ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

“ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ & ΥΠΗΡΕΣΙΕΣ”

Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet): Λειτουργικότητα, Αρχιτεκτονική και Πρωτότυπη Υλοποίηση

Από

Δημήτριο Μανωλόπουλο

Υποβάλλεται

για την εκπλήρωση των προϋποθέσεων λήψης

Μεταπτυχιακού Διπλώματος

Στην ειδίκευση «Προηγμένα Πληροφοριακά Συστήματα»

του ΠΜΣ “Πληροφοριακά Συστήματα & Υπηρεσίες”

στο

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Φεβρουάριος 2026

Επιβλέπουσα: Ανδριάνα Πρέντζα

Ακαδημαϊκή θέση: Καθηγήτρια

ΣΕΛΙΔΑ ΕΓΚΥΡΟΤΗΤΑΣ

Ονοματεπώνυμο Φοιτητή: Μανωλόπουλος Δημήτριος

Τίτλος Μεταπτυχιακής Διπλωματικής Εργασίας: Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet): Λειτουργικότητα, Αρχιτεκτονική και Πρωτότυπη Υλοποίηση

Η παρούσα Μεταπτυχιακή Διπλωματική Εργασία υποβάλλεται ως μερική εκπλήρωση των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών "Πληροφοριακά Συστήματα & Υπηρεσίες" του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς και εγκρίθηκε στις 25/2/2026 από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή

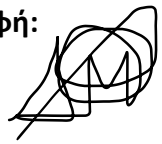
Επιβλέπουσα (Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς): Ανδριάνα Πρέντζα, Καθηγήτρια
Μέλος Εξεταστικής Επιτροπής: Μιχαήλ Φιλιππάκης, Καθηγητής
Μέλος Εξεταστικής Επιτροπής: Ανδρέας Μενύχτας, Επίκουρος Καθηγητής

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

Ο Δημήτριος Μανωλόπουλος, γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet): Λειτουργικότητα, Αρχιτεκτονική και Πρωτότυπη Υλοποίηση», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.
Επιπλέον *δηλώνω υπεύθυνα ότι η συγκεκριμένη Μεταπτυχιακή Διπλωματική Εργασία έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει αξιολογηθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου. Σε κάθε περίπτωση, αναληθούς ή ανακριβούς δηλώσεως, υπόκειμαι στις συνέπειες που προβλέπονται τις διατάξεις που προβλέπει η Ελληνική και Κοινοτική Νομοθεσία περί πνευματικής ιδιοκτησίας.*

Ο ΔΗΛΩΝ

Ονοματεπώνυμο: Δημήτριος Μανωλόπουλος
Αριθμός Μητρώου: ΜΕ2345
Υπογραφή:



Ευχαριστίες

Θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη στην επιβλέπουσα καθηγήτρια, κυρία Ανδριάνα Πρέντζα, για την αφοσιωμένη καθοδήγηση, την επιστημονική της κατάρτιση και την ουσιαστική συμβολή της τόσο στον σχεδιασμό όσο και στην υλοποίηση της παρούσας διπλωματικής εργασίας. Η διακριτική αλλά σταθερή της παρουσία υπήρξε καταλυτική στην εξέλιξή μου ως ερευνητής και φοιτητής. Παράλληλα, θα ήθελα να ευχαριστήσω από καρδιάς τον φίλο και συνοδοιπόρο σε αυτή τη διαδρομή, Περικλή Βαϊρακταρίδη, για την έμπρακτη συμπαράσταση, τη συνεργασία και την ειλικρινή του διάθεση για βοήθεια, στοιχεία που αποδείχθηκαν ανεκτίμητα σε κρίσιμες στιγμές της διαδικασίας. Ομοίως, αισθάνομαι βαθιά υποχρεωμένος απέναντι στη σύντροφό μου, η οποία με αστείρευτη υπομονή και διαρκή ενθάρρυνση με στήριξε σε κάθε στάδιο αυτής της διαρκούς προσπάθειας που θύμισε μαραθώνιο. Τέλος, η στήριξη και η παρουσία της οικογένειάς μου αποτέλεσαν ένα σταθερό σημείο αναφοράς, προσφέροντάς μου την ψυχική ηρεμία και το αίσθημα ασφάλειας που ήταν απαραίτητα για την ολοκλήρωση του εγχειρήματος.

Πίνακας περιεχομένων

Λίστα εικόνων

Λίστα Πινάκων

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet) ως κρίσιμο πυλώνα του ευρωπαϊκού πλαισίου ψηφιακής ταυτότητας στο πλαίσιο του eIDAS 2.0 και διερευνά πώς μπορεί να υποστηρίξει ασφαλή και διαλειτουργική ηλεκτρονική ταυτοποίηση σε διασυνοριακά σενάρια. Στο θεωρητικό μέρος παρουσιάζονται οι βασικές έννοιες της ψηφιακής ταυτοποίησης και των ψηφιακών διαπιστευτηρίων, οι ρόλοι του οικοσυστήματος (Issuer–Holder/Wallet–Verifier) και οι τρόποι αλληλεπίδρασης σε απομακρυσμένα σενάρια και σενάρια εγγύτητας, με αναφορά σε πρότυπα όπως OpenID4VP και ISO/IEC 18013-5 (mdoc/mDL). Κεντρικό σημείο αναφοράς αποτελεί το Architecture and Reference Framework (ARF) του EUDI Wallet, καθώς λειτουργεί ως ο βασικός τεχνικός “οδικός χάρτης” που συγκεντρώνει προδιαγραφές, αρχιτεκτονικές αρχές και απαιτήσεις για διαλειτουργικότητα, ασφάλεια και προστασία ιδιωτικότητας στο οικοσύστημα του πορτοφολιού.

Για τη γεφύρωση θεωρίας και πράξης αναπτύσσεται ένα εκπαιδευτικό πρωτότυπο web εφαρμογής σε Python/Flask, που προσομοιώνει τους ρόλους Issuer, Wallet, Verifier και ένα υποσύστημα “Mock Certificates”. Τα διαπιστευτήρια υλοποιούνται ως JWT, η κατάσταση διαχειρίζεται με sessions (χωρίς βάση δεδομένων), ενώ ο Verifier επαληθεύει υπογραφή και χρονική ισχύ, αποτυπώνοντας καθαρά το αποτέλεσμα επικύρωσης. Τέλος, καταγράφονται περιορισμοί και προτείνονται επεκτάσεις όπως ασύμμετρη κρυπτογραφία, πιο άμεση ευθυγράμμιση με OpenID4VCI/OpenID4VP, επιλεκτική αποκάλυψη και μηχανισμοί ανάκλησης/συμμόρφωσης.

Η συνολική προσέγγιση στηρίζεται σε στοχευμένη βιβλιογραφική και τεχνική έρευνα, ώστε οι επιλογές σχεδίασης του πρωτοτύπου να ευθυγραμμίζονται με τις σύγχρονες κατευθύνσεις του ευρωπαϊκού οικοσυστήματος ψηφιακής ταυτότητας.

Λέξεις κλειδιά

EUDI Wallet, eIDAS 2.0, ψηφιακή ταυτότητα, διαλειτουργικότητα, προστασία δεδομένων, ARF, διαπιστευτήρια, Issuer–Holder–Verifier.

Abstract

This master's thesis examines the European Digital Identity Wallet (EUDI Wallet) as a critical pillar of the European digital identity framework within the context of eIDAS 2.0 and investigates how it can support secure and interoperable electronic identification in cross-border scenarios. The theoretical part presents the core concepts of digital identification and digital credentials, the roles of the ecosystem (Issuer–Holder/Wallet–Verifier), and the modes of interaction in remote and proximity scenarios, with reference to standards such as OpenID4VP and ISO/IEC 18013-5 (mdoc/mDL). A central point of reference is the EUDI Wallet Architecture and Reference Framework (ARF), as it functions as the main technical "roadmap" that consolidates specifications, architectural principles, and requirements for interoperability, security, and privacy protection within the wallet ecosystem.

To bridge theory and practice, an educational prototype web application is developed in Python/Flask, which simulates the roles of Issuer, Wallet, Verifier, and a "Mock Certificates" subsystem. The credentials are implemented as JWTs, state is managed with sessions (without a database), and the Verifier validates the signature and temporal validity, clearly presenting the validation outcome. Finally, limitations are documented and extensions are proposed, such as asymmetric cryptography, closer alignment with OpenID4VCI/OpenID4VP, selective disclosure, and revocation/compliance mechanisms.

The overall approach is based on targeted bibliographic and technical research, so that the design choices of the prototype align with contemporary directions of the European digital identity ecosystem.

Keywords

EUDI Wallet, eIDAS 2.0, digital identity, interoperability, data protection, ARF, credentials, Issuer–Holder–Verifier.

1. Εισαγωγή

Η ψηφιακή ταυτότητα και η αξιόπιστη ηλεκτρονική ταυτοποίηση αποτελούν πλέον θεμέλιο για την παροχή σύγχρονων ψηφιακών υπηρεσιών τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Καθώς αυξάνονται οι ηλεκτρονικές συναλλαγές, η ανάγκη για ασφαλείς μηχανισμούς αναγνώρισης χρηστών, προστασίας προσωπικών δεδομένων και διαλειτουργικότητας μεταξύ διαφορετικών φορέων γίνεται εντονότερη. Στο πλαίσιο αυτό, η Ευρωπαϊκή Ένωση προωθεί μια ενοποιημένη προσέγγιση μέσω της αναβάθμισης του κανονιστικού πλαισίου eIDAS και της εισαγωγής του Ευρωπαϊκού Πορτοφολιού ψηφιακής Ταυτότητας (European Digital Identity Wallet – EUDI Wallet), με στόχο μια κοινή, διασυνοριακά αποδεκτή και περισσότερο «χρήστη-κεντρική» ψηφιακή εμπειρία ταυτοποίησης και ανταλλαγής διαπιστευτηρίων [3].

1.1. Αντικείμενο και Σκοπός της έρευνας

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη του Ευρωπαϊκού Πορτοφολιού ψηφιακής Ταυτότητας (EUDI Wallet), εστιάζοντας στη λειτουργικότητα, στο οικοσύστημα και στις αρχιτεκτονικές αρχές που το υποστηρίζουν. Το EUDI Wallet αντιμετωπίζεται ως μια νέα γενιά «πορτοφολιού ψηφιακής ταυτότητας», το οποίο δεν περιορίζεται στην αποθήκευση απλών στοιχείων χρήστη, αλλά στοχεύει να επιτρέψει την ασφαλή διαχείριση και παρουσίαση ψηφιακών διαπιστευτηρίων (credentials/attestations) σε πολλαπλά σενάρια χρήσης, διατηρώντας την απαίτηση για υψηλή εμπιστοσύνη και προστασία δεδομένων [1].

Ο σκοπός της έρευνας είναι τριπλός. Πρώτον, να εδραιωθεί η απαραίτητη εννοιολογική βάση γύρω από την ψηφιακή ταυτότητα, την ηλεκτρονική ταυτοποίηση και τον ρόλο των ψηφιακών πορτοφολιών. Δεύτερον, να παρουσιαστεί και να αναλυθεί το EUDI Wallet ως τεχνολογική και θεσμική πρωτοβουλία, αναδεικνύοντας τους βασικούς ρόλους του οικοσυστήματος (Issuer, Holder/Wallet, Verifier/Relying Party) και τις ροές έκδοσης, παρουσίασης και επαλήθευσης διαπιστευτηρίων, τόσο σε σενάρια «εγγύτητας» (proximity) όσο και σε σενάρια απομακρυσμένης αλληλεπίδρασης [3]. Τρίτον, να γεφυρωθεί η θεωρία με την πράξη μέσω της ανάπτυξης ενός λειτουργικού πρωτοτύπου, το οποίο προσομοιώνει με απλό και κατανοητό

τρόπο την ανταλλαγή και την επαλήθευση ψηφιακών διαπιστευτηρίων, ώστε να αποκτηθεί πρακτική κατανόηση της λογικής και των βασικών μηχανισμών ενός σύγχρονου πορτοφολιού ταυτοποίησης.

1.2. Μεθοδολογία της διπλωματικής εργασίας

Η μεθοδολογία που ακολουθήθηκε συνδυάζει βιβλιογραφική έρευνα, ανάλυση κανονιστικού πλαισίου, συγκριτική αξιολόγηση και πρακτική υλοποίηση. Αρχικά πραγματοποιείται βιβλιογραφική ανασκόπηση και αποσαφήνιση βασικών εννοιών σχετικά με την ψηφιακή ταυτότητα, την ηλεκτρονική ταυτοποίηση και τα ψηφιακά πορτοφόλια, ώστε να τεκμηριωθεί το θεωρητικό υπόβαθρο πάνω στο οποίο «χτίζεται» η υπόλοιπη εργασία [1]. Στη συνέχεια, εξετάζεται το EUDI Wallet ως έννοια και ως οικοσύστημα, ενώ παράλληλα πραγματοποιείται συγκριτική προσέγγιση ανάμεσα στο EUDI Wallet και σε καθιερωμένες εμπορικές λύσεις πορτοφολιών, με στόχο να αναδειχθούν διαφορές στη φιλοσοφία, στις δυνατότητες, στις προκλήσεις και στα πιθανά οφέλη για πολίτες και φορείς [1].

Παράλληλα, γίνεται ανάλυση του κανονιστικού πλαισίου eIDAS, αρχικά ως eIDAS 1.0 και στη συνέχεια ως αναθεωρημένο eIDAS 2.0, ώστε να αποτυπωθεί πώς το θεσμικό πλαίσιο επηρεάζει την υλοποίηση, τις απαιτήσεις συμμόρφωσης και τις προβλεπόμενες χρήσεις του EUDI Wallet [3], [14]. Η μεθοδολογική προσέγγιση ολοκληρώνεται με την ανάπτυξη ενός πρωτοτύπου πορτοφολιού ψηφιακής ταυτοποίησης, το οποίο δεν στοχεύει σε παραγωγική/εμπορική χρήση, αλλά λειτουργεί ως πρακτική επιβεβαίωση της θεωρίας: αποτυπώνει βασικές ροές (έκδοση, αποθήκευση, παρουσίαση, επαλήθευση) και επιτρέπει την κατανόηση σχεδιαστικών επιλογών και περιορισμών σε ένα ελεγχόμενο περιβάλλον.

1.3. Δομή της διπλωματικής εργασίας

Η εργασία οργανώνεται σε κεφάλαια που προχωρούν από τις βασικές έννοιες προς την κανονιστική/αρχιτεκτονική ανάλυση και, τέλος, προς την υλοποίηση. Μετά το Κεφάλαιο 1 της εισαγωγής, στο Κεφάλαιο 2 παρουσιάζονται οι βασικές έννοιες της ψηφιακής ταυτότητας και της ηλεκτρονικής ταυτοποίησης, ο ορισμός και οι λειτουργίες των ψηφιακών πορτοφολιών,

καθώς και μια συνοπτική επισκόπηση εμπορικών ψηφιακών πορτοφολιών, με στόχο να τεθεί η εννοιολογική βάση της μελέτης. Στο Κεφάλαιο 3 αναπτύσσεται το θεωρητικό υπόβαθρο γύρω από τα σύγχρονα ψηφιακά πορτοφόλια, παρουσιάζεται το EUDI Wallet ως προσέγγιση, πραγματοποιείται συγκριτική αξιολόγηση με εμπορικές λύσεις και καταγράφονται προκλήσεις και πλεονεκτήματα. Στο Κεφάλαιο 4 αναλύεται το κανονιστικό πλαίσιο eIDAS, παρουσιάζοντας τη μετάβαση από το eIDAS 1.0 στο eIDAS 2.0 και τη σημασία της εξέλιξης αυτής για το EUDI Wallet και τις εφαρμογές του.

Στο Κεφάλαιο 5 εστιάζουμε στη λειτουργικότητα και την αρχιτεκτονική του EUDI Wallet, παρουσιάζοντας το οικοσύστημα, τους εμπλεκόμενους ρόλους, τις ροές έκδοσης/παρουσίασης διαπιστευτηρίων και την αρχιτεκτονική υψηλού επιπέδου που υποστηρίζει τα βασικά σενάρια χρήσης. Στο Κεφάλαιο 6 παρουσιάζεται η πρόταση υλοποίησης και αναλύεται ένα λειτουργικό πρωτότυπο, περιγράφοντας την αρχιτεκτονική, τα επιμέρους υποσυστήματα και τις τεχνικές επιλογές/περιορισμούς, καθώς και δυνατότητες μελλοντικής επέκτασης και βελτίωσης. Τέλος, στο Κεφάλαιο 7 συνοψίζονται τα συμπεράσματα της εργασίας και παρουσιάζονται προοπτικές για μελλοντική εξέλιξη και περαιτέρω έρευνα.

2. Βασικές Έννοιες και Βιβλιογραφική Ανασκόπηση

Η ταχεία ψηφιοποίηση των οικονομικών συναλλαγών και των δημόσιων υπηρεσιών έχει δημιουργήσει την ανάγκη για ασφαλείς, διαλειτουργικές και εύχρηστες λύσεις ηλεκτρονικής ταυτοποίησης. Στο πλαίσιο αυτό, τα *ψηφιακά πορτοφόλια (digital wallets)* αποτελούν πλέον κεντρικό μηχανισμό διαχείρισης ψηφιακών ταυτοτήτων, διαπιστευτηρίων και μέσων πληρωμής [1]. Η κατανόηση των θεμελιωδών εννοιών γύρω από τα ψηφιακά πορτοφόλια, καθώς και η εξέλιξη της βιβλιογραφίας σχετικά με την ταυτοποίηση, την ασφάλεια και τις διεθνείς προσεγγίσεις, αποτελεί θεμέλιο για την ανάλυση και τη μελέτη του Ευρωπαϊκού Πορτοφολιού ψηφιακής Ταυτότητας (EUDI Wallet).

2.1. Βασικές Έννοιες Ψηφιακής Ταυτότητας και Ηλεκτρονικής Ταυτοποίησης

Η έννοια της *ψηφιακής ταυτότητας (digital identity)* ορίζεται ως το σύνολο ηλεκτρονικών πληροφοριών που αναγνωρίζουν μοναδικά ένα άτομο ή οργανισμό σε ψηφιακό περιβάλλον [2]. Στο ευρωπαϊκό πλαίσιο, ο κανονισμός eIDAS ορίζει την *ηλεκτρονική ταυτοποίηση (eID)* ως τη διαδικασία σύνδεσης ενός φυσικού προσώπου με δεδομένα ταυτοποίησης σε ηλεκτρονική μορφή, που επιτρέπουν την πρόσβαση σε υπηρεσίες με ασφαλή και νομικά αναγνωρισμένο τρόπο [3].

Η *ηλεκτρονική αυθεντικοποίηση (authentication)* είναι η διαδικασία επαλήθευσης ότι ο χρήστης που παρουσιάζει τα διαπιστευτήριά του είναι πράγματι ο νόμιμος κάτοχος αυτών. Οι μέθοδοι αυθεντικοποίησης περιλαμβάνουν κωδικούς πρόσβασης, one-time passwords (OTP), βιομετρικά δεδομένα, καθώς και κρυπτογραφικές τεχνικές βασισμένες σε δημόσια και ιδιωτικά κλειδιά [4].

Διεθνώς, η ερευνητική βιβλιογραφία καταγράφει μία ισχυρή μετάβαση προς μοντέλα *Self-Sovereign Identity (SSI)*, στα οποία ο χρήστης διατηρεί τον πλήρη έλεγχο των δεδομένων του και αποκαλύπτει μόνο το απολύτως απαραίτητο σύνολο χαρακτηριστικών μέσω τεχνικών *selective disclosure* και *zero-knowledge proofs [5].*

2.2. Ψηφιακά Πορτοφόλια: Ορισμός, Ρόλος και Λειτουργίες

Τα ψηφιακά πορτοφόλια αποτελούν εφαρμογές λογισμικού που επιτρέπουν την αποθήκευση, διαχείριση και παρουσίαση διαπιστευτηρίων, την αυθεντικοποίηση σε υπηρεσίες και τη διενέργεια πληρωμών σε ασφαλές περιβάλλον [6].

Σύμφωνα με τις προδιαγραφές του W3C, ένα σύγχρονο πορτοφόλι μπορεί να αποθηκεύει και να παρουσιάζει *Verifiable Credentials,* στο πλαίσιο αποκεντρωμένων μοντέλων ταυτότητας [7].

Οι βασικές λειτουργίες περιλαμβάνουν:

- Αποθήκευση διαπιστευτηρίων (π.χ. ταυτότητα, άδεια οδήγησης, εισιτήρια)
- Ηλεκτρονική αυθεντικοποίηση χρήστη
- Υποστήριξη ηλεκτρονικών πληρωμών

- Επιλεκτική αποκάλυψη στοιχείων (selective disclosure)
- Κρυπτογραφική υπογραφή

Αυτά συνθέτουν τις θεμελιακές λειτουργίες πάνω στις οποίες συγκρίνονται τα εμπορικά και τα θεσμικά πορτοφόλια.

2.3. Εμπορικά Ψηφιακά Πορτοφόλια

Πριν παρουσιαστεί το EUDI Wallet, είναι απαραίτητο να παρουσιαστούν οι κυριότερες εμπορικές λύσεις, ώστε στο Κεφάλαιο 3 να υπάρχει πλήρες υπόβαθρο για συγκριτική αξιολόγηση.

Apple Wallet

Το Apple Wallet λειτουργεί εντός του οικοσυστήματος iOS και βασίζεται σε κρυπτογραφική προστασία μέσω Secure Enclave [8]. Επιτρέπει την αποθήκευση καρτών πληρωμής, εισιτηρίων, boarding passes, loyalty cards. Παρά το υψηλό επίπεδο ασφάλειας, δεν παρέχει νομική αναγνώριση για επίσημη ηλεκτρονική ταυτοποίηση.

Google Wallet

Το Google Wallet αποτελεί την αντίστοιχη λύση για Android συσκευές. Υποστηρίζει πληρωμές, εισιτήρια και κάρτες, ενώ σε ορισμένες χώρες επιτρέπει mobile IDs. Ωστόσο δεν διαθέτει νομική ισχύ στην ΕΕ για επίσημες συναλλαγές και δεν συμμορφώνεται με ευρωπαϊκές απαιτήσεις eIDAS [9], [14].

Samsung Wallet

Το Samsung Wallet, παρόμοια λύση ενσωματωμένη σε συσκευές Samsung, καλύπτει λειτουργίες πληρωμών και διαχείρισης καρτών, αλλά δεν προσφέρει επίσημη ταυτοποίηση με νομική ισχύ [10].

Wallets τρίτων εταιρειών (Revolut, PayPal κ.λ.π.)

Επικεντρώνονται κυρίως σε τραπεζικές συναλλαγές, αναγνωρίζονται για τις πληρωμές και τη χρηστικότητα, αλλά δεν εποπτεύονται από δημόσια αρχή και δεν αποτελούν λύσεις ταυτοποίησης [11].

Συνολικά λοιπόν, τα εμπορικά πορτοφόλια:

- λειτουργούν εντός ιδιωτικών οικοσυστημάτων,
- δεν πληρούν τις απαιτήσεις eIDAS,
- δεν προσφέρουν privacy-by-design σε επίπεδο κανονισμού,
- και δεν διαθέτουν νομικά ισχυρή ταυτοποίηση [1], [8]–[11].

Αυτοί οι περιορισμοί δημιούργησαν την ανάγκη για ένα ενιαίο, θεσμικά εποπτευόμενο, διαλειτουργικό και νομικά αναγνωρισμένο πορτοφόλι ψηφιακής ταυτότητας: το EUDI Wallet.

2.4. Βιβλιογραφική Ανασκόπηση για την Ηλεκτρονική Ταυτοποίηση

Η διεθνής βιβλιογραφία αναδεικνύει την ανάγκη για ασφαλείς ηλεκτρονικές ταυτότητες, λόγω της αύξησης των διαδικτυακών συναλλαγών και των απαιτήσεων κυβερνοασφάλειας και για σταδιακή μετάβαση από τα συμβατικά wallets πληρωμών σε wallets πολλαπλών λειτουργιών μέσω ισχυρών μηχανισμών σύγκλισης τεχνολογικών και νομικών προϋποθέσεων.

Πιο συγκεκριμένα επισημαίνει τα εξής:

1. Υψηλή ανάγκη ασφαλούς ψηφιακής ταυτοποίησης λόγω της αύξησης των κυβερνοαπειλών [1].
2. Περιορισμένη διαλειτουργικότητα των εθνικών eID συστημάτων πριν τον eIDAS 2.0 [3].
3. Στροφή σε αποκεντρωμένα standards όπως τα Verifiable Credentials και το ISO 18013-5 για mobile IDs [7], [12].
4. Ανάγκη κοινής αρχιτεκτονικής αναφοράς για εναρμόνιση (ARF) [13].
5. Ενδυνάμωση του χρήστη μέσω privacy-preserving τεχνολογιών όπως ZKPs [5].

Το EUDI Wallet σχεδιάστηκε ακριβώς για να καλύψει αυτά τα κενά.

Η ανάλυση των βασικών εννοιών, της βιβλιογραφίας και των εμπορικών λύσεων θέτει τις βάσεις για μία ολοκληρωμένη κατανόηση του οικοσυστήματος των ψηφιακών πορτοφολιών. Στο επόμενο κεφάλαιο παρουσιάζεται το *EUDI Wallet,* το οποίο διαφοροποιείται ριζικά από τις εμπορικές λύσεις τόσο σε τεχνολογικό όσο και σε θεσμικό επίπεδο.

3. Θεωρητικό Υπόβαθρο

Το θεωρητικό υπόβαθρο της εργασίας εστιάζει στην κατανόηση των βασικών τεχνολογικών, αρχιτεκτονικών και λειτουργικών παραμέτρων που καθορίζουν το οικοσύστημα των σύγχρονων ψηφιακών πορτοφολιών. Η κατανόηση αυτών των εννοιών είναι απαραίτητη για την αξιολόγηση του Ευρωπαϊκού Πορτοφολιού ψηφιακής Ταυτότητας (EUDI Wallet) και τη σύγκρισή του με υπάρχουσες εμπορικές λύσεις [1].

Το παρόν κεφάλαιο αναφέρεται στις θεμελιώδεις θεωρητικές και πρακτικές διαστάσεις του Ευρωπαϊκού Ψηφιακού Πορτοφολιού, αναλύοντας τις αρχές, τη λειτουργικότητά του, τις προκλήσεις που αντιμετωπίζει για την επίτευξη των φιλόδοξων στόχων του και τα πλεονεκτήματα που προκύπτουν για πολίτες και φορείς.

3.1. Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet)

Στην ολοένα και περισσότερο ψηφιοποιημένη παγκόσμια οικονομία, τα ψηφιακά πορτοφόλια έχουν αναδειχθεί σε βασικά εργαλεία για τη διευκόλυνση απρόσκοπτων συναλλαγών, την ασφαλή επαλήθευση της ταυτότητας και την ενσωμάτωση στα χρηματοπιστωτικά οικοσυστήματα. Μεταξύ αυτών των καινοτομιών, η πρωτοβουλία European Digital (EUDI) Wallet αποτελεί μια προσπάθεια ορόσημο της Ευρωπαϊκής Ένωσης (ΕΕ) για την ενοποίηση των συστημάτων ψηφιακής ταυτότητας και πληρωμών σε ένα ενιαίο, διαλειτουργικό πλαίσιο. Το EUDI Wallet, το οποίο δρομολογήθηκε στο πλαίσιο της στρατηγικής ψηφιακού μετασχηματισμού της ΕΕ, έχει ως στόχο να παρέχει μια ασφαλή και αποτελεσματική πλατφόρμα λειτουργώντας ως *ενιαίο σημείο ταυτοποίησης* σε όλη την ΕΕ, υποστηρίζοντας *ασφαλή διαλειτουργικότητα* ανάμεσα στα κράτη μέλη, καλύπτοντας *δημόσιες και ιδιωτικές υπηρεσίες*,

δίνοντας *πλήρη έλεγχο στον πολίτη* και ελαχιστοποιώντας την αποκάλυψη περιττών δεδομένων χάρη στην τεχνολογία *zero-knowledge proofs* [5].

Τα ψηφιακά πορτοφόλια λειτουργούν με βάση τις θεμελιώδεις αρχές της ασφαλούς, user-centric τεχνολογίας, επιτρέποντας στους χρήστες να αποθηκεύουν διαπιστευτήρια, να έχουν πρόσβαση σε υπηρεσίες και να πραγματοποιούν συναλλαγές. Στο επίκεντρο του EUDI Wallet βρίσκεται η αρχή της διαλειτουργικότητας, η οποία επιβάλλεται από τον κανονισμό eIDAS 2.0 της ΕΕ (Ηλεκτρονική ταυτοποίηση, πιστοποίηση ταυτότητας και υπηρεσίες εμπιστοσύνης) [14]. Αυτό το πλαίσιο διασφαλίζει ότι τα ψηφιακά πορτοφόλια πληρούν αυστηρά κριτήρια για την ασφάλεια, την προστασία της ιδιωτικής ζωής των δεδομένων και τη διασυνοριακή αναγνώριση.

Τα κρυπτογραφικά πρωτόκολλα διαδραματίζουν κεντρικό ρόλο στην ασφάλεια του EUDI Wallet, διασφαλίζοντας ότι τα ευαίσθητα δεδομένα κρυπτογραφούνται και παραμένουν απρόσιτα σε μη εξουσιοδοτημένα μέρη. Οι αναδυόμενες τεχνολογίες, όπως το blockchain, ενισχύουν περαιτέρω την εμπιστοσύνη παρέχοντας αμετάβλητα αρχεία συναλλαγών και αποκεντρωμένους μηχανισμούς επαλήθευσης. Οι προδιαγραφές για την υλοποίηση του EUDI Wallet βασίζονται στο *Architecture and Reference Framework (ARF)***,** το οποίο καθορίζει τις απαιτήσεις ασφαλείας, τα πρότυπα ανταλλαγής δεδομένων, την αρχιτεκτονική ροών, τα υποχρεωτικά interfaces καθώς και προδιαγραφές για issuers, verifiers και wallets [13].

Το ευρωπαϊκό ψηφιακό πορτοφόλι έχει σχεδιαστεί για να χρησιμεύσει ως κάτι περισσότερο από μια απλή πλατφόρμα πληρωμών. Ενσωματώνει λειτουργίες όπως η αποθήκευση ψηφιακών ταυτοτήτων, τα αρχεία υγειονομικής περίθαλψης, τα ταξιδιωτικά έγγραφα, ακόμη και την πρόσβαση σε κυβερνητικές υπηρεσίες. Αυτή η πολυλειτουργικότητα το τοποθετεί ως ένα ολοκληρωμένο εργαλείο για τις καθημερινές αλληλεπιδράσεις σε μια ψηφιακή κοινωνία.

3.2. Συγκριτική Αξιολόγηση EUDI Wallet vs Εμπορικά Wallets

Το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet), όπως ορίζεται από τον Κανονισμό (ΕΕ) 2024/1183 – eIDAS 2.0**,** διαφοροποιείται ουσιαστικά από τα εμπορικά ψηφιακά πορτοφόλια που προσφέρονται από ιδιωτικούς φορείς όπως η Apple (Apple Wallet) και η Google (Google Wallet)**.** Η διαφορά δεν περιορίζεται μόνο στην τεχνολογική υλοποίηση, αλλά

επεκτείνεται στη νομική ισχύ, την προστασία της ιδιωτικότητας και τη διακυβέρνηση του οικοσυστήματος**.**

Ο παρακάτω πίνακας παρουσιάζει τις βασικές διαφορές μεταξύ του EUDI Wallet και των εμπορικών wallets με βάση κάποια κριτήρια.

Κριτήριο	**EUDI Wallet (European Digital Identity Wallet)**	**Εμπορικά Wallets (Apple Wallet, Google Wallet)**
Νομική Ισχύς (Legal Validity)	Έχει επίσημη νομική ισχύ βάσει του Κανονισμού eIDAS 2.0 (ΕΕ 2024/1183). Τα διαπιστευτήρια που εκδίδονται μέσω EUDI αναγνωρίζονται ισότιμα με φυσικά έγγραφα σε όλα τα κράτη-μέλη της Ε.Ε.	Δεν διαθέτουν νομική ισχύ για επίσημη ταυτοποίηση ή δημόσια έγγραφα. Χρησιμοποιούνται μόνο για πληρωμές, εισιτήρια, loyalty cards ή, σε κάποιες χώρες, mobile ID χωρίς ευρωπαϊκή αναγνώριση.
Ιδιωτικότητα (Privacy)	Privacy by Design και Data Minimization. Τα δεδομένα αποθηκεύονται τοπικά στη συσκευή και ο χρήστης ελέγχει πλήρως ποια στοιχεία κοινοποιούνται. Πλήρης συμμόρφωση με GDPR.	Η προστασία εξαρτάται από τις πολιτικές των εταιρειών (Apple, Google). Ενδέχεται να χρησιμοποιούνται δεδομένα για αναλύσεις ή εμπορικούς σκοπούς. Ο έλεγχος είναι μερικός και όχι αποκλειστικά στον χρήστη.
Διακυβέρνηση (Governance)	Διοικούμενο από δημόσιους φορείς: τα κράτη-μέλη και η Ευρωπαϊκή Επιτροπή εποπτεύουν και πιστοποιούν τους παρόχους wallet. Υπάρχει κρατική λογοδοσία και διαφάνεια.	Ιδιωτική διακυβέρνηση: ανήκουν σε Apple Inc. και Google LLC, χωρίς υποχρέωση διαφάνειας ή δημόσιας εποπτείας.
Διαλειτουργικότητα (Interoperability)	Πανευρωπαϊκή διαλειτουργικότητα – αποδοχή σε όλους τους δημόσιους και ιδιωτικούς φορείς της Ε.Ε.	Περιορισμένη εντός του οικοσυστήματος της κάθε εταιρείας (Apple Pay, Google Pay), χωρίς διασυνοριακή εγγύηση συμβατότητας.
Πεδίο Εφαρμογής	Επίσημη ταυτοποίηση, ηλεκτρονική υπογραφή, πρόσβαση σε δημόσιες υπηρεσίες, ακαδημαϊκά ή επαγγελματικά διαπιστευτήρια.	Πληρωμές, boarding passes, κάρτες επιβράβευσης, εισιτήρια και, σε ορισμένες περιπτώσεις, μη αναγνωρισμένα mobile IDs.

Πίνακας 1- Σύγκριση EUDI Wallet vs Εμπορικά Wallets

Η βασική διαφοροποίηση του EUDI Wallet από τα εμπορικά πορτοφόλια [8]–[11] έγκειται στην κρατική εποπτεία και τη νομική αναγνώριση των διαπιστευτηρίων του. Ενώ οι πλατφόρμες της Apple και της Google [8], [9] επικεντρώνονται στην εμπορική ευκολία και στη χρηστικότητα εντός των δικών τους οικοσυστημάτων, το EUDI Wallet αποτελεί μέρος μιας θεσμικής υποδομής εμπιστοσύνης με πλήρη προστασία ιδιωτικότητας και συμμόρφωση με το GDPR (General Data Protection Regulation)**.** Η κυριαρχία του πολίτη πάνω στα προσωπικά του δεδομένα αποτελεί θεμελιώδη διαφορά, καθώς στο EUDI Wallet κανένα δεδομένο δεν κοινοποιείται χωρίς ρητή συναίνεση του χρήστη.

Η σύγκριση του EUDI Wallet με τα υπάρχοντα ψηφιακά πορτοφόλια αναδεικνύει τη μοναδική πρόταση αξίας του. Σε αντίθεση με εμπορικά πορτοφόλια όπως το Apple Pay ή το Google Pay, το EUDI Wallet έχει σχεδιαστεί για να είναι περιεκτικό, καλύπτοντας ένα ευρύτερο φάσμα εφαρμογών πέραν των πληρωμών. Τα διδάγματα από άλλες πρωτοβουλίες της ΕΕ, όπως ο SEPA (Ενιαίος Χώρος Πληρωμών σε Ευρώ), υπογραμμίζουν τη σημασία των σαφών ρυθμιστικών κατευθυντήριων γραμμών και της συνεργασίας των ενδιαφερομένων μερών για την επίτευξη ευρείας υιοθέτησης.

3.3. Προκλήσεις

Η υλοποίηση του ευρωπαϊκού ψηφιακού πορτοφολιού αντιμετωπίζει πολλά εμπόδια, από τεχνικά έως κοινωνικά. Οι ανησυχίες για την προστασία της ιδιωτικής ζωής είναι υψίστης σημασίας, καθώς το πορτοφόλι συγκεντρώνει ευαίσθητες προσωπικές πληροφορίες. Οι επικριτές υποστηρίζουν ότι οποιαδήποτε παραβίαση θα μπορούσε να έχει καταστροφικές συνέπειες, υπονομεύοντας την εμπιστοσύνη του κοινού στα συστήματα ψηφιακής ταυτότητας.

Η υιοθέτηση από τους χρήστες είναι μια άλλη σημαντική πρόκληση. Ενώ οι νεότερες, τεχνολογικά καταρτισμένες γενιές μπορεί να αγκαλιάσουν το πορτοφόλι, οι μεγαλύτερες ηλικίες με περιορισμένο ψηφιακό αλφαβητισμό μπορεί να αντισταθούν ή να δυσκολευτούν να το χρησιμοποιήσουν αποτελεσματικά. Η γεφύρωση αυτού του χάσματος απαιτεί στοχευμένες εκστρατείες εκπαίδευσης και προβολής.

Η διασυνοριακή λειτουργικότητα, αν και αποτελεί ακρογωνιαίο λίθο της πρωτοβουλίας, εισάγει πολυπλοκότητα. Τα διαφορετικά νομικά πλαίσια, οι γλώσσες και τα χρηματοπιστωτικά συστήματα σε ολόκληρη την ΕΕ πρέπει να εναρμονιστούν για να εξασφαλιστεί η απρόσκοπτη λειτουργία. Επιπλέον, η ενσωμάτωση του πορτοφολιού με τα υφιστάμενα συστήματα ταυτότητας, όπως οι εθνικές ταυτότητες και τα τραπεζικά δίκτυα, απαιτεί σημαντικό συντονισμό αλλά και επενδύσεις. Έτσι, ενώ το eIDAS αποτελεί σημαντικό βήμα προς την κατεύθυνση της εναρμόνισης της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης σε ολόκληρη την ΕΕ, η εφαρμογή του δημιούργησε αρκετές προκλήσεις για τα κράτη μέλη και τους ενδιαφερόμενους φορείς.

Συνοψίζοντας, ορισμένες από τις βασικές προκλήσεις είναι οι εξής:

Τεχνική διαλειτουργικότητα: Η διασφάλιση της συμβατότητας με διαφορετικές πλατφόρμες (Android, iOS) [15] καθώς και της απρόσκοπτης διαλειτουργικότητας μεταξύ διαφορετικών εθνικών συστημάτων ηλεκτρονικής ταυτότητας και υποδομών υπηρεσιών εμπιστοσύνης παραμένει ένα πολύπλοκο έργο, που απαιτεί προσπάθειες τυποποίησης και συμβατότητας.

Νομική εναρμόνιση: Η επίτευξη ομοιόμορφης ερμηνείας και εφαρμογής των διατάξεων του eIDAS σε όλα τα νομικά συστήματα των κρατών μελών απαιτεί συνεχή συντονισμό και συνεργασία μεταξύ των εθνικών αρχών και των δικαστικών οργάνων.

Κοινωνικές και Οικονομικές Προκλήσεις: Η ενθάρρυνση της ευρείας υιοθέτησης της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης μεταξύ των πολιτών, των επιχειρήσεων και των δημόσιων διοικήσεων απαιτεί εκστρατείες ευαισθητοποίησης και εκπαίδευσης, φιλικές προς το χρήστη διεπαφές και αποτελεσματικές στρατηγικές επικοινωνίας. Επιπλέον, σε οικονομικό επίπεδο απαιτούνται πλάνα διαχείρισης του κόστους υλοποίησης για τα κράτη αλλά και τους ιδιωτικούς φορείς [16].

Προβλήματα ασφάλειας και προστασίας της ιδιωτικής ζωής: Η αντιμετώπιση των ανησυχιών που σχετίζονται με την προστασία της ιδιωτικής ζωής, την ασφάλεια των προσωπικών δεδομένων υπό το GDPR [17] και τις απειλές της κυβερνοασφάλειας είναι απαραίτητη για τη διατήρηση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές και την πρόληψη της απάτης ή της κατάχρησης των ηλεκτρονικών ταυτοτήτων και υπογραφών.

3.4. Πλεονεκτήματα

Παρά τις προκλήσεις, το ευρωπαϊκό ψηφιακό πορτοφόλι προσφέρει μετασχηματιστικές ευκαιρίες. Υπόσχεται να εξορθολογήσει τις συναλλαγές και να μειώσει τον διοικητικό φόρτο τόσο για τους ιδιώτες όσο και για τις επιχειρήσεις. Για παράδειγμα, οι πολίτες μπορούν να χρησιμοποιούν το πορτοφόλι για την υποβολή φορολογικών δηλώσεων, την πρόσβαση στην υγειονομική περίθαλψη και την εκπαίδευση, την υποβολή αιτήσεων για δάνεια χωρίς περιττή γραφειοκρατία ή τη διασυνοριακή κινητικότητά τους [18].

Εξαιρετικά σημαντικό πλεονέκτημα είναι ότι προσφέρει ενιαία ταυτοποίηση στην ΕΕ κι επιτρέπει πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες σε όλα τα κράτη-μέλη [14]. Από οικονομικής άποψης, το EUDI Wallet έχει τη δυνατότητα να ενισχύσει την ανταγωνιστικότητα με την προώθηση της καινοτομίας στις ψηφιακές υπηρεσίες. Θέτοντας ένα παγκόσμιο σημείο αναφοράς για ασφαλή και διαλειτουργικά συστήματα ψηφιακής ταυτότητας, η ΕΕ μπορεί να ενισχύσει τη θέση της ως ηγέτης στην ψηφιακή διακυβέρνηση.

Επιπλέον, το πορτοφόλι προωθεί τη διαφάνεια, καθώς οι χρήστες διατηρούν τον πλήρη έλεγχο των δεδομένων τους, επιλέγουν ποια στοιχεία αποκαλύπτουν και συναινούν στη χρήση τους (Self-Sovereign Identity-SSI) [5]. Αυτή η προσέγγιση με επίκεντρο τον χρήστη ευθυγραμμίζεται με τη δέσμευση της ΕΕ για τη διασφάλιση της ιδιωτικής ζωής των ατόμων και την οικοδόμηση εμπιστοσύνης στα ψηφιακά συστήματα.

4. Κανονιστικό πλαίσιο eIDAS και Εφαρμογές

Το παρόν κεφάλαιο εξετάζει το κανονιστικό πλαίσιο που διέπει την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης στην Ευρωπαϊκή Ένωση, με επίκεντρο τον κανονισμό eIDAS. Αρχικά παρουσιάζεται η πρώτη έκδοση του κανονισμού eIDAS 1.0, η οποία αποτέλεσε το θεμέλιο για τη διασυνοριακή αναγνώριση ηλεκτρονικών ταυτοτήτων. Στη συνέχεια αναλύεται η αναθεωρημένη έκδοση eIDAS 2.0**,** η οποία εισάγει το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet) και επεκτείνει σημαντικά το πεδίο εφαρμογής και τις δυνατότητες του αρχικού πλαισίου.

4.1. Πρώτη έκδοση eIDAS 1.0 (2014)

Ο κανονισμός eIDAS (Electronic Identification, Authentication and Trust Services) θεσπίστηκε το 2014 με στόχο τη δημιουργία ενός ενιαίου νομικού πλαισίου για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης εντός της Ευρωπαϊκής Ένωσης [3]. Η βασική επιδίωξη του κανονισμού ήταν η ενίσχυση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές και η διευκόλυνση της διασυνοριακής πρόσβασης πολιτών και επιχειρήσεων σε ψηφιακές υπηρεσίες.

Ο eIDAS 1.0 εισήγαγε την αμοιβαία αναγνώριση των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης**,** επιτρέποντας σε έναν πολίτη ενός κράτους μέλους να χρησιμοποιεί την εθνική του ηλεκτρονική ταυτότητα για πρόσβαση σε δημόσιες υπηρεσίες άλλου κράτους μέλους [3]. Ωστόσο, η εφαρμογή του μηχανισμού αυτού προϋπέθετε την κοινοποίηση (notification) των εθνικών eID συστημάτων στην Ευρωπαϊκή Επιτροπή, γεγονός που οδήγησε σε ανομοιογενή υιοθέτηση μεταξύ των κρατών μελών.

Παράλληλα, ο κανονισμός καθόρισε το νομικό πλαίσιο για τις υπηρεσίες εμπιστοσύνης (trust services)**,** όπως οι ηλεκτρονικές υπογραφές, οι ηλεκτρονικές σφραγίδες, οι χρονοσφραγίδες, οι υπηρεσίες ηλεκτρονικής συστημένης παράδοσης και τα πιστοποιητικά αυθεντικοποίησης ιστοτόπων [3]. Οι υπηρεσίες αυτές κατηγοριοποιήθηκαν σε διαφορετικά επίπεδα ασφάλειας και αξιοπιστίας, με κορυφαία κατηγορία τις υπηρεσίες υψηλής διασφάλισης (qualified trust services)**,** οι οποίες παρέχουν νομική ισοδυναμία με τις παραδοσιακές έντυπες διαδικασίες [3].

Παρότι ο eIDAS 1.0 αποτέλεσε σημαντικό βήμα προς την εναρμόνιση των ψηφιακών υπηρεσιών στην ΕΕ, παρουσίασε ορισμένους περιορισμούς. Συγκεκριμένα, δεν προέβλεπε ενιαία ευρωπαϊκή λύση ψηφιακής ταυτότητας, ουσιαστικό έλεγχο του χρήστη επί των προσωπικών του δεδομένων, μηχανισμούς επιλεκτικής αποκάλυψης, ούτε ενσωμάτωση σύγχρονων αποκεντρωμένων τεχνολογιών [3], [1]. Οι αδυναμίες αυτές, σε συνδυασμό με τη ραγδαία ανάπτυξη των ψηφιακών υπηρεσιών και την αυξανόμενη εξάρτηση από ιδιωτικές πλατφόρμες ταυτοποίησης, οδήγησαν στην ανάγκη αναθεώρησης του κανονισμού.

4.2. Νέα έκδοση eIDAS 2.0 (2024)

Η αναθεωρημένη έκδοση eIDAS 2.0**,** η οποία εγκρίθηκε το 2024, σηματοδοτεί μια ουσιαστική μετάβαση από το μοντέλο της διασύνδεσης εθνικών συστημάτων σε ένα ενιαίο ευρωπαϊκό οικοσύστημα ψηφιακής ταυτότητας [14]. Είναι η μεγαλύτερη μεταρρύθμιση στο θεσμικό πλαίσιο ταυτοποίησης στην ΕΕ από το 2014. Κεντρικό στοιχείο της νέας έκδοσης αποτελεί το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet), ενισχύοντας τα δικαιώματα και τις δυνατότητες των πολιτών και των επιχειρήσεων αναφορικά με τον ψηφιακό τους βίο [14].

Ο eIDAS 2.0 επεκτείνει το πεδίο εφαρμογής του αρχικού κανονισμού, εισάγοντας υποχρέωση των κρατών μελών να παρέχουν τουλάχιστον ένα EUDI Wallet, δυνατότητα χρήσης του Wallet τόσο σε δημόσιες όσο και σε ιδιωτικές υπηρεσίες, αυξημένες απαιτήσεις ασφάλειας και προστασίας προσωπικών δεδομένων, καθώς και σαφή διαχωρισμό ρόλων μεταξύ εκδότη (issuer), κατόχου (holder) και επαληθευτή (verifier) [13], [14].

Σε αντίθεση με τον eIDAS 1.0, ο νέος κανονισμός δίνει έμφαση στον έλεγχο του χρήστη και στη φιλοσοφία privacy by design**.** Ο πολίτης έχει τη δυνατότητα να επιλέγει ποια δεδομένα θα αποκαλύψει, για ποιο σκοπό και σε ποιον φορέα, μειώνοντας σημαντικά τον κίνδυνο υπερβολικής συλλογής προσωπικών πληροφοριών [14], [19].

Επιπλέον, ο eIDAS 2.0 ενσωματώνει σύγχρονα τεχνολογικά πρότυπα και αρχιτεκτονικές, όπως verifiable credentials, selective disclosure, προηγμένους κρυπτογραφικούς μηχανισμούς και κοινή αρχιτεκτονική αναφοράς (ARF) για διαλειτουργικότητα [13].

Σημαντική καινοτομία της νέας έκδοσης αποτελεί επίσης η επέκταση των trust services**,** με την εισαγωγή νέων κατηγοριών και την ενίσχυση της νομικής ισχύος των ηλεκτρονικών συναλλαγών σε διασυνοριακό επίπεδο [14]. Έτσι, το eIDAS 2.0 δεν περιορίζεται πλέον στην απλή αναγνώριση ταυτοτήτων, αλλά λειτουργεί ως θεμέλιο για ένα ευρύτερο οικοσύστημα ψηφιακής εμπιστοσύνης στην Ευρωπαϊκή Ένωση [14], [1].

4.3. Συγκριτική Ανάλυση eIDAS 1.0 vs eIDAS 2.0

Το νέο κανονιστικό πλαίσιο eIDAS 2.0 φέρνει σημαντικές αλλαγές στην ψηφιακή ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης στην ΕΕ σε σχέση με τον αρχικό κανονισμό του 2014. Ο παρακάτω πίνακας παρουσιάζει μία συγκριτική ανάλυση με αναφορές στις δύο εκδόσεις eIDAS 1.0 και eIDAS 2.0.

Χαρακτηριστικό	eIDAS 1.0	eIDAS 2.0
Ψηφιακή Ταυτότητα	Θεσμικό πλαίσιο για eID, όχι πορτοφόλι	Εισαγωγή Ευρωπαϊκού Ψηφιακού Πορτοφολιού (EUDI Wallet) [20], [21]
Διαλειτουργικότητα	Περιορισμένη, εθνικά συστήματα	Ενιαίο πλαίσιο, πανευρωπαϊκή διαλειτουργικότητα
Ασφάλεια/Έλεγχος	Βασικές απαιτήσεις, περιορισμένος έλεγχος χρήστη	Αυστηρές απαιτήσεις, ισχυρός έλεγχος και προστασία προσωπικών δεδομένων [22]
Υπηρεσίες Εμπιστοσύνης	Υπογραφές, σφραγίδες, χρονικές σφραγίδες	Διευρυμένες υπηρεσίες, νέα εμπλουτισμένα σενάρια [23]
Τεχνολογίες	Υφιστάμενες τεχνολογίες	Blockchain, SSI, βιομετρικά, web standards
Συμμόρφωση με GDPR	Μερική	Απόλυτη εναρμόνιση με GDPR [22], [23]

Πίνακας 2 - Σύγκριση eIDAS 1.0 vs eIDAS 2.0

Η μετάβαση από τον πρώτο κανονισμό eIDAS (2014) στη δεύτερη έκδοση (2024) σηματοδοτεί τη στροφή από τα εθνικά, περιορισμένα συστήματα σε μια πανευρωπαϊκή αρχιτεκτονική που προάγει την ασφάλεια, το χρήστη-κεντρικό σχεδιασμό και την ψηφιακή αυτονομία. Το πλαίσιο του 2024 ανταποκρίνεται στις ανάγκες για διάφανη, ασφαλή και διαλειτουργική ψηφιακή ταυτότητα εντός της ΕΕ.

Συμπερασματικά, ο κανονισμός eIDAS έχει σημαντικές επιπτώσεις για τις επιχειρήσεις, τις κυβερνήσεις και τους ιδιώτες που δραστηριοποιούνται εντός της ΕΕ.

Για τις *επιχειρήσεις*, ο κανονισμός eIDAS προσφέρει ευκαιρίες για τον εξορθολογισμό των διοικητικών διαδικασιών, τη μείωση του κόστους και την επέκταση της εμβέλειας της αγοράς μέσω της αξιοποίησης της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης. Οι ειδικευμένοι πάροχοι υπηρεσιών εμπιστοσύνης μπορούν να προσφέρουν καινοτόμες λύσεις για την ηλεκτρονική πιστοποίηση ταυτότητας, την υπογραφή εγγράφων και την ασφαλή επικοινωνία, ενισχύοντας την αποδοτικότητα και την ανταγωνιστικότητα των επιχειρήσεων.

Για τους *ιδιώτες*, ο κανονισμός eIDAS παρέχει μεγαλύτερη ευκολία και προσβασιμότητα στην πρόσβαση σε ψηφιακές υπηρεσίες, στη διενέργεια ηλεκτρονικών συναλλαγών και στην αλληλεπίδραση με τις δημόσιες αρχές σε διασυνοριακό επίπεδο. Παρέχοντας ασφαλείς και αξιόπιστες λύσεις ηλεκτρονικής ταυτοποίησης και υπογραφής, ο κανονισμός eIDAS δίνει τη δυνατότητα στους πολίτες να συμμετέχουν πιο ενεργά στην ψηφιακή οικονομία και να ασκούν τα δικαιώματά τους σε μια ψηφιοποιημένη κοινωνία.

Ο κανονισμός eIDAS αποτελεί σημαντικό ορόσημο για την ανάπτυξη ενός εναρμονισμένου νομικού πλαισίου για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης στην Ευρωπαϊκή Ένωση. Με τη θέσπιση κοινών προτύπων, την προώθηση της διαλειτουργικότητας και την ενίσχυση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές, ο κανονισμός eIDAS αποσκοπεί στη διευκόλυνση του ψηφιακού μετασχηματισμού των επιχειρήσεων και των δημόσιων υπηρεσιών, στην ενίσχυση της διασυνοριακής συνεργασίας και στην ενδυνάμωση των πολιτών στην ψηφιακή εποχή.

4.4. Χρήσεις και Εφαρμογές

Η ενότητα αυτή αποσκοπεί στο να αποτυπώσει πώς το κανονιστικό πλαίσιο του eIDAS μεταφράζεται σε πρακτικές δυνατότητες για πολίτες, επιχειρήσεις και δημόσιους φορείς, τόσο σε εθνικό όσο και σε διασυνοριακό επίπεδο. Εξετάζονται οι βασικοί άξονες λειτουργίας που θεμελιώνει ο κανονισμός —η ηλεκτρονική ταυτοποίηση, οι ηλεκτρονικές υπογραφές και οι υπηρεσίες εμπιστοσύνης— και παρουσιάζεται πώς αυτές οι δυνατότητες επεκτείνονται σε κρίσιμα πεδία εφαρμογής, όπως οι χρηματοοικονομικές υπηρεσίες και οι διαδικασίες KYC (Know

Your Customer), αλλά και σε σενάρια κινητικότητας εντός της Ευρωπαϊκής Ένωσης. Τέλος, επισημαίνονται συνοπτικά οι τεχνικές και οργανωτικές προκλήσεις που συνοδεύουν την υλοποίηση ενός πανευρωπαϊκού, ασφαλούς και διαλειτουργικού οικοσυστήματος ψηφιακής ταυτότητας.

Ο κανονισμός eIDAS ορίζει την *ηλεκτρονική ταυτοποίηση (electronic identification – eID)* ως τη διαδικασία χρήσης δεδομένων ταυτοποίησης προσώπου σε ηλεκτρονική μορφή, με σκοπό τη μοναδική αναγνώριση φυσικών ή νομικών προσώπων στις ηλεκτρονικές συναλλαγές [3]. Στο πλαίσιο αυτό, τα κράτη μέλη θεσπίζουν και διατηρούν συστήματα ηλεκτρονικής ταυτοποίησης που οφείλουν να ανταποκρίνονται σε απαιτήσεις όπως η ασφάλεια, η αξιοπιστία και η διαλειτουργικότητα, ενώ η αναγνώριση και χρήση τους σε διασυνοριακό περιβάλλον βασίζεται σε κανόνες που περιγράφονται στο κανονιστικό πλαίσιο eIDAS και στην εξέλιξή του με το eIDAS 2.0 [3], [14].

Παράλληλα, ο κανονισμός eIDAS διακρίνει διαφορετικούς τύπους *ηλεκτρονικών υπογραφών***,** από απλές μορφές έως τις προηγμένες και τις αναγνωρισμένες (qualified) ηλεκτρονικές υπογραφές, θέτοντας συγκεκριμένες απαιτήσεις για θέματα όπως η γνησιότητα, η ακεραιότητα και η μη αποκήρυξη (non-repudiation) [3], [24]. Ιδιαίτερη σημασία έχει η αναγνωρισμένη ηλεκτρονική υπογραφή (*Qualified Electronic Signature – QES*)**,** η οποία, σύμφωνα με τον κανονισμό, έχει νομικό αποτέλεσμα ισοδύναμο με τη χειρόγραφη υπογραφή, ενισχύοντας σημαντικά την ασφάλεια δικαίου στις ηλεκτρονικές συναλλαγές [3].

Επιπλέον, ο κανονισμός eIDAS θεσπίζει πλαίσιο για τις *υπηρεσίες εμπιστοσύνης (trust services)***,** οι οποίες καλύπτουν μεταξύ άλλων τις ηλεκτρονικές σφραγίδες, τις ηλεκτρονικές χρονοσφραγίδες, τις υπηρεσίες ηλεκτρονικής συστημένης παράδοσης (Electronic Registered Delivery Service – ERDS) και τα πιστοποιητικά αυθεντικοποίησης ιστοτόπων, ενώ προβλέπει και αυξημένες υποχρεώσεις συμμόρφωσης για τους παρόχους, ειδικά όταν πρόκειται για αναγνωρισμένους παρόχους υπηρεσιών εμπιστοσύνης (Qualified Trust Service Providers – QTSPs) [3]. Η ύπαρξη αυτών των μηχανισμών είναι κρίσιμη για την εμπέδωση εμπιστοσύνης σε δημόσιες και ιδιωτικές διαδικασίες, όπως υπογραφές συμβάσεων, αυθεντικοποίηση υπηρεσιών και ασφαλή διαβίβαση ψηφιακών εγγράφων [3].

Σε ό,τι αφορά τις χρηματοοικονομικές υπηρεσίες και τις διαδικασίες *Know Your Customer (KYC)*, η αξιοποίηση ενός πορτοφολιού ψηφιακής ταυτότητας μπορεί να επιταχύνει τον έλεγχο πελάτη, καθώς παρέχει επαληθεύσιμα και τυποποιημένα δεδομένα ταυτότητας ή ιδιοτήτων, μειώνοντας το κόστος και τον χρόνο onboarding σε οργανισμούς που απαιτούν υψηλό επίπεδο βεβαιότητας [25]. Η κατεύθυνση αυτή συνδέεται άμεσα με το ευρύτερο οικοσύστημα εφαρμογών του EUDI Wallet σε ιδιωτικούς φορείς και υπηρεσίες που χρειάζονται ισχυρή ταυτοποίηση ή/και επιβεβαίωση ιδιοτήτων [26].

Μία ιδιαίτερα σημαντική κατηγορία εφαρμογών σχετίζεται με τη *διασυνοριακή χρήση*. Η γενική λογική του EUDI Wallet είναι να υποστηρίζει πρακτικά σενάρια μετακίνησης και αλληλεπίδρασης σε διαφορετικά κράτη μέλη, μέσω ασφαλούς παρουσίασης εγγράφων ή διαπιστευτηρίων όπου αυτό απαιτείται [26]. Ενδεικτικά, στο πεδίο των ταξιδιών αναδεικνύονται σενάρια χρήσης που σχετίζονται με ταξιδιωτικά διαπιστευτήρια (*Travel Credentials / Digital Travel Credentials*), τα οποία μπορούν να μοιράζονται με αρμόδιες αρχές πριν ή κατά τη μετακίνηση, με στόχο την αποτελεσματικότερη προετοιμασία/επαλήθευση σε ελέγχους και διαδικασίες [27]. Παρόμοια, η αξιοποίηση του πορτοφολιού σε υπηρεσίες τουρισμού ή μεταφορών (π.χ. ταυτοποίηση σε κρατήσεις) περιγράφεται ως μέρος του ευρύτερου πλέγματος “use cases” του EUDI Wallet [26], [27].

Ωστόσο, όπως προαναφέρθηκε, η ανάπτυξη ενός τόσο εξελιγμένου συστήματος συνοδεύεται από ουσιαστικές τεχνικές και οργανωτικές προκλήσεις. Η διασφάλιση συμβατότητας με διαφορετικές συσκευές, λειτουργικά συστήματα και υφιστάμενες υποδομές σε όλα τα κράτη μέλη αποτελεί απαιτητικό έργο, ενώ παράλληλα το πορτοφόλι πρέπει να παραμένει διαισθητικό για ευρεία υιοθέτηση, χωρίς να υποχωρεί από τα υψηλά πρότυπα ασφάλειας και διαλειτουργικότητας που αναμένονται σε ένα θεσμικά κατοχυρωμένο σύστημα [13], [14].

5. Λειτουργικότητα και Αρχιτεκτονική EUDI Wallet

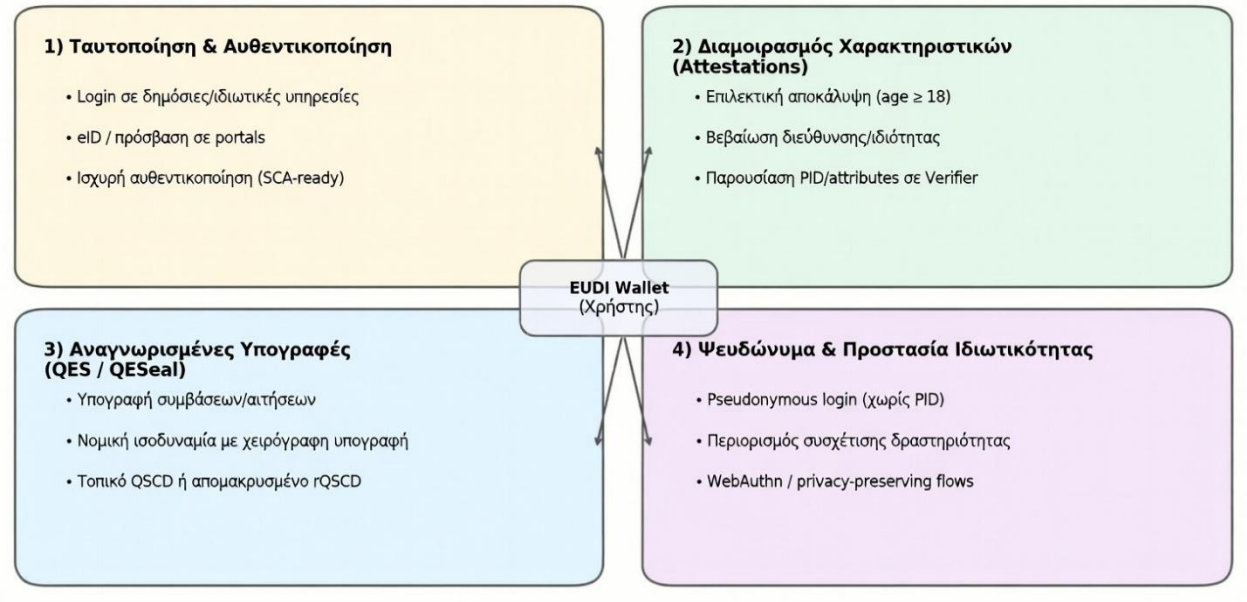
Το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet) αποτελεί τον βασικό πυλώνα του νέου πλαισίου European Digital Identity (EUDI) και έχει ως στόχο να προσφέρει στους πολίτες

της Ευρωπαϊκής Ένωσης μια ενιαία, ασφαλή και ελεγχόμενη από τον χρήστη πλατφόρμα ψηφιακής ταυτότητας [14], [2]. Η λειτουργία του επιτρέπει τη διαχείριση και χρήση ψηφιακών διαπιστευτηρίων σε διασυνοριακό επίπεδο, ακολουθώντας κοινές τεχνικές προδιαγραφές και απαιτήσεις συμμόρφωσης, ώστε να εξασφαλίζεται υψηλό επίπεδο εμπιστοσύνης, προστασίας προσωπικών δεδομένων και διαλειτουργικότητας μεταξύ κρατών μελών και παρόχων υπηρεσιών [29].

Το παρόν κεφάλαιο εστιάζει στη λειτουργικότητα, στο οικοσύστημα και στην αρχιτεκτονική υψηλού επιπέδου του EUDI Wallet, όπως προκύπτουν από το κανονιστικό πλαίσιο του eIDAS 2.0 και τις τεχνικές προδιαγραφές του Architecture Reference Framework (ARF) [14]. Η ανάλυση δίνει έμφαση στις ροές έκδοσης και παρουσίασης διαπιστευτηρίων, στους ρόλους των εμπλεκόμενων φορέων, καθώς και στα σενάρια χρήσης «εγγύς» και «απομακρυσμένης» αλληλεπίδρασης [29].

5.1. Λειτουργικότητα EUDI Wallet

Το οικοσύστημα EUDI Wallet παρέχει μια ασφαλή, ελεγχόμενη από τον χρήστη πλατφόρμα για τη διαχείριση της ψηφιακής ταυτότητας σε ολόκληρη την Ευρωπαϊκή Ένωση, βασισμένη σε τέσσερις βασικές λειτουργίες: (α) ασφαλή ταυτοποίηση και αυθεντικοποίηση, (β) ανταλλαγή χαρακτηριστικών μέσω ηλεκτρονικών πιστοποιητικών/διαπιστευτηρίων, (γ) δημιουργία αναγνωρισμένων ηλεκτρονικών υπογραφών και σφραγίδων, και (δ) αυθεντικοποίηση με ψευδώνυμα και μηχανισμούς προστασίας ιδιωτικότητας [29]. Ο χρήστης διατηρεί κεντρικό έλεγχο στη χρήση των δεδομένων του, καθώς μπορεί να επιλέγει ποια στοιχεία αποκαλύπτει, σε ποιον φορέα και για ποιο σκοπό, σύμφωνα με τις αρχές ελαχιστοποίησης δεδομένων και τις απαιτήσεις προστασίας προσωπικών δεδομένων. Στην εικόνα 1 απεικονίζονται οι τέσσερις βασικές λειτουργίες του οικοσυστήματος EUDI Wallet.



Εικόνα 1 - Χάρτης λειτουργιών EUDI Wallet

Στο επίπεδο αυθεντικοποίησης, το πορτοφόλι επιτρέπει ισχυρή σύνδεση σε δημόσιες και ιδιωτικές υπηρεσίες μέσω διαλειτουργικών μηχανισμών ταυτοποίησης, υποστηρίζοντας χρήση σε ολόκληρη την ΕΕ [29]. Παράλληλα, τα ηλεκτρονικά πιστοποιητικά/διαπιστευτήρια αποτελούν τον πυρήνα της λειτουργικότητάς του, καθώς επιτρέπουν στον χρήστη να παρουσιάζει επαληθεύσιμες πληροφορίες (όπως ηλικία, κατοικία, επαγγελματική ιδιότητα ή άλλα attributes) με τρόπο που διασφαλίζει επιλεκτική αποκάλυψη και περιορισμό αποκάλυψης πέραν του απολύτως αναγκαίου.

Επιπλέον, το EUDI Wallet υποστηρίζει τη δημιουργία αναγνωρισμένων ηλεκτρονικών υπογραφών και σφραγίδων, συμβατών με τις απαιτήσεις του πλαισίου eIDAS, ώστε οι χρήστες να μπορούν να υπογράφουν ψηφιακά έγγραφα και συμβάσεις με νομική ισχύ αντίστοιχη της ιδιόχειρης υπογραφής [14]. Η δυνατότητα αυτή προϋποθέτει υψηλού επιπέδου κρυπτογραφική προστασία των κλειδιών υπογραφής και κατάλληλες υποδομές ή συσκευές δημιουργίας υπογραφής, ώστε να εξασφαλίζεται η ακεραιότητα και η μη αποποίηση της υπογεγραμμένης πράξης [29].

Παράλληλα, η λειτουργία αυθεντικοποίησης με ψευδώνυμα επιτρέπει την πρόσβαση σε υπηρεσίες χωρίς την αποκάλυψη πλήρους ταυτότητας, προσφέροντας ενισχυμένη προστασία

ιδιωτικότητας και μείωση της δυνατότητας συσχέτισης ενεργειών του χρήστη μεταξύ διαφορετικών υπηρεσιών [29], [30]. Σε τέτοια σενάρια, ο στόχος δεν είναι η πλήρης ταυτοποίηση αλλά η ισχυρή απόδειξη ότι ο χρήστης διαθέτει ένα έγκυρο διαπιστευτήριο ή δικαίωμα πρόσβασης, σε συνδυασμό με τεχνικές που περιορίζουν την ιχνηλασιμότητα [32].

Ως προς τα σενάρια αλληλεπίδρασης, το EUDI Wallet μπορεί να λειτουργεί τόσο σε same-device όσο και σε cross-device περιβάλλον [30]. Στην πρώτη περίπτωση, η υπηρεσία του relying party (βασιζόμενου μέρους) και το wallet χρησιμοποιούνται στην ίδια συσκευή (π.χ. κινητό), ενώ στη δεύτερη περίπτωση η υπηρεσία εκτελείται σε διαφορετική συσκευή (π.χ. υπολογιστής) και η αλληλεπίδραση ολοκληρώνεται μέσω μηχανισμών γεφύρωσης, όπως QR codes ή deep links [33]. Επιπρόσθετα, υποστηρίζονται proximity σενάρια, όπου η παρουσίαση και επαλήθευση δεδομένων γίνεται σε φυσική εγγύτητα (π.χ. μέσω NFC ή Bluetooth), γεγονός που είναι ιδιαίτερα χρήσιμο σε offline ή φυσικούς ελέγχους, όπως η παρουσίαση mobile driving licence ή η επαλήθευση ηλικίας.

Τέλος, η συνολική αρχιτεκτονική λειτουργικότητας ενισχύεται από την απαίτηση χρήσης ισχυρών μηχανισμών ασφάλειας και αυθεντικοποίησης, όπως Strong Customer Authentication (SCA) όπου απαιτείται, καθώς και από τη χρήση σύγχρονων προτύπων και πρωτοκόλλων, ώστε να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των συναλλαγών [31], [32]. Με αυτόν τον τρόπο, το EUDI Wallet επιδιώκει να αποτελέσει ένα κεντρικό, αξιόπιστο και πρακτικό εργαλείο ψηφιακής ταυτότητας, ικανό να καλύψει πλήθος καθημερινών και θεσμικών περιπτώσεων χρήσης σε ευρωπαϊκό επίπεδο [29].

Για να αποτυπωθεί με σαφήνεια η πρακτική διάσταση των παραπάνω λειτουργιών, είναι χρήσιμο να διακριθούν οι βασικοί τύποι ροών αλληλεπίδρασης ανάμεσα στο πορτοφόλι και έναν φορέα που ζητά επαλήθευση (Relying Party / Verifier): (α) απομακρυσμένη παρουσίαση (remote presentation), όπου η αλληλεπίδραση γίνεται «online» μέσω διαδικτυακών μηχανισμών, και (β) εγγύς παρουσίαση (proximity presentation), όπου η αλληλεπίδραση γίνεται «in person» με φυσική εγγύτητα συσκευών και τοπικά κανάλια επικοινωνίας [29], [30]. Οι δύο κατηγορίες δεν

αφορούν μόνο την εμπειρία χρήστη, αλλά και τις τεχνικές επιλογές (πρωτόκολλα, μεταφορά μηνυμάτων, εμπιστοσύνη, έλεγχο συνεδρίας) που πρέπει να υποστηρίζει η αρχιτεκτονική [12].

Στις απομακρυσμένες ροές, το EUDI Wallet λειτουργεί ως «Wallet» που παράγει ένα verifiable presentation (VP token) ή ισοδύναμο αντικείμενο παρουσίασης, σύμφωνα με το OpenID4VP, το οποίο στη συνέχεια παραδίδεται στον Verifier για έλεγχο [30]. Η διαδικασία υλοποιείται συνήθως με ανακατευθύνσεις (redirects), deep links ή μηχανισμούς Digital Credentials API, ώστε ο χρήστης να εγκρίνει ρητά τη γνωστοποίηση (consent) και να εφαρμόσει επιλεκτική αποκάλυψη (selective disclosure) στα ζητούμενα χαρακτηριστικά [39].

Στις ροές εγγύτητας , η παρουσίαση πραγματοποιείται μεταξύ συσκευών σε μικρή απόσταση (π.χ. smartphone–reader) και βασίζεται σε πρότυπα όπως το ISO/IEC 18013-5 (mdoc/mDL), με τεχνολογίες όπως NFC ή Bluetooth Low Energy (BLE) [12]. Στόχος είναι η επιβεβαίωση ιδιοτήτων σε φυσικές συναλλαγές (π.χ. έλεγχος ταυτότητας, ηλικιακή επαλήθευση, mDL), με χαρακτηριστικό ότι η επικοινωνία και η ασφάλεια της συνεδρίας υλοποιούνται σε επίπεδο συσκευών/τοπικού καναλιού [29].

Ο όρος same-device χρησιμοποιείται όταν ο χρήστης εκτελεί την υπηρεσία του Relying Party (π.χ. web ή app) και το πορτοφόλι στην ίδια συσκευή: το αίτημα παρουσίασης ανοίγει το Wallet με deep link και η απάντηση επιστρέφει στην αρχική εφαρμογή/φυλλομετρητή [30]. Αντίθετα, ως cross-device χαρακτηρίζονται οι ροές όπου ο Relying Party βρίσκεται σε διαφορετική συσκευή (π.χ. υπολογιστής ή reader), και η έναρξη της διαδικασίας γίνεται συνήθως με QR code ή άλλο out-of-band μηχανισμό που «γεφυρώνει» τις συσκευές [12]. Και στις δύο περιπτώσεις, ο πυρήνας είναι κοινός: ο Verifier ζητά συγκεκριμένα attributes, ο χρήστης εγκρίνει, το Wallet δημιουργεί το VP/credential presentation, και ο Verifier επαληθεύει κρυπτογραφικά την εγκυρότητα και την ακεραιότητα.

5.2. Οικοσύστημα EUDI Wallet

Το οικοσύστημα EUDI Wallet είναι ένα ρυθμιζόμενο πλαίσιο που έχει θεσπιστεί βάσει του Ευρωπαϊκού Κανονισμού για την Ψηφιακή Ταυτότητα, με σκοπό την παροχή ασφαλούς και διαλειτουργικής διαχείρισης της ψηφιακής ταυτότητας σε ολόκληρη την ΕΕ [14]. Περιλαμβάνει πολλαπλούς ρόλους, όπως χρήστες, παρόχους πορτοφολιών, παρόχους PID (Personal

Identification Data), παρόχους πιστοποίησης (QEAA, PuB-EAA, EAA), εξαρτώμενα μέρη και εποπτικές αρχές, όπως οργανισμοί αξιολόγησης της συμμόρφωσης (CAB) και εποπτικές αρχές [28]. Οι χρήστες ελέγχουν τις μονάδες πορτοφολιού τους για την αποθήκευση και τον διαμοιρασμό δεδομένων ταυτοποίησης προσώπων (PID) και πιστοποιητικών, ενώ οι πάροχοι πορτοφολιών διασφαλίζουν τη συμμόρφωση με τα τεχνικά πρότυπα και τα πρότυπα ασφάλειας [29]. Το οικοσύστημα δίνει έμφαση στην προστασία της ιδιωτικής ζωής από το σχεδιασμό, την εστίαση στον χρήστη και τη διασυνοριακή διαλειτουργικότητα, με αυστηρές απαιτήσεις για όλους τους συμμετέχοντες.

Στην πράξη, το «οικοσύστημα» περιγράφει ένα σύνολο από ρόλους, τεχνικές διεπαφές και μηχανισμούς εμπιστοσύνης (trust model) που επιτρέπουν σε ένα πορτοφόλι να λειτουργεί πανευρωπαϊκά [29]. Το ARF ορίζει τις βασικές οντότητες (π.χ. Wallet Provider, PID Provider, Attestation Providers, Relying Parties/Verifiers, Trust Service Providers, Registries/Trust Lists) και περιγράφει τις μεταξύ τους σχέσεις, ώστε η έκδοση, η παρουσίαση και η επαλήθευση να είναι διαλειτουργικές.

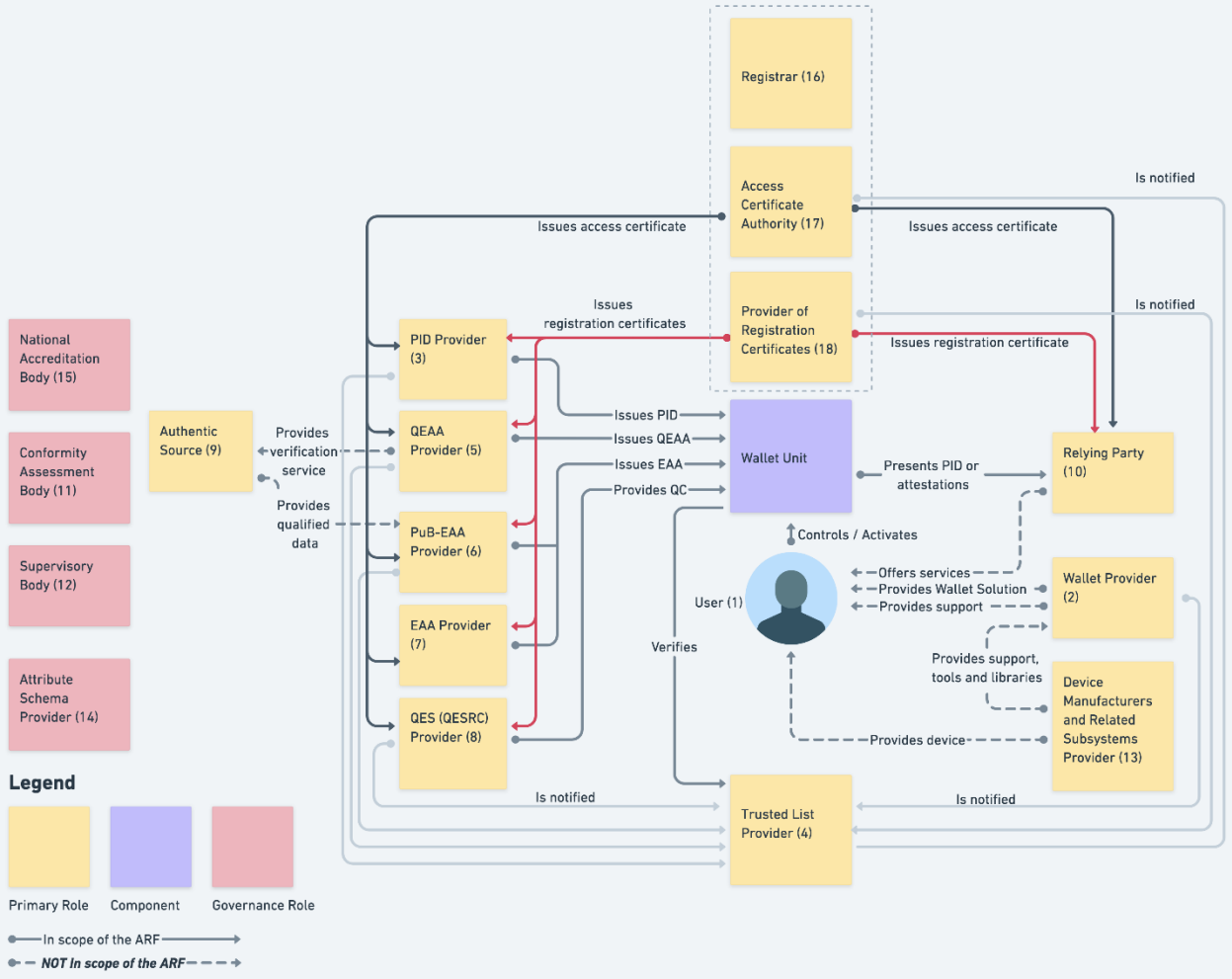
Ένα κρίσιμο στοιχείο για τη λειτουργία του οικοσυστήματος είναι η ύπαρξη κοινών μηχανισμών «αγκύρωσης εμπιστοσύνης», όπως κατάλογοι εμπιστοσύνης (trust lists), καταχωρητές (registries) και υπηρεσίες επικύρωσης κατάστασης πιστοποιητικών/οντοτήτων [29], [34]. Μέσω αυτών, ένας Verifier μπορεί να ελέγξει ότι ένα Wallet Provider ή ένας Issuer/Attestation Provider είναι νόμιμα εξουσιοδοτημένος και πιστοποιημένος, ενώ παράλληλα καθίσταται εφικτή η διαχείριση ανάκλησης ή αλλαγής κατάστασης (status) διαπιστευτηρίων ή οντοτήτων [14].

Οι Πάροχοι Πορτοφολιών, εξουσιοδοτημένοι από τα κράτη μέλη, παρέχουν πιστοποιημένες Λύσεις Πορτοφολιών που ενσωματώνουν κρυπτογραφική ασφάλεια (π.χ. WSCD) για την επίτευξη Υψηλού Επιπέδου Διασφάλισης [29]. Εκδίδουν Βεβαιώσεις Μονάδων Πορτοφολιών (WUAs) για την επικύρωση της συμμόρφωσης. Οι πάροχοι PID επαληθεύουν την ταυτότητα των χρηστών και εκδίδουν PID, ενώ οι πάροχοι πιστοποιητικών (π.χ. QTSP για QEAA, δημόσιοι φορείς για PuB-EAA) εκδίδουν ηλεκτρονικά πιστοποιητικά με νομική ισοδυναμία με τα έντυπα έγγραφα. Οι εξαρτώμενοι φορείς — πάροχοι υπηρεσιών που ζητούν χαρακτηριστικά — πρέπει να καταχωρίζουν τις ανάγκες τους σε δεδομένα και να πιστοποιούνται μέσω πιστοποιητικών

πρόσβασης. Οι μεσάζοντες ενεργούν για λογαριασμό των εξαρτώμενων φορέων, αλλά απαγορεύεται να αποθηκεύουν δεδομένα συναλλαγών.

Οι αξιόπιστοι κατάλογοι, που τηρούνται από παρόχους αξιόπιστων καταλόγων, επικυρώνουν την κατάσταση των παρόχων πορτοφολιών, των παρόχων PID και άλλων οντοτήτων [29]. Οι καταχωρητές καταχωρούν τους συμμετέχοντες στο οικοσύστημα (π.χ. βασιζόμενα μέρη, πάροχοι πιστοποίησης), ενώ οι αρχές έκδοσης πιστοποιητικών πρόσβασης εκδίδουν πιστοποιητικά για ασφαλείς αλληλεπιδράσεις [29]. Οι πάροχοι σχημάτων χαρακτηριστικών τυποποιούν τις δομές πιστοποίησης και οι κατασκευαστές συσκευών παρέχουν ασφαλείς πλατφόρμες υλικού/λογισμικού. Το οικοσύστημα υποστηρίζει απομακρυσμένες αλληλεπιδράσεις και αλληλεπιδράσεις εγγύτητας , με πρωτόκολλα όπως το OpenID4VP και το ISO/IEC 18013-5 που επιτρέπουν την ασφαλή ανταλλαγή δεδομένων.

Η διακυβέρνηση και η συμμόρφωση επιβάλλονται μέσω οργανισμών αξιολόγησης της συμμόρφωσης (CAB), οι οποίοι πιστοποιούν τις λύσεις πορτοφολιού και ελέγχουν τους QTSP, καθώς και εποπτικών οργανισμών που εποπτεύουν την ακεραιότητα του οικοσυστήματος [14]. Οι εθνικοί φορείς διαπίστευσης διασφαλίζουν την ικανότητα των CAB, ενώ η Επιτροπή συντονίζει τις τεχνικές προδιαγραφές και καταρτίζει έναν κατάλογο αξιόπιστων καταλόγων για λόγους διαφάνειας [29]. Το πλαίσιο επιτρέπει στους φορείς να αναλαμβάνουν πολλαπλούς ρόλους (π.χ. ένας πάροχος PID μπορεί επίσης να είναι πάροχος πορτοφολιού), αλλά επιβάλλει την αποφυγή συγκρούσεων και την τήρηση όλων των απαιτήσεων που αφορούν τον εκάστοτε ρόλο.



Εικόνα 2 - Επισκόπηση των ρόλων του οικοσυστήματος EUDI Wallet

Η εικόνα 2 συνοψίζει τους «primary roles» που εμφανίζονται συνήθως στο οικοσύστημα του EUDI Wallet [14]. Ο χρήστης (Wallet User) είναι ο κάτοχος των διαπιστευτηρίων και ελέγχει την παρουσίαση δεδομένων [29]. Ο Wallet Provider διαθέτει/διαχειρίζεται τη λύση πορτοφολιού (wallet solution) και την υποστηρικτική υποδομή της, ενώ ο PID Provider και οι Attestation Providers εκδίδουν ψηφιακές βεβαιώσεις (PID και λοιπές attestations) που αποθηκεύονται στο πορτοφόλι. Ο Relying Party/Verifier είναι ο φορέας που ζητά δεδομένα/αποδείξεις και εκτελεί την κρυπτογραφική επαλήθευση. Συμπληρωματικά, οι Trust Service Providers (π.χ. για υπογραφές/QES) και οι φορείς αξιολόγησης συμμόρφωσης (CAB) διασφαλίζουν ότι τα

πορτοφόλια και οι σχετικές υπηρεσίες πληρούν απαιτήσεις ασφάλειας, πιστοποίησης και κανονιστικής συμμόρφωσης.

Η ευελιξία του οικοσυστήματος καλύπτει ποικίλες περιπτώσεις χρήσης, από υπηρεσίες ηλεκτρονικής διακυβέρνησης έως εφαρμογές του ιδιωτικού τομέα, διασφαλίζοντας παράλληλα την ελαχιστοποίηση των δεδομένων και τη συγκατάθεση των χρηστών. Τα ψευδώνυμα (μέσω W3C WebAuthn) επιτρέπουν την αυθεντικοποίηση με διαφύλαξη της ιδιωτικής ζωής, ενώ οι εγκεκριμένες ηλεκτρονικές υπογραφές ενισχύουν την εμπιστοσύνη στις συναλλαγές. Με την ενοποίηση των προτύπων και την προώθηση του ανταγωνισμού, το EUDI Wallet στοχεύει να καταστεί ο ακρογωνιαίος λίθος της ψηφιακής ταυτότητας σε ολόκληρη την ΕΕ, με τα κράτη μέλη να υποχρεούνται να προσφέρουν τουλάχιστον μία λύση πορτοφολιού εντός 24 μηνών από την έναρξη ισχύος των εκτελεστικών πράξεων.

5.3. Αρχιτεκτονική Υψηλού Επιπέδου

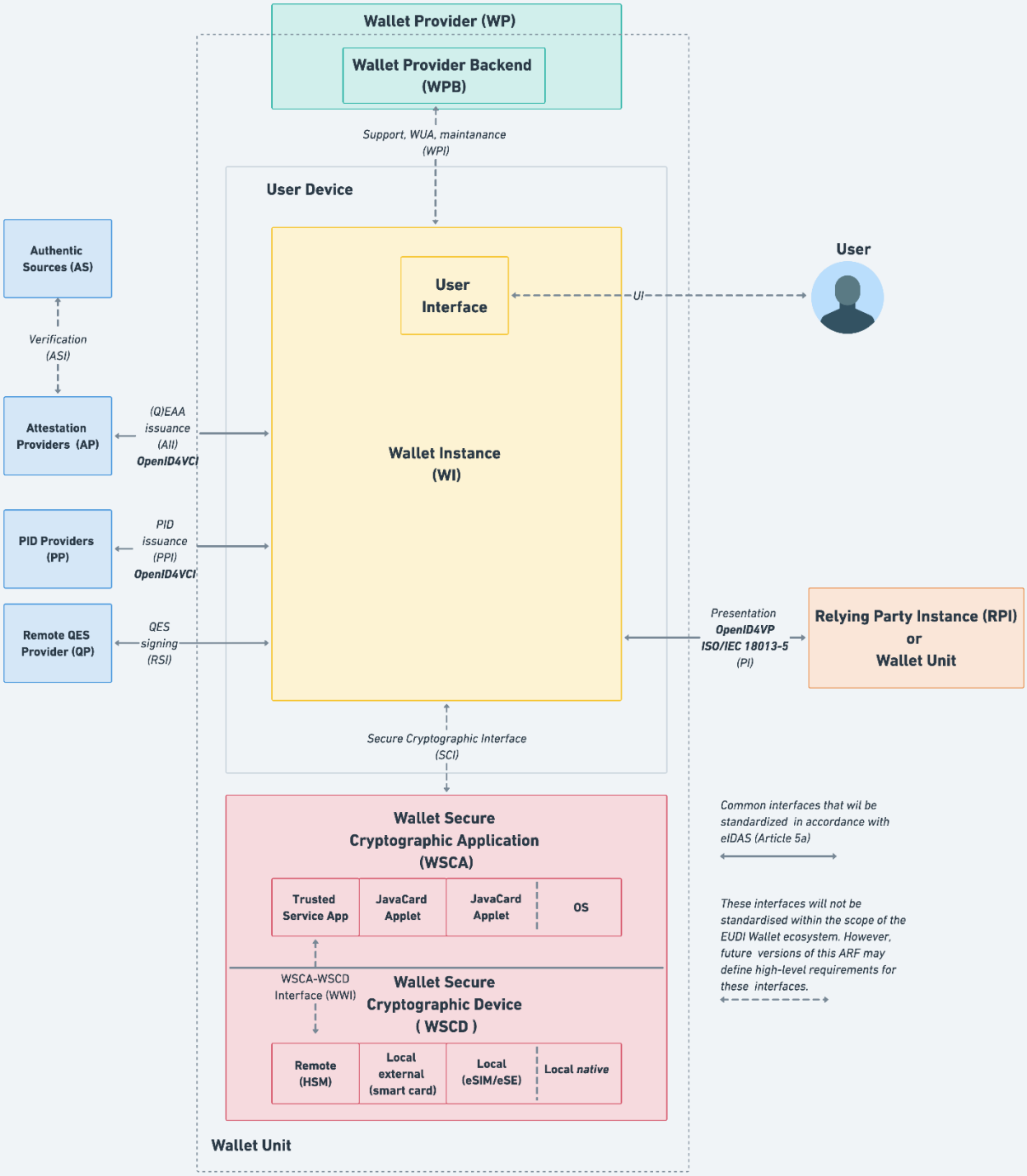
Το οικοσύστημα EUDI Wallet είναι δομημένο γύρω από βασικές αρχές εστίασης στον χρήστη, διαλειτουργικότητας, ιδιωτικότητας και ασφάλειας από το σχεδιασμό [29]. Η αρχιτεκτονική του εξασφαλίζει τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό για την Ψηφιακή Ταυτότητα, δίνοντας έμφαση στον διαισθητικό έλεγχο από τον χρήστη, τη διασυνοριακή λειτουργικότητα και την ισχυρή προστασία των δεδομένων. Τα βασικά στοιχεία περιλαμβάνουν τη Μονάδα Πορτοφολιού (που αποτελείται από μια Συσκευή Χρήστη, μια Εφαρμογή Πορτοφολιού και μια Ασφαλή Κρυπτογραφική Συσκευή), τυποποιημένες διεπαφές για την έκδοση και την παρουσίαση πιστοποιητικών, καθώς και υποστήριξη για πολλαπλές ροές πιστοποίησης. Οι αρχές σχεδιασμού καθοδηγούν την ανάπτυξη του οικοσυστήματος, δίνοντας προτεραιότητα στη διαφάνεια, στην ελάχιστη αποκάλυψη δεδομένων και στην ανθεκτικότητα στις απειλές στον κυβερνοχώρο.

Η αρχιτεκτονική αναφοράς περιγράφει λεπτομερώς τη σύνθεση της μονάδας πορτοφολιού, συμπεριλαμβανομένης της ασφαλούς κρυπτογραφικής συσκευής πορτοφολιού (WSCD), η οποία υποστηρίζει τέσσερα μοντέλα ανάπτυξης: απομακρυσμένο (π.χ. HSM), τοπικό εξωτερικό (π.χ. έξυπνη κάρτα), τοπικό εσωτερικό (π.χ. e-SIM) και εγγενές (ενσωματωμένο στο λειτουργικό σύστημα). Διεπαφές όπως η Διεπαφή Παρουσίασης (PI) και η Διεπαφή Έκδοσης PID (PII)

επιτρέπουν ασφαλείς αλληλεπιδράσεις με τα Εξαρτώμενα Μέρη και τους Παρόχους, χρησιμοποιώντας πρωτόκολλα όπως το OpenID4VP και το ISO/IEC 18013-5. Το σύστημα υποστηρίζει υβριδικές αρχιτεκτονικές, επιτρέποντας ευελιξία στην υλοποίηση κρυπτογραφικού υλικού, διατηρώντας παράλληλα υψηλά επίπεδα ασφάλειας.

Σε επίπεδο «Wallet Unit», η αρχιτεκτονική διαχωρίζει λογικά: (α) το περιβάλλον διεπαφής χρήστη (UI) και τις εφαρμογές/λειτουργίες πορτοφολιού, (β) τον πυρήνα πορτοφολιού (wallet core) που υλοποιεί τις ροές έκδοσης και παρουσίασης, (γ) την ασφαλή αποθήκευση και χρήση κρυπτογραφικών κλειδιών (WSCD/secure hardware ή TEE), και (δ) τα υποστηρικτικά στοιχεία δικτύου/παραμετροποίησης που επιτρέπουν την επικοινωνία με Issuers, Verifiers και trust infrastructure [29]. Ο διαχωρισμός αυτός διευκολύνει τη συμμόρφωση με απαιτήσεις ασφάλειας, καθώς επιτρέπει να τοποθετούνται κρίσιμες λειτουργίες (π.χ. υπογραφή, αποθήκευση κλειδιών) σε πιο προστατευμένα υποσυστήματα της συσκευής [14].

Η έννοια του WSCD (Wallet Secure Cryptographic Device) αφορά την ασφαλή συνιστώσα που εκτελεί κρυπτογραφικές πράξεις και προστατεύει ιδιωτικά κλειδιά, παρέχοντας επιπλέον μηχανισμούς όπως anti-tamper προστασία ή/και απομόνωση εκτέλεσης [29]. Ανάλογα με την υλοποίηση, μπορεί να αντιστοιχεί σε Secure Element, TEE, ή άλλη πιστοποιήσιμη ασφαλή μονάδα [14]. Η ύπαρξη WSCD είναι σημαντική γιατί στηρίζει την αξιοπιστία της απόδειξης ότι μια παρουσίαση/υπογραφή προέρχεται όντως από το πορτοφόλι του χρήστη και δεν έχει παραποιηθεί από κακόβουλο λογισμικό.



Εικόνα 3 - Αναφορά αρχιτεκτονικής οικοσυστήματος του πορτοφολιού EUDI

Στην εικόνα 3 η αλληλεπίδραση του χρήστη με έναν Relying Party διατρέχει έναν κύκλο: ο Relying Party δημιουργεί ένα αίτημα (presentation request) που περιγράφει ποια attributes χρειάζεται

και υπό ποιες πολιτικές [29]. Το αίτημα φτάνει στο Wallet (remote μέσω web/redirects ή proximity μέσω τοπικού καναλιού) [30]. Ο χρήστης εγκρίνει τη γνωστοποίηση, το Wallet παράγει την απόκριση παρουσίασης (VP token / mdoc response), και ο Relying Party εκτελεί verification (έλεγχος υπογραφών, status/revocation, policy checks) πριν αποδεχθεί το αποτέλεσμα [30]. Η ροή υποστηρίζεται από τις υποδομές εμπιστοσύνης (π.χ. trust lists, certificates) που επιτρέπουν στον Relying Party να «πιστέψει» ότι ο εκδότης και το πορτοφόλι είναι έγκυροι.

Οι ροές παρουσίασης δεδομένων κατηγοριοποιούνται σε ροές εγγύτητας (εποπτευόμενες/μη εποπτευόμενες) και απομακρυσμένες (στην ίδια συσκευή/σε διαφορετικές συσκευές) [29]. Οι ροές εγγύτητας αξιοποιούν NFC ή Bluetooth, ενώ οι απομακρυσμένες ροές βασίζονται στο W3C Digital Credentials API για ανταλλαγές μέσω του προγράμματος περιήγησης [39]. Οι ροές σε διαφορετικές συσκευές χρησιμοποιούν FIDO CTAP 2.2 για τη δημιουργία ασφαλών σηράγγων μεταξύ συσκευών, μειώνοντας τους κινδύνους ηλεκτρονικού ψαρέματος [33]. Προκλήσεις όπως η επιλογή μονάδας πορτοφολιού και η σύνδεση συνεδρίας αντιμετωπίζονται μέσω τυποποιημένων API, αν και οι προσαρμοσμένες λύσεις απαιτούν πρόσθετα μέτρα ασφαλείας.

Τα διαγράμματα κατάστασης ορίζουν τους κύκλους ζωής για τις λύσεις πορτοφολιού, τις μονάδες, τους παρόχους και τις πιστοποιήσεις, εξασφαλίζοντας σαφείς λειτουργικούς τρόπους και τρόπους αποτυχίας [29]. Για παράδειγμα, οι μονάδες πορτοφολιού μεταβαίνουν από την κατάσταση *Εγκατεστημένο* στην κατάσταση *Έγκυρο* μετά την ενεργοποίηση και την έκδοση PID, ενώ οι πάροχοι αντιμετωπίζουν αναστολή/ακύρωση για μη συμμόρφωση.

Τα ψευδώνυμα, που υλοποιούνται μέσω W3C WebAuthn Passkeys, επιτρέπουν την αυθεντικοποίηση χωρίς κωδικό πρόσβασης, με επιλογές πιστοποίησης που εξισορροπούν την ιδιωτικότητα και την ασφάλεια [34]. Τα μοναδικά ψευδώνυμα ανά Relying Party αποτρέπουν την παρακολούθηση, σύμφωνα με τις κανονιστικές απαιτήσεις.

Τέλος, η αρθρωτή δομή του οικοσυστήματος επιτρέπει στους Wallet Providers να υιοθετούν διαφορετικές αρχιτεκτονικές WSCD, διασφαλίζοντας παράλληλα συνεπή ασφάλεια και διαλειτουργικότητα [29]. Τα απομακρυσμένα HSM εξυπηρετούν συσκευές που δεν διαθέτουν ασφαλές υλικό, ενώ οι ενσωματωμένες λύσεις (π.χ. e-SIM) βελτιστοποιούν την απόδοση. Η προσαρμοστικότητα της αρχιτεκτονικής υποστηρίζει μελλοντικές καινοτομίες, όπως υβριδικά

μοντέλα κρυπτογράφησης. Με την ενσωμάτωση σχεδιασμού με επίκεντρο τον χρήστη, τυποποιημένων πρωτοκόλλων και αυστηρής διαχείρισης κατάστασης, το πλαίσιο EUDI Wallet δημιουργεί μια επεκτάσιμη, ασφαλή βάση για την ψηφιακή ταυτότητα σε ολόκληρη την ΕΕ.

6. Πρόταση Υλοποίησης

Το παρόν κεφάλαιο επικεντρώνεται στην παρουσίαση και ανάλυση της υλοποίησης ενός πρωτοτύπου ψηφιακού πορτοφολιού, το οποίο αναπτύχθηκε στο πλαίσιο της παρούσας διπλωματικής εργασίας. Η υλοποίηση αυτή δεν αποσκοπεί στη δημιουργία ενός παραγωγικού ή εμπορικού συστήματος, αλλά στη διερεύνηση και πρακτική κατανόηση των βασικών αρχών που διέπουν τη λειτουργία σύγχρονων ψηφιακών πορτοφολιών ταυτοποίησης, όπως αυτά που προβλέπονται από το ευρωπαϊκό πλαίσιο του European Digital Identity Wallet (EUDI Wallet) [35].

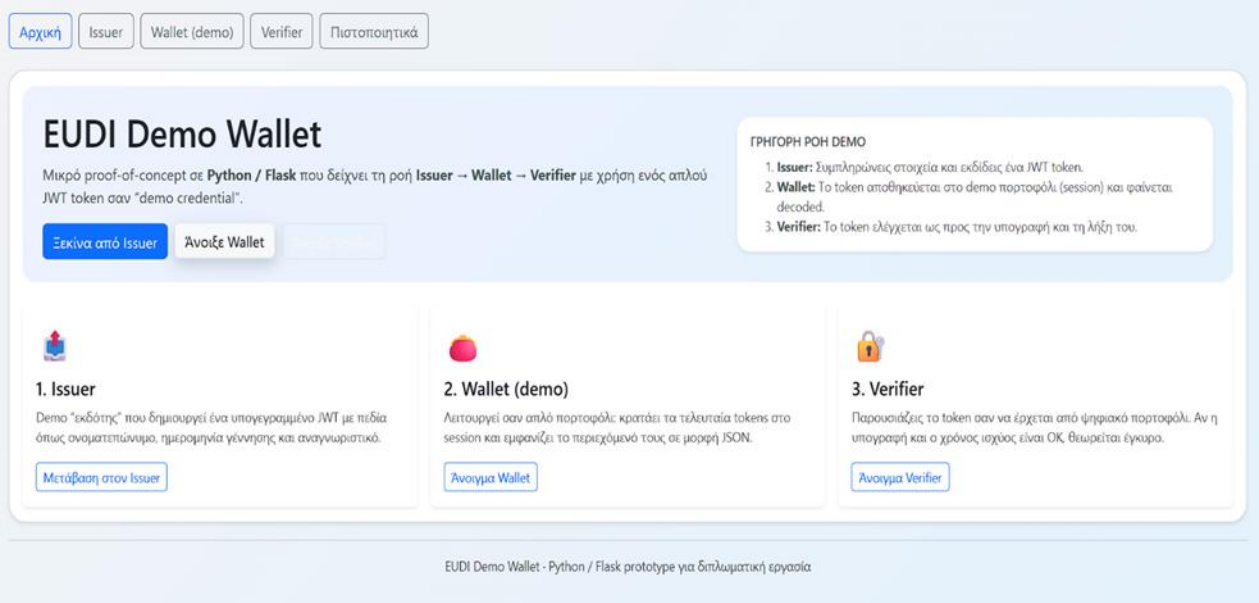
6.1. Στόχος και φιλοσοφία της υλοποίησης

Ο βασικός στόχος της εφαρμογής είναι η προσομοίωση της αρχιτεκτονικής Issuer–Wallet–Verifier, η οποία αποτελεί θεμέλιο λίθο των συστημάτων ψηφιακής ταυτότητας και των Verifiable Credentials. Μέσα από αυτή τη δομή, καθίσταται δυνατή η απεικόνιση της διαδικασίας έκδοσης ενός ψηφιακού διαπιστευτηρίου, της αποθήκευσής του σε ένα ψηφιακό πορτοφόλι και, τέλος, της παρουσίασης και επαλήθευσής του από έναν τρίτο φορέα.

Ιδιαίτερη έμφαση δόθηκε στη σαφήνεια της ροής και στην κατανόηση των επιμέρους σταδίων από τον αναγνώστη. Για τον λόγο αυτό, επιλέχθηκε η υλοποίηση ενός web-based πρωτοτύπου με γραφικό περιβάλλον, το οποίο επιτρέπει την άμεση αλληλεπίδραση με την εφαρμογή και την οπτική παρακολούθηση των αποτελεσμάτων κάθε ενέργειας. Η επιλογή αυτή διευκολύνει σημαντικά τη σύνδεση της θεωρητικής ανάλυσης των προηγούμενων κεφαλαίων με την πρακτική εφαρμογή των εννοιών που παρουσιάζονται.

Επιπλέον, η εφαρμογή σχεδιάστηκε με τρόπο ώστε να προσομοιώνει, σε απλουστευμένη μορφή, τη λειτουργικότητα πραγματικών κρατικών ψηφιακών υπηρεσιών. Η αισθητική και η δομή του γραφικού περιβάλλοντος αντλούν έμπνευση από σύγχρονες κυβερνητικές πλατφόρμες, όπως το ελληνικό Gov Wallet, με στόχο τη δημιουργία μιας οικείας εμπειρίας

χρήστη. Παράλληλα, ενσωματώθηκαν μηχανισμοί ελέγχου πρόσβασης και χρονικής ισχύος των διαπιστευτηρίων, ώστε να αναδειχθούν βασικές αρχές ασφάλειας που συναντώνται σε πραγματικά συστήματα ψηφιακής ταυτότητας. Στην παρακάτω εικόνα 4 φαίνεται η αρχική σελίδα της υλοποίησης.



Εικόνα 4 - Αρχική σελίδα της εφαρμογής, όπου παρουσιάζονται οι βασικές επιλογές πλοήγησης (Issuer, Wallet, Verifier και Mock Certificates)

Συνοψίζοντας, η φιλοσοφία της υλοποίησης βασίζεται στην ισορροπία μεταξύ απλότητας και ρεαλισμού. Από τη μία πλευρά, αποφεύγονται περίπλοκες τεχνολογίες που θα δυσχέραιναν την κατανόηση της εφαρμογής, όπως υποδομές δημόσιου κλειδιού ή αποκεντρωμένα αναγνωριστικά. Από την άλλη πλευρά, διατηρούνται όλες οι κρίσιμες έννοιες που απαιτούνται για να αποτυπωθεί με ακρίβεια η λειτουργία ενός ψηφιακού πορτοφολιού στο σύγχρονο ευρωπαϊκό ψηφιακό οικοσύστημα.

6.2. Τεχνολογικό περιβάλλον και εργαλεία υλοποίησης

Η υλοποίηση του πρωτοτύπου ψηφιακού πορτοφολιού βασίστηκε σε σύγχρονες, ευρέως διαδεδομένες τεχνολογίες, οι οποίες επιλέχθηκαν με γνώμονα τη σταθερότητα, την ευκολία χρήσης και την εκπαιδευτική τους αξία. Κεντρική γλώσσα ανάπτυξης αποτέλεσε η Python, η

οποία προσφέρει απλό συντακτικό και πλούσιο οικοσύστημα βιβλιοθηκών, γεγονός που την καθιστά ιδιαίτερα κατάλληλη για ταχεία ανάπτυξη πρωτοτύπων.

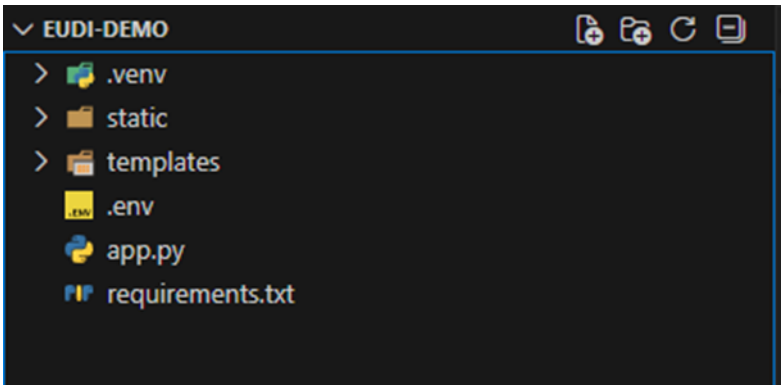
Για την ανάπτυξη της web εφαρμογής χρησιμοποιήθηκε το framework Flask [36]. Το Flask επιτρέπει τη δημιουργία ελαφριών web εφαρμογών χωρίς περιττή πολυπλοκότητα, παρέχοντας παράλληλα τον απαραίτητο έλεγχο στον προγραμματιστή για τη διαχείριση των routes, των αιτημάτων και των συνεδριών χρηστών. Η επιλογή του συγκεκριμένου framework ευθυγραμμίζεται με τον στόχο της εργασίας, καθώς επιτρέπει τη συγκέντρωση της ανάλυσης στη λογική της εφαρμογής και όχι στη ρύθμιση σύνθετων υποδομών.

Η αναπαράσταση και η υπογραφή των ψηφιακών διαπιστευτηρίων πραγματοποιήθηκε με τη χρήση JSON Web Tokens (JWT), σύμφωνα με το πρότυπο RFC 7519 [37]. Τα JWT χρησιμοποιούνται για την ασφαλή μεταφορά πληροφοριών μεταξύ μερών και αποτελούν θεμελιώδες δομικό στοιχείο πολλών σύγχρονων συστημάτων ταυτοποίησης. Στο πλαίσιο της εφαρμογής, τα JWT χρησιμοποιούνται για την ενσωμάτωση των προσωπικών δεδομένων του χρήστη, τον καθορισμό του χρόνου ισχύος του διαπιστευτηρίου και την επαλήθευση της αυθεντικότητάς του.

Για το γραφικό περιβάλλον της εφαρμογής αξιοποιήθηκε το Bootstrap 5 [38], το οποίο προσφέρει έτοιμα στοιχεία διεπαφής και υποστηρίζει responsive σχεδίαση. Μέσω του Bootstrap κατέστη δυνατή η δημιουργία ενός καθαρού και συνεκτικού UI, με κάρτες, φόρμες και ειδοποιήσεις, χωρίς την ανάγκη εκτεταμένης ενασχόλησης με CSS από την αρχή. Η επιλογή αυτή συνέβαλε στη δημιουργία μιας αισθητικά οικείας εμπειρίας χρήστη, η οποία προσομοιώνει σύγχρονες ψηφιακές κυβερνητικές εφαρμογές.

Η διαχείριση της κατάστασης του χρήστη πραγματοποιείται μέσω session-based μηχανισμών του Flask. Τα δεδομένα αποθηκεύονται προσωρινά στη συνεδρία του χρήστη και δεν γίνεται χρήση βάσης δεδομένων. Η συγκεκριμένη επιλογή έγινε συνειδητά, καθώς στόχος της υλοποίησης δεν είναι η μόνιμη αποθήκευση δεδομένων, αλλά η κατανόηση της ροής και της λογικής ενός ψηφιακού πορτοφολιού. Παράλληλα, η απουσία βάσης δεδομένων μειώνει την πολυπλοκότητα της εφαρμογής και επιτρέπει την εστίαση στις βασικές έννοιες της έκδοσης και επικύρωσης διαπιστευτηρίων.

Στην εικόνα 5 παρουσιάζεται, στο περιβάλλον ανάπτυξης (Visual Studio Code), η δομή των αρχείων και οι φάκελοι του έργου EUDI-DEMO.



Εικόνα 5 - Δομή του έργου στο περιβάλλον ανάπτυξης, με το αρχείο app.py και τους φακέλους templates και static

Το σύνολο των παραπάνω τεχνολογιών συνδυάζεται ώστε να δημιουργηθεί ένα συνεκτικό και λειτουργικό πρωτότυπο, το οποίο επιτρέπει την πρακτική διερεύνηση των εννοιών που αναπτύχθηκαν στα προηγούμενα κεφάλαια της διπλωματικής εργασίας.

6.3. Γενική αρχιτεκτονική και ροή της εφαρμογής

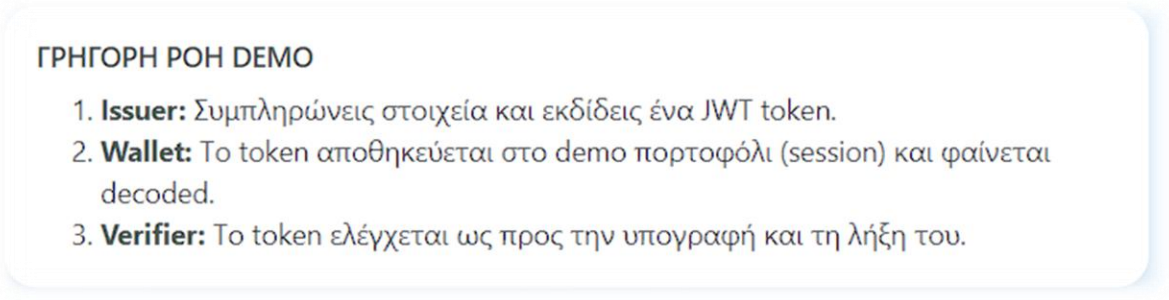
Η εφαρμογή που αναπτύχθηκε στο πλαίσιο της παρούσας διπλωματικής εργασίας ακολουθεί μια αρχιτεκτονική τριών βασικών ρόλων, η οποία συναντάται σε σύγχρονα συστήματα ψηφιακής ταυτότητας και Verifiable Credentials. Οι ρόλοι αυτοί είναι ο Εκδότης (Issuer), το Ψηφιακό Πορτοφόλι (Wallet) και ο Επαληθευτής (Verifier). Η συγκεκριμένη προσέγγιση επιλέχθηκε, καθώς αντικατοπτρίζει με σαφήνεια το μοντέλο εμπιστοσύνης που υιοθετείται σε ευρωπαϊκές και διεθνείς πρωτοβουλίες ψηφιακής ταυτοποίησης, όπως το European Digital Identity Wallet [35].

Η ροή της εφαρμογής ξεκινά από τον Issuer, ο οποίος είναι υπεύθυνος για την έκδοση ενός ψηφιακού διαπιστευτηρίου. Στο πρωτότυπο αυτό σύστημα, ο Issuer λαμβάνει από τον χρήστη βασικά προσωπικά δεδομένα μέσω μιας φόρμας και δημιουργεί ένα ψηφιακό πιστοποιητικό με τη μορφή JSON Web Token. Το token αυτό λειτουργεί ως το ψηφιακό ισοδύναμο ενός εγγράφου ταυτότητας ή άλλου επίσημου πιστοποιητικού.

Στη συνέχεια, το εκδοθέν token αποθηκεύεται στο Wallet του χρήστη. Το Wallet λειτουργεί ως ο κεντρικός χώρος συγκέντρωσης ψηφιακών διαπιστευτηρίων και επιπλέον δεδομένων, όπως εισιτήρια ή mock έγγραφα. Ιδιαίτερο χαρακτηριστικό της υλοποίησης αποτελεί το γεγονός ότι η πρόσβαση στο Wallet δεν είναι άμεση, αλλά προϋποθέτει την επιτυχή επαλήθευση ενός έγκυρου token. Με τον τρόπο αυτό προσομοιώνεται η έννοια της ασφαλούς πρόσβασης σε ψηφιακά πορτοφόλια, όπως αυτή υλοποιείται σε πραγματικά συστήματα.

Ο τρίτος ρόλος είναι ο Verifier, ο οποίος λαμβάνει ένα token από τον χρήστη και ελέγχει την εγκυρότητά του. Ο έλεγχος περιλαμβάνει τόσο την επαλήθευση της υπογραφής όσο και τον έλεγχο της χρονικής ισχύος του token. Το αποτέλεσμα της επαλήθευσης παρουσιάζεται στον χρήστη με σαφή και κατανοητό τρόπο, προσομοιώνοντας τη διαδικασία ελέγχου ταυτότητας ή δικαιώματος πρόσβασης σε μια υπηρεσία.

Στην εικόνα 6 παρουσιάζεται η ολοκληρωμένη ροή της εφαρμογής.



Εικόνα 6 - Γενική ροή της εφαρμογής, από την έκδοση διαπιστευτηρίου (Issuer) έως την αποθήκευση στο Wallet και την επαλήθευση από τον Verifier.

Η παραπάνω αρχιτεκτονική επιτρέπει τη σαφή διάκριση ευθυνών μεταξύ των επιμέρους υποσυστημάτων. Κάθε ρόλος έχει συγκεκριμένο σκοπό και περιορισμένο σύνολο λειτουργιών, γεγονός που διευκολύνει τόσο την κατανόηση της εφαρμογής όσο και την ανάλυση της ασφάλειας. Επιπλέον, η επιλογή αυτή καθιστά την υλοποίηση επεκτάσιμη, καθώς νέα είδη διαπιστευτηρίων ή νέοι μηχανισμοί επαλήθευσης μπορούν να ενσωματωθούν χωρίς ριζικές αλλαγές στη βασική δομή.

Αξίζει να σημειωθεί ότι, παρόλο που η εφαρμογή υλοποιείται ως ενιαίο web σύστημα, η λογική της παραμένει πλήρως διαχωρισμένη. Αυτό αντικατοπτρίζεται και στον κώδικα του αρχείου app.py, όπου οι διαδρομές (routes) οργανώνονται ανά ρόλο, με σαφή διαχωρισμό μεταξύ Issuer, Wallet και Verifier. Η επιλογή αυτή δεν είναι τυχαία, καθώς προσομοιώνει την κατανεμημένη φύση πραγματικών συστημάτων ψηφιακής ταυτότητας, όπου οι ρόλοι αυτοί συχνά υλοποιούνται από διαφορετικούς οργανισμούς ή υπηρεσίες.

Στις εικόνες 7 και 8 παρουσιάζονται αποσπάσματα του αρχείου app.py στο περιβάλλον VS Code, όπου φαίνεται ο διαχωρισμός των routes ανά υποσύστημα (Issuer, Wallet, Verifier) και ειδικότερα το route του υποσυστήματος Verifier που υλοποιεί τη διαδικασία επαλήθευσης του token που υποβάλλεται από τον χρήστη.

```python
@app.route("/issuer", methods=["GET", "POST"])
def issuer():
    if request.method == "POST":
        full_name    = (request.form.get("full_name") or "").strip()
        birth_date   = (request.form.get("birth_date") or "").strip()
        national_id = (request.form.get("national_id") or "").strip()

        nationality    = (request.form.get("nationality") or "").strip()
        gender         = (request.form.get("gender") or "").strip()
        id_issue_date = (request.form.get("id_issue_date") or "").strip()
        amka           = (request.form.get("amka") or "").strip()
        blood_type     = (request.form.get("blood_type") or "").strip()
```

Εικόνα 7 - Απόσπασμα του αρχείου app.py στο VS Code, όπου φαίνεται ο διαχωρισμός των routes ανά υποσύστημα (Issuer, Wallet, Verifier).

```python
@app.route("/verify", methods=["GET", "POST"])
def verify():
    if request.method == "POST":
        t = (request.form.get("token") or "").strip()
        ok, out = verify_token(t)
        pretty = json.dumps(out, ensure_ascii=False, indent=2) if ok else None

        return render_template("verify_result.html", ok=ok, out=out, pretty=pretty)

    return render_template("verify.html")
```

Εικόνα 8 - Απόσπασμα του αρχείου app.py στο περιβάλλον VS Code, στο οποίο παρουσιάζεται το route του υποσυστήματος Verifier και η διαδικασία επαλήθευσης του token που υποβάλλεται από τον χρήστη.

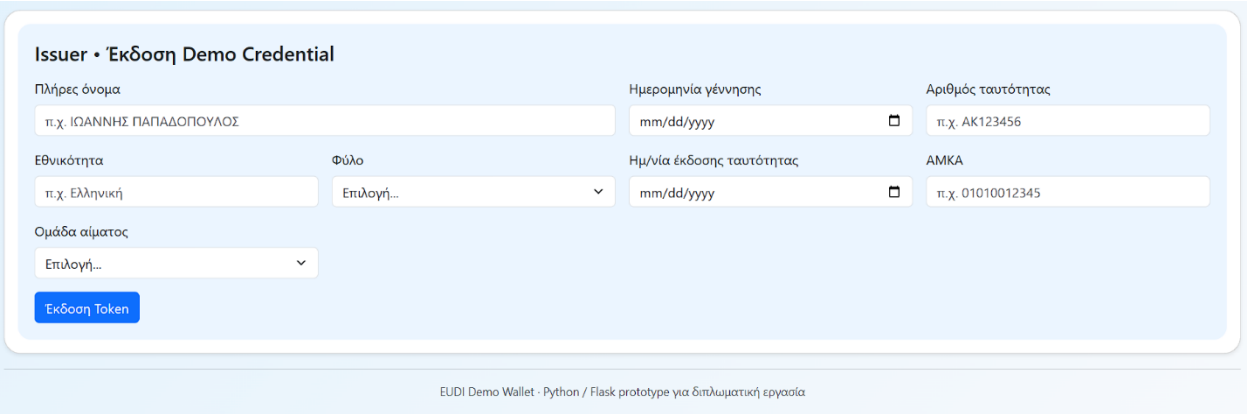
Με τη συγκεκριμένη προσέγγιση, η εφαρμογή καταφέρνει να αποδώσει με ρεαλιστικό τρόπο τις βασικές αρχές λειτουργίας ενός ψηφιακού οικοσυστήματος ταυτοποίησης, διατηρώντας παράλληλα την απλότητα που απαιτείται για εκπαιδευτικούς και ερευνητικούς σκοπούς. Η γενική αρχιτεκτονική λειτουργεί ως θεμέλιο για την αναλυτικότερη παρουσίαση των επιμέρους υποσυστημάτων, η οποία ακολουθεί στις επόμενες ενότητες του κεφαλαίου.

6.4. Υποσύστημα Issuer – Έκδοση ψηφιακών διαπιστευτηρίων

Το υποσύστημα Issuer αποτελεί το πρώτο και θεμελιώδες στάδιο στη λειτουργία της εφαρμογής, καθώς είναι υπεύθυνο για τη δημιουργία και έκδοση των ψηφιακών διαπιστευτηρίων. Στο πλαίσιο της παρούσας υλοποίησης, ο Issuer προσομοιώνει έναν επίσημο φορέα έκδοσης εγγράφων, όπως για παράδειγμα μια κρατική υπηρεσία ή έναν οργανισμό που διαθέτει την αρμοδιότητα να πιστοποιεί την ταυτότητα και τα χαρακτηριστικά ενός πολίτη.

Η βασική λειτουργία του Issuer υλοποιείται μέσω μιας web φόρμας, στην οποία ο χρήστης εισάγει προσωπικά στοιχεία. Τα στοιχεία αυτά επιλέχθηκαν με τρόπο ώστε να προσεγγίζουν ρεαλιστικά το περιεχόμενο ενός σύγχρονου εγγράφου ταυτότητας, χωρίς ωστόσο να εισάγεται υπερβολική πολυπλοκότητα. Συγκεκριμένα, περιλαμβάνονται πληροφορίες όπως το ονοματεπώνυμο, η ημερομηνία γέννησης, ο αριθμός ταυτότητας, η εθνικότητα, το φύλο, η ημερομηνία έκδοσης του εγγράφου, ο ΑΜΚΑ και η ομάδα αίματος. Η επιλογή αυτών των πεδίων δεν είναι τυχαία, καθώς συνδυάζει βασικά αναγνωριστικά στοιχεία με πρόσθετα χαρακτηριστικά

που συναντώνται συχνά σε επίσημα κρατικά έγγραφα. Στην εικόνα 9 απεικονίζεται η φόρμα του issuer και όλες οι πληροφορίες που δίνονται προς συμπλήρωση.



Εικόνα 9 - Φόρμα Issuer για την εισαγωγή προσωπικών στοιχείων και την έκδοση ψηφιακού διαπιστευτηρίου

Η φόρμα του Issuer λειτουργεί ως το σημείο εισόδου των δεδομένων στο σύστημα. Πριν από την έκδοση οποιουδήποτε διαπιστευτηρίου, πραγματοποιείται ένας βασικός έλεγχος πληρότητας των πεδίων. Ο έλεγχος αυτός διασφαλίζει ότι όλα τα απαιτούμενα δεδομένα έχουν συμπληρωθεί, αποτρέποντας τη δημιουργία ελλιπών ή λανθασμένων διαπιστευτηρίων. Αν και ο έλεγχος αυτός είναι απλός, αντικατοπτρίζει μια βασική αρχή πραγματικών συστημάτων έκδοσης εγγράφων, όπου η ακρίβεια και η πληρότητα των δεδομένων αποτελούν κρίσιμους παράγοντες αξιοπιστίας.

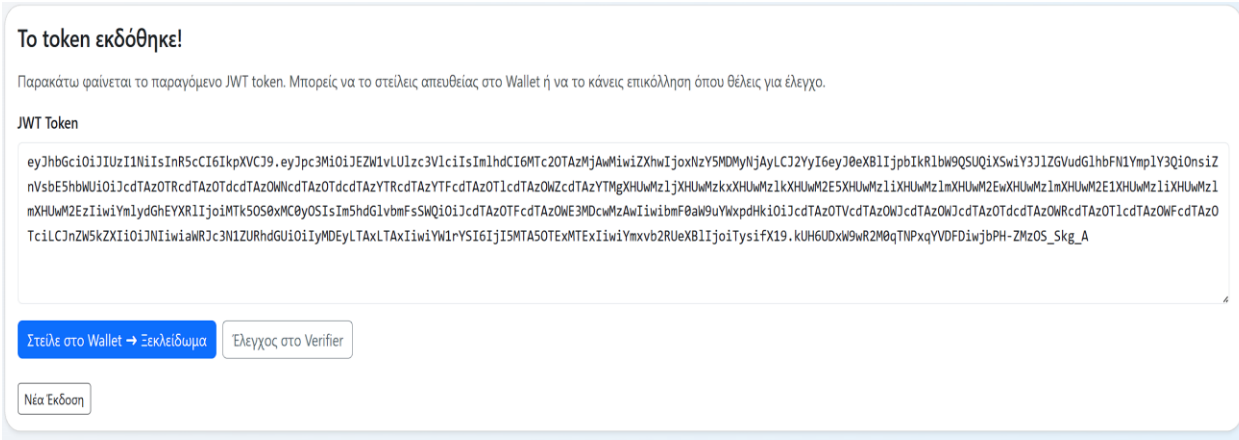
Μετά την επιτυχή υποβολή της φόρμας, τα δεδομένα που εισήχθησαν χρησιμοποιούνται για τη δημιουργία ενός JSON Web Token. Η διαδικασία αυτή υλοποιείται μέσω της συνάρτησης make_token(), η οποία συγκεντρώνει τα προσωπικά στοιχεία και τα ενσωματώνει στο payload του token. Στο ίδιο στάδιο προστίθενται και μεταδεδομένα που αφορούν τον εκδότη, καθώς και χρονικές πληροφορίες, όπως η στιγμή έκδοσης και η ημερομηνία λήξης του διαπιστευτηρίου. Στην εικόνα 10 φαίνεται η συνάρτηση make_token(), η οποία δημιουργεί και υπογράφει ένα JWT token με τα claims του χρήστη.

```python
def make_token(claims):
    now = datetime.now(timezone.utc)
    payload = {
        "iss": "Demo-Issuer",
        "iat": int(now.timestamp()),
        "exp": int((now + timedelta(minutes=TOKEN_TTL_MIN)).timestamp()),
        "vc": {
            "type": ["DemoPID"],
            "credentialSubject": claims
        }
    }
    return jwt.encode(payload, JWT_SECRET, algorithm=JWT_ALGO)
```

Εικόνα 10 - Απόσπασμα κώδικα από το αρχείο app.py που απεικονίζει τη συνάρτηση make_token() στο περιβάλλον VS Code

Η χρήση χρονικών περιορισμών (time-to-live) στο token αποτελεί συνειδητή σχεδιαστική επιλογή, καθώς αναδεικνύει τη σημασία της χρονικής ισχύος στα ψηφιακά διαπιστευτήρια. Σε πραγματικά συστήματα, ένα έγγραφο ταυτότητας ή πιστοποιητικό δεν είναι απεριόριστης διάρκειας, αλλά υπόκειται σε ημερομηνία λήξης ή επανέκδοσης. Με την ενσωμάτωση της πληροφορίας αυτής στο token, η εφαρμογή προσομοιώνει ένα βασικό χαρακτηριστικό ασφάλειας, το οποίο προστατεύει από την κατάχρηση παλαιών ή μη έγκυρων διαπιστευτηρίων.

Το εκδοθέν token παρουσιάζεται στον χρήστη σε ξεχωριστή οθόνη, όπου εμφανίζεται τόσο η συμβολοσειρά του JWT όσο και πληροφορίες σχετικά με τη διάρκεια ισχύος του. Στο σημείο αυτό, ο χρήστης έχει τη δυνατότητα να αποθηκεύσει το token στο Wallet της εφαρμογής. Η επιλογή αυτή δεν γίνεται αυτόματα, αλλά απαιτεί ρητή ενέργεια από τον χρήστη, γεγονός που ενισχύει την κατανόηση της ροής και διαχωρίζει καθαρά το στάδιο της έκδοσης από το στάδιο της αποθήκευσης. Η εικόνα 11 παρουσιάζει την οθόνη του αποτελέσματος έκδοσης διαπιστευτηρίου.



Εικόνα 11 - Οθόνη αποτελέσματος έκδοσης διαπιστευτηρίου, όπου εμφανίζεται το JWT token και η επιλογή αποθήκευσης στο Wallet

Ιδιαίτερη σημασία έχει το γεγονός ότι η αποθήκευση του token στο Wallet δεν συνεπάγεται αυτόματα και πρόσβαση στο περιεχόμενό του. Αντιθέτως, η εφαρμογή απαιτεί την επαλήθευση ενός έγκυρου token προκειμένου να «ξεκλειδωθεί» το Wallet. Με τον τρόπο αυτό, ο Issuer περιορίζεται αυστηρά στον ρόλο του εκδότη και δεν παρεμβαίνει στη διαχείριση ή παρουσίαση των διαπιστευτηρίων, ακολουθώντας τη φιλοσοφία του διαχωρισμού ρόλων που χαρακτηρίζει τα σύγχρονα συστήματα ψηφιακής ταυτότητας.

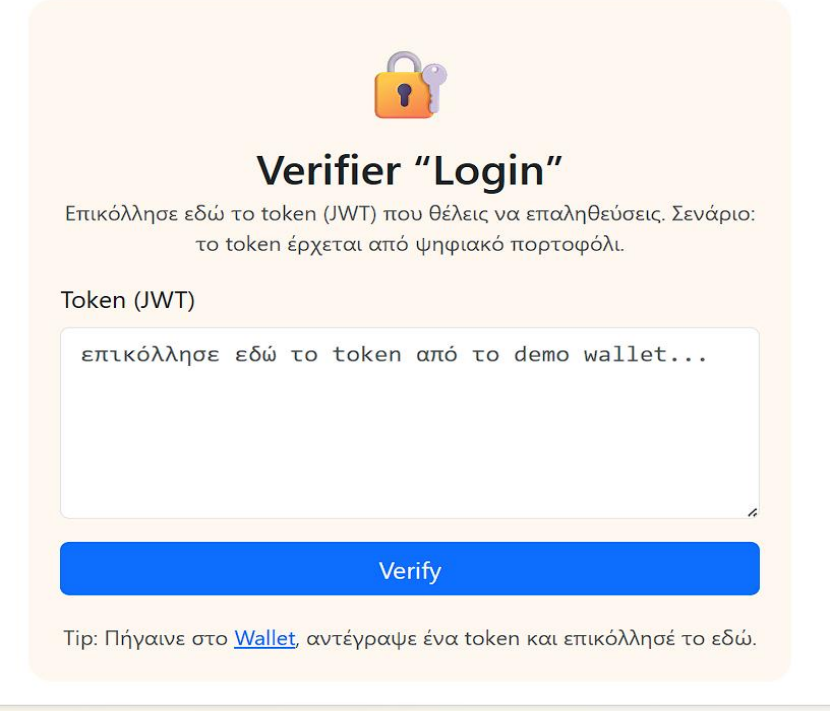
Από σχεδιαστική άποψη, το υποσύστημα Issuer υλοποιήθηκε με τρόπο απλό και κατανοητό, αποφεύγοντας σύνθετους μηχανισμούς πιστοποίησης ή διασύνδεσης με εξωτερικά μητρώα. Η επιλογή αυτή κρίθηκε σκόπιμη, καθώς στόχος της διπλωματικής εργασίας δεν είναι η πλήρης αναπαραγωγή ενός κρατικού πληροφοριακού συστήματος, αλλά η ανάδειξη των βασικών εννοιών και ροών που διέπουν τη διαδικασία έκδοσης ψηφιακών διαπιστευτηρίων.

Συνολικά, το υποσύστημα Issuer λειτουργεί ως το σημείο εκκίνησης της εφαρμογής και θέτει τις βάσεις για τη μετέπειτα διαχείριση και επαλήθευση των διαπιστευτηρίων. Η σαφής οριοθέτηση των λειτουργιών του και η απλή, αλλά ρεαλιστική, υλοποίησή του καθιστούν το υποσύστημα αυτό ιδιαίτερα κατάλληλο για εκπαιδευτική και ερευνητική χρήση.

6.5. Μηχανισμός Wallet Access και προστασία πρόσβασης

Ένα από τα βασικά χαρακτηριστικά της υλοποίησης που διαφοροποιεί την εφαρμογή από ένα απλό demo αποθήκευσης δεδομένων είναι η ύπαρξη μηχανισμού ελεγχόμενης πρόσβασης στο ψηφιακό πορτοφόλι. Αντί το Wallet να είναι άμεσα προσβάσιμο μετά την έκδοση ενός διαπιστευτηρίου, η εφαρμογή απαιτεί από τον χρήστη να αποδείξει ότι κατέχει ένα έγκυρο token πριν αποκτήσει πρόσβαση στο περιεχόμενο του πορτοφολιού. Η σχεδιαστική αυτή επιλογή αποσκοπεί στην προσομοίωση της λογικής ασφαλούς πρόσβασης που συναντάται σε πραγματικά ψηφιακά πορτοφόλια, τόσο σε κρατικές όσο και σε ιδιωτικές εφαρμογές.

Ο μηχανισμός αυτός υλοποιείται μέσω μιας ενδιάμεσης σελίδας, η οποία λειτουργεί ως “πύλη” προς το Wallet. Ο χρήστης, αφού αποκτήσει ένα token από τον Issuer, καλείται να το εισαγάγει στη σελίδα Wallet Access. Στο σημείο αυτό, το token ελέγχεται ως προς την εγκυρότητά του, πριν επιτραπεί οποιαδήποτε περαιτέρω ενέργεια. Η εικόνα 12 παρουσιάζει την σελίδα όπου επικυρώνεται το διαπιστευτήριο πριν επιτευχθεί η σύνδεση στο wallet.



Εικόνα 12 - Σελίδα Wallet Access, όπου ο χρήστης καλείται να εισαγάγει έγκυρο token για την πρόσβαση στο ψηφιακό πορτοφόλι

Η διαδικασία επαλήθευσης βασίζεται στη συνάρτηση verify_token(), η οποία ελέγχει τόσο την υπογραφή όσο και τη χρονική ισχύ του token. Αν το token είναι ληγμένο ή αλλοιωμένο, η πρόσβαση απορρίπτεται και ο χρήστης ενημερώνεται κατάλληλα μέσω μηνύματος ειδοποίησης. Αντιθέτως, σε περίπτωση επιτυχούς επαλήθευσης, το σύστημα καταγράφει στη συνεδρία του χρήστη ότι το Wallet έχει «ξεκλειδωθεί». Η πληροφορία αυτή αποθηκεύεται προσωρινά στο session και χρησιμοποιείται ως προϋπόθεση για την εμφάνιση της σελίδας του Wallet. Η εικόνα 13 απεικονίζει τον έλεγχο wallet_unlocked.

```python
@app.route("/wallet")
def wallet():
    if not session.get("WALLET_UNLOCKED"):
        flash("Για πρόσβαση στο wallet χρειάζεται πρώτα έγκυρο token.", "warning")
        return redirect(url_for("wallet_access"))
```

Εικόνα 13 - Απόσπασμα κώδικα από το app.py που απεικονίζει τον έλεγχο WALLET_UNLOCKED πριν την πρόσβαση στο Wallet

Η χρήση session-based μεταβλητών για τον έλεγχο πρόσβασης αποτελεί συνειδητή επιλογή απλότητας. Παρότι σε ένα παραγωγικό σύστημα θα απαιτούνταν πιο σύνθετοι μηχανισμοί αυθεντικοποίησης και διαχείρισης χρηστών, η συγκεκριμένη προσέγγιση επαρκεί για την προσομοίωση της βασικής λογικής ελέγχου πρόσβασης και επιτρέπει την καθαρή κατανόηση της ροής από τον αναγνώστη.

Η ύπαρξη του Wallet Access προσθέτει ένα επιπλέον επίπεδο ρεαλισμού στην εφαρμογή. Ο χρήστης δεν αντιμετωπίζει το Wallet ως έναν απλό αποθηκευτικό χώρο, αλλά ως ένα προστατευμένο περιβάλλον, στο οποίο αποκτά πρόσβαση μόνο εφόσον αποδείξει ότι κατέχει έγκυρα διαπιστευτήρια. Με τον τρόπο αυτό, αναδεικνύεται στην πράξη η σημασία της έννοιας της κατοχής (possession) ενός ψηφιακού διαπιστευτηρίου.

6.6. Υποσύστημα Wallet – Διαχείριση ψηφιακών διαπιστευτηρίων

Αφού ολοκληρωθεί επιτυχώς η διαδικασία Wallet Access, ο χρήστης αποκτά πρόσβαση στο κύριο υποσύστημα Wallet. Το Wallet αποτελεί τον κεντρικό κόμβο της εφαρμογής, καθώς συγκεντρώνει όλα τα ψηφιακά διαπιστευτήρια και τα πρόσθετα δεδομένα που σχετίζονται με τον χρήστη. Η υλοποίησή του σχεδιάστηκε με τρόπο που να προσομοιώνει τη δομή και τη λογική σύγχρονων κυβερνητικών ψηφιακών πορτοφολιών.

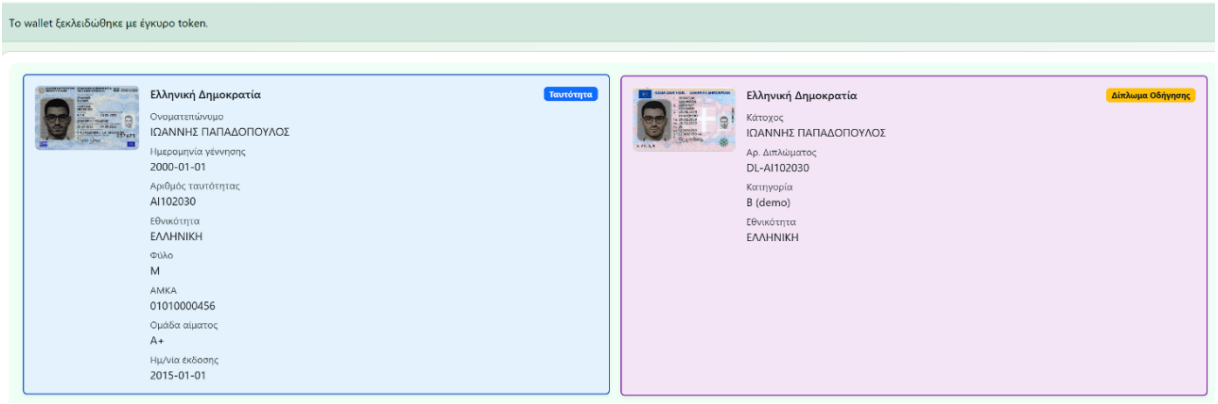
Κατά την είσοδο στο Wallet, ο χρήστης βλέπει μια συνολική απεικόνιση των διαθέσιμων διαπιστευτηρίων. Τα tokens που έχουν αποθηκευτεί στο Wallet αποκωδικοποιούνται τοπικά, χωρίς έλεγχο υπογραφής, με αποκλειστικό σκοπό την προβολή των περιεχομένων τους. Η επιλογή αυτή έγινε για λόγους ευχρηστίας και οπτικοποίησης των δεδομένων, καθώς επιτρέπει την άμεση κατανόηση του τι περιέχει κάθε διαπιστευτήριο. Στην εικόνα 14 παρουσιάζονται τα αποθηκευμένα tokens που έχουν ήδη εγκριθεί.

Εικόνα 14 - Κύρια οθόνη του Wallet με απεικόνιση αποθηκευμένων tokens και αποκωδικοποιημένων δεδομένων

Ιδιαίτερη έμφαση δόθηκε στην παρουσίαση ενός «κύριου υποκειμένου», το οποίο προκύπτει από το πιο πρόσφατο token που έχει εκδοθεί. Τα προσωπικά στοιχεία του χρήστη, όπως το ονοματεπώνυμο, η ημερομηνία γέννησης και ο αριθμός ταυτότητας, εμφανίζονται με τρόπο που θυμίζει πραγματικό έγγραφο ταυτοποίησης. Η αισθητική αυτή επιλογή δεν είναι απλώς διακοσμητική, αλλά στοχεύει στη δημιουργία μιας εμπειρίας χρήστη που προσεγγίζει πραγματικές εφαρμογές ψηφιακής ταυτότητας.

Παράλληλα, στο Wallet ενσωματώνονται mock αναπαραστάσεις επίσημων εγγράφων, όπως δελτίο ταυτότητας και άδεια οδήγησης. Τα έγγραφα αυτά εμφανίζονται ως κάρτες, με διακριτό

χρωματικό πλαίσιο και ενδεικτική φωτογραφία, ενισχύοντας τον ρεαλισμό της εφαρμογής. Αν και τα δεδομένα τους δεν προέρχονται από ξεχωριστά tokens, η παρουσία τους στο Wallet αναδεικνύει τη δυνατότητα συγκέντρωσης πολλαπλών ειδών διαπιστευτηρίων σε ένα ενιαίο ψηφιακό περιβάλλον. Η εικόνα 15 απεικονίζει την οθόνη αποθήκευσης των mock διαπιστευτηρίων ψηφιακής ταυτότητας και άδειας οδήγησης.



Εικόνα 15 - Mock ψηφιακή ταυτότητα και άδεια οδήγησης όπως εμφανίζονται στο Wallet

Ένα επιπλέον στοιχείο που ενισχύει τη λειτουργικότητα του Wallet είναι η διαχείριση εισιτηρίων. Ο χρήστης μπορεί να προσθέσει mock εισιτήρια για αθλητικές ή άλλες εκδηλώσεις, τα οποία αποθηκεύονται προσωρινά στη συνεδρία του. Η λειτουργία αυτή αντλεί έμπνευση από το ελληνικό Gov Wallet, στο οποίο ο πολίτης είναι υποχρεωμένος να αποθηκεύει τα εισιτήριά του για την είσοδο σε αθλητικές διοργανώσεις. Μέσα από αυτή τη λειτουργία, αναδεικνύεται η ευελιξία ενός ψηφιακού πορτοφολιού να φιλοξενεί όχι μόνο διαπιστευτήρια ταυτοποίησης, αλλά και έγγραφα προσωρινού χαρακτήρα. Στην εικόνα 16 φαίνονται τα αποθηκευμένα εισιτήρια του ψηφιακού πορτοφολιού.

Εικόνα 16 - Διαχείριση εισιτηρίων στο Wallet, με επιλογές προσθήκης και διαγραφής

Η δυνατότητα διαγραφής εισιτηρίων και συνολικού καθαρισμού του Wallet ενσωματώνει την έννοια του ελέγχου από τον χρήστη. Ο χρήστης μπορεί οποιαδήποτε στιγμή να αφαιρέσει δεδομένα από το Wallet ή να αποσυνδεθεί πλήρως, γεγονός που ενισχύει τη φιλοσοφία της κυριαρχίας του χρήστη πάνω στα προσωπικά του δεδομένα. Η συγκεκριμένη προσέγγιση συνάδει με τις αρχές προστασίας προσωπικών δεδομένων και ιδιωτικότητας που διέπουν τα σύγχρονα ευρωπαϊκά ψηφιακά συστήματα [35].

Συνολικά, το υποσύστημα Wallet δεν λειτουργεί απλώς ως αποθήκη δεδομένων, αλλά ως κεντρικό σημείο αλληλεπίδρασης του χρήστη με τα ψηφιακά του διαπιστευτήρια. Μέσα από την ελεγχόμενη πρόσβαση, την οπτικοποίηση των δεδομένων και την ενσωμάτωση πρόσθετων εγγράφων, η εφαρμογή καταφέρνει να αποδώσει με ρεαλιστικό και κατανοητό τρόπο τη λειτουργία ενός σύγχρονου ψηφιακού πορτοφολιού.

6.7. Υποσύστημα Verifier – Επικύρωση ψηφιακών διαπιστευτηρίων

Το υποσύστημα Verifier αποτελεί το τελικό στάδιο στη ροή της εφαρμογής και είναι υπεύθυνο για την επαλήθευση της εγκυρότητας των ψηφιακών διαπιστευτηρίων που παρουσιάζονται από τον χρήστη. Στο πλαίσιο της παρούσας υλοποίησης, ο Verifier προσομοιώνει έναν τρίτο φορέα, ο οποίος δεν συμμετέχει ούτε στην έκδοση ούτε στην αποθήκευση των διαπιστευτηρίων, αλλά περιορίζεται αποκλειστικά στον έλεγχο της αυθεντικότητας και της ισχύος τους.

Η λειτουργία του Verifier υλοποιείται μέσω μιας ξεχωριστής σελίδας της εφαρμογής, η οποία έχει σχεδιαστεί με τρόπο που θυμίζει σελίδα σύνδεσης ή ελέγχου πρόσβασης. Ο χρήστης καλείται να εισαγάγει ένα token, το οποίο στη συνέχεια αποστέλλεται προς επαλήθευση. Η επιλογή αυτής της σχεδίασης δεν είναι τυχαία, καθώς αντανακλά τη λογική πραγματικών σεναρίων, όπου ένας πολίτης παρουσιάζει το ψηφιακό του διαπιστευτήριο για να αποκτήσει πρόσβαση σε μια υπηρεσία ή να αποδείξει την ταυτότητά του.

Η διαδικασία επαλήθευσης βασίζεται στη συνάρτηση verify_token(), η οποία αποτελεί κρίσιμο στοιχείο της εφαρμογής. Η συνάρτηση αυτή λαμβάνει ως είσοδο το token και επιχειρεί να το αποκωδικοποιήσει χρησιμοποιώντας το μυστικό κλειδί και τον αλγόριθμο υπογραφής που έχουν οριστεί στο σύστημα. Σε περίπτωση που η αποκωδικοποίηση είναι επιτυχής και το token δεν έχει λήξει, η επαλήθευση θεωρείται επιτυχής. Αντιθέτως, σε περίπτωση αλλοιωμένου ή ληγμένου

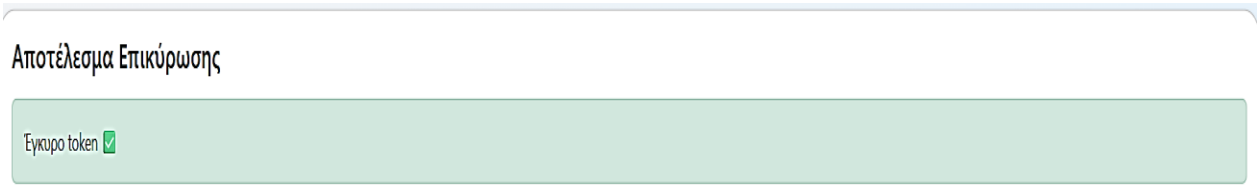
token, η επαλήθευση αποτυγχάνει. Η εικόνα 17 απεικονίζει το κομμάτι κώδικα που δίνει έμφαση στην συνάρτηση verify_token().

```python
def verify_token(t):
    try:
        data = jwt.decode(t, JWT_SECRET, algorithms=[JWT_ALGO])
        return True, data
    except jwt.ExpiredSignatureError:
        return False, "Το token έληξε."
    except Exception as e:
        return False, f"Μη έγκυρο token: {e}"
```

Εικόνα 17 - Απόσπασμα κώδικα από το αρχείο app.py που απεικονίζει τη συνάρτηση verify_token()

Η επιλογή να πραγματοποιείται έλεγχος τόσο της υπογραφής όσο και της χρονικής ισχύος του token είναι καθοριστική για την αξιοπιστία του Verifier. Μέσα από τον έλεγχο της υπογραφής διασφαλίζεται ότι το token έχει εκδοθεί από έμπιστο Issuer και δεν έχει τροποποιηθεί. Παράλληλα, ο έλεγχος της ημερομηνίας λήξης αποτρέπει τη χρήση παλαιών διαπιστευτηρίων, τα οποία ενδέχεται να μην αντικατοπτρίζουν πλέον την τρέχουσα κατάσταση του χρήστη.

Το αποτέλεσμα της επαλήθευσης παρουσιάζεται στον χρήστη σε ξεχωριστή οθόνη αποτελέσματος. Σε περίπτωση επιτυχίας, εμφανίζεται σαφής ένδειξη ότι το token είναι έγκυρο, συνοδευόμενη από τα αποκωδικοποιημένα δεδομένα του διαπιστευτηρίου. Σε περίπτωση αποτυχίας, ο χρήστης ενημερώνεται με αντίστοιχο μήνυμα σφάλματος, το οποίο εξηγεί συνοπτικά τον λόγο της αποτυχίας, όπως για παράδειγμα τη λήξη του token. Στην εικόνα 18 απεικονίζεται το αποτέλεσμα της επικύρωσης ενός διαπιστευτηρίου.



Εικόνα 18 - Οθόνη αποτελέσματος επαλήθευσης με επιτυχή επικύρωση ψηφιακού διαπιστευτηρίου

Η συγκεκριμένη προσέγγιση ενισχύει τη διαφάνεια της διαδικασίας επαλήθευσης, καθώς ο χρήστης μπορεί να δει όχι μόνο το αποτέλεσμα, αλλά και το περιεχόμενο του διαπιστευτηρίου που επαληθεύτηκε. Αν και σε ένα πραγματικό σύστημα ο Verifier δεν θα είχε απαραίτητα πρόσβαση σε όλα τα δεδομένα, η επιλογή αυτή εξυπηρετεί εκπαιδευτικούς σκοπούς και διευκολύνει την κατανόηση της δομής των ψηφιακών διαπιστευτηρίων.

Αξίζει να σημειωθεί ότι το υποσύστημα Verifier είναι πλήρως ανεξάρτητο από το Wallet. Ο Verifier δεν γνωρίζει αν το token προέρχεται από το Wallet της εφαρμογής ή αν έχει εισαχθεί χειροκίνητα από τον χρήστη. Το γεγονός αυτό αντικατοπτρίζει την αρχή της ελαχιστοποίησης εμπιστοσύνης, σύμφωνα με την οποία ο Verifier δεν βασίζεται σε εσωτερικές καταστάσεις της εφαρμογής, αλλά αποκλειστικά στην εγκυρότητα του ίδιου του διαπιστευτηρίου.

Συνολικά, το υποσύστημα Verifier ολοκληρώνει τη βασική λειτουργική αλυσίδα της εφαρμογής και αποδεικνύει στην πράξη τον τρόπο με τον οποίο ένα ψηφιακό διαπιστευτήριο μπορεί να παρουσιαστεί και να επαληθευτεί από έναν τρίτο φορέα. Μέσα από τη σαφή απεικόνιση της διαδικασίας επαλήθευσης, ο αναγνώστης αποκτά ολοκληρωμένη εικόνα της λειτουργίας ενός συστήματος ψηφιακής ταυτότητας, από την έκδοση έως την τελική χρήση.

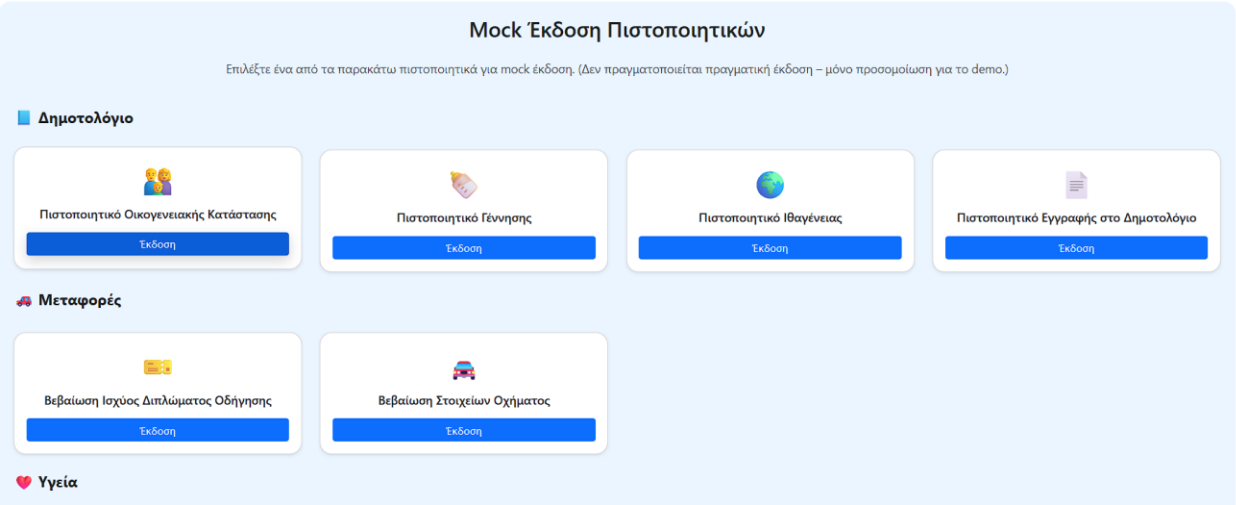
6.8. Υποσύστημα Mock Certificates – Προσομοίωση έκδοσης ψηφιακών πιστοποιητικών

Το υποσύστημα Mock Certificates σχεδιάστηκε με σκοπό την προσομοίωση της διαδικασίας έκδοσης ψηφιακών πιστοποιητικών από κρατικές ή θεσμικές υπηρεσίες. Σε αντίθεση με τον Issuer, ο οποίος εκδίδει ένα γενικό ψηφιακό διαπιστευτήριο ταυτοποίησης, το συγκεκριμένο υποσύστημα λειτουργεί ως μια ενοποιημένη ψηφιακή πύλη, μέσω της οποίας ο χρήστης μπορεί να αιτηθεί διαφορετικά είδη πιστοποιητικών, χωρίς αυτά να οδηγούν σε πραγματική έκδοση ή αποθήκευση δεδομένων.

Η επιλογή να υλοποιηθεί το υποσύστημα αυτό σε μορφή mock σελίδας είναι απολύτως συνειδητή. Στόχος δεν είναι η τεχνική υλοποίηση πλήρους μηχανισμού έκδοσης πιστοποιητικών, αλλά η απεικόνιση της εμπειρίας χρήστη και της λογικής που διέπει τις σύγχρονες ψηφιακές

κρατικές πλατφόρμες. Με τον τρόπο αυτό, ο αναγνώστης μπορεί να κατανοήσει πώς ένα ψηφιακό πορτοφόλι θα μπορούσε να επεκταθεί ώστε να περιλαμβάνει πλήθος διαφορετικών εγγράφων και πιστοποιητικών.

Η σελίδα Mock Certificates παρουσιάζει στον χρήστη μια οργανωμένη λίστα διαθέσιμων πιστοποιητικών, τα οποία είναι ομαδοποιημένα σε θεματικές κατηγορίες. Οι κατηγορίες αυτές περιλαμβάνουν, μεταξύ άλλων, πιστοποιητικά οικογενειακής κατάστασης, φορολογικά πιστοποιητικά, εκπαιδευτικά έγγραφα και λοιπά διοικητικά πιστοποιητικά. Η συγκεκριμένη ομαδοποίηση δεν είναι τυχαία, καθώς αντικατοπτρίζει τον τρόπο με τον οποίο οργανώνονται οι υπηρεσίες σε πραγματικές πλατφόρμες ηλεκτρονικής διακυβέρνησης, διευκολύνοντας την πλοήγηση και την αναζήτηση από τον χρήστη. Στην εικόνα 19 παρουσιάζονται κάποια από τα mock πιστοποιητικά που μπορούν να εκδοθούν μέσω της υλοποίησης ψηφιακού πορτοφολιού.



Εικόνα 19 - Σελίδα Mock Certificates με κατηγοριοποιημένα πιστοποιητικά και επιλογές έκδοσης

Η επιλογή των πιστοποιητικών που εμφανίζονται στη σελίδα έγινε με γνώμονα τη ρεαλιστικότητα και τη συνάφεια με το ελληνικό και ευρωπαϊκό διοικητικό περιβάλλον. Ενδεικτικά, περιλαμβάνεται το πιστοποιητικό οικογενειακής κατάστασης, το οποίο αποτελεί ένα από τα πιο συχνά ζητούμενα διοικητικά έγγραφα. Παρακάτω, ενσωματώνονται βεβαιώσεις Διπλώματος Οδήγησης και Στοιχείων Οχήματος, οι οποίες αναδεικνύουν τη δυνατότητα ενός

ψηφιακού πορτοφολιού να φιλοξενεί έγγραφα από διαφορετικούς τομείς της δημόσιας διοίκησης.

Από λειτουργικής άποψης, τα κουμπιά έκδοσης των πιστοποιητικών δεν ενεργοποιούν κάποια πραγματική διαδικασία δημιουργίας εγγράφου. Αντίθετα, λειτουργούν ως ενδεικτικά στοιχεία διεπαφής, τα οποία επιτρέπουν στον χρήστη να αντιληφθεί πώς θα μπορούσε να εξελιχθεί η εφαρμογή σε ένα πλήρες σύστημα. Η επιλογή αυτή αποτρέπει την υπερφόρτωση της υλοποίησης με πολύπλοκες διαδικασίες, ενώ ταυτόχρονα διατηρεί τον εκπαιδευτικό και ερευνητικό χαρακτήρα της εφαρμογής.

Η ύπαρξη του υποσυστήματος Mock Certificates προσθέτει σημαντική αξία στην εφαρμογή, καθώς μετατοπίζει την προσοχή από την απλή ταυτοποίηση προς ένα ευρύτερο οικοσύστημα ψηφιακών υπηρεσιών. Ο χρήστης δεν αντιμετωπίζει πλέον το ψηφιακό πορτοφόλι αποκλειστικά ως μέσο απόδειξης ταυτότητας, αλλά ως κεντρικό αποθετήριο ψηφιακών εγγράφων, τα οποία μπορούν να χρησιμοποιηθούν σε ποικίλα διοικητικά σενάρια.

Από σχεδιαστική σκοπιά, το υποσύστημα αυτό συμβάλλει στη συνοχή της εφαρμογής, καθώς εναρμονίζεται αισθητικά και λειτουργικά με το Wallet. Τα πιστοποιητικά παρουσιάζονται ως κάρτες με σαφή τίτλο και περιγραφή, ενώ η χρωματική παλέτα και η διάταξη των στοιχείων παραμένουν συνεπείς με το υπόλοιπο περιβάλλον της εφαρμογής. Η συνέπεια αυτή ενισχύει την αίσθηση ότι όλα τα υποσυστήματα αποτελούν μέρη ενός ενιαίου ψηφιακού οικοσυστήματος.

Σε θεωρητικό επίπεδο, η προσθήκη των Mock Certificates επιτρέπει τη σύνδεση της υλοποίησης με τις έννοιες της επεκτασιμότητας και της διαλειτουργικότητας. Ένα πραγματικό ψηφιακό πορτοφόλι δεν περιορίζεται σε ένα μόνο είδος διαπιστευτηρίου, αλλά οφείλει να υποστηρίζει πολλαπλές πηγές δεδομένων και διαφορετικούς τύπους εγγράφων. Η παρούσα υλοποίηση, παρότι απλουστευμένη, αναδεικνύει αυτή τη λογική και δημιουργεί γέφυρα μεταξύ της θεωρίας και της πρακτικής εφαρμογής.

Συνολικά, το υποσύστημα Mock Certificates λειτουργεί ως συμπληρωματικό στοιχείο της εφαρμογής, το οποίο ενισχύει τον ρεαλισμό και διευρύνει το πεδίο εφαρμογής του ψηφιακού πορτοφολιού. Μέσα από τη συγκεκριμένη σελίδα, ο αναγνώστης μπορεί να αντιληφθεί πώς ένα

τέτοιο σύστημα θα μπορούσε να εξελιχθεί σε πλήρη ψηφιακή πλατφόρμα εξυπηρέτησης πολιτών.

6.9. Θέματα ασφάλειας, σχεδιαστικοί περιορισμοί και τεχνικές επιλογές

Η υλοποίηση του πρωτοτύπου ψηφιακού πορτοφολιού συνοδεύεται από συγκεκριμένες σχεδιαστικές επιλογές που σχετίζονται άμεσα με ζητήματα ασφάλειας, αλλά και από περιορισμούς που προκύπτουν τόσο από τον εκπαιδευτικό χαρακτήρα της εφαρμογής όσο και από τη συνειδητή απόφαση διατήρησης της απλότητας. Η ανάλυση των στοιχείων αυτών κρίνεται ιδιαίτερα σημαντική, καθώς επιτρέπει την κατανόηση των διαφορών μεταξύ ενός ερευνητικού πρωτοτύπου και ενός πλήρως παραγωγικού συστήματος ψηφιακής ταυτότητας.

Σε επίπεδο ασφάλειας, ο βασικός μηχανισμός προστασίας της εφαρμογής στηρίζεται στη χρήση JSON Web Tokens για την αναπαράσταση των ψηφιακών διαπιστευτηρίων. Τα JWT παρέχουν έναν δομημένο και τυποποιημένο τρόπο ενσωμάτωσης δεδομένων, υπογραφής και ελέγχου χρονικής ισχύος. Στο πλαίσιο της υλοποίησης, κάθε token περιλαμβάνει πληροφορίες σχετικά με τον εκδότη, τον χρόνο έκδοσης και την ημερομηνία λήξης, στοιχεία τα οποία αξιοποιούνται κατά τη διαδικασία επαλήθευσης από τον Verifier. Η ύπαρξη ημερομηνίας λήξης αποτελεί κρίσιμο χαρακτηριστικό, καθώς αποτρέπει τη χρήση παρωχημένων διαπιστευτηρίων και αναδεικνύει τη σημασία της χρονικής εγκυρότητας στα συστήματα ψηφιακής ταυτοποίησης.

Ωστόσο, η εφαρμογή δεν υλοποιεί πλήρη υποδομή διαχείρισης κλειδιών ή μηχανισμούς ασύμμετρης κρυπτογραφίας. Η υπογραφή των tokens πραγματοποιείται με συμμετρικό μυστικό κλειδί, το οποίο είναι κοινό τόσο στον Issuer όσο και στον Verifier. Η επιλογή αυτή έγινε με γνώμονα την απλότητα και τη διδακτική αξία της υλοποίησης, καθώς επιτρέπει την κατανόηση της βασικής λογικής των JWT χωρίς την ανάγκη διαχείρισης πιστοποιητικών, δημόσιων κλειδιών ή υποδομών PKI. Παρόλα αυτά, ο συγκεκριμένος σχεδιασμός δεν θα ήταν επαρκής σε ένα πραγματικό παραγωγικό περιβάλλον, όπου απαιτείται αυστηρός διαχωρισμός ρόλων και ισχυρότερη κρυπτογραφική ασφάλεια.

Ένας ακόμη σημαντικός σχεδιαστικός περιορισμός αφορά τη διαχείριση της κατάστασης του χρήστη. Η εφαρμογή χρησιμοποιεί session-based μηχανισμούς για την αποθήκευση πληροφοριών, όπως το αν το Wallet έχει ξεκλειδωθεί ή ποια tokens και εισιτήρια είναι

διαθέσιμα. Η προσέγγιση αυτή είναι επαρκής για ένα demo περιβάλλον, καθώς επιτρέπει την προσωρινή αποθήκευση δεδομένων χωρίς τη χρήση βάσης δεδομένων. Ωστόσο, σε ένα πραγματικό σύστημα ψηφιακού πορτοφολιού, η αποθήκευση κρίσιμων δεδομένων στη μνήμη της συνεδρίας θα θεωρούνταν ανεπαρκής και ενδεχομένως επισφαλής, ιδιαίτερα σε περιβάλλοντα με πολλούς χρήστες ή κατανε‘μημένες υποδομές. Στην εικόνα 20 φαίνεται το απόσπασμα κώδικα όπου ελέγχεται η πρόσβαση στο wallet και εμφανίζονται τα αποθηκευμένα tokens.

```python
@app.route("/wallet")
def wallet():
    if not session.get("WALLET_UNLOCKED"):
        flash("Για πρόσβαση στο wallet χρειάζεται πρώτα έγκυρο token.", "warning")
        return redirect(url_for("wallet_access"))

    items = []
    for t in session.get("WALLET", []):
        try:
            dec = jwt.decode(t, options={"verify_signature": False})
            pretty = json.dumps(dec, ensure_ascii=False, indent=2)
        except Exception:
            dec = None
            pretty = "{}"
        items.append({"token": t, "decoded": dec, "pretty": pretty})

    primary = None
    if items and items[-1]["decoded"]:
        vc = items[-1]["decoded"].get("vc", {})
        primary = vc.get("credentialSubject")

    tickets = session.get("TICKETS", [])

    return render_template("wallet.html", items=items, primary=primary, tickets=tickets)
```

Εικόνα 20 - Απόσπασμα κώδικα που απεικονίζει τη χρήση session μεταβλητών για τον έλεγχο πρόσβασης στο Wallet

Ιδιαίτερη σημασία έχει επίσης το γεγονός ότι η εφαρμογή δεν υλοποιεί μηχανισμούς ισχυρής αυθεντικοποίησης χρήστη, όπως πολυπαραγοντικό έλεγχο ή βιομετρικά δεδομένα. Η πρόσβαση στο Wallet βασίζεται αποκλειστικά στην κατοχή ενός έγκυρου token, γεγονός που εξυπηρετεί τον σκοπό της προσομοίωσης αλλά δεν ανταποκρίνεται στις απαιτήσεις πραγματικών ψηφιακών πορτοφολιών, όπου η προστασία της ταυτότητας του χρήστη αποτελεί ύψιστη προτεραιότητα.

Παρά ταύτα, η συγκεκριμένη επιλογή επιτρέπει την ανάδειξη της έννοιας της «κατοχής διαπιστευτηρίου» ως βασικού παράγοντα πρόσβασης.

Από πλευράς ιδιωτικότητας, η εφαρμογή υιοθετεί μια απλουστευμένη προσέγγιση παρουσίασης δεδομένων. Κατά την επαλήθευση ενός token, εμφανίζονται όλα τα περιεχόμενα του διαπιστευτηρίου, ώστε ο χρήστης να μπορεί να κατανοήσει πλήρως τη δομή και το περιεχόμενό του. Σε πραγματικά συστήματα, ωστόσο, εφαρμόζεται συχνά η αρχή της ελαχιστοποίησης δεδομένων, σύμφωνα με την οποία ο Verifier λαμβάνει μόνο τις απολύτως απαραίτητες πληροφορίες για τον συγκεκριμένο σκοπό επαλήθευσης. Η απουσία τέτοιων μηχανισμών στην παρούσα υλοποίηση αποτελεί συνειδητό περιορισμό, ο οποίος δικαιολογείται από τον εκπαιδευτικό χαρακτήρα του έργου.

Ένας ακόμη περιορισμός αφορά τη μη ύπαρξη μόνιμης αποθήκευσης δεδομένων. Η εφαρμογή δεν χρησιμοποιεί βάση δεδομένων, γεγονός που σημαίνει ότι όλα τα δεδομένα χάνονται με τον τερματισμό της συνεδρίας. Η επιλογή αυτή απλοποιεί σημαντικά την υλοποίηση και μειώνει τον τεχνικό φόρτο, αλλά ταυτόχρονα περιορίζει τη δυνατότητα μακροχρόνιας διαχείρισης διαπιστευτηρίων. Σε ένα πλήρες σύστημα, θα απαιτούνταν μηχανισμοί ασφαλούς αποθήκευσης, κρυπτογράφησης δεδομένων σε κατάσταση ηρεμίας και διαχείρισης αντιγράφων ασφαλείας.

Παρά τους παραπάνω περιορισμούς, η υλοποίηση θεωρείται επαρκής για την επίτευξη των στόχων της διπλωματικής εργασίας. Η εφαρμογή καταφέρνει να αναδείξει με σαφή τρόπο τις βασικές αρχές λειτουργίας ενός ψηφιακού πορτοφολιού, να προσομοιώσει ρεαλιστικά σενάρια χρήσης και να επιτρέψει την πρακτική διερεύνηση κρίσιμων εννοιών, όπως η έκδοση, η αποθήκευση και η επαλήθευση ψηφιακών διαπιστευτηρίων.

Συνολικά, η ανάλυση των θεμάτων ασφάλειας και των σχεδιαστικών περιορισμών δεν μειώνει την αξία της υλοποίησης, αλλά αντιθέτως ενισχύει τον επιστημονικό της χαρακτήρα. Μέσα από τη συνειδητή αναγνώριση των ορίων του συστήματος, καθίσταται σαφές ότι το πρωτότυπο λειτουργεί ως ερευνητικό εργαλείο και όχι ως τελικό προϊόν, δημιουργώντας ταυτόχρονα γόνιμο έδαφος για μελλοντικές επεκτάσεις και βελτιώσεις.

6.10. Επεκτασιμότητα, μελλοντικές βελτιώσεις και συνολική αξιολόγηση της υλοποίησης

Η υλοποίηση του πρωτοτύπου ψηφιακού πορτοφολιού που παρουσιάστηκε στο παρόν κεφάλαιο σχεδιάστηκε εξαρχής με γνώμονα την απλότητα και τον εκπαιδευτικό χαρακτήρα. Παρόλα αυτά, η αρχιτεκτονική και οι τεχνολογικές επιλογές που υιοθετήθηκαν επιτρέπουν την εύκολη επέκταση του συστήματος, τόσο σε επίπεδο λειτουργικότητας όσο και σε επίπεδο ασφάλειας και διαλειτουργικότητας. Η ανάλυση των δυνατοτήτων επεκτασιμότητας κρίνεται ιδιαίτερα σημαντική, καθώς αναδεικνύει τη δυναμική της υλοποίησης και τη δυνατότητα μετεξέλιξής της σε ένα πιο ολοκληρωμένο σύστημα.

Ένα από τα βασικά σημεία μελλοντικής βελτίωσης αφορά τον μηχανισμό έκδοσης και υπογραφής των ψηφιακών διαπιστευτηρίων. Στην παρούσα υλοποίηση, χρησιμοποιείται συμμετρική κρυπτογραφία για την υπογραφή των JWT, γεγονός που απλοποιεί τη διαδικασία αλλά περιορίζει τον διαχωρισμό ρόλων μεταξύ Issuer και Verifier [37]. Σε ένα πιο προχωρημένο σύστημα, θα μπορούσε να υιοθετηθεί ασύμμετρη κρυπτογραφία, με τη χρήση δημόσιων και ιδιωτικών κλειδιών, ώστε ο Verifier να επαληθεύει την υπογραφή χωρίς να κατέχει το μυστικό κλειδί του Issuer. Η προσέγγιση αυτή ευθυγραμμίζεται περισσότερο με τα πρότυπα Verifiable Credentials και τις αρχές του European Digital Identity Wallet [35].

Επιπλέον, η ενσωμάτωση αποκεντρωμένων αναγνωριστικών (Decentralized Identifiers – DIDs) θα μπορούσε να αποτελέσει σημαντικό βήμα προς την κατεύθυνση της διαλειτουργικότητας και της αποκέντρωσης. Μέσω των DIDs, κάθε Issuer και Verifier θα μπορούσε να διαθέτει ένα μοναδικό, επαληθεύσιμο αναγνωριστικό, μειώνοντας την εξάρτηση από κεντρικές αρχές και ενισχύοντας την εμπιστοσύνη στο οικοσύστημα. Αν και η υλοποίηση τέτοιων μηχανισμών ξεπερνά τους στόχους της παρούσας διπλωματικής εργασίας, η αρχιτεκτονική της εφαρμογής επιτρέπει τη μελλοντική ενσωμάτωσή τους χωρίς ριζικές αλλαγές.

Ένα ακόμη πεδίο επεκτασιμότητας αφορά τη διαχείριση δεδομένων και τη μόνιμη αποθήκευση διαπιστευτηρίων. Η παρούσα εφαρμογή βασίζεται αποκλειστικά σε session-based αποθήκευση, γεγονός που εξυπηρετεί τον σκοπό της προσομοίωσης αλλά περιορίζει τη λειτουργικότητα σε βάθος χρόνου. Σε ένα μελλοντικό σενάριο, θα μπορούσε να ενσωματωθεί βάση δεδομένων για

την ασφαλή αποθήκευση κρυπτογραφημένων διαπιστευτηρίων, καθώς και μηχανισμοί συγχρονισμού μεταξύ συσκευών. Μια τέτοια προσέγγιση θα προσέδιδε στο Wallet χαρακτηριστικά πραγματικής εφαρμογής, επιτρέποντας στον χρήστη να διαχειρίζεται τα διαπιστευτήριά του ανεξάρτητα από τη διάρκεια της συνεδρίας.

Σε επίπεδο διεπαφής χρήστη, η εφαρμογή θα μπορούσε να εμπλουτιστεί με επιπλέον λειτουργίες που συναντώνται σε σύγχρονα ψηφιακά πορτοφόλια. Ενδεικτικά, θα μπορούσε να προστεθεί μηχανισμός επιλεκτικής αποκάλυψης δεδομένων (selective disclosure), όπου ο χρήστης θα έχει τη δυνατότητα να επιλέγει ποια πεδία του διαπιστευτηρίου του θα παρουσιάζονται σε έναν Verifier. Η λειτουργία αυτή είναι ιδιαίτερα σημαντική για την προστασία της ιδιωτικότητας και ευθυγραμμίζεται με τις αρχές του GDPR και της ελαχιστοποίησης δεδομένων.

Παράλληλα, θα μπορούσε να υλοποιηθεί σύστημα ειδοποιήσεων σχετικά με τη λήξη διαπιστευτηρίων ή την ανάγκη επανέκδοσής τους. Με τον τρόπο αυτό, το Wallet θα μετατρεπόταν από παθητικό αποθετήριο εγγράφων σε ενεργό εργαλείο διαχείρισης ψηφιακής ταυτότητας, προσφέροντας αυξημένη χρηστικότητα στον τελικό χρήστη.

Όσον αφορά το υποσύστημα Mock Certificates, μελλοντικές επεκτάσεις θα μπορούσαν να περιλαμβάνουν τη σύνδεση της έκδοσης πιστοποιητικών με πραγματικά δεδομένα ή εξωτερικές υπηρεσίες. Για παράδειγμα, ένα πιστοποιητικό οικογενειακής κατάστασης θα μπορούσε να αντλεί πληροφορίες από μητρώα πολιτών, ενώ εκπαιδευτικά πιστοποιητικά θα μπορούσαν να συνδέονται με ιδρύματα εκπαίδευσης. Αν και τέτοιες επεκτάσεις απαιτούν αυξημένο επίπεδο ασφάλειας και διακυβέρνησης, η υφιστάμενη δομή της εφαρμογής παρέχει ένα σταθερό σημείο εκκίνησης.

Συνολικά, η παρούσα υλοποίηση επικεντρώνεται στον βασικό στόχο της διπλωματικής εργασίας, δηλαδή τη γεφύρωση της θεωρίας με την πράξη. Μέσα από την ανάπτυξη ενός λειτουργικού πρωτοτύπου, κατέστη δυνατή η πρακτική διερεύνηση των εννοιών που παρουσιάστηκαν στα προηγούμενα κεφάλαια, καθώς και η κατανόηση των προκλήσεων που συνοδεύουν τη σχεδίαση ψηφιακών πορτοφολιών και συστημάτων ταυτοποίησης.

Συνολικά, η εφαρμογή προσφέρει μια συνεκτική και κατανοητή απεικόνιση της λειτουργίας ενός ψηφιακού πορτοφολιού, χωρίς να θυσιάζει την επιστημονική ακρίβεια. Οι περιορισμοί που εντοπίστηκαν αποτελούν αναμενόμενες συνέπειες της ερευνητικής και εκπαιδευτικής φύσης του έργου και λειτουργούν ως αφετηρία για περαιτέρω μελέτη και εξέλιξη, υπογραμμίζοντας τη σημασία της συνεχούς έρευνας στον τομέα της ψηφιακής ταυτότητας και της ηλεκτρονικής διακυβέρνησης.

Η ανάλυση της υλοποίησης που παρουσιάστηκε στο παρόν κεφάλαιο ανέδειξε στην πράξη τον τρόπο με τον οποίο οι θεωρητικές έννοιες της ψηφιακής ταυτότητας και των ψηφιακών διαπιστευτηρίων μπορούν να μετασχηματιστούν σε ένα λειτουργικό πρωτότυπο σύστημα. Μέσα από τη μελέτη της αρχιτεκτονικής, των επιμέρους υποσυστημάτων και των σχεδιαστικών περιορισμών, κατέστη δυνατή η αποτίμηση τόσο των δυνατοτήτων όσο και των ορίων της συγκεκριμένης προσέγγισης. Στο επόμενο κεφάλαιο ακολουθεί η παρουσίαση των συμπερασμάτων και των μελλοντικών προοπτικών που προκύπτουν από την εκπόνηση της εργασίας.

7. Συμπεράσματα και Προοπτικές

Η παρούσα διπλωματική εργασία μελέτησε το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας (EUDI Wallet) ως βασικό δομικό στοιχείο του νέου ευρωπαϊκού πλαισίου ψηφιακής ταυτότητας, αναδεικνύοντας τον τρόπο με τον οποίο η αναθεώρηση του eIDAS οδηγεί από μια κυρίως διασυνδετική προσέγγιση εθνικών eID (eIDAS 1.0) σε ένα πιο ενοποιημένο, θεσμικά κατοχυρωμένο και «χρήστη-κεντρικό» οικοσύστημα (eIDAS 2.0). Η εξέλιξη αυτή δεν αφορά μόνο την τεχνολογία, αλλά πρωτίστως τον ορισμό σαφών ρόλων (Issuer–Holder/Wallet–Verifier), την παροχή νομικής ισχύος και την καθιέρωση απαιτήσεων για διαλειτουργικότητα, ασφάλεια και προστασία δεδομένων σε διασυνοριακό επίπεδο, ώστε η ψηφιακή ταυτοποίηση και η ανταλλαγή διαπιστευτηρίων να γίνουν πρακτικά αξιοποιήσιμες σε δημόσιες και ιδιωτικές υπηρεσίες εντός της ΕΕ [14], [3]. Παράλληλα, η φιλοσοφία privacy-by-design και η ελαχιστοποίηση δεδομένων τοποθετούνται στον πυρήνα της λύσης, σε ευθυγράμμιση με το

ευρωπαϊκό πλαίσιο προστασίας προσωπικών δεδομένων, γεγονός που ενισχύει τη θεσμική εμπιστοσύνη και μειώνει κινδύνους υπερσυλλογής/δευτερογενούς χρήσης δεδομένων [19], [17].

Κεντρικό συμπέρασμα από τη συγκριτική αξιολόγηση είναι ότι το EUDI Wallet διαφοροποιείται ουσιαστικά από τα εμπορικά πορτοφόλια (π.χ. Apple/Google/Samsung ή fintech πλατφόρμες), καθώς η πρόταση αξίας του δεν εστιάζει πρωτίστως στην ευκολία συναλλαγών εντός ενός ιδιωτικού οικοσυστήματος, αλλά στη δημιουργία μιας ενιαίας ευρωπαϊκής υποδομής εμπιστοσύνης με νομική αναγνώριση, σαφές μοντέλο διακυβέρνησης και προδιαγεγραμμένες απαιτήσεις συμμόρφωσης [14], [8], [9]. Αυτό μεταφράζεται σε μεγαλύτερη κανονιστική σαφήνεια για τους φορείς που βασίζονται σε διαπιστευτήρια, σε διευρυμένο πεδίο χρήσεων (ταυτοποίηση, υπογραφές, attestations ιδιοτήτων) και σε δυνατότητα διασυνοριακής αξιοποίησης που δεν εξαρτάται από ιδιωτικές πολιτικές πλατφορμών [29], [26]. Ταυτόχρονα, καταγράφηκε ότι οι προκλήσεις παραμένουν σημαντικές: η τεχνική και οργανωτική εναρμόνιση μεταξύ κρατών-μελών, η πρακτική υιοθέτηση από χρήστες με διαφορετικά επίπεδα ψηφιακού αλφαβητισμού, καθώς και η διαχείριση κινδύνων κυβερνοασφάλειας αποτελούν κρίσιμους παράγοντες επιτυχίας, οι οποίοι απαιτούν συντονισμό πολιτικής, προδιαγραφών και εφαρμογών στην πράξη [1], [14].

Σε επίπεδο αρχιτεκτονικής, η μελέτη κατέδειξε ότι το EUDI Wallet στηρίζεται σε κοινό πλαίσιο αναφοράς (ARF), το οποίο λειτουργεί ως «γλώσσα» διαλειτουργικότητας: ορίζει ρόλους, διεπαφές, ροές, μηχανισμούς εμπιστοσύνης και ελάχιστες απαιτήσεις ασφάλειας ώστε η έκδοση και η παρουσίαση διαπιστευτηρίων να είναι συνεπείς σε όλη την ΕΕ [29], [13]. Ιδιαίτερη σημασία έχουν οι κατηγορίες ροών (remote/proximity, same-device/cross-device) και η αντιστοίχισή τους με πρότυπα όπως OpenID4VP για παρουσιάσεις και ISO/IEC 18013-5 για εγγύς σενάρια (mdoc/mDL), που επιτρέπουν τη μεταφορά της «θεωρίας» σε συγκεκριμένες τεχνικές επιλογές επικοινωνίας και επαλήθευσης [30], [12]. Επιπλέον, η υιοθέτηση μηχανισμών ισχυρής αυθεντικοποίησης και phishing-resistant ροών (π.χ. passkeys/WebAuthn και σχετικά πρωτόκολλα συσκευών) αναδεικνύεται ως κρίσιμη συνιστώσα για τη μετάβαση σε πρακτικές, ασφαλείς εμπειρίες χρήσης, ειδικά σε cross-device αλληλεπιδράσεις [34], [33].

Η πρακτική συνεισφορά της εργασίας ενισχύθηκε μέσω της ανάπτυξης λειτουργικού πρωτοτύπου, το οποίο προσομοιώνει την αλυσίδα Issuer–Wallet–Verifier και καθιστά ορατές τις βασικές έννοιες έκδοσης, αποθήκευσης, παρουσίασης και επαλήθευσης διαπιστευτηρίων σε ένα ελεγχόμενο περιβάλλον. Η επιλογή τεχνολογιών (Python/Flask) και η αξιοποίηση JWT ως δομικού μηχανισμού διαπιστευτηρίου επέτρεψαν μια καθαρή, εκπαιδευτικά κατανοητή προσέγγιση, με έμφαση στον έλεγχο ισχύος και στην επαλήθευση υπογραφής σύμφωνα με το σχετικό πρότυπο [37], [40]. Παράλληλα, η ανάλυση των περιορισμών του πρωτοτύπου αναδεικνύει σαφείς προοπτικές εξέλιξης: μετάβαση σε ασύμμετρη κρυπτογραφία και πιο ρεαλιστικό μοντέλο εμπιστοσύνης μεταξύ εκδότη και επαληθευτή, υποστήριξη ροών που ευθυγραμμίζονται πιο άμεσα με OpenID4VCI/OpenID4VP για έκδοση και παρουσίαση, ενσωμάτωση επιλεκτικής αποκάλυψης και privacy-preserving τεχνικών (π.χ. σε SSI προσεγγίσεις) και επέκταση της υλοποίησης προς μηχανισμούς κατάστασης/ανάκλησης και ελέγχους συμμόρφωσης που προβλέπονται στο ευρύτερο οικοσύστημα [15], [5], [29]. Συνολικά, η εργασία καταλήγει ότι το EUDI Wallet αποτελεί μια θεσμικά ισχυρή και τεχνικά απαιτητική μετάβαση προς ένα κοινό ευρωπαϊκό «στρώμα εμπιστοσύνης», όπου η επιτυχία θα κριθεί τόσο από την ποιότητα υλοποίησης των προτύπων όσο και από την ικανότητα των κρατών-μελών και των φορέων να μετατρέψουν το πλαίσιο σε αξιόπιστες, καθημερινά χρήσιμες υπηρεσίες για πολίτες και επιχειρήσεις [14], [29].

Βιβλιογραφία

[1] ENISA (2023). *Digital Identity and Trust Services in the EU.* European Union Agency for Cybersecurity.

[2] Cameron, K. (2005). *The Laws of Identity.* Microsoft Research.

[3] European Parliament and Council (2014) Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

[4] Bonneau, J., Herley, C., Oorschot, P. & Stajano, F. (2012). *The Quest to Replace Passwords.* IEEE Symposium on Security and Privacy.

[5] Mühle, A., Grüner, A., Gayvoronskaya, T. & Meinel, C. (2018). *A Survey on Self-Sovereign Identity.* Computer Science Review, 30, 80–86.

[6] Kang, J. & Park, Y. (2020). *Mobile Wallet Adoption and Security Perceptions.* Journal of Information Systems, 34(1), 147–168.

[7] W3C (2023). *Verifiable Credentials Data Model v2.0.* Available at: https://www.w3.org/TR/vc-data-model-2.0/

[8] Apple Inc. (2024). *Wallet & Apple Pay – Privacy Overview.* Available at: https://www.apple.com/privacy

[9] Google LLC (2024). *Google Wallet Privacy Policy.* Available at: https://policies.google.com/privacy

[10] Samsung Electronics (2024). *Samsung Wallet Security.* Available at: https://www.samsung.com

[11] Revolut (2024). *Security Overview.* Available at: https://www.revolut.com

[12] ISO/IEC (2021) ISO/IEC 18013-5:2021 – Mobile driving licence (mDL) application. International Organization for Standardization. Available at: https://www.iso.org/standard/69084.html

[13] European Commission (2023). *EUDI Wallet Architecture and Reference Framework (ARF).* Available at: https://eu-digital-identity-wallet.github.io

[14] European Parliament and Council (2024) Regulation (EU) 2024/1183 *(eIDAS 2.0)* amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[15] OpenID Foundation (2023). *OpenID4VP & OpenID4VCI Technical Overview.*

[16] Digital Europe (2023). *Economic Impact Study on EUDI Wallet Adoption.*

[17] European Data Protection Board (EDPB) (2023). *Opinion on the European Digital Identity Wallet.*

[18] European Commission (2023). *Analysis of EUDI Wallet Use Cases.* Public eID Working Group.

[19] European Parliament and Council (2016) Regulation (EU) 2016/679 on the protection of natural persons regarding the processing of personal data (GDPR). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[20] Fabasoft AG. (2025) 'eIDAS 2.0: New rules for digital signatures'. Available at: https://www.fabasoft.com/en/news/eidas-new-rules-digital-signatures

[21] iGrant.io. (2024) 'Introduction to eIDAS 2.0 and Digital Wallets'. Available at: https://igrant.io/articles/introduction-to-eidas20-and-digital-wallet

[22] SSL2BUY. (2024) eIDAS 2.0: Your Comprehensive Guide to Protect Digital Identity. Available at: https://www.ssl2buy.com/cybersecurity/eidas-2-comprehensive-guide

[23] Ascertia. (2024) 'eIDAS 1.0 and eIDAS 2.0 differences'. Available at: https://blog.ascertia.com/eidas-1.0-eidas-2.0-differences

[24] European Commission (2025). *What is eSignature.* Digital Building Blocks. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109069/What%2Bis%2BeSignature

[25] European Commission (2025). *EU Digital Identity Wallets for service providers.* European Commission – EU Digital Identity Wallet. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/881984674/Wallet%2Bfor%2Bservice%2Bproviders

[26] European Commission (2025). *The many use cases of the EU Digital Identity Wallet.* European Commission – EU Digital Identity Wallet. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/716146139/The%2Bmany%2Buse%2Bcases%2Bof%2Bthe%2BEU%2BDigital%2BIdentity%2BWallet

[27] European Commission (2025). *Travel Credentials.* European Commission – EU Digital Identity Wallet. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/930451772/Travel%2BCredentials

[28] European Commission (2021) Commission Recommendation (EU) 2021/946 on a Toolbox for a coordinated approach towards a European Digital Identity Framework. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021H0946

[29] European Digital Identity Cooperation Group (2025) Architecture and Reference Framework (ARF), Version 2.4.0. Available at: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/

[30] OpenID Foundation (2025) OpenID for Verifiable Presentations 1.0. Final Specification, 9 July 2025. Available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[31] European Parliament and Council (2015) Directive (EU) 2015/2366 on payment services in the internal market (PSD2). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng

[32] European Commission (2018) Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 regarding regulatory technical standards for strong customer authentication and common and secure open standards of communication. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/eng

[33] FIDO Alliance (2025) Client to Authenticator Protocol (CTAP) 2.2. Proposed Standard, 14 July 2025. Available at: https://fidoalliance.org/specs/fido-v2.2-ps-20250714/fido-client-to-authenticator-protocol-v2.2-ps-20250714.html

[34] W3C (2025) Web Authentication: An API for accessing Public Key Credentials – Level 3. W3C Working Draft, 27 January 2025. Available at: https://www.w3.org/TR/webauthn-3/

[35] European Commission (2021). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0281

[36] Flask Documentation (2024). *Flask Web Development Framework – Official Documentation*. Available at: https://flask.palletsprojects.com

[37] Jones, M., Bradley, J. and Sakimura, N. (2015). *JSON Web Token (JWT)*. RFC 7519. Internet Engineering Task Force (IETF). Available at: https://datatracker.ietf.org/doc/html/rfc7519

[38] Bootstrap (2025). Get started with Bootstrap (v5.3) – Official Documentation. Available at: https://getbootstrap.com/docs/5.3/getting-started/introduction

[39] W3C (2025). Digital Credentials. W3C Working Draft. Available at: https://www.w3.org/TR/digital-credentials

[40] Jones, M., Bradley, J. and Sakimura, N. (2015). RFC 7515: JSON Web Signature (JWS). IETF. Available at: https://www.rfc-editor.org/info/rfc7515