντάται είναι: *«το σύνολο των στοιχείων που συνιστούν τη μοναδικότητα κάθε ατόμου, που επιτρέπουν να το αναγνωρίζουν ως τέτοιο και να μην το συγχέουν με κάποιο άλλο».* Η δεύτερη ερμηνεία αφορά στην αστυνομική ταυτότητα, δηλαδή *«το δελτίο με τα στοιχεία και με τη φωτογραφία του κατόχου, που εκδίδει η αστυνομία για την αναγνώριση και την απόδειξη της ταυτότητας των πολιτών»*, ενώ η τρίτη αποδίδει τον όρο ως *«έγγραφο ή άλλο στοιχείο που πιστοποιεί τις ιδιότητες και τη γνησιότητα ενός προϊόντος»*. [5]

Ωστόσο, για τους σκοπούς της παρούσας εργασίας, έχει ιδιαίτερη σημασία η απόδοση της έννοιας στο κατάλληλο εννοιολογικό πλαίσιο. Στο πλαίσιο του προτύπου ISO/IEC 24760-1:2019, η ταυτότητα αποδίδεται ως ένα σύνολο χαρακτηριστικών (attributes) που σχετίζονται με μία οντότητα (entity). Αντίστοιχα, στο πλαίσιο του NIST SP 800-63-3, ως ταυτότητα θεωρείται ένα χαρακτηριστικό ή ένα σύνολο χαρακτηριστικών που περιγράφουν με μοναδικό τρόπο ένα υποκείμενο σε ένα συγκεκριμένο πλαίσιο.

Στο ίδιο πλαίσιο, παρέχεται και η απόδοση του όρου της ψηφιακής ταυτότητας, όπου θεωρείται η μοναδική αναπαράσταση ενός υποκειμένου που εμπλέκεται σε μία επιγραμμική συναλλαγή, που είναι δηλαδή διαθέσιμη μέσω διαδικτύου. [6] [7]

Στις βασικές έννοιες που θα αναπτυχθούν περιλαμβάνονται η «ηλεκτρονική ταυτοποίηση» (electronic identification) και η «επαλήθευση ταυτότητας» (authentication). Για τους ανωτέρω όρους (καθώς και άλλους σχετικούς όρους εκτός αν αναφέρεται διαφορετικά) στο πλαίσιο της εργασίας χρησιμοποιείται η απόδοση από τον κανονισμό της Ευρωπαϊκής Ένωσης σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά[1], στο εξής eIDAS (electronic Identification, Authentication and Trust Services).

Με τον όρο «ηλεκτρονική ταυτοποίηση» εννοείται η διαδικασία χρήσης δεδομένων ταυτοποίησης προσώπου (person identification data) σε ηλεκτρονική μορφή που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο ή ένα φυσικό πρόσωπο που εκπροσωπεί ένα νομικό πρόσωπο[2]. Τα δεδομένα ταυτοποίησης προσώπου είναι μία δέσμη δεδομένων (που εκδίδεται σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο) και επιτρέπει την εξακρίβωση της ταυτότητας φυσικού ή νομικού προσώπου ή φυσικού προσώπου που εκπροσωπεί ένα νομικό πρόσωπο[3]. [8]

Με τον όρο «επαλήθευση ταυτότητας» αποδίδεται η ηλεκτρονική διαδικασία που επιτρέπει να επιβεβαιωθεί η ηλεκτρονική ταυτοποίηση φυσικού ή νομικού προσώπου ή της προέλευσης και της ακεραιότητας δεδομένων σε ηλεκτρονική μορφή. [8]

Οι ανάγκες που οδήγησαν στον κανονισμό eIDAS

Τα τελευταία χρόνια πάρα πολλές αλληλεπιδράσεις γίνονται πλέον ηλεκτρονικά. Υπάρχει μία πληθώρα διαφορετικών υπηρεσιών που αρχίζουν να προσφέρονται σε ψηφιακή μορφή, είτε παράλληλα με, είτε αντικαθιστώντας την παραδοσιακή τους μορφή. Οι υπηρεσίες αυτές μπορεί να προσφέρονται από ιδιωτικές επιχειρήσεις προς άλλες επιχειρήσεις ή τους καταναλωτές, αλλά και από δημόσιους φορείς προς επιχειρήσεις ή τους πολίτες.

Ενδεικτικά, μια βασική κατηγορία υπηρεσιών αφορά τα ηλεκτρονικά καταστήματα και τις ηλεκτρονικές συναλλαγές, με ένα ευρέως χρησιμοποιούμενο παράδειγμα να αποτελεί η πώληση αλκοολούχων ποτών, όπου οι επιχειρήσεις πρέπει να διασφαλίζουν ότι οι αγοραστές πληρούν το ηλικιακό όριο, ζητώντας συνήθως την ταυτότητα των τελευταίων. Αντίστοιχα, οι πελάτες, θέλουν να είναι βέβαιοι ότι αγοράζουν από κάποιο νόμιμο κατάστημα και δεν έχουν πέσει θύμα απάτης. Προσθέτοντας μία ακόμα παράμετρο με τον πελάτη να είναι κάτοικος μίας διαφορετικής χώρας της Ευρωπαϊκής Ένωσης (ΕΕ) από αυτή που η επιχείρηση έχει την έδρα της, προκύπτουν επιπλέον δυσκολίες για την ασφαλή και πρακτική ολοκλήρωση της συναλλαγής, παρά την θεωρητική λειτουργία της ενιαίας αγοράς. [9]

Στην ΕΕ αναγνωρίστηκαν με την πάροδο των ετών τα εμπόδια και οι ελλείψεις που δυσκόλευαν την περαιτέρω ανάπτυξη των ηλεκτρονικών αυτών αλληλεπιδράσεων. Όπως προκύπτει και από το απλό παράδειγμα που παρουσιάστηκε, μία βασική ανάγκη που διαπιστώθηκε αφορούσε την οικοδόμηση εμπιστοσύνης στην εσωτερική αγορά για να μπορούν να υλοποιούνται με ασφάλεια ηλεκτρονικές συναλλαγές αλλά και να διευρύνονται οι υπηρεσίες που δύνανται να παρέχονται. Παράλληλα, παρατηρήθηκε αύξηση του ηλεκτρονικού εγκλήματος, ως εμπόδιο.

[1] Η εσωτερική αγορά της Ευρωπαϊκής Ένωσης (ΕΕ) είναι μια ενιαία αγορά στην οποία τα αγαθά, οι υπηρεσίες, τα κεφάλαια και τα πρόσωπα κυκλοφορούν ελεύθερα και στο εσωτερικό της οποίας οι ευρωπαίοι πολίτες μπορούν να ζουν, να εργάζονται, να σπουδάζουν ή να ασκούν επιχειρηματική δραστηριότητα ελεύθερα. [89]
[2] ή άλλο φυσικό πρόσωπο (σύμφωνα με τον τροποποιημένο κανονισμό eIDAS 2.0 2024/1183) [39]
[3] ή άλλο φυσικό πρόσωπο (σύμφωνα με τον τροποποιημένο κανονισμό eIDAS 2.0 2024/1183) [39]

Ταυτόχρονα, μέχρι πριν από μία δεκαετία δεν υπήρχε κάποιο διασυνοριακό πλαίσιο το οποίο να διέπει αυτές τις συναλλαγές, ενώ η αγορά ήταν κατακερματισμένη και δεν απολάμβανε τον ενιαίο χαρακτήρα της. Σε αυτό σημαντικό ρόλο έπαιζε και η έλλειψη διαλειτουργικότητας μεταξύ συστημάτων και υπηρεσιών που προσφέρονταν από τα κράτη-μέλη. [8]

Με την διαμόρφωση και εφαρμογή του κανονισμού eIDAS, η ΕΕ έθεσε τις βάσεις για ένα κοινό νομικό πλαίσιο σε όλα τα κράτη-μέλη ώστε οι πολίτες, οι εταιρίες και οι δημόσιοι φορείς να μπορούν να κάνουν απρόσκοπτα και με ασφάλεια ηλεκτρονικές αλληλεπιδράσεις, απολαμβάνοντας τα πλεονεκτήματα των συστημάτων ηλεκτρονικής ταυτοποίησης (eID schemes) αλλά και των υπηρεσιών εμπιστοσύνης (Trust Services) που περιγράφονταν από τον κανονισμό. [9] [10] [11]

1.2 Ο κανονισμός eIDAS 1.0

Στόχος, αντικείμενο & πεδίο εφαρμογής

Η πρώτη έκδοση του ευρωπαϊκού κανονισμού eIDAS (910/2014) υιοθετήθηκε το 2014, αντικαθιστώντας την μέχρι τότε ισχύουσα οδηγία 1993/93/ΕΚ. Στόχος του νέου ενιαίου πλαισίου ήταν η διασφάλιση της εύρυθμης λειτουργίας της εσωτερικής αγοράς στην ΕΕ παράλληλα με την επίτευξη ενός επαρκούς επιπέδου ασφάλειας στα μέσα ηλεκτρονικής ταυτοποίησης και στις υπηρεσίες εμπιστοσύνης. [9]

Συγκεκριμένα, μέσω του κανονισμού καθορίζονταν οι όροι (α) για την αναγνώριση μέσων ηλεκτρονικής ταυτοποίησης[4] φυσικών και νομικών προσώπων που εμπίπτουν σε κοινοποιημένο σύστημα ηλεκτρονικής ταυτοποίησης[5] άλλου κράτους μέλους, (β) θεσπίστηκαν κανόνες για υπηρεσίες εμπιστοσύνης καθώς και (γ) νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές (e-Signature), τις ηλεκτρονικές σφραγίδες (e-Seal), τις ηλεκτρονικές χρονοσφραγίδες (e-Timestamp), τα ηλεκτρονικά έγγραφα, τις ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (Electronic Registered Delivery Services) και τις υπηρεσίες πιστοποιητικών για την επαλήθευση της ταυτότητας ιστοτόπων (Qualified Web Authentication Certificates). [9]

Με τη βοήθεια της ηλεκτρονικής ταυτοποίησης καθίσταται πιο εύκολη η αναγνώριση και η επαλήθευση ταυτότητας φυσικών και νομικών προσώπων για την απόκτηση πρόσβασης σε υπηρεσίες και για την ευκολότερη πραγματοποίηση συναλλαγών, ιδίως διασυνοριακού χαρακτήρα. Με τη χρήση των υπηρεσιών εμπιστοσύνης, αυξάνεται η εμπιστοσύνη, ασφάλεια και η ευκολία για τις συναλλαγές, και πάλι ιδίως διασυνοριακού χαρακτήρα. [9] [12]

Πρακτικά, μέσω του eIDAS προωθήθηκε η ιδέα της διαλειτουργικότητας μεταξύ των χωρών της ΕΕ, διασφαλίζοντας ότι οι τελευταίες μπορούν να αναγνωρίζουν τα κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης άλλων χωρών της ΕΕ καθώς και ότι υπηρεσίες που παρέχονταν από παρόχους που συμμορφώνονταν με την απαιτήσεις του κανονισμού, μπορούσαν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες. [10]

Ο κανονισμός τέθηκε σε ισχύ από τον Ιούλιο του 2016 με εξαίρεση τα κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης, τα οποία έπρεπε να αναγνωρίζονται από άλλες χώρες από το Σεπτέμβριο του 2018. Παράλληλα, προέβλεπε την επανεξέταση της εφαρμογής του κανονισμού με την υποβολή έκθεσης στο Ευρωπαϊκό Κοινοβούλιο, το αργότερο μέχρι τον Ιούλιο του 2020.

[4] υλική και/ή άυλη μονάδα η οποία περιέχει δεδομένα ταυτοποίησης προσώπου και χρησιμοποιείται για την επαλήθευση ταυτότητας σε επιγραμμικές υπηρεσίες (ή, κατά περίπτωση, μη επιγραμμική υπηρεσία, βάσει του αναθεωρημένου κανονισμού 2024/1183)

[5] σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου εκδίδονται μέσα ηλεκτρονικής ταυτοποίησης σε φυσικά ή νομικά πρόσωπα, ή σε φυσικά πρόσωπα που εκπροσωπούν νομικά πρόσωπα

Στην αξιολόγηση που πραγματοποιήθηκε από το Σεπτέμβριο του 2019 ως το Δεκέμβριο του 2020, εντοπίστηκαν οι αδυναμίες που οδήγησαν στην επανεξέταση του κανονισμού. Τον Ιούνιο του 2021, έχοντας λάβει υπόψη τα συμπεράσματα από την αξιολόγηση, η Ευρωπαϊκή Επιτροπή κατέθεσε πρόταση για την τροποποίηση του. Τον Φεβρουάριο του 2024 και έπειτα από πολλές διαβουλεύσεις, το Κοινοβούλιο ενέκρινε τον αναθεωρημένο κανονισμό, το Συμβούλιο κατά σειρά τον αποδέχθηκε τον Μάρτιο, με το επίσημο κείμενο να υπογράφεται στις 11 Απριλίου και να δημοσιεύεται στην εφημερίδα της ΕΕ στις 30 Απριλίου του 2024. Το eIDAS 2.0 είναι σε ισχύ από τις 20 Μαΐου 2024. [9] [12] [13] [14]

Η ηλεκτρονική ταυτοποίηση

Γενικές πληροφορίες

Το eID είναι ένα σύνολο από υπηρεσίες (συμπεριλαμβανομένου λογισμικού, οδηγιών, εκπαίδευσης και υποστήριξης) που παρέχονται από την Ευρωπαϊκή Επιτροπή ώστε να είναι εφικτή η αμοιβαία αναγνώριση των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης διασυνοριακά. Επιτρέπεται με αυτό τον τρόπο στους πολίτες να χρησιμοποιούν τις ηλεκτρονικές ταυτότητες που έχουν εκδοθεί στη χώρα τους για την πρόσβαση σε ηλεκτρονικές υπηρεσίες άλλων ευρωπαϊκών χωρών. [15] [16]

Ο κανονισμός eIDAS πρακτικά επιβάλλει στα κράτη μέλη να δέχονται τα μέσα ηλεκτρονικής ταυτοποίησης που έχουν εκδοθεί σε άλλο κράτος μέλος, όταν απαιτείται ηλεκτρονική ταυτοποίηση ή επαλήθευση ταυτότητας για την πρόσβαση σε υπηρεσία που παρέχεται από δημόσιο φορέα του πρώτου κράτους μέλους, εφόσον πληρούνται ορισμένες προϋποθέσεις.

Αναλυτικά, απαιτείται το μέσο ηλεκτρονικής ταυτοποίησης να έχει εκδοθεί από σύστημα το οποίο να ανήκει στον κατάλογο κοινοποιημένων συστημάτων (περιγράφεται στην ενότητα: Κοινοποίηση) που δημοσιεύει η Επιτροπή, παράλληλα πρέπει το επίπεδο διασφάλισης (περιγράφεται στην ενότητα: Επίπεδα διασφάλισης (Levels of Assurance)) του μέσου αυτού να είναι ίσο ή υψηλότερο από το αντίστοιχο που απαιτείται από τον οικείο φορέα για την πρόσβαση στην υπηρεσία, ενώ τέλος πρέπει και ο οικείος φορέας να χρησιμοποιεί ο ίδιος το βασικό ή υψηλό επίπεδο διασφάλισης. [8]

Κοινοποίηση

Η διαδικασία της κοινοποίησης (notification) περιλαμβάνει την επιλογή, επισκόπηση και προσθήκη εθνικών eID συστημάτων στο δίκτυο του eIDAS (βλ. ενότητα 1.4). Με αυτόν τον τρόπο εξασφαλίζεται ότι τα συστήματα αυτά πληρούν τις προϋποθέσεις ποιότητας και ασφάλειας που ορίζονται από τον κανονισμό (άρθρο 7). Ενδεικτικά, ορισμένες από τις προϋποθέσεις αυτές που καθιστούν ένα σύστημα επιλέξιμο προς κοινοποίηση είναι: [15]

- Τα μέσα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του συστήματος πρέπει να εκδίδονται είτε από το κοινοποιούν κράτος-μέλος, είτε με εντολή του, είτε ανεξάρτητα από αυτό αλλά να είναι αναγνωρισμένα από το κράτος-μέλος.
- Τα μέσα πρέπει να μπορούν να χρησιμοποιηθούν για την πρόσβαση σε τουλάχιστον μία υπηρεσία του δημοσίου τομέα.
- Τόσο τα μέσα όσο και το σύστημα πρέπει να πληρούν τις απαιτήσεις ενός τουλάχιστον από τα επίπεδα διασφάλισης. [8]

Κάθε κράτος-μέλος είναι υπεύθυνο για την κοινοποίηση των δικών του συστημάτων. Οι πληροφορίες που πρέπει να κοινοποιεί (καθώς και τροποποιήσεις σε αυτές) παρουσιάζονται στο άρθρο 9 και περιλαμβάνουν συνοπτικά: (α) την περιγραφή του συστήματος ηλεκτρονικής ταυτοποίησης, αναφορά στον εκδότη των μέσων ηλεκτρονικής ταυτοποίησης και στο επίπεδο διασφάλισής του, (β) το καθεστώς εποπτείας και πληροφορίες για το καθεστώς ευθύνης, (γ) την αρχή που είναι υπεύθυνη για το σύστημα, (δ) πληροφορίες για τις οντότητες που διαχειρίζονται την καταγραφή των μοναδικών δεδομένων ταυτοποίησης προσώπου, (ε) πληροφορίες για τον τρόπο ικανοποίησης απαιτήσεων που αφορούν στο πλαίσιο διαλειτουργικότητας, (στ) περιγραφή της επαλήθευσης ταυτότητας και (ζ) ρυθμίσεις για την αναστολή ή ανάκληση του συστήματος, της επαλήθευσης ταυτότητας ή τμημάτων αυτών, εφόσον έχουν εκτεθεί σε κίνδυνο. [8]

Επίπεδα διασφάλισης (Levels of Assurance)

Βάσει του κανονισμού eIDAS, τα συστήματα eID κατηγοριοποιούνται σε 3 επίπεδα διασφάλισης ανάλογα με το βαθμό βεβαιότητας που υπάρχει στο κάθε σύστημα ότι το χρησιμοποιεί ο εν λόγω χρήστης κάθε φορά και όχι κάποιος άλλος, δηλαδή πόσο «ισχυρό» είναι το σύστημα, άρα δύσκολο να παρακαμφθεί. Οι ελάχιστες τεχνικές προδιαγραφές και διαδικασίες για τα επίπεδα διασφάλισης ορίζονται στον εκτελεστικό κανονισμό 2015/1502 της Επιτροπής και αφορούν τις εξής συνιστώσες:

- Την διαδικασία που ακολουθείται για την απόκτηση της ηλεκτρονικής ταυτότητας (αίτηση και καταχώρηση)
- Τον τρόπο διαχείρισης των μέσων ηλεκτρονικής ταυτοποίησης
- Τον τρόπο με τον οποίο γίνεται η επαλήθευση ταυτότητας
- Την διαχείριση και οργάνωση για την ασφάλεια πληροφοριών και διαχείριση κινδύνων

Ανάλογα με την αξιοπιστία και την ποιότητα των παραπάνω στοιχείων, υπάρχουν 3 επίπεδα διασφάλισης: το χαμηλό, το βασικό και το υψηλό. Για κάθε επίπεδο περιγράφονται αναλυτικά οι προδιαγραφές στον εκτελεστικό κανονισμό, ενώ παρακάτω παρουσιάζονται ενδεικτικά οι προϋποθέσεις για την απόδειξη και επαλήθευση ταυτότητας ενός φυσικού προσώπου: [8]

- Χαμηλό: Για την επαλήθευση ταυτότητας δεν απαιτείται η επαλήθευση στοιχείων, αλλά θεωρείται ότι το φυσικό πρόσωπο κατέχει αποδεικτικά στοιχεία που αναγνωρίζονται από το κράτος μέλος που υποβάλει την αίτηση για το μέσο ηλεκτρονικής ταυτοποίησης, τα αποδεικτικά στοιχεία φαίνεται ότι είναι έγκυρα, είναι γνωστό από έγκυρη πηγή ότι η δηλωθείσα ταυτότητα υφίσταται και το πρόσωπο που τη διεκδικεί είναι το ίδιο.
- Βασικό: Όταν ισχύουν οι προδιαγραφές του χαμηλού επιπέδου και επιπλέον ισχύει μία εκ των τεσσάρων εναλλακτικών που περιγράφονται στον κανονισμό, όπως για παράδειγμα ότι "*υποβάλλεται έγγραφο ταυτότητας κατά τη διάρκεια της διαδικασίας καταχώρισης στο κράτος μέλος όπου έχει εκδοθεί το έγγραφο και το έγγραφο φαίνεται ότι σχετίζεται με το πρόσωπο που το προσκομίζει και παράλληλα έχουν ληφθεί μέτρα για την ελαχιστοποίηση του κινδύνου η ταυτότητα του προσώπου να μην είναι η δηλωθείσα ταυτότητα, λαμβάνοντας υπόψη, για παράδειγμα, τον κίνδυνο απώλειας, κλοπής, αναστολής, ανάκλησης ή λήξης της ισχύος των εγγράφων*".
- Υψηλό: Όταν ισχύουν οι προδιαγραφές του βασικού επιπέδου και επιπλέον μία εκ των τριών εναλλακτικών απαιτήσεων όπως: *"Όταν το πρόσωπο έχει επαληθευθεί ότι διαθέτει φωτογραφία ή βιομετρικά στοιχεία ταυτοποίησης που αναγνωρίζονται από το κράτος μέλος στο οποίο υποβλήθηκε η αίτηση για το μέσο ηλεκτρονικής ταυτότητας, και τα εν λόγω αποδεικτικά στοιχεία αντιπροσωπεύουν τη δηλωθείσα ταυτότητα, τα αποδεικτικά στοιχεία ελέγχονται προκειμένου να διαπιστωθεί ότι είναι έγκυρα σύμφωνα με έγκυρη πηγή· και ο αιτών ταυτοποιείται με τη δηλωθείσα ταυτότητα με σύγκριση ενός ή*

περισσότερων σωματικών χαρακτηριστικών του προσώπου με έγκυρη πηγή" και επιπλέον *"εάν ο αιτών δεν υποβάλει κάποια αναγνωρισμένη φωτογραφία ή βιομετρικά στοιχεία ταυτοποίησης, εφαρμόζονται οι ίδιες διαδικασίες που εφαρμόζονται σε εθνικό επίπεδο στο κράτος μέλος του φορέα που είναι αρμόδιος για την καταχώρηση όσον αφορά την απόκτηση αναγνωρισμένης φωτογραφίας ή των βιομετρικών στοιχείων ταυτοποίησης".* [17] [18]

Διαλειτουργικότητα

Βάσει του άρθρου 12 του κανονισμού, τα εθνικά κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης πρέπει να είναι διαλειτουργικά. Το πλαίσιο που θεσπίζεται για το σκοπό αυτό έχει στόχο να είναι τεχνολογικά ουδέτερο, να ακολουθεί διεθνή πρότυπα, να διευκολύνει την εφαρμογή της αρχής προστασίας της ιδιωτικής ζωής ήδη από το σχεδιασμό αλλά και να διασφαλίζει την επεξεργασία των προσωπικών δεδομένων βάσει της οδηγίας 95/46/ΕΚ. [8]

Ο εν λόγω εκτελεστικός κανονισμός της επιτροπής είναι ο 2015/1501 και περιλαμβάνει τις τεχνικές και λειτουργικές απαιτήσεις του πλαισίου που αφορούν: (α) ελάχιστες τεχνικές απαιτήσεις για τα επίπεδα διασφάλισης και τη χαρτογράφηση των εθνικών επιπέδων διασφάλισης των κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης που εκδίδονται στο πλαίσιο των κοινοποιημένων συστημάτων, (β) ελάχιστες τεχνικές προδιαγραφές για τη διαλειτουργικότητα, (γ) το ελάχιστο σύνολο δεδομένων ταυτοποίησης προσώπου που αντιπροσωπεύουν κατά τρόπο μοναδικό ένα φυσικό ή νομικό πρόσωπο, (δ) κοινά πρότυπα επιχειρησιακής ασφάλειας και (ε) ρυθμίσεις για την επίλυση διαφορών. [19]

Αναλυτική αναφορά στην αρχιτεκτονική και τον τρόπο λειτουργίας του δικτύου eIDAS γίνεται στην ενότητα 1.4.

Οι υπηρεσίες εμπιστοσύνης

Γενικές πληροφορίες

Το eIDAS ορίζει ως υπηρεσία εμπιστοσύνης *μία ηλεκτρονική υπηρεσία, συνήθως παρεχόμενη έναντι αμοιβής, η οποία συνίσταται α) στη δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσφραγίδων, ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές, ή β) στη δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων, ή γ) στη διαφύλαξη ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές*. Αναλυτικές πληροφορίες για τις υπηρεσίες εμπιστοσύνης αναφέρονται στις επόμενες ενότητες. [8]

Για την ενίσχυση της χρήσης των υπηρεσιών (και των σχετικών προϊόντων) εμπιστοσύνης, ο κανονισμός eIDAS εισήγαγε επίσης την έννοια της εγκεκριμένης (qualified) κατάστασης με την οποία υποδεικνύεται ότι είτε το προϊόν/υπηρεσία του συμμορφώνεται με ένα σύνολο υψηλών προδιαγραφών και απαιτήσεων ασφαλείας που ορίζονται από τον κανονισμό. Αντίστοιχα, η έννοια του εγκεκριμένου παρόχου δηλώνει ότι ο τελευταίος παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιος από τον εποπτικό φορέα. [20]

Βάσει του άρθρου 17, κάθε κράτος μέλος πρέπει να ορίζει εποπτικό φορέα του οποίου τα στοιχεία κοινοποιεί στην Επιτροπή (όνομα και διεύθυνση) και στον οποίο ανατίθενται εξουσίες και διατίθενται πόροι ώστε να εκτελεί το ρόλο του, ο οποίος περιλαμβάνει: (α) την εποπτεία των εγκεκριμένων παρόχων εμπιστοσύνης και των εγκεκριμένων υπηρεσιών που παρέχουν ώστε να διασφαλίζει ότι πληρούν τις απαιτήσεις του κανονισμού και (β) να αναλαμβάνει δράση όταν ενημερώνεται ότι υπάρχουν εικασίες ότι οι μη εγκεκριμένοι πάροχοι ή οι υπηρεσίες τους δεν πληρούν τις απαιτήσεις του κανονισμού.

Περισσότερες πληροφορίες για τους εποπτικούς φορείς αλλά και τους οργανισμούς συμμόρφωσης αναφέρονται στην ενότητα Εποπτεία & συμμόρφωση. [8]

Στο άρθρο 24 του κανονισμού ορίζονται απαιτήσεις για τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης, οι βασικότερες εκ των οποίων είναι:

1. Η εξακρίβωση της ταυτότητας αλλά και των ειδικών χαρακτηριστικών του φυσικού ή νομικού προσώπου για το οποίο εκδίδουν εγκεκριμένο πιστοποιητικό
2. Η ενημέρωση του εποπτικού φορέα για αλλαγές στις παρεχόμενες εγκεκριμένες υπηρεσίες, αλλά και σε περίπτωση που υπάρχει πρόθεση παύσης των δραστηριοτήτων αυτών
3. Η χρήση αξιόπιστων συστημάτων και προϊόντων για τις διεργασίες που αυτά υποστηρίζουν
4. Η λήψη μέτρων κατά της πλαστογραφίας και κλοπής δεδομένων
5. Η καταγραφή και η διατήρηση προσβάσιμων των πληροφοριών για τα δεδομένα που έχουν εκδώσει και λάβει
6. Η συγκρότηση και διατήρηση ενημερωμένης βάσης δεδομένων για εγκεκριμένα πιστοποιητικά, εφόσον η έκδοσή τους εμπίπτει στις δραστηριότητές τους
7. Η άμεση καταχώρηση ανακλήσεων πιστοποιητικών στη βάση δεδομένων
8. Η παροχή στα βασιζόμενα μέρη[6] με τρόπο δωρεάν, αυτοματοποιημένο και αξιόπιστο, πληροφοριών για την ισχύ και ανάκληση πιστοποιητικών που έχουν εκδώσει, ακόμα και μετά την περίοδο ισχύος του εν λόγω πιστοποιητικού

Επιπροσθέτως, σύμφωνα με το άρθρο 14 του κανονισμού, οι υπηρεσίες εμπιστοσύνης που παρέχονται από παρόχους εγκατεστημένους σε τρίτες χώρες ή διεθνείς οργανισμούς αναγνωρίζονται ως νομικά ισοδύναμες με τις αντίστοιχες εγκεκριμένες υπηρεσίες που παρέχονται από εγκεκριμένους παρόχους εντός ΕΕ, εφόσον κυρίως πληρούνται οι εξής προϋποθέσεις: (α) Οι τρίτοι πάροχοι και οργανισμοί καθώς και οι σχετικές υπηρεσίες εμπιστοσύνης που προσφέρουν τηρούν τις ίδιες απαιτήσεις που εφαρμόζονται σε αυτούς της ΕΕ και (β) οι υπηρεσίες εμπιστοσύνης των παρόχων και των οργανισμών αυτών αναγνωρίζονται ως νομικά ισοδύναμες με τις εγκεκριμένες υπηρεσίες των εγκεκριμένων παρόχων εντός της ΕΕ. [8]

Οι πάροχοι των υπηρεσιών εμπιστοσύνης πρέπει βάσει του άρθρου 19 να λαμβάνουν κατάλληλα τεχνικά και οργανωτικά μέτρα διαχείρισης κινδύνων (πρόληψης αλλά και ελαχιστοποίησης αντικτύπου) για την ασφάλεια των υπηρεσιών τους, διασφαλίζοντας ότι το επίπεδο ασφάλειας είναι ανάλογο προς το βαθμό του κινδύνου. Επιπλέον, είναι υποχρεωμένοι να ενημερώνουν τους αρμόδιους φορείς (κατά περίπτωση μπορεί να είναι οι εποπτικοί φορείς, αρχές προστασίας δεδομένων, άλλες αρχές, φορείς άλλων κρατών μελών ή και το κοινό που επηρεάζεται), όταν υπάρχει παραβίαση ασφαλείας ή απώλεια ακεραιότητας με σημαντικό αντίκτυπο στη σχετική υπηρεσία. [8]

Ηλεκτρονική υπογραφή

Με τον όρο ηλεκτρονική υπογραφή γίνεται αναφορά σε δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει, όπου ο υπογράφων είναι φυσικό πρόσωπο.

[6] Φυσικό ή νομικό πρόσωπο που βασίζεται σε ηλεκτρονική ταυτοποίηση ή υπηρεσία εμπιστοσύνης [8]

Ουσιαστικά αποτελεί την έκφραση σε ηλεκτρονική μορφή, της συγκατάθεσης ενός ατόμου στο περιεχόμενο ενός εγγράφου ή ενός συνόλου δεδομένων ενώ μπορεί να χρησιμοποιηθεί και για παράδειγμα για να δηλώσει ότι το άτομο συνέταξε το έγγραφο ή ακόμα και για να βεβαιώσει την παρουσία του ως μάρτυρα. [8] [9] [21]

Βάσει του κανονισμού, υπάρχουν τρία είδη ηλεκτρονικών υπογραφών: η απλή, η προηγμένη και η εγκεκριμένη. Ο ορισμός της απλής ηλεκτρονικής υπογραφής παρουσιάστηκε ανωτέρω και παράδειγμα αυτής μπορεί να είναι ακόμα και η χρήση του ονοματεπωνύμου του συντάκτη μίας ηλεκτρονικής αλληλογραφίας στο τέλος του κειμένου. Η προηγμένη ηλεκτρονική υπογραφή έχει επιπλέον χαρακτηριστικά καθώς (α) συνδέεται με μοναδικό τρόπο με τον υπογράφοντα και (β) μπορεί να τον ταυτοποιεί, (γ) δημιουργείται με τέτοιο τρόπο που επιτρέπει στον υπογράφοντα να διατηρεί τον έλεγχο και (δ) συνδέεται με τέτοιο τρόπο με τα δεδομένα όπου κάθε μεταγενέστερη αλλαγή σε αυτά είναι αναγνωρίσιμη. Η πλέον γνωστή τεχνολογία με την οποία καλύπτονται οι παραπάνω προϋποθέσεις είναι αυτή της υποδομής δημοσίου κλειδιού με τη χρήση πιστοποιητικών και κρυπτογραφικών κλειδιών. [8] [21]

Η εγκεκριμένη ηλεκτρονική υπογραφή τέλος είναι μία προηγμένη υπογραφή που επιπρόσθετα έχει δημιουργηθεί από μία εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής (qualified signature creation device) και βασίζεται σε εγκεκριμένο πιστοποιητικό για ηλεκτρονικές υπογραφές. [8]

- Εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής: Πρόκειται για διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για τη δημιουργία ηλεκτρονικής υπογραφής και πληροί τις απαιτήσεις του παραρτήματος ΙΙ του κανονισμού. Οι απαιτήσεις αυτές ορίζουν μεταξύ άλλων την ύπαρξη κατάλληλων μέτρων για να διασφαλίζεται η εμπιστευτικότητα των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής, η μοναδικότητα τους, η προστασία τους από πλαστογραφία και από χρήση από τρίτων. Παράλληλα ορίζουν ότι οι διατάξεις αυτές δεν μεταβάλλουν τα προς υπογραφή δεδομένα ούτε εμποδίζουν την υποβολή των δεδομένων αυτών στον υπογράφοντα πριν από την υπογραφή.

  Βάσει του άρθρου 30, η συμμόρφωση με τις απαιτήσεις αυτές πιστοποιείται από αρμόδιους φορείς που ορίζουν τα κράτη μέλη βάσει διαδικασίας αξιολόγησης ασφάλειας, όπως αναλυτικότερα περιγράφεται και στην ενότητα Εποπτεία & συμμόρφωση. Όπως ορίζει το άρθρο 31, μετά την χορήγηση της πιστοποίησης (αλλά και σε περίπτωση ακύρωσής της) τα κράτη μέλη οφείλουν να κοινοποιούν στην Επιτροπή τις εγκεκριμένες διατάξεις, και κατόπιν η Επιτροπή καταρτίζει, δημοσιεύει και συντηρεί κατάλογο με τις εν λόγω πιστοποιημένες εγκεκριμένες διατάξεις. [8]

- Εγκεκριμένο πιστοποιητικό για ηλεκτρονικές υπογραφές: Ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης ηλεκτρονικής υπογραφής με φυσικό πρόσωπο και επιβεβαιώνει τουλάχιστον το όνομα ή το ψευδώνυμο του εν λόγω προσώπου, εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις απαιτήσεις του παραρτήματος Ι του κανονισμού για την εγκεκριμένη μορφή. Βάσει του άρθρου 28 του κανονισμού, ένα εγκεκριμένο πιστοποιητικό μπορεί είτε να ανακληθεί μετά την αρχική ενεργοποίησή του, οπότε και παύει να ισχύει και δεν μπορεί να επανέλθει στην αρχική του κατάσταση, είτε να ανασταλεί προσωρινά, οπότε παύει να ισχύει όσο ισχύει η αναστολή. Σε αυτή την περίπτωση, πρέπει η διάρκεια της αναστολής να αναφέρεται σαφώς στη βάση δεδομένων για πιστοποιητικά και η αναστολή να είναι ορατή στην υπηρεσία που παρέχει πληροφορίες για το καθεστώς ισχύος του πιστοποιητικού. [8]

Μέσω της διαδικασία επικύρωσης εγκεκριμένης ηλεκτρονικής υπογραφής επιβεβαιώνεται η εγκυρότητα της εγκεκριμένης ηλεκτρονικής υπογραφής εφόσον πληρούνται οι προϋποθέσεις που ορίζονται στο άρθρο 32. Η διαδικασία αυτή παρέχεται μόνο από εγκεκριμένους παρόχους επικύρωσης που τηρούν τις προδιαγραφές αυτές, προσφέρουν το αποτέλεσμα της κοινοποίησης στα βασιζόμενα μέρη με αυτοματοποιημένο τρόπο και το αποτέλεσμα φέρει προηγμένη ηλεκτρονική υπογραφή ή σφραγίδα τους. Ακόμα, στο άρθρο 34 ορίζεται η εγκεκριμένη υπηρεσία διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών η οποία μπορεί να παρέχεται μόνο από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης ο οποίος χρησιμοποιεί διαδικασίες και τεχνολογίες ικανές να επεκτείνουν την αξιοπιστία της εγκεκριμένης ηλεκτρονικής υπογραφής πέραν της περιόδου τεχνολογικής ισχύος. [8]

Σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπογραφές. Ακόμα, οι εγκεκριμένες ηλεκτρονικές υπογραφές έχουν την ίδια νομική ισχύ με τις χειρόγραφες υπογραφές, ενώ εγκεκριμένη ηλεκτρονική υπογραφή βασιζόμενη σε εγκεκριμένο πιστοποιητικό που έχει εκδοθεί σε ένα κράτος μέλος αναγνωρίζεται ως τέτοια σε όλα τα άλλα κράτη μέλη. [8] [21]

Τέλος, για την χρήση σε δημόσιες υπηρεσίες ισχύουν βάσει του άρθρου 27 τα εξής: Σε περίπτωση που ένα κράτος μέλος απαιτεί προηγμένη ηλεκτρονική υπογραφή για τη χρήση δημόσιας επιγραμμικής υπηρεσίας πρέπει το κράτος μέλος αυτό να αναγνωρίζει, με μορφότυπους (format) και μεθόδους που ορίζονται από εκτελεστικές πράξεις, τις προηγμένες ηλεκτρονικές υπογραφές, τις προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής και τις εγκεκριμένες ηλεκτρονικές υπογραφές. Αν απαιτεί προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε εγκεκριμένο πιστοποιητικό, τότε πρέπει να αναγνωρίζει, πάλι με μορφότυπους και μεθόδους που ορίζονται από εκτελεστικές πράξεις τις προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής και τις εγκεκριμένες ηλεκτρονικές υπογραφές. Τέλος, τα κράτη μέλη δεν μπορούν να απαιτούν για τη διασυνοριακή χρήση μιας επιγραμμικής δημόσιας υπηρεσίας ηλεκτρονική υπογραφή με επίπεδο ασφάλειας υψηλότερο από αυτό της εγκεκριμένης ηλεκτρονικής υπογραφής. [8]

Ηλεκτρονική σφραγίδα

Πρόκειται για δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή, με σκοπό τη διασφάλιση της προέλευσης και της ακεραιότητάς τους και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει, όπου ο υπογράφων είναι νομικό πρόσωπο. Είναι το ισοδύναμο σε ηλεκτρονική μορφή της σφραγίδας που εφαρμόζεται σε ένα έγγραφο και μπορεί να χρησιμοποιηθεί επίσης και για να δηλώσει ότι το νομικό πρόσωπο συνέταξε το έγγραφο, ότι συμφωνεί με το περιεχόμενο του εγγράφου ή ακόμα και για να βεβαιώσει την παρουσία του ως μάρτυρα. [8] [9] [21]

Όπως και με τις ηλεκτρονικές υπογραφές, υπάρχουν τρία είδη ηλεκτρονικών σφραγίδων: η απλή, η προηγμένη και η εγκεκριμένη. Η προηγμένη ηλεκτρονική σφραγίδα έχει επιπλέον χαρακτηριστικά από την απλή καθώς (α) συνδέεται με μοναδικό τρόπο με τον δημιουργό της σφραγίδας, (β) μπορεί να τον ταυτοποιεί, (γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής σφραγίδας που επιτρέπουν στον υπογράφοντα να δημιουργεί σφραγίδες με υψηλό βαθμό εμπιστοσύνης και υπό τον έλεγχό του και (δ) συνδέεται με τέτοιο τρόπο με τα δεδομένα όπου κάθε μεταγενέστερη αλλαγή σε αυτά είναι αναγνωρίσιμη. Και σε αυτή την περίπτωση, η πλέον γνωστή τεχνολογία με την οποία καλύπτονται οι παραπάνω προϋποθέσεις είναι αυτή της υποδομής δημοσίου κλειδιού με τη χρήση πιστοποιητικών και κρυπτογραφικών κλειδιών.

Η εγκεκριμένη ηλεκτρονική σφραγίδα τέλος είναι μία προηγμένη υπογραφή που επιπρόσθετα έχει δημιουργηθεί από μία εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας (qualified seal creation device) και βασίζεται σε εγκεκριμένο πιστοποιητικό για ηλεκτρονικές σφραγίδες.

- Εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας: Πρόκειται για διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για τη δημιουργία ηλεκτρονικής σφραγίδας και πληροί τις απαιτήσεις του παραρτήματος ΙΙ του κανονισμού. Τα άρθρα 30 και 31 του κανονισμού για την πιστοποίηση και δημοσίευση καταλόγου με τις πιστοποιημένες διατάξεις δημιουργίας ηλεκτρονικών υπογραφών εφαρμόζονται κατ' αναλογία για τις διατάξεις ηλεκτρονικής σφραγίδας.
- Εγκεκριμένο πιστοποιητικό για ηλεκτρονικές σφραγίδες: Ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης ηλεκτρονικής υπογραφής με νομικό πρόσωπο και επιβεβαιώνει το όνομα του εν λόγω προσώπου, εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις απαιτήσεις του παραρτήματος ΙΙΙ του κανονισμού για την εγκεκριμένη μορφή. Βάσει του άρθρου 38 του κανονισμού, ένα εγκεκριμένο πιστοποιητικό μπορεί είτε να ανακληθεί μετά την αρχική ενεργοποίησή του, οπότε και παύει να ισχύει και δεν μπορεί να επανέλθει στην αρχική του κατάσταση, είτε να ανασταλεί προσωρινά, οπότε παύει να ισχύει όσο ισχύει η αναστολή. Σε αυτή την περίπτωση, πρέπει η διάρκεια της αναστολής να αναφέρεται σαφώς στη βάση δεδομένων για πιστοποιητικά και η αναστολή να είναι ορατή στην υπηρεσία που παρέχει πληροφορίες για το καθεστώς ισχύος του πιστοποιητικού. [8]

Τα άρθρα 32, 33 και 34 του κανονισμού για την επικύρωση και διαφύλαξη των ηλεκτρονικών υπογραφών εφαρμόζονται κατ' αναλογία για τις διατάξεις ηλεκτρονικής σφραγίδας.

Σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής σφραγίδας ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές σφραγίδες.

Η εγκεκριμένη ηλεκτρονική σφραγίδα αποδεικνύει την ακεραιότητα και ορθότητα προέλευσης των δεδομένων, ενώ εγκεκριμένη ηλεκτρονική σφραγίδα βασιζόμενη σε εγκεκριμένο πιστοποιητικό που έχει εκδοθεί σε ένα κράτος μέλος αναγνωρίζεται ως τέτοια σε όλα τα άλλα κράτη μέλη. [21]

Τέλος, κατ' αναλογία με τις ηλεκτρονικές υπογραφές για την χρήση σε δημόσιες υπηρεσίες ισχύουν βάσει του άρθρου 37 τα εξής: Σε περίπτωση που ένα κράτος μέλος απαιτεί προηγμένη ηλεκτρονική σφραγίδα για τη χρήση δημόσιας επιγραμμικής υπηρεσίας πρέπει το κράτος μέλος αυτό να αναγνωρίζει, με μορφότυπους και μεθόδους που ορίζονται από εκτελεστικές πράξεις, τις προηγμένες ηλεκτρονικές σφραγίδες, τις προηγμένες ηλεκτρονικές σφραγίδες που βασίζονται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας και τις εγκεκριμένες ηλεκτρονικές σφραγίδες. Αν απαιτεί προηγμένη ηλεκτρονική σφραγίδα που βασίζεται σε εγκεκριμένο πιστοποιητικό, τότε πρέπει να αναγνωρίζει, πάλι με μορφότυπους και μεθόδους που ορίζονται από εκτελεστικές πράξεις, τις προηγμένες ηλεκτρονικές σφραγίδες που βασίζονται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας και τις εγκεκριμένες ηλεκτρονικές σφραγίδες. Τέλος, τα κράτη μέλη δεν μπορούν να απαιτούν για τη διασυνοριακή χρήση μιας επιγραμμικής δημόσιας υπηρεσίας ηλεκτρονική σφραγίδα με επίπεδο ασφάλειας υψηλότερο από αυτό της εγκεκριμένης ηλεκτρονικής σφραγίδας. [8]

Ηλεκτρονική χρονοσφραγίδα

Πρόκειται για δεδομένα σε ηλεκτρονική μορφή τα οποία συνδέουν άλλα δεδομένα σε ηλεκτρονική μορφή με ένα συγκεκριμένο χρονικό σημείο, τεκμηριώνοντας ότι τα εν λόγω δεδομένα υπήρχαν κατά το χρονικό σημείο εκείνο. Ουσιαστικά μπορεί να χρησιμοποιηθεί για να αποδείξει την ύπαρξη ενός αρχείου μία δεδομένη χρονική στιγμή. [8] [9] [21]

Εκτός από την απλή μορφή, υπάρχει και η εγκεκριμένη ηλεκτρονική χρονοσφραγίδα, όπου οι απαιτήσεις τις είναι: (α) να υπάρχει σύνδεση ώρας και ημερομηνίας με τα δεδομένα ώστε η όποια τροποποίηση αυτών να είναι ανιχνεύσιμη, (β) η χρονική πηγή ακρίβειας να είναι συνδεδεμένη με την Συντονισμένη Παγκόσμια Ώρα και (γ) να φέρει εγκεκριμένη ηλεκτρονική υπογραφή ή ηλεκτρονική σφραγίδα εγκεκριμένου παρόχου ή ανάλογης μεθόδου. [8]

Σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής χρονοσφραγίδας ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες. Η εγκεκριμένη ηλεκτρονική χρονοσφραγίδα αποδεικνύει ακεραιότητα των δεδομένων και ακρίβεια ώρας και ημερομηνίας που αναφέρει, ενώ εγκεκριμένη ηλεκτρονική χρονοσφραγίδα που έχει εκδοθεί σε ένα κράτος μέλος αναγνωρίζεται ως τέτοια σε όλα τα άλλα κράτη μέλη. [21] [8]

Ηλεκτρονική υπηρεσία συστημένης παράδοσης

Πρόκειται για υπηρεσία που επιτρέπει την ηλεκτρονική μεταφορά δεδομένων μεταξύ επιχειρήσεων, δημοσίων φορέων και πολιτών, παρέχοντας αποδείξεις για την αποστολή και λήψη των δεδομένων, ενώ παράλληλα τα προστατεύει από απώλεια, κλοπή, ζημιά και μη εξουσιοδοτημένες τροποποιήσεις. [9]

Οι απαιτήσεις για την εγκεκριμένη ηλεκτρονική υπηρεσία συστημένης παράδοσης είναι: (α) να παρέχεται από εγκεκριμένο πάροχο, (β) να εξασφαλίζει ταυτοποίηση αποστολέα με υψηλό επίπεδο εμπιστοσύνης, (γ) να εξασφαλίζει ταυτοποίηση αποδέκτη πριν την παράδοση, (δ) η αποστολή/λήψη δεδομένων να εξασφαλίζεται με προηγμένη ηλεκτρονική υπογραφή ή σφραγίδα εγκεκριμένου παρόχου, (ε) οι απαιτούμενες τροποποιήσεις δεδομένων για την αποστολή/λήψη να δηλώνονται σαφώς, (στ) η ημερομηνία, ο χρόνος αποστολής, παραλαβής και οι αλλαγές να δηλώνονται με εγκεκριμένη ηλεκτρονική χρονοσφραγίδα και (ζ) για μεταφορά δεδομένων μεταξύ 2 παρόχων να ισχύουν όλα τα παραπάνω. [8]

Σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής χρονοσφραγίδας ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για την εγκεκριμένη ηλεκτρονική υπηρεσία συστημένης παράδοσης.

Η εγκεκριμένη ηλεκτρονική υπηρεσία συστημένης παράδοσης αποδεικνύει την ακεραιότητα των δεδομένων, την ακρίβεια ώρας και ημερομηνίας αποστολής και λήψης, καθώς και την αποστολή και λήψη από ταυτοποιημένο αποστολέα και παραλήπτη αντίστοιχα. [8]

Υπηρεσία πιστοποιητικών για την επαλήθευση της ταυτότητας ιστοτόπων

Πρόκειται για ηλεκτρονικά πιστοποιητικά που εκδίδονται με σκοπό την απόδειξη ότι μία ιστοσελίδα ανήκει σε ένα συγκεκριμένο φυσικό ή νομικό πρόσωπο, ενώ παράλληλα βοηθούν στην επαλήθευση γνησιότητας του ιστοτόπου και κατά συνέπεια στην αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος (phishing attacks). [8] [9]

Οι απαιτήσεις για τα εγκεκριμένα πιστοποιητικά γνησιότητας ιστοτόπου παρουσιάζονται στο παράρτημα IV του κανονισμού και περιλαμβάνουν ενδεικτικά: (α) ένδειξη σε μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία ότι το πιστοποιητικό είναι εγκεκριμένο, (β) ένα σύνολο δεδομένων που αντιπροσωπεύει αδιαμφισβήτητα τον εγκεκριμένο πάροχο που εκδίδει το εν λόγω πιστοποιητικό, (γ) το όνομα του φυσικού ή νομικού προσώπου και τον αριθμό μητρώου αν πρόκειται για νομικό πρόσωπο, (δ) στοιχεία διεύθυνσης του προσώπου, (ε) το όνομα χώρου (domain name) που ανήκει στο φυσικό ή νομικό πρόσωπο για το οποίο έχει εκδοθεί το πιστοποιητικό, (στ) πληροφορίες για την έναρξη και λήξη ισχύος του, (ζ) κωδικό ταυτότητας πιστοποιητικού, (η) την προηγμένη ηλεκτρονική υπογραφή ή σφραγίδα του παρόχου που το εκδίδει, (θ) την τοποθεσία που διατίθεται δωρεάν το πιστοποιητικό και (ι) την τοποθεσία στην οποία παρέχονται πληροφορίες για την κατάσταση ισχύος των πιστοποιητικών. [8]

Εποπτεία & συμμόρφωση

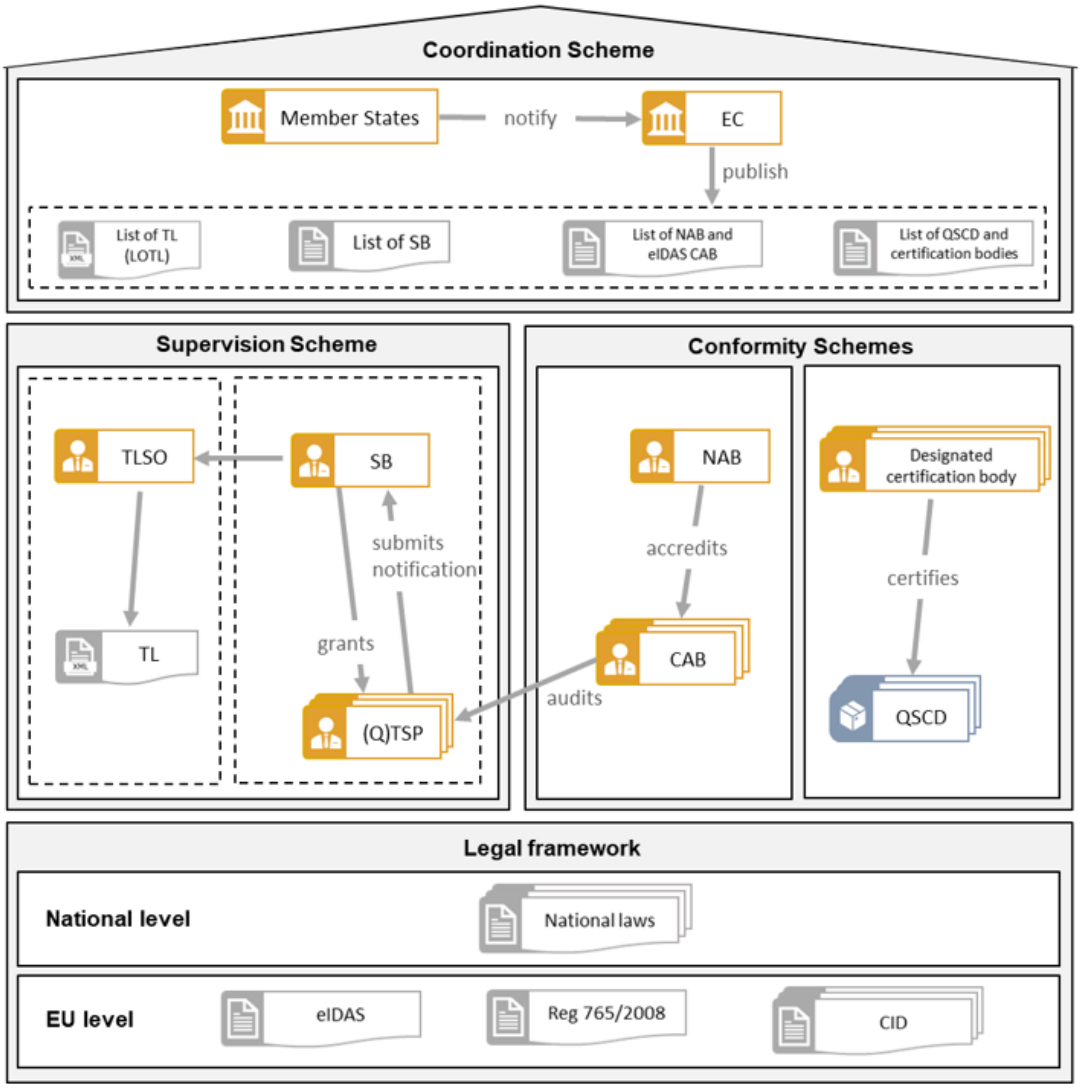
Η συμμόρφωση με τις απαιτήσεις του κανονισμού ελέγχεται, εποπτεύεται και πιστοποιείται ανά τακτά χρονικά διαστήματα. Για το σκοπό αυτό αναγνωρίζονται τα ακόλουθα σχήματα: [20]

- Σχήματα συμμόρφωσης [20]:
    1. Η συμμόρφωση ενός εγκεκριμένου παρόχου υπηρεσιών εμπιστοσύνης (Qualified Trust Service Provider - QTSP) με τις προδιαγραφές του eIDAS ελέγχεται στην αρχή αλλά και σε τακτά χρονικά διαστήματα από έναν οργανισμό αξιολόγησης συμμόρφωσης (Conformity Assessment Body - CAB). Ο οργανισμός αυτός διαπιστεύεται από έναν εθνικό οργανισμό διαπίστευσης (National Accreditation Body - NAB) ως ικανός να μπορεί να αξιολογεί τη συμμόρφωση των εν λόγω παρόχων.
    2. Η συμμόρφωση των εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής/σφραγίδας με τις προδιαγραφές του eIDAS πιστοποιείται από κάποιο κατάλληλο ιδιωτικό ή δημόσιο οργανισμό πιστοποίησης που υποδεικνύεται από τα κράτη-μέλη (designated certification bodies).
- Σχήματα εποπτείας [20]:
    1. Η αναγνώριση ενός παρόχου υπηρεσιών εμπιστοσύνης και των υπηρεσιών του ως εγκεκριμένων γίνεται μετά την απόφαση ενός εποπτικού φορέα (Supervisory Body - SB) βάσει της αναφοράς αξιολόγησης συμμόρφωσης που εκδίδει ο οργανισμός αξιολόγησης συμμόρφωσης.

       Η απόφαση αυτή αντικατοπτρίζεται στον εθνικό κατάλογο εμπιστοσύνης (Trusted List - TL). Πρόκειται για ένα αρχείο σε μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία που είναι ηλεκτρονικά υπογεγραμμένο ή σφραγισμένο και περιλαμβάνει πληροφορίες για τους εγκεκριμένους παρόχους και τις εγκεκριμένες υπηρεσίες που οι τελευταίοι παρέχουν. Το αρχείο αυτό καταρτίζεται και συντηρείται από κάποιον φορέα του κάθε κράτους μέλους που ονομάζεται χειριστής του σχήματος καταλόγου εμπιστοσύνης (TL scheme operator – TLSO). Τα στοιχεία του χειριστή κοινοποιούνται από τα κράτη μέλη στην Επιτροπή και η τελευταία τα θέτει στη διάθεση του κοινού μέσω ασφαλούς διαύλου. [8] [20]

Οι εγκεκριμένοι πάροχοι και υπηρεσίες εποπτεύονται από τους εποπτικούς φορείς καθ' όλη τη διάρκεια του κύκλο ζωής τους και οι όποιες αλλαγές αντικατοπτρίζονται στον κατάλογο. [20]

Τέλος, μετά την καταχώρηση της έγκρισης στον κατάλογο εμπιστοσύνης, βάσει του άρθρου 23 του κανονισμού, οι εγκεκριμένοι πάροχοι μπορούν να χρησιμοποιούν το ενωσιακό σήμα εμπιστοσύνης (EU Trusted Mark) ώστε να επισημαίνουν τις εγκεκριμένες υπηρεσίες που προσφέρουν και πρέπει να φροντίζουν να υπάρχει στον ιστότοπό τους σύνδεσμος προς τον σχετικό κατάλογο εμπιστοσύνης.



Εικόνα 1.1: Το πλαίσιο των υπηρεσιών εμπιστοσύνης του eIDAS

Όλοι οι εθνικοί οργανισμοί που ορίζονται στο eIDAS, οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής σφραγίδας/υπογραφής και οι πληροφορίες σχετικές με τους καταλόγους εμπιστοσύνης, κοινοποιούνται από τα κράτη μέλη για δημοσίευση σε ευρωπαϊκούς κεντρικούς καταλόγους που διαχειρίζεται η Ευρωπαϊκή Επιτροπή. [20]

Οι κατάλογοι αυτοί είναι [20]:

- Ο κατάλογος των καταλόγων εμπιστοσύνης που περιλαμβάνει πληροφορίες για τους επιμέρους καταλόγους όπως την τοποθεσία τους και τα πιστοποιητικά με τα οποία υπογράφονται ψηφιακά
- Ο κατάλογος των εποπτικών φορέων
- Ο κατάλογος των εθνικών οργανισμών διαπίστευσης και των οργανισμών αξιολόγησης συμμόρφωσης που οι πρώτοι έχουν διαπιστεύσει
- Ο κατάλογος των κατάλληλων οργανισμών πιστοποίησης και των εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής/σφραγίδας που οι πρώτοι έχουν πιστοποιήσει

Το σύνολο των οργανισμών και προϊόντων που καταγράφονται στους κεντρικούς ευρωπαϊκούς καταλόγους, καθώς και το περιεχόμενο του καταλόγου εμπιστοσύνης συγκροτούν την «βάση εμπιστοσύνης» (trust backbone - TB), η οποία αναλυτικότερα περιλαμβάνει [20]:

- Καταλόγους εμπιστοσύνης
- Πληροφορίες που έχουν κοινοποιηθεί από τα κράτη-μέλη και έχουν δημοσιευθεί από την Ευρωπαϊκή Επιτροπή:
    - Πληροφορίες που έχουν κοινοποιηθεί από τους χειριστές των σχημάτων καταλόγων εμπιστοσύνης και έχουν δημοσιευθεί στον κατάλογο των καταλόγων εμπιστοσύνης (όπως η τοποθεσία του καταλόγου εμπιστοσύνης, το πιστοποιητικό με το οποίο υπογράφεται, πληροφορίες για τους χειριστές)
    - Τον κατάλογο των εποπτικών φορέων
    - Τον κατάλογο των εθνικών οργανισμών διαπίστευσης και των οργανισμών αξιολόγησης συμμόρφωσης που οι πρώτοι έχουν διαπιστεύσει
    - Τον κατάλογο των κατάλληλων οργανισμών πιστοποίησης και των εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής/σφραγίδας που οι πρώτοι έχουν πιστοποιήσει (συμπεριλαμβανομένων και των εναλλακτικών διαδικασιών πιστοποίησης που ορίζονται από τους εν λόγω οργανισμούς)

1.3 Οφέλη κανονισμού για πολίτες και επιχειρήσεις

Πιο αναλυτικά, με την εφαρμογή του eIDAS 1.0 στην ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης, τόσο οι επιχειρήσεις όσο και οι πολίτες επωφελούνται σε πολλά επίπεδα. Οι πολίτες απολαμβάνουν μία πιο αποδοτική και ασφαλή ψηφιακή ζωή, ενώ οι επιχειρήσεις μπορούν να αξιοποιούν διασυνοριακές επιχειρηματικές ευκαιρίες και να προσφέρουν καλύτερη εμπειρία χρήστη με μεγαλύτερη ασφάλεια και αποδοτικότητα στις υπηρεσίες τους. [22] [23]

Ένα απλό παράδειγμα από τα πλεονεκτήματα για τον πολίτη φαίνεται μέσα από τη βελτιωμένη διαδικασία που μπορεί ένας φοιτητής να ακολουθήσει για την εγγραφή σε ένα πανεπιστήμιο του εξωτερικού για μεταπτυχιακό. Μέσω της ιστοσελίδας του πανεπιστημίου μπορεί ο φοιτητής να κάνει την αίτησή του χρησιμοποιώντας στη διαδικασία την ηλεκτρονική ταυτοποίηση αντί να ταξιδέψει και να ταυτοποιηθεί δια ζώσης. Την αίτηση μπορεί να υπογράψει απευθείας ηλεκτρονικά χωρίς να χρειαστεί να την τυπώσει, ενώ στη συνέχεια μπορεί να αποστείλει το πτυχίο του με την υπηρεσία συστημένης παράδοσης για να ολοκληρώσει τη διαδικασία. Τέλος το πανεπιστήμιο θα αποστείλει την επιβεβαίωση της εγγραφής με ηλεκτρονική σφραγίδα, εξασφαλίζοντας τη γνησιότητα και προέλευση του αρχείου, και πάλι με την υπηρεσία συστημένης παράδοσης. [24]

Ένα δεύτερο παράδειγμα που αναδεικνύει τα οφέλη για μία επιχείρηση μεταφορών είναι το εξής: Ένας πελάτης από την Πορτογαλία επιθυμεί να μεταφέρει κάποια έργα τέχνης στην Γαλλία, μέσω μίας μεταφορικής εταιρίας που έχει τη βάση της στην Ισπανία. Η σύμβαση για τη μεταφορά φέρει ηλεκτρονική σφραγίδα για την επιβεβαίωση της προέλευσης και της ακεραιότητάς της. Στη συνέχεια γίνεται χρήση ηλεκτρονικής χρονοσφραγίδας όταν τα προϊόντα αλλάζουν μεταφορέα. Τα έγγραφα αποστέλλονται στους μεταφορείς μέσω της ηλεκτρονικής υπηρεσίας συστημένης παράδοσης, ενώ με τη βοήθεια της ηλεκτρονικής χρονοσφραγίδας αποδεικνύεται ότι μία καθυστέρηση στην παράδοση οφείλεται σε ένα συγκεκριμένο μεταφορέα. Συνολικά η διαδικασία έχει μικρότερα κόστη, απαιτεί λιγότερο χρόνο για την ανταλλαγή εγγράφων και προσφέρει μεγαλύτερη αξιοπιστία καθ' όλη τη διάρκεια.

Ο Πίνακας *1.1* παρουσιάζει συγκεντρωτικά τα πλεονεκτήματα της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης: [22] [23]

Πίνακας 1.1: Πλεονεκτήματα ηλεκτρονικής ταυτοποίησης και υπηρεσιών εμπιστοσύνης

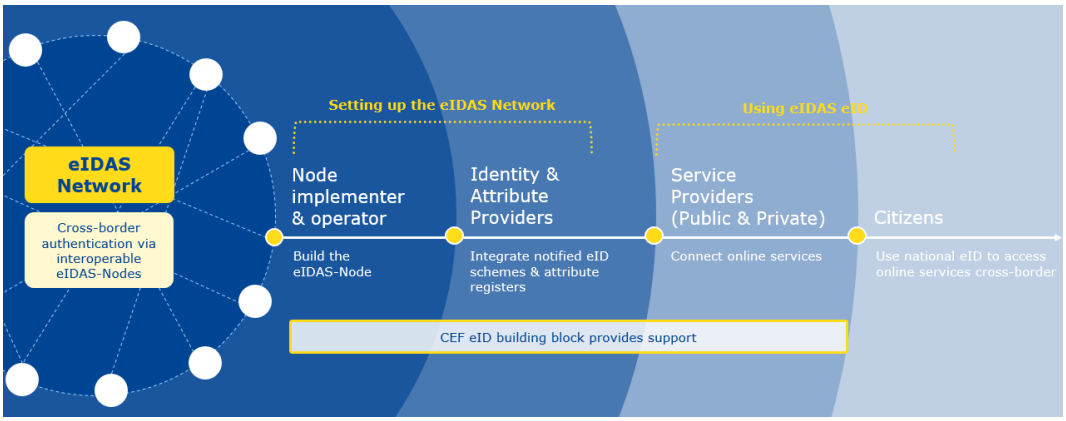
	Πολίτες	Επιχειρήσεις
Ηλεκτρονική Ταυτοποίηση	Διευκόλυνση για την απομακρυσμένη ταυτο-ποίηση πχ. για άνοιγμα λογαριασμού σε ξένη χώρα με την εθνική ταυτότητα	Μεγαλύτερη βάση πελατών Εμπιστοσύνη σε διασυνοριακές συναλλαγές Διευκόλυνση για επιχειρήσεις και πολίτες
Ηλεκτρονική Υπογραφή	Υπογραφή εγγράφων & emails χωρίς την ανάγκη εκτύπωσης	Μικρότερα κόστη και διάρκεια ολοκλήρωσης διαδικασιών που απαιτούν υπογραφές
Ηλεκτρονική Χρονοσφραγίδα	Απόδειξη αγοράς προϊόντος	Καλύτερη παρακολούθηση εγγράφων και υψηλότερη λογοδοσία
Υπηρεσία πιστοποιητικών για την επαλήθευση της ταυτότητας ιστοτόπων	Επιβεβαίωση της γνησιότητας και ασφάλειας των ιστοσελίδων που επισκέπτονται οι χρήστες	Μεγαλύτερη εμπιστοσύνη από τους καταναλωτές και συμβολή στην αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος προστατεύοντας την φήμη της επιχείρησης
Ηλεκτρονική υπηρεσία συστημένης παράδοσης	Επιβεβαίωση ότι δέματα φτάνουν στον προορισμό τους με ασφάλεια	Μικρότερα κόστη και διάρκεια για την ανταλλαγή εγγράφων Μεγαλύτερη αποδοτικότητα και εμπιστοσύνη Βελτιωμένη παρακολούθηση πορείας εγγράφων
Ηλεκτρονική Σφραγίδα	Επιβεβαίωση γνησιότητας προϊόντων που έχουν αγοραστεί ηλεκτρονικά	Μικρότερα κόστη και διάρκεια μέσα από βελτιωμένες διαδικασίες

1.4 Τεχνική περιγραφή δικτύου eIDAS

Το δίκτυο του eIDAS είναι η τεχνική υποδομή που διασυνδέει τα εθνικά συστήματα eID και αποτελείται από ένα σύνολο διασυνδεδεμένων κόμβων[7], οι οποίοι ζητούν ή απαντούν στα αιτήματα για διασυνοριακή ταυτοποίηση. Κάθε κράτος μέλος έχει υπ' ευθύνη του την υλοποίηση και υποστήριξη ενός κόμβου, καθώς επίσης και τη σύνδεση αυτού με τους εθνικούς παρόχους ταυτότητας και αναγνωριστικών (Identity & Attribute providers) ώστε τα εθνικά συστήματα eID να είναι προσβάσιμα από διασυνοριακές ηλεκτρονικές υπηρεσίες. [16]

Οντότητες οικοσυστήματος

Στο οικοσύστημα αυτό συμμετέχουν δημόσιες και ιδιωτικές οντότητες οι οποίες διακρίνονται σε δύο ομάδες ανάλογα με το αν συμμετέχουν στην οργάνωση και λειτουργία του δικτύου κάνοντας τα εθνικά συστήματα eID διαλειτουργικά με τη βοήθεια του "ψηφιακού δομικού στοιχείου eID" (digital eID building block[8]), ή αν χρησιμοποιούν το eID ώστε να κάνουν τις ηλεκτρονικές υπηρεσίες τους διαθέσιμες από ξένα κοινοποιημένα συστήματα, με την υποστήριξη των κρατών-μελών. Στην Εικόνα 1.2 φαίνονται αναλυτικά οι οντότητες. [25]



Εικόνα 1.2: Οντότητες και λειτουργίες δικτύου eIDAS

Οντότητες που συμμετέχουν στη διαμόρφωση του δικτύου eIDAS

- Υπεύθυνοι υλοποίησης & λειτουργίας κόμβων (Node implementers & operators): Πρόκειται για δημόσιους φορείς ή ιδιωτικούς οργανισμούς που ορίζονται από κάθε κράτος μέλος και έχουν υπό την ευθύνη τους την υλοποίηση και λειτουργία του εθνικού κόμβου. Η υλοποίηση και η λειτουργία μπορεί να υποστηρίζονται από διαφορετικές ή την ίδια οντότητα, ενώ κατά τη φάση της υλοποίησης, υποχρεωτική είναι η διασύνδεση με το δίκτυο eIDAS, ενώ προαιρετική είναι η διασύνδεση με εθνικούς παρόχους ταυτότητας και αναγνωριστικών. [25]

[7] Στον εκτελεστικό κανονισμό 2015/1501 ως κόμβος 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 άλλους κόμβους, επιτρέποντας τις εθνικές υποδομές ηλεκτρονικής ταυτοποίησης ενός κράτους μέλους να διασυνδέεται με τις εθνικές υποδομές ηλεκτρονικής ταυτοποίησης άλλων κρατών μελών»* [19]

[8] Τα εν λόγω δομικά στοιχεία είναι ψηφιακές λύσεις ανοιχτές και επαναχρησιμοποιήσιμες, που βασίζονται σε πρότυπα και επιτελούν βασικές λειτουργίες όπως επαλήθευση ταυτότητας και η ασφαλή ανταλλαγή δεδομένων. Μπορούν να αξιοποιούνται σε διάφορα ευρωπαϊκά έργα για να διευκολύνουν την διασυνοριακή υλοποίηση ψηφιακών δημόσιων υπηρεσιών. [90]

- Ενιαίο σημείο επαφής/εξυπηρέτησης (Single point of contact): Πρόκειται για μία δημόσια οντότητα ανά χώρα ή ένα πρόσωπο που την εκπροσωπεί, που έχει ως αρμοδιότητα να υποστηρίζει τους παρόχους ταυτότητας και υπηρεσιών να συνδεθούν με το δίκτυο eIDAS, ενώ πρέπει να έχει γνώσεις επί των τεχνικών, εκτελεστικών και νομικών διαδικασιών. [25]
- Πάροχοι ταυτότητας (Identity providers): Είναι οι δημόσιοι φορείς ή ιδιωτικοί οργανισμοί που εκδίδουν τα μέσα ηλεκτρονικής ταυτοποίησης και είναι υπεύθυνοι για την λειτουργία της διαδικασίας της ταυτοποίησης. Παρέχουν στους χρήστες μία ασφαλή ηλεκτρονική ταυτότητα η οποία μπορεί να χρησιμοποιηθεί με ένα εθνικό eID σύστημα. Για να μπορεί να είναι διαθέσιμο το σύστημα τους σε πολίτες και επιχειρήσεις ώστε να το αξιοποιήσουν για να αποκτήσουν πρόσβαση σε ηλεκτρονικές υπηρεσίες άλλων χωρών, πρέπει να συνδεθούν με τον εθνικό κόμβο eIDAS. Επιπρόσθετα, οι πάροχοι αυτοί λαμβάνουν μέρος στη διαδικασία κοινοποίησης δίνοντας τις απαραίτητες πληροφορίες για το εθνικό eID σύστημα, για τον καθορισμό του επιπέδου διασφάλισής του. [25]

  Πάροχοι αναγνωριστικών (Attribute providers): Αναφέρεται στις οντότητες που διαχειρίζονται και παρέχουν πληροφορίες σχετικές με την ηλεκτρονική ταυτότητα, που είναι πρόσθετες από τις ελάχιστες που ορίζονται από τον κανονισμό ως απαραίτητες και μπορεί να απαιτούνται για την ταυτοποίηση σε συγκεκριμένες περιπτώσεις. Οι πάροχοι αυτοί πρέπει να συνδέονται με τον εθνικό eIDAS κόμβο ώστε να καταστήσουν διαθέσιμα τα μητρώα δεδομένων τους στο δίκτυο eIDAS. [25]

Οντότητες που συμμετέχουν στην χρήση του δικτύου eIDAS

- Δημόσιοι πάροχοι υπηρεσιών (Public Service providers): Πρόκειται για τους δημόσιους φορείς που παρέχουν ηλεκτρονικές υπηρεσίες στους πολίτες της Ένωσης. Οι φορείς των οποίων οι υπηρεσίες παρέχονται σε εθνικό επίπεδο και απαιτούν διασφάλιση επιπέδου υψηλού (substantial/high level) είναι υποχρεωμένοι από τον κανονισμό να δίνουν πρόσβαση και σε χρήστες άλλων χωρών της Ένωσης, που χρησιμοποιούν εθνικό σύστημα eID που έχει κοινοποιηθεί. Για την σύνδεσή τους με τον εθνικό κόμβο, υποστηρίζονται από τα κράτη-μέλη. [25]
- Ιδιωτικοί πάροχοι υπηρεσιών (Private Service providers): Είναι ιδιωτικοί οργανισμοί που παρέχουν υπηρεσίες στους πολίτες της Ένωσης που είτε χρησιμοποιούν ήδη εθνικά μέσα ηλεκτρονικής ταυτοποίησης ή θα μπορούσαν να επωφεληθούν από τη χρήση τους. Δεν υποχρεούνται βάσει του κανονισμού να δέχονται ηλεκτρονικές ταυτότητες άλλων χωρών αλλά έχουν κίνητρο ως προς αυτή την κατεύθυνση. [25]
- Έργα της ΕΕ σε συγκεκριμένους τομείς (Sector-specific EU projects): Πρόκειται για συγκεκριμένα έργα που προσφέρουν κάποια ηλεκτρονική υπηρεσία που χρησιμοποιεί ηλεκτρονική ταυτότητα για την πρόσβαση σε αυτή. [25]
- Πολίτες της ΕΕ (EU Citizens): Είναι οι τελικοί επωφελούμενοι από τη χρήση του eID, καθώς μπορούν να χρησιμοποιούν τις ταυτότητες που έχουν εκδοθεί στη χώρα τους για να έχουν πρόσβαση σε υπηρεσίες άλλων χωρών. [25]
- Ευρωπαϊκή επιτροπή (EU Commission) [25]
    - Η Γενική Διεύθυνση Ψηφιακών Υπηρεσιών (Directorate-General for Informatics - DIGIT) είναι υπεύθυνη για την τεχνική διαχείριση του ψηφιακού δομικού στοιχείου eID.

- Η Γενική Διεύθυνση για Δίκτυα Επικοινωνιών, Περιεχομένου και Τεχνολογίας (Directorate-General for Communications Networks, Content and Technology - DG CNECT) είναι υπεύθυνη για την εφαρμογή της πολιτικής που σχετίζεται με την ηλεκτρονική ταυτότητα και τις υπηρεσίες εμπιστοσύνης.
- Ο Εκτελεστικός Οργανισμός Καινοτομίας και Δικτύων (Innovation and Networks Executive Agency - INEA) είναι υπεύθυνος για την εφαρμογή των επιχορηγήσεων του DIGITAL Telecom) σε συνεργασία με την Επιτροπή.

- Συμμετοχή κρατών-μελών (Member state participation): Ομάδες εκπροσώπησης των κρατών μελών που συντονίζονται από την Επιτροπή περιλαμβάνουν: Το δίκτυο συνεργασίας (Cooperation Network), την ομάδα εμπειρογνωμόνων του eIDAS (eIDAS Expert Group) και την τεχνική υπο-ομάδα του eIDAS (eIDAS Technical Sub-group). Οι ομάδες αυτές συμβάλλουν τακτικά στη διαχείριση διαφόρων πτυχών της διαδικασίας εφαρμογής του eIDAS, συμπεριλαμβανομένου του συντονισμού της πολιτικής για το eIDAS, της διαδικασίας κοινοποίησης του eIDAS και της ανάπτυξης, συντήρησης και λειτουργίας του ψηφιακού δομικού στοιχείου eID. [25]

Τρόπος λειτουργίας

Όπως έχει αναφερθεί και ανωτέρω μέσω της εφαρμογής της λύσης του eIDAS, οι πολίτες μπορούν να αποδεικνύουν αλλά και να επαληθεύουν την ταυτότητά τους όταν αποκτούν πρόσβαση σε υπηρεσίες άλλων κρατών μελών, με τη χρήση του eID. Πιο αναλυτικά, όταν θέλουν να χρησιμοποιήσουν τις εν λόγω υπηρεσίες και τους ζητείται να επαληθεύσουν την ταυτότητά τους, το αίτημα για ταυτοποίηση μεταφέρεται μέσω του eIDAS δικτύου στο κράτος-μέλος του χρήστη και συγκεκριμένα στον πάροχο ταυτότητάς του. Μετά, το αποτέλεσμα της ταυτοποίησης επιστρέφεται στον πάροχο της υπηρεσίας και ο χρήστης αποκτά πρόσβαση σε αυτή. [26]

Πρακτικά καθίσταται εφικτή η διαλειτουργικότητα μεταξύ των διάφορων εθνικών πρωτοκόλλων eID, με τη βοήθεια του πρωτοκόλλου eIDAS που «μεταφράζει» τα δεδομένα ταυτοποίησης της κάθε χώρας σε μία κοινώς αποδεκτή μορφή που είναι κατανοητή από όλα τα κράτη-μέλη. Το κύριο πλεονέκτημα της λύσης αυτής είναι ότι κάθε χώρα μπορεί και διατηρεί τα δικά της πρωτόκολλα που χρησιμοποιούνται για την επαλήθευση ταυτότητας σε εθνικό επίπεδο, χωρίς την ανάγκη εφαρμογής αλλαγών στην υπάρχουσα αρχιτεκτονική. Κάθε κόμβος eIDAS ωστόσο περιέχει ένα κομμάτι διαφορετικό για κάθε χώρα που πρέπει να υλοποιηθεί, ώστε τα «τοπικά» πρωτόκολλα να μεταφραστούν στο πρωτόκολλο eIDAS. [26]

- Αίτηση διασυνοριακής ταυτοποίησης: Όταν κατά την αίτηση επαλήθευσης ταυτότητας για την πρόσβαση σε μία ηλεκτρονική υπηρεσία διαπιστώνεται ότι ο χρήστης ανήκει σε άλλο κράτος-μέλος, εκδίδεται ένα αίτημα ταυτοποίησης προς αυτή τη χώρα, το οποίο μεταφράζεται με τη βοήθεια του πρωτοκόλλου eIDAS και δρομολογείται μέσω του δικτύου eIDAS από τον έναν εθνικό κόμβο στον άλλο.

  Το στοιχείο των κόμβων eIDAS που χρησιμοποιείται για τα αιτήματα διασυνοριακής ταυτοποίησης ονομάζεται eIDAS-Connector. [26]

- Παροχή διασυνοριακής ταυτοποίησης: Για την παροχή της υπηρεσίας επαλήθευσης ταυτότητας του χρήστη από το κράτος-μέλος στο οποίο ανήκει χρησιμοποιείται ο αντίστοιχος κόμβος eIDAS και συγκεκριμένα η υπηρεσία με το όνομα eIDAS-service, που λειτουργεί με δύο τρόπους: [26]
  - eIDAS-Proxy-Service: Η υπηρεσία λειτουργείται από το κράτος μέλος του χρήστη και παρέχει τα δεδομένα ηλεκτρονικής ταυτοποίησης.

- eIDAS-Middleware-Service: Η υπηρεσία και τα δεδομένα ηλεκτρονικής ταυτοποίησης παρέχονται σε ένα ενδιάμεσο λογισμικό από το κράτος-μέλος του χρήστη στην χώρα που ο τελευταίος αιτείται πρόσβασης στην υπηρεσία. Το ενδιάμεσο αυτό λογισμικό πρέπει να ενσωματωθεί με τον eIDAS-connector στο κράτος-μέλος που λαμβάνει αρχικά το αίτημα ταυτοποίησης.

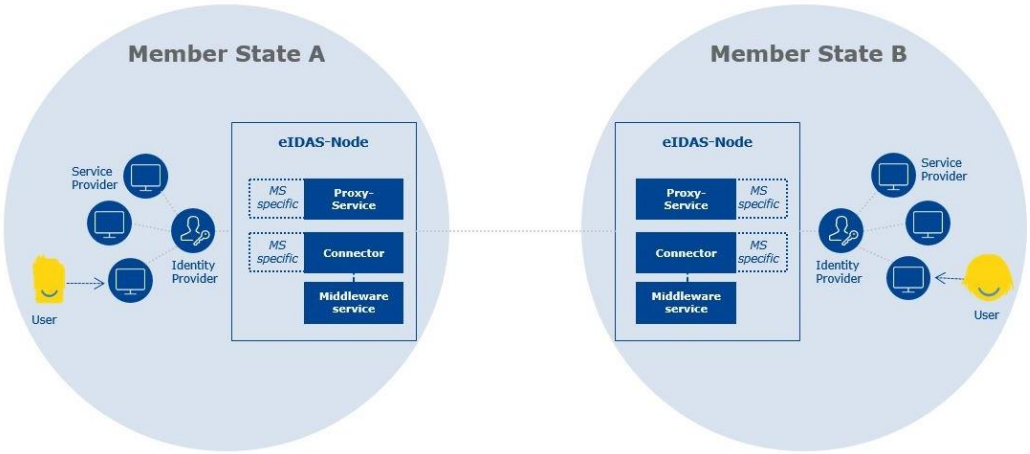
Ως εκ τούτου, η διασυνοριακή επαλήθευση ταυτότητας μπορεί να γίνει με 4 πιθανούς τρόπους (proxy to proxy, proxy to middleware, middleware to proxy, middleware to middleware), ανάλογα με τον τρόπο λειτουργίας του eIDAS-service στην χώρα του χρήστη που αιτείται την ταυτοποίηση και αντίστοιχα ανάλογα με τον τρόπο λειτουργίας του eIDAS-service στην χώρα που προσφέρεται η ηλεκτρονική υπηρεσία στην οποία θέλει να έχει πρόσβαση ο χρήστης.

Για τη διασύνδεση των διαφόρων μερών στο δίκτυο του eIDAS, ο κάθε κόμβος παρέχει ένα σύνολο από διεπαφές: [26]

- Διεπαφή για εθνικούς παρόχους ταυτοτήτων: Χρησιμοποιείται για τη σύνδεση του κόμβου του κράτους-μέλους που ανήκει ο χρήστης με τον εθνικό πάροχο ταυτότητας.
- Διεπαφή για παρόχους υπηρεσιών στο κράτος μέλος που είναι εγκατεστημένος ο κόμβος eIDAS: Πρόκειται για τη διεπαφή του κόμβου eIDAS μέσω της οποίας οι πάροχοι υπηρεσιών στέλνουν αιτήματα επαλήθευσης ταυτότητας και λαμβάνουν τις απαντήσεις.
- Διεπαφή με άλλους κόμβους eIDAS: Χρησιμοποιείται για την επικοινωνία μεταξύ κόμβων των διαφόρων κρατών μελών, ώστε να καθίσταται δυνατή η διαλειτουργικότητα της λύσης eID και υλοποιείται με τη βοήθεια δύο eIDAS-connectors, έναν σε κάθε κόμβο που ζητάει και παρέχει τις πληροφορίες σχετικές με την ταυτότητα του χρήστη αντίστοιχα.

  Επίσης ο κόμβος επιτρέπει στο χρήστη να επιλέξει ο ίδιος τη χώρα της οποίας το σύστημα eID θα χρησιμοποιηθεί, αν δεν έχει ήδη γίνει η επιλογή από τον πάροχο της υπηρεσίας.

Στην Εικόνα 1.3 παρουσιάζονται τα μέρη και τα συστατικά στοιχεία της αρχιτεκτονικής eIDAS. Όπως αναφέρθηκε και ανωτέρω, μεταξύ δύο κόμβων η επικοινωνία γίνεται μέσω του πρωτοκόλλου eIDAS στο οποίο έχουν μεταφραστεί τα εθνικά πρωτόκολλα. [26]



Εικόνα 1.3: Συστατικά στοιχεία αρχιτεκτονικής eIDAS

Στη διαδικασία συμμετέχουν:

- Δύο κράτη μέλη (A & B): Το σύστημα eID ενός κράτους-μέλους χρησιμοποιείται στη διαδικασία επαλήθευσης ταυτότητας και στέλνει τα δεδομένα στο άλλο μέλος, όπου βρίσκεται η υπηρεσία μέσω της οποίας ζητείται η επαλήθευση ταυτότητας.
- Ένας χρήστης που μπορεί να είναι φυσικό ή νομικό πρόσωπο
- Ένας πάροχος υπηρεσίας που μπορεί να είναι δημόσιος ή ιδιωτικός
- Οι κόμβοι eIDAS των δύο κρατών μελών
- Ο εθνικός πάροχος ταυτότητας του κράτους μέλους που κάνει την επαλήθευση ταυτότητας και στέλνει τα δεδομένα μετά την επιτυχή ολοκλήρωση της διαδικασίας
- Ο εθνικός πάροχος ταυτότητας του άλλου κράτους μέλους, που ενδέχεται ανά περιπτώσεις να μην χρησιμοποιείται, και ο πάροχος υπηρεσίας να αλληλεπιδρά απευθείας με τον κόμβο eIDAS. [26]

1.5 Στατιστικά υιοθέτησης κανονισμού από τα κράτη μέλη ως το 2024

Βάσει των τελευταίων δημοσιευμένων στατιστικών στοιχείων (Q2 2024) για την μέχρι τώρα εφαρμογή του eID στην ΕΕ ισχύουν τα εξής [27]:

- 24 από τις 30 χώρες της ΕΕ & ΕΟΧ έχουν 36 κοινοποιημένα συστήματα eID, με την Εσθονία να παρέχει 7 από αυτά, ενώ η Ελλάδα δεν διαθέτει κοινοποιημένο σύστημα.
- 16 χώρες έχουν συνδεθεί μέσω των eIDAS κόμβων τους στο EU login[9] ενώ 4 είναι στη διαδικασία
- 10 μόλις χώρες χρησιμοποιούν την πλέον πρόσφατη έκδοση του λογισμικού eIDAS
- 5351 ηλεκτρονικές υπηρεσίες από 11 χώρες έχουν συνδεθεί με eID συστήματα, με τις 2650 από αυτές να έχουν βάση στο Βέλγιο
- 823.668 αιτήματα διασυνοριακής επαλήθευσης ταυτότητας έχουν γίνει μέσω του eID, με τα 1.109.451 να προέρχονται από το Βέλγιο
- 65 έργα επαναχρησιμοποιούν το eID, ενώ 15 εστιάζουν στην ανάλυση ή επαναχρησιμοποίηση του eID [15]

Η Ελλάδα δεν έχει αναπτύξει σύστημα eID που να έχει κοινοποιηθεί. Η Ελλάδα έχει διασυνδεδεμένο eIDAS κόμβο με άλλες δώδεκα χώρες: Βέλγιο, Τσεχία, Εσθονία, Ιταλία, Λουξεμβούργο, Μάλτα, Ολλανδία, Ρουμανία, Σλοβακία, Σλοβενία, Ισπανία και Σουηδία. Ειδικότερα, τα υποστηριζόμενα μέσα ηλεκτρονικής ταυτοποίησης της Ελλάδας μπορούν να χρησιμοποιηθούν για την επαλήθευση ταυτότητας σε υποστηριζόμενες υπηρεσίες της Ρουμανίας μόνο, ενώ τα υποστηριζόμενα μέσα ηλεκτρονικής ταυτοποίησης των άλλων 11 χωρών μπορούν να χρησιμοποιηθούν για την επαλήθευση ταυτότητας σε υποστηριζόμενες υπηρεσίες της Ελλάδας. Ως ενιαίο σημείο επαφής έχει οριστεί το υπουργείο Ψηφιακής Διακυβέρνησης. [28] [29]

Σε ό,τι αφορά την υιοθέτηση των υπηρεσιών εμπιστοσύνης, υπάρχουν 247 εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης σε 29 χώρες με τους 170 από αυτούς να παρέχουν υπηρεσίες εγκεκριμένων πιστοποιητικών για ηλεκτρονικές υπογραφές. [30]

[9] Πρόκειται για ένα μηχανισμό ταυτοποίησης που έχει αναπτύξει η Ευρωπαϊκή Επιτροπή με στόχο να διευκολύνει την πρόσβαση των χρηστών σε ένα σύνολο πληροφοριακών συστημάτων της Επιτροπής. [91]

Η Ελλάδα έχει 5 ενεργούς παρόχους υπηρεσιών εμπιστοσύνης, που προσφέρουν τις παρακάτω υπηρεσίες εμπιστοσύνης όπως φαίνεται από τον Πίνακας 1.2 [31]:

Πίνακας 1.2: Πάροχοι υπηρεσιών εμπιστοσύνης στην Ελλάδα

Πάροχος / Υπηρεσία	ADACOM	BYTE Computer	Ελληνικά Χρηματιστήρια	Ακαδημαϊκό Διαδίκτυο	Αρχή Πιστοποίησης Ελληνικού Δημοσίου
Εγκεκριμένα πιστοποιητικά για ηλεκτρονική υπογραφή	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Εγκεκριμένα πιστοποιητικά για ηλεκτρονική σφραγίδα	ΝΑΙ	ΝΑΙ	ΝΑΙ	-	ΝΑΙ
Εγκεκριμένη χρονοσφραγίδα	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
Πιστοποιητικά για ηλεκτρονική υπογραφή	-	-	-	ΝΑΙ	-
Εγκεκριμένα πιστοποιητικά γνησιότητας ιστοτόπου	-	-	ΝΑΙ	ΝΑΙ	-

1.6 Συμπεράσματα αξιολόγησης του κανονισμού

Ο κανονισμός eIDAS έθεσε τις βάσεις και το κοινό νομικό πλαίσιο για την ηλεκτρονική επαλήθευση ταυτότητας και χρήση υπηρεσιών εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές σε όλη την ΕΕ. Στα πλαίσια του κανονισμού απαιτούνταν η επισκόπησή του ώστε να διαπιστωθεί ο βαθμός στον οποίο πέτυχε το στόχο του, καθώς και αλλαγές που πρέπει να πραγματοποιηθούν είτε στο πεδίο εφαρμογής του είτε σε διατάξεις του, λαμβάνοντας υπόψη τόσο τη μέχρι τώρα εφαρμογή του αλλά και τις εξελίξεις σε τεχνολογικό, κοινωνικό και οικονομικό επίπεδο. Τα αποτελέσματα της αξιολόγησης που πραγματοποιήθηκε το 2020 από μία ομάδα ειδικών χρησιμοποιήθηκαν κατόπιν ως τροφοδότηση για την πρόταση αλλαγής του κανονισμού.

Παρά το γεγονός ότι το eIDAS υλοποίησε σε μεγάλο βαθμό τους στόχους του, εντοπίστηκαν αρκετά σημεία προς βελτίωση, τόσο λόγω των περιορισμών που έχει ο ίδιος ο κανονισμός, αλλά και λόγω των εξελίξεων στις οποίες συνέβαλε και ο COVID-19. Τα κύρια συμπεράσματα που προέκυψαν από την ανάλυση όλων των πτυχών του κανονισμού και της μέχρι τότε εφαρμογής του αναλύονται στις παρακάτω συνιστώσες:

- Αποτελεσματικότητα: Η αποτελεσματικότητα του κανονισμού θεωρήθηκε μερική. Σε ό,τι αφορά την ηλεκτρονική ταυτοποίηση, παρατηρήθηκε περιορισμένος αριθμός κοινοποιημένων συστημάτων eID σε μόλις 14 χώρες καλύπτοντας το 59% των πολιτών[10], καθώς και περιορισμένη αποδοχή τους λόγω είτε της μη λειτουργίας όλων των κόμβων eIDAS, των λίγων δημόσιων υπηρεσιών που συνδέονται με την υποδομή αλλά και λόγω τεχνικών σφαλμάτων. Σχετικά με τις υπηρεσίες εμπιστοσύνης, παρότι ο κανονισμός δημιούργησε ένα ισχυρό πλαίσιο, οδήγησε σε διαφορετικές ερμηνείες και αποκλίσεις από τα κράτη μέλη, λόγω της τεχνολογικής ουδετερότητάς του και της μη δημοσίευσης πρόσθετων κατευθυντήριων γραμμών.
- Αποδοτικότητα: Παρά το γεγονός ότι τόσο τα κόστη αλλά και τα οφέλη από την εφαρμογή του κανονισμού δεν ήταν εύκολο να ποσοτικοποιηθούν, η αξιολόγηση οδήγησε στο συμπέρασμα ότι τα οφέλη ήταν υψηλότερα από τα κόστη.
- Συνάφεια: Ενώ οι στόχοι του κανονισμού αξιολογήθηκαν ότι παραμένουν συναφείς με τις ανάγκες που αρχικά ήθελε να καλύψει (όπως κατακερματισμός αγοράς, ανάγκη για διατομεακή διαλειτουργικότητα), το πεδίο εφαρμογής του κρίθηκε ιδιαίτερα περιορισμένο. Παρατηρήθηκε μικρή ενσωμάτωσή του σε τομεακές νομοθετικές πράξεις, χωρίς να ανταποκρίνεται στις ανάγκες συγκεκριμένων τομέων κυρίως λόγω της έλλειψης πλαισίου που να επιτρέπει την ανταλλαγή ειδικών αναγνωριστικών. Επίσης, οι τεχνολογικές εξελίξεις των τελευταίων ετών, οδήγησαν στο συμπέρασμα ότι ο κανονισμός έπρεπε να επεκτείνει τον κατάλογο υπηρεσιών εμπιστοσύνης για να καλύψει νέες ανάγκες και περιπτώσεις χρήσης.
- Συνοχή: Παρά το γεγονός ότι το πλαίσιο θεωρήθηκε γενικά συνεκτικό, παρουσιάστηκαν κάποια στοιχεία του που διαφωνούσαν. Αρχικά, δεν υπήρχε ενιαία άποψη από τα κράτη μέλη για το σημαντικό και υψηλό επίπεδο διασφάλισης. Επίσης, λόγω της εστίασης σε δημόσιες υπηρεσίες, υπήρχε δυσκολία στον περιορισμό των διαβιβαζόμενων δεδομένων στα ελάχιστα αναγκαία, δυσχεραίνοντας την επιβολή των αρχών του Γενικού Κανονισμού Προστασίας Δεδομένων[11] (ΓΚΠΔ).

[10] Μέχρι τη στιγμή της αξιολόγησης

[11] Κανονισμός 2016/679 της Ευρωπαϊκής Ένωσης για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

Ακόμα, δεν γινόταν σαφής ο ρόλος των οργανισμών αξιολόγησης της συμμόρφωσης, ενώ τέλος κάποιες μέθοδοι ταυτοποίησης εναπόκειντο στα κράτη μέλη αν θα τις αναγνωρίσουν, κάνοντας άνιση την εφαρμογή του κανονισμού.

- Ενωσιακή προστιθέμενη αξία: Σε ό,τι αφορά στην ηλεκτρονική ταυτοποίηση, από την αξιολόγηση εκτιμήθηκε ότι η προστιθέμενη αξία ήταν περιορισμένη, παρά τα κίνητρα για τα κράτη να αναπτύξουν συστήματα eID, λόγω της μικρής υιοθέτησης και χρήσης τους, οδηγώντας στο συμπέρασμα ότι υπάρχει ανάγκη για προσαρμογές και χρήση ταυτοτήτων από τον ιδιωτικό τομέα μαζί με ειδικά αναγνωριστικά. Σχετικά με τις υπηρεσίες εμπιστοσύνης, το πόρισμα έδειξε ότι ναι μεν μειώνεται ο κατακερματισμός της αγοράς και οι αυξάνεται ο εκσυγχρονισμός των δημοσίων διοικήσεων μειώνοντας έτσι το φόρτο εργασίας τους. Ωστόσο για να υπάρξει μεγαλύτερη αξία πρέπει να αρθούν οι φραγμοί από τις αντικρουόμενες ερμηνείες στοιχείων του πλαισίου αλλά και να γίνει διεύρυνση των παρεχόμενων υπηρεσιών. [13] [32] [33] [34]

2. Ο ΚΑΝΟΝΙΣΜΟΣ EIDAS 2.0

2.1 Εισαγωγή: Η μετάβαση στο eIDAS 2.0

Όπως παρουσιάστηκε και στην ενότητα 1.2, το 2021 παρουσιάστηκε η πρόταση για την τροποποίηση του κανονισμού, βάσει της εκτενούς αξιολόγησής του, αλλά και των μέχρι τότε εξελίξεων σε κοινωνικό-οικονομικό αλλά και τεχνολογικό επίπεδο, καθώς και των προσδοκιών των πολιτών.

Εντοπίστηκαν αρκετά σημεία που ο κανονισμός δεν είχε καταφέρει να αντιμετωπίσει, με αποτέλεσμα να μην αξιοποιεί πλήρως τις δυνατότητές του. Αρχικά, τα τελευταία χρόνια είχε αυξηθεί θεαματικά η ανάγκη για ηλεκτρονική ταυτοποίηση και ανταλλαγή χαρακτηριστικών διαφόρων ειδών στα πλαίσια των υπηρεσιών του δημόσιου αλλά και του ιδιωτικού τομέα. Σημαντικό ρόλο σε αυτό διαδραμάτισε η πανδημία του Covid-19, η οποία επέφερε ταχύτατη ψηφιοποίηση πολλών υπηρεσιών, με αρκετές από αυτές να αφορούν κρίσιμους τομείς όπως της υγείας, όπου η προστασία των δεδομένων ήταν ιδιάζουσας σημασίας. Ωστόσο, ο κανονισμός δεν προσέφερε πλαίσιο για τον ιδιωτικό τομέα, ώστε να μπορεί να αξιοποιήσει τα εθνικά eID συστήματα, ούτε λάμβανε υπόψη ένα μεγάλο εύρος περιπτώσεων χρήσης της ηλεκτρονικής ταυτοποίησης. [34] [35]

Παράλληλα, η εύκολη και απρόσκοπτη διαδικασία ηλεκτρονικής ταυτοποίησης από τους πολίτες, ενώ αποτελούσε βασικό στόχο, δεν φαίνεται να επετεύχθη σε μεγάλο βαθμό με τους χρήστες να αντιμετωπίζουν δυσκολίες, ενώ οι διάφορες λύσεις που υιοθετήθηκαν από τα κράτη μέλη τελικά παρουσίαζαν μεγάλες ανομοιογένειες. Επίσης, ο έλεγχος των δεδομένων που ανταλλάσσονταν καθώς και ο βαθμός ασφάλειας και ιδιωτικότητας που παρέχονταν από τις υπηρεσίες δεν καλύπτονταν επαρκώς, με αποτέλεσμα πολλοί χρήστες να ανησυχούν για φαινόμενα παρακολούθησης ή κατάρτισης προφίλ από τα δεδομένα τους. [34] [36]

Παράλληλα, το 2021 παρουσιάστηκε το όραμα της Ευρωπαϊκής Επιτροπής για την ενδυνάμωση πολιτών και επιχειρήσεων μέσω του ψηφιακού μετασχηματισμού ως το 2030 (Ψηφιακή Δεκαετία).

Στους ψηφιακούς στόχους συμπεριλαμβανόταν και η ψηφιοποίηση των δημόσιων υπηρεσιών, με στόχο το 100% των πολιτών να έχουν πρόσβαση σε ασφαλή μέσα ηλεκτρονικής ταυτοποίησης αναγνωρισμένα σε ολόκληρη την Ένωση, τα οποία τους επιτρέπουν να έχουν τον πλήρη έλεγχο των συναλλαγών που περιλαμβάνουν ταυτοποίηση και των δεδομένων προσωπικού χαρακτήρα που κοινοποιούν (Άρθρο 4, Στόχος 4[12]). [37]

Λαμβάνοντας υπόψη τα παραπάνω, ο τροποποιημένος κανονισμός eIDAS 2.0 αποσκοπεί στο να συμβάλλει στην επίτευξη των στόχων της Ψηφιακής Δεκαετίας, ενώ παράλληλα να αντιμετωπίζει αποτελεσματικά όλα τις αδυναμίες της αρχικής εκδοχής του. Συνοπτικά, ο στόχος είναι να γίνεται χρήση μίας ασφαλούς ηλεκτρονικής ταυτότητας την οποία οι πολίτες μπορούν να χρησιμοποιούν για να αποδεικνύουν την ταυτότητά τους οπουδήποτε στην ΕΕ, και μέσα από αυτή την τεχνολογία, να μπορούν να ελέγχουν οι ίδιοι ποια στοιχεία μοιράζονται, να δίνουν την ρητή τους συγκατάθεση, να γνωρίζουν και να επιβεβαιώνουν με ποιον τα μοιράζονται αλλά και για ποιο σκοπό. [34] [38]

[12] Τα άλλα 2 μέρη του στόχου ήταν να είναι κατά 100% προσβάσιμη διαδικτυακή παροχή βασικών δημόσιων υπηρεσιών και το 100 % των πολιτών της Ένωσης έχει πρόσβαση στα ηλεκτρονικά μητρώα υγείας τους

2.2 Ο κανονισμός EIDAS 2.0

Τροποποιήσεις στο στόχο, αντικείμενο & πεδίο εφαρμογής

Ο αναθεωρημένος κανονισμός eIDAS 2.0, μετά και την επίσημη αποδοχή του και υπογραφή του από τον πρόεδρο του Ευρωπαϊκού Κοινοβουλίου και του Προέδρου του Συμβουλίου στις 11 Απριλίου 2024, δημοσιεύτηκε στην επίσημη εφημερίδα της ΕΕ στις 30 Απριλίου του 2024 και είναι σε ισχύ από τις 20 Μαΐου του ίδιου έτους. [14]

Ενώ στόχος του κανονισμού παραμένει η διασφάλιση της εύρυθμης λειτουργίας της εσωτερικής αγοράς και η επίτευξη ενός επαρκούς επιπέδου ασφάλειας στα μέσα ηλεκτρονικής ταυτοποίησης και στις υπηρεσίες εμπιστοσύνης, αυτός συμπληρώνεται με το στόχο *«να καταστεί δυνατή και να διευκολυνθεί η άσκηση του δικαιώματος των φυσικών και νομικών προσώπων να συμμετέχουν στην ψηφιακή κοινωνία με ασφάλεια και να έχουν πρόσβαση σε επιγραμμικές δημόσιες και ιδιωτικές υπηρεσίες σε ολόκληρη την Ένωση».* [39]

Στο αντικείμενο του κανονισμού πλέον εντάσσεται και ο καθορισμός των όρων υπό τους οποίους τα κράτη μέλη πρέπει να παρέχουν και να αναγνωρίζουν ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας (η βασικότερη νέα έννοια που παρουσιάζεται). Επιπλέον, στο αντικείμενο παραμένει η θέσπιση νομικού πλαισίου για τις υπηρεσίες εμπιστοσύνης, ωστόσο εντάσσονται σε αυτές πλέον και η ηλεκτρονική αρχειοθέτηση, η ηλεκτρονική βεβαίωση χαρακτηριστικών, οι διατάξεις δημιουργίας ηλεκτρονικής υπογραφής, οι διατάξεις δημιουργίας ηλεκτρονικής σφραγίδας και τα ηλεκτρονικά καθολικά. Οι έννοιες αυτές και οι σχετικές απαιτήσεις παρουσιάζονται αναλυτικά στην ενότητα: Οι βασικές αλλαγές του κανονισμού – Νέες υπηρεσίες εμπιστοσύνης. Σε ό,τι αφορά στο πεδίο εφαρμογής του κανονισμού, αυτό διευρύνεται ώστε να καλύπτει και τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας που παρέχονται από κράτος μέλος.

Συνολικά, ο αναθεωρημένος κανονισμός περιλαμβάνει νέους όρους, ενώ εισάγει τροποποιήσεις και σε υπάρχουσες έννοιες, οι κυριότερες εκ των οποίων αναφέρονται στα αντίστοιχα σημεία. Ακόμα, εκτός από τα ψηφιακά πορτοφόλια και τις νέες υπηρεσίες εμπιστοσύνης, έμφαση δίνεται στους όρους για την διασυνοριακή αντιστοίχιση ταυτότητας και στον τρόπο πιστοποίησης των συστημάτων ηλεκτρονικής ταυτοποίησης και γίνεται μεγαλύτερη ανάλυση στις απαιτήσεις για τους εγκεκριμένους και μη παρόχους υπηρεσιών εμπιστοσύνης και για τις εγκεκριμένες υπηρεσίες. Τέλος ορίζεται σαφέστερα πλαίσιο διακυβέρνησης για τους εποπτικούς φορείς και την συνεργασία μεταξύ κρατών μελών. [39]

Οι βασικές αλλαγές του κανονισμού – Ψηφιακό πορτοφόλι

Η βασικότερη αλλαγή που παρουσιάζει το eIDAS 2.0 είναι η εισαγωγή της έννοιας του ευρωπαϊκού ψηφιακού πορτοφολιού ηλεκτρονικής ταυτότητας (EU Digital Identity Wallet – EUDI Wallet). Οι σχετικοί ορισμοί που παρουσιάζονται είναι:

- Ως ευρωπαϊκό πορτοφόλι ευρωπαϊκής ταυτότητας (European Digital Identity Wallet – EUDI Wallet) από τον κανονισμό ορίζεται 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.
- Βασιζόμενο μέρος (relying party): φυσικό ή νομικό πρόσωπο που βασίζεται σε ηλεκτρονική ταυτοποίηση, ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας ή άλλα μέσα ηλεκτρονικής ταυτοποίησης, ή σε υπηρεσία εμπιστοσύνης·
- Χαρακτηριστικό (attribute): το ιδιοχαρακτηριστικό, η ιδιότητα, το δικαίωμα ή η άδεια φυσικού ή νομικού προσώπου ή αντικειμένου
- Ηλεκτρονική βεβαίωση χαρακτηριστικών (electronic attestation of attributes): Βεβαίωση σε ηλεκτρονική μορφή που επιτρέπει την επαλήθευση της γνησιότητας των χαρακτηριστικών.
- Εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών: Βεβαίωση σε ηλεκτρονική μορφή που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις απαιτήσεις του παραρτήματος 5 του κανονισμού

Βάσει του άρθρου 5α, τουλάχιστον ένα ψηφιακό πορτοφόλι θα πρέπει να παρέχεται από κάθε κράτος μέλος, ώστε φυσικά αλλά και νομικά πρόσωπα να έχουν ασφαλή, αξιόπιστη και απρόσκοπτη διασυνοριακή πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες, διατηρώντας παράλληλα τον πλήρη έλεγχο των δεδομένων τους.

Επίσης, τα ψηφιακά πορτοφόλια πρέπει να παρέχονται είτε απευθείας από το κράτος-μέλος, είτε με εντολή του, είτε ανεξάρτητα από αυτό αλλά πρέπει να αναγνωρίζονται από αυτό το κράτος-μέλος. Επίσης, τα βασικά στοιχεία του κώδικα του λογισμικού πρέπει να διαθέτουν άδεια ανοιχτής πηγής[13], εκτός από συγκεκριμένα στοιχεία. [39]

[13] Ο πηγαίος κώδικας των στοιχείων αυτών είναι δημόσια διαθέσιμος ώστε να είναι δυνατή η μελέτη, τροποποίηση και βελτίωσή του

Τα ψηφιακά πορτοφόλια πρέπει να προσφέρουν ένα σύνολο από δυνατότητες με τρόπο που να είναι διαφανής, ανιχνεύσιμος και φιλικός προς το χρήστη. Σε αυτές περιλαμβάνονται συνοπτικά: [39]

- η δυνατότητα ασφαλούς διαχείρισης των δεδομένων ταυτοποίησής του (ζήτηση, απόκτηση, επιλογή, συνδυασμός, αποθήκευση, διαμοιρασμός, διαγραφή, προσκόμιση) και σε συνδυασμό κατά περίπτωση με ηλεκτρονικές βεβαιώσεις χαρακτηριστικών η χρήση τους για την επαλήθευση ταυτότητας έναντι βασιζόμενων μερών με σκοπό την πρόσβαση σε ιδιωτικές και δημόσιες υπηρεσίες με παράλληλη διασφάλιση της δυνατότητας επιλεκτικής γνωστοποίησης δεδομένων
- η δημιουργία και κρυπτογραφημένη αποθήκευση ψευδωνύμων τοπικά στο πορτοφόλι
- η επιβεβαίωση γνησιότητας άλλων ψηφιακών πορτοφολιών και ο ασφαλής διαμοιρασμός δεδομένων ταυτοποίησης και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών με αυτά
- η πρόσβαση σε σύστημα καταγραφών των συναλλαγών που εκτελούνται με το πορτοφόλι και επιτρέπει: (α) την πρόσβαση σε κατάλογο με τα βασιζόμενα μέρη που έχει γίνει σύνδεση και στα δεδομένα που έχουν ανταλλαχθεί, (β) την εύκολη αίτηση σε βασιζόμενο μέρος για διαγραφή δεδομένων προσωπικού χαρακτήρα και (γ) την εύκολη καταγγελία βασιζόμενου μέρους στην αρμόδια εθνική αρχή προστασίας δεδομένων όταν λαμβάνεται αίτημα παροχής δεδομένων που φαίνεται ύποπτο
- η χρήση εγκεκριμένων υπογραφών και σφραγίδων μέσω αυτού
- η τηλεφόρτωση δεδομένων ταυτοποίησης, ηλεκτρονικών βεβαιώσεων χαρακτηριστικών και ρυθμίσεων
- η άσκηση δικαιωμάτων φορητότητας[14]

Η πλήρης ανάλυση των δυνατοτήτων και προδιαγραφών για το ψηφιακό πορτοφόλι παρέχονται στο Κεφάλαιο 3.

Οι βασικές αλλαγές του κανονισμού – Ηλεκτρονική ταυτοποίηση

Στο κεφάλαιο 2 του κανονισμού, παρεμβάλλεται πλέον το άρθρο 11α για την διασυνοριακή αντιστοίχιση ταυτότητας. Με τον όρο αυτό εννοείται η διαδικασία κατά την οποία δεδομένα ταυτοποίησης προσώπου ή μέσα ηλεκτρονικής ταυτοποίησης αντιστοιχίζονται ή συνδέονται με υφιστάμενο λογαριασμό που ανήκει στο ίδιο πρόσωπο. Στο άρθρο αυτό ορίζεται ότι τα κράτη μέλη, όταν ενεργούν ως βασιζόμενα μέρη για διασυνοριακές υπηρεσίες, πρέπει να εξασφαλίζουν αδιαμφισβήτητη αντιστοίχιση ταυτότητας για τα φυσικά πρόσωπα που χρησιμοποιούν κοινοποιημένα μέσα ηλεκτρονικής ταυτοποίησης ή ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας και παράλληλα πρέπει να 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. [39]

Ακόμα, προστίθεται άρθρο ($12^{α}$) για την πιστοποίηση των συστημάτων ηλεκτρονικής ταυτοποίησης στο οποίο αναφέρεται ότι τα κράτη μέλη πρέπει να ορίζουν οργανισμούς αξιολόγησης συμμόρφωσης για να πιστοποιούν την συμμόρφωση των κοινοποιητέων συστημάτων ηλεκτρονικής ταυτοποίησης προς τις απαιτήσεις κυβερνοασφάλειας του

[14] Σύμφωνα με το άρθρο 20 του ΓΚΠΔ, το δικαίωμα στη φορητότητα προσφέρει στα φυσικά πρόσωπα (υποκείμενα των δεδομένων) έναν εύκολο τρόπο να διαχειρίζονται τα ίδια τα προσωπικά τους δεδομένα. Τα διευκολύνει να διακινούν, να αντιγράφουν ή να μεταφέρουν, εύκολα, δεδομένα προσωπικού χαρακτήρα από ένα περιβάλλον τεχνολογιών πληροφορικής σε άλλο. [92]

κανονισμού καθώς και ότι η πιστοποίηση πρέπει να διενεργείται στο πλαίσιο συστήματος πιστοποίησης κυβερνοασφάλειας βάσει του Κανονισμού 2019/881 ή τμημάτων του. Η μέγιστη διάρκεια αυτής είναι 5 έτη, εφόσον πραγματοποιείται αξιολόγηση τρωτότητας κάθε 2 έτη, και τυχόν ευπάθειες που εντοπίζονται διορθώνονται εντός 3 μηνών, διαφορετικά η πιστοποίηση ακυρώνεται. Επίσης, τα κράτη μέλη πρέπει να ενημερώνουν την Επιτροπή για τα ονόματα και τις διευθύνσεις των οργανισμών αξιολόγησης και εκείνη να τα κοινοποιεί σε όλα τα κράτη μέλη. [39]

Τέλος, προστίθεται το άρθρο 12β, όπου ορίζει ότι οι πάροχοι ψηφιακών πορτοφολιών και οι εκδότες κοινοποιημένων μέσων ηλεκτρονικής ταυτοποίησης που ενεργούν υπό εμπορική ή επαγγελματική ιδιότητα και χρησιμοποιούν βασικές υπηρεσίες πλατφόρμας όπως ορίζονται τον κανονισμό 2022/1925[15] με σκοπό/κατά την παροχή υπηρεσιών ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας και μέσων ηλεκτρονικής ταυτοποίησης σε τελικούς χρήστες, τότε οι επιχειρήσεις - πυλωροί[16] πρέπει να παρέχουν ιδίως αποτελεσματική διαλειτουργικότητα με τα ίδια χαρακτηριστικά λειτουργικού συστήματος, υλικού ή λογισμικού, και, για τους σκοπούς της διαλειτουργικότητας, πρόσβαση στα ίδια χαρακτηριστικά δωρεάν και ανεξαρτήτως του αν τα χαρακτηριστικά υλικού ή λογισμικού αποτελούν μέρος του λειτουργικού συστήματος όπως διατίθενται στον εν λόγω πυλωρό, ή χρησιμοποιούνται από αυτόν, κατά την παροχή των εν λόγω υπηρεσιών. [39] [40]

Οι βασικές αλλαγές του κανονισμού – Πάροχοι και υπηρεσίες εμπιστοσύνης

Νέοι ή τροποποιημένοι ορισμοί

- Ηλεκτρονικό καθολικό (electronic ledger): ακολουθία ηλεκτρονικών εγγραφών δεδομένων, η οποία διασφαλίζει την ακεραιότητα των εν λόγω εγγραφών και την ακρίβεια της χρονολογικής σειράς των εν λόγω εγγραφών.
- Ηλεκτρονική αρχειοθέτηση (electronic archiving): υπηρεσία που εξασφαλίζει την παραλαβή, αποθήκευση, ανάκτηση και διαγραφή ηλεκτρονικών δεδομένων και ηλεκτρονικών εγγράφων, προκειμένου να διασφαλίζεται η ανθεκτικότητα και η αναγνωσιμότητά τους, καθώς και να διαφυλάσσεται η ακεραιότητα, η εμπιστευτικότητα και η απόδειξη της προέλευσής τους καθ' όλη τη διάρκεια της περιόδου διαφύλαξης.
- Υπηρεσία εμπιστοσύνης: πλέον ορίζεται ως η ηλεκτρονική υπηρεσία, συνήθως παρεχόμενη έναντι αμοιβής, η οποία συνίσταται σε οιοδήποτε από τα ακόλουθα:
    - στην έκδοση πιστοποιητικών ηλεκτρονικών υπογραφών, πιστοποιητικών ηλεκτρονικών σφραγίδων, πιστοποιητικών γνησιότητας ιστοτόπου ή πιστοποιητικών για την παροχή άλλων υπηρεσιών εμπιστοσύνης
    - στην επικύρωση πιστοποιητικών ηλεκτρονικών υπογραφών, πιστοποιητικών ηλεκτρονικών σφραγίδων, πιστοποιητικών γνησιότητας ιστοτόπου ή πιστοποιητικών για την παροχή άλλων υπηρεσιών εμπιστοσύνης
    - στη δημιουργία ηλεκτρονικών υπογραφών ή ηλεκτρονικών σφραγίδων
    - στην επικύρωση ηλεκτρονικών υπογραφών ή ηλεκτρονικών σφραγίδων

[15]Βάσει του κανονισμού 2022/1925 βασικές υπηρεσίες πλατφόρμας είναι: α) επιγραμμικές υπηρεσίες διαμεσολάβησης· β) επιγραμμικές μηχανές αναζήτησης· γ) επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης· δ) υπηρεσίες πλατφόρμας διαμοιρασμού βίντεο· ε) υπηρεσίες διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών· στ) λειτουργικά συστήματα· ζ) φυλλομετρητές· η) εικονικοί βοηθοί· θ) υπηρεσίες νεφοϋπολογιστικής

[16] Βάσει του κανονισμού 2022/1925 μια επιχείρηση ορίζεται ως πυλωρός εάν: α) έχει σημαντικό αντίκτυπο στην εσωτερική αγορά· β) παρέχει βασική υπηρεσία πλατφόρμας η οποία αποτελεί σημαντική πύλη για να συνδέονται οι επαγγελματίες χρήστες με τελικούς χρήστες· και γ) κατέχει παγιωμένη και σταθερή θέση, στο πλαίσιο των δραστηριοτήτων της, ή αναμένεται ότι θα κατέχει τέτοια θέση στο εγγύς μέλλον.

- στη διαφύλαξη ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων, πιστοποιητικών ηλεκτρονικών υπογραφών ή πιστοποιητικών ηλεκτρονικών σφραγίδων
- στη διαχείριση διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής ή διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής σφραγίδας
- στην έκδοση ηλεκτρονικών βεβαιώσεων χαρακτηριστικών
- στην επικύρωση ηλεκτρονικής βεβαίωσης χαρακτηριστικών
- στη δημιουργία ηλεκτρονικών χρονοσφραγίδων
- στην επικύρωση ηλεκτρονικών χρονοσφραγίδων
- στην παροχή ηλεκτρονικών υπηρεσιών συστημένης παράδοσης
- στην επικύρωση των δεδομένων που διαβιβάζονται μέσω ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και των σχετικών αποδεικτικών στοιχείων
- στην ηλεκτρονική αρχειοθέτηση ηλεκτρονικών δεδομένων και ηλεκτρονικών εγγράφων
- στην καταχώριση ηλεκτρονικών δεδομένων σε ηλεκτρονικό καθολικό

Γενικές αλλαγές

Στο άρθρο 14 του κανονισμού “Διεθνείς πτυχές” προστίθεται ότι η νομική ισοδυναμία των εγκεκριμένων υπηρεσιών εμπιστοσύνης από εγκεκριμένους παρόχους εγκατεστημένους στην ΕΕ με τρίτες χώρες οι οργανισμούς μπορεί να αναγνωριστεί πλέον και μέσω εκτελεστικών πράξεων καθώς και ότι οι εν λόγω τρίτες χώρες και οι διεθνείς οργανισμοί πρέπει να καταρτίζουν, τηρούν και δημοσιεύουν κατάλογο εμπιστοσύνης των αναγνωρισμένων παρόχων υπηρεσιών εμπιστοσύνης. [39]

Σχετικά με τη θέσπιση κανόνων από τα κράτη μέλη για κυρώσεις που θα επιβάλλονται όταν υπάρχει παραβίαση του κανονισμού, προστίθεται στο άρθρο 16 του κανονισμού η απαίτηση διασφάλισης ότι οι παραβάσεις εγκεκριμένων ή μη παρόχων υπηρεσιών εμπιστοσύνης υπόκεινται σε διοικητικά πρόστιμα ανώτατου ύψους τουλάχιστον: (α) 5 εκατομμυρίων ευρώ όταν ο πάροχος υπηρεσιών εμπιστοσύνης είναι φυσικό πρόσωπο ή (β) όταν ο πάροχος υπηρεσιών εμπιστοσύνης είναι νομικό πρόσωπο, 5 εκατομμυρίων ευρώ ή 1% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκε ο πάροχος υπηρεσιών εμπιστοσύνης κατά το οικονομικό έτος που προηγείται του έτους κατά το οποίο σημειώθηκε η παράβαση, ανάλογα με το ποιο ποσό είναι υψηλότερο. [39]

Τα άρθρα 17 και 18 για τους εποπτικούς φορείς και την αμοιβαία συνδρομή απαλείφονται, ενώ προστίθεται νέο άρθρο 19α σχετικά με γενικές απαιτήσεις για μη εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης. Συγκεκριμένα ορίζεται ότι πρέπει να έχουν πολιτικές και κατάλληλα μέτρα για τη διαχείριση νομικών, επιχειρηματικών, λειτουργικών και άλλων άμεσων ή έμμεσων κινδύνων σχετικών με την παροχή της μη εγκεκριμένης υπηρεσίας εμπιστοσύνης. Τα μέτρα αυτά πρέπει να αφορούν κατ’ ελάχιστο (α) διαδικασίες εγγραφής και ένταξης για υπηρεσία εμπιστοσύνης, (β) διαδικαστικούς ή διοικητικούς ελέγχους που απαιτούνται για την παροχή υπηρεσιών εμπιστοσύνης και (γ) τη διαχείριση και την παροχή υπηρεσιών εμπιστοσύνης. Επίσης οι πάροχοι είναι υποχρεωμένοι να ενημερώνουν άμεσα (και το πολύ εντός 24 ωρών) τα ενδιαφερόμενα μέρη όταν υπάρχουν παραβιάσεις ασφάλειας, διαταραχές στην παροχή της υπηρεσίας ή στην εφαρμογή των ανωτέρω μέτρων που έχουν σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα δεδομένα προσωπικού χαρακτήρα. [39]

Αλλαγές γίνονται και στο άρθρο 20 σχετικά με την εποπτεία των εγκεκριμένων παρόχων, όπου οι έλεγχοι που γίνονται σε αυτούς θα πρέπει πλέον να επιβεβαιώνουν όχι μόνο τη συμμόρφωση με τον νέο κανονισμό αλλά και με το άρθρο 21 της οδηγίας 2022/2555 NIS 2. Επίσης αναφέρεται ότι οι εγκεκριμένοι πάροχοι πρέπει να ενημερώνουν τον εποπτικό φορέα το αργότερο ένα μήνα πριν τον σχεδιασμένο έλεγχο, ενώ πρέπει να επιτρέπουν και τη συμμετοχή αυτού ως παρατηρητή κατόπιν αιτήματος. Ακόμη, θα πρέπει να κοινοποιούνται από τα κράτη μέλη στην Επιτροπή στοιχεία των φορέων αξιολόγησης συμμόρφωσης, και η Επιτροπή θα διαθέτει τις πληροφορίες αυτές σε όλα τα κράτη μέλη. [39]

Επιπροσθέτως, όταν είτε οι αρμόδιες αρχές που έχουν συσταθεί βάσει του άρθρου 8, παρ. 1 της οδηγίας NIS 2 είτε οι εποπτικές αρχές που έχουν συσταθεί βάσει του άρθρου 51 του ΓΚΠΔ ενημερώνουν τον εποπτικό φορέα ότι ο πάροχος δεν πληροί τις απαιτήσεις της σχετικής οδηγίας ή κανονισμού αντίστοιχα, τότε ο φορέας μπορεί να αποσύρει την έγκριση του παρόχου, αν δικαιολογείται λόγω έκτασης, διάρκειας και συνεπειών της παράλειψης που εντοπίστηκε. Ακόμα, ο φορέας πρέπει να ενημερώνει τον πάροχο σχετικά με αυτή την απόφαση και τον φορέα που είναι υπεύθυνος για τον εθνικό κατάλογο εμπιστοσύνης ώστε να τον ενημερώσει. [39]

Στο άρθρο 21 που αφορά στην έναρξη εγκεκριμένης υπηρεσίας εμπιστοσύνης, προστίθεται ότι η έκθεση αξιολόγησης συμμόρφωσης που υποβάλλεται θα πρέπει να επιβεβαιώνει όχι μόνο τις απαιτήσεις του eIDAS 2.0 αλλά και του άρθρου 21 της οδηγίας NIS 2. Για την επαλήθευση της συμμόρφωσης με τις απαιτήσεις του NIS 2, ο εποπτικός φορέας ζητά από τις αρμόδιες αρχές που έχουν συσταθεί βάσει της οδηγίας να πραγματοποιήσουν τις σχετικές εποπτικές ενέργειες και να τον ενημερώσουν το αργότερο εντός δύο μηνών. [39]

Στο άρθρο 24 για τις απαιτήσεις των εγκεκριμένων παρόχων εμπιστοσύνης, παρουσιάζονται αλλαγές στις μεθόδους που μπορεί να χρησιμοποιούνται για την εξακρίβωση της ταυτότητας ή των ειδικών χαρακτηριστικών του φυσικού ή νομικού προσώπου για το οποίο εκδίδεται εγκεκριμένο πιστοποιητικό ή εγκεκριμένη βεβαίωση χαρακτηριστικών. Συγκεκριμένα στις μεθόδους προστίθεται η χρήση του ψηφιακού πορτοφολιού ή κοινοποιημένου μέσου ηλεκτρονικής ταυτοποίησης που πληροί τις απαιτήσεις υψηλού επιπέδου διασφάλισης, αναφέρεται ότι άλλες μέθοδοι ταυτοποίησης/εξακρίβωσης χαρακτηριστικών που χρησιμοποιούνται πρέπει να εξασφαλίζουν ότι η διαδικασία γίνεται με υψηλό επίπεδο εμπιστοσύνης και τέλος ότι αν η διαδικασία γίνεται με φυσική παρουσία πρέπει να υπάρχουν κατάλληλα αποδεικτικά στοιχεία και διαδικασίες σύμφωνα με το εθνικό δίκαιο. Ειδικά για την εξακρίβωση ειδικών χαρακτηριστικών δύναται να χρησιμοποιηθεί και εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών. [39]

Ακόμα, τροποποιήσεις γίνονται και στις λοιπές απαιτήσεις που περιγράφονται στο άρθρο 24 όπου οι κυριότερες είναι ότι: (α) ορίζεται χρονοδιάγραμμα ενημέρωσης των εποπτικών φορέων τουλάχιστον ένα μήνα πριν την οποιαδήποτε αλλαγή στην παροχή εγκεκριμένων υπηρεσιών και τριών μηνών όταν υπάρχει πρόθεση παύσης παροχής αυτών, (β) προστίθεται στην ενημέρωση των προσώπων σχετικά με όρους και προϋποθέσεις χρήσης της υπηρεσίας πριν την σύναψη σύμβασης, ο όρος αυτή να γίνεται με εύκολα προσβάσιμο τρόπο, σε δημόσια προσβάσιμο χώρο αλλά και μεμονωμένα, ενώ στην παράγραφο $2^{ε}$ για την χρήση αξιόπιστων συστημάτων και προϊόντων γίνεται αναφορά στη χρήση κρυπτογραφικών εργαλείων. Επίσης, προστίθενται οι παράγραφοι $2^{στα}$ και $2^{στβ}$ όπου ορίζονται τα ίδια όπως στην παράγραφο $19^{α}$ που περιγράφηκε ανωτέρω. [39]

Τέλος, προστίθεται νέο άρθρο $24^{α}$ σχετικά με την αναγνώριση των εγκεκριμένων υπηρεσιών εμπιστοσύνης και ορίζει ότι [39]:

- Ηλεκτρονική υπογραφή ή σφραγίδα που βασίζεται σε εγκεκριμένο πιστοποιητικό, εγκεκριμένο πιστοποιητικό για την επαλήθευση γνησιότητας ιστοτόπου και εγκεκριμένη

ηλεκτρονική βεβαίωση χαρακτηριστικών που εκδίδεται σε ένα κράτος μέλος αναγνωρίζεται ως τέτοιο/α σε όλα τα άλλα κράτη μέλη

- Εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας που έχει πιστοποιηθεί σε ένα κράτος μέλος αναγνωρίζεται ως τέτοιο/α σε όλα τα άλλα κράτη μέλη
- Εγκεκριμένο πιστοποιητικό ηλεκτρονικών υπογραφών ή σφραγίδων, εγκεκριμένη υπηρεσία εμπιστοσύνης για τη διαχείριση εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας[17], εγκεκριμένη υπηρεσία επικύρωσης ή διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών ή σφραγίδων, εγκεκριμένη ηλεκτρονική χρονοσφραγίδα, εγκεκριμένη ηλεκτρονική υπηρεσία συστημένης παράδοσης, εγκεκριμένη υπηρεσία ηλεκτρονικής αρχειοθέτησης ή εγκεκριμένο ηλεκτρονικό καθολικό που παρέχεται σε ένα κράτος μέλος αναγνωρίζεται ως τέτοιο/α σε όλα τα άλλα κράτη μέλη.

Ηλεκτρονική υπογραφή

Στις ηλεκτρονικές υπογραφές, προστίθεται νέα παράγραφος που ορίζει ότι η δημιουργία, διαχείριση ή η αναπαραγωγή για δημιουργία αντιγράφων των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής πραγματοποιείται μόνο για λογαριασμό του υπογράφοντος, κατόπιν αιτήματος του υπογράφοντος, και από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης που παρέχει εγκεκριμένη υπηρεσία εμπιστοσύνης για τη διαχείριση εγκεκριμένης διάταξης εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής. [39]
Ακόμα, προστίθεται άρθρο 29^{α} με απαιτήσεις για την εγκεκριμένη υπηρεσία διαχείρισης εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής. Σε αυτές περιλαμβάνονται συνοπτικά: Η διαχείριση των εν λόγω διατάξεων ως εγκεκριμένη υπηρεσία προσφέρεται από εγκεκριμένο πάροχο που (α) δημιουργεί ή διαχειρίζεται δεδομένα δημιουργίας ηλεκτρονικής υπογραφής εξ ονόματος του υπογράφοντος, (β) αναπαράγει τα δεδομένα αυτά μόνο για τη δημιουργία εφεδρικών αντιγράφων με τις προϋποθέσεις ότι η ασφάλεια των εφεδρικών δεδομένων είναι στο ίδιο επίπεδο με αυτή των πρωτότυπων και ότι ο αριθμός των συνόλων των εφεδρικών δεδομένων δεν ξεπερνά τον ελάχιστο που απαιτείται για την εξασφάλιση της συνέχισης της υπηρεσίας και (γ) εφόσον προκύπτουν απαιτήσεις από έκθεση πιστοποίησης της διάταξης αυτής, συμμορφώνονται με αυτές. [39]
Επιπλέον, στο άρθρο 30 για την πιστοποίηση των διατάξεων δημιουργίας ηλεκτρονικής υπογραφής ορίζεται πλέον σαφώς ότι η ισχύς της πιστοποίησης είναι το πολύ πέντε έτη, με την προϋπόθεση πραγματοποίησης αξιολόγησης τρωτών σημείων ανά δύο έτη και διόρθωσης τυχόν ευρημάτων, διαφορετικά, η πιστοποίηση ακυρώνεται. Ακόμα, προστίθεται νέο άρθρο 32^{α} που περιλαμβάνει απαιτήσεις για την επικύρωση προηγμένων ηλεκτρονικών υπογραφών βάσει εγκεκριμένων πιστοποιητικών. Σε αυτό προσδιορίζεται ότι η διαδικασία της επικύρωσης επιβεβαιώνει την εγκυρότητα της εν λόγω υπογραφής εφόσον: (α) το πιστοποιητικό που χρησιμοποιήθηκε ήταν εγκεκριμένο κατά τη στιγμή της υπογραφής, (β) εκδόθηκε από εγκεκριμένο πάροχο και ήταν έγκυρο τη στιγμή της υπογραφής, (γ) τα στοιχεία επικύρωσης της υπογραφής αντιστοιχούν στα δεδομένα που παρέχονται στο βασιζόμενο μέρος, (δ) το μοναδικό σύνολο δεδομένων που αντιπροσωπεύουν τον υπογράφοντα στο πιστοποιητικό παρέχεται ορθώς στο βασιζόμενο μέρος, (ε) αν γίνεται χρήση ψευδωνύμου κατά την υπογραφή, αυτή δηλώνεται εμφανώς στο βασιζόμενο μέρος, (στ) ισχύει η ακεραιότητα των υπογεγραμμένων δεδομένων και (ζ) κατά την υπογραφή πληρούνταν οι απαιτήσεις για τις προηγμένες ηλεκτρονικές υπογραφές του άρθρου 26. Ακόμα, το σύστημα που χρησιμοποιείται για την επικύρωση πρέπει να δίνει το σωστό αποτέλεσμα της διαδικασίας και να επιτρέπει τον εντοπισμό τυχόν λαθών. [39]

[17] εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας, την οποία διαχειρίζεται εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης σύμφωνα με το άρθρο 29^{α} ή 39^{α} αντίστοιχα για λογαριασμό υπογράφοντος·

Ηλεκτρονική σφραγίδα

Προστίθεται στον κανονισμό το άρθρο 39α που εφαρμόζεται κατ' αναλογία με το άρθρο 29α σχετικά με τις απαιτήσεις για εγκεκριμένη υπηρεσία διαχείρισης εγκεκριμένων διατάξεων εξ αποστάσεως δημιουργίας ηλεκτρονικής σφραγίδας» και το άρθρο 40α σχετικά με τις απαιτήσεις για την επικύρωση προηγμένων ηλεκτρονικών σφραγίδων με βάση εγκεκριμένα πιστοποιητικά που εφαρμόζεται, αντίστοιχα κατ' αναλογία με το άρθρο 32α. [39]

Ηλεκτρονική χρονοσφραγίδα

Σχετικά με τις απαιτήσεις για την εγκεκριμένη ηλεκτρονική χρονοσφραγίδα, στον αναθεωρημένο κανονισμό ορίζεται ότι η συμμόρφωση με αυτές συμπεραίνεται μόνο αν η σύνδεση ημερομηνίας και ώρας με τα δεδομένα και η ακρίβεια της χρονικής πηγής πληρούν τα πρότυπα, τις προδιαγραφές και τις διαδικασίες που αναμένεται να οριστούν μέσω εκτελεστικών πράξεων που θα εκδώσει η Επιτροπή ως τις 21 Μαΐου 2025. [39]

Ηλεκτρονική υπηρεσία συστημένης παράδοσης

Σχετικά με τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης, στον αναθεωρημένο κανονισμό ορίζεται ότι η συμμόρφωση με αυτές συμπεραίνεται μόνο αν η διαδικασία αποστολής και λήψης δεδομένων πληροί τα πρότυπα, τις προδιαγραφές και τις διαδικασίες που αναμένεται να οριστούν μέσω εκτελεστικών πράξεων που θα εκδώσει η Επιτροπή ως τις 21 Μαΐου 2025. Ακόμα, προστίθεται ότι οι πάροχοι έχουν τη δυνατότητα να συμφωνούν σχετικά τη διαλειτουργικότητα των εν λόγω εγκεκριμένων υπηρεσιών, εφόσον το πλαίσιο αυτό συμμορφώνεται με τις απαιτήσεις που αναφέρθηκαν ανωτέρω, ενώ η Επιτροπή μπορεί μελλοντικά μέσω εκτελεστικών πράξεων να καθορίσει κατάλογο προτύπων αναφοράς, προδιαγραφές και διαδικασίες για το πλαίσιο της διαλειτουργικότητας. [39]

Υπηρεσία πιστοποιητικών για την επαλήθευση της γνησιότητας ιστοτόπων

Στον νέο κανονισμό αλλάζουν ορισμένες από τις προδιαγραφές για τα εγκεκριμένα πιστοποιητικά επαλήθευσης γνησιότητας ιστοτόπων, με την σημαντικότερη να είναι ότι για τα νομικά πρόσωπα πρέπει να παρέχουν ένα μοναδικό σύνολο δεδομένων που να το αντιπροσωπεύει χωρίς αμφιβολία και να περιλαμβάνει τουλάχιστον την επωνυμία του. Η σχετική αξιολόγηση συμμόρφωσης με τις απαιτήσεις θα πρέπει να διενεργείται σύμφωνα με πρότυπα αναφοράς, προδιαγραφές και διαδικασίες που αναμένεται να οριστούν μέσω εκτελεστικών πράξεων που θα εκδώσει η Επιτροπή ως τις 21 Μαΐου 2025. [39]

Επιπλέον, προστίθεται παράγραφος που ορίζει ότι οι (περισσότεροι) πάροχοι φυλλομετρητών ιστού (browsers) θα πρέπει να αναγνωρίζουν τα εγκεκριμένα πιστοποιητικά, να τα εμφανίζουν με τρόπο φιλικό προς το χρήστη αλλά και να διασφαλίζουν την υποστήριξη και διαλειτουργικότητα με αυτά. Για την νέα αυτή προδιαγραφή εντάσσεται νέο άρθρο 45α σχετικά με προληπτικά μέτρα κυβερνοασφάλειας που μπορούν να λάβουν οι πάροχοι φυλλομετρητών ιστού. Συγκεκριμένα αναφέρεται ότι οι πάροχοι αυτοί δεν παίρνουν μέτρα που να είναι αντίθετα με τις υποχρεώσεις που ορίστηκαν στο άρθρο 45, εκτός αν υπάρχουν βάσιμες ανησυχίες για παραβίαση ασφάλειας ή απώλεια ακεραιότητας ενός ή περισσότερων πιστοποιητικών, οπότε και μπορούν κατ' εξαίρεση να λάβουν προληπτικά μέτρα. Σε αυτή την περίπτωση, οφείλουν να ενημερώνουν γραπτώς την Επιτροπή, τον αρμόδιο εποπτικό φορέα, την οντότητα για την οποία έχει εκδοθεί το πιστοποιητικό και τον εγκεκριμένο πάροχο που το εξέδωσε, τόσο για τις ανησυχίες αλλά και τα μέτρα που εφάρμοσαν. Κατόπιν, ο εποπτικός φορέας, οφείλει να διερευνήσει τους ισχυρισμός και εφόσον δεν συντρέχει λόγος ακύρωσης του πιστοποιητικού, θα ενημερώνει τον πάροχο φυλλομετρητή ιστού για την απόφασή του ώστε να αποσύρει τα ληφθέντα μέτρα. [39]

Αξίζει να αναφερθεί ότι όταν εκδόθηκε η πρόταση για την τροποποίηση του κανονισμού, υπήρξαν αντιδράσεις από ειδικούς στον τομέα της κυβερνοασφάλειας σχετικά με τις επιπτώσεις που οι νέες απαιτήσεις για τα πιστοποιητικά επαλήθευσης γνησιότητας ιστοτόπου θα είχαν για την ασφάλεια στο διαδίκτυο. Ειδικότερα, η απαίτηση αναγνώρισης των εγκεκριμένων πιστοποιητικών από τους παρόχους φυλλομετρητών ιστού ανεξάρτητα από τα χαρακτηριστικά ασφαλείας των εν λόγω πιστοποιητικών και των πολιτικών που διέπουν την έκδοσή τους, οι ειδικοί θεωρούσαν πως θα έκανε δυσκολότερη την προστασία από κυβερνοεγκληματίες, λόγω της ασθενέστερης επαλήθευσης ταυτότητας. Παράλληλα θα ενίσχυε λανθασμένα την αντίληψη ότι τα εν λόγω πιστοποιητικά δεν εγκυμονούν κινδύνους ασφαλείας λόγω του πλαισίου στο οποίο εκδίδονται και των κυβερνητικών πλαισίων στα οποία υπόκεινται, με αποτέλεσμα οι υπεύθυνοι φορείς να αμελούν τις αρμοδιότητές τους για τη διαχείριση των σχετικών ρίσκων. [41]

Παρά τις αλλαγές που έγιναν στο κείμενο, οι προβληματισμοί για την τεχνολογική ουδετερότητα, την ιδιωτικότητα των χρηστών και την παρεχόμενη ασφάλεια παρέμειναν και μετά την έκδοση του συμφωνημένου προσχεδίου τον Νοέμβριο του 2023. [42] [43]

Οι βασικές αλλαγές του κανονισμού – Νέες υπηρεσίες εμπιστοσύνης

Ηλεκτρονική βεβαίωση χαρακτηριστικών

Σε ό,τι αφορά στην νομική ισχύ, βάσει του άρθρου 45β του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής βεβαίωσης ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές βεβαιώσεις. Ακόμα, οι εγκεκριμένες ηλεκτρονικές βεβαιώσεις ή ηλεκτρονικές βεβαιώσεις που εκδίδονται από/για λογαριασμό δημοσίου φορέα υπεύθυνου για αυθεντική πηγή[18] έχουν την ίδια νομική ισχύ με τις βεβαιώσεις που έχουν εκδοθεί νόμιμα σε έντυπη μορφή, ενώ ηλεκτρονικές βεβαιώσεις που εκδίδονται από/για λογαριασμό δημοσίου φορέα υπεύθυνου για αυθεντική πηγή σε ένα κράτος μέλος αναγνωρίζεται ως τέτοια σε όλα τα άλλα κράτη μέλη.

Για την πρόσβαση σε επιγραμμικές δημόσιες υπηρεσίες βάσει του άρθρου 45γ ισχύει ότι αν απαιτείται ηλεκτρονική ταυτοποίηση με τη χρήση μέσου ηλεκτρονικής ταυτοποίησης και επαλήθευσης ταυτότητας, τότε τα δεδομένα ταυτοποίησης προσώπου στην ηλεκτρονική βεβαίωση δεν υποκαθιστούν ηλεκτρονική ταυτοποίηση και την επαλήθευση ταυτότητας εκτός αν επιτρέπεται ρητά από το κράτος-μέλος, οπότε και γίνεται επίσης δεκτή εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών από άλλα κράτη μέλη.

Όπως και σε άλλες υπηρεσίες εμπιστοσύνης έτσι και η ηλεκτρονική βεβαίωση μπορεί να έχει εγκεκριμένη μορφή εφόσον, σύμφωνα με το άρθρο 45δ ισχύει ότι: (α) πληρούνται οι απαιτήσεις του παραρτήματος V του κανονισμού, (β) η αξιολόγηση συμμόρφωσης με τις απαιτήσεις γίνεται σύμφωνα με πρότυπα, τις προδιαγραφές και τις διαδικασίες της παραγράφου 5 του παρόντος άρθρου που αναμένεται να καθοριστούν μέσω εκτελεστικών πράξεων ως τις 21 Νοεμβρίου του 2024 και (γ) σε περίπτωση που η εγκεκριμένη βεβαίωση ανακληθεί, παύει να ισχύει και δεν μπορεί να επανέλθει σε ισχύ.

[18] ηλεκτρονική βεβαίωση χαρακτηριστικών εκδιδόμενη από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή: ηλεκτρονική βεβαίωση χαρακτηριστικών που εκδίδεται από φορέα του δημόσιου τομέα που είναι υπεύθυνος για αυθεντική πηγή ή από φορέα του δημόσιου τομέα που έχει οριστεί από το κράτος μέλος για την έκδοση των εν λόγω βεβαιώσεων χαρακτηριστικών εξ ονόματος των φορέων του δημόσιου τομέα που είναι υπεύθυνοι για αυθεντικές πηγές σύμφωνα με το άρθρο 45στ και με το παράρτημα VII· [39]
αυθεντική πηγή: αποθετήριο ή σύστημα, που τηρείται υπό την ευθύνη φορέα του δημόσιου τομέα ή ιδιωτικής οντότητας, περιέχει και παρέχει χαρακτηριστικά σχετικά με φυσικό ή νομικό πρόσωπο ή αντικείμενο και θεωρείται ως πρωταρχική πηγή των εν λόγω πληροφοριών ή αναγνωρίζεται ως αυθεντική πηγή σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο, συμπεριλαμβανομένης της διοικητικής πρακτικής· [39]

Στον κανονισμό προστίθεται επίσης άρθρο σχετικά με τις απαιτήσεις για την ηλεκτρονική βεβαίωση χαρακτηριστικών που εκδίδεται από ή για λογαριασμό φορέα του δημόσιου τομέα που είναι υπεύθυνος για αυθεντική πηγή.

Τέλος, κάποιες βασικές απαιτήσεις που θέτει ο κανονισμός είναι ότι: (α) οι πάροχοι ηλεκτρονικών βεβαιώσεων πρέπει να δίνουν στους χρήστες των ψηφιακών πορτοφολιών τη δυνατότητα να ζητούν, να λαμβάνουν, να αποθηκεύουν και να διαχειρίζονται την βεβαίωση ανεξάρτητα από το κράτος μέλος όπου παρέχεται το ψηφιακό πορτοφόλι, (β) οι πάροχοι (εγκεκριμένων ή μη) ηλεκτρονικών βεβαιώσεων απαγορεύεται να συνδυάζουν δεδομένα σχετικά με την υπηρεσία που προσφέρουν με δεδομένα προσωπικού χαρακτήρα από άλλες υπηρεσίες των ιδίων ή συνεργατών τους, (γ) τα δεδομένα προσωπικού χαρακτήρα που αφορούν την παροχή υπηρεσιών ηλεκτρονικής βεβαίωσης χαρακτηριστικών φυλάσσονται σε λογικά διαχωρισμένο χώρο από τα υπόλοιπα δεδομένα που τηρούνται από τον πάροχο υπηρεσιών ηλεκτρονικής βεβαίωσης χαρακτηριστικών και τέλος (δ) οι πάροχοι υπηρεσιών εγκεκριμένης ηλεκτρονικής βεβαίωσης χαρακτηριστικών εφαρμόζουν την παροχή των εν λόγω εγκεκριμένων υπηρεσιών εμπιστοσύνης κατά τρόπο λειτουργικά διαχωρισμένο από άλλες υπηρεσίες που παρέχουν. [39]

Υπηρεσίες ηλεκτρονικής αρχειοθέτησης

Η δεύτερη νέα υπηρεσία εμπιστοσύνης είναι αυτή της ηλεκτρονικής αρχειοθέτησης που αναλύεται στα άρθρα 45θ και 45ι. Η υπηρεσία της ηλεκτρονικής αρχειοθέτησης έχει ως στόχο την διατήρηση και δυνατότητα χρήσης πληροφοριών σε μεγάλο βάθος χρόνου. Συγκεκριμένα, σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό ηλεκτρονικών δεδομένων/εγγράφων που διαφυλάσσονται μέσω υπηρεσίας ηλεκτρονικής αρχειοθέτησης ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για την εγκεκριμένη υπηρεσία ηλεκτρονικής αρχειοθέτησης. Η εγκεκριμένη υπηρεσία ηλεκτρονικής αρχειοθέτησης αποδεικνύει την ακεραιότητα και την προέλευση των δεδομένων ή εγγράφων που διαφυλάσσονται μέσω αυτής, για όλο το διάστημα διαφύλαξης. [39]

Οι απαιτήσεις για την εγκεκριμένη υπηρεσία ηλεκτρονικής αρχειοθέτησης είναι: (α) να παρέχεται από εγκεκριμένο πάροχο, (β) γίνεται χρήση διαδικασιών και τεχνολογιών που εξασφαλίσουν την αναγνωσιμότητα των σχετικών δεδομένων ή εγγράφων για όσο διαρκεί η νόμιμη ή συμβατική περίοδος διαφύλαξης και παράλληλα να φροντίζουν για τη διατήρηση ακεραιότητας και ακρίβειας προέλευσής τους, (γ) να προστατεύουν τα δεδομένα ή έγγραφα από απώλεια ή αλλοίωση εκτός αν αυτή αφορά το μέσο ή τον ηλεκτρονικό μορφότυπό τους και (δ) να είναι δυνατό τα εγκεκριμένα βασιζόμενα μέρη να λαμβάνουν έκθεση, η οποία να παρέχεται με αξιόπιστο, αποτελεσματικό τρόπο και φέρει εγκεκριμένη ηλεκτρονική υπογραφή ή σφραγίδα του παρόχου, και επιβεβαιώνει την ακεραιότητα των δεδομένων/εγγράφων για όλη τη διάρκεια διαφύλαξης ως τη στιγμή ανάκτησης. [39]

Ηλεκτρονικά καθολικά

Η τελευταία νέα υπηρεσία εμπιστοσύνης είναι αυτή των ηλεκτρονικών καθολικών που αναλύεται στα άρθρα 45ια και 45ιβ. Τα ηλεκτρονικά καθολικά αποτελούν την ψηφιακή μορφή ενός συστήματος τήρησης καταγραφών που διασφαλίζει την ακεραιότητα και ακρίβεια των δεδομένων μέσω μίας σειράς ηλεκτρονικών εγγραφών. Συγκεκριμένα, σε ό,τι αφορά στην νομική ισχύ, βάσει του κανονισμού, δεν απορρίπτονται η νομική ισχύς και το παραδεκτό ηλεκτρονικού καθολικού ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για εγκεκριμένο ηλεκτρονικό καθολικό. Το εγκεκριμένο ηλεκτρονικό καθολικό αποδεικνύει την ακεραιότητα των αρχείων δεδομένων που περιέχονται σε αυτό καθώς επίσης και την μοναδική και ακριβή διαδοχική χρονολογική σειρά τους. [39]

Οι απαιτήσεις για τα εγκεκριμένα ηλεκτρονικά καθολικά είναι: (α) να παρέχονται και να διαχειρίζονται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, (β) να προσδιορίζουν την προέλευση των εγγραφών δεδομένων στο καθολικό, (γ) να διασφαλίζουν τη μοναδική διαδοχική χρονολογική σειρά των εγγραφών δεδομένων στο καθολικό και (δ) η καταγραφή δεδομένων να επιτρέπει την ανίχνευση κάθε μεταγενέστερης μεταβολής τους, εξασφαλίζοντας την ακεραιότητα. Επίσης ορίζεται ότι η συμμόρφωση με τις απαιτήσεις συμπεραίνεται μόνο αν τα ηλεκτρονικά καθολικά πληρούν τα πρότυπα, τις προδιαγραφές και τις διαδικασίες που αναμένεται να οριστούν μέσω εκτελεστικών πράξεων που θα εκδώσει η Επιτροπή ως τις 21 Μαΐου 2025. [39]

Βασικές αλλαγές του κανονισμού – Πλαίσιο διακυβέρνησης

Στον αναθεωρημένο κανονισμό εντάσσεται ξεχωριστό κεφάλαιο σχετικά με το πλαίσιο διακυβέρνησης της ηλεκτρονικής ταυτοποίησης, του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας και των υπηρεσιών εμπιστοσύνης. [39]

Εποπτεία του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας

Βάσει του άρθρου 46α, κάθε κράτος μέλος πρέπει να ορίζει εποπτικό φορέα του οποίου τα στοιχεία κοινοποιεί στην Επιτροπή (όνομα και διεύθυνση) και στον οποίο ανατίθενται εξουσίες και διατίθενται πόροι ώστε να εκτελεί το ρόλο του, ο οποίος περιλαμβάνει: (α) την (εκ των προτέρων και εκ των υστέρων) εποπτεία των παρόχων ψηφιακών πορτοφολιών ώστε να διασφαλίζει ότι πληρούν τις απαιτήσεις του κανονισμού και (β) να αναλαμβάνει δράση όταν ενημερώνεται ότι υπάρχουν εικασίες ότι οι μη εγκεκριμένοι πάροχοι ή οι τα πορτοφόλια τους δεν πληρούν τις απαιτήσεις του κανονισμού. Οι εποπτικοί φορείς οφείλουν (α) να συνεργάζονται με άλλους φορείς, (β) να ζητούν πληροφορίες που απαιτούνται για την παρακολούθηση συμμόρφωσης με τον κανονισμό, (γ) να ενημερώνουν τις αρμόδιες αρχές βάσει της οδηγίας NIS 2 όταν υπάρχει σημαντική παραβίαση ασφαλείας ή απώλεια ακεραιότητας, καθώς και άλλα ενδιαφερόμενα μέρη ανάλογα με το περιστατικό, (δ) να διενεργούν επιθεωρήσεις, (ε) να απαιτούν από τους παρόχους πορτοφολιών να προχωρούν σε διορθωτικές ενέργειες όταν εντοπίζονται παραλείψεις συμμόρφωσης, (στ) όταν εντοπίζουν παράνομη ή δόλια χρήση του πορτοφολιού να αναστέλλουν ή να ακυρώνουν την καταχώρηση ή συμπερίληψη βασιζόμενων μερών στον μηχανισμό που επιτρέπει την ταυτοποίηση και επαλήθευση της ταυτότητάς τους και (ζ) να συνεργάζονται με τις αρμόδιες αρχές που έχουν συσταθεί βάσει του ΓΚΠΔ όταν υπάρχουν ενδείξεις παραβίασής του. [39]

Εποπτεία των υπηρεσιών εμπιστοσύνης

Αντίστοιχα με την εποπτεία των ψηφιακών πορτοφολιών στο άρθρο 46β ορίζονται εκ νέου οι απαιτήσεις για την εποπτεία των υπηρεσιών εμπιστοσύνης. Κάθε κράτος μέλος πρέπει να ορίζει εποπτικό φορέα που έχει συσταθεί στην επικράτειά του ή σε άλλο κράτος μέλος (κατόπιν συμφωνίας με το εν λόγω κράτος μέλος) του οποίου τα στοιχεία κοινοποιεί στην Επιτροπή (όνομα και διεύθυνση) και στον οποίο ανατίθενται εξουσίες και διατίθενται πόροι ώστε να εκτελεί το ρόλο του, κατ' αναλογία με το άρθρο 17 του eIDAS 1.0.

Συγκεκριμένα, οι εποπτικοί φορείς οφείλουν (α) να ενημερώνουν τις αρμόδιες αρχές βάσει της οδηγίας NIS 2 όταν υπάρχει σημαντική παραβίαση ασφαλείας ή απώλεια ακεραιότητας, καθώς και άλλα ενδιαφερόμενα μέρη ανάλογα με το περιστατικό, (β) να συνεργάζονται με άλλους φορείς, (γ) να αναλύουν τις εκθέσεις αξιολόγησης συμμόρφωσης, (δ) να υποβάλλουν στην Επιτροπή έκθεση με τις δραστηριότητές τους (ε) να διενεργούν ελέγχους ή να ζητούν από οργανισμούς αξιολόγησης συμμόρφωσης να το κάνουν, (στ) να συνεργάζονται με τις αρμόδιες αρχές που έχουν συσταθεί βάσει του ΓΚΠΔ όταν υπάρχουν ενδείξεις παραβίασής του, (η) να ενημερώνουν τον υπεύθυνο φορέα για τον εθνικό κατάλογο εμπιστοσύνης σχετικά με χορηγήσεις/αποσύρσεις εγκρίσεων, (θ) να ελέγχουν την ύπαρξη και την ορθή εφαρμογή των διατάξεων σχετικά με τα σχέδια τερματισμού, (ι) να απαιτούν από τους παρόχους να προχωρούν σε διορθωτικές ενέργειες όταν εντοπίζονται παραλείψεις συμμόρφωσης και τέλος να διερευνούν ισχυρισμούς που διατυπώνονται από παρόχους φυλλομετρητών ιστού και να λαμβάνουν μέτρα, εφόσον απαιτείται. [39]

Ενιαία σημεία επαφής, αμοιβαία συνδρομή και ομάδα συνεργασίας

Για την καλύτερη συνεργασία μεταξύ των εποπτικών φορέων των υπηρεσιών εμπιστοσύνης, των ψηφιακών πορτοφολιών, του ENISA και άλλων αρμόδιων αρχών βάσει του άρθρου 46γ ορίζεται ένα ενιαίο σημείο επαφής για τις υπηρεσίες εμπιστοσύνης, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας και τα κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης που λειτουργεί ως σύνδεσμος.

Για την διευκόλυνση της εποπτείας και της επιβολής υποχρεώσεων, οι εποπτικοί φορείς μπορεί να ζητούν μέσω ομάδας συνεργασίας βοήθεια από εποπτικούς φορείς άλλου κράτους μέλους. Η βοήθεια αυτή μπορεί να έχει τη μορφή ενημέρωσης, διαβούλευσης με τον άλλο φορέα, διεξαγωγής κοινής έρευνας ή της λήψης μέτρων εποπτείας ή επιβολής από τον άλλο φορέα, ενώ υπάρχουν περιπτώσεις που ο τελευταίος μπορεί να αρνηθεί τη συνδρομή, εφόσον δεν είναι αρμόδιος ή η βοήθεια που του ζητείται δεν είναι ανάλογη των εποπτικών του δραστηριοτήτων ή είναι αντίθετη με τον κανονισμό.
Τέλος, για την καλύτερη συνεργασία μεταξύ των κρατών μελών και την ανταλλαγή πληροφοριών σχετικά με τις υπηρεσίες εμπιστοσύνης, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας και τα κοινοποιημένα συστήματα ηλεκτρονικής ταυτοποίησης, συγκροτείται ομάδα συνεργασίας, βάσει του άρθρου 46ε. [39]

Χρονοδιάγραμμα εφαρμογής – Επόμενα βήματα

Ο κανονισμός έχει πλέον δημοσιευθεί στην επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης στις 30 Απριλίου και είναι σε ισχύ από τις 20 Μάϊου 2024 (20η ημέρα από τη δημοσίευση, όπως αναφέρεται στον κανονισμό). Σε ό,τι αφορά τις πιο λεπτομερείς τεχνικές προδιαγραφές και διαδικασίες για την εφαρμογή και πιστοποίηση των ψηφιακών πορτοφολιών θα περιλαμβάνονται σε εκτελεστικές πράξεις οι οποίες θα πρέπει να υιοθετηθούν μέσα σε διάστημα 6 μηνών από την αποδοχή του κανονισμού (έως τις 20 Νοεμβρίου του 2024). Παράλληλα, κάθε κράτος μέλος έχει στη διάθεσή του 24 μήνες από την ημερομηνία έναρξης ισχύος αυτών των εκτελεστικών πράξεων για να παρέχει τουλάχιστον ένα ψηφιακό πορτοφόλι στους πολίτες, με καταληκτική ημερομηνία την 20η Νοεμβρίου του 2026, ενώ 12 μήνες αργότερα (20η Νοεμβρίου του 2027) τα βασιζόμενα μέρη[19] θα πρέπει υποχρεωτικά να αποδέχονται τη χρήση των ψηφιακών πορτοφολιών. [39] [44]

Το περιεχόμενό των εκτελεστικών πράξεων αναμένεται να τροφοδοτηθεί από την λεγόμενη «εργαλειοθήκη» για τη δημιουργία των πορτοφολιών (EU Digital Identity Wallet Toolbox), ώστε να εξασφαλιστεί μία ενιαία εφαρμογή σε όλη την ΕΕ. Παράλληλα, υλοποιούνται τα πιλοτικά έργα μεγάλης κλίμακας (Large Scale Pilots) από το 2023 μέχρι το 2025 που έχουν ως στόχο να δοκιμάσουν την εφαρμογή, λειτουργικότητα, ασφάλεια και πρακτικότητα του πορτοφολιού αναφοράς ώστε να ανατροφοδοτήσουν τις διαδικασίες για την ανάπτυξή του. [45] [46]

Αναλυτικότερα, ως τις 21 Νοεμβρίου 2024, θα πρέπει μέσω εκτελεστικών πράξεων να δημιουργηθούν κατάλογοι προτύπων αναφοράς, καθώς επίσης να καθοριστούν προδιαγραφές και διαδικασίες σχετικά με:

- Τις απαιτήσεις που ορίζονται για τις δυνατότητες των ψηφιακών πορτοφολιών, τους μηχανισμούς επικύρωσής τους και την διαδικασία κοινοποίησης στην οποία υποχρεούνται τα κράτη μέλη (άρθρο 5α παρ. 23)
- Τις απαιτήσεις σχετικά με τα βασιζόμενα μέρη και την εφαρμογή των ψηφιακών πορτοφολιών (άρθρο 5β παρ. 11)
- Την πιστοποίηση των ψηφιακών πορτοφολιών (Άρθρο 5γ, παρ. 6)
- Τα μέτρα σχετικά με την παραβίαση της ασφάλειας των ψηφιακών πορτοφολιών (Άρθρο 5ε παρ. 5)

Ακόμα, μέχρι την ίδια ημερομηνία θα πρέπει να καθοριστούν μορφότυποι και διαδικασίες σχετικά με την ενημέρωση της Επιτροπής και της ομάδας συνεργασίας για τα πιστοποιημένα ψηφιακά πορτοφόλια, αλλαγές σε αυτά αλλά και τα αιτήματα διαγραφής από τον κατάλογο πιστοποιημένων πορτοφολιών (Άρθρο 5δ παρ. 7)

Σχετικά με την ηλεκτρονική ταυτοποίηση, αναμένονται επιπλέον εκτελεστικές πράξεις: Ως τις 21 Νοεμβρίου 2024, θα πρέπει να εκδοθεί εκτελεστική πράξη για τα πρότυπα αναφοράς, τις προδιαγραφές και τις διαδικασίες για την διασυνοριακή αναμφισβήτητη αντιστοίχιση ταυτότητας του άρθρου 11α του κανονισμού. Μέχρι τις 18 Μαρτίου του 25 θα πρέπει να καθοριστούν οι διαδικαστικές λεπτομέρειες για τις αξιολογήσεις από ομότιμους για την προώθηση υψηλού επιπέδου εμπιστοσύνης και ασφάλειας αντίστοιχης με το βαθμό κινδύνου. Τέλος, ως τις 18 Σεπτεμβρίου του 2025 αναμένονται εκτελεστικές πράξεις για το πλαίσιο διαλειτουργικότητας των εθνικών eID συστημάτων ώστε να υπάρχουν οι αναγκαίες ενιαίες προϋποθέσεις. [39]

[19] Λεπτομέρειες για την υποχρεωτική αποδοχή ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας παρουσιάζονται στην ενότητα Διασυνοριακή χρήση

Τέλος, θα εκδοθούν και εκτελεστικές πράξεις σχετικές τις υπηρεσίες εμπιστοσύνης και τους παρόχους αυτών. Συγκεκριμένα:

Αρχικά, μέχρι τις 21 Νοεμβρίου 2024, θα πρέπει μέσω εκτελεστικών πράξεων να δημιουργηθούν κατάλογοι προτύπων αναφοράς, καθώς επίσης να καθοριστούν προδιαγραφές και διαδικασίες σχετικά με:

- Τις εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (Άρθρο 45δ παρ. 5)
- Τον κατάλογο χαρακτηριστικών, καθώς και τα συστήματα για τη βεβαίωση χαρακτηριστικών και τις διαδικασίες εξακρίβωσης για τις εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών, ώστε όταν τα χαρακτηριστικά αυτά βασίζονται σε αυθεντικές πηγές εντός του δημόσιου τομέα, να διασφαλίζεται ότι λαμβάνονται μέτρα που επιτρέπουν στους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης που παρέχουν ηλεκτρονικές βεβαιώσεις χαρακτηριστικών να εξακριβώνουν τα εν λόγω χαρακτηριστικά με ηλεκτρονικά μέσα κατόπιν αιτήματος του χρήστη. (Άρθρο 45ε παρ. 2)
- Την ηλεκτρονική βεβαίωση χαρακτηριστικών που εκδίδεται από ή για λογαριασμό φορέα του δημόσιου τομέα που είναι υπεύθυνος για αυθεντική πηγή (Άρθρο 45στ παρ. 6)
- Την κοινοποίηση των φορέων του δημοσίου τομέα υπεύθυνου για αυθεντική πηγή, συμπεριλαμβανομένης της έκθεσης αξιολόγησης συμμόρφωσης (Άρθρο 45στ παρ. 7)

Κατόπιν, μέχρι τις 21 Μαΐου 2025, θα πρέπει μέσω εκτελεστικών πράξεων να δημιουργηθούν κατάλογοι προτύπων αναφοράς, καθώς επίσης να καθοριστούν προδιαγραφές και διαδικασίες σχετικά με:

- Τις πολιτικές και τα μέτρα που πρέπει να λαμβάνουν οι μη εγκεκριμένοι πάροχοι για τη διαχείριση κινδύνων για την παροχή μη εγκεκριμένης υπηρεσίας εμπιστοσύνης (Άρθρο 19α παρ. 2)
- Την διαπίστευση των οργανισμών αξιολόγησης της συμμόρφωσης και για την έκθεση αξιολόγησης της συμμόρφωσης, με τις απαιτήσεις ελέγχου με τις οποίες γίνονται οι αξιολογήσεις αυτές και για τα συστήματα αξιολόγησης της συμμόρφωσης των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης και την υποβολή της σχετικής έκθεσης. (Άρθρο 20 παρ. 4)
- Την εξακρίβωση της ταυτότητας και την επαλήθευση των χαρακτηριστικών που πραγματοποιεί εγκεκριμένος πάροχος εμπιστοσύνης (Άρθρο 24 παρ. 1γ)
- Τις απαιτήσεις για εγκεκριμένους παρόχους εμπιστοσύνης (Άρθρο 24 παρ. 5)
- Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικής υπογραφής (Άρθρο 28 παρ. 6)
- Τις απαιτήσεις για τις εγκεκριμένες υπηρεσίες διατάξεων εκ αποστάσεως δημιουργίας ηλεκτρονικής υπογραφής (Άρθρο 29α παρ. 1)
- Την επικύρωση εγκεκριμένων ηλεκτρονικών υπογραφών (Άρθρο 32 παρ. 3)
- Την επικύρωση των προηγμένων ηλεκτρονικών υπογραφών με βάση εγκεκριμένα πιστοποιητικά (Άρθρο 32α παρ. 2)
- Την εγκεκριμένη υπηρεσία επικύρωσης προηγμένων ηλεκτρονικών υπογραφών με βάση εγκεκριμένα πιστοποιητικά (Άρθρο 33 παρ. 2)
- Την εγκεκριμένη υπηρεσία διαφύλαξης για εγκεκριμένες ηλεκτρονικές υπογραφές (Άρθρο 34 παρ. 2)
- Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων (Άρθρο 38 παρ. 6)
- Τη σύνδεση της ημερομηνίας και της ώρας με τα δεδομένα καθώς και για την τεκμηρίωση της ακρίβειας των χρονικών πηγών που αφορά τις απαιτήσεις για εγκεκριμένες ηλεκτρονικές χρονοσφραγίδες (Άρθρο 42 παρ. 2)

- Τις διαδικασίες αποστολής και λήψης δεδομένων που αφορά τις απαιτήσεις για εγκεκριμένες ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (Άρθρο 44 παρ. 2)
- Τα εγκεκριμένα πιστοποιητικά για την επαλήθευση της γνησιότητας ιστοτόπου (Άρθρο 45 παρ. 2)
- Τις εγκεκριμένες υπηρεσίες ηλεκτρονικής αρχειοθέτησης (Άρθρο 45θ παρ. 2)
- Τις απαιτήσεις για τα εγκεκριμένα ηλεκτρονικά καθολικά (Άρθρο 45ιβ παρ. 2)

Μέχρι τις 21 Μαΐου 2025, θα πρέπει ακόμα μέσω εκτελεστικών πράξεων:

- Να γίνει κατάρτιση των μορφότυπων και διαδικασιών κοινοποίησης και επαλήθευσης, σχετικά με την επιβεβαίωση συμμόρφωσης με τις απαιτήσεις για την έναρξη εγκεκριμένης υπηρεσίας εμπιστοσύνης (Άρθρο 21 παρ. 4)
- Να θεσπιστούν οι μορφότυποι και οι διαδικασίες που εφαρμόζονται για την κοινοποίηση των πληροφοριών για τις εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής (Άρθρο 31 παρ. 3)
- Να γίνει κατάρτιση των μορφότυπων και διαδικασιών σχετικά με την έκθεση δραστηριοτήτων που πρέπει να υποβάλλουν οι εποπτικοί φορείς των ψηφιακών πορτοφολιών και των υπηρεσιών εμπιστοσύνης στην Επιτροπή. (Άρθρο 46β παρ. 7 και άρθρο 46γ παρ. 7)
- Να οριστούν οι διαδικαστικές λεπτομέρειες, που αφορούν τα καθήκοντα της ομάδας συνεργασίας (Άρθρο 47ε παρ. 7)

Τέλος, ως τις 21 Μαΐου 2026, η Επιτροπή θα πρέπει να αξιολογήσει αν απαιτείται η έκδοση εκτελεστικών πράξεων για την κατάρτιση καταλόγου προτύπων αναφοράς και τον καθορισμό προδιαγραφών και διαδικασιών για τις προηγμένες ηλεκτρονικές υπογραφές και τις προηγμένες ηλεκτρονικές σφραγίδες αντίστοιχα. (Άρθρα 26 παρ. 2 και άρθρο 36 παρ. 2)

2.3 EU Digital Identity Wallet Toolbox & Large-Scale Pilots

Στα πλαίσια ενεργειών της ΕΕ για την αναθεώρηση του κανονισμού, η Ευρωπαϊκή Επιτροπή αποδέχθηκε τον Ιούνιο του 2021 την πρόταση ανάπτυξης ενός «συνόλου εργαλείων» συμπεριλαμβανομένου ενός πλαισίου αναφοράς και αρχιτεκτονικής (Architecture & Reference Framework - ARF) το οποίο θα περιέχει κοινές τεχνικές προδιαγραφές, πρότυπα και κατευθυντήριες γραμμές για την ανάπτυξή του πορτοφολιού. Οι μέχρι τώρα γνωστές πληροφορίες για το ARF αναλύονται στην ενότητα 3. Το πρώτο προσχέδιο του ARF δημοσιεύτηκε Η πρώτη έκδοση του ARF δημοσιεύθηκε από την Επιτροπή το Φεβρουάριο του 2023[20], ενώ έχουν ακολουθήσει και νεότερες εκδόσεις. Η εργαλειοθήκη αυτή περιέχει επίσης το βασικότερο υλικό (πηγαίος κώδικας, βιβλιοθήκες και μία ενδεικτική εφαρμογή) για την ανάπτυξη ενός πορτοφολιού προτύπου (wallet prototype) το οποίο και θα δοκιμαστεί ποικιλοτρόπως από τα προαναφερθέντα πιλοτικά έργα μεγάλης κλίμακας. [47]

Όπως αναφέρθηκε και ανωτέρω, τα πιλοτικά έργα μεγάλης κλίμακας αποτελούν μία από τις ενέργειες που πραγματοποιείται στα πλαίσια του προγράμματος της Ψηφιακής Ευρώπης, με χρονικό ορίζοντα από το 2023 ως το 2025 για την δοκιμαστική εφαρμογή του πορτοφολιού σε ποικίλες διαφορετικές περιπτώσεις που αναμένονται να χρησιμοποιηθούν στην πράξη από τους πολίτες της Ένωσης, πριν την επίσημη και ευρεία εφαρμογή του. Από τις δοκιμές αυτές αναμένεται να εντοπιστούν μεταξύ άλλων αστοχίες και ελλείψεις στην εφαρμογή του ώστε κατόπιν να υπάρξει ανατροφοδότηση για την καλύτερη υλοποίησή του αλλά και τη βελτίωση σε επίπεδο σχεδιασμού, ασφάλειας, και διαλειτουργικότητας. [46] [48]

Τα πιλοτικά έργα που είναι σε ισχύ είναι 4, λειτουργούν υπό τη μορφή συμπράξεων (consortium) από δημόσιους και ιδιωτικούς φορείς με την κατάλληλη εξειδίκευση, ενώ χρηματοδοτούνται από πόρους της Ευρωπαϊκής Επιτροπής. Στα έργα αυτά εξετάζονται 11 σενάρια, συμμετέχουν συνολικά 360 (δημόσιοι αλλά και ιδιωτικοί φορείς) από 26 χώρες της Ένωσης καθώς επίσης και η Νορβηγία, η Ισλανδία και η Ουκρανία. [46]

- POTENTIAL: Η σύμπραξη «Potential» έχει εκπροσώπους από 19 χώρες της ΕΕ (συμπεριλαμβανομένης και της Ελλάδας) καθώς και την Ουκρανία, στο έργο συμμετέχουν πάνω από 140 φορείς, ενώ εστιάζει σε 6 βασικές περιπτώσεις χρήσης: [48] [49]
    - Μία ασφαλής ηλεκτρονική ταυτότητα για πρόσβαση και χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης (eGov services) με τη γρήγορη και ασφαλή επαλήθευση ταυτότητας
    - Μία ασφαλής ηλεκτρονική ταυτότητα για άνοιγμα τραπεζικού λογαριασμού τρεχούμενου ή καταθέσεων ακόμα και διασυνοριακά (bank account opening)
    - Μία ασφαλής ηλεκτρονική ταυτότητα για την εγγραφή και ενεργοποίηση προπληρωμένων ή μη συμβολαίων κινητής τηλεφωνίας ηλεκτρονικά, ακόμα και για διασυνοριακές συνδρομές (SIM card registration)
    - Μια ασφαλής ηλεκτρονική άδεια οδήγησης για την χρήση σε υπηρεσίες ενοικίασης οχημάτων, που παράλληλα θα γίνεται αποδεκτή από αστυνομικούς οπουδήποτε στην Ευρώπη (Mobile Driving License)
    - Μία ασφαλής εγκεκριμένη ηλεκτρονική υπογραφή που θα επιτρέπει στους πολίτες να υπογράφουν έγγραφα και δηλώσεις εξ αποστάσεως (Qualified e-Signature)
    - Ένας ασφαλής ψηφιακός τρόπος για την ηλεκτρονική συνταγογράφηση σε όλη την Ευρώπη (ePerscription)

[20] Το πρώτο προσχέδιο (ARF outline) είχε δημοσιευθεί τον Φεβρουάριο του 2022.

Αξίζει να αναφερθεί πως, στη Γερμανία, είναι ενεργό ένα έργο για την δημιουργία ενός πρωτοτύπου ψηφιακού πορτοφολιού βάσει των προδιαγραφών του αναθεωρημένου κανονισμού που θα θέσει βάσεις για την διαλειτουργικότητα σε όλη την ΕΕ. Το έργο το διαχειρίζεται το Υπουργείο Εσωτερικών, ενώ υλοποιείται από μία διεπιστημονική ομάδα ειδικών (SPRIND). Ο βασικός στόχος είναι η δημιουργία ενός σεναρίου αρχιτεκτονικής (architecture concept) μέσα από το οποίο θα μπορέσουν να απαντηθούν ερωτήματα σχετικά με το οικοσύστημα του ψηφιακού πορτοφολιού που θα επικρατήσει στη χώρα. Υπάρχει ενεργός συμμετοχή του κοινού στη διαδικασία αυτή, τόσο μέσω της ανατροφοδότησης στα σενάρια αρχιτεκτονικής που δημοσιοποιούνται αλλά και μέσα από διαδικασίες συμβουλευτικής.

Ακόμα, πραγματοποιείται και ένας διαγωνισμός καινοτομίας για την ανάπτυξη πρωτοτύπων ψηφιακών πορτοφολιών που να είναι διαλειτουργικά, ασφαλή και φιλικά προς το χρήστη. Τα πρωτότυπα αυτά, θα διατεθούν στο πιλοτικό έργο μεγάλης κλίμακας POTENTIAL για την πραγματοποίηση δοκιμών στα πλαίσια των περιπτώσεων χρήσης που εξετάζονται από την εν λόγω σύμπραξη. Μέχρι τη συγγραφή της εργασίας, στις οκτώ ομάδες που λαμβάνουν μέρος στο διαγωνισμό και έχουν περάσει στην επόμενη φάση συμπεριλαμβάνονται: μία ομάδα από τη Google που αναπτύσσει ένα πρωτότυπο πάνω στις βέλτιστες πρακτικές του λειτουργικού Android και του εξυπηρετητή Google chrome, μία ομάδα από τη Samsung, μία ομάδα με μέλη από την γερμανική νεοφυή εταιρία Lissi Gmbh και μία ομάδα με μέλη από την ελληνική μη κερδοσκοπική εταιρία Gunet, από την αντίστοιχη σουηδική Sunet, και την εταιρία Yubico. Οι ομάδες αυτές δεν λαμβάνουν κάποια χρηματοδότηση, ενώ οι άλλες τέσσερις ομάδες (με μέλη από τις εταιρίες Sepheron, Ubique, Animo και AUTHADA) έχουν λάβει χρηματοδότηση. [50] [51]

- EWC: Η σύμπραξη του EWC (EU Digital Wallet Consortium) έχει ως βασικό στόχο τη δημιουργία ενός πορτοφολιού αναφοράς για την διερεύνηση της χρήσης της ηλεκτρονικής ταυτότητας και ηλεκτρονικής βεβαίωσης χαρακτηριστικών ως διαπιστευτήρια στα πλαίσια ταξιδιών. Ως δευτερεύουσες περιπτώσεις χρήσης εξετάζει τη χρήση του πορτοφολιού για ηλεκτρονικές πληρωμές και την χρήση διαπιστευτηρίων για την απόδειξη ότι ένα πρόσωπο είναι ο νόμιμος εκπρόσωπος ενός οργανισμού και για την εξουσιοδότηση εκτέλεσης ενεργειών. Στο έργο αυτό συμμετέχουν εκπρόσωποι και των 27 κρατών-μελών της ΕΕ (συμπεριλαμβανομένης και της Ελλάδας), άλλων χωρών, αλλά και διάφοροι συνεργάτες. [48] [52]
- DC4EU: Η σύμπραξη του DC4EU (Digital Credential for Europe) εφαρμόζει πιλοτικά έργα σε 2 βασικούς τομείς: της εκπαίδευσης και της κοινωνικής ασφάλισης. Αναλυτικότερα, εστιάζει στις απαιτήσεις για την ταυτοποίηση στον τομέα της εκπαίδευσης καθώς και στην έκδοση αλλά και χρήση σχετικών διαπιστευτηρίων και επαγγελματικών προσόντων (professional qualifications) για ακαδημαϊκούς και σπουδαστές, με υψηλό επίπεδο εμπιστοσύνης και διασυνοριακή αναγνώριση. Η έρευνα και οι εργασίες θα βασιστούν σε άλλα υπάρχοντα μοντέλα δεδομένων, πλαίσια και στρατηγικές. Στα πιλοτικά έργα στον τομέα της υγείας αναμένεται να δοθεί έμφαση στη διαλειτουργικότητα και δυνατότητα επεκτασιμότητας σε διασυνοριακό επίπεδο στις απαιτήσεις για την κοινωνική ασφάλιση, ιδιαίτερα σε ό,τι αφορά στην έκδοση του τυποποιημένου εγγράφου A1[21] και της ευρωπαϊκής κάρτας ασφάλισης υγείας.

[21] Αποτελεί απόδειξη ότι καταβάλλονται εισφορές κοινωνικής ασφάλισης σε άλλη χώρα της ΕΕ, στην Ισλανδία, στο Λιχτενστάιν, στη Νορβηγία, στην Ελβετία ή στο Ηνωμένο Βασίλειο. Αφορά συνήθως αποσπασμένους εργαζόμενους ή άτομα που εργάζονται ταυτόχρονα σε περισσότερες από μία χώρες. [93]

Στη σύμπραξη αυτή συμμετέχουν 22 χώρες της ΕΕ (συμπεριλαμβανομένης και της Ελλάδας) καθώς επίσης η Νορβηγία, η Ουκρανία και η Ελβετία, με συνολικά 99 εμπλεκόμενους φορείς. [53]

- NOBID: Η τέταρτη σύμπραξη αποτελείται από σκανδιναβικές χώρες (Νορβηγία, Δανία), χώρες της Βαλτικής (Λετονία, Εσθονία) μαζί με την Ιταλία και τη Γερμανία, μαζί με άλλες εθνικές υπηρεσίες και συνεργάτες. Εστιάζει στην περίπτωση χρήσης του πορτοφολιού για τις ηλεκτρονικές πληρωμές τόσο εντός της ίδιας της χώρας αλλά και διασυνοριακά. Συγκεκριμένα τα πορτοφόλια θα εκδίδονται από τη Νορβηγία, Δανία, Λετονία, Ισλανδία και Ιταλία ενώ η Ένωση των Γερμανικών Ταμιευτηρίων θα συμπεριλάβει υπηρεσίες/λύσεις της στο πιλοτικό πορτοφόλι για να γίνουν δοκιμές στη Γερμανία. [54]

Πίνακας 2.1: Πιλοτικά έργα μεγάλης κλίμακας

	POTENTIAL	EWC	DC4U	NOBID
Συμμετοχή Χωρών ΕΕ	19	27	22	5
Συμμετοχή Ελλάδας	Ναι	Ναι	Ναι	Όχι
Συμμετοχή Χωρών εκτός ΕΕ	1 (Ουκρανία)	4 (Ουκρανία, Νορβηγία, Ηνωμένο Βασίλειο, Ελβετία)	3 (Νορβηγία, Ουκρανία, Ελβετία)	1 (Νορβηγία)
Συνεργα-ζόμενοι Φορείς	140 ιδιωτικοί και δημόσιοι οργανισμοί	41 συνεργάτες 35 βοηθητικές οντότητες	99 φορείς	7 εθνικοί φορείς 20 συνεργάτες
Σενάρια	• Υπηρεσίες eGov • Άνοιγμα τραπεζικού λογαριασμού • Εγγραφή κάρτας SIM • Χρήση άδειας οδήγησης • Χρήση εγκεκριμένων ηλεκτρονικών υπογραφών • Ηλεκτρονική συνταγογράφηση	• Διαπιστευτήρια για ταξίδια • Υπηρεσίες πληρωμών • Υπηρεσίες σχετικές εκπροσώπηση οργανισμών	• Διαπιστευτήρια στον τομέα της εκπαίδευσης • Κοινωνική ασφάλιση	• Υπηρεσίες πληρωμών

2.4 Αναμενόμενα οφέλη από τη χρήση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας

Πολίτες

- Ευρεία χρήση των πορτοφολιών σε ολόκληρη την ΕΕ για πιο αποδοτική και εκτεταμένη πρόσβαση σε υπηρεσίες
- Ταχύτερη & απλούστερη πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες καθώς μέσω του πορτοφολιού διευκολύνεται σημαντικά η διαδικασία διαχείρισης της ηλεκτρονικής ταυτότητας αλλά και χρήσης άλλων υπηρεσιών εμπιστοσύνης όπως η δημιουργία ηλεκτρονικών υπογραφών
- Διεπαφή φιλική προς το χρήστη για τη χρήση των δυνατοτήτων του πορτοφολιού
- Προστασία προσωπικών δεδομένων καθώς ο χρήστης έχει τον έλεγχο των δεδομένων του και επιλέγει να διαμοιράζεται μόνο τα απολύτως απαραίτητα στοιχεία ανά περίπτωση
- Μεγαλύτερη διαφάνεια και ασφάλεια λόγω της ανάπτυξης λογισμικού με άδεια ανοιχτής πηγής, μειώνοντας τον κίνδυνο κατάχρησης και δημιουργίας προφίλ
- Απλή μετάβαση στο ηλεκτρονικό πορτοφόλι μέσω εγγραφής με τη χρήση της ηλεκτρονικής ταυτότητας
- Δυνατότητα ανώνυμης ταυτοποίησης υπό συνθήκες για μεγαλύτερη ασφάλεια και ιδιωτικότητα

Ιδιωτικές επιχειρήσεις

- Μειωμένο κόστος & μεγαλύτερη αξιοπιστία ως προς την επαλήθευση ταυτότητας των χρηστών που χρησιμοποιούν τις υπηρεσίες, αυξάνοντας κατά συνέπεια τον όγκο και των τύπο συναλλαγών που μπορούν να γίνουν ηλεκτρονικά, βελτιώνοντας την αποδοτικότητα της επιχείρησης
- Μεγαλύτερη εμπιστοσύνη από τους χρήστες για την πραγματοποίηση «ευαίσθητων» συναλλαγών ηλεκτρονικά χάρη στην συμμόρφωση των πορτοφολιών με το ΓΚΠΔ και άλλες απαιτήσεις κυβερνοασφάλειας
- Χρήση ουδέτερης λύσης που έχει αναπτυχθεί από το δημόσιο τομέα και δεν εξαρτάται από ιδιωτικούς οργανισμούς μειώνοντας τον κίνδυνο χρήσης των δεδομένων για σκοπούς κατάρτισης προφίλ

Δημόσιοι φορείς

- Παροχή μεγαλύτερου αριθμού ψηφιακών υπηρεσιών και υψηλότερος βαθμός υιοθέτησης της χρήσης τους χάρη στην πρόσβαση των πολιτών στην ηλεκτρονική ταυτοποίηση και τα πορτοφόλια
- Μεγαλύτερη ασφάλεια και προστασία προσωπικών δεδομένων σε όλες τις συναλλαγές/διαμοιρασμό δεδομένων, χάρη στα ισχυρά τεχνικά πρότυπα που θα χρησιμοποιούνται και κατά συνέπεια στις υψηλές απαιτήσεις που θα τίθενται αλλά και την πιστοποίηση συμμόρφωσης με αυτές
- Καταπολέμηση περιπτώσεων απάτης (περιπτώσεων χρηστών που υποδύονται άλλους χρήστες, αλλά και κλοπής ταυτότητας)

Κοινωνία

Συμπερασματικά, η σταδιακή υιοθέτηση των ηλεκτρονικών πορτοφολιών θα αποτελέσει κομβικό σημείο για την ψηφιακή εξέλιξη της ΕΕ. Αναμένεται ευρεία πρόσβαση των πολιτών στις υπηρεσίες αυτές με γνώμονα την ασφάλεια, την ιδιωτικότητα, την εμπιστοσύνη και τη διαλειτουργικότητα, μεγαλύτερη υιοθέτηση εύκολων και ασφαλών ηλεκτρονικών συναλλαγών, κινητοποίηση των επιχειρήσεων για διεύρυνση των υπηρεσιών που προσφέρουν αλλά και αποδοτικότερη διαχείριση διεργασιών όπως για παράδειγμα της επαλήθευσης ταυτότητας και κατά συνέπεια οικονομική ανάπτυξη. [45] [55]

3 ΤΟ ΕΥΡΩΠΑΪΚΟ ΨΗΦΙΑΚΟ ΠΟΡΤΟΦΟΛΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΤΗΤΑΣ

3.1 Λεπτομέρειες από τον αναθεωρημένο κανονισμό

Γενικές προδιαγραφές για τα ψηφιακά πορτοφόλια

Με την εισαγωγή και αξιοποίηση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας, όπως περιεγράφηκε και στο κεφάλαιο 2, αναμένεται οι χρήστες του σε όλη την ΕΕ να μπορούν με ασφάλεια να επαληθεύουν την ταυτότητά τους όταν θέλουν να έχουν πρόσβαση σε ιδιωτικές και δημόσιες υπηρεσίες, να αποθηκεύουν ή να παρουσιάζουν ψηφιακά έγγραφα μέσα από τα κινητά τους τηλέφωνα, αλλά και να υπογράφουν ή σφραγίζουν έγγραφα ηλεκτρονικά. Παράλληλα θα διασφαλίζεται η ιδιωτικότητά τους, καθώς οι χρήστες θα διατηρούν τον έλεγχο των πληροφοριών που μοιράζονται και με ποιες οντότητες. [56]

Σύμφωνα με τον κανονισμό, τα ψηφιακά πορτοφόλια πρέπει να παρέχονται είτε απευθείας από το κράτος-μέλος, είτε με εντολή του, είτε ανεξάρτητα από αυτό αλλά να είναι αναγνωρισμένα από το κράτος-μέλος. Επίσης, τα βασικά στοιχεία του κώδικα του λογισμικού πρέπει να διαθέτουν άδεια ανοιχτής πηγής, εκτός από συγκεκριμένα στοιχεία. Τα ψηφιακά πορτοφόλια πρέπει να υποστηρίζουν ένα σύνολο δυνατοτήτων που περιγράφονται στον κανονισμό, ενώ υπάρχει δυνατότητα τα κράτη-μέλη να προβλέπουν και πρόσθετες λειτουργίες. Καίριο στοιχείο των ψηφιακών πορτοφολιών είναι ο πλήρης έλεγχος από τον χρήστη των ίδιων του των δεδομένων. Η χρήση των ψηφιακών πορτοφολιών είναι εθελοντική ενώ η έκδοση, χρήση και ανάκληση τους πρέπει να γίνεται δωρεάν για τα φυσικά πρόσωπα.

Τα κράτη μέλη οφείλουν να προσφέρουν μηχανισμούς επικύρωσης δωρεάν ώστε να επαληθεύεται η ισχύς και γνησιότητα των πορτοφολιών αλλά και η γνησιότητα και η εγκυρότητα των βασιζόμενων μερών. Τα κράτη-μέλη πρέπει επίσης να διασφαλίζουν την ανάκληση της ισχύος των πορτοφολιών είτε βάσει αιτήματος χρήστη, όταν έχει τεθεί ζήτημα παραβίασης ασφάλειας του πορτοφολιού ή σε περίπτωση θανάτου του χρήστη ή παύση δραστηριότητας του νομικού προσώπου.

Θα πρέπει επίσης να προβλέπεται η ασφάλεια ήδη από το σχεδιασμό (security by design), ενώ σε περίπτωση παραβίασης ασφαλείας που αφορά το πορτοφόλι ή τα δεδομένα του, θα πρέπει οι χρήστες να ενημερώνονται άμεσα.

Τα ψηφιακά πορτοφόλια πρέπει να παρέχονται στο πλαίσιο συστήματος ηλεκτρονικής ταυτοποίησης με υψηλό επίπεδο διασφάλισης και οι πάροχοι θα πρέπει να προσφέρουν μηχανισμούς ώστε οι χρήστες να αναφέρουν εύκολα τεχνικά προβλήματα και να ζητούν τεχνική υποστήριξη. Παράλληλα, οι πάροχοι πρέπει να συλλέγουν τις ελάχιστες δυνατές πληροφορίες για την παροχή των υπηρεσιών τους και δεν επιτρέπεται να συνδυάζουν δεδομένα ταυτοποίησης ή προσωπικού χαρακτήρα που έχουν δοθεί από το χρήστη για άλλες υπηρεσίες, εκτός αν υπάρχει ρητή αίτηση του χρήστη.

Από τον τεχνικό σχεδιασμό, πρέπει να διασφαλίζεται επίσης ότι οι πάροχοι ηλ. βεβαιώσεων χαρακτηριστικών μετά την έκδοσή της βεβαίωσης δεν συλλέγουν δεδομένα που καθιστούν εφικτή τη συσχέτιση στοιχείων και την παρακολούθηση της συμπεριφοράς του χρήστη, ενώ πρέπει να επιτρέπονται τεχνικές για την προστασία της ιδιωτικής ζωής ώστε να διασφαλίζεται η αδυναμία σύνδεσης, όταν η βεβαίωση χαρακτηριστικών δεν απαιτεί την ταυτοποίηση του χρήστη. [39]

Τα ευρωπαϊκά πορτοφόλια πρέπει να πιστοποιούνται για τη συμμόρφωση με τις απαιτήσεις του κανονισμού, διαδικασία που διενεργείται από οργανισμούς που ορίζονται από τα κράτη μέλη (εκτός από συγκεκριμένες απαιτήσεις που αφορούν για παράδειγμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα που γίνεται βάσει του κανονισμού 2016/679).

Η πιστοποίηση διαρκεί 3 ως 5 έτη, εφόσον διενεργείται στο ενδιάμεσο αξιολόγηση τρωτότητας κάθε 2 έτη και διορθώνονται τα όποια ευρήματα. Τα πιστοποιημένα πορτοφόλια κοινοποιούνται στην Επιτροπή και στην ομάδα συνεργασίας και δημοσιεύονται σε σχετικό κατάλογο ο οποίος καταρτίζεται, δημοσιεύεται και διατηρείται από την Επιτροπή. Τα κράτη μέλη έχουν την ευθύνη να ενημερώνουν για τυχόν αλλαγές, ενώ μπορούν να υποβάλλουν και αίτημα διαγραφής ενός πορτοφολιού από τον κατάλογο. [39]

Δυνατότητες ψηφιακών πορτοφολιών

Τα ψηφιακά πορτοφόλια πρέπει να προσφέρουν ένα σύνολο από δυνατότητες με τρόπο που να είναι διαφανής, ανιχνεύσιμος και φιλικός προς το χρήστη που παρουσιάστηκαν στην ενότητα Οι βασικές αλλαγές του κανονισμού – Ψηφιακό πορτοφόλι. Αναλυτικότερα βάσει του άρθρου 5^{α} παρ.5, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας πρέπει να σχεδιαστούν με τέτοιο τρόπο ώστε να διαθέτουν κοινά πρωτόκολλα και διεπαφές μέσα από τις οποίες να υποστηρίζονται οι παρακάτω λειτουργικότητες:

- Να μπορούν να εκδίδονται δεδομένα ταυτοποίησης προσώπου, εγκεκριμένων και μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή εγκεκριμένων και μη εγκεκριμένων πιστοποιητικών για το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας
- Τα βασιζόμενα μέρη να ζητούν και να επικυρώνουν δεδομένα ταυτοποίησης προσώπου και ηλεκτρονικές βεβαιώσεις χαρακτηριστικών
- Να είναι εφικτός ο διαμοιρασμός και η προσκόμιση, στα βασιζόμενα μέρη, δεδομένων ταυτοποίησης προσώπου, ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή επιλεκτικά γνωστοποιούμενων συναφών δεδομένων εντός διαδικτύου και, κατά περίπτωση, σε λειτουργία εκτός διαδικτύου
- Ο χρήστης να μπορεί να αλληλεπιδρά με το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας και να επιδεικνύει σήμα εμπιστοσύνης πορτοφολιού[22] ψηφιακής ταυτότητας της ΕΕ
- Να είναι εφικτή η ασφαλής ένταξη του χρήστη με τη χρήση μέσου ηλεκτρονικής ταυτοποίησης σύμφωνα με το άρθρο 5α παράγραφος 24·
- Να είναι εφικτή η αλληλεπίδραση μεταξύ των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας δύο προσώπων με σκοπό τη λήψη, την επικύρωση και τον διαμοιρασμό δεδομένων ταυτοποίησης προσώπου και ηλεκτρονικών βεβαιώσεων χαρακτηριστικών με ασφαλή τρόπο·
- Να είναι εφικτή η επαλήθευση της ταυτότητας και η ταυτοποίηση βασιζόμενων μερών μέσω της εφαρμογής μηχανισμών επαλήθευσης ταυτότητας σύμφωνα με το άρθρο 5β·
- Τα βασιζόμενα μέρη να επαληθεύουν τη γνησιότητα και την ισχύ των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας·
- Να είναι εφικτή η υποβολή αιτήματος σε βασιζόμενο μέρος προκειμένου να διαγράψει τα δεδομένα προσωπικού χαρακτήρα δυνάμει του άρθρου 17 του κανονισμού (ΕΕ) 2016/679·

[22] επαληθεύσιμη, απλή και αναγνωρίσιμη ένδειξη που αναφέρει με σαφή τρόπο ότι ένα ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας έχει παρασχεθεί σύμφωνα με τον κανονισμό eIDAS 2 [39]

- Να είναι εφικτή η καταγγελία βασιζόμενου μέρους στην αρμόδια εθνική αρχή προστασίας δεδομένων όταν λαμβάνεται αίτημα παροχής δεδομένων που εικάζεται ότι είναι παράνομο ή ύποπτο·
- Να μπορούν να δημιουργηθούν εγκεκριμένες ηλεκτρονικές υπογραφές ή εγκεκριμένες ηλεκτρονικές σφραγίδες μέσω εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής ή ηλεκτρονικής σφραγίδας·

[39]

Επίσης, τα ψηφιακά πορτοφόλια πρέπει να καλύπτουν τις παρακάτω προδιαγραφές, όπως παρουσιάζονται στον κανονισμό:

- Να μην παρέχουν πληροφορίες στους παρόχους υπηρεσιών εμπιστοσύνης ηλεκτρονικών βεβαιώσεων χαρακτηριστικών σχετικά με τη χρήση των εν λόγω ηλεκτρονικών βεβαιώσεων·
- Να διασφαλίζουν ότι μπορεί να επαληθευτεί η ταυτότητα και να γίνει ταυτοποίηση των βασιζόμενων μερών με την εφαρμογή μηχανισμών επαλήθευσης της ταυτότητας σύμφωνα με το άρθρο 5β·
- Να πληρούν τις απαιτήσεις που ορίζονται στο άρθρο 8 του κανονισμού όσον αφορά το υψηλό επίπεδο διασφάλισης, ιδιαίτερα όπως αυτό εφαρμόζεται στις απαιτήσεις για απόδειξη ταυτότητας και εξακρίβωση και για τη διαχείριση των μέσων ηλεκτρονικής ταυτοποίησης και την επαλήθευση ταυτότητας·
- Στην περίπτωση της ηλεκτρονικής βεβαίωσης χαρακτηριστικών με ενσωματωμένες πολιτικές γνωστοποίησης, να εφαρμόζουν τον κατάλληλο μηχανισμό προκειμένου να ενημερώνεται ο χρήστης ότι το βασιζόμενο μέρος ή ο χρήστης του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας που ζητά την ηλεκτρονική βεβαίωση χαρακτηριστικών έχει την άδεια πρόσβασης σε τέτοια βεβαίωση·
- Να διασφαλίζουν ότι τα δεδομένα ταυτοποίησης προσώπου, τα οποία διατίθενται από το σύστημα ηλεκτρονικής ταυτοποίησης στο πλαίσιο του οποίου παρέχεται το ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας, αντιπροσωπεύουν κατά τρόπο μοναδικό το φυσικό ή νομικό πρόσωπο ή το φυσικό πρόσωπο που εκπροσωπεί το φυσικό ή νομικό πρόσωπο, και συνδέονται με το εν λόγω ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας·
- Να παρέχουν σε όλα τα φυσικά πρόσωπα τη δυνατότητα να υπογράφουν μέσω εγκεκριμένων ηλεκτρονικών υπογραφών εξ ορισμού και δωρεάν. Ωστόσο, τα κράτη μέλη μπορούν μέσα από πρόσθετα μέτρα να διασφαλίζουν ότι αυτή η δυνατότητα προσφέρεται για μη επαγγελματικούς σκοπούς.

[39]

Βασιζόμενα μέρη

Όπως ορίζεται από τον αναθεωρημένο κανονισμό, τα βασιζόμενα μέρη είναι φυσικά ή νομικά πρόσωπα που βασίζονται μεταξύ άλλων και στα ψηφιακά πορτοφόλια. Αν το μέρος αυτό σκοπεύει να προσφέρει δημόσιες ή ιδιωτικές υπηρεσίες μέσω ψηφιακής αλληλεπίδρασης πρέπει να καταχωρείται σε κατάλογο του κράτους μέλους που είναι εγκατεστημένο. Για την καταχώρηση πρέπει να παρέχει κάποιες ελάχιστες πληροφορίες όπως αυτές που απαιτούνται για την επαλήθευση της ταυτότητάς του στα πορτοφόλια, τα στοιχεία επικοινωνίας του και την προβλεπόμενη χρήση του πορτοφολιού. Οι ανωτέρω πληροφορίες πρέπει να δημοσιοποιούνται σε ηλεκτρονικά σφραγισμένη ή υπογεγραμμένη μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία, ενώ οφείλουν να ενημερώνουν για τυχόν αλλαγές σε αυτές. Τα μέρη αυτά ταυτοποιούνται στο χρήστη, ενώ από τα κράτη-μέλη προσφέρεται κοινός μηχανισμός για την διαδικασία ταυτοποίησης και επαλήθευσης ταυτότητας τους.

Επιπρόσθετα, τα βασιζόμενα μέρη έχουν την ευθύνη επαλήθευσης και επικύρωσης των δεδομένων ταυτοποίησης προσώπου και της ηλεκτρονικής βεβαίωσης χαρακτηριστικών που ζητούνται από τα πορτοφόλια, ενώ δεν πρέπει να απορρίπτουν τη χρήση ψευδωνύμων όταν η ταυτοποίηση δεν είναι απαραίτητη. [39]

Παραβίαση ασφάλειας

Σε περίπτωση που εντοπιστεί ότι είτε τα ίδια τα πορτοφόλια, είτε οι μηχανισμοί επικύρωσής τους, ή τα συστήματα ηλεκτρονικής ταυτοποίησης στο πλαίσιο των οποίων παρέχονται έχουν παραβιαστεί, ή έχει τεθεί σε κίνδυνο η αξιοπιστία τους, τότε αρχικά το κράτος μέλος πρέπει να αναστείλει άμεσα την παροχή και χρήση των πορτοφολιών και να τα αποσύρει εντελώς αν δικαιολογείται από την σοβαρότητα της παραβίασης ή του κινδύνου ή αν δεν αντιμετωπιστεί μέσα σε 3 μήνες. Σε περίπτωση αντιμετώπισης, μπορεί το κράτος μέλος να αποκαταστήσει την παροχή και χρήση τους. Τέλος, το κράτος μέλος οφείλει να ενημερώσει τους χρήστες, τα ενιαία σημεία επαφής, την Επιτροπή και τα βασιζόμενα μέρη τόσο για την αναστολή, την απόσυρση, αλλά και την αποκατάσταση παροχής και χρήσης των πορτοφολιών. [39]

Διασυνοριακή χρήση

Σε ό,τι αφορά στη διασυνοριακή χρήση και αποδοχή των ψηφιακών πορτοφολιών, ο κανονισμός ορίζει ότι:

- Όταν τα κράτη μέλη απαιτούν ηλεκτρονική ταυτοποίηση και επαλήθευση ταυτότητας για πρόσβαση σε δημόσιες υπηρεσίες, πρέπει να αποδέχονται τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας.
- Οι μεγάλες και μεσαίες επιχειρήσεις του ιδιωτικού τομέα που είναι υποχρεωμένες (βάσει εθνικού, ενωσιακού δικαίου ή συμβατικής υποχρέωσης) να απαιτούν ισχυρή επαλήθευση ταυτότητας για επιγραμμική ταυτοποίηση , πρέπει να αποδέχονται τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας, μόνο εφόσον το ζητήσει ο χρήστης, με αρχική ημερομηνία τις 21 Νοεμβρίου 2027 και μετά.
- Οι πολύ μεγάλες επιγραμμικές πλατφόρμες πρέπει να αποδέχονται και να διευκολύνουν τη χρήση των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας για την επαλήθευση ταυτότητας, εφόσον το ζητήσει ο χρήστης και σχετικά με τα ελάχιστα δεδομένα που απαιτούνται για την επιγραμμική υπηρεσία που απαιτεί την επαλήθευση ταυτότητας.

[39]

3.2 Περιγραφή του πλαισίου αναφοράς και αρχιτεκτονικής

Στόχος και περιεχόμενα του ARF

Όπως ήδη έχει αναφερθεί, για να είναι εφικτή η επιτυχής υλοποίηση του πλαισίου για τα ψηφιακά πορτοφόλια, είναι σημαντικό να αποφευχθεί η εφαρμογή πολλών διαφορετικών προτύπων και τεχνολογιών. Μία τέτοια προσέγγιση θα μπορούσε να οδηγήσει ενδεχομένως σε τεχνικούς περιορισμούς και προβλήματα διαλειτουργικότητας με αποτέλεσμα τον κατακερματισμό της αγοράς, όπως είχε γίνει σε ένα βαθμό με τα σχήματα ηλεκτρονικής ταυτοποίησης. Για το σκοπό αυτό, ο κανονισμός προβλέπει μία στενή συνεργασία μεταξύ Επιτροπής, των κρατών μελών, της κοινωνίας των πολιτών, της ακαδημαϊκής κοινότητας και του ιδιωτικού τομέα και την ανάπτυξη μίας εργαλειοθήκης που θα περιέχει μεταξύ άλλων και ένα κοινό πλαίσιο αναφοράς και αρχιτεκτονικής για το ψηφιακό πορτοφόλι (ARF). Στο πλαίσιο αυτό θα περιλαμβάνονται κοινά πρότυπα, τεχνικές αναφορές, κατευθυντήριες γραμμές και βέλτιστες πρακτικές που μπορούν να αξιοποιηθούν για την υλοποίηση όλων των αναμενόμενων λειτουργιών των ψηφιακών πορτοφολιών αλλά και της διαλειτουργικότητας τους, συμπεριλαμβανομένων των ηλεκτρονικών υπογραφών και των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης για την ηλεκτρονική βεβαίωση χαρακτηριστικών, όπως προβλέπεται στον παρόντα κανονισμό. [39]

Το πλαίσιο αυτό είναι διαρκώς αναπτυσσόμενο και στην κάθε νεότερη έκδοση προστίθενται περισσότερες λεπτομέρειες για την υλοποίηση του πορτοφολιού:

- ARF Outline: Μία υψηλού επιπέδου περιγραφή της κεντρικής ιδέας του ψηφιακού πορτοφολιού, συμπεριλαμβανομένων των στόχων, των εμπλεκόμενων μερών, τεχνικών και μη απαιτήσεων καθώς και κάποιων βασικών συστατικών στοιχείων [57]
- ARF v.1.0.0: Η πρώτη πιο αναλυτική έκδοση του πλαισίου, που δημιουργήθηκε μετά την ανατροφοδότηση που δόθηκε, περιγράφει τις βασικές έννοιες, τους στόχους του πορτοφολιού, το οικοσύστημα του, τις απαιτήσεις για την έκδοση δεδομένων ταυτοποίησης προσώπου και εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, μία βασική περιγραφή της αρχιτεκτονικής του πορτοφολιού και των ροών μεταξύ των διαφόρων συστατικών στοιχείων και τη διαδικασία πιστοποίησης των πορτοφολιών. [58]
- ARF v.1.1.0: Στην έκδοση αυτή προστέθηκαν προσχέδια για τα σενάρια ταυτοποίησης και επαλήθευσης ταυτότητας για την πρόσβαση σε επιγραμμικές υπηρεσίες καθώς και για τη χρήση ηλεκτρονικής άδειας οδήγησης [59]
- ARF v.1.2.0: Στην έκδοση αυτή προστέθηκε η ενότητα με την περιγραφή του μοντέλου εμπιστοσύνης του οικοσυστήματος του ψηφιακού πορτοφολιού και προστέθηκαν 2 νέα παραρτήματα με τους κανόνες για τα δεδομένα ταυτοποίησης προσώπων και την ηλεκτρονική άδεια οδήγησης [60]
- ARF v.1.3.0: Στην έκδοση τροποποιήθηκε η ενότητα 5η με το μοντέλο δεδομένων του ψηφιακού πορτοφολιού, τροποποιήθηκε η 6^{η} ενότητα με το μοντέλο εμπιστοσύνης, τροποποιήθηκαν οι προδιαγραφές των λύσεων ψηφιακών πορτοφολιών ενώ προστέθηκαν και 2 ακόμα παραρτήματα με τον οδηγό για το σχεδιασμό ψηφιακών πορτοφολιών και τον οδηγό για το σχεδιασμό σεναρίων διαμοιρασμού δεδομένων. [61]

- ARF v.1.4.0: Η πλέον πρόσφατη έκδοση βασίζεται στο νομικό κείμενο που υιοθετήθηκε και επίσημα και αποσκοπεί στην παρουσίαση ενός συνόλου βασικών κοινών απαιτήσεων που μπορούν να χρησιμοποιηθούν ως αναφορά για την εφαρμογή του αλλά και τον ορισμό των προδιαγραφών, προτύπων και διαδικασιών που πρέπει να αναπτύξει η Ευρωπαϊκή Επιτροπή για την υλοποίηση του νέου κανονισμού. Οι απαιτήσεις αυτές αφορούν: [62]
    - Τις βασικές δυνατότητες του ψηφιακού πορτοφολιού
    - Τα βασιζόμενα μέρη του ψηφιακού πορτοφολιού
    - Απαιτήσεις για εγκεκριμένες ηλεκτρονικές βεβαιώσεις χαρακτηριστικών
    - Την επαλήθευση χαρακτηριστικών από αυθεντικές
    - Απαιτήσεις για ηλεκτρονικές βεβαιώσεις χαρακτηριστικών που εκδίδονται από ή εκ μέρους ενός φορέα του δημοσίου τομέα (public sector body) και ζητήματα κοινοποίησης αυτών
    - Διασυνοριακή αντιστοίχιση ταυτότητας
    - Πιστοποίηση των ψηφιακών πορτοφολιών
    - Δημοσίευση του καταλόγου πιστοποιημένων ψηφιακών πορτοφολιών
    - Παραβίαση ασφαλείας ψηφιακών πορτοφολιών

Το οικοσύστημα του ψηφιακού πορτοφολιού

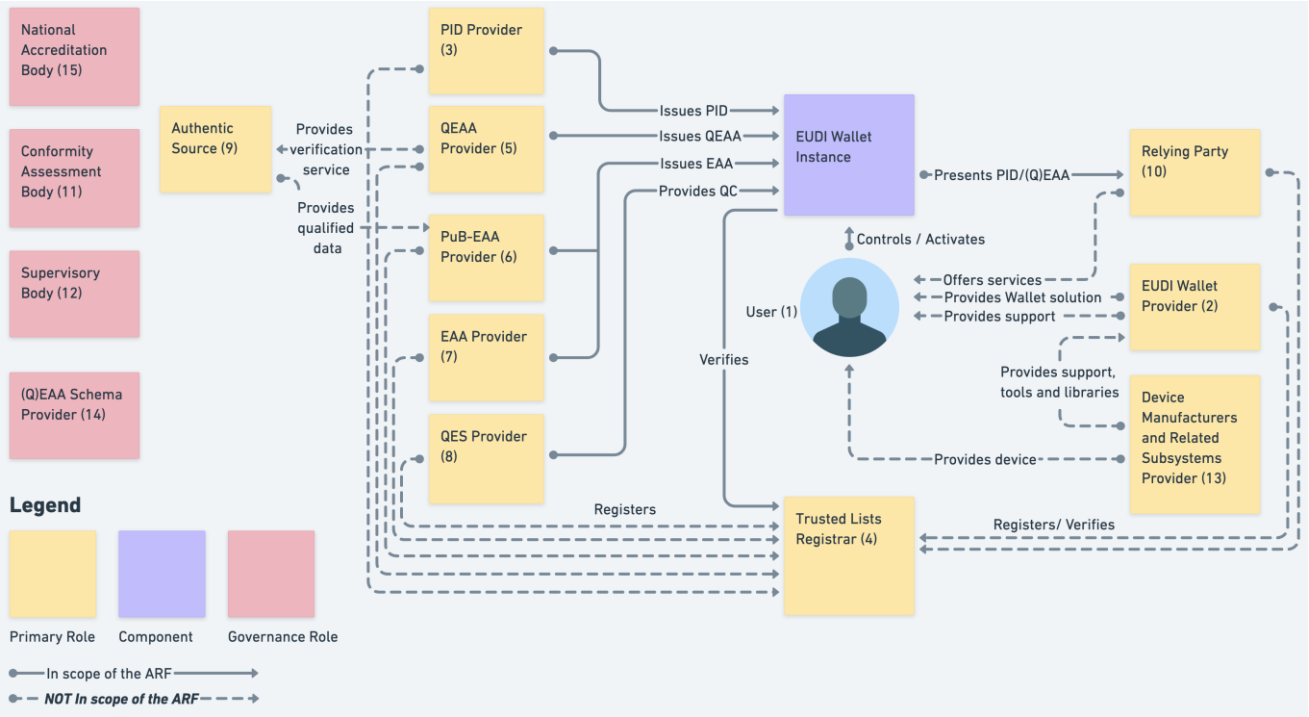
Στην Εικόνα 3.1 παρουσιάζονται οι οντότητες και βασικές ενέργειες που επιτελούν στο οικοσύστημα του ψηφιακού πορτοφολιού. Οι ενέργειες που παρουσιάζονται με συνεχόμενες γραμμές είναι εντός του πεδίου που εξετάζει το ARF. Όπως φαίνεται και από την εικόνα, ο χρήστης (1) έχει τον έλεγχο και μπορεί να ενεργοποιήσει και να χρησιμοποιήσει μία εκδοχή/ένα αντίγραφο της λύσης του πορτοφολιού που προσφέρεται από κάποιον πάροχο (2) και περιλαμβάνει την πρόσβαση διάφορες υπηρεσίες εμπιστοσύνης και προϊόντα. Ο πάροχος αυτός επίσης πρέπει να προσφέρει υπηρεσίες υποστήριξης στους χρήστες.

Μέσω του πορτοφολιού, ο χρήσης μπορεί να επιδείξει δεδομένα ταυτοποίησης ή ηλεκτρονικές βεβαιώσεις χαρακτηριστικών (εγκεκριμένες ή μη) σε βασιζόμενα μέρη (10). Το πορτοφόλι του χρήστη περιλαμβάνει δεδομένα που εκδίδονται από διαφορετικούς παρόχους:

- Οι πάροχοι δεδομένων ταυτοποίησης προσώπου (3) οφείλουν να επιβεβαιώνουν την ταυτότητα του χρήστη βάσει των προδιαγραφών υψηλού επιπέδου, να εκδίδουν τα εν λόγω δεδομένα σε μία κοινή μορφή και να παρέχουν δεδομένα στα βασιζόμενα μέρη για να μπορούν να επιβεβαιώνουν την ισχύ των δεδομένων ταυτοποίησης προσώπου.
- Οι πάροχοι εγκεκριμένων ηλεκτρονικών βεβαιώσεων χαρακτηριστικών (5) ακολουθούν το γενικό πλαίσιο εμπιστοσύνης των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης, πρέπει να έχουν μία διεπαφή για την αίτηση/αποστολή των εν λόγω βεβαιώσεων, μία διεπαφή για την αμοιβαία επαλήθευση ταυτότητας με τα πορτοφόλια και μία διεπαφή για προς τις αυθεντικές πηγές για την επιβεβαίωση των χαρακτηριστικών αυτών. Πρέπει επίσης να παρέχουν πληροφορίες για μέρη όπου είναι δυνατή η επιβεβαίωση της ισχύος των εγκεκριμένων ηλ. βεβαιώσεων χαρακτηριστικών.
- Οι ηλεκτρονικές βεβαιώσεις χαρακτηριστικών αυθεντικών πηγών δημοσίων φορέων (Public Body Authentic Source Electronic Attestation of Attributes PuB-EAA) εκδίδονται από ή εκ μέρους δημοσίων φορέων που είναι υπεύθυνοι για μία αυθεντική πηγή (6). Οι απαιτήσεις για αυτές τις αυθεντικές πηγές έχουν ως στόχο να επιτρέπουν στα βασιζόμενα μέρα να αναγνωρίζουν τις ηλ. βεβαιώσεις που εκδίδονται ως εγκεκριμένες.
- Οι μη εγκεκριμένες ηλεκτρονικές βεβαιώσεων χαρακτηριστικών μπορεί να είναι οποιοιδήποτε πάροχο υπηρεσιών εμπιστοσύνης (7). Σε ό,τι αφορά την έκδοση, χρήση και αναγνώριση των βεβαιώσεων αυτών, καλύπτεται από άλλα νομικά ή συμβατικά πλαίσια που μπορεί να αφορούν για παράδειγμα διαπιστευτήρια σχετικά με την εκπαίδευση, ηλεκτρονικές πληρωμές, ωστόσο οι πάροχοι για να μπορούν να προσφέρουν τις υπηρεσίες τους πρέπει τεχνικά να συμμορφώνονται με τις προδιαγραφές για τις διεπαφές του πορτοφολιού.
- Μέσω των ψηφιακών πορτοφολιών ο χρήστης θα έχει τη δυνατότητα να δημιουργεί δωρεάν εγκεκριμένες ηλεκτρονικές υπογραφές σε δεδομένα, είτε μέσω του ίδιου του πορτοφολιού αν είναι πιστοποιημένο ως εγκεκριμένη συσκευή δημιουργίας σφραγίδας ή υπογραφής ή απομακρυσμένα μέσω παρόχων εγκεκριμένων ηλεκτρονικών υπογραφών (8).

Σε ό,τι αφορά τις αυθεντικές πηγές (9) δηλαδή τα αποθετήρια που περιέχουν τα χαρακτηριστικά των φυσικών και νομικών προσώπων, παρέχουν εγκεκριμένα δεδομένα σε παρόχους αλλά και υπηρεσίες επιβεβαίωσης ισχύος των δεδομένων αυτών. Ο τρόπος με τον οποίο γίνονται τα ανωτέρω είναι εκτός του πεδίου εφαρμογής του πλαισίου.

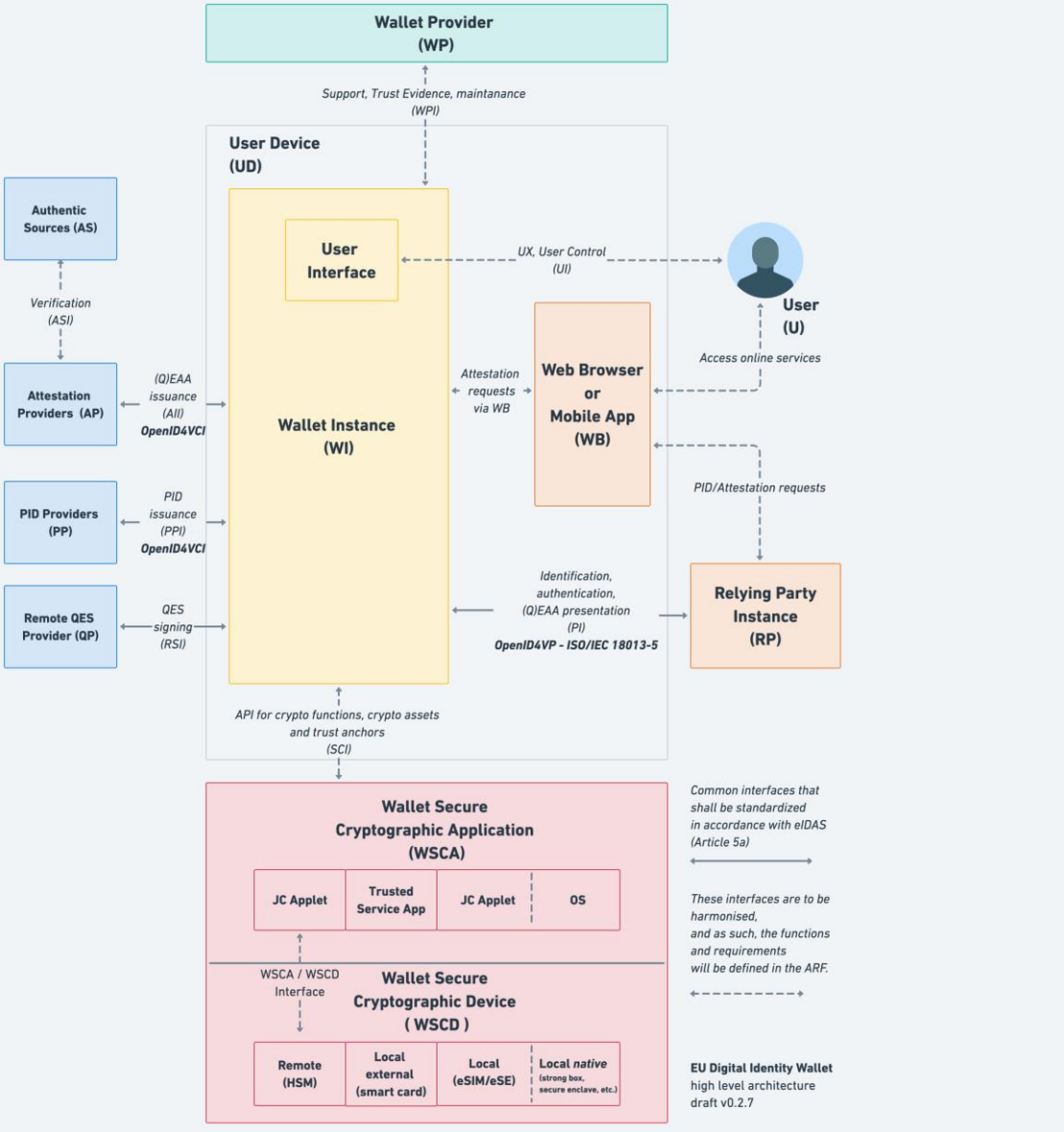
Τέλος, οι υπεύθυνοι τήρησης καταλόγων εμπιστοσύνης (4) διατηρούν τους καταλόγους με τους παρόχους υπηρεσιών & ψηφιακών πορτοφολιών που αναφέρθηκαν παραπάνω, ενώ σε αυτές έχουν πρόσβαση και τα βασιζόμενα μέρη. [62]



Εικόνα 3.1: Οντότητες και ενέργειες του οικοσυστήματος ψηφιακού πορτοφολιού

Αρχιτεκτονική του ψηφιακού πορτοφολιού

Στην πλέον πρόσφατη έκδοση του ARF, παρουσιάζονται οι σχεδιαστικές αρχές που πρέπει να τηρούνται στα ψηφιακά πορτοφόλια και κατόπιν αναλύεται η αρχιτεκτονική αναφοράς (Εικόνα 3.2), όπου περιγράφονται τα συστατικά στοιχεία των πορτοφολιών, οι βασικές σχετιζόμενες οντότητες, οι διεπαφές, τα πρωτόκολλα και οι ροές επικοινωνίας με το πορτοφόλι. [62]



Εικόνα 3.2: Αρχιτεκτονική αναφοράς ψηφιακού πορτοφολιού

Σχεδιαστικές αρχές

- Επικέντρωση στο χρήστη (user-centricity): Ο σχεδιασμός του πορτοφολιού γίνεται με βάση τις ανάγκες και την εμπειρία του χρήστη, ενώ πρέπει να είναι τέτοιος ώστε χρήστες με διαφορετικό τεχνολογικό επίπεδο ή ανάγκες να έχουν πρόσβαση σε αυτό και να αξιοποιούν τις δυνατότητες που προσφέρει. Η λύση επίσης οφείλει να είναι εύχρηστη και να μπορεί να ενσωματωθεί απλά και χωρίς προβλήματα σε διάφορα υπάρχοντα σενάρια χρήσης, ενώ οι χρήστες παράλληλα να διατηρούν τον πλήρη έλεγχο των δεδομένων τους. [62]

- Διαλειτουργικότητα: Είναι απαραίτητη η διαλειτουργικότητα ως αρχή για να είναι εφικτή η χρήση των πορτοφολιών σε όλη την ΕΕ σε ποικίλες υπηρεσίες εύκολα και χωρίς τεχνικούς περιορισμούς, όπου η ανταλλαγή δεδομένων γίνεται με ασφάλεια και με κοινά πρωτόκολλα. [62]
- Ιδιωτικότητα ήδη από το σχεδιασμό (privacy by design): Κρίσιμη έννοια για τα ψηφιακά πορτοφόλια είναι να λαμβάνεται υπόψη η ιδιωτικότητα και προστασία των δεδομένων του χρήστη ήδη από το σχεδιασμό. Τα δεδομένα που διαμοιράζονται πρέπει να είναι τα ελάχιστα απαραίτητα σε κάθε περίπτωση, ο χρήστης έχει έλεγχο στο ποια δεδομένα μοιράζεται και με ποιους ενώ υπάρχει διαφάνεια για τον τρόπο χρήσης και προστασίας τους. [62]
- Ασφάλεια ήδη από το σχεδιασμό: Αντίστοιχα με την ιδιωτικότητα, η ασφάλεια ήδη από το σχεδιασμό είναι καίρια ώστε να καθ' όλη τη διάρκεια σχεδιασμού μίας λύσης πορτοφολιού να εντοπίζονται και να διορθώνονται αδυναμίες/κενά ασφαλείας, να εφαρμόζονται τεχνικές για προγραμματισμό με γνώμονα την ασφάλεια, ενώ να ελαχιστοποιούνται τα τρωτά σημεία «εισόδου» μέσα από κατακερματισμό ευαίσθητων δεδομένων και ισχυρών μεθόδων πρόσβασης, ώστε τελικά τα πορτοφόλια να είναι ανθεκτικά σε κυβερνοεπιθέσεις και διαρροές δεδομένων. [62]

Συστατικά στοιχεία της αρχιτεκτονικής αναφοράς του ψηφιακού πορτοφολιού

- Συσκευή του χρήστη (User Device): Η συσκευή που φιλοξενεί το ψηφιακό πορτοφόλι και μπορεί να είναι κάποια κινητή συσκευή για φυσικά πρόσωπα, ή κάποιος cloud server για νομικά πρόσωπα. [62]
- Εκδοχή του πορτοφολιού[23] (Wallet Instance): Πρόκειται για την εφαρμογή που εγκαθίσταται στη συσκευή του χρήστη, χρησιμοποιείται και ελέγχεται από αυτόν, ενώ είναι μέρος της ευρύτερης λύσης του πορτοφολιού που προφέρει ο πάροχος. Η πρόσβαση σε αυτή γίνεται μέσω ενός εξυπηρετητή ή διεπαφής της ίδιας της εφαρμογής. Η εφαρμογή επικοινωνεί άμεσα με τα 2 στοιχεία που περιγράφονται παρακάτω για την ασφαλή διαχείριση κρυπτογραφικών στοιχείων και υλοποίηση κρυπτογραφικών ενεργειών, ώστε να υπάρχει υψηλό επίπεδο διασφάλισης κατά την επαλήθευση ταυτότητας. [62]
- Κρυπτογραφική συσκευή ασφαλείας πορτοφολιού (Wallet Secure Cryptographic Device - WSCD): Είναι το υλισμικό (hardware) όπου αποθηκεύονται τα κρυπτογραφικά στοιχεία (όπως κρυπτογραφικά κλειδιά), λειτουργεί η εφαρμογή ασφαλείας (που εξηγείται αμέσως παρακάτω) και εκτελούνται ενέργειες που έχουν υψηλή σημασία ως προς την ασφάλεια. Θεωρείται αδύνατο να παραβιαστεί αλλά και να αναπαραχθεί. Η συσκευή αυτή μπορεί να χρησιμοποιείται από πολλές εκδοχές του πορτοφολιού. [62]
- Κρυπτογραφική εφαρμογή ασφαλείας πορτοφολιού (Wallet Secure Cryptographic Application): είναι η ασφαλής εφαρμογή που λειτουργεί πάνω στην κρυπτογραφική συσκευή ασφαλείας και την χρησιμοποιεί, ενώ μπορεί να συσχετιστεί με μία μόνο εκδοχή του πορτοφολιού. [62]
- Σύστημα υποστήριξης παρόχου πορτοφολιού (Wallet Provider backend): Προσφέρει υπηρεσίες υποστήριξης του χρήστη, υπηρεσίες ενημερώσεων και συντήρησης ενώ προσφέρει αποδεικτικά στοιχεία εμπιστοσύνης και βεβαιώσεις για το πορτοφόλι. [62]

[23] Για τους σκοπούς της εργασίας οι έννοιες αντίγραφο/εκδοχή πορτοφολιού αλλά και εγκατεστημένο πορτοφόλι αποδίδουν τον αγγλικό όρο «wallet instance».

Διεπαφές και πρωτόκολλα

- Διεπαφή του παρόχου του πορτοφολιού (Wallet Provider Interface) χρησιμοποιείται για την επικοινωνία με τον πάροχο, ώστε να προσφέρονται υπηρεσίες υποστήριξης του χρήστη, να παρέχονται αποδεικτικά στοιχεία εμπιστοσύνης και βεβαιώσεις για το πορτοφόλι αλλά και να συλλέγονται πληροφορίες για λόγους λογοδοσίας. [62]
- Διεπαφή του χρήστη (User Interface): Μέσω αυτής ο χρήσης αλληλεπιδρά με τη δική του εκδοχή του πορτοφολιού (Instance) [62]
- Διεπαφή παρουσίασης (Presentation Interface) χρησιμοποιείται από τα βασιζόμενα μέρα ώστε να ζητούν και να λαμβάνουν δεδομένα ταυτοποίησης προσώπων και άλλες βεβαιώσεις από τα πορτοφόλια είτε απομακρυσμένα είτε όταν υπάρχει μικρή απόσταση (proximity interaction). Στην περίπτωση της απομακρυσμένης επικοινωνίας χρησιμοποιείται το πρωτόκολλο OpenId4VP, ενώ όταν υπάρχει εγγύτητα χρησιμοποιείται το πλαίσιο ISO/IEC 18013-5. Κατά την απομακρυσμένη επικοινωνία, όταν το βασιζόμενο μέρος απαιτεί επαλήθευση ταυτότητας του χρήστη και πρόσβαση στα δεδομένα για να παρέχει την υπηρεσία, η διαδικασία εκκινείται μέσω ενός εξυπηρετητή ή εφαρμογής. [62]
- Η ασφαλής κρυπτογραφική διεπαφή (Secure Cryptographic Interface) επιτρέπει την επικοινωνία του εγκατεστημένου πορτοφολιού με την κρυπτογραφική εφαρμογή ασφαλείας πορτοφολιού για την διαχείριση κρυπτογραφικών στοιχείων και την εκτέλεση κρυπτογραφικών λειτουργιών. [62]
- Η διεπαφή έκδοσης δεδομένων ταυτοποίησης προσώπου (Person Identification Data - PID Issuance Interface) βασίζεται στο πρωτόκολλο OpenID4VCI και χρησιμοποιείται για την επικοινωνία του εγκατεστημένου πορτοφολιού με τον πάροχο των δεδομένων αυτών ώστε να τα αιτείται, να τα λαμβάνει και να τα αποθηκεύει. [62]
- Οι διεπαφές για την έκδοση βεβαιώσεων (Attestation Issuance Interfaces) βασίζονται και αυτές στο πρωτόκολλο OpenID4VCI και χρησιμοποιείται ώστε το εγκατεστημένο πορτοφόλι να αιτείται τις διάφορες βεβαιώσεις που θέλει να συμπεριλάβει και να αποθηκεύσει. [62]
- Η διεπαφή απομακρυσμένης υπογραφής (Remote Signing Interface) διευκολύνει την επικοινωνία μεταξύ του εγκατεστημένου πορτοφολιού και του απομακρυσμένου παρόχου υπηρεσίας εγκεκριμένης ηλεκτρονικής υπογραφής. [62]
- Η διεπαφή αναφοράς (reporting interface) και η διεπαφή αίτησης διαγραφής (deletion request interface) δεν παρουσιάζονται στο διάγραμμα, ωστόσο είναι απαραίτητη η υλοποίησή τους ώστε να μπορεί ο χρήστης να κάνει αναφορές και να αιτείται τη διαγραφή των προσωπικών του δεδομένων. [62]

Ροές επικοινωνίας

Η επικοινωνία μεταξύ του εκάστοτε εγκατεστημένου πορτοφολιού και ενός βασιζόμενου μέρους μπορεί να γίνει με 4 διαφορετικούς τρόπους:

- Ροή εγγύτητας με επίβλεψη (Proximity Supervised Flow): Ο χρήστης του πορτοφολιού βρίσκεται σε κοντινή απόσταση από το βασιζόμενο μέρος και ένας εκπρόσωπος (φυσικό πρόσωπο) επιβλέπει τη διαδικασία ανταλλαγής δεδομένων η οποία γίνεται με κάποια τεχνολογία «εγγύτητας» όπως NFC ή Bluetooth.

- Ροή εγγύτητας χωρίς επίβλεψη (Proximity Unsupervised Flow): Ο χρήστης του πορτοφολιού βρίσκεται σε κοντινή απόσταση από το βασιζόμενο μέρος και η ανταλλαγή δεδομένων γίνεται και πάλι με κάποια τεχνολογία «εγγύτητας» όπως NFC ή Bluetooth, χωρίς όμως να υπάρχει εκπρόσωπος (φυσικό πρόσωπο) που να επιβλέπει τη διαδικασία.
- Απομακρυσμένη ροή μεταξύ διαφορετικών συσκευών (Remote Cross-Device Flow): Σε αυτή την περίπτωση ο χρήστης βλέπει τις πληροφορίες της υπηρεσίας σε διαφορετική συσκευή από αυτή που έχει εγκατεστημένο το πορτοφόλι, που χρησιμοποιείται μόνο ώστε να υπάρχει ασφάλεια κατά την περίοδο της σύνδεσης (πχ. Σαρώνοντας μέσω του πορτοφολιού ένα κωδικό QR από μία αρχική σελίδα πρόσβασης, για να αποκτήσει πρόσβαση στην υπηρεσία)
- Απομακρυσμένη ροή με χρήση μίας συσκευής (Remote Same-Device Flow): Σε αυτή την περίπτωση ο χρήστης χρησιμοποιεί τη συσκευή που έχει εγκατεστημένο το πορτοφόλι και για την ασφάλεια κατά την περίοδο της σύνδεσης στην υπηρεσία αλλά και για τη χρήση της ίδιας της υπηρεσίας, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών.

  [62]

Τύποι αρχιτεκτονικής

Βάσει της γενικής αρχιτεκτονικής του πορτοφολιού, είναι δυνατός ο σχεδιασμός 4 διαφορετικών λύσεων, όπου σε κάθε μία χρησιμοποιείται μία άλλη μορφή κρυπτογραφικής συσκευής ασφαλείας πορτοφολιού.

1. Απομακρυσμένη κρυπτογραφική συσκευή ασφαλείας πορτοφολιού *(Remote WSCD)*: Η κρυπτογραφική συσκευή είναι ξεχωριστή από τη συσκευή του χρήστη, δηλαδή βρίσκεται σε διαφορετικό σημείο, όπου για παράδειγμα ο πάροχος του πορτοφολιού μπορεί έχει υλοποιήσει μία υλική μονάδα ασφαλείας (hardware security module).
2. Τοπική εξωτερική κρυπτογραφική συσκευή ασφαλείας πορτοφολιού *(Local External WSCD)*: Εξωτερικά στοιχεία υλικού όπως «έξυπνες κάρτες» μπορεί να χρησιμοποιούνται όταν το υλισμικό της συσκευής του χρήστη δεν προσφέρει ικανοποιητική ασφάλεια. Σε αυτή την περίπτωση η συσκευή του χρήστη με κάποιο τρόπο συνδέεται ή αλληλεπιδρά με τον εξωτερική συσκευή για την πραγματοποίηση των κρυπτογραφικών λειτουργιών.
3. Τοπική κρυπτογραφική συσκευή ασφαλείας πορτοφολιού *(Local WSCD)*: Σε αυτή την περίπτωση η κρυπτογραφική συσκευή είναι ενσωματωμένη στη συσκευή του χρήστη για παράδειγμα μέσω eSIM[24], eUICC[25] ή eSE[26] και η κρυπτογραφική εφαρμογή μπορεί να εγκατασταθεί (deployed) από τον πάροχο του πορτοφολιού .
4. Υβριδική αρχιτεκτονική: Σε αυτή την περίπτωση συνδυάζονται δύο ή περισσότερα από τα παραπάνω σενάρια.

[62]

[24] eSIM: Η ενσωματωμένη κάρτα SIM που μπορεί να έχει μία κινητή συσκευή, δεν μπορεί να αφαιρεθεί από αυτή καθώς είναι κολλημένη στη μητρική πλακέτα και μπορεί να προγραμματιστεί ώστε να επιτελεί διάφορες λειτουργίες. [94]

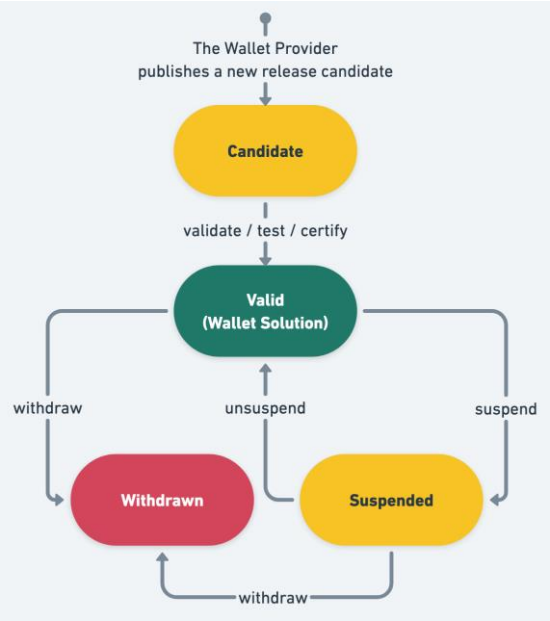
[25] eUICC: Η ενσωματωμένη κάρτα ολοκληρωμένου κυκλώματος γενικής χρήσης. Πρόκειται για το λογισμικό μίας eSIM που δίνει τη δυνατότητα αποθήκευσης πολλαπλών προφίλ δικτύου που μπορούν να είναι διαχειρίσιμα ασύρματα. [95]

[26] eSE: Είναι το ασφαλές στοιχείο, δηλαδή ένα chip που είναι απαραβίαστο (tamper-proof) και είναι ενσωματωμένο σε μία κινητή συσκευή. [96]

Κύκλος ζωής της λύσης του πορτοφολιού

Κάθε λύση πορτοφολιού μπορεί να βρίσκεται ανά πάσα στιγμή σε μία από τις 4 οριζόμενες καταστάσεις, όπως φαίνεται και στην Εικόνα 3.3. Η κατάσταση αυτή επηρεάζει την κατάσταση στην οποία θα βρίσκονται και όλα τα εγκατεστημένα πορτοφόλια αυτής της λύσης.

- Κατάσταση «υποψηφιότητας» (candidate state): Η λύση έχει υλοποιηθεί και ο πάροχός της ζητά την πιστοποίηση της στα πλαίσια ενός EUDI Wallet eID scheme.
- Κατάσταση «ισχύος» (valid state): Η λύση πληροί τις απαραίτητες τεχνικές και νομικές απαιτήσεις συμπεριλαμβανομένης της πιστοποίησης, της δημοσίευσης του παρόχου στον κατάλογο εμπιστοσύνης, οπότε το κράτος μέλος μπορεί να αποφασίσει την έναρξη παροχής πορτοφολιών αυτής της λύσης σε χρήστες.
- Κατάσταση «αναστολής» (suspended state): Η κατάσταση στην οποία βρίσκεται η λύση, όταν το κράτος μέλος αποφασίζει να διακόψει προσωρινά την ισχύ της, όταν για παράδειγμα εντοπιστεί ένα κρίσιμο γεγονός ασφαλείας σε αυτή. Μετά, μπορεί η λύση να επιστρέψει είτε σε κατάσταση ισχύος και να συνεχιστεί κανονικά η έκδοση πορτοφολιών ή να αποσυρθεί εντελώς.
- Κατάσταση «απόσυρσης» (withdrawn state): Η κατάσταση στην οποία βρίσκεται η λύση, όταν το κράτος μέλος αποφασίζει να διακόψει εντελώς την ισχύ της, και μπορεί να προέρχεται είτε από κατάσταση ισχύος είτε αναστολής.



Εικόνα 3.3: Διάγραμμα κατάστασης λύσης του ψηφιακού πορτοφολιού

[62]

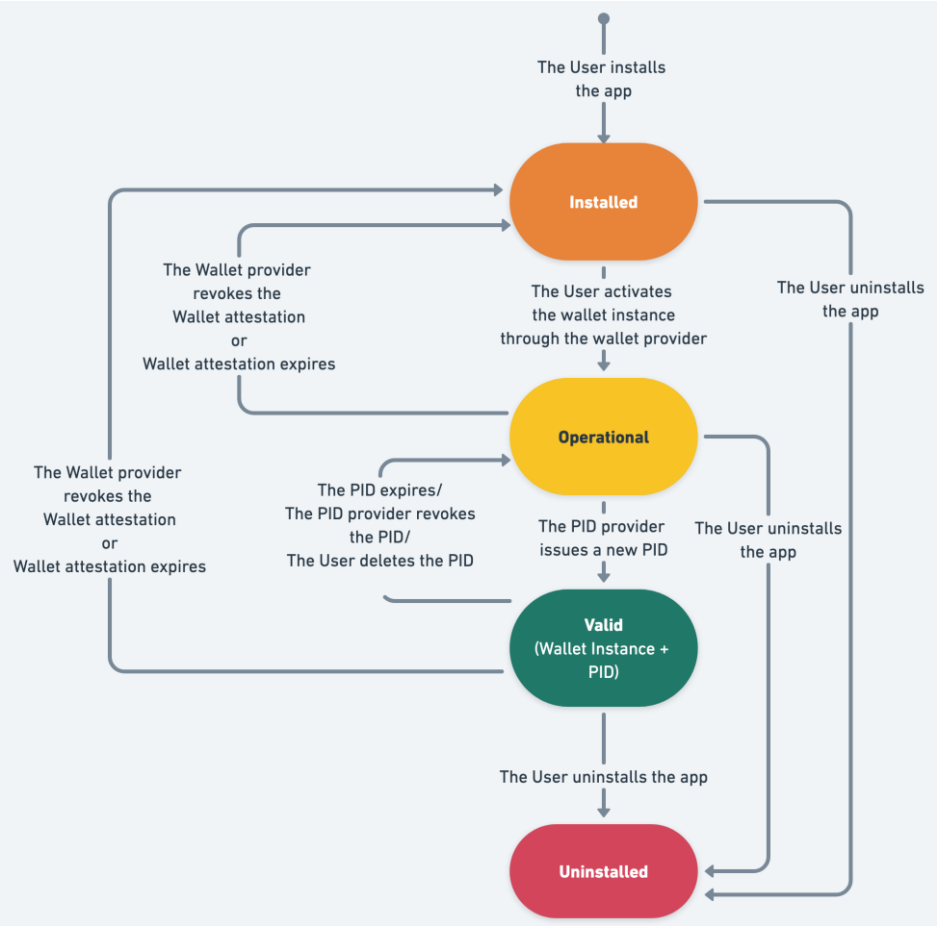
Κύκλος ζωής μεμονωμένων πορτοφολιών

- Κατάσταση «εγκατεστημένη» (installed state): Είναι το πρώτο στάδιο του κύκλου ζωής ενός πορτοφολιού και ξεκινά όταν ο χρήστης το εγκαταστήσει στη συσκευή του.
- Κατάσταση «λειτουργική» (operational state): Είναι η κατάσταση που βρίσκεται το πορτοφόλι αφού ο χρήστης το έχει ενεργοποιήσει μέσω του παρόχου και σε αυτό έχουν αποδοθεί «αποδεικτικά στοιχεία εμπιστοσύνης» (Wallet Trust Evidence) και μία βεβαίωση (Wallet Instance Attestation) από τον πάροχο.
    - Τα αποδεικτικά στοιχεία εμπιστοσύνης περιλαμβάνουν πληροφορίες για τις λειτουργικές δυνατότητες του πορτοφολιού καθώς και το επίπεδο ασφαλείας της κρυπτογραφικής συσκευής και εφαρμογής που χρειάζονται οι πάροχοι δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων προτού εκδώσουν τις ζητούμενες πληροφορίες. Ακόμα περιλαμβάνει ένα δημόσιο κλειδί, του οποίου το ιδιωτικό κλειδί αποθηκεύεται στην κρυπτογραφική συσκευή ασφαλείας. Με τη βοήθεια αυτού του ζεύγους κλειδιών μπορεί να παραχθεί ένα νέο ζεύγος κλειδιών και μέσω ενός μηχανισμού συσχέτισης (key association mechanism) μπορεί να αποδειχθεί ότι το νέο ιδιωτικό κλειδί φυλάσσεται στην ίδια κρυπτογραφική συσκευή ασφαλείας, άρα έχει το ίδιο επίπεδο ασφαλείας με το αρχικό.
    - Η βεβαίωση του πορτοφολιού περιέχει πληροφορίες που δίνουν τη δυνατότητα σε ένα πάροχο στοιχείων ή βεβαιώσεων αλλά και στα βασιζόμενα μέρη να επιβεβαιώνουν ότι η βεβαίωση και κατά συνέπεια το εγκατεστημένο πορτοφόλι δεν έχουν ανακληθεί.

  Στην «λειτουργική» κατάσταση μπορούν να πραγματοποιηθούν διαχειριστικές ή λειτουργικές ενέργειες όπως:

    - Ενημέρωση του πορτοφολιού από τον πάροχο
    - Ανάκληση του πορτοφολιού από τον πάροχο με ή χωρίς αίτημα του χρήστη, μέσω της ανάκλησης της βεβαίωσης που έχει εκδοθεί για αυτό.
    - Απεγκατάσταση του πορτοφολιού από τον χρήστη
    - Αίτηση από τον χρήστη για έκδοση δεδομένων ταυτοποίησης προσώπου και προαιρετικά εγκεκριμένης ή μη ηλεκτρονικής βεβαίωσης χαρακτηριστικών ή ηλεκτρονικής βεβαίωσης χαρακτηριστικών αυθεντικής πηγής δημοσίου φορέα
- Κατάσταση «ισχύος» (valid state): Είναι η κατάσταση που βρίσκεται το πορτοφόλι αφού σε αυτό υπάρχει ένα ισχύον σετ δεδομένων ταυτοποίησης προσώπου. Σε αυτό το στάδιο ο χρήστης μπορεί να επιδείξει τα δεδομένα ταυτοποίησης. Σε περίπτωση που τα δεδομένα αυτά λήξουν ή ανακληθούν το πορτοφόλι επιστρέφει στην «λειτουργική» κατάσταση και μπορεί να επηρεαστεί η ισχύς και η δυνατότητα χρήσης των ηλεκτρονικών βεβαιώσεων (εγκεκριμένων ή μη), των ηλεκτρονικών βεβαιώσεων χαρακτηριστικών αυθεντικών πηγών δημοσίων φορέων ή των πιστοποιητικών εγκεκριμένων ηλεκτρονικών υπογραφών ή σφραγίδων.
- Κατάσταση «απεγκατεστημένη» (uninstalled state): Όταν ο χρήστης απεγκαθιστά την εφαρμογή του πορτοφολιού.

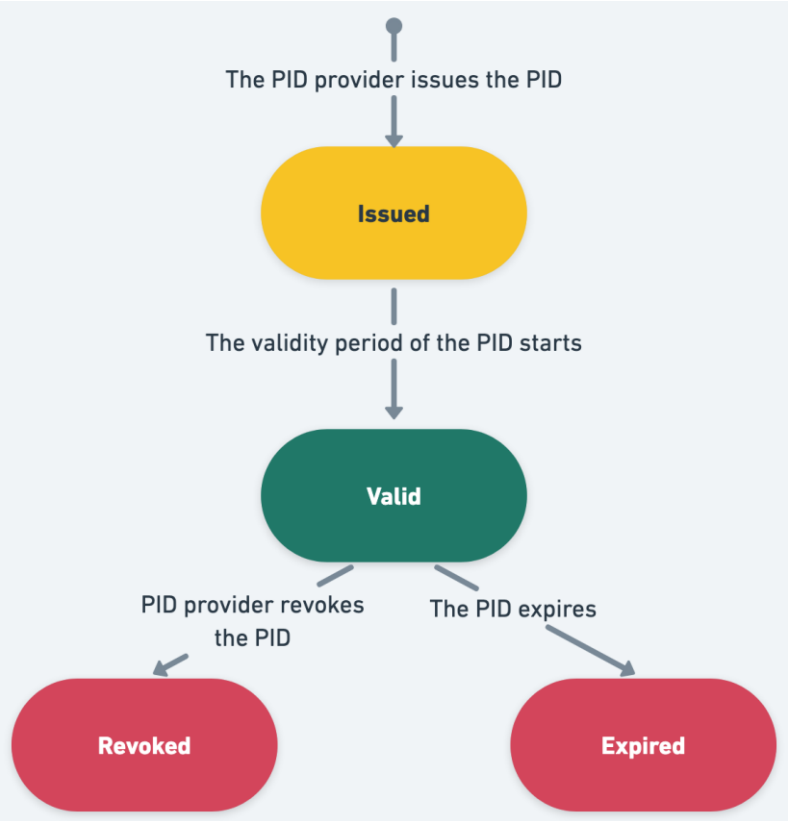
  [62]



Εικόνα 3.4: Διάγραμμα κατάστασης μεμονωμένου ψηφιακού πορτοφολιού

Κύκλος ζωής δεδομένων ταυτοποίησης προσώπου

- Κατάσταση «έκδοσης» (Issued state): Είναι το πρώτο στάδιο του κύκλου ζωής των δεδομένων ταυτοποίησης προσώπου στο οποίο «εισέρχονται» όταν εκδοθούν σε ένα εγκατεστημένο πορτοφόλι.
- Κατάσταση «ισχύος» (Valid state): Είναι το στάδιο του κύκλου ζωής των δεδομένων ταυτοποίησης προσώπου στο οποίο βρίσκονται όσο είναι σε ισχύ. Υπάρχει η περίπτωση τα δεδομένα να εκδοθούν προκαταβολικά, οπότε να μην μπουν σε ισχύ «αυτόματα» αλλά η κατάστασή τους να αλλάξει την ημερομηνία έναρξης της ισχύος.
- Κατάσταση «ανάκλησης» (Revoked state): Είναι η κατάσταση στην οποία βρίσκονται τα δεδομένα ταυτοποίησης προσώπου όταν ο πάροχος τους τα ανακαλέσει και δεν μπορούν να επανέλθουν σε κατάσταση «ισχύος».
- Κατάσταση «λήξης» (Expired state): Είναι η κατάσταση στην οποία βρίσκονται τα δεδομένα ταυτοποίησης προσώπου όταν περάσει η ημερομηνία λήξης της ισχύος τους και δεν μπορούν να επανέλθουν σε κατάσταση «ισχύος».



Εικόνα 3.5: Διάγραμμα κατάστασης δεδομένων ταυτοποίησης προσώπου

[62]

Βεβαιώσεις: κατηγορίες, μορφότυποι, διαθέσιμα πρότυπα και εγχειρίδια

Βάσει του κανονισμού, και όπως έχουν παρουσιαστεί στις προηγούμενες ενότητες, στο οικοσύστημα του ψηφιακού πορτοφολιού, εντοπίζονται τέσσερις νομικά διαφορετικές κατηγορίες βεβαιώσεων: δεδομένα ταυτοποίησης προσώπου, εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών, ηλεκτρονική βεβαίωση χαρακτηριστικών εκδιδόμενη από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή και μη εγκεκριμένη ηλεκτρονική βεβαίωση χαρακτηριστικών[27].Οι διαφοροποιήσεις μεταξύ των κατηγοριών είναι καθαρά νομικές καθώς το ίδιο διαπιστευτήριο μπορεί να είναι εγκεκριμένο ή όχι, ανάλογα με το αν ο πάροχος που το εκδίδει είναι εγκεκριμένος ή όχι. Οι βεβαιώσεις περιέχουν τα εξής στοιχεία:

- Σχήμα χαρακτηριστικών (attribute schema): Ορίζει τη δομή, τη λογική οργάνωση, τον τύπο και τον χώρο ονομάτων (namespace) για τα εν λόγω χαρακτηριστικά, μαζί με επιπλέον στοιχεία όπως πληροφορίες για την βεβαίωση, τον εκδότη, τους μηχανισμούς επικύρωσης και την απόδειξη κατοχής από τον νόμιμο χρήστη.
- Μορφότυποι δεδομένων: Ορίζουν τον τρόπο που παρουσιάζονται τα δεδομένα μέσα στη βεβαίωση όπως για παράδειγμα το σύνολο χαρακτήρων και την κωδικοποίηση που χρησιμοποιούνται.
- Μηχανισμοί απόδειξης (proof mechanisms): Ορίζουν τις μεθόδους που χρησιμοποιούνται για να την απόδειξη ακεραιότητας και αυθεντικότητας, συμπεριλαμβανομένης και της επιλεκτικής αποκάλυψης.

Παρακάτω παρουσιάζονται οι μέχρι στιγμής οι διαθέσιμοι προτυποποιημένοι μορφότυποι για την έκδοση ηλεκτρονικών βεβαιώσεων χαρακτηριστικών, ενώ για λόγους πληρότητας, τα αναφερόμενα πρότυπα αναλύονται περαιτέρω στην ενότητα 3.3.

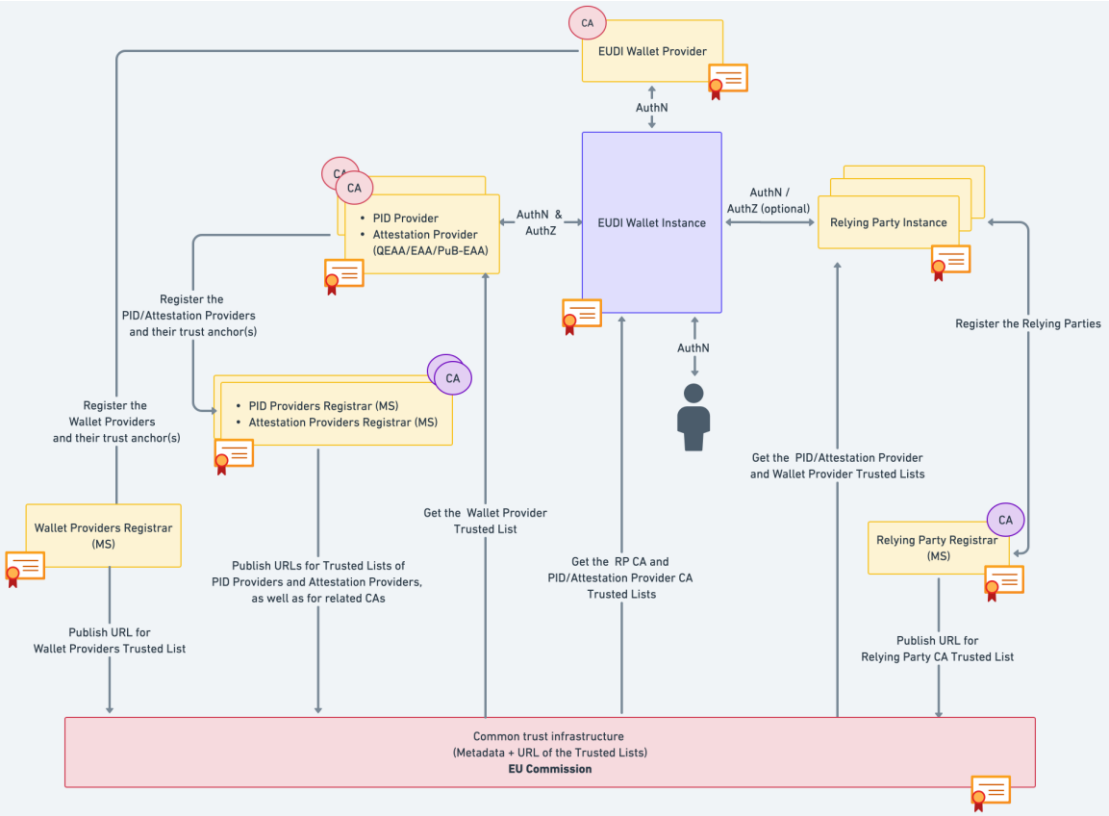
1. Στο πρότυπο ISO/IEC 18013-5 ορίζεται ένα σχήμα χαρακτηριστικών, ο μορφότυπος δεδομένων και μηχανισμοί απόδειξης για την ηλεκτρονική άδεια οδήγησης, που μπορούν να χρησιμοποιηθούν σε συνδυασμό και με άλλα σχήματα χαρακτηριστικών
2. Οι τεχνικές προδιαγραφές SD-JWT ορίζουν ένα μηχανισμό απόδειξης παρόμοιο με αυτόν του προτύπου ISO/IEC 18013-5 αλλά για διαφορετικό μορφότυπο δεδομένων.
3. Οι τεχνικές προδιαγραφές W3C VC DM v1.1 ορίζουν ένα γενικευμένο σχήμα χαρακτηριστικών που είναι αγνωστικό ως προς τους μορφότυπους δεδομένων και τους μηχανισμούς απόδειξης, ενώ στην δεύτερη έκδοση (W3C VC DM v2.0) παρουσιάζονται οι απαιτήσεις για τον μορφότυπο και προτάσεις για τους μηχανισμούς απόδειξης.
4. Οι τεχνικές προδιαγραφές SD-JWT VC ορίζουν ένα γενικευμένο σχήμα χαρακτηριστικών καθώς επίσης απαιτήσεις για τον μορφότυπο δεδομένων και τους μηχανισμούς απόδειξης.

Τέλος, στο ARF παρουσιάζεται η έννοια του εγχειριδίου βεβαίωσης (attestation rulebook), στο οποίο για κάθε τύπο βεβαίωσης ορίζεται ένα σχήμα χαρακτηριστικών, ο μορφότυπος των δεδομένων, οι μηχανισμοί απόδειξης και όταν απαιτείται οι μηχανισμοί εμπιστοσύνης για την επαλήθευση ταυτότητας και την εξουσιοδότηση (authorization). Σε κάθε εγχειρίδιο γίνονται επιλέγονται και ορισμένα πρωτόκολλα παρουσίασης (presentation protocols) που πρέπει να υποστηρίζονται από τις σχετικές βεβαιώσεις.

[27] Βεβαίωση που δεν είναι εγκεκριμένη, ούτε είναι εκδιδόμενη από ή για λογαριασμό φορέα του δημόσιου τομέα υπεύθυνου για αυθεντική πηγή

Μοντέλο εμπιστοσύνης

Στην Εικόνα 3.6 παρουσιάζεται η αρχιτεκτονική εμπιστοσύνης στο οικοσύστημα του ψηφιακού πορτοφολιού και περιλαμβάνει τα εμπλεκόμενα μέρη και τις σχετικές ενέργειες. Το μοντέλο αυτό είναι εννοιολογικό και μπορεί να εφαρμοστεί με διαφορετικούς τρόπους από τα κράτη μέλη, ενώ δεν θεωρεί ως δεδομένη κάποια συγκεκριμένη υλοποίηση. Επίσης, ισχύει τόσο για ροές εγγύτητας αλλά και απομακρυσμένες ροές, ωστόσο μπορεί να απαιτεί διαφορετικά μέτρα για την επιβεβαίωση ότι οι σχετικές απαιτήσεις πληρούνται στις δύο αυτές περιπτώσεις.



Εικόνα 3.6: Αρχιτεκτονική εμπιστοσύνης στο οικοσύστημα του ψηφιακού πορτοφολιού

Στο οικοσύστημα του ψηφιακού πορτοφολιού, υπάρχει ένα σύνολο από αλληλεπιδράσεις μεταξύ των εμπλεκόμενων μερών, για παράδειγμα όταν ένας χρήστης ζητά κάποια βεβαίωση χαρακτηριστικών από τον πάροχο ή όταν ένα βασιζόμενο μέρος ζητά από το χρήστη να του παρουσιάσει κάποια χαρακτηριστικά που έχει στο πορτοφόλι του. Οι αλληλεπιδράσεις αυτές στηρίζονται την ύπαρξη εμπιστοσύνης μεταξύ των μερών η οποία προϋποθέτει:

1. Ο αιτών να είναι σίγουρος για την ταυτότητα του μέρους που λαμβάνει το αίτημά του, και προαιρετικά το μέρος που λαμβάνει το αίτημα να είναι σίγουρο για την ταυτότητα του αιτούντος (μονομερής ή αμοιβαία επαλήθευση ταυτότητας).
2. Το μέρος που λαμβάνει το αίτημα να είναι σίγουρο ότι ο αιτών έχει το δικαίωμα να ζητήσει τα δεδομένα ή τη συγκεκριμένη ενέργεια (εξουσιοδότηση)

Σχετικά με την απαίτηση εμπιστοσύνης, γίνονται οι παραδοχές ότι: (α) κάθε οντότητα στο οικοσύστημα ενδέχεται να μην είναι αυτή που ισχυρίζεται (impersonation), (β) κάποια οντότητα να προσπαθήσει να κάνει ενέργειες που δεν επιτρέπεται και (γ) κάποιο βασιζόμενο μέρος μπορεί να προσπαθήσει να παραβιάσει την ιδιωτικότητα του χρήστη. [62]

Η εμπιστοσύνη στα στάδια του κύκλου ζωής της λύσης ψηφιακού πορτοφολιού

Εγγραφή και κοινοποίηση παρόχου ψηφιακού πορτοφολιού:

Όπως φαίνεται και από την Εικόνα 3.6, ο πάροχος απεικονίζεται πάνω από το ψηφιακό πορτοφόλι. Ο πάροχος αρχικά κάνει τόσο τη δική του εγγραφή όσο και της λύσης του στο αντίστοιχο μητρώο του κράτους μέλους του και το κράτος μέλος κοινοποιεί τον πάροχο στην Ευρωπαϊκή Επιτροπή, ενώ η λύση που παρέχει πιστοποιείται από ένα κοινοποιημένο μέρος.

Εφόσον οι διαδικασίες της εγγραφής και κοινοποίησης του παρόχου ολοκληρωθούν με επιτυχία, οι «άγκυρες εμπιστοσύνης» (trust anchors) του παρόχου συμπεριλαμβάνονται στον κατάλογο εμπιστοσύνης παρόχων πορτοφολιών. Ως «άγκυρα εμπιστοσύνης» ορίζεται ο συνδυασμός ενός δημοσίου κλειδιού και ενός αναγνωριστικού μίας οντότητας που μπορεί να χρησιμοποιηθεί για την επαλήθευση των υπογραφών ή των σφραγίδων που η οντότητα αυτή έχει δημιουργήσει. Κατά την έκδοση δεδομένων ταυτοποίησης προσώπου, ο πάροχος των στοιχείων μπορεί να χρησιμοποιήσει τις άγκυρες εμπιστοσύνης ώστε να επιβεβαιώσει τη γνησιότητα των αποδεικτικών στοιχείων εμπιστοσύνης που έχουν υπογραφεί από τον πάροχο του πορτοφολιού, ώστε να είναι σίγουρος ότι πρόκειται για ένα γνήσιο εγκατεστημένο πορτοφόλι από έναν πάροχο που θεωρείται έμπιστος. Αντίστοιχα, όταν ένα εγκατεστημένο πορτοφόλι χρησιμοποιείται για την επίδειξη κάποιων στοιχείων, το βασιζόμενο μέρος μπορεί να χρησιμοποιήσει τις άγκυρες εμπιστοσύνης ώστε να επιβεβαιώσει τη γνησιότητα της βεβαίωσης που έχει υπογράψει ο πάροχος του πορτοφολιού. [62]

Αναστολή ή απόσυρση παρόχου ψηφιακού πορτοφολιού

Όταν παρθεί η απόφαση για την αναστολή ή την απόσυρση ενός παρόχου ψηφιακού πορτοφολιού από το μητρώο (οι συνθήκες μπορεί να διαφέρουν ανά περίπτωση), τότε ο πάροχος αφαιρείται από τον αντίστοιχο κατάλογο εμπιστοσύνης. Ως αποτέλεσμα της απεγγραφής του, οι άγκυρες εμπιστοσύνης δεν θεωρούνται πλέον έμπιστες από τους παρόχους προσωπικών στοιχείων ταυτότητας, βεβαιώσεων και τα βασιζόμενα μέρη, οπότε δεν αλληλεπιδρούν πλέον με εγκατεστημένα πορτοφόλια αυτού του παρόχου. [62]

Η εμπιστοσύνη στα στάδια του κύκλου ζωής ενός παρόχου δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων

Εγγραφή και κοινοποίηση παρόχου δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων

Όπως φαίνεται και από την Εικόνα 3.6, ο πάροχος δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων απεικονίζεται αριστερά από το ψηφιακό πορτοφόλι. Ο πάροχος αρχικά κάνει την εγγραφή του στο αντίστοιχο μητρώο του κράτους μέλους του και το κράτος μέλος κοινοποιεί τον πάροχο στην Ευρωπαϊκή Επιτροπή. Εφόσον οι διαδικασίες της εγγραφής και κοινοποίησης του παρόχου ολοκληρωθούν με επιτυχία, τότε ο πάροχος λαμβάνει ένα πιστοποιητικό πρόσβασης (access certificate) και οι «άγκυρες εμπιστοσύνης» του παρόχου συμπεριλαμβάνονται στον αντίστοιχο κατάλογο εμπιστοσύνης.

Το πιστοποιητικό πρόσβασης παρέχεται από μία αρχή έκδοσης πιστοποιητικών για παρόχους δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων αντίστοιχα και χρησιμοποιείται για την επαλήθευση της ταυτότητάς τους σε ένα εγκατεστημένο πορτοφόλι όταν εκδίδουν δεδομένα ταυτοποίησης προσώπου ή βεβαιώσεις σε αυτό. Το πιστοποιητικό δηλώνει ότι το υποκείμενό του είναι πάροχος δεδομένων ταυτοποίησης προσώπου ή πάροχος εγκεκριμένων ηλεκτρονικών βεβαιώσεων ή πάροχος μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων ή πάροχος ηλεκτρονικών βεβαιώσεων χαρακτηριστικών αυθεντικών πηγών δημοσίων φορέων.

Ωστόσο, το πιστοποιητικό πρόσβασης δεν περιλαμβάνει πληροφορίες για την εξουσιοδότηση του παρόχου να εκδίδει πληροφορίες/χαρακτηριστικά. Για όλες τις περιπτώσεις εκτός των παρόχων μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων, η επαλήθευση της εξουσιοδότησης δεν απαιτείται, καθώς θεωρείται ότι αυτοί οι πάροχοι είναι νομικά έμπιστοι εξ αρχής. Για τους παρόχους μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων αναπτύσσονται μηχανισμοί ώστε να επιβεβαιώνεται η εξουσιοδότησή τους για να εκδίδουν τις βεβαιώσεις που ζητείται από ένα πορτοφόλι.

Κάθε μητρώο συμπεριλαμβάνει τις αντίστοιχες αρχές έκδοσης πιστοποιητικών στις λίστες του και πρέπει να περιλαμβάνονται κατ' ελάχιστο σε αυτές οι άγκυρες εμπιστοσύνης των αρχών αυτών.

Κατά την έκδοση δεδομένων ταυτοποίησης προσώπου, το ψηφιακό πορτοφόλι μπορεί να χρησιμοποιήσει τις άγκυρες εμπιστοσύνης ώστε να επιβεβαιώσει τη γνησιότητα του πιστοποιητικού πρόσβασης του παρόχου προσωπικών στοιχείων ή χαρακτηριστικών.

Σε ό,τι αφορά στις άγκυρες εμπιστοσύνης, για όλες τις περιπτώσεις εκτός των παρόχων μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων, με την επιτυχημένη εγγραφή και κοινοποίησή τους, οι άγκυρες συμπεριλαμβάνονται στις λίστες εμπιστοσύνης και τα βασιζόμενα μέρη μπορούν να τις χρησιμοποιήσουν για να επαληθεύσουν την γνησιότητα των δεδομένων ταυτοποίησης προσώπου και των ηλεκτρονικών βεβαιώσεων που λαμβάνουν από τα εγκατεστημένα πορτοφόλια. Οι άγκυρες εμπιστοσύνης των παρόχων μη εγκεκριμένων ηλεκτρονικών βεβαιώσεων μπορούν και αυτές να συμπεριληφθούν σε έναν κατάλογο εμπιστοσύνης, παρόλο που δεν απαιτείται. [62]

Αναστολή ή απόσυρση παρόχου δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων

Όταν παρθεί η απόφαση για την αναστολή ή την απόσυρση ενός παρόχου δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων από το μητρώο (οι συνθήκες μπορεί να διαφέρουν ανά περίπτωση), τότε οι άγκυρες εμπιστοσύνης αφαιρούνται από τον αντίστοιχο κατάλογο εμπιστοσύνης. Ως αποτέλεσμα τα βασιζόμενα μέρη δεν εμπιστεύονται πια τα στοιχεία ή τις βεβαιώσεις που εκδίδονται από τους παρόχους που έχουν ανασταλθεί ή αποσυρθεί, ενώ μπορεί να οριστούν επιπλέον μηχανισμοί για να εξασφαλιστεί ότι τα βασιζόμενα μέρη δεν θα εμπιστεύονται πλέον και τις άγκυρες εμπιστοσύνης αυτών των παρόχων. [62]

Η εμπιστοσύνη στα στάδια του κύκλου ζωής ενός βασιζόμενου μέρους

Εγγραφή βασιζόμενου μέρους

Όπως φαίνεται και από την εικόνα, το βασιζόμενο μέρος απεικονίζεται δεξιά από το ψηφιακό πορτοφόλι. Το βασιζόμενο μέρος αρχικά κάνει την εγγραφή του στο αντίστοιχο μητρώο του κράτους μέλους του και εφόσον η διαδικασία ολοκληρωθεί με επιτυχία, τότε το μητρώο το συμπεριλαμβάνει στο δημόσιο κατάλογο του και το βασιζόμενο μέρος λαμβάνει ένα πιστοποιητικό πρόσβασης από την Αρχή Έκδοσης Πιστοποιητικών βασιζόμενων μερών, για να μπορεί να επαληθεύει την ταυτότητα του όταν ζητά την επίδειξη κάποιων χαρακτηριστικών.

Επίσης, κάθε μητρώο δημιουργεί έναν κατάλογο εμπιστοσύνης Αρχών Έκδοσης Πιστοποιητικών πρόσβασης βασιζόμενων μερών που περιλαμβάνει τις «άγκυρες εμπιστοσύνης» τους. Ένα εγκατεστημένο πορτοφόλι μπορεί να χρησιμοποιήσει αυτές τις άγκυρες για να επιβεβαιώσει τη γνησιότητα του πιστοποιητικού πρόσβασης του βασιζόμενου μέρους. Το μητρώο επίσης υπογράφει και δημοσιεύει τον κατάλογο εμπιστοσύνης και κάνει το σύνδεσμο για την πρόσβαση σε αυτή δημόσια διαθέσιμο μέσω του καταλόγου των καταλόγων εμπιστοσύνης. [62]

Απεγγραφή βασιζόμενου μέρους

Όταν παρθεί η απόφαση για την απεγγραφή ενός βασιζόμενου μέρους από το μητρώο (οι συνθήκες μπορεί να διαφέρουν ανά περίπτωση), τότε ανακαλούνται όλα τα μέχρι τότε ισχύοντα πιστοποιητικά και το βασιζόμενο μέρος δεν μπορεί να αλληλεπιδράσει με τα εγκατεστημένα πορτοφόλια. [62]

Η εμπιστοσύνη στα στάδια του κύκλου ζωής ενός εγκατεστημένου πορτοφολιού

Εγκατάσταση εκδοχής/αντιγράφου πορτοφολιού

Με την μεταφόρτωση και εγκατάσταση ενός αντιγράφου της λύσης του πορτοφολιού στην συσκευή του χρήστη δημιουργούνται δύο σχέσεις εμπιστοσύνης:

- Ο χρήστης επιβεβαιώνει ότι η εφαρμογή του πορτοφολιού είναι αυθεντική και δεν περιέχει κακόβουλο λογισμικό ή άλλες απειλές. Για το σκοπό αυτό προτείνεται η εφαρμογή να είναι διαθέσιμη μόνο μέσω του επίσημου ηλεκτρονικού καταστήματος του εκάστοτε λειτουργικού, ώστε να γίνονται αυτόματοι έλεγχοι και να μην ενθαρρύνεται η μεταφόρτωση από μη επίσημα κανάλια που εγκυμονούν μεγαλύτερους κινδύνους. Στην περίπτωση που το πορτοφόλι προορίζεται για εγκατασταθεί σε συσκευή που δεν είναι κινητή, η ευθύνη επιβεβαίωσης της αυθεντικότητάς του βαραίνει τον χρήστη.
- Ο χρήστης επιβεβαιώνει ότι μπορεί να χρησιμοποιήσει την εφαρμογή για να αποκτήσει τα δεδομένα ταυτοποίησης προσώπου ή τις βεβαιώσεις, καθώς οι πάροχοι των εν λόγω στοιχείων και βεβαιώσεων δεν υποχρεούνται από τον κανονισμό να υποστηρίζουν όλες τις λύσεις ψηφιακού πορτοφολιού. Για την διευκόλυνση των χρηστών, οι πάροχοι των πορτοφολιών δημοσιεύουν λίστες με τους παρόχους στοιχείων και βεβαιώσεων που είναι συμβατοί και το αντίστροφο. [62]

Ενεργοποίηση εγκατεστημένου πορτοφολιού

Κατά την ενεργοποίηση του πορτοφολιού από τον πάροχο συμβαίνουν τα εξής:

- Ο πάροχος ζητά πληροφορίες σχετικά με τη συσκευή του χρήστη, όπως τις τεχνολογίες επικοινωνίας που υποστηρίζονται και τα χαρακτηριστικά της κρυπτογραφικής συσκευής ασφαλείας.
- Ο πάροχος εκδίδει τα αποδεικτικά στοιχεία εμπιστοσύνης που (α) περιγράφουν τις ιδιότητες και δυνατότητες του εγκατεστημένου πορτοφολιού, της συσκευής του χρήστη και της κρυπτογραφικής συσκευής ασφαλείας ώστε να μπορεί ο πάροχος στοιχείων/βεβαιώσεων να επιβεβαιώνει τη συμβατότητά του με αυτά και (β) περιέχουν ένα δημόσιο κλειδί που χρησιμοποιείται για να εξασφαλιστεί η εμπιστοσύνη σε ένα δεύτερο παραγόμενο κλειδί.
- Ο πάροχος εκδίδει τη βεβαίωση του εγκατεστημένου πορτοφολιού που δίνει τη δυνατότητα στον πάροχο στοιχείων/βεβαιώσεων και στα βασιζόμενα μέρη να επιβεβαιώνουν ότι η βεβαίωση και κατά συνέπεια το εγκατεστημένο πορτοφόλι δεν έχει ανακληθεί.
- Ο πάροχος ζητάει από τον χρήστη να ορίσει ένα μηχανισμό επαλήθευσης ταυτότητας ο οποίος απαιτείται όταν ή προτού ζητηθεί η έγκριση του χρήστη για την παρουσίαση στοιχείων σε ένα βασιζόμενο μέρος. Ο μηχανισμός αυτός μπορεί να υλοποιείται είτε από την ίδια την εφαρμογή του εγκατεστημένου πορτοφολιού είτε από την κρυπτογραφική συσκευή ασφαλείας.

- Τέλος, ο πάροχος δημιουργεί ένα λογαριασμό χρήστη, συσχετίζει το εγκατεστημένο πορτοφόλι με αυτόν, ώστε να είναι εφικτή η αίτηση αναστολής ή ανάκλησης του πορτοφολιού σε περίπτωση απώλειας ή κλοπής και δηλώνει μία ή περισσότερες μεθόδους επαλήθευσης ταυτότητας του χρήστη. Κατά την εγγραφή του χρήστη είναι δυνατό να χρησιμοποιηθούν ψευδώνυμα, ενώ ο πάροχος του πορτοφολιού μπορεί να ζητήσει περισσότερα χαρακτηριστικά για την παροχή περαιτέρω υπηρεσιών, με τη συγκατάθεση του χρήστη.

Με την ενεργοποίηση του πορτοφολιού δημιουργούνται δύο σχέσεις εμπιστοσύνης με ευθύνη του παρόχου του πορτοφολιού και δεν αναλύονται στο ARF: (α) Μέσω του εγκατεστημένου πορτοφολιού γίνεται επαλήθευση ταυτότητας του παρόχου του, επιβεβαιώνοντας ότι ο πάροχος είναι αυθεντικός και (β) ο πάροχος του πορτοφολιού επαληθεύει το πορτοφόλι, επιβεβαιώνοντας ότι πρόκειται για αυθεντική εκδοχή του, και όχι κάποια απομίμηση. [62]

Διαχείριση εγκατεστημένου πορτοφολιού

Από την ενεργοποίηση και μέχρι την απεγκατάσταση του πορτοφολιού, ο πάροχος του και ο χρήσης είναι υπεύθυνοι για τη διαχείρισή του. Από την πλευρά του παρόχου η διαχείριση περιλαμβάνει κατ' ελάχιστο τις εξής ενέργειες: (α) την εγκατάσταση νέων εκδόσεων της λύσης, (β) την ενημέρωση των αποδεικτικών στοιχείων εμπιστοσύνης και (γ) την αναστολή ή απόσυρση του εγκατεστημένου πορτοφολιού σε περίπτωση παραβίασης ασφαλείας. Παράλληλα, ο χρήστης μπορεί να ζητήσει την αναστολή ή απόσυρση του εγκατεστημένου πορτοφολιού, σε περίπτωση απώλειας ή κλοπής της συσκευής του. Αν περιέχονται στο πορτοφόλι δεδομένα ταυτοποίησης προσώπου, ο πάροχός τους μπορεί να ζητήσει την απόσυρση του εν λόγω πορτοφολιού όταν είτε το φυσικό πρόσωπο πεθαίνει, είτε το νομικό πρόσωπο σταματά τις επιχειρηματικές του δραστηριότητες. Τέλος, θα πρέπει να υποστηρίζονται διαδικασίες για δημιουργία και ανάκτηση εφεδρικών αντιγράφων των βεβαιώσεων που περιέχονται σε αυτό, αλλά και για τη μεταφορά τους σε άλλη λύση ψηφιακού πορτοφολιού.

Για την διαχείριση του εγκατεστημένου πορτοφολιού, δημιουργούνται οι παρακάτω σχέσεις εμπιστοσύνης:

- Κατά την επικοινωνία με τον πάροχο του πορτοφολιού, ο χρήστης επαληθεύει την ταυτότητα του παρόχου για να επιβεβαιώσει ότι επισκέπτεται τον αυθεντικό ιστότοπο ή πύλη του παρόχου και ότι κάποια απομίμηση, με μηχανισμούς όπως το πρωτόκολλο TLS.
- Κατά την επικοινωνία με τον πάροχο του πορτοφολιού, ο πάροχος επαληθεύει την ταυτότητα του χρήστη για να επιβεβαιώσει ότι πρόκειται για τον χρήστη που συσχετίστηκε με το πορτοφόλι κατά την ενεργοποίησή του χρησιμοποιώντας τους μηχανισμούς επαλήθευσης ταυτότητας που ορίστηκαν σε αυτό το στάδιο.
- Μέσω του εγκατεστημένου πορτοφολιού γίνεται επαλήθευση ταυτότητας του παρόχου του, επιβεβαιώνοντας ότι ο πάροχος είναι αυθεντικός.
- Ο πάροχος του πορτοφολιού επαληθεύει το πορτοφόλι, επιβεβαιώνοντας ότι πρόκειται για αυθεντική εκδοχή του, και όχι κάποια απομίμηση.

[62]

Απεγκατάσταση πορτοφολιού

Δεν απαιτούνται σχέσεις εμπιστοσύνης σε αυτό το στάδιο. Όποιος έχει πρόσβαση στη συσκευή του χρήστη μπορεί να απεγκαταστήσει την εφαρμογή. [62]

Η εμπιστοσύνη στα στάδια του κύκλου ζωής των δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων

Έκδοση στοιχείων ή βεβαιώσεων

Κατά το στάδιο έκδοσης, εγκαθιδρύονται οι ακόλουθες σχέσεις εμπιστοσύνης:

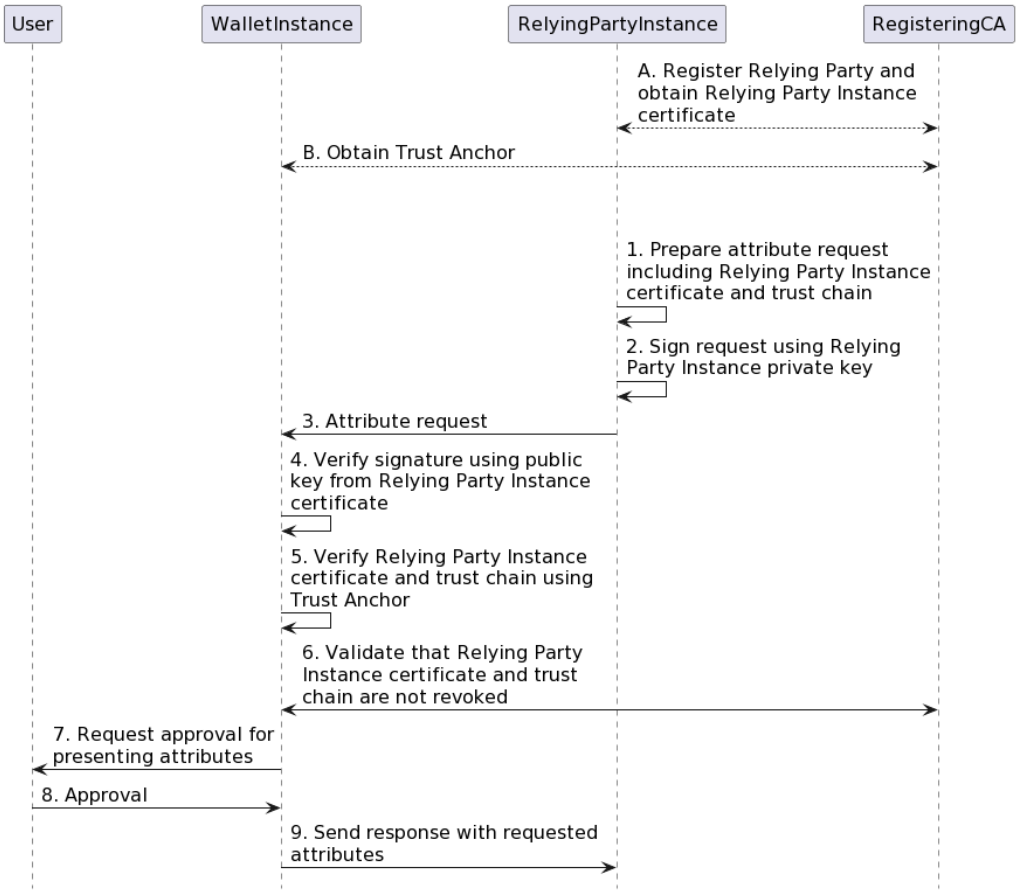
- Μέσω του εγκατεστημένου πορτοφολιού γίνεται επαλήθευση ταυτότητας του παρόχου των στοιχείων/βεβαιώσεων, επιβεβαιώνοντας ότι ο χρήστης μπορεί να εμπιστευθεί τα δεδομένα που θα λάβει. Για το σκοπό αυτό ελέγχεται το πιστοποιητικό πρόσβασης του παρόχου για να επιβεβαιωθεί ότι το υποκείμενό του είναι πράγματι πάροχος στοιχείων/βεβαιώσεων, ότι το πιστοποιητικό είναι αυθεντικό, ότι είναι σε ισχύ και ότι ο εκδότης του ανήκει στον κατάλογο εμπιστοσύνης της Αρχής έκδοσης πιστοποιητικών με τους παρόχους στοιχείων/βεβαιώσεων, η οποία έχει πρώτα μεταφορτωθεί στο πορτοφόλι. Μετά, επιβεβαιώνεται ότι τα στοιχεία/βεβαιώσεις που λήφθηκαν αντιστοιχούν στο αίτημα του χρήστη και ζητείται η έγκριση του πριν την αποθήκευσή τους.
- Ο πάροχος των στοιχείων/βεβαιώσεων επαληθεύει την ταυτότητα του χρήστη ώστε να μπορεί να εκδώσει τις κατάλληλες πληροφορίες.
- Ο πάροχος των στοιχείων/βεβαιώσεων επαληθεύει το εγκατεστημένο πορτοφόλι, με τη βοήθεια των αποδεικτικών στοιχείων εμπιστοσύνης που περιέχονται στο αίτημα έκδοσης. Ο πάροχος επιβεβαιώνει την υπογραφή του πορτοφολιού μέσω της άγκυρας εμπιστοσύνης που έχει μεταφορτώσει από τον αντίστοιχο κατάλογο εμπιστοσύνης και ότι το εγκατεστημένο πορτοφόλι κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιέχεται στα αποδεικτικά στοιχεία εμπιστοσύνης. Προαιρετικά επαληθεύεται ότι το εν λόγω πορτοφόλι υποστηρίζει όλα τα απαραίτητα χαρακτηριστικά που ο πάροχος απαιτεί, επαληθεύονται οι ιδιότητες της κρυπτογραφικής συσκευής ασφαλείας και ότι το κλειδί των στοιχείων/βεβαιώσεων προστατεύεται από τη συσκευή αυτή.
- Ο πάροχος των στοιχείων/βεβαιώσεων επιβεβαιώνει ότι το εν λόγω πορτοφόλι δεν έχει ανακληθεί ή αποσυρθεί μέσω της βεβαίωσης του πορτοφολιού.
- Μετά την έκδοση των στοιχείων/βεβαιώσεων ο χρήστης μπορεί να ενεργοποιήσει το εγκατεστημένο πορτοφόλι πριν το χρησιμοποιήσει, παραδείγματος χάριν εισάγοντας κάποιον κωδικό που έχει σταλεί από τον πάροχο του πορτοφολιού με διαφορετικό μέσο.

[62]

Παρουσίαση/Επίδειξη στοιχείων ή βεβαιώσεων σε βασιζόμενο μέρος

Κατά την επεξεργασία του αιτήματος για παρουσίαση στοιχείων/βεβαιώσεων σε βασιζόμενο μέρος εγκαθιδρύονται οι ακόλουθες σχέσεις εμπιστοσύνης:

- Μέσω του εγκατεστημένου πορτοφολιού γίνεται επαλήθευση ταυτότητας του βασιζόμενου μέρους με τη βοήθεια του πιστοποιητικού πρόσβασης του βασιζόμενου μέρους με τα πρωτόκολλα που περιγράφονται στα πρότυπα ISO/IEC 18013-5 και OpenID4VP, επιβεβαιώνοντας ότι ο χρήστης μπορεί να τον εμπιστευθεί. Τα πρότυπα αυτά περιγράφονται στην ενότητα 3.3, ωστόσο ο τρόπος λειτουργίας τους σε υψηλό επίπεδο φαίνεται στην Εικόνα 3.7.



Εικόνα 3.7: Λειτουργία πρωτοκόλλων ISO/IEC 18013-5 και OpenID4VP

- Ενδέχεται ο πάροχος στοιχείων/βεβαιώσεων να έχει ενσωματωμένη κάποια πολιτική δημοσιοποίησης. Η πολιτική αυτή (αν υπάρχει) περιλαμβάνει κανόνες που περιγράφουν ποια είδη των βασιζόμενων μερών επιτρέπεται να λαμβάνουν ποια χαρακτηριστικά από τα δεδομένα ταυτοποίησης προσώπου ή τις βεβαιώσεις που ο πάροχος αυτός εκδίδει.

  Σε αυτή την περίπτωση, γίνεται αυτόματη αξιολόγηση της πολιτικής μέσω του πορτοφολιού και ο χρήστης ενημερώνεται για το σχετικό αποτέλεσμα με τη μορφή συμβουλής (πχ. «Ο πάροχος των στοιχείων δεν επιθυμεί να παρουσιάσετε τα χαρακτηριστικά Α, Β στο βασιζόμενο μέρος «όνομα». Θέλετε να συνεχίσετε;»). Κατόπιν, ο χρήστης μπορεί να επιλέξει αν θα να προχωρήσει ή όχι ακολουθώντας ή παρακάμπτοντας το αποτέλεσμα της αξιολόγησης.

- Ο χρήστης αποδέχεται ή απορρίπτει την παρουσίαση κάποιων ή όλων των στοιχείων/βεβαιώσεων βάσει του αποτελέσματος της αξιολόγησης που περιεγράφηκε παραπάνω. Η έγκριση του χρήστη[28] ζητείται σε κάθε περίπτωση και απαιτεί την επαλήθευση της ταυτότητας του χρήστη πριν ή κατά τη διάρκεια της διαδικασίας αυτής, που γίνεται με τις μεθόδους που έχουν οριστεί κατά την ενεργοποίηση του πορτοφολιού.

Μετά την παρουσίαση των στοιχείων/βεβαιώσεων για τα οποία ο χρήστης έδωσε έγκριση, το βασιζόμενο μέρος επαληθεύει την απάντηση του εγκατεστημένου πορτοφολιού και δημιουργούνται οι παρακάτω σχέσεις εμπιστοσύνης:

[28] Η έγκριση του χρήστη σε αυτό το πλαίσιο δεν πρέπει να συγχέεται με την νόμιμη βάση της συγκατάθεσης του ΓΚΠΔ για συλλογή και επεξεργασία προσωπικών δεδομένων.

- Το βασιζόμενο μέρος επιβεβαιώνει την ηλεκτρονική υπογραφή/σφραγίδα που συνοδεύει την βεβαίωση ή τα στοιχεία επιβεβαιώνοντας ότι έχουν προέλθει από αυθεντικό πάροχο και δεν έχουν μεταβληθεί. Για τον σκοπό αυτό αξιοποιούνται και πάλι οι άγκυρες εμπιστοσύνης.
- Το βασιζόμενο μέρος επιβεβαιώνει ότι τα στοιχεία ή βεβαιώσεις δεν έχουν αποσυρθεί ή ανασταλεί. Για το σκοπό αυτό, σε αυτά υπάρχουν σχετικές πληροφορίες που περιλαμβάνουν ένα σύνδεσμο με την τοποθεσία που το βασιζόμενο μέρος μπορεί να βρει τον κατάλογο με την κατάσταση των δεδομένων ή με τα αποσυρθέντα δεδομένα (status list / revocation list) και έναν δείκτη που δηλώνει τη θέση του εν λόγω στοιχείου/βεβαίωσης, ώστε να το εντοπίσει και να επιβεβαιώσει την κατάσταση του.
- Το βασιζόμενο μέρος επιβεβαιώνει ότι ο πάροχος στοιχείων ή βεβαιώσεων τα εξέδωσε για το εγκατεστημένο πορτοφόλι και όχι κάποιο άλλο. Η ιδιότητα αυτή ονομάζεται «σύνδεση συσκευής» (device binding) και εξασφαλίζει ότι τα στοιχεία/βεβαιώσεις δεν μπορούν να χρησιμοποιηθούν ανεξάρτητα από αυτή.

  Η σύνδεση γίνεται με την βοήθεια ενός δημοσίου κλειδιού που ο πάροχος υπογράφει και συμπεριλαμβάνει στα δεδομένα που εκδίδει. Το δημόσιο αυτό κλειδί ανήκει στο ζεύγος κλειδιών που έχουν παραχθεί από την κρυπτογραφική συσκευή ασφαλείας, όπου το ιδιωτικό κλειδί φυλάσσεται σε αυτή και το δημόσιο αποστέλλεται στον πάροχο των στοιχείων/βεβαιώσεων. Το βασιζόμενο μέρος κατά την επιβεβαίωση, ζητά από το πορτοφόλι να υπογράψει κάποια δεδομένα με το ιδιωτικό κλειδί. Η ακριβής διαδικασία επιβεβαίωσης εξαρτάται από τα πρότυπα που υποστηρίζονται (ISO/IEC 18013-5, SD-JWT VC, W3C VCDM που περιγράφονται στην ενότητα 3.3).
- Το βασιζόμενο μέρος επιβεβαιώνει ότι ο χρήστης που παρουσιάζει τα στοιχεία είναι αυτός για τα οποίον εκδόθηκαν, ώστε να μην είναι εφικτή η παράνομη χρήση τους. Η διαδικασία ονομάζεται «σύνδεση χρήστη» (user binding) και εξαρτάται από την μορφή της ροής επικοινωνίας και τα στοιχεία που έχουν εκδοθεί για το χρήστη. Για την επιβεβαίωση αυτή, το βασιζόμενο μέρος μπορεί να αξιοποιήσει την επαλήθευση ταυτότητας που εφαρμόζονται στο εγκατεστημένο πορτοφόλι και την κρυπτογραφική συσκευή ασφαλείας ή να ζητήσει επιπλέον χαρακτηριστικά. Για παράδειγμα αν στα στοιχεία περιλαμβάνεται φωτογραφία του χρήστη μπορεί να τη συγκρίνει με κάποια φωτογραφία που λαμβάνεται εκείνη τη στιγμή μέσω της κάμερας της συσκευής.
- Σε περίπτωση που το βασιζόμενο μέρος ζητήσει (στην ίδια αλληλεπίδραση) στοιχεία από διαφορετικές βεβαιώσεις, πρέπει να βεβαιωθεί ότι ανήκουν στον ίδιο χρήστη με τη βοήθεια των δημόσιων κρυπτογραφικών κλειδιών που περιλαμβάνονται σε αυτές και με χρήση του μηχανισμού συσχέτισης.
- Πριν ή μετά την επιβεβαίωση των στοιχείων ή βεβαιώσεων το βασιζόμενο μέρος επιβεβαιώνει την ταυτότητα του παρόχου του πορτοφολιού και του εγκατεστημένου πορτοφολιού παίρνοντας την βεβαίωση του πορτοφολιού, επιβεβαιώνοντας την υπογραφή της με τη βοήθεια της άγκυρας εμπιστοσύνης που έχει λάβει από τον κατάλογο εμπιστοσύνης του παρόχου του πορτοφολιού και επιβεβαιώνοντας ότι το πορτοφόλι έχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στην βεβαίωση. Το βασιζόμενο μέρος επίσης επιβεβαιώνει ότι ο πάροχος δεν έχει αποσύρει ή αναστείλει το εν λόγω εγκατεστημένο πορτοφόλι με τον ίδιο τρόπο που ακολουθούν και οι πάροχοι στοιχείων ή βεβαιώσεων.
- Τέλος, το πορτοφόλι επιτρέπει στον χρήστη να αναφέρει ύποπτες αιτήσεις για παρουσίαση προσωπικών στοιχείων, αλλά και να ζητήσει από το βασιζόμενο μέρος να διαγράψει προσωπικά στοιχεία που έχουν συλλεχθεί από το εν λόγω εγκατεστημένο πορτοφόλι.

Για το σκοπό αυτό διατηρείται ιστορικό που δεν μπορεί να τροποποιηθεί και περιλαμβάνει τουλάχιστον τα χαρακτηριστικά που ζητήθηκαν και παρουσιάστηκαν σε βασιζόμενα μέρη, η ακριβής ημερομηνία και ώρα των κινήσεων, τα ονόματα των βασιζόμενων μερών. Οι πληροφορίες παρουσιάζονται συγκεντρωτικά και αναλυτικά με τη μορφή ενός πίνακα εργαλείων (dashboard). Ακόμα, υπάρχουν οι κατάλληλες διεπαφές για την αναφορά των ύποπτων αιτήσεων και για τα αιτήματα διαγραφής.

[62]

Παρουσίαση/Επίδειξη στοιχείων ή βεβαιώσεων σε άλλο εγκατεστημένο πορτοφόλι

Όπως ένα βασιζόμενο μέρος μπορεί να ζητήσει την επίδειξη στοιχείων από ένα εγκατεστημένο πορτοφόλι, το ίδιο μπορεί να κάνει και ένα άλλο πορτοφόλι. Οι απαραίτητες προϋποθέσεις για να μπορούν να αλληλεπιδράσουν δύο πορτοφόλια που βρίσκονται φυσικά κοντά (με ή χωρίς σύνδεση στο διαδίκτυο) είναι:

- Να υποστηρίζουν διεπαφές και πρωτόκολλα ώστε να μπορούν εγκαθιδρύουν σύνδεση με άλλα πορτοφόλια, να λαμβάνουν και να επαληθεύουν αιτήματα για επίδειξη στοιχείων ή βεβαιώσεων από άλλα πορτοφόλια και να απαντούν σε αυτά βάσει των προδιαγραφών που ορίζουν τα πρότυπα OpenID4VP & ISO/IEC 18013-5
- Ο ορισμός από την Επιτροπή των τεχνικών προδιαγραφών για την ανταλλαγή στοιχείων ταυτότητας και βεβαιώσεων βάσει των δύο ανωτέρων προτύπων
- Το πορτοφόλι που αιτείται την επίδειξη στοιχείων πρέπει να επαληθεύει την ταυτότητα του χρήστη πριν προχωρήσει σε αυτή την ενέργεια
- Το πορτοφόλι που λαμβάνει το αίτημα για επίδειξη στοιχείων ή βεβαιώσεων πρέπει να ενημερώνει το χρήστη για τα ακριβή χαρακτηριστικά που ζητούνται, για το αποτέλεσμα ελέγχων επικύρωσης του ίδιου του αιτήματος αλλά και του αιτούντος, ενώ ζητά την έγκριση του χρήστη πριν ικανοποιήσει το αίτημα.
- Το πορτοφόλι που αιτείται την επίδειξη στοιχείων πρέπει να έχει ορίσει εκ των προτέρων μία λίστα με τα χαρακτηριστικά που μπορεί να ζητήσει από άλλο πορτοφόλι
- Το πορτοφόλι που λαμβάνει το αίτημα για επίδειξη στοιχείων ή βεβαιώσεων πρέπει να επαληθεύει την ταυτότητα του αιτούντος και να επικυρώνει το αίτημα, ώστε να επιβεβαιώνεται η εγκυρότητα του πορτοφολιού και του αιτήματος.
- Το πορτοφόλι που αιτείται την επίδειξη στοιχείων πρέπει να παρουσιάζει τις ληφθείσες πληροφορίες στον χρήστη από τον οποίο τις ζήτησε.

Διαχείριση στοιχείων ή βεβαιώσεων

Μετά την έκδοση στοιχείων/βεβαιώσεων η διαχείρισή τους γίνεται από τον χρήστη και τον πάροχο του πορτοφολιού μέχρι την διαγραφή τους ή την απεγκατάσταση της εφαρμογής από τον χρήστη. Ακόμα, ο χρήστης μπορεί να ζητήσει την απόσυρση των στοιχείων/βεβαιώσεων σε περίπτωση κλοπής ή απώλειας της συσκευής του. [62]

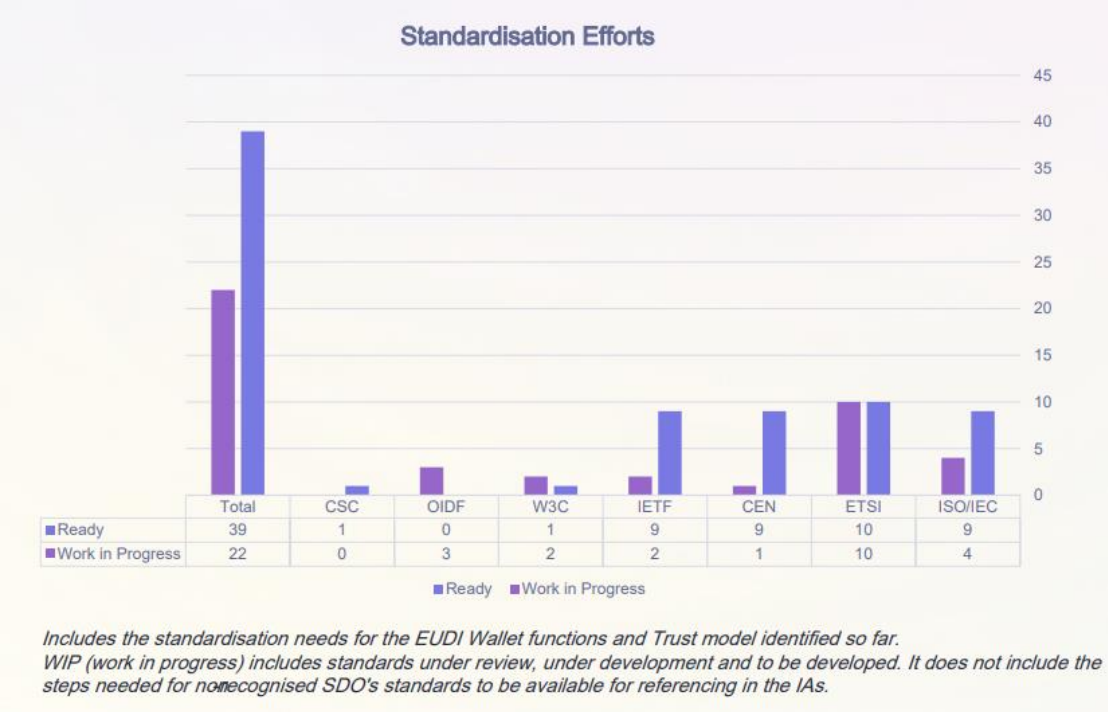
Διαγραφή στοιχείων ή βεβαιώσεων

Όταν ο χρήστης δεν επιθυμεί τη διατήρηση κάποιων στοιχείων/βεβαιώσεων στο εγκατεστημένο πορτοφόλι του, μπορεί να τα διαγράψει. Σε περίπτωση που έχουν εκδοθεί περισσότερες βεβαιώσεις με το ίδιο περιεχόμενο που είναι σε ισχύ, διαγράφονται όλες. Η διαγραφή συνεπάγεται την καταστροφή του σχετικού κρυπτογραφικού υλικού από την κρυπτογραφική συσκευή ασφαλείας, η οποία γίνεται μετά την επαλήθευση της ταυτότητας του χρήστη. [62]

3.3 Περιγραφή αναγκαίων προτύπων για την ανάπτυξη ψηφιακών πορτοφολιών

Για την αποτελεσματική υλοποίηση των ψηφιακών πορτοφολιών είναι αναγκαία η χρήση κοινών προτύπων και προδιαγραφών. Μέσω της προσπάθειας για μία ενιαία προσέγγιση, αναμένονται οφέλη όπως η διαλειτουργικότητα, η απρόσκοπτη ενσωμάτωση, η ασφάλεια, η συμμόρφωση με τους κανονισμούς, η μείωση κόστους ανάπτυξης των πορτοφολιών αλλά και ο δικαιότερος ανταγωνισμός μεταξύ των παρόχων. [63]

Υπάρχουν αρκετοί οργανισμοί ανάπτυξης προτύπων (Standards Development Organizations - SDO), κάποιοι εκ των οποίων είναι διεθνώς αναγνωρισμένοι, όπως ο ISO/IEC[29], ο ETSI[30] και ο CEN/CENELEC[31] και αρκετοί μη αναγνωρισμένοι όπως οι: W3C[32], IETF[33], OIDF[34] και CSC[35]. Σε μία έρευνα σχετικά με τις προσπάθειες προτυποποίησης τεχνικών προδιαγραφών σχετικών με την ανάπτυξη του ψηφιακού πορτοφολιού, καταγράφηκαν τα έργα των ανωτέρω οργανισμών όπως παρουσιάζονται στην Εικόνα 3.8: [63]



Εικόνα 3.8: Προσπάθειες προτυποποίησης για το ψηφιακό πορτοφόλι

Για λόγους πληρότητας, παρακάτω παρουσιάζονται συνοπτικά τα πρότυπα που προτείνονται από το ARF.

[29] International Organization for Standardisation / International Electrotechnical Commission
[30] European Telecommunications Standards Institute
[31] European Committee for Standardization/ European Committee for Electrotechnical Standardization
[32] World Wide Web Consortium
[33] Internet Engineering Task Force
[34] OpenID Foundation
[35] Cloud Signature Consortium

OpenID for Verifiable Credential

Το ίδρυμα OpenID είναι ένας μη κερδοσκοπικός οργανισμός που αναπτύσσει ανοιχτές προδιαγραφές (open specifications). Η ομάδα εργασίας του αναπτύσσει την οικογένεια προδιαγραφών με τίτλο «OpenID for Verifiable Credentials», που περιλαμβάνει προδιαγραφές για:

- Την έκδοση επαληθεύσιμων στοιχείων ταυτοποίησης (OpenID for Verifiable Credential Issuance - OID4VCI)
- Την παρουσίαση στοιχείων ταυτοποίησης με τρόπο επαληθεύσιμο (OpenID for Verifiable Presentations - OID4VP)
- Τη χρήση παρόχων OpenID που οι ίδιοι οι χρήστες ελέγχουν (Self-Issued OpenID Provider v2 – SIOPv2) για την επαλήθευση ταυτότητας και την παρουσίαση στοιχείων σε άλλους παρόχους

Οι προδιαγραφές αυτές βασίζονται στο πρωτόκολλο OpenID Connect. Η λογική του πρωτοκόλλου είναι ότι τα στοιχεία ταυτότητας ζητούνται και παρέχονται από το χρήστη με βάση την αρχή της ελαχιστοποίησης των δεδομένων, ενώ παρέχει τη δυνατότητα στον πάροχο ταυτότητας να επικοινωνεί απευθείας με τον τελικό χρήστη και να παίρνει την άδειά του προτού να δώσει τα στοιχεία στον ελεγκτή. Ο πάροχος παρουσιάζει στον χρήστη τα στοιχεία αλλά και τον αποδέκτη τους (τον ελεγκτή) ώστε ο χρήστης να μπορεί να αποφασίσει αν θα τα κοινοποιήσει ή όχι.

Με τον όρο «επαληθεύσιμα στοιχεία ταυτότητας» εννοούνται τα στοιχεία αυτά στα οποία κάποια παραποίηση είναι εμφανής (tamper-evident), έχουν πατρότητα και μπορούν να επαληθευτούν με κρυπτογραφικούς μηχανισμούς.

[64] [65] [66] [67] [68]

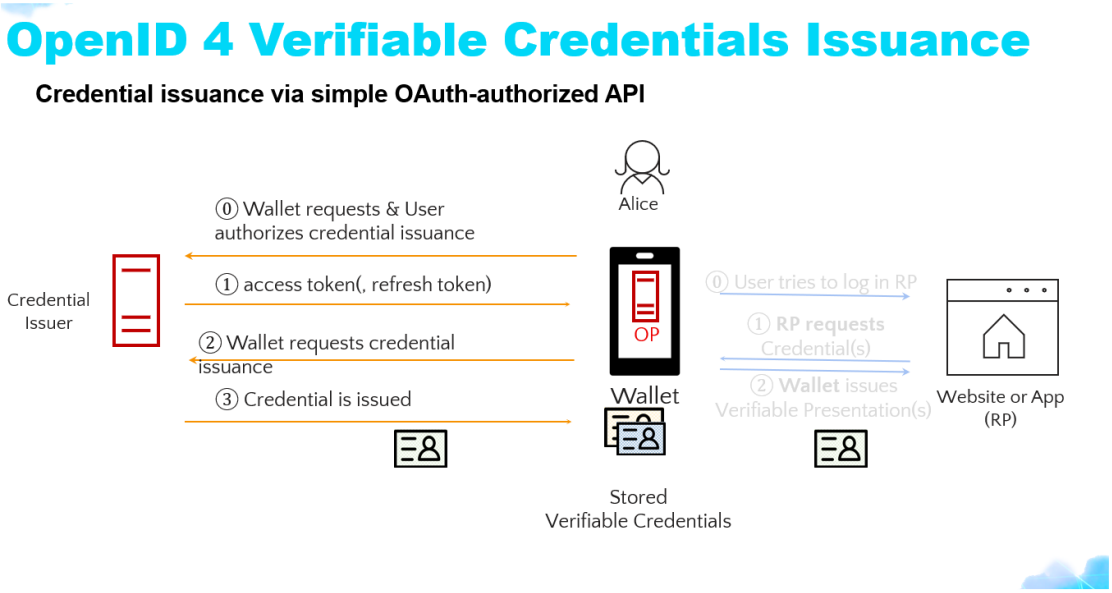
OpenID for Verifiable Credential Issuance (OpenID4VCI)

Το OpenID4VCI ορίζει μία διεπαφή (API[36]) και τους μηχανισμούς εξουσιοδότησης που βασίζονται στο πρωτόκολλο OpenID Connect για την έκδοση επαληθεύσιμων στοιχείων ταυτοποίησης. Σε σχέση με το ψηφιακό πορτοφόλι, όπως φαίνεται από την Εικόνα 3.2 χρησιμοποιείται κατά την έκδοση δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων χαρακτηριστικών με τα εμπλεκόμενα μέρη να είναι το εγκατεστημένο πορτοφόλι και ο πάροχος των στοιχείων/βεβαιώσεων. [62]

Όπως φαίνεται από την Εικόνα 3.9, η διαδικασία ξεκινά το με το πορτοφόλι να στέλνει ένα αίτημα εξουσιοδότησης στον εκδότη διαπιστευτηρίων, εκείνος επαληθεύει ή/και αναγνωρίζει το χρήστη και ενδεχομένως ζητά και συγκατάθεση για την έκδοση ενός ή περισσότερων διαπιστευτηρίων. Μετά την επιτυχή ολοκλήρωση του αιτήματος εξουσιοδότησης, εκδίδεται ένας κωδικός εξουσιοδότησης για το πορτοφόλι, το οποίο εξαργυρώνει για να λάβει ένα “token”. Υπάρχει περίπτωση, ο εκδότης διαπιστευτηρίων να εκδώσει ένα token ανανέωσης, ώστε π.χ. να επιτρέπεται κατ' απαίτηση έκδοση ή ανανέωση διαπιστευτηρίων χωρίς περαιτέρω αλληλεπιδράσεις με τον χρήστη.

[68]

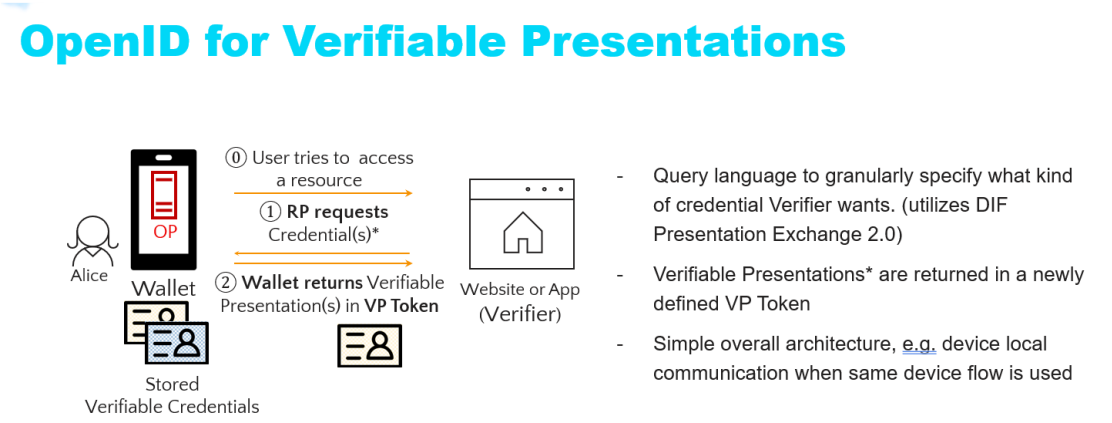
[36] Application Programming Interface: Διεπαφή προγραμματισμού εφαρμογών που επιτρέπει σε 2 ή περισσότερα προγράμματα να επικοινωνούν μεταξύ τους.



Εικόνα 3.9: Λειτουργία πρωτοκόλλου OpenID4VCI

OpenID for Verifiable Presentations (OpenID4VP)

Το OpenID4VP ορίζει ένα μηχανισμό που βασίζεται στο πλαίσιο OAuth 2.0 που επιτρέπει την παρουσίαση πληροφοριών με τη μορφή επαληθεύσιμων στοιχείων ταυτότητας ως μέρος της ροής του πρωτοκόλλου. Σε σχέση με το ψηφιακό πορτοφόλι, όπως φαίνεται από την Εικόνα 3.2 χρησιμοποιείται κατά την επίδειξη δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων χαρακτηριστικών, όταν τα εμπλεκόμενα μέρη, δηλαδή το εγκατεστημένο πορτοφόλι και το βασιζόμενο μέρος που ζητά τις πληροφορίες, είναι μεταξύ τους φυσικά απομακρυσμένα (remote presentation flow). [62]



Εικόνα 3.10: Λειτουργία πρωτοκόλλου OpenID4VP

Σε αυτήν τη ροή, ο χρήστης θέλει να αποκτήσει πρόσβαση σε μία υπηρεσία και ο πάροχος ζητά την παρουσίαση ενός επαληθεύσιμου διαπιστευτηρίου πάνω από ένα αίτημα Self-Issued OP. Ο πάροχος αυτός (που είναι επίσης πορτοφόλι σε αυτήν την περίπτωση), αλληλεπιδρά με τον κάτοχο για να επιλέξει το διαπιστευτήριο που θα παρουσιαστεί και δημιουργεί μια επαληθεύσιμη παρουσίαση που αποστέλλεται πίσω στον ελεγκτή με τη μορφή ενός token (VP token) μαζί με το ID token. Ο ελεγκτής επαληθεύει την ακεραιότητα και τη γνησιότητα των διαπιστευτηρίων, καθώς και την συσχέτισή τους με τον κάτοχό τους (holder binding) πριν τα επεξεργαστεί.

[64] [65] [66] [67] [68]

ISO/IEC 18013-5

Στο πρότυπο αυτό περιγράφεται η διεπαφή και προδιαγραφές που απαιτούνται για λειτουργικότητες (συμβατές με το εν λόγω πρότυπο) μίας άδειας οδήγησης σε μία κινητή συσκευή. Οι προδιαγραφές αυτές στοχεύουν στο να επιτρέπουν σε ελεγκτές (verifier) που δεν σχετίζονται με την εκδοτική αρχή να αποκτούν πρόσβαση και να επαληθεύουν τα στοιχεία που εκείνη έχει εκδώσει, ενώ παράλληλα ο κάτοχος της άδειας οδήγησης μπορεί να κοινοποιεί επιλεκτικά πληροφορίες στους ελεγκτές. Ακόμα, δίνουν τη δυνατότητα συχνής ανανέωσης των πληροφοριών και της επαλήθευσής τους με υψηλό επίπεδο εμπιστοσύνης. Στο πρότυπο ορίζονται η δομή των χαρακτηριστικών, η μορφή των δεδομένων καθώς και οι μηχανισμοί επαλήθευσης που μπορούν να χρησιμοποιηθούν και με άλλες μορφές δεδομένων.

Σε σχέση με το ψηφιακό πορτοφόλι, όπως φαίνεται από την Εικόνα 3.2 χρησιμοποιείται κατά την επίδειξη δεδομένων ταυτοποίησης προσώπου ή βεβαιώσεων χαρακτηριστικών όταν τα εμπλεκόμενα μέρη, δηλαδή το εγκατεστημένο πορτοφόλι και το βασιζόμενο μέρος που ζητά τις πληροφορίες, είναι μεταξύ τους φυσικά κοντά (proximity presentation flow). Επίσης είναι ένα από τα διαθέσιμα πρότυπα που μπορεί να χρησιμοποιηθεί για τον καθορισμό της μορφής μίας βεβαίωσης χαρακτηριστικών κατά την έκδοσή της μαζί με τις προδιαγραφές SD-JWT VC και VCDM v1.1/v2.0. [62] [69]

W3C Verifiable Credentials Data Model (W3C VCDM)

Η ομάδα εργασίας «Verifiable Credentials» του διεθνούς οργανισμού W3C έχει εκδώσει προδιαγραφές που αφορούν το μοντέλο δεδομένων για τα επαληθεύσιμα στοιχεία ταυτότητας. Στην πρώτη έκδοση VCDM v1.1, ορίζεται ένα σχήμα χαρακτηριστικών που δε λαμβάνει υπόψη το μορφότυπο των δεδομένων και τους μηχανισμούς επαλήθευσης, ενώ στη δεύτερη VCDM v2.0 εισάγονται προδιαγραφές για το μορφότυπο και προτάσεις για τους μηχανισμούς επαλήθευσης. Σχετικά με το ψηφιακό πορτοφόλι, είναι ένα από τα διαθέσιμα πρότυπα που μπορεί να χρησιμοποιηθεί για τον καθορισμό της μορφής μίας βεβαίωσης χαρακτηριστικών κατά την έκδοσή της μαζί με τις προδιαγραφές SD-JWT VC και ISO/IEC 18013-5. [62] [70] [71]

SD-JWT-based Verifiable Credentials (SD-JWT VC)

Η ομάδα εργασίας «Web Authorization Protocol» του διεθνούς οργανισμού IETF ανάπτυξης προτύπων έχει εκδώσει προδιαγραφές που αφορούν το μοντέλο δεδομένων και μηχανισμούς επεξεργασίας και επαλήθευσης για τα επαληθεύσιμα στοιχεία ταυτότητας. Σχετικά με το ψηφιακό πορτοφόλι, είναι ένα από τα διαθέσιμα πρότυπα που μπορεί να χρησιμοποιηθεί για τον καθορισμό της μορφής μίας βεβαίωσης χαρακτηριστικών κατά την έκδοσή της μαζί με τις προδιαγραφές VCDM v1.1/v2.0 και ISO/IEC 18013-5. [62] [72]

4. ΑΝΟΙΧΤΑ ΘΕΜΑΤΑ & ΣΥΜΠΕΡΑΣΜΑΤΑ

4.1 Κενά, ελλείψεις και προβληματισμοί σχετικά με το ψηφιακό πορτοφόλι

Εισαγωγή

Το οικοσύστημα του ψηφιακού πορτοφολιού αναμένεται να είναι μία ιδιαίτερα σύνθετη δομή η οποία θα απαιτεί την απρόσκοπτη λειτουργία και συνεργασία μεταξύ πολλών διαφορετικών οντοτήτων, λύσεων, συσκευών, τεχνολογιών, διαδικασιών και προτύπων. Η ανάπτυξη του οικοσυστήματος αυτού, με επίκεντρο το πρωτότυπο ψηφιακό πορτοφόλι είναι σε εξέλιξη και όσο προχωρά εντοπίζονται κενά, δυσκολίες και ελλείψεις. Στην ενότητα αυτή γίνεται μία προσπάθεια καταγραφής των διαφόρων προβληματισμών και ανοιχτών ζητημάτων που έχουν εντοπιστεί ως τώρα από τους ειδικούς και έχουν παρουσιαστεί είτε στο πλαίσιο ανατροφοδότησης, είτε στο πλαίσιο συνεδρίων και εργαστηρίων είτε και ανεξάρτητα από αυτά.

Ανοιχτά θέματα σχετικά με τα διαθέσιμα πρότυπα και τεχνικές προδιαγραφές

Η αναγκαιότητα για κοινά πρότυπα και προδιαγραφές που θα ακολουθούνται κατά την υλοποίηση του ψηφιακού πορτοφολιού έχει παρουσιαστεί αναλυτικά παραπάνω. Ωστόσο, ακόμα[37] υπάρχουν αρκετές ελλείψεις που πρέπει να αντιμετωπιστούν, και συγκεκριμένα:

- Πολλά πρότυπα ή τεχνικές προδιαγραφές είναι ακόμα σε μορφή προσχεδίου (draft) και πρέπει να ολοκληρωθεί η συγγραφή τους, να εγκριθούν και να δημοσιοποιηθούν. Σε αυτά περιλαμβάνονται:
    - [προσχέδιο] OpenID4VP
    - [προσχέδιο] OpenID4VCI
    - [προσχέδιο] HAIP (OpenID4VC High Assurance Interoperability Profile with SD-JWT VC)
    - [υπό έκδοση] ISO/IEC 18013-7 (Personal identification - ISO-compliant driving license, part 7: Mobile driving license add-on functions)
    - [υπό αξιολόγηση] ISO/IEC 23220-4 (Cards and security devices for personal identification — Building blocks for identity management via mobile devices, Part 4: Protocols and services for operational phase)
- Αναμένονται ακόμα προσθήκες σε υπάρχοντα πρότυπα για την κάλυψη συγκεκριμένων προδιαγραφών του πορτοφολιού:
    - ETSI TS 119 432 (Electronic Signatures and Infrastructures, Protocols for remote digital signature creation)
    - ISO/IEC 18013-5 (Το κομμάτι του καταλόγου κατάστασης για τη διαχείριση της ανάκλησης)
    - Cloud Signature Consortium (Το κομμάτι της εφαρμογής απομακρυσμένων υπογραφών)
- Επιπροσθέτως, δεν υπάρχουν πρότυπα ή τεχνικές προδιαγραφές για την κάλυψη συγκεκριμένων προδιαγραφών του πορτοφολιού:
    - Κοινοί μορφότυποι για τις πληροφορίες στο μητρώο βασιζόμενων μερών
    - Πολιτική κοινής πρόσβασης πιστοποιητικών Αρχών έκδοσης
    - Κοινές πληροφορίες βασιζόμενων μερών που θα πρέπει να δηλώνονται κατά την εγγραφή τους
    - Προδιαγραφές για την εφαρμογή της απόδειξης συσχέτισης (Proof of Association)

[37] Μέχρι τη στιγμή συγγραφής της παρούσας εργασίας

- Προδιαγραφές για το ενωσιακό σήμα εμπιστοσύνης του ψηφιακού πορτοφολιού (EUDI Trust Mark)
- Προδιαγραφές για την κοινή διεπαφή υποβολής παραπόνων στις Αρχές Προστασίας Δεδομένων
- Προδιαγραφές για την κοινή διεπαφή υποβολής αιτήσεων διαγραφής δεδομένων σε βασιζόμενα μέρη
- Προδιαγραφές για την βεβαίωση των εγκατεστημένων πορτοφολιών
- Προδιαγραφές για μηχανισμούς σχετικά με τις ενσωματωμένες πολιτικές δημοσιοποίησης

- Υπάρχουν τέλος σημαντικά έγγραφα τεκμηρίωσης που είναι σε εξέλιξη και πρέπει να ολοκληρωθούν:
  - Το πλαίσιο αναφοράς και αρχιτεκτονικής (ARF)
  - Το εγχειρίδιο για τα δεδομένα ταυτοποίησης προσώπου των φυσικών προσώπων (Natural person PID Rulebook)
  - Το εγχειρίδιο για τα δεδομένα ταυτοποίησης προσώπου των νομικών προσώπων (Legal-person PID Rulebook)
  - Το εγχειρίδιο για τα ψευδώνυμα (Pseudonym Rulebook)

[73]

Ελλείψεις και σημεία προσοχής που έχουν εντοπιστεί από τα πιλοτικά έργα μεγάλης κλίμακας

Στα πλαίσια του εργαστηρίου που διοργανώθηκε το Σεπτέβριο του 2024 από τους ευρωπαϊκούς οργανισμούς προτυποποίησης CEN και ETSI, παρουσιάστηκαν σημεία προσοχής αλλά και κενά που έχουν μέχρι τώρα εντοπιστεί από τα πιλοτικά έργα μεγάλης κλίμακας. [74] [75] [76] [77]

- Η σύμπραξη DC4EU έδωσε έμφαση στην ανάγκες σε επίπεδο προτυποποίησης που περιλαμβάνουν:
    - Την εναρμόνιση με την κατεύθυνση των τεχνικών προδιαγραφών VCDM 2.0
    - Την προτυποποίηση μεθόδων αποκεντρωμένων αναγνωριστικών (Decentralized Identifiers) με υποστήριξη για πιστοποιητικά της μορφής X509v3
    - Το μοντέλο δεδομένων των καταλόγων εμπιστοσύνης και την εφαρμογή του με τη βοήθεια αποθετηρίων που βασίζονται σε κατανεμημένα καθολικά (distributed ledgers registry)
    - Τη χρήση του OIDC federation ως ενδιάμεσο επίπεδο διαλειτουργικότητας για την ανάκτηση πληροφοριών σχετικά με τις άγκυρες εμπιστοσύνης
    - Την περαιτέρω ανάπτυξη των τεχνικών προδιαγραφών OpenID4VCI και OpenID4VP για καλύτερη διαλειτουργικότητα
    - Την ευθυγράμμιση με την 2^{η} έκδοση των προδιαγραφών του CSC καθώς και την αυτοματοποίση της δημιουργίας εγκεκτιμένων ηλεκτρονικών υπογραφών και σφραγίδων για ηλεκτρονικές βεβαιώσεις χαρακτηριστικών
- Από την σύμπραξη του EWC παρουσιάστηκαν τρία βασικά σημεία προβληματισμού:
    - Η δυσκολία επίτευξης διαλειτουργικότητας μεταξύ διαφορετικών λύσεων πορτοφολιού, μορφότυπων και πρωτοκόλλων που εντείνεται λόγω των πολλών παράλληλων προσπαθειών από διαφορετικές ομάδες και οργανισμούς προς αυτή την κατεύθυνση αλλά και λόγω της πολύ μεγάλης λεπτομέρειας που χρήζει προσοχής. Παράλληλα, η λειτουργία, διαχείριση, εμπιστοσύνη αλλά και οικονομική προσέγγιση στο ευρύτερο οικοσύστημα του eIDAS αποτελεί μεγαλεπήβολο έργο.
    - Η ανάπτυξη του πλαισίου εμπιστοσύνης και των καταλόγων εμπιστοσύνης στο πλαίσιο των βεβαιώσεων χαρακτηριστικών
    - Στα πλαίσια των δοκιμών, η υλοποίηση διατομεακών πιλοτικών έργων και η δημιουργία επαναχρησιμοποιούμενων δομών (building blocks)
- Στην παρουσίαση του NOBID δόθηκε έμφαση στην ανάγκη ενεργού ρόλου από τη συμβουλευτική επιτροπή που αποτελείται από Αρχές πληρωμών για την συμμόρφωση με κανόνες, βέλτιστες πρακτικές και μελλοντική στρατηγική στο πλαίσιο των πληρωμών ώστε να διευκολύνεται η λήψη των αποφάσεων.
- Από την τέταρτη σύμπραξη (POTENTIAL) παρουσιάστηκε η ανατροφοδότηση που συγκέντρωσαν σχετικά με την έκδοση 1.3 του ARF και το βαθμό στον οποίο αντιμετωπίστηκαν ζητήματα προηγούμενων εκδόσεων. Από τα κομμάτια που εντοπίστηκε ότι καλύφθηκαν μερικώς, οι περισσότεροι συμμετέχοντες στην έρευνα αναγνώρισαν το μοντέλο και τους καταλόγους εμπιστοσύνης, την σταθερότητα των πρωτοκόλλων και προτύπων που προτείνονται και την ασφάλεια ως τα τρία ζητήματα που πρέπει να αποτελέσουν προτεραιότητα σε επόμενες εκδόσεις.

Ακόμα παρουσιάστηκε η ανατροφοδότηση σχετικά με τους επερχόμενους εκτελεστικούς κανονισμούς όπου εντοπίστηκαν μεταξύ άλλων ανάγκες όπως:

- Η διαχείριση της περίπτωσης μη αδιαμφισβήτητης αντιστοίχισης ταυτότητας (identity matching)
- Η περαιτέρω εμβάθυνση στον ορισμό, δημιουργία και χρήση ψευδωνύμων
- Ο σαφής ορισμός του μοντέλου εμπιστοσύνης
- Η περιγραφή του τρόπου εγγραφής των βασιζόμενων μερών
- Η διαδικασία διασυνοριακής έκδοσης στοιχείων ταυτότητας καθώς και της περίπτωσης διπλής ιθαγένειας

Σχετικά με την πιστοποίηση των ψηφιακών πορτοφολιών, παρουσιάστηκαν οι ενδεχόμενες προκλήσεις όπως:

- Οι αβεβαιότητες στον χρονικό προγραμματισμό
- Οι εξαρτήσεις και πιθανές αντιφάσεις με τον κανονισμό eIDAS 2.0 αλλά και άλλους κανονισμούς ή νομοθετικές πράξεις
- Οι πιθανές επιπλοκές στον κύκλο ζωής των πορτοφολιών και σε υπάρχοντα πρότυπα

Τέλος, ένα σημαντικό πρόβλημα που έχει εντοπιστεί από τα πιλοτικά έργα αφορά την μονοσήμαντη (αδιαμφισβήτητη) ταυτοποίηση ενός προσώπου σε όλα τα κράτη μέλη με τη χρήση των δεδομένων ταυτοποίησης προσώπου. Τα υποχρεωτικά στοιχεία (όνομα, επώνυμο, ημερομηνία γέννησης, ενήλικος/ανήλικος, χώρα έκδοσης, ημερομηνία έκδοσης, ημερομηνία λήξης, εκδοτική αρχή) δεν επαρκούν για την μοναδική ταυτοποίηση του προσώπου, για την πρόσβαση σε κάποια δημόσια ή άλλη υπηρεσία. Η λύση της έκδοσης επιπλέον εγκεκριμένης βεβαίωσης χαρακτηριστικών για την επίτευξη της μοναδικότητας, επιβαρύνει τα πορτοφόλια με επιπλέον στοιχεία για κάθε υπηρεσία, ενώ παράλληλα δεν επιτυγχάνεται και ο στόχος των υποχρεωτικών δεδομένων ταυτοποίησης προσώπου που πρέπει να είναι μοναδικά για κάθε πρόσωπο. [78]

Κενά στο μοντέλο εμπιστοσύνης

Όπως είναι ήδη σαφές, το πλαίσιο εμπιστοσύνης αποτελεί ένα από τα σημαντικότερα σημεία προσοχής. Ειδικά οι κατάλογοι εμπιστοσύνης είναι καίριοι στη διαδικασία επαλήθευσης της αυθεντικότητας των εκδοτών διαπιστευτηρίων, ψηφιακών πορτοφολιών αλλά και των βασιζόμενων μερών. Η διαδικασία διαχείρισης πολλαπλών λιστών είναι από μόνη της σύνθετη, ειδικά λαμβάνοντας υπόψη την ανάγκη για αδιάλειπτη διαθεσιμότητα, διατηρώντας παράλληλα την ασφάλεια και την ακεραιότητα των παρεχόμενων πληροφοριών. Έχει σημασία το γεγονός ότι το οικοσύστημα του eIDAS είναι ιδιαίτερα ποικιλόμορφο, με διαφορετικές λίστες να υπόκεινται σε διαφορετικές νομοθεσίες από τα κράτη μέλη, να καλύπτουν διαφορετικές περιπτώσεις χρήσης, ενώ παράλληλα δεν υπάρχει ακόμα μία κοινή συμφωνημένη δομή. Ελλείψει μίας κοινής προσέγγισης υπάρχει ο κίνδυνος δημιουργίας δομών που δεν έχουν κάποια συνέπεια, οδηγώντας σε προβλήματα διαλειτουργικότητας.

Η προσέγγιση των καταλόγων εμπιστοσύνης από το eIDAS 1.0, ενώ αποτελεί μία καλή αρχή έχει ως μειονεκτήματα την χειροκίνητη διαχείριση των αγκυρών εμπιστοσύνης, την δυσκολία επεκτασιμότητας ως προς τους καταλόγους των υπηρεσιών εμπιστοσύνης και την αδυναμία υποστήριξης βεβαιώσεων χαρακτηριστικών αυθεντικών πηγών δημοσίων φορέων. Ακόμα, αξίζει να αναφερθεί ότι μέχρι στιγμής η διαχείριση των αγκυρών εμπιστοσύνης μη κυβερνητικών οργανισμών δεν καλύπτεται από το eIDAS 2.0 με αποτέλεσμα να υπάρχει ανάγκη αξιοποίησης υπαρχόντων μη κυβερνητικών μοντέλων εμπιστοσύνης με τη δυνατότητα παράλληλης χρήσης ηλεκτρονικής ταυτότητας με υψηλό επίπεδο διασφάλισης αλλά και βεβαιώσεις του δημοσίου τομέα. Χωρίς την απαιτούμενη έμφαση και παράλληλα εναρμόνιση με μοντέλα κατάλληλα για τον ιδιωτικό τομέα, υπάρχει μεγάλος κίνδυνος για μειωμένη υιοθέτηση των ψηφιακών πορτοφολιών (πέρα από τις απαιτούμενες περιπτώσεις).

[79] [80] [81]

Κενά στην πιστοποίηση των πορτοφολιών

Όπως έχει παρουσιαστεί και νωρίτερα οι λύσεις των ψηφιακών πορτοφολιών πρέπει να πιστοποιούνται από οργανισμούς αξιολόγησης συμμόρφωσης που θα ορίζονται από τα κράτη μέλη. Ο κανονισμός ορίζει την απαίτηση για δημοσίευση εκτελεστικών κανονισμών που θα περιλαμβάνουν πρότυπα, προδιαγραφές και διαδικασίες για την υλοποίηση της πιστοποίησης. Στα πλαίσια αυτά, έχει ζητηθεί από τον ENISA να αναπτύξει ένα ευρωπαϊκό σχήμα, διαδικασία που θα ξεκινήσει το 2025, ωστόσο αυτό δεν θα καλύπτει το λειτουργικό κομμάτι της πιστοποίησης ενώ παράλληλα θα δημοσιευθεί μετά την πρώτη γενιά πορτοφολιών, για αυτό και είναι επιτακτική η δημοσιοποίηση των εθνικών σχημάτων.

Ένα σημαντικό θέμα είναι ότι σύντομα θα πρέπει να ολοκληρωθούν οι εκτελεστικές πράξεις, ενώ υπάρχουν πολλά κενά και σημεία προβληματισμού καθώς ο σκοπός της πιστοποίησης είναι ασυνήθιστος και ευρύς, οι απαιτήσεις που πρέπει να περιλαμβάνονται δεν είναι καλώς καθορισμένες και τα απαιτούμενα πρότυπα αναφοράς δεν είναι ακόμα έτοιμα.

Στο επίπεδο ανάπτυξης του ευρωπαϊκού σχήματος, θα αντιμετωπιστούν προκλήσεις με το ίδιο το σχήμα να αναμένεται ιδιαίτερα σύνθετο καθώς θα πρέπει περιλαμβάνει πιστοποιήσεις για προϊόντα και διαδικασίες ενώ θα λαμβάνει υπόψη και ζητήματα κυβερνοασφάλειας. Θα πρέπει να λαμβάνει υπόψη πολλαπλές αρχιτεκτονικές λύσεων πορτοφολιού σε επίπεδο υλισμικού, όπου πολλές ενδέχεται να μην είναι ευρέως διαθέσιμες ή να μην προσφέρουν καλή εμπειρία χρήστη. Τέλος, υπάρχει πολύ μεγάλη πίεση στον ρυθμό ανάπτυξης με τα σχήματα πιστοποίησης να πρέπει να είναι έτοιμα σε περίπου ένα χρόνο από τώρα ενώ παράλληλα όλες οι τεχνολογίες δεν είναι ακόμα έτοιμες.

4.2 Αξιολόγηση του ARF σχετικά με την ασφάλεια και την ιδιωτικότητα

Ανάλυση ως προς τα προσωπικά δεδομένα από τον οργανισμό epicenter.works

Η πιο πρόσφατη έκδοση του ARF έχει προκαλέσει προβληματισμούς καθώς ο τρόπος υλοποίησης που προτείνει σε αρκετά σημεία είτε έρχεται σε αντιδιαστολή με τον κανονισμό, είτε αγνοεί σημαντικά στοιχεία του, είτε δημιουργεί νέες απαιτήσεις που δεν υπάρχουν, είτε προσεγγίζει τις ήδη υπάρχουσες με απλοϊκό τρόπο με αποτέλεσμα να δημιουργούνται νέοι κίνδυνοι. Σε μία ανάλυση του πλαισίου που πραγματοποιήθηκε από τον οργανισμό epicenter.works[38] με έμφαση στα προσωπικά δεδομένα εντοπίστηκαν σημαντικά σημεία προς βελτίωση. [82]

1. Ο κανονισμός ορίζει σαφώς ότι οι χρήστες θα πρέπει λαμβάνουν αιτήματα μόνο για συγκεκριμένες περιπτώσεις χρήσης των στοιχείων τους που θα πρέπει να ορίζονται εκ των προτέρων σε κάποιο δημόσιο μητρώο. Μάλιστα κατά τη διαδικασία εγγραφής των βασιζόμενων μερών θα πρέπει να παρέχονται (εκτός από το όνομα, τη χώρα λειτουργίας και τις περιπτώσεις χρήσης του πορτοφολιού) οι ακριβείς πληροφορίες που μπορεί να ζητήσουν από τους χρήστες. Ωστόσο, στο πλαίσιο δεν υπάρχουν καθόλου τεχνικές λεπτομέρειες για την μορφή που πρέπει να έχουν τα δεδομένα που τα βασιζόμενα μέρη θα ζητούν από τους χρήστες. Επίσης δεν παρουσιάζονται τα τεχνικά μέτρα που θα εμποδίζουν τα βασιζόμενα μέρη από το να ζητούν εξ' αρχής στοιχεία που δεν δικαιούνται, καθιστώντας τα αιτήματα «άκυρα» με κάποιο αυτοματοποιημένο τρόπο. Ως αποτέλεσμα, ο χρήστης είναι δυνητικά εκτεθειμένος σε υπερβολικά αιτήματα, ενώ η πολιτική δημοσιοποίησης του βασιζόμενου μέρος που μπορεί να συμβουλευτεί, μπορεί να επιδέχεται μεγάλης ερμηνείας χωρίς να συνδέεται με κάποιο τεχνικό περιορισμό.
2. Ο κανονισμός δίνει το δικαίωμα στο χρήστη να επιλέγει ελεύθερα ένα ψευδώνυμο αντί της νομικής του ταυτότητας, εφόσον αυτή δεν απαιτείται νομικά. Στο ARF εισάγεται η έννοια του παρόχου ψευδωνύμων (pseudonym provider), η οποία ωστόσο δεν εντοπίζεται σε κανένα σημείο του κανονισμού. Η αιτιολόγηση της αναγκαιότητας αυτού του ρόλου γίνεται με δύο παραδείγματα νομικής φύσεως (περίπτωση νομική αντιπαράθεσης ή απαίτησης από κάποια νομική υπηρεσία) ωστόσο με αυτό τον τρόπο αναφέρεται πως διευκολύνεται η αναδρομική ταυτοποίηση των χρηστών από νομικές υπηρεσίες ενώ υποβαθμίζονται σημαντικά τα πλεονεκτήματα που τα ψευδώνυμα προσφέρουν. Επίσης, η υλοποίηση ενός τέτοιου ρόλου έρχεται σε αντιπαράθεση με την προδιαγραφή του κανονισμού που θέλει τα ψευδώνυμα να δημιουργούνται και να αποθηκεύονται τοπικά και μόνο. Γίνεται ακόμα αναφορά ότι με αυτόν τον τρόπο ανοίγει «πόρτα» για μαζική παρακολούθηση.
3. Ο κανονισμός ορίζει ότι μέσα από το ψηφιακό πορτοφόλι οι χρήστες θα πρέπει να έχουν τη δυνατότητα να δουν το ιστορικό των αλληλεπιδράσεών τους με τα βασιζόμενα μέρη, να αιτηθούν διαγραφής των προσωπικών τους δεδομένων αλλά και να αναφέρουν κάποια ύποπτη αλληλεπίδραση που είχαν. Ωστόσο, στην πλέον πρόσφατη έκδοση του ARF δεν παρουσιάζεται κάποια τεχνική λύση παραδείγματος χάριν στην ενότητα που αναλύονται τα κοινά πρωτόκολλα και διεπαφές ενώ η υλοποίηση των παραπάνω δυνατοτήτων αφήνεται στα κράτη-μέλη.

[38] Μη κερδοσκοπικός οργανισμός από την Αυστρία, που εστιάζει στη διατήρηση των θεμελιωδών δικαιωμάτων στην ψηφιακή εποχή μέσα από ένα εύρος δραστηριοτήτων. [88]

Ως εκ τούτου, χωρίς μία ενιαία προσέγγιση και την απαραίτητη διαλειτουργικότητα, υπάρχει μεγάλος κίνδυνος να μην υπάρχει ουσιαστική υποστήριξη προς τους χρήστες ώστε να έχουν τον έλεγχο των δεδομένων τους σε αυτές τις περιπτώσεις και να λαμβάνουν έγκαιρα την βοήθεια που χρειάζονται. Σχετικά με τις ανωτέρω απαιτήσεις, εντοπίζεται ένα ακόμα σημείο διαφοροποίησης κανονισμού και πλαισίου.

Συγκεκριμένα, στο πλαίσιο αναφέρεται ότι ο χρήστης θα μπορεί να αναφέρει κάποιο παράπονο στην Αρχή Προστασίας Δεδομένων της χώρας που του παρείχε το πορτοφόλι, περιορίζοντας έτσι το δικαίωμα του βάσει του ΓΚΠΔ να κάνει αναφορά σε οποιαδήποτε Αρχή Προστασίας Δεδομένων εντός της ΕΕ.

4. Καθώς μέσα από τα ψηφιακά πορτοφόλια αναμένεται ανταλλαγή μεγάλου όγκου και ποικιλίας διαφορετικών πληροφοριών χρηστών, υπάρχει μεγάλος κίνδυνος για την ιδιωτικότητα των χρηστών από την ενδεχόμενη συλλογή, την πραγματοποίηση αναλύσεων και τον συσχετισμό των δεδομένων τους για τον εντοπισμό μοτίβων. Ως αντίμετρο, ο κανονισμός δίνει έμφαση στην απαίτηση για μη παρατηρησιμότητα (unobservability). Αναλυτικά, απαγορεύει ρητά από τους παρόχους των πορτοφολιών να έχουν πρόσβαση στις λεπτομέρειες των αλληλεπιδράσεων των χρηστών καθώς και να συλλέγουν και να επεξεργάζονται δεδομένα εκτός των απολύτως απαραίτητων για την παροχή της υπηρεσίας τους. Ακόμα, στην ίδια λογική, απαγορεύει τον συσχετισμό των πληροφοριών, ή προσωπικών δεδομένων από άλλες υπηρεσίες που προσφέρουν οι ίδιοι ή τρίτα μέρη, εκτός των απολύτως απαραίτητων για την παροχή της υπηρεσίας τους και εκτός αν ο χρήστης έχει ρητά έχει δώσει εξουσιοδότηση. Ωστόσο, στο ARF δεν παρουσιάζονται καθόλου σχετικές προδιαγραφές για την υλοποίηση των απαιτήσεων αυτών που αφορούν την εξασφάλιση της ιδιωτικότητας ήδη από το σχεδιασμό.

5. Στον κανονισμό ορίζεται επίσης ότι το τεχνικό πλαίσιο που θα διέπει το ψηφιακό πορτοφόλι θα πρέπει επιτρέπει τη χρήση τεχνικών διατήρησης της ιδιωτικότητας, ώστε να διασφαλίζεται η «μη συνδεσιμότητα»[39] (unlinkability). Ακόμα στα ψηφιακά πορτοφόλια θα πρέπει να εφαρμόζονται αρχές ιδιωτικότητας ήδη από το σχεδιασμό, ασφάλειας ήδη από το σχεδιασμό και προηγμένες τεχνολογίες, ενώ υπάρχει και η απαίτηση για «περιορισμό του σκοπού» που θα επιτρέπει στο χρήστη να έχει τον απόλυτο έλεγχο για τις αλληλεπιδράσεις που γίνονται με τα δεδομένα του. Παρόλο που οι απαιτήσεις αυτές καλύπτονται μέσω τεχνολογιών μη συνδεσιμότητας, τα πρότυπα/τεχνικές προδιαγραφές που παρουσιάζονται στο πλαίσιο ως προτεινόμενα για χρήση δεν είναι διαμορφωμένα κατάλληλα για να την εξασφαλίζουν. Επιπλέον επισημαίνεται ότι οι προτεινόμενες μορφές δεδομένων στηρίζονται στα ίδια αυτά πρότυπα, με αποτέλεσμα να εμποδίζεται μελλοντικά η υιοθέτηση νέων τεχνολογιών.

6. Στο πλαίσιο της αξιολόγησης, προτείνεται η ενσωμάτωση της αρχής της δυνατότητας άρνησης/αμφισβήτησης (repudiation/deniability) σε επόμενη έκδοση. Η ιδιότητα αυτή επιτρέπει στο χρήστη να αρνηθεί εύλογα την αυθεντικότητα των διαπιστευτηρίων και των σχετικών χαρακτηριστικών, μετά την παρουσίασή τους στο βασιζόμενο μέρος. Ως αποτέλεσμα δεν μπορεί το βασιζόμενο μέρος να αποδείξει την αυθεντικότητα και την ακεραιότητα παλαιότερα ληφθέντων διαπιστευτηρίων σε άλλα τρίτα μέρη, και ο χρήστης μπορεί να περιορίσει την μεταφορά των υπογεγραμμένων προσωπικών του δεδομένων μόνο στην συναλλαγή για την οποία αρχικά έδωσε την άδειά του.

[39] Στην ορολογία των ψηφιακών διαπιστευτηρίων με τον όρο «μη συνδεσιμότητα» εννοείται ότι διαφορετικές συναλλαγές του ίδιου χρήστη δεν μπορούν να συσχετιστούν ή να ανιχνευθούν. [84]

7. Μία ακόμα επισήμανση αφορά τον ΓΚΠΔ που παρέχει στους χρήστες το δικαίωμα φορητότητας με το οποίο μπορούν να λάβουν αντίγραφο των δεδομένων τους και να τα μεταφέρουν σε άλλο πάροχο. Ωστόσο, στο ARF δεν υπάρχει κάποια πρόταση για την τεχνική υλοποίηση του δικαιώματος αυτού μέσω του ψηφιακού πορτοφολιού.
8. Τέλος στην αξιολόγηση επισημαίνεται ότι πολλά χαρακτηριστικά που θα συμπεριλαμβάνονται στα πορτοφόλια όπως το φύλο, η οικογενειακή κατάσταση, ή η διεύθυνση κατοικίας δεν αντιμετωπίζονται και παρουσιάζονται με τον ίδιο τρόπο σε όλες τις χώρες της Ένωσης οπότε απαιτείται ιδιαίτερη προσοχή στην σύνταξη που θα χρησιμοποιηθεί και στην σημειολογία των σχετικών παραμέτρων.

[82] [83]

Ανάλυση για τους μηχανισμούς διαπιστευτηρίων

Στα πλαίσια της παρουσίασης της τελευταίας έκδοσης του πλαισίου σε ειδικούς καταρτισμένους σε σχετικά αντικείμενα τον Ιούνιο του 2024, ζητήθηκε η ανατροφοδότησή τους. Μία ομάδα από επαγγελματίες στον τομέα της κρυπτογραφίας συνέταξε αναφορά πάνω στον προτεινόμενο σχεδιασμό του ψηφιακού πορτοφολιού και ειδικότερα στους σχετικούς μηχανισμούς για τα διαπιστευτήρια. Η κύρια παρατήρηση ήταν ότι οι προτεινόμενες κρυπτογραφικές μέθοδοι δεν έχουν σχεδιαστεί για να ανταποκρίνονται στις απαιτήσεις ιδιωτικότητας του κανονισμού, με έμφαση στην «μη συνδεσιμότητα». Προτείνουν τον επανασχεδιασμό του πλαισίου με χρήση της τεχνολογίας των ανώνυμων διαπιστευτηρίων (anonymous credentials) για την ταυτοποίηση και επαλήθευση ταυτότητας διατηρώντας την ασφάλεια και την ιδιωτικότητα των χρηστών [84].

Στην ανάλυσή τους, παρουσιάζουν τις τρεις μορφές της «μη συνδεσιμότητας» που απαιτεί ο κανονισμός:

- Μη συνδεσιμότητα σε σχέση με τα βασιζόμενα μέρη: Όταν ο χρήστης παρουσιάζει τα διαπιστευτήριά του σε διαφορετικά βασιζόμενα μέρη, εκείνα δεν πρέπει να είναι σε θέση να διαπιστώσουν αν οι δύο αυτές αλληλεπιδράσεις προέρχονται από τον ίδιο ή διαφορετικούς χρήστες, ανεξάρτητα από τις συμπληρωματικές πληροφορίες που ενδεχομένως έχουν στη διάθεσή τους. Επίσης, εκτός αν ο χρήστης απαιτείται να διατηρεί ένα ψευδώνυμο για όλες τις συναλλαγές του με το βασιζόμενο μέρος, η αρχή της μη συνδεσιμότητας πρέπει να ισχύει και όταν ο χρήστης παρουσιάζει δύο φορές τα διαπιστευτήριά του στο ίδιο βασιζόμενο μέρος.
- Μη συνδεσιμότητα σε σχέση με τα παρόχους ταυτότητας: Ένας πάροχος ταυτότητας δεν πρέπει να μπορεί να αποκτήσει καμία πληροφορία για το πότε, που και σε ποια βασιζόμενα μέρη ένας χρήστης παρουσίασε τα διαπιστευτήριά τους.
- Μη συνδεσιμότητα σε σχέση με τα βασιζόμενα μέρη και παρόχους ταυτότητας: Ο πάροχος δεν μπορεί να αποκτήσει καμία πληροφορία από το βασιζόμενο μέρος που να του επιτρέπει να εντοπίσει και να αναγνωρίσει το χρήστη πίσω από κάποια αλληλεπίδραση, ακόμα και αν πάροχος ταυτότητας και βασιζόμενο μέρος συνεργάζονται.

Οι κρυπτογραφικές τεχνικές στα προτεινόμενα πρότυπα προς χρήση δεν εξασφαλίζουν τη μη συνδεσιμότητα σε σχέση με τα βασιζόμενα μέρη ούτε σε σχέση με τα βασιζόμενα μέρη και παρόχους ταυτότητας, οπότε και προτείνεται η χρήστη των ανώνυμων διαπιστευτηρίων, με τα οποία ένας χρήστης μπορεί να αποδείξει κάτι για τον εαυτό του, χωρίς να αποκαλύψει καμία επιπλέον πληροφορία. Για τη δημιουργία αυτών των διαπιστευτηρίων ο χρήστης, και ο εκδότης τους, τρέχουν ένα πρωτόκολλο υπολογισμού όπου μόνο ο χρήστης λαμβάνει κάποια έξοδο (μία υπογραφή που έχει προκύψει από το δικό του μυστικό κλειδί και ένα σύνολο από χαρακτηριστικά) και κανένα από τα δύο μέρη δεν μαθαίνει τις μυστικές τιμές του άλλου.

Τα χαρακτηριστικά των ανώνυμων διαπιστευτηρίων είναι: (α) δεν περιλαμβάνουν πληροφορίες για την ταυτότητα του «ιδιοκτήτη» τους δηλαδή είναι ανώνυμα, (β) υποστηρίζουν την αρχή της επιλεκτικής αποκάλυψης (selective disclosure) οπότε σε κάθε αλληλεπίδραση μοιράζονται μόνο το τμήμα των πληροφοριών που είναι απαραίτητες, (γ) υποστηρίζουν την αρχή της «μη συνδεσιμότητας» καθώς δύο αλληλεπιδράσεις δεν μπορούν να συσχετιστούν και (δ) αποσυνδέουν την οντότητα που έχει επικυρώσει τα δεδομένα από την διαδικασία της επαλήθευσης τους.

Κατά την παρουσίαση των επιλεγμένων στοιχείων, χρησιμοποιούνται τεχνικές απόδειξης μηδενικής γνώσης (zero-knowledge proof) ώστε ο χρήστης να μπορεί να αποδείξει στον ελεγκτή ότι τα στοιχεία του έχουν επικυρωθεί από τον εκδότη τους με τρόπο τέτοιο ώστε να μην αποκαλύπτεται καμία περαιτέρω πληροφορία ως προς το γιατί τα στοιχεία αυτά είναι ορθά. Εφόσον ο αλγόριθμος του ελεγκτή αποδέχεται τα στοιχεία που το παρουσιάζονται σημαίνει αυτόματα ότι ο αλγόριθμος του χρήστη κατέχει το μυστικό κλειδί που αναφέρθηκε παραπάνω και ότι έχει επικυρωθεί από τον εκδότη. Για τη λειτουργία αυτού του σχήματος απαιτείται οι εκδότες να έχουν δημόσια κλειδιά και πιστοποιητικά από τις αρχές, και οι ελεγκτές να μπορούν να επιβεβαιώνουν ότι ένα δημόσιο κλειδί αντιστοιχεί σε έναν έγκυρο εκδότη. Τέλος, το ποιο κοινό και γνωστό σχήμα που υποστηρίζει τα ανώνυμα διαπιστευτήρια είναι το BBS/BBS+.

[84]

4.3 Συμπεράσματα

Ο κανονισμός eIDAS 2.0 θέτει τις βάσεις για το οικοσύστημα των ψηφιακών πορτοφολιών. Η υλοποίησή του να αποτελεί ένα μεγαλεπήβολο σχέδιο, το οποίο είναι ακόμα σε πολύ πρώιμο στάδιο. Ως εκ τούτου, πολλά τεχνικά αλλά και οργανωτικά ζητήματα ακόμα δεν έχουν οριστικοποιηθεί, υπάρχουν κενά που δεν έχουν αντιμετωπιστεί και σίγουρα θα υπάρξουν και άλλες προκλήσεις που ακόμα δεν έχουν εντοπιστεί. Η ΕΕ κάνει σημαντική προσπάθεια να εξοπλίσει τα κράτη-μέλη με τα απαραίτητα εφόδια ώστε να μπορούν πιο εύκολα να υλοποιήσουν τις δικές τους λύσεις πορτοφολιών χωρίς να χρειαστεί να ξεκινήσουν από το μηδέν. Το πλαίσιο αναφοράς και αρχιτεκτονικής μαζί με τα πιλοτικά έργα μεγάλης κλίμακας θα αποτελέσουν τη βάση για την οικοδόμηση ολόκληρου του οικοσυστήματος, για αυτό και απαιτείται ιδιαίτερη προσοχή στη φάση αυτή.

Σε ό,τι αφορά στα πιλοτικά έργα, ακόμα δεν είναι γνωστές πολλές πληροφορίες για την πρόοδο των δοκιμών στις επιλεγμένες περιπτώσεις χρήσης. Σε κάθε περίπτωση όμως αναμένεται πως θα έρθουν αντιμέτωποι με πρακτικά προβλήματα από διαφορετικές διαδικασίες που μπορεί να ακολουθούνται στα κράτη μέλη και την έλλειψη κοινής προσέγγισης. Ακόμα, καλούνται να προχωρούν τις δοκιμές τους απουσία των εκτελεστικών πράξεων και την σταδιακή προσαρμογή τους σε αυτές, με την δημοσιοποίησή τους το επόμενο διάστημα. Φυσικά, οι περιπτώσεις χρήσης, όπως είναι αναμενόμενο, είναι ένα πολύ μικρό υποσύνολο των πραγματικών σεναρίων χρήσης των πορτοφολιών και πιθανά προβλήματα δεν έχουν καν εντοπιστεί ακόμα.

Ένας πολύ κρίσιμος παράγοντας στην επιτυχία του εγχειρήματος αυτού είναι οι χρήστες των πορτοφολιών. Αρχικά, ακόμα δεν υπάρχει επαρκής ενημέρωση από τα κράτη μέλη στους πολίτες. Ωστόσο, σε επίπεδο ΕΕ γίνεται προσπάθεια διαφήμισης και υποστήριξης του ψηφιακού πορτοφολιού, παρέχοντας υψηλού επιπέδου πληροφορίες με έμφαση στα πλεονεκτήματα που θα υπάρχουν από τη χρήση του αλλά και στα μέτρα ασφάλειας και ιδιωτικότητας που λαμβάνονται κυρίως μέσα από τον σχετικό ιστότοπο. Βέβαια, ενέργειες θα πρέπει να γίνουν σε εθνικό επίπεδο και αυτές θα πρέπει να λαμβάνουν υπόψιν το μορφωτικό επίπεδο των πολιτών αλλά και την «ψηφιακή» ωριμότητα της χώρας. Για την ευρεία αποδοχή και εν τέλει χρήση των πορτοφολιών, χρειάζεται να αναγνωριστούν οι ιδιαιτερότητες που μπορεί να υπάρχουν τόσο σε επίπεδο χώρας αλλά και ομάδων πολιτών ώστε να μπορούν να αντιμετωπιστούν οι προβληματισμοί και οι δυσκολίες κατάλληλα και να μην αποτελέσουν φραγμό για τη χρήση της λύσης. Ένα πολύ απλό παράδειγμα είναι ότι υπάρχουν χώρες όπως η Εσθονία με πολύ προηγμένη ψηφιακή κοινωνία, όπου είναι εξοικειωμένη σε αντίστοιχες πρωτοβουλίες και υψηλό ρυθμό υιοθέτησης, αλλά και χώρες όπως η Ελλάδα που παρά την μεγάλη προσπάθεια των τελευταίων ετών για ψηφιακό μετασχηματισμό, υπάρχει ακόμα μεγάλο χάσμα. Φυσικά, όλες οι λύσεις που θα σχεδιαστούν, θα πρέπει να συνυπολογίσουν όλα τα τεχνικά μέτρα που θα διευκολύνουν τη χρήση τους από πολίτες που έχουν από πολύ μεγάλο μέχρι πολύ μικρό βαθμό εξοικείωσης με τέτοιες τεχνολογίες αλλά και τα δικαιώματα που έχουν βάσει των κανονισμών, ώστε οι εφαρμογές να είναι στην πράξη «φιλικές προς το χρήστη» και να του επιτρέπουν πραγματικά να τις λειτουργεί εύκολα και να ασκεί τα όποια δικαιώματά του χωρίς φραγμούς.

Στην προηγούμενη ενότητα δόθηκε έμφαση σε προβληματισμούς σχετικά με την ασφάλεια και την ιδιωτικότητα των δεδομένων των χρηστών. Η ευθύνη για την ανάπτυξη και υλοποίηση κατάλληλων προδιαγραφών που θα εξασφαλίζουν αυτές της δύο παραμέτρους είναι τεράστιες. Για την οικοδόμηση και τη διατήρηση της εμπιστοσύνης σε βάθος χρόνου σε τέτοια συστήματα, πρέπει να εξεταστούν με ιδιαίτερη προσοχή οι απαιτήσεις αυτών των συνιστωσών και η κάλυψή τους. Θα πρέπει να εξεταστούν οι συνέπειες από την μη ικανοποίηση των απαιτήσεων αλλά και πιθανοί τρόποι ανάκαμψης από αυτές. Ειδικά σε αυτό το πλαίσιο, καίριος είναι ο ρόλος των οργανισμών πιστοποίησης των πορτοφολιών.

Οι οργανισμοί πιστοποίησης σε όλα τα κράτη μέλη θα πρέπει να έχουν τις απαιτούμενες τεχνικές γνώσεις, τα εργαλεία, τις τεχνικές και τις διαδικασίες για να επιτελούν σωστά το έργο τους. Παρόλο που σε υψηλό επίπεδο οι απαιτήσεις αυτές παρουσιάζονται τόσο στον κανονισμό όσο και σε συνέδρια ή αξιολογήσεις, η ουσία βρίσκεται στην υλοποίησή τους και στην δυνατότητα διατήρησής τους σε βάθος χρόνου. Πολλές φορές έχουν εντοπιστεί μηχανισμοί αξιολόγησης που καταλήγουν να λειτουργούν εκτελεστικά και τυπικά, με αποτέλεσμα να είναι εκτεθειμένα τα όποια ενδιαφερόμενα μέρη από τη μη συνέπεια με τις απαιτήσεις. Μία κακή ή ελλιπής προσέγγιση στο ζήτημα της πιστοποίησης μπορεί να οδηγήσει σε χρήση πορτοφολιών που δεν πληρούν τις προδιαγραφές, σε πολλές διαφορετικές συνέπειες από τα κενά τους (επιθέσεις, διαρροή δεδομένων κ.ο.κ.) και φυσικά σε βλάβη της εμπιστοσύνης στο σύστημα.

Πολύ σημαντικός είναι και ο ρόλος των καταλόγων εμπιστοσύνης. Παρά τα αρχικά καλά δείγματα λειτουργίας τους για τις υπηρεσίες εμπιστοσύνης, οι κατάλογοι εμπιστοσύνης που θα πρέπει σε βάθος χρόνου να συντηρούνται και τα δεδομένα τους να παραμένουν ακέραια και διαθέσιμα είναι αρχικά πολλοί λόγω των απαιτήσεων, των κρατών μελών και φυσικά του όγκου της πληροφορίας που θα πρέπει να διατηρούν. Μία ενδεχόμενη παραβίαση σε λίστες και εισαγωγή ψεύτικων στοιχείων σε αυτές μπορεί να διαταράξει τις ισορροπίες και την εμπιστοσύνη του οικοσυστήματος.

Ένας άλλος κρίσιμος παράγοντας είναι η καταλληλόλητα και η διαθεσιμότητα των τεχνολογιών για την υποστήριξη του οικοσυστήματος όχι μόνο βραχυπρόθεσμα αλλά μακροπρόθεσμα. Στην προηγούμενη ενότητα παρουσιάστηκαν οι προβληματισμοί ειδικών ως προς την κατεύθυνση που έχει πάρει μέχρι στιγμής το πλαίσιο αναφοράς και αρχιτεκτονικής, με τη χρήση τεχνολογιών που δεν έχουν σχεδιαστεί για τις ανάγκες του ψηφιακού πορτοφολιού και δεν τις καλύπτουν. Σε αυτούς τους προβληματισμούς, σημαντική είναι και η αξιολόγηση της προόδου της τεχνολογίας και των κινδύνων από τη χρήση παρωχημένων τεχνικών λύσεων. Ο σχεδιασμός των πορτοφολιών πρέπει να είναι τέτοιος που να επιτρέπει την υιοθέτηση νέων τεχνολογιών ώστε να ελαχιστοποιούνται και οι κίνδυνοι, ενώ παράλληλα θα πρέπει και να δίνεται η απαιτούμενη προσοχή στην ωριμότητα των προτύπων και προδιαγραφών που θα επιλέγονται, ώστε να έχουν αξιολογηθεί όχι μόνο ως προς τη δυνατότητα να καλύπτουν τις απαιτήσεις αλλά να έχει παρακολουθηθεί η λειτουργικότητά τους σε ένα ικανό βάθος χρόνου.

Ένας ακόμα παράγοντας που συνεχώς εξετάζεται και εντοπίζονται δυσκολίες είναι αυτός της διαλειτουργικότητας. Οι απαιτήσεις διαλειτουργικότητας στο οικοσύστημα του ψηφιακού πορτοφολιού είναι εξαιρετικά υψηλές ιδίως λαμβάνοντας υπόψη την ανάγκη να λειτουργήσει «ενωτικά» και να μην οδηγηθούμε σε πρόσθετο κατακερματισμό της αγοράς. Ωστόσο, η απαίτηση για διαλειτουργικότητα μαζί με την τεχνολογική ουδετερότητα που (εύλογα) διατηρεί ο κανονισμός αφήνει χώρο για πολλές πιθανές ασυμβατότητες.

Παρόλο που δεν δόθηκε έμφαση στις προηγούμενες ενότητες, μία βασική συνιστώσα για την επιτυχία του εγχειρήματος αφορά και το κόστος υλοποίησης, λειτουργίας και συντήρησης του. Υπενθυμίζεται πως η παροχή ενός τουλάχιστον πορτοφολιού ανά κράτος μέλος τους πολίτες πρέπει να γίνεται δωρεάν. Θα πρέπει λοιπόν να υπάρχουν επαρκείς οικονομικοί πόροι για την ανάπτυξή και συντήρησή τους ώστε αυτή να γίνεται σωστά και να μην οδηγούνται οι εκάστοτε φορείς σε οποιουδήποτε είδους περικοπές λόγω κόστους. Αντίστοιχα, είναι σημαντικό να δίνονται και να επικοινωνούνται σωστά τα κίνητρα και στα βασιζόμενα μέρη που θα πρέπει να καταβάλλουν προσπάθεια ώστε να γίνουν και να παραμένουν μέρος του οικοσυστήματος.

Ακόμα, στο οικοσύστημα του πορτοφολιού θα γίνονται καθημερινά εκατομμύρια αλληλεπιδράσεις που θα συνεπάγονται την ανάγκη διαχείρισης τεράστιου όγκου δεδομένων. Η σωστή εφαρμογή των τεχνικών μέτρων για την διατήρηση της μη συνδεσιμότητας και της μη παρατηρησιμότητας είναι κρίσιμη ώστε οι χρήστες να παραμένουν πραγματικά κύριοι των δεδομένων τους σε βάθος χρόνου και να ελαχιστοποιηθούν οι κίνδυνοι συλλογής και επεξεργασίας τους με στόχο την δημιουργία προφίλ όπως ρητά απαγορεύει ο κανονισμός.

Συμπερασματικά, είναι πολλοί οι κίνδυνοι που συνοδεύουν την εφαρμογή του οικοσυστήματος του ψηφιακού πορτοφολιού. Παράλληλα όμως είναι και μία μεγάλη ευκαιρία στα πλαίσια της ψηφιακής εποχής που θα ωφελήσει σε πολλά επίπεδα πολίτες, επιχειρήσεις και το δημόσιο τομέα με την ασφαλή και εύκολη ολοκλήρωση διαφόρων τύπων αλληλεπιδράσεων που σήμερα γίνονται με «δυσκολότερο τρόπο» ενώ υπάρχει και η βάση ώστε να είναι οι χρήστες κύριοι των δεδομένων τους.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	Ελληνικός όρος
Digital identity	Ψηφιακή ταυτότητα
Attribute	Χαρακτηριστικό
Entity	Οντότητα
Electronic identification	Ηλεκτρονική ταυτοποίηση
Authentication	Επαλήθευση ταυτότητας
Person identification data	Δεδομένα ταυτοποίησης προσώπου
eID scheme	Σύστημα ηλεκτρονικής ταυτοποίησης
Trust service	Υπηρεσία εμπιστοσύνης
E-Signature	Ηλεκτρονική υπογραφή
E-Seal	Ηλεκτρονική σφραγίδα
E-Timestamp	Ηλεκτρονική χρονοσφραγίδα
Electronic registered delivery service	Ηλεκτρονική υπηρεσία συστημένης παράδοσης
Qualified web authentication certificates	Υπηρεσία πιστοποιητικών για την επαλήθευση της ταυτότητας ιστοτόπων
Notification	Κοινοποίηση
Levels of Assurance	Επίπεδα διασφάλισης
Qualified	Εγκεκριμένος/η
Qualified signature creation device	Εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής
Format	Μορφότυπος
Qualified seal creation device	Εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας
Phishing attack	Επίθεση ηλεκτρονικού ψαρέματος
Domain name	Όνομα χώρου
Qualified trust service provider	Εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης
Conformity assessment body	Οργανισμός αξιολόγησης συμμόρφωσης
National accreditation body	Εθνικός οργανισμός διαπίστευσης
Designated certification body	Υποδειγμένος οργανισμός πιστοποίησης
Supervisory body	Εποπτικός φορέας
Trusted list	Κατάλογος εμπιστοσύνης
TL scheme operator	Χειριστής του σχήματος καταλόγου εμπιστοσύνης
EU trusted mark	Ενωσιακό σήμα εμπιστοσύνης

Trust backbone	Βάση εμπιστοσύνης
Identity & Attribute providers	Πάροχοι ταυτότητας και αναγνωριστικών
Digital eID building block	Ψηφιακό δομικό στοιχείο eID
Node implementers & operators	Υπεύθυνοι υλοποίησης & λειτουργίας κόμβων
Single point of contact	Ενιαίο σημείο επαφής/εξυπηρέτησης
Identity providers	Πάροχοι ταυτότητας
Attribute providers	Πάροχοι αναγνωριστικών
Public Service providers	Δημόσιοι πάροχοι υπηρεσιών
Substantial/high level	Υψηλό επίπεδο
Private Service providers	Ιδιωτικοί πάροχοι υπηρεσιών
Sector-specific EU projects	Έργα της ΕΕ σε συγκεκριμένους τομείς
EU citizens	Πολίτες της ΕΕ
EU Commission	Ευρωπαϊκή επιτροπή
Directorate-General for Informatics - DIGIT	Γενική διεύθυνση ψηφιακών υπηρεσιών
Directorate-General for Communications Networks, Content and Technology - DG CNECT	Γενική Διεύθυνση για Δίκτυα Επικοινωνιών, Περιεχομένου και Τεχνολογίας
Innovation and Networks Executive Agency	Εκτελεστικός Οργανισμός Καινοτομίας και Δικτύων
Member state participation	Συμμετοχή κρατών-μελών
Cooperation network	Δίκτυο συνεργασίας
Expert group	Ομάδα εμπειρογνωμόνων
eIDAS Technical Sub-group	Τεχνική υπο-ομάδα του eIDAS
Eu digital identity wallet	Ευρωπαϊκό ψηφιακό πορτοφόλι ηλεκτρονικής ταυτότητας
Relying party	Βασιζόμενο μέρος
Electronic attestation of attributes	Ηλεκτρονική βεβαίωση χαρακτηριστικών
Electronic ledger	Ηλεκτρονικό καθολικό
Electronic archiving	Ηλεκτρονική αρχειοθέτηση
Browser	Φυλλομετρητής ιστού
EU digital identity wallet toolbox	Εργαλειοθήκη του ευρωπαϊκού ψηφιακού πορτοφολιού ηλεκτρονικής ταυτότητας
Large scale pilots	Πιλοτικά έργα μεγάλης κλίμακας
Architecture & reference framework	Πλαίσιο αναφοράς και αρχιτεκτονικής
Wallet prototype	Πρότυπο πορτοφόλι
Consortium	Σύμπραξη

eGov services	Υπηρεσίες ηλεκτρονικής διακυβέρνησης
Bank account opening	Άνοιγμα τραπεζικού λογαριασμού
SIM card registration	Εγγραφή και ενεργοποίηση προπληρωμένων ή μη συμβολαίων κινητής τηλεφωνίας
Mobile driving license	Ηλεκτρονική άδεια οδήγησης
ePerscription	Ηλεκτρονική συνταγογράφηση
Architecture concept	Σενάριο αρχιτεκτονικής
Pprofessional qualifications	Επαγγελματικά προσόντα
Security by design	Ασφάλεια ήδη από το σχεδιασμό
Public sector body	Φορέας του δημοσίου τομέα
Public Body Authentic Source Electronic Attestation of Attributes	Ηλεκτρονικές βεβαιώσεις χαρακτηριστικών αυθεντικών πηγών δημοσίων φορέων
User-centricity	Επικέντρωση στο χρήστη
Privacy by design	Ιδιωτικότητα ήδη από το σχεδιασμό
User device	Συσκευή του χρήστη
Wallet instance	αντίγραφο/εκδοχή πορτοφολιού ή εγκατεστημένο πορτοφόλι
Wallet secure cryptographic device	Κρυπτογραφική συσκευή ασφαλείας πορτοφολιού
Hardware	Υλισμικό
Wallet secure cryptographic application	Κρυπτογραφική εφαρμογή ασφαλείας πορτοφολιού
Wallet Provider backend	Σύστημα υποστήριξης παρόχου πορτοφολιού
Wallet provider interface	Διεπαφή του παρόχου του πορτοφολιού
User interface	Διεπαφή του χρήστη
Presentation interface	Διεπαφή παρουσίασης
Proximity interaction	Αλληλεπίδραση εγγύτητας
Secure cryptographic interface	Ασφαλής κρυπτογραφική διεπαφή
Person Identification Data issuance interface	Η διεπαφή για την έκδοση δεδομένων ταυτοποίησης προσώπου
Attestation issuance interfaces	Διεπαφές για την έκδοση βεβαιώσεων
Remote signing interface	Διεπαφή απομακρυσμένης υπογραφής
Reporting interface	Διεπαφή αναφοράς
Deletion request interface	Διεπαφή αίτησης διαγραφής
Proximity supervised flow	Ροή εγγύτητας με επίβλεψη

Proximity unsupervised flow	Ροή εγγύτητας χωρίς επίβλεψη
Remote cross-device flow	Απομακρυσμένη ροή μεταξύ διαφορετικών συσκευών
Remote same-device flow	Απομακρυσμένη ροή με χρήση μίας συσκευής
Remote wscd	Απομακρυσμένη κρυπτογραφική συσκευή ασφαλείας πορτοφολιού
Hardware security module	Υλική μονάδα ασφαλείας
Local external wscd	Τοπική εξωτερική κρυπτογραφική συσκευή ασφαλείας πορτοφολιού
Local wscd	Τοπική κρυπτογραφική συσκευή ασφαλείας πορτοφολιού
Candidate state	Κατάσταση υποψηφιότητας
Valid state	Κατάσταση ισχύος
Suspended state	Κατάσταση αναστολή
Withdrawn state	Κατάσταση απόσυρσης
Installed state	Κατάσταση εγκατεστημένη
Operational state	Κατάσταση λειτουργική
Wallet trust evidence	Αποδεικτικά στοιχεία εμπιστοσύνης
Wallet instance attestation	Βεβαίωση εγκατεστημένου πορτοφολιού
Key association mechanism	Μηχανισμός συσχέτισης κλειδιού
Uninstalled state	Κατάσταση απεγκατεστημένη
Issued state	Κατάσταση έκδοσης
Revoked state	Κατάσταση ανάκλησης
Expired state	Κατάσταση λήξης
Attribute schema	Σχήμα χαρακτηριστικών
Namespace	Χώρος ονομάτων
Proof mechanism	Μηχανισμός απόδειξης
Attestation rulebook	Εγχειρίδιο βεβαίωσης
Authorization	Εξουσιοδότηση
Impersonation	Αντιποίηση ταυτότητας
Notified body	Κοινοποιημένο μέρος
Trust anchors	Άγκυρες εμπιστοσύνης
Access certificate	Πιστοποιητικό πρόσβασης
Status list	Κατάλογος κατάστασης των δεδομένων ή με τα αποσυρθέντα δεδομένα
Revocation list	Κατάλογος με τα αποσυρθέντα δεδομένα

Device binding	Σύνδεση συσκευής
User binding	Σύνδεση χρήστη
Standards development organizations	Οργανισμοί ανάπτυξης προτύπων
Tamper-evident	Εμφανής παραποίηση
Holder binding	Συσχέτιση κατόχου
Proof of Association	Απόδειξη συσχέτισης
Natural person PID Rulebook	Εγχειρίδιο για τα δεδομένα ταυτοποίησης προσώπου των φυσικών προσώπων
Legal-person PID Rulebook	Εγχειρίδιο για τα δεδομένα ταυτοποίησης προσώπου των νομικών προσώπων
Pseudonym Rulebook	Εγχειρίδιο για τα ψευδώνυμα
Decentralized Identifiers	Αποκεντρωμένα αναγνωριστικά
Distributed ledgers registry	Αποθετήριο κατανεμημένων καθολικων
Pseudonym provider	Πάροχος ψευδωνύμων
Identity matching	Μη αδιαμφισβήτητη αντιστοίχιση ταυτότητας
Unobservability	Μη παρατηρησιμότητα
Unlinkability	Μη συνδεσιμότητα
Repudiation/deniability	Δυνατότητας άρνησης/αμφισβήτησης
Selective disclosure	Επιλεκτική αποκάλυψη
Zero-knowledge proof	Τεχνική απόδειξης μηδενικής γνώσης

ΣΥΝΤΟΜΕΥΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
NIST	National Institute of Standards and Technology
eIDAS	electronic Identification, Authentication and Trust Services
ΕΕ	Ευρωπαϊκή Ένωση
eID	electronic Identification
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
EUDI Wallet	European Digital Identity Wallet
NIS	Network and Information Security
ENISA	European Union Agency for Cybersecurity
ARF	Architecture & Reference Framework
EWC	EU Digital Wallet Consortium
DC4EU	Digital Credential for Europe
WSCD	Wallet Secure Cryptographic Device
PID	Person Identification Data
OpenId4VP	OpenID for Verifiable Presentations
OpenID4VCI	OpenID for Verifiable Credential Issuance
NFC	Near Field Communication
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
eSE	Embedded Secure Element
TLS	Transport Layer Security
SD-JWT VC	SD-JWT-based Verifiable Credentials
W3C VCDM	W3C Verifiable Credentials Data Model
ETSI	European Telecommunications Standards Institute
CEN/CENELEC	European Committee for Standardization/ European Committee for Electrotechnical Standardization
W3C	World Wide Web Consortium

IETF	Internet Engineering Task Force
OIDF	OpenID Foundation
CSC	Cloud Signature Consortium
SIOP	Self-Issued OpenID Provider
API	Application Programming Interface
OAuth	Open Authorization
HAIP	High-Assurance Interoperability Profile

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] R. Maheshwari, «A brief history of “Identity” | IDcentral,» 17 Ιούλιος 2019. [Ηλεκτρονικό]. Available: https://www.idcentral.io/blog/history-of-identity/. [Πρόσβαση Σεπτέμβριος 2024].

[2] D. Gupta, "A History of Human Identity in Pictures - Part 1 | LoginRadius," 17 Αύγουστος 2019. [Online]. Available: https://www.loginradius.com/blog/identity/history-identity-part-1/. [Accessed Σεπτέμβριος 2024].

[3] D. Gupta, «A History of Human Identity in Pictures Part 2 | LoginRadius,» 20 Αύγουστος 2019. [Ηλεκτρονικό]. Available: https://www.loginradius.com/blog/identity/history-identity-part-2/. [Πρόσβαση Σεπτέμβριος 2024].

[4] J. Burton, «Digital Identity: Where We Began, Where We Are And Where We Are Going,» 24 Μάρτιος 2022. [Ηλεκτρονικό]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/03/24/digital-identity-where-we-began-where-we-are-and-where-we-are-going/. [Πρόσβαση Σεπτέμβριος 2024].

[5] «Λεξικό της κοινής νεοελληνικής,» [Ηλεκτρονικό]. Available: https://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=%CF%84%CE%B1%CF%85%CF%84%CF%8C%CF%84%CE%B7%CF%84%CE%B1&dq=. [Πρόσβαση Σεπτέμβριος 2024].

[6] P. A. G. M. E. a. F. J. L. Grassi, Digital Identity Guidelines (Special Publication NIST SP 800-63-3), NIST, 2017.

[7] IT security and privacy – A framework for identity management – Part 1: Terminology and concepts (International Standard ISO/IEC 24760-1:2019), ISO/IEC, 2019.

[8] «ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 910/2014 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ,» 2014.

[9] [Ηλεκτρονικό]. Available: https://ec.europa.eu/futurium/sites/futurium/files/eidas-guidebooken.pdf. [Πρόσβαση Σεπτέμβριος 2024].

[10] «Discover eIDAS | Shaping Europe’s digital future,» 17 Μάιος 2023. [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas. [Πρόσβαση Σεπτέμβριος 2024].

[11] «eIDAS Regulation | Shaping Europe’s digital future,» 4 Απρίλιος 2024. [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. [Πρόσβαση Σεπτέμβριος 2024].

[12] «Building Trusted Digital Identity in EU (Efficient & Secure Digital Life),» 2019.

[13] T. Susanna, «Revision of the eIDAS Regulation - Findings on its implementation and application,» 7 Μάρτιος 2022. [Ηλεκτρονικό]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491#:~:t

ext=The%20Commission%20proposal%20amends%20and%20updates. [Πρόσβαση Σεπτέμβριος 2024].

[14] R. JERKOVIĆ, « Carriages preview | Legislative Train Schedule,» 20 Σεπτέμβριος 2024. [Ηλεκτρονικό]. Available: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid. [Πρόσβαση Σεπτέμβριος 2024].

[15] «eID,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID. [Πρόσβαση Σεπτέμβριος 2024].

[16] «What is eID,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/What+is+eID. [Πρόσβαση Σεπτέμβριος 2024].

[17] «eIDAS Levels of Assurance,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+Levels+of+Assurance. [Πρόσβαση Σεπτέμβριος 2024].

[18] «ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2015/1502 ΤΗΣ ΕΠΙΤΡΟΠΗΣ 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. 910/2014,» 2015.

[19] «ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2015/1501 ΤΗΣ ΕΠΙΤΡΟΠΗΣ για το πλαίσιο διαλειτουργικότητας σύμφωνα με το άρθρο 12 παράγραφος 8 του κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου,» 2015.

[20] «eIDAS Dashboard,» [Ηλεκτρονικό]. Available: https://eidas.ec.europa.eu/efda/discover/eu-trust-service-framework. [Πρόσβαση Σεπτέμβριος 2024].

[21] «eSignature FAQ,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ. [Πρόσβαση Σεπτέμβριος 2024].

[22] [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. [Πρόσβαση Σεπτέμβριος 2024].

[23] [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. [Πρόσβαση Σεπτέμβριος 2024].

[24] [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. [Πρόσβαση Σεπτέμβριος 2024].

[25] «Who is involved in eID?,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=467109829. [Πρόσβαση Σεπτέμβριος 2024].

[26] «How does it work?,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=467109866. [Πρόσβαση Σεπτέμβριος 2024].

[27] «eID Digital Monitoring Dashboard,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID+Digital+Monitoring+Dashboard. [Πρόσβαση Σεπτέμβριος 2024].

[28] «eIDAS Dashboard,» [Ηλεκτρονικό]. Available: https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts/EL. [Πρόσβαση Σεπτέμβριος 2024].

[29] E. Commission, «Report on the state of the Digital Decade 2023 | Shaping Europe's digital future,» [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade. [Πρόσβαση Σεπτέμβριος 2024].

[30] «eIDAS Dashboard,» [Ηλεκτρονικό]. Available: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/statistics. [Πρόσβαση Σεπτέμβριος 2024].

[31] «eIDAS Dashboard,» [Ηλεκτρονικό]. Available: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/EL. [Πρόσβαση Σεπτέμβριος 2024].

[32] E. Commision, «REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS),» 2021.

[33] Ε. Επιτροπή, «ΕΚΘΕΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ όσον αφορά την αξιολόγηση του κανονισμού (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά,» 2021.

[34] V. Manaila, Interviewee, *eIDAS 2.0 and EU Digital Identity Wallter, with Viky Manaila, Intesi Group.* [Συνέντευξη]. 16th November 2022.

[35] M. N. a. M. Niestadt. [Ηλεκτρονικό]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698772/EPRS_BRI(2021)698772_EN.pdf. [Πρόσβαση Σεπτέμβριος 2024].

[36] «About the initiative - EU Digital Identity Wallet,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/About+the+initiative. [Πρόσβαση Σεπτέμβριος 2024].

[37] «ΑΠΟΦΑΣΗ (ΕΕ) 2022/2481 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία»,» Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2022.

[38] «eIDAS regulation - EU Digital ID wallet,» [Ηλεκτρονικό]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/eidas-regulations. [Πρόσβαση Σεπτέμβριος 2024].

[39] «ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1183 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα,» 2024.

[40] «ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2022/1925 σχετικά με διεκδικήσιμες και δίκαιες αγορές στον ψηφιακό τομέα και για την τροποποίηση των οδηγιών (ΕΕ) 2019/1937 και (ΕΕ) 2020/1828 (Πράξη για τις Ψηφιακές Αγορές),» 2022.

[41] «eDIAS Letter 2022 | Electronic Frontier Foundation,» 3 Μάρτιος 2022. [Ηλεκτρονικό]. Available:

https://www.eff.org/files/2022/03/02/eidas_cybersecurity_community_open_letter_1_1.pdf. [Πρόσβαση Σεπτέμβριος 2024].

[42] J. L. D. MANNO, «A « QWAC » in the eiDAS directive revision | LinkedIn,» 6 Νοέμβριος 2023. [Ηλεκτρονικό]. Available: https://www.linkedin.com/pulse/qwac-eidas-directive-revision-jean-luc-di-manno-iksze/. [Πρόσβαση Σεπτέμβριος 2024].

[43] 23 Νοέμβριος 2023. [Ηλεκτρονικό]. Available: https://eidas-open-letter.org/statement-23-11-2023.pdf#:~:text=At%20the%20beginning%20of%20November%202023,. [Πρόσβαση Σεπτέμβριος 2024].

[44] J. Lenz. [Ηλεκτρονικό]. Available: https://www.linkedin.com/feed/update/urn:li:activity:7187083041876385793/. [Πρόσβαση Σεπτέμβριος 2024].

[45] «European Digital Identity (EUDI) Regulation | Shaping Europe’s digital future,» [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation. [Πρόσβαση Σεπτέμβριος 2024].

[46] «What are the Large Scale Pilots,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects. [Πρόσβαση Σεπτέμβριος 2024].

[47] «EU Digital Identity Wallet Toolbox Process | Shaping Europe’s digital future,» [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox. [Πρόσβαση Σεπτέμβριος 2024].

[48] «EU Digital Identity Wallet Pilot implementation | Shaping Europe’s digital future,» [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation. [Πρόσβαση Σεπτέμβριος 2024].

[49] «Potential - For European Digital Identity,» [Ηλεκτρονικό]. Available: https://www.digital-identity-wallet.eu/. [Πρόσβαση Σεπτέμβριος 2024].

[50] «Our Project - EUDI-Wallets / eIDAS 2,» [Ηλεκτρονικό]. Available: https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/en/projekt/. [Πρόσβαση September 2024].

[51] «EUDI WALLET Prototypes | SPRIND,» [Ηλεκτρονικό]. Available: https://www.sprind.org/en/challenges/eudi-wallet-prototypes/. [Πρόσβαση Σεπτέμβριος 2024].

[52] «Home - EUDI Wallet Consortium,» [Ηλεκτρονικό]. Available: https://eudiwalletconsortium.org/. [Πρόσβαση Σεπτέμβριος 2024].

[53] «Digital Credentials for Europe | DC4EU,» [Ηλεκτρονικό]. Available: https://www.dc4eu.eu/.

[54] «Welcome to the NOBID Consortium,» [Ηλεκτρονικό]. Available: https://www.nobidconsortium.com/. [Πρόσβαση Σεπτέμβριος 2024].

[55] «Benefits - EU Digital Identity Wallets,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Benefits. [Πρόσβαση Σεπτέμβριος 2024].

[56] «European Digital Identity Wallet | Shaping Europe’s digital future,» [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/factpages/european-digital-identity-wallet. [Πρόσβαση Σεπτέμβριος 2024].

[57] «European Digital Identity Architecture and Reference Framework – Outline | Shaping Europe’s digital future,» 22 Φεβρουάριος 2022. [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline. [Πρόσβαση Σεπτέμβριος 2024].

[58] «The Europen Digital Identity Wallet Architecture and Reference Framework - Version 1.0.0».

[59] «The Europen Digital Identity Wallet Architecture and Reference Framework - Version 1.1.0».

[60] «The Europen Digital Identity Wallet Architecture and Reference Framework - Version 1.2.0».

[61] «The Europen Digital Identity Wallet Architecture and Reference Framework - Version 1.3.0».

[62] «The Europen Digital Identity Wallet Architecture and Reference Framework - Version 1.4.0».

[63] C. f. E. W. C. Paolo De Rosa, «Standardising the EU Digital Identity (EUDI) Wallet Ecosystem,» 2024.

[64] «How OpenID Connect Works - OpenID Foundation,» [Ηλεκτρονικό]. Available: https://openid.net/developers/how-connect-works/. [Πρόσβαση Σεπτέμβριος 2024].

[65] «OpenID for Verifiable Credentials - Overview | OpenID Foundation,» [Ηλεκτρονικό]. Available: https://openid.net/sg/openid4vc/. [Πρόσβαση Σεπτέμβριος 2024].

[66] «Foundation - OpenID Foundation,» [Ηλεκτρονικό]. Available: https://openid.net/foundation/. [Πρόσβαση Σεπτέμβριος 2024].

[67] «OpenID for Verifiable Credentials - Specifications - OpenID Foundation,» [Ηλεκτρονικό]. Available: https://openid.net/sg/openid4vc/specifications/. [Πρόσβαση Σεπτέμβριος 2024].

[68] «OpenID for Verifiable Credentials A Shift in the Trust Model Brought by Verifiable Credentials White Paper, Version 2nd Editor's Draft,» OpenID, 2022.

[69] «ISO/IEC DIS 18013-5(en), Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application,» [Ηλεκτρονικό]. Available: https://inen.isolutions.iso.org/obp/ui#iso:std:iso-iec:18013:-5:dis:ed-1:v1:en. [Πρόσβαση Σεπτέμβριος 2024].

[70] «Verifiable Credentials Data Model v1.1,» 3 Μάρτιος 2022. [Ηλεκτρονικό]. Available: https://www.w3.org/TR/vc-data-model/. [Πρόσβαση Σεπτέμβριος 2024].

[71] «Verifiable Credentials Data Model v2.0,» Οκτώβριος 2024. [Ηλεκτρονικό]. Available: https://www.w3.org/TR/vc-data-model-2.0/. [Πρόσβαση Οκτώβριος 2024].

[72] [Ηλεκτρονικό]. Available: https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-01.html.

[73] N. Evangelos SAKKOPOULOS, «EUDI Wallet open-source repositories Overview,» 2024.

[74] L. Dr.Ignacio Alamillo-Domingo, «LS Pilots: DC4EU and standardisation,» 2024.

[75] V. M. –. I. Group, «EWC & Standardisation,» 2024.

[76] S. Jon Ølnes, «NOBID Large-Scale Pilot and Standardization,» 2024.

[77] P. N. &. S. Mouille, «POTENTIAL LSP contribution,» 2024.

[78] R. D. Chiara, «European Digital Identity Wallet: the PID and its Big Problem | LinkedIn,» Μάιος 2024. [Ηλεκτρονικό]. Available: https://www.linkedin.com/pulse/european-digital-identity-wallet-pid-its-big-problem-de-chiara-uxi8f. [Πρόσβαση Σεπτέμβριος 2024].

[79] T. F. T. A. Antti Kettunen, «EWC: Exploring Trust Models in the EUDI ecosystem,» 2024.

[80] L. Dr.Ignacio Alamillo-Domingo, «Trust models: Distributed trust,» 2024.

[81] A. Tobin, 14 Φεβρουάριος 2023. [Ηλεκτρονικό]. Available: https://www.linkedin.com/pulse/eu-wallet-depth-1-trusted-lists-andrew-tobin/. [Πρόσβαση Σεπτέμβριος 2024].

[82] epicenter.works, «Data Protection Analysis - eIDAS Architecture Reference Framework 1.4,» 2024.

[83] epicenter.works, *eIDAS - European eID Implementation Open Letter,* 2024.

[84] O. B. J. C. J.-H. H. E. L. A. L. A. L. R. M. H. M. N. K. N. B. P. a. s. D. S. S. T. S. E. T. C. T. Carsten Baum, *Cryptographers' Feedback on the EU Digital Identity's ARF,* June 2024.

[85] [Ηλεκτρονικό]. Available: What is eID (europa.eu).

[86] [Ηλεκτρονικό]. Available: Who is involved in eID? (europa.eu).

[87] [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects.

[88] [Ηλεκτρονικό]. Available: https://epicenter.works/en/about-us.

[89] «Internal market - EUR-Lex,» [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/summary/chapter/24.html. [Πρόσβαση Σεπτέμβριος 2024].

[90] «About us,» [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/About+us. [Πρόσβαση Σεπτέμβριος 2024].

[91] E. Commission, «EU Login Authentication System Connected to the eIDAS Network,» 2017. [Ηλεκτρονικό]. Available: https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=533365618. [Πρόσβαση Σεπτέμβριος 2024].

[92] «Δικαίωμα στη φορητότητα των δεδομένων | Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,» [Ηλεκτρονικό]. Available:

https://www.dpa.gr/el/polites/gkpd/dikaiwma_foritotitas_dedomenwn. [Πρόσβαση Σεπτέμβριος 2024].

[93] «Συχνές ερωτήσεις | Τυποποιημένα έντυπα για τα δικαιώματα κοινωνικής ασφάλισης - Your Europe,» [Ηλεκτρονικό]. Available: https://europa.eu/youreurope/citizens/work/unemployment-and-benefits/social-security-forms/faq/index_el.htm.

[94] J. H. a. M. Jansen, «What is an eSIM? Here’s everything you need to know | Digital Trends,» 19 Μάρτιος 2024. [Ηλεκτρονικό]. Available: https://www.digitaltrends.com/mobile/esim-explainer/. [Πρόσβαση Σεπτέμβριος 2024].

[95] «What is eUICC and why is it important for IoT? | Eseye,» 8 Ιούλιος 2020. [Ηλεκτρονικό]. Available: https://www.eseye.com/resources/iot-explained/what-is-euicc/. [Πρόσβαση Σεπτέμβριος 2024].

[96] «SIM, EcoSIM, eSIM and Secure Elements (2024 Portfolio),» [Ηλεκτρονικό]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements. [Πρόσβαση Σεπτέμβριος 2024].