



ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΑΝΑΠΤΥΞΗ ANDROID ΕΦΑΡΜΟΓΗΣ
PASSWORD MANAGER

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εισηγητής: Γεώργιος Μαχραμάς, ΔΕ20156

Επιβλέπων: Μιχαήλ Περονικολής

©
2026



HELLENIC MEDITERRANEAN UNIVERSITY

**SCHOOL OF MANAGEMENT AND ECONOMICS
SCIENCE**

**DEPARTMENT OF MANAGEMENT SCIENCE AND
TECHNOLOGY**

**ANDROID PASSWORD MANAGER
APPLICATION DEVELOPMENT**

DIPLOMA THESIS

Student : Georgios Machramas, de20156

Supervisor : Michail Peronikolis

©
2026

Υπεύθυνη Δήλωση: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Διοικητικής Επιστήμης και Τεχνολογίας του ΕΛ.ΜΕ.ΠΑ.

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή επικεντρώνεται στην ανάπτυξη μιας εφαρμογής Android, Password Manager (Διαχειριστή κωδικών πρόσβασης) χρησιμοποιώντας το Flutter framework της γλώσσας προγραμματισμού Dart και την υπηρεσία Flutterflow. Στόχος της εφαρμογής είναι η παροχή ενός ασφαλούς και εύχρηστου περιβάλλοντος για την αποθήκευση και την διαχείριση κωδικών πρόσβασης. Με την χρήση του Flutterflow, η ανάπτυξη εφαρμογών επιταχύνεται σημαντικά, επιτρέποντας την δημιουργία ενός λειτουργικού και οπτικά ελκυστικού περιβάλλοντος με ελάχιστο κώδικα. Η εφαρμογή ενσωματώνει ισχυρές πρακτικές ασφάλειας, όπως κρυπτογράφηση δεδομένων χρησιμοποιώντας το plugin sqllite sqlcipher για την προστασία των δεδομένων του χρήστη. Η προσέγγιση αυτή αναδεικνύει την αποτελεσματικότητα των low-code, no-code υπηρεσιών και παράλληλα με λίγο αλλαγή στον κώδικα εξασφαλίζουμε υψηλό επίπεδο ασφάλειας και λειτουργικότητας.

Λέξεις Κλειδιά : Προστασία, Ασφάλεια, Android, Εφαρμογή, Flutterflow

ABSTRACT

This thesis is focused on the development of an Android Password Manager application using the Flutter framework of Dart programming language and Flutterflow, a “hybrid”-low code or no code editor which is used to creating applications fast using UI and not coding without much knowledge. The application aims to serve a safe and easy to use environment for saving and managing user credentials. The application incorporates strong security practices such as passcode login and encrypted database using the plugin `sqflite_sqlicipher` for the safety of the user’s credentials. This approach shows the efficiency and the effectiveness of these services such as Flutterflow and other, also with a little bit of code we can achieve more security.

Key Words : Security, Safety, Android, Application, Flutterflow

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ.....	1
ABSTRACT.....	2
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ.....	3
ΛΙΣΤΑ ΕΙΚΟΝΩΝ.....	5
ΚΕΦΑΛΑΙΟ 1.....	1
ΕΙΣΑΓΩΓΗ.....	1
1.1 ΙΣΤΟΡΙΑ ΤΩΝ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ.....	2
1.2 PASSWORD MANAGER.....	3
1.3 ΤΥΠΟΙ PASSWORD MANAGER.....	4
1.4 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ PASSWORD MANAGER.....	5
1.5 ΚΡΥΠΤΟΓΡΑΦΙΑ.....	6
1.6 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΕΦΑΡΜΟΓΕΣ PASSWORD MANAGER.....	8
1.7 ΣΚΟΠΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ.....	8
ΚΕΦΑΛΑΙΟ 2	9
ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ANDROID	9
2.1 LINUX KERNEL.....	9
2.2 ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ANDROID.....	10
2.2.1 ΕΚΔΟΣΕΙΣ ANDROID.....	11
2.2.2 ΤΕΛΕΥΤΑΙΑ ΕΚΔΟΣΗ ANDROID (16)	12
2.3 ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΕΦΑΡΜΟΓΩΝ ANDROID.....	13
2.4 ΓΛΩΣΣΕΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ANDROID.....	14
2.4.1 ΓΛΩΣΣΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ DART.....	15
2.4.2 ΓΛΩΣΣΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ KOTLIN.....	15
2.5 SQLITE.....	16
ΚΕΦΑΛΑΙΟ 3.....	19
FLUTTERFLOW.....	19
3.1 FLUTTER.....	19
3.1.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ FLUTTER.....	19
3.2 FLUTTERFLOW.....	20
3.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ FLUTTERFLOW.....	21
3.4 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ FLUTTERFLOW.....	22
3.4.1 Project Dashboard.....	22
3.4.2 Custom Code.....	22
3.4.3 Action Flow Editor.....	24
3.4.4 SQLite Integration.....	25
3.4.5 Live Preview - Test Mode.....	27
3.5 ΑΡΝΗΤΙΚΑ FLUTTERFLOW.....	27
ΚΕΦΑΛΑΙΟ 4.....	28
Η ΕΦΑΡΜΟΓΗ - SHIELDKEY.....	28

4.1.1 Login Page.....	28
4.1.2 Homepage.....	30
4.1.3 Add Entry.....	32
4.1.4 View Entry / Edit Entry.....	34
4.2 Password Generator.....	36
4.3 Secure Notes.....	38
ΑΠΟΤΕΛΕΣΜΑΤΑ.....	40
Υλοποίηση εφαρμογής.....	40
Η σημασία της ασφάλειας των κωδικών πρόσβασης.....	40
Περιορισμοί και εμπορικές λύσεις.....	41
Ασφάλεια γενικότερα.....	41
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	41
Α. ΞΕΝΟΓΛΩΣΣΗ.....	42
Β.ΣΥΝΔΕΣΜΟΙ.....	43

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

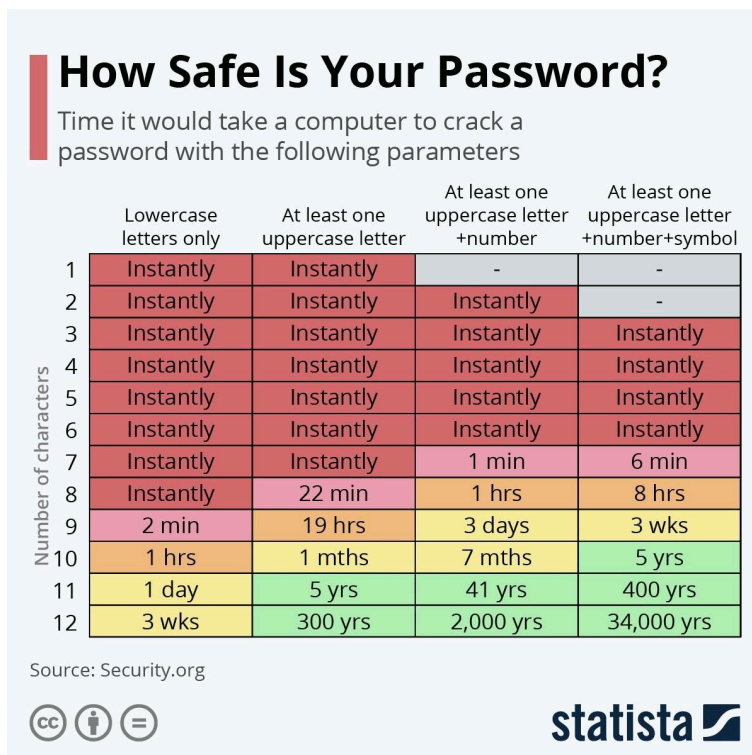
Εικόνα 1:How safe is your password
Εικόνα 2:Android logo
Εικόνα 3:Android 14 logo
Εικόνα 4:Android studio logo
Εικόνα 5:Dart logo
Εικόνα 6:SQLite logo
Εικόνα 7:Flutter logo
Εικόνα 8:Flutterflow logo
Εικόνα 9: Project Dashboard
Εικόνα 10:Custom Code
Εικόνα 11:Action Flow
Εικόνα 12:Sqlite integration
Εικόνα 13:Sqlite integration
Εικόνα 14:Live preview
Εικόνα 15:Login Page
Εικόνα 16:Homepage
Εικόνα 17:Homepage (menu)
Εικόνα 18:Add entry
Εικόνα 19:View entry
Εικόνα 20>Edit entry
Εικόνα 21>Password Generator
Εικόνα 22:Notes Homepage
Εικόνα 23:Add/Edit Note

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Το κίνητρο για την ανάπτυξη αυτής της εφαρμογής είναι η προώθηση αυτού του μέτρου ασφαλείας που έχει εξελιχθεί πάρα πολύ τα τελευταία χρόνια στην τεχνολογία. Ο καθημερινός χρήστης του διαδικτύου συνήθως δεν το παρατηρεί αλλά οι επιθέσεις σε βάσεις δεδομένων διάσημων ιστοσελίδων είναι πολύ συχνές, επίσης το password cracking είναι πάρα πολύ εξελιγμένο. Με μια γρήγορη αναζήτηση μπορούμε να ανακαλύψουμε χρησιμοποιώντας την διάσημη ιστοσελίδα “have i been pwned ?” πως έως τώρα έχουν εκτεθεί 13,614,756,460 (ημέρα συγγραφής) λογαριασμοί στο διαδίκτυο από 780 διαφορετικές ιστοσελίδες όπως το Facebook (509 εκατομμύρια λογαριασμοί σε μία μόνο παραβίαση, Απρίλιος 2019). Επίσης στην ιστοσελίδα μπορούμε να ελέγξουμε βάζοντας το email μας, αν έχει εκτεθεί κάποιος λογαριασμός μας στο διαδίκτυο.

ΕΙΚΟΝΑ 1 ([ΠΗΓΗ - STATISTA](#))



Στην εικόνα 1 από ερευνητικό άρθρο στο statista παρατηρούμε πόσο χρόνο χρειάζεται ένας υπολογιστής για να βρει τον κωδικό ενός λογαριασμού.

1.1 ΙΣΤΟΡΙΑ ΤΩΝ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Η ιδέα των κωδικών χρονολογείται πίσω στους αρχαίους χρόνους όταν οι ρωμαίοι στρατιωτικοί φρουροί χρησιμοποιούσαν λέξεις για την ταυτοποίηση τους. Η πρακτική αυτή εξελίχθηκε μέσα από την ιστορία. Αξιοσημείωτο παράδειγμα είναι η χρήση κωδικών στην ποτοαπαγόρευση στις Ηνωμένες Πολιτείες για την είσοδο σε παράνομα μπαρ. Το πρώτο σύστημα κωδικών πρόσβασης δημιουργήθηκε από τον Fernando Corbató στο MIT το 1961. Δημιούργησε έναν κοινόχρηστο ηλεκτρονικό υπολογιστή που απαιτούσε κωδικό πρόσβασης από κάθε ξεχωριστό χρήστη, σηματοδοτώντας την αρχή της χρήσης ψηφιακών κωδικών πρόσβασης. Το 1962 γίνεται η πρώτη παραβίαση δεδομένων όταν ο υποψήφιος διδάκτορας Alan Scheer κατάφερε να εκτυπώσει τους κωδικούς που ήταν αποθηκευμένοι στο Compatible Time-Sharing System (CTSS), για να αποκτήσει περισσότερο χρόνο στον υπολογιστή. Το διαδίκτυο και το ηλεκτρονικό εμπόριο αναπτύχθηκαν την δεκαετία του 1990, έτσι και η ανάγκη για την ασφαλή διαχείριση κωδικών πρόσβασης. Με την έλευση του διαδικτύου, ηλεκτρονικού εμπορίου και την χρήση προσωπικών υπολογιστών χρήστες δεν μπορούν πλέον να έχουν έναν κωδικό για ένα σύστημα αλλά διαφορετικούς για διάφορες υπηρεσίες. Το 50% των δεδομένων που είχαν παραβιαστεί από βάσεις δεδομένων αφορούσαν κωδικούς πρόσβασης. 1995 η AT&T εφηύρε το Two-Factor Authentication. ¹

¹ <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m11/security-timeline.html>

1.2 PASSWORD MANAGER

Τα Password Manager είναι εφαρμογές-υπηρεσίες σχεδιασμένες για την ασφαλή δημιουργία αποθήκευση και διαχείριση στοιχείων σύνδεσης(email/username,password) προσωπικών λογαριασμών στο διαδίκτυο χρησιμοποιώντας ένα ψευδώνυμο και κύριο κωδικό πρόσβασης.Βοηθούν τον χρήστη να δημιουργήσει σύνθετους κωδικούς για τον λογαριασμό χωρίς να τους θυμάται.Όταν ο χρήστης επισκεφτεί μια ιστοσελίδα το password manager ανιχνεύει τα πεδία συμπλήρωσης στοιχείων και προσφέρει την δυνατότητα αυτόματης συμπλήρωσης,όταν πρόκειται για νέο λογαριασμό προσφέρει την επιλογή αποθήκευσης στοιχείων για την επόμενη σύνδεση.Τα στοιχεία αποθηκεύονται σε μια κρυπτογραφημένη βάση δεδομένων.Τα Password Manager ξεκίνησαν ως απλές εφαρμογές υπολογιστή και πλέον υπάρχουν και cloud υπηρεσίες με πολλά προνόμια όπως ειδοποιήσεις για ασφάλεια.Το 1997 ο Bruce Schneier δημιούργησε την πρώτη εξειδικευμένη εφαρμογή password manager που αποθήκευε στα στοιχεία σε ασφαλή κρυπτογραφημένο αρχείο.Το 2003 δημιουργήθηκε το KeePass,μια εφαρμογή ανοικτού κώδικα με δυνατές μεθόδους κρυπτογράφησης η οποία χρησιμοποιείται μέχρι και σήμερα.Πλέον το password manager είναι ένα απαραίτητο εργαλείο για τον καθημερινό χρήστη.Οι εταιρείες έχουν εξελιχθεί πάρα πολύ και προσφέρουν υπηρεσίες όπως επαλήθευση δύο βημάτων(2fa),ασφαλή κοινή χρήση κωδικών,δημιουργία δύσκολων κωδικών πρόσβασης²

² https://en.wikipedia.org/wiki/Password_manager

1.3 ΤΥΠΟΙ PASSWORD MANAGER

Οι πιο γνωστοί password managers χωρίζονται σε 5 τύπους:

- **Browser-Based:** Είναι τα password manager που υπάρχουν μέσα στους περιηγητές και προσφέρουν την υπηρεσία τους μέσα από την χρήση του περιηγητή, βέβαια δεν έχουν παραπάνω λειτουργίες από την βασική και οι περισσότεροι έχουν αδύναμη κρυπτογράφηση ή καθόλου.
- **Local:** Είναι οι εφαρμογές password manager που μπορούμε να εγκαταστήσουμε στους υπολογιστές μας και αποθηκεύουν τα δεδομένα σε ένα τοπικό αρχείο. Μια διάσημη επιλογή είναι το KeePass όπου προσφέρει δυνατή κρυπτογραφία για ασφάλεια.
- **Cloud-Based:** Είναι οι υπηρεσίες που προσφέρουν ασφαλή αποθήκευση με κρυπτογράφηση στο cloud και στις μέρες μας η πιο διάσημη επιλογή των χρηστών, προσφέρουν αυτόματο συγχρονισμό ανάμεσα στις συσκευές και αυτόματο έλεγχο για διαρροή δεδομένων σε γνωστές βάσεις δεδομένων. Επίσης μια ιδιαίτερη προσέγγιση είναι αυτή του Self-Hosting όπου διαχειριστές συστημάτων τρέχουν δικό σε δικό τους μηχάνημα Server κάποιες λύσεις όπως Bitwarden, Vaultwarden, Passbolt.
- **Enterprise:** Είναι οι υπηρεσίες password manager σχεδιασμένες ειδικά για επιχειρήσεις, συνήθως οι cloud-based υπηρεσίες παρέχουν και λύσεις για μεγάλες επιχειρήσεις.
- **Hardware:** Είναι μια μικρή φυσική συσκευή με σύνδεση usb, usb type-c και nfc, προσφέρει μια μέθοδο αυθεντικοποίησης που πολλές ιστοσελίδες υποστηρίζουν, με την σύνδεση του η ιστοσελίδα επαληθεύει την σύνδεση του χρήστη. Αρκετές ιστοσελίδες υποστηρίζουν την μέθοδο της συσκευής ως επαλήθευσης 2 βημάτων ενώ κάποιες έχουν υλοποιήσει passwordless σύνδεση και χρησιμοποιούν την συσκευή ως κύρια μέθοδο επαλήθευσης.³

³ https://en.wikipedia.org/wiki/Password_manager

1.4 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ PASSWORD MANAGER

Η πιο συνήθης ευπάθεια προκαλείται από τον χρήστη,η προτεραιότητα της ευκολίας απομνημόνευσης έναντι της πολυπλοκότητας,με αποτέλεσμα την επιλογή εύκολων κωδικών πρόσβασης.Με την χρήση μια υπηρεσίας password manager η ασφάλεια εξαρτάται από τον κύριο κωδικό πρόσβασης με μερικές υπηρεσίες να μην επιβάλλουν την χρήση ισχυρών κύριων κωδικών,όμως αυτό φέρνει ένα σημαντικό μειονέκτημα,την εξάρτηση και εμπιστοσύνη στις πρακτικές ασφάλειας του παρόχου που επιλέγουν οι χρήστες..Η αρχιτεκτονική των υπηρεσιών password manager παρουσιάζει ένα μοναδικό σημείο αποτυχίας(single point of failure),αν παραβιαστεί η υπηρεσία όλα τα δεδομένα του χρήστη θα μπορούν να γίνουν προσβάσιμα,η υπηρεσία LastPass είχε υποστεί μία τέτοια επίθεση το 2022⁴.Μετά από έρευνα,μερικοί πάροχοι Password Manager βρέθηκαν με ελάττωματα όπως την μη επιβολή χρήσης περίπλοκου κύριου κωδικού,αποθήκευση των username σε plain text και παραμένοντας ευάλωτα σε keylogger και clipboard attacks⁵.Τέλος,ενώ οι υπηρεσίες password manager ενισχύουν την ασφάλεια με πολλούς τρόπους,μπορούν επίσης να παρουσιάσουν ευπάθειες εάν δεν χρησιμοποιούνται προσεκτικά.Οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί ενάντια σε επιθέσεις phishing που στοχεύουν στους λογαριασμούς των password manager και να διασφαλίζουν ότι χρησιμοποιούν ισχυρές διαδικασίες ανάκτησης⁶.

⁴ <https://blog.lastpass.com/posts/notice-of-recent-security-incident>

⁵ <https://doi.org/10.1109/pdcat.2017.00013>

⁶ <https://www.staysafeonline.org/articles/what-about-password-manager-risks>

1.5 ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι η πρακτική και η μελέτη των τεχνικών για την ασφαλή επικοινωνία, ιδίως σε περίπτωση αντιπάλων. Η ιστορία της ξεκινάει από την αρχαιότητα, όταν οι άνθρωποι προσπαθούσαν να εξασφαλίσουν την ασφάλεια επικοινωνιών τους. Οι πρώτες μέθοδοι μυστικής γραφής και απόκρυψης πληροφοριών χρησιμοποιήθηκαν κατά την διάρκεια των παγκόσμιων πολέμων με τεχνικές όπως η στεγανογραφία⁷. Η κρυπτογραφία περιλαμβάνει τη μετατροπή των πληροφοριών σε μορφή που δεν είναι αναγνώσιμη από μη εξουσιοδοτημένους χρήστες, εξασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικοποίηση και τη μη αποκήρυξη των δεδομένων, προστατεύει τις πληροφορίες και τις επικοινωνίες με τη μετατροπή του απλού κειμένου σε κρυπτογραφημένο κείμενο με τη χρήση αλγορίθμων, γεγονός που καθιστά δύσκολη την αποκρυπτογράφηση των πληροφοριών από μη εξουσιοδοτημένα μέρη. Η σύγχρονη κρυπτογραφία εμφανίστηκε με την εφεύρεση των υπολογιστών και το έργο του Claude Shannon, ο οποίος θεωρείται ο πατέρας του κλάδου για τον για τον προσδιορισμό της ασφάλειας και της αυθεντικότητας ως κύριους στόχους του. Η ψηφιακή εποχή έφερε την ανάπτυξη τυποποιημένων κρυπτογραφικών αλγορίθμων συμμετρικής κρυπτογράφησης όπως το Data Encryption Standard (DES) και το Advanced Encryption Standard (AES). Η ασύμμετρη κρυπτογράφηση επαναστάτησε με την ανάπτυξη του public-key cryptography και RSA Algorithm, όπου επίλυσε το μακροχρόνιο πρόβλημα διανομής κλειδιών και τώρα χρησιμοποιείται για την ψηφιακή υπογραφή⁸. Η κρυπτογραφία είναι απαραίτητη σε διάφορους τομείς, όπως:

⁷ <https://doi.org/10.13140/RG.2.2.12086.72000>

⁸ <https://doi.org/10.13140/RG.2.2.12086.72000>

- Ψηφιακές υπογραφές: Χρησιμοποιούνται για την επαλήθευση της γνησιότητας ψηφιακών εγγράφων και συναλλαγών.
- Κρυπτονομίσματα: εξασφαλίζει ασφαλείς συναλλαγές και προστατεύει τα πορτοφόλια των χρηστών από απάτες.
- Ασφαλής επικοινωνία Ιστότοπου: Πρωτόκολλα όπως το SSL/TLS χρησιμοποιούν κρυπτογραφικές μεθόδους για την ασφάλεια των δεδομένων που ανταλλάσσονται μεταξύ διακομιστών ιστού και πελατών όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

Συνοψίζοντας, η κρυπτογραφία διαδραματίζει κρίσιμο ρόλο στη σύγχρονη κυβερνοασφάλεια, επιτρέποντας την ασφαλή επικοινωνία και προστατεύοντας ευαίσθητα δεδομένα από μη εξουσιοδοτημένη πρόσβαση. Οι αρχές και οι τεχνικές της εξελίσσονται συνεχώς για την αντιμετώπιση των αναδυόμενων απειλών σε έναν ολοένα και πιο ψηφιακό κόσμο.⁹¹⁰

⁹ <https://en.wikipedia.org/wiki/Cryptography>

¹⁰ <https://www.ibm.com/think/topics/cryptography>

1.6 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΕΦΑΡΜΟΓΕΣ PASSWORD MANAGER

Οι εφαρμογές password manager χρησιμοποιούν κρυπτογραφικές τεχνικές για την ασφαλή αποθήκευση και διαχείριση των κωδικών πρόσβασης των χρηστών. Η ασφάλεια αυτών των εφαρμογών εξαρτάται από ισχυρούς αλγορίθμους κρυπτογράφησης, λειτουργίες εξαγωγής κλειδιών και αρχιτεκτονικά σχέδια που δίνουν προτεραιότητα στην προστασία των χρηστών. Οι περισσότερες υπηρεσίες χρησιμοποιούν AES-256 (Advanced Encryption Standard) για την κρυπτογράφηση των αποθηκευμένων κωδικών πρόσβασης¹¹. Αυτό το πρότυπο κρυπτογράφησης θεωρείται ευρέως ασφαλές και χρησιμοποιείται από κυβερνήσεις για την προστασία ευαίσθητων δεδομένων λόγω του τεράστιου χώρου κλειδιών που διαθέτει, καθιστώντας το ανθεκτικό σε επιθέσεις. Επίσης, χρησιμοποιούν αρχιτεκτονική zero-knowledge, αυτό σημαίνει ότι δεν έχουν πρόσβαση στα δεδομένα και τον master password του χρήστη, αυτό ασφαλίζει τα δεδομένα από εσωτερικές παραβιάσεις.¹²

1.7 ΣΚΟΠΟΣ ΤΗΣ ΕΡΓΑΣΙΑΣ

Ο σκοπός της εργασίας είναι η δημιουργία μιας εφαρμογής Password Manager με χρήση της πλατφόρμας low-code Flutterflow για την ανάπτυξη του μεγαλύτερου μέρους της. Η προώθηση τέτοιων πλατφορμών είναι πολύ σημαντική γιατί το φιλικό περιβάλλον προς τον χρήστη που προσφέρουν μπορεί να γίνει κίνητρο για νέους χρήστες με λίγες γνώσεις προγραμματισμού να βρουν μια έναρξη στην ανάπτυξη εφαρμογών για κινητά τηλέφωνα και όχι μόνο.

¹¹ <https://keepass.info/help/base/security.html>

¹² <https://bitwarden.com/resources/zero-knowledge-encryption/>

ΚΕΦΑΛΑΙΟ 2

ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ANDROID

2.1 LINUX KERNEL

Το Linux Kernel, δημιουργήθηκε από τον Linus Torvalds το 1991, είναι βασικό κομμάτι των λειτουργικών συστημάτων Linux, χρησιμοποιείται στην διασύνδεση μεταξύ των λειτουργιών – εφαρμογών με τα εξαρτήματα του υπολογιστή. Ξεκίνησε ως ένα ατομικό πρότζεκτ όταν ο Linus ήταν φοιτητής πληροφορικής στο Πανεπιστήμιο του Ελσίνκι, και τώρα είναι το ανοιχτού κώδικα kernel που χρησιμοποιούν εκατομμύρια συσκευές παγκοσμίως. Η αρχιτεκτονική του είναι οργανωμένη μέσα σε υποσυστήματα, επιτρέποντας αποτελεσματική διαχείριση πόρων και επεκτασιμότητα. Με τα χρόνια, το Linux Kernel έχει αναπτυχθεί σημαντικά, με την συνεισφορά χιλιάδων προγραμματιστών, κάνοντας το θεμέλιο σε σύγχρονους υπολογιστές και διάσημη επιλογή για Servers και υπολογιστές γραφείου. Η νοοτροπία του ανοιχτού κώδικα δημιούργησε ένα συνεργατικό περιβάλλον που οδήγησε στην ευρεία υιοθέτηση και την συνεχή βελτίωση του. Το τροποποιημένο Kernel που χρησιμοποιεί το Android προσθέτει την υποστήριξη που χρειάζεται για το Android όπως αρχιτεκτονικές, διαχείριση ενέργειας και χαρακτηριστικά ασφάλειας.¹³

¹³ http://en.wikipedia.org/wiki/Linux_kernel

2.2 ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ANDROID

Το Android είναι ένα λειτουργικό σύστημα που βασίζεται σε μια τροποποιημένη έκδοση του linux kernel και σε άλλο λογισμικό ανοιχτού κώδικα. Το Android αναπτύχθηκε από την Open Handset Alliance, με την Google να είναι ο κύριος συντελεστής στην πιο δημοφιλή έκδοση του. Η πρώτη εμπορική συσκευή Android, το HTC Dream παρουσιάστηκε τον Σεπτέμβριο του 2008. Το Android είναι το πιο δημοφιλές λειτουργικό σύστημα σε smartphone και tablet. Τον Μάιο του 2021 είχε πάνω από 3 δισεκατομμύρια χρήστες και το Google Play Store πάνω από 3 εκατομμύρια εφαρμογές. Ο πυρήνας του είναι το Android Open Source Project (AOSP) και είναι free open-source. Ωστόσο οι περισσότερες συσκευές android τρέχουν κλειστού κώδικα λογισμικό android και εφαρμογές όπως οι βασικές εφαρμογές της Google, Google Mobile Services (GMS), Google Play Services. Μερικοί κατασκευαστές που βασίζονται στο Android λειτουργούν το οικοσύστημα της Google και προσαρμόζουν την διεπαφή του χρήστη και προσθέτουν λειτουργίες και εφαρμογές. Τον Οκτώβριο του 2003 η Android Inc. ιδρύθηκε στη California από τον Andy Rubin και Chris White, με τους Rich Miner και Nick Sears να συμμετάσχουν αργότερα. Στην αρχή ξεκίνησαν να αναπτύξουν ένα λειτουργικό σύστημα για ψηφιακές κάμερες το οποίο απέτυχε να φέρει επενδυτές, έτσι τον Απρίλιο του 2004 ξεκίνησαν την ανάπτυξη ενός λειτουργικού συστήματος για κινητά με στόχο να ανταγωνιστούν τα Symbian και Microsoft Windows Mobile. Το 2005 η Google απέκτησε το Android για τουλάχιστον 50 εκατομμύρια. Τον Νοέμβριο του 2007, Ιδρύθηκε η Open Handset Alliance, μία ένωση από εταιρείες στον κλάδο της τεχνολογίας με σκοπό την ανάπτυξη μιας ανοιχτής και ολοκληρωμένης πλατφόρμας για κινητές συσκευές. Τον Σεπτέμβριο του 2008 το Android ανακοινώθηκε σε συνέντευξη τύπου σε ένα σταθμό μετρό της Νέας Υόρκης.

ΕΙΚΟΝΑ 2 ([ΠΗΓΗ – WIKIPEDIA](#))



2.2.1 ΕΚΔΟΣΕΙΣ ANDROID

- 1.0 (2008)
- 1.1 (2009)
- Cupcake 1.5 (2009)
- Donut 1.6 (2009)
- Eclair 2.0-2.1 (2009-2010)
- Froyo 2.2-2.3 (2010)
- Gingerbread 2.3 (2010-2011)
- Honeycomb 3.0-3.2 (2011)
- Ice Cream Sandwich 4.0 (2011)
- Jelly Bean 4.1-4.3 (2012-2013)
- KitKat 4.4 (2013-2014)
- Lollipop 5.0-5.1 (2014-2015)
- Marshmallow 6.0 (2015)
- Nougat 7.0-7.1 (2016)
- Oreo 8.0-8.1 (2017)
- Pie 9.0 (2018)
- 10 (2019)
- 11 (2020)
- 12 (2021)
- 12L (2022)
- 13 (2023)
- 14 (2023)
- 15 (2024)
- 16 (2025)

2.2.2 ΤΕΛΕΥΤΑΙΑ ΕΚΔΟΣΗ ANDROID (16)

Το Android 16 είναι η 16η κύρια έκδοση Android,εκδόθηκε στις 10 Ιουνίου 2025.Αναπτύχθηκε από την Open Handset Alliance καθοδηγούμενη από την Google.Η εσωτερική κωδική ονομασία του είναι “Baklava”,προέρχεται από τον παραδοσιακό τρόπο κωδικής ονομασίας με θέμα τα επιδόρπια σε αλφαβητική σειρά.Οι νέες λειτουργίες και νέα χαρακτηριστικά που έφερε το Android 16 είναι:

- Αναμόρφωση της διεπαφή χρήστη παρουσιάζοντας το νέο Material 3 expressive,όπου φέρνει νέα σχέδια και χρώματα.
- Το νέο Desktop mode,προσφέρει στο κινητό την εμπειρία χρήσης ενός υπολογιστή.
- Απευθείας επιλογή φωτογραφιών απο το Cloud μέσω του Android photo picker.
- Linux terminal το οποίο επιτρέπει στον χρήστη την εγκατάσταση και linux εφαρμογών.
- Βελτίωση λειτουργικότητας του Health Connect με νέα API για πρόσβαση και διαχείριση ιατρικών δεδομένων από εφαρμογές
- Μετάδοση ήχου με πολλαπλές συσκευές bluetooth.
- Notification cooldown επιλογή για την μείωση απόσπασης προσοχής.
- Νέος τύπος ειδοποιήσεων,Live Updates,σχεδιασμένο για την βοήθεια παρακολούθησης και γρήγορης πρόσβασης σε σημαντικές δραστηριότητες.
- Privacy Sandbox,διασφάλιση ιδιωτικότητας χρησιμοποιώντας ανώνυμα δεδομένα για την παραγωγή εξατομικευμένου περιεχομένου.
- Adaptive apps,λειτουργία αυτόματης προσαρμογής εφαρμογών σε διάφορα μεγέθη συσκευών.
- Υποστήριξη APV Codec,Advanced professional Video (APV) για επαγγελματική καταγραφή και post-production.
- Vertical Text Rendering,υποστήριξη γλωσσών που χρησιμοποιούν κάθετη γραφή.

ΕΙΚΟΝΑ 3 ([ΠΗΓΗ – WIKIPEDIA](#))



2.3 ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΕΦΑΡΜΟΓΩΝ ANDROID

Ο προγραμματισμός εφαρμογών Android μπορεί να γίνει στις γλώσσες προγραμματισμού Kotlin, Java και C++ χρησιμοποιώντας το Android Software Development kit (SDK)¹⁴. Το Android Software Development Kit, είναι ένα σετ εργαλείων ανάπτυξης εφαρμογών, προσφέρει βιβλιοθήκες και εργαλεία για την διευκόλυνση της σύνταξης κώδικα όπως σύστημα εντοπισμού σφαλμάτων (debugger) και εικονικό προσομοιωτή Android συσκευής βασισμένο στο QEMU. Μέχρι το 2014, το επίσημο ολοκληρωμένο περιβάλλον ανάπτυξης ήταν το Eclipse με την χρήση του Android Development Tools (ADT). Το 2015 η Google σταμάτησε επίσημα την υποστήριξη του για να εστιάσει στην ανάπτυξη του Android Studio ως το επίσημο ολοκληρωμένο περιβάλλον ανάπτυξης. Μερικές γλώσσες προγραμματισμού επιτρέπουν την ανάπτυξη cross-platform εφαρμογών¹⁵. Το Play Store είναι το επίσημο κατάστημα εφαρμογών το οποίο είναι προεγκατεστημένο στα περισσότερα κινητά Android.

¹⁴ https://en.wikipedia.org/wiki/Android_software_development

¹⁵ https://en.wikipedia.org/wiki/Android_SDK

ΕΙΚΟΝΑ 4 ([ΠΗΓΗ – WIKIPEDIA](#))



2.4 ΓΛΩΣΣΕΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ANDROID

Η ανάπτυξη εφαρμογών Android βασίζεται σε μια πολυγλωσσική προσέγγιση, ενσωματώνοντας διάφορες γλώσσες προσαρμοσμένες σε διαφορετικά αρχιτεκτονικά παραδείγματα. Ιστορικά, η γλώσσα προγραμματισμού Java ήταν η επίσημη γλώσσα για την ανάπτυξη εφαρμογών, τα τελευταία χρόνια αντικαταστάθηκε από την Kotlin ως η κύρια γλώσσα. Για εργασίες με υψηλές υπολογιστικές απαιτήσεις, οι προγραμματιστές μπορούν να επιλέξουν την χρήση της γλώσσας C ή C++ μέσω του Android Native Development Kit (NDK), αλλά σε μερικές περιπτώσεις αυτό είναι δυσκολότερο και περίπλοκο¹⁶. Για μια διαφορετική αγορά, υπάρχουν τα cross-platform frameworks που προσφέρουν βιώσιμες επιλογές χρησιμοποιώντας κοινό κώδικα. Η Dart είναι μια σύγχρονη γλώσσα προγραμματισμού και χρησιμοποιείται από το Flutter, που αναπτύχθηκε από την Google. Το Flutter παρέχει υψηλή απόδοση σε εφαρμογές για Android, iOS, Web και PC.

¹⁶<https://www.geeksforgeeks.org/android/top-programming-languages-for-android-app-development/>

2.4.1 ΓΛΩΣΣΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ DART

Η γλώσσα προγραμματισμού Dart, αναπτύχθηκε από την Google για την δημιουργία γρήγορων εφαρμογών με υποστήριξη πολλαπλών πλατφορμών. Χρησιμοποιεί C-στυλ συντακτικό, αντικειμενοστραφή προγραμματισμό, καθιστώντας την προσβάσιμη σε προγραμματιστές που γνωρίζουν Java ή Javascript. Προσφέρει υποστήριξη ασύγχρονου προγραμματισμού, null safety και πολλές βιβλιοθήκες. Η Dart έχει ιδιαίτερη διάκριση διότι είναι η γλώσσα που χρησιμοποιεί το Flutter UI Framework. Με λειτουργίες όπως το hot reload και την δυνατότητα να συντάσσει native code ή JavaScript, η Dart προσφέρει ένα πολυχρηστικό περιβάλλον για μοντέρνα ανάπτυξη εφαρμογών¹⁷

ΕΙΚΟΝΑ 5 ([WIKI – WIKIPEDIA](https://en.wikipedia.org/wiki/Dart_(programming_language)))



2.4.2 ΓΛΩΣΣΑ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ KOTLIN

Η Kotlin είναι μια μοντέρνα και ασφαλέστερη γλώσσα προγραμματισμού, αναπτύχθηκε από την JetBrains και ανακοινώθηκε ως η επίσημη γλώσσα προγραμματισμού για την ανάπτυξη εφαρμογών android από την Google τον Μάιο του 2019. Είναι μια στατικά τυποποιημένη γλώσσα που είναι πλήρως διαλειτουργική με την Java και εκτελείται στο Java Virtual Machine (JVM), καθιστώντας εύκολη την ενσωμάτωση της σε υπάρχοντες εφαρμογές Java. Η γλώσσα θεωρείται εύκολη στην εκμάθηση της ειδικότερα από όσους έχουν εμπειρία σε Java και C# και συχνά προωθείται από προγραμματιστές. Είναι ενσωματωμένη σε περιβάλλοντα ανάπτυξης όπως το Android Studio και το IntelliJ IDEA, τα οποία παρέχουν εργαλεία για την

¹⁷ <https://dart.dev/overview>.

διαμόρφωση,εντοπισμό σφαλμάτων και την ολοκλήρωση κώδικα.Έρευνα έδειξε πως εφαρμογές που ήταν ανεπτυγμένες μερικώς ή πλήρως με Kotlin παρουσίασαν βελτιωμένη ποιότητα κώδικα¹⁸.Το 2020,ήταν η πιο ευρέως χρησιμοποιημένη γλώσσα με την Google να υπολογίζει πως χρησιμοποιείται σε περίπου το 70% των 1000 κορυφαίων εφαρμογών Android,γεγονός που δείχνει την σημαντική διείσδυση της στην επαγγελματική αγορά¹⁹.

2.5 SQLITE

Το SQLite είναι ένα ελεύθερο και ανοικτού κώδικα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων που αναπτύχθηκε στη γλώσσα προγραμματισμού C. Λειτουργεί ως βιβλιοθήκη που μπορεί να ενσωματωθεί σε άλλες εφαρμογές, καθιστώντας το ιδιαίτερα κατάλληλο για τοπική αποθήκευση δεδομένων ή αποθήκευση στην πλευρά του client σε εφαρμογές λογισμικού.Η SQLite δημιουργήθηκε από τον Dr. Richard Hipp τον Μάιο του 2000. Εμπνεύστηκε να το αναπτύξει ενώ εργαζόταν σε λογισμικό για ένα πολεμικό πλοίο του Πολεμικού Ναυτικού των ΗΠΑ, όπου αντιμετώπισε προβλήματα με την αξιοπιστία ενός υπάρχοντος συστήματος βάσεων δεδομένων.Το SQLite σχεδιάστηκε για να λειτουργεί χωρίς να χρειάζεται ξεχωριστό διακομιστή, καθιστώντας το αξιόπιστο, ειδικά σε σημαντικές καταστάσεις. Δοκιμάστηκε για πρώτη φορά τον Ιούνιο του 2000 και κυκλοφόρησε επίσημα ως έκδοση 1.0.Το SQLite είναι μια self-contained,serverless,zero-configuration relational database engine που προσφέρει ένα ευρύ φάσμα χαρακτηριστικών,καθιστώντας την κατάλληλη για διάφορες εφαρμογές.Ο σκοπός της SQLite στην ανάπτυξη εφαρμογών είναι να προσφέρει μία ελαφριά, αξιόπιστη και εύχρηστη λύση βάσης δεδομένων, η οποία μπορεί να ενσωματωθεί απευθείας στις εφαρμογές, αποφεύγοντας την ανάγκη για ξεχωριστή διαδικασία διακομιστή.

¹⁸ <https://arxiv.org/pdf/1808.00025>

¹⁹ <https://en.wikipedia.org/wiki/Kotlin>

Βασικά χαρακτηριστικά:

1. Serverless Αρχιτεκτονική: Η SQLite λειτουργεί απευθείας εντός της εφαρμογής χωρίς την χρήση ενός ξεχωριστού διακομιστή.
2. Μηδενική Ρύθμιση: Η SQLite δεν απαιτεί ρυθμίσεις ή διαμόρφωση, διευκολύνοντας την ενσωμάτωση σε εφαρμογές
3. Υποστήριξη πολλαπλών πλατφορμών: Οι βάσεις δεδομένων SQLite αποθηκεύονται σε ένα ενιαίο αρχείο, επιτρέποντας την εύκολη μεταφορά τους μεταξύ διαφορετικών λειτουργικών συστημάτων.²⁰

Υποστήριξη SQL:

1. Πλήρης υποστήριξη SQL: Η SQLite υποστηρίζει τα περισσότερα χαρακτηριστικά της SQL, περιλαμβάνοντας πίνακες, δείκτες, εναύσματα, προβολές και σύνθετα ερωτήματα, όπως υποερωτήματα και συνδέσεις.
2. Συμμόρφωση ACID: οι συναλλαγές τηρούν τις αρχές ατομικότητας, συνέπειας, απομόνωσης και ανθεκτικότητας, εξασφαλίζοντας την ακεραιότητα των δεδομένων²¹.
3. Υποστήριξη JSON: Η SQLite περιλαμβάνει ενσωματωμένη υποστήριξη για τύπους δεδομένων JSON, επιτρέποντας την αποτελεσματική αναζήτηση και επεξεργασία των δεδομένων JSON²²

²⁰ <https://www.sqlite.org/different.html>

²¹ <https://codedamn.com/news/sqlite/introduction-to-sqlite>

²² <https://en.wikipedia.org/wiki/SQLite>



ΚΕΦΑΛΑΙΟ 3

FLUTTERFLOW

3.1 FLUTTER

Το Flutter είναι ένα δωρεάν UI framework ανοιχτού κώδικα φτιαγμένο από την Google το 2017 και είναι δημοφιλής για την απόδοση, όμορφη διεπαφή με το χρήστη και την παραγωγικότητα που προσφέρει στους προγραμματιστές. Η κύρια χρήση του είναι στην ανάπτυξη εφαρμογών που υποστηρίζονται ταυτόχρονα σε πολλαπλά λειτουργικά συστήματα όπως Android, iOS, Linux, Windows, macOS χρησιμοποιώντας τον ίδιο κώδικα βασισμένο πάνω στην γλώσσα προγραμματισμού Dart. Το Flutter χρησιμοποιείται από την Google για την ανάπτυξη των εφαρμογών της.²³

3.1.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ FLUTTER

1. Hot Reload: Επιτρέπει στους προγραμματιστές να βλέπουν τις αλλαγές σε πραγματικό χρόνο.
2. Widget-Based Αρχιτεκτονική: ο Πυρήνας του Flutter Ui είναι σχεδιασμένος γύρω από widgets, όπου μπορούν να προσαρμοστούν και να συνδυαστούν για την δημιουργία πολύπλοκων διεπαφών. Τα Widget μπορούν να αλλάξουν ανάλογα με την αλληλεπίδραση του χρήστη.
3. Single Codebase: Οι προγραμματιστές γράφουν την εφαρμογή σε έναν κώδικα και έχουν την δυνατότητα να την εγκαταστήσουν σε πολλαπλές πλατφόρμες
4. Rich Widget Library: Το flutter προσφέρει προσχεδιασμένα widgets που χρησιμοποιούν τον σχεδιασμό του Material Design για Android και Cupertino για iOS.²⁴

²³ <https://flutter.dev/>

²⁴ [https://en.wikipedia.org/wiki/Flutter_\(software\)](https://en.wikipedia.org/wiki/Flutter_(software))

ΕΙΚΟΝΑ 7 ([ΠΗΓΗ – FLUTTER](#))



3.2 FLUTTERFLOW

Το FlutterFlow είναι μια platforma low-code ανάπτυξης εφαρμογών σχεδιασμένη για την δημιουργία εφαρμογών cross-platform για κινητά χρησιμοποιώντας το Flutter Framework της Google. Επιτρέπει στους χρήστες να χτίσουν υψηλής ποιότητας εφαρμογές για android και IOS ταυτόχρονα χωρίς γνώση προγραμματισμού προσφέροντας μια εύχρηστη οπτική διεπαφή. Το FlutterFlow δημιουργήθηκε από 2 πρώην εργαζόμενους της Google με σκοπό την διευκόλυνση σχεδίασης και ανάπτυξης εφαρμογών, προορίζεται και σε προγραμματιστές και σε μη προγραμματιστές.

ΕΙΚΟΝΑ 8 ([ΠΗΓΗ – BRANDFETCH](#))



3.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ FLUTTERFLOW

Το FlutterFlow περιέχει αρκετά χαρακτηριστικά που το μετατρέπουν στο τέλειο εργαλείο για την ανάπτυξη εφαρμογών, τα οποία είναι :

1. Οπτική διεπαφή σχεδιασμού (Visual design interface): με το VDI μπορεί ο χρήστης να σχεδιάσει εύκολα την εφαρμογή του με την λειτουργία drag-and-drop και τα έτοιμα UI elements χωρίς την χρήση κώδικα.
2. Συνεργασία σε πραγματικό χρόνο (Real-Time Collaboration): Οι ομάδες μπορούν να συνεργάζονται ταυτόχρονα στο ίδιο έργο, αυτό βοηθάει στην επιτάχυνση της ανάπτυξης.
3. Απόκριση διάταξης (Responsive Layouts): Εξασφαλίζει την απόκριση των εφαρμογών αυτόματα προσαρμόζοντας ανάλογα την οθόνη του κινητού, έτσι προσφέρει σταθερή εμπειρία σε όλες τις συσκευές
4. Ενσωμάτωση προσαρμοσμένου κώδικα (Custom Code Integration): Επιτρέπει στον χρήστη να προσθέσει δικό του κώδικα για προηγμένες λειτουργίες και αρκετά ευέλικτο για να εξυπηρετήσει προχωρημένους προγραμματιστές.
5. Προ-κατασκευασμένα Widgets και Templates: Πολλαπλά έτοιμα Widgets και Templates για τον απλοποίηση της διαδικασίας και γρήγορο prototyping.
6. Προεπισκόπηση (Live Preview): Απευθείας προεπισκόπηση αλλαγών UI, παρόμοια με την λειτουργία hot reload του Flutter.
7. Ενσωματώσεις βάσεων δεδομένων (Database Integrations): Παροχή βάσεων δεδομένων ανάμεσα σε Google Firebase, Supabase και SQLite.
8. Γενικές ενσωματώσεις (Integrations): Πολλές ενσωματώσεις όπως Google maps , codemagic, stripe, RevenueCat, algolia, openAI, GitHub.²⁵

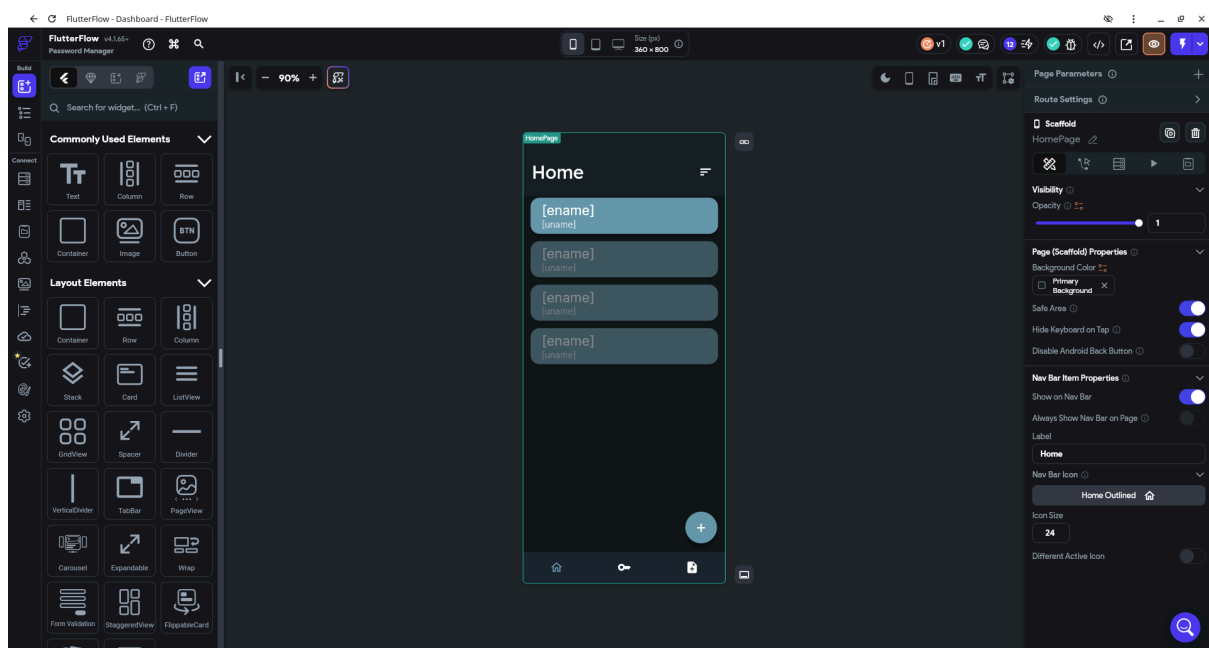
²⁵ <https://www.flutterflow.io/product>

3.4 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ FLUTTERFLOW

3.4.1 Project Dashboard

Το Dashboard αποτελεί την αρχική σελίδα ενός προτζεκτ. Στην μέση της οθόνης βλέπουμε την επισκόπηση της εφαρμογής εμφανισιακά (UI), δεξιά είναι το menu επιλογών για το επιλεγμένο στοιχείο ή οθόνης, αριστερά είναι το menu με τα έτοιμα προκατασκευασμένα στοιχεία όπου μπορούμε να τοποθετήσουμε στην επιλεγμένη οθόνη με απλό drag-and-drop και να τα προσαρμόσουμε.

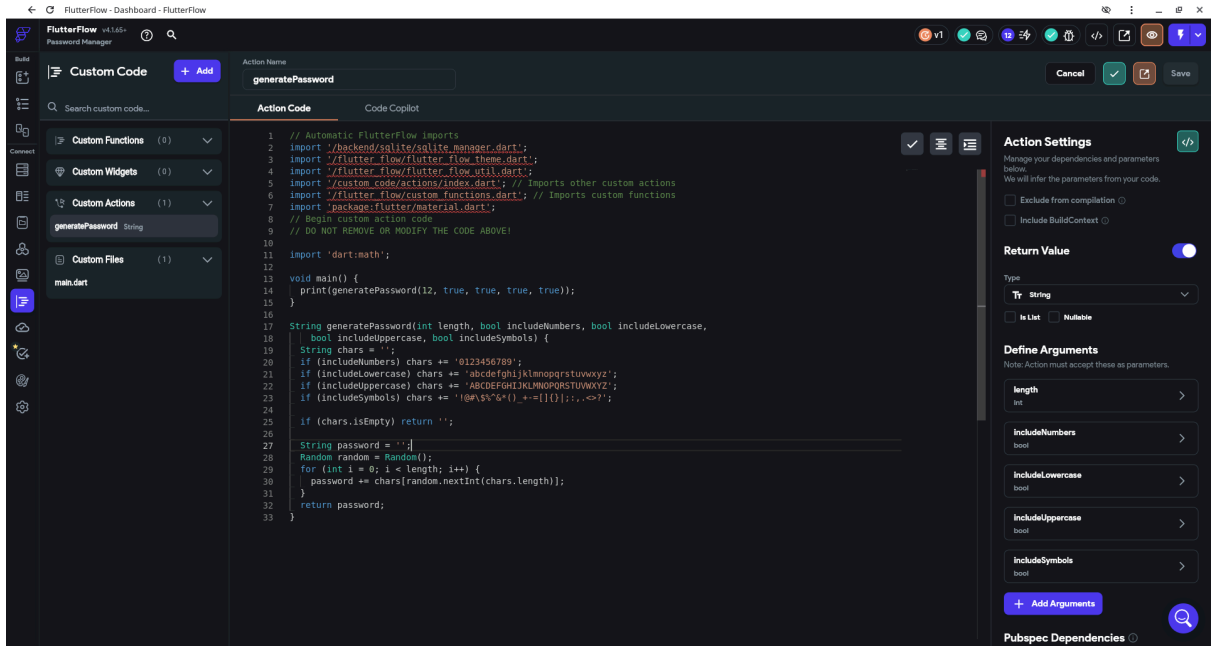
EIKONA 9 (Project Dashboard)



3.4.2 Custom Code

Στην σελίδα Custom Code μπορούμε να δημιουργήσουμε προσαρμοσμένα Functions, Widgets, Actions. Στην φωτογραφία βλέπουμε την τοποθέτηση του κώδικα για το Password Generator Screen της εφαρμογής, παρατηρούμε στο δεξί μενού την προσαρμογή-δήλωση των Variables κάτι που προσφέρει μεγάλη ευχρηστία στο κάλεσμα του κώδικα από το Action Flow Editor.

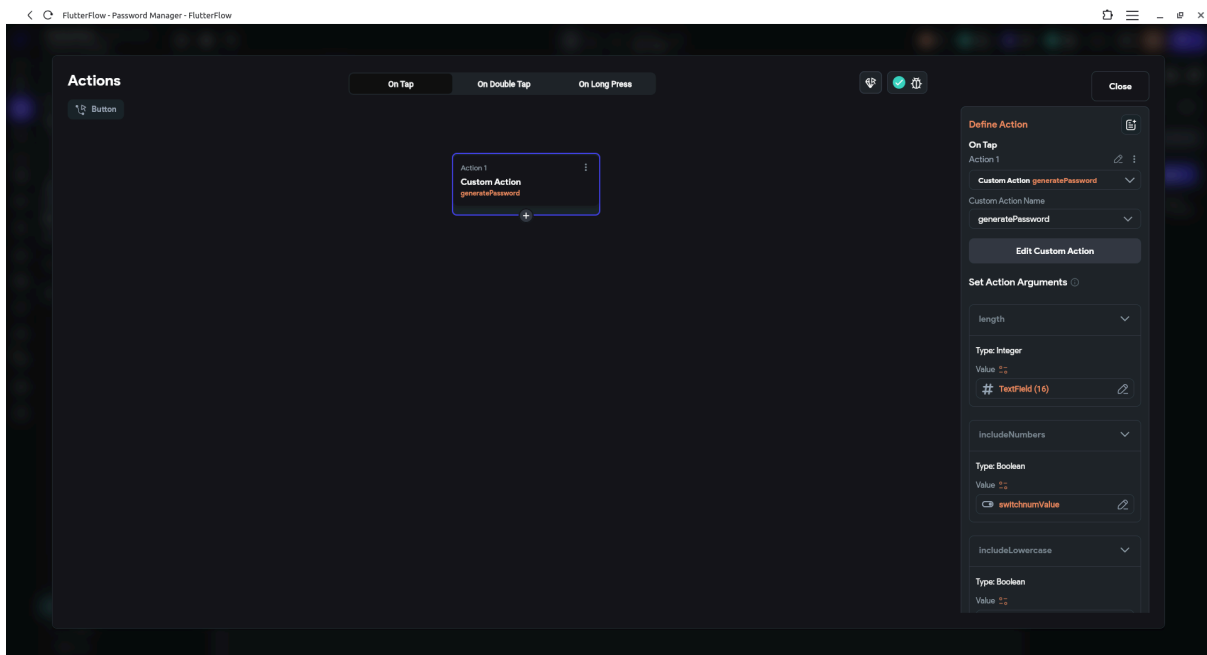
EIKONA 10 (Custom Code)



3.4.3 Action Flow Editor

Με το action flow editor δημιουργούμε μια σειρά ενεργειών,πολλαπλών άμα χρειαστεί και διαφορετικών ανάλογα την περίσταση.Στην φωτογραφία βλέπουμε την ενέργεια που καλεί το κουμπί “Generate” στην σελίδα Password Generator.

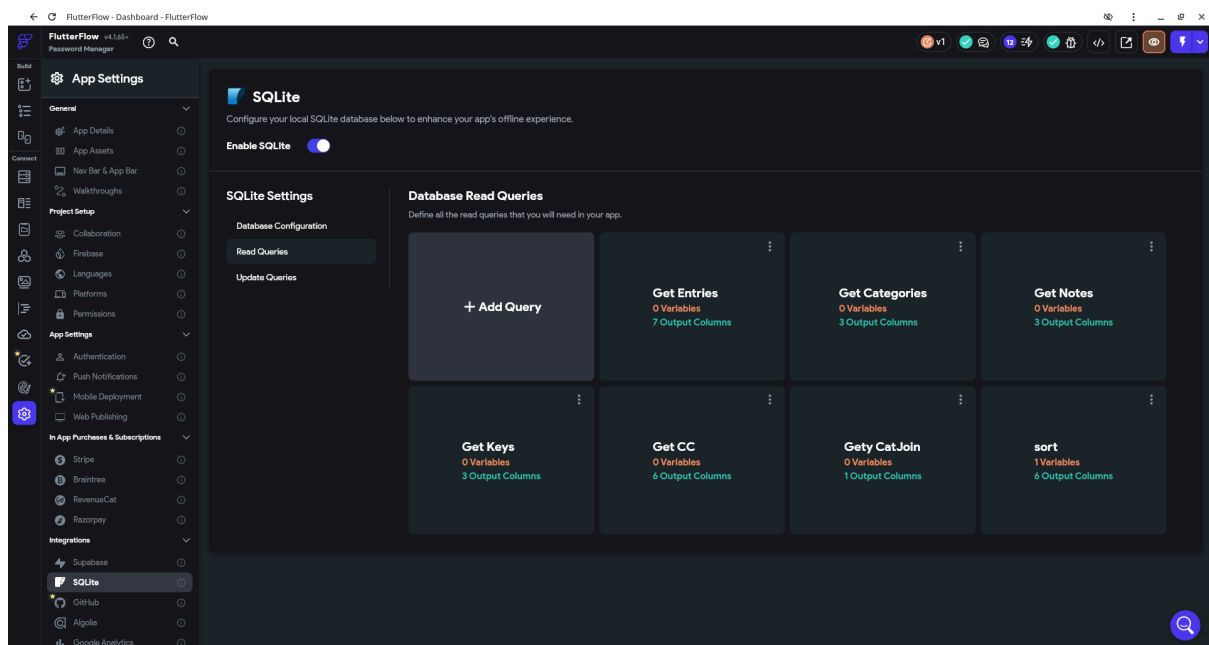
EIKONA 11 (Action Flow)



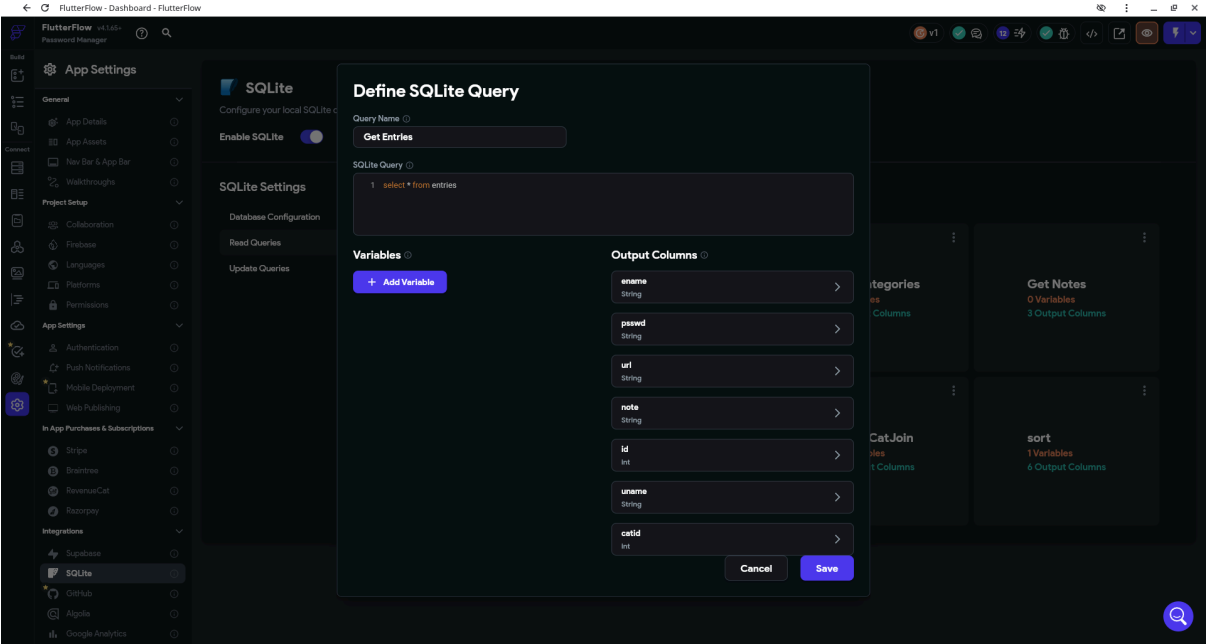
3.4.4 SQLite Integration

Απο τις ρυθμίσεις μπορούμε να ενεργοποιήσουμε όλα τα διαθέσιμα integrations. Στην εφαρμογή χρησιμοποίησα το SQLite integration για την εισαγωγή του database και την δημιουργία των Read και Update Queries

EIKONA 12 (Sqlite Integration)



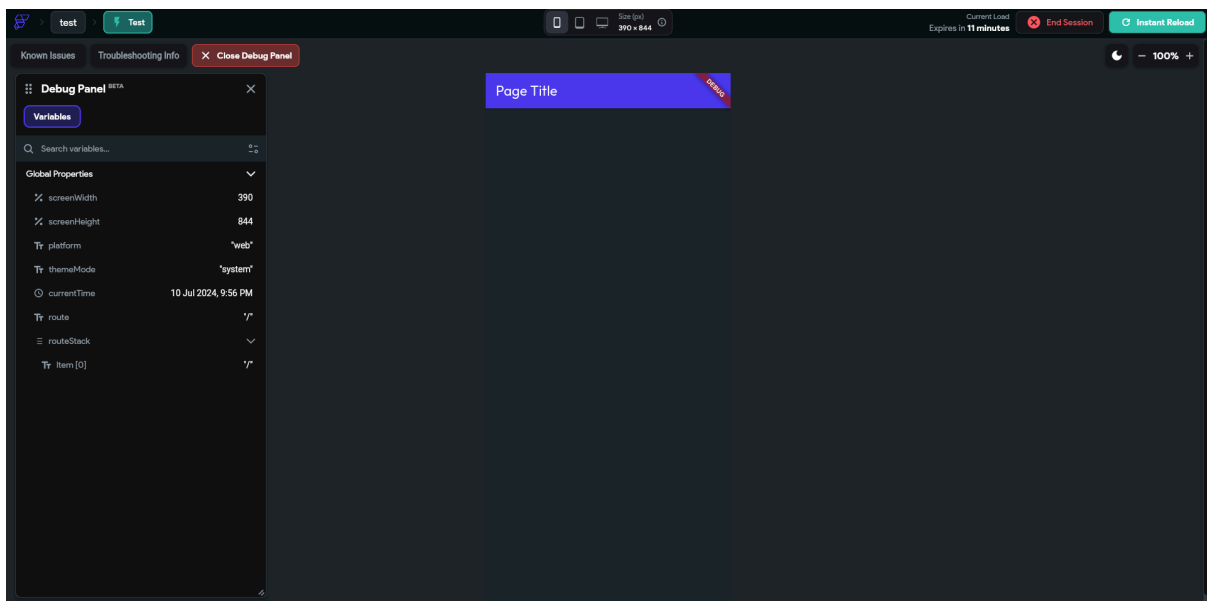
EIKONA 13 (Sqlite Integration)



3.4.5 Live Preview - Test Mode

Με το Test Mode μπορούμε να χρησιμοποιήσουμε την εφαρμογή μέσα από την ιστοσελίδα χωρίς να χρειαστεί να κατεβάσουμε κάτι στον υπολογιστή, μπορούμε να κάνουμε αλλαγές στην εφαρμογή και ταυτόχρονα να περάσουν στο test mode. Η λειτουργία έχει διάρκεια 15 λεπτά και μπορεί να ξαναχρησιμοποιηθεί απευθείας μετά την λήξη.

ΕΙΚΟΝΑ 14 (Live Preview)



3.5 ΑΡΗΤΙΚΑ FLUTTERFLOW

Το FlutterFlow αποτελεί μια εξαιρετική πλατφόρμα για την ανάπτυξη εφαρμογών, ωστόσο, όπως συμβαίνει με κάθε εργαλείο, υπάρχουν κάποιες προκλήσεις. Ένα συγκεκριμένο ζήτημα που αντιμετώπισα είναι ότι το Test Mode δεν λειτουργεί με βάσεις δεδομένων SQLite, γεγονός που περιορίζει τη δυνατότητά μου να το χρησιμοποιήσω. Επιβεβαίωσα ότι το πρόβλημα αυτό δεν οφείλεται σε δική μου αμέλεια.

ΚΕΦΑΛΑΙΟ 4

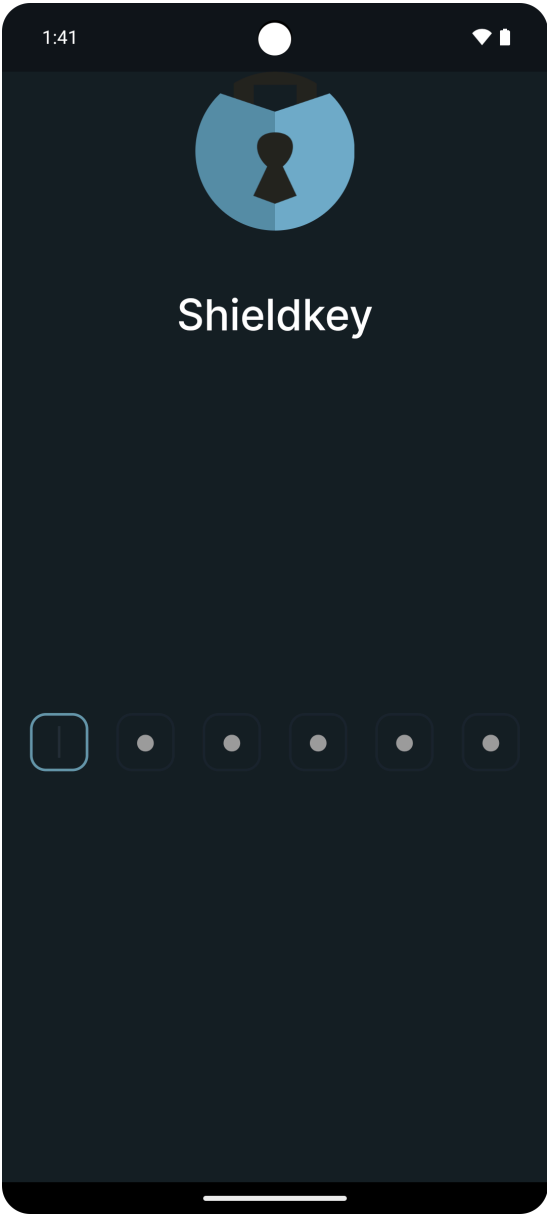
Η ΕΦΑΡΜΟΓΗ - SHIELDKEY

Η εφαρμογή ShieldKey έχει αναπτυχθεί με σκοπό την ασφαλή αποθήκευση κωδικών πρόσβασης και σημειώσεων. Περιλαμβάνει τρεις βασικές λειτουργίες: την αποθήκευση κωδικών πρόσβασης, την αποθήκευση σημειώσεων και την παραγωγή κωδικών πρόσβασης (password generator). Στοχεύει σε όλους τους χρήστες του διαδικτύου και παροτρύνει τη χρήση εφαρμογών password manager για την ενίσχυση της ασφάλειας στο διαδίκτυο. Η εφαρμογή αξιοποιεί κρυπτογραφημένη βάση δεδομένων μέσω του sqflite_sqlcipher το οποίο προστέθηκε εξωτερικά χρησιμοποιώντας το Android Studio.

4.1.1 Login Page

Κατά την πρώτη σύνδεση στην εφαρμογή, ο χρήστης παρακαλείται να εισαγάγει έναν 6ψήφιο κωδικό ελέγχου ταυτότητας προκειμένου να διασφαλιστεί η ασφάλεια των δεδομένων του και να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση.

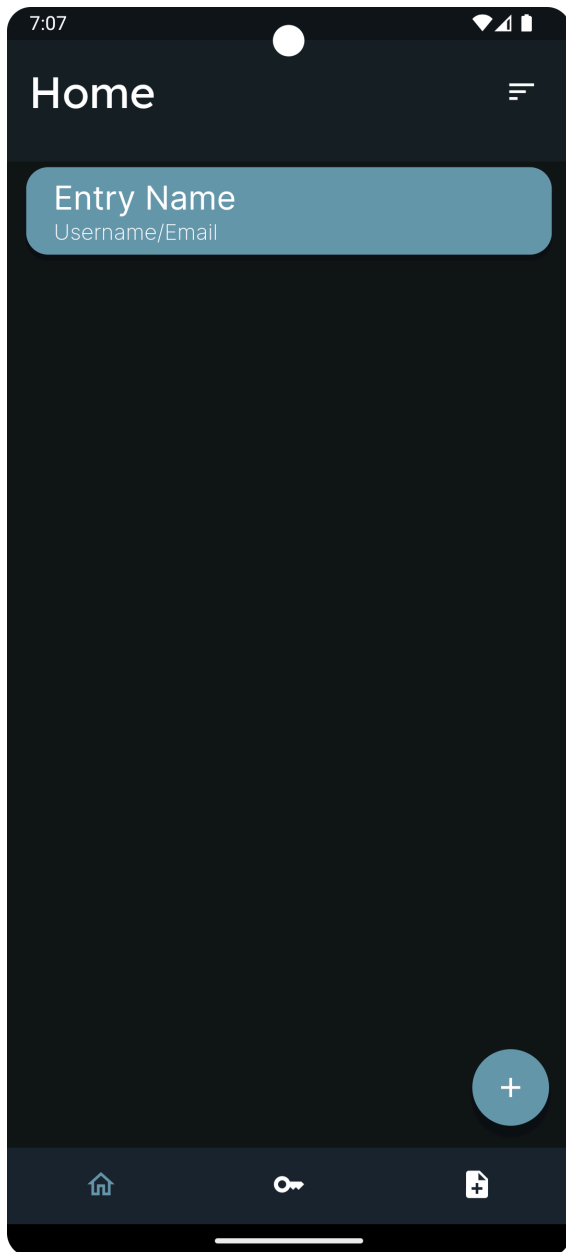
EIKONA 15 (Login Page)



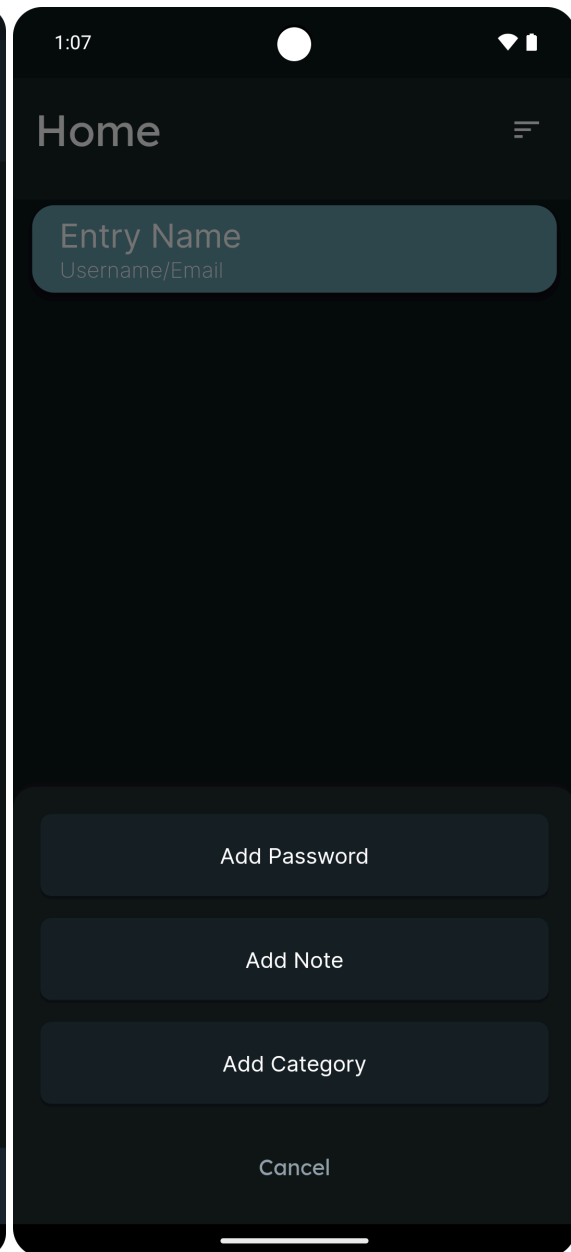
4.1.2 Homepage

Μετά την επιτυχή ολοκλήρωση της διαδικασίας πιστοποίησης, ο χρήστης θα ανακατευθυνθεί αυτόματα στην κύρια σελίδα, όπου θα έχει πρόσβαση σε μια λίστα με τους καταχωρημένους κωδικούς πρόσβασης. Αυτή η λίστα εμφανίζεται σε μορφή κάρτας, όπου παρουσιάζεται το όνομα και το email ή το όνομα χρήστη για κάθε καταχώριση. Η σελίδα διαθέτει επίσης λειτουργία φιλτραρίσματος ανά κατηγορία, που μπορεί να χρησιμοποιηθεί από τον χρήστη εφόσον το επιθυμεί. Επιπλέον, στην κάτω δεξιά γωνία της σελίδας υπάρχει ένα floating Action Button, το οποίο παρέχει πρόσβαση σε επιλογές για την προσθήκη νέου κωδικού, κατηγορίας ή σημείωσης.

EIKONA 16 (Homepage)



EIKONA 17 (Homepage Menu)



4.1.3 Add Entry

Η σελίδα "Add Entry" σας επιτρέπει να δημιουργήσετε μια νέα καταχώρηση συμπληρώνοντας την αντίστοιχη φόρμα. Η φόρμα απαιτεί την εισαγωγή του ονόματος της καταχώρισης, του email ή του ονόματος χρήστη, του κωδικού πρόσβασης, του συνδέσμου ιστότοπου και μιας σημείωσης. Είναι απαραίτητο να συμπληρώσετε τουλάχιστον το πεδίο του ονόματος προκειμένου να αποθηκεύσετε την καταχώρισή σας.

EIKONA 18 (Add Entry)

1:08

←

Add Entry

Entry name

Username/Email

Password

URL

Notes

Please select... ▾

Add

4.1.4 View Entry / Edit Entry

Η σελίδα "View Entry" λειτουργεί ως συνοπτική παρουσίαση για κάθε επιμέρους καταχώριση. Ο χρήστης έχει τη δυνατότητα να αποκαλύψει τον κωδικό πρόσβασης, επιλέγοντας την σχετική επιλογή μέσω ενός κουμπιού που επιτρέπει την αποκάλυψή του. Επιπλέον, παρέχονται κουμπιά για την αντιγραφή των στοιχείων email/όνομα χρήστη, κωδικού πρόσβασης και διεύθυνσης URL, με στόχο τη βελτίωση της χρηστικότητας. Στην κορυφή της οθόνης, υπάρχει ένα κουμπί που διευκολύνει τον χρήστη να πλοηγηθεί στην οθόνη επεξεργασίας ή διαγραφής της καταχώρησής του, όπου μπορούν να γίνουν οι κατάλληλες τροποποιήσεις σε όλα τα στοιχεία.

Σημείωση: Το στοιχείο σημείωσης δεν είναι συνδεδεμένο με την λειτουργία σημειώσεων, αποθηκεύεται και αναφέρεται στην καταχώρηση του κωδικού

EIKONA 19 (View Entry)

1:08

←

Entry Name 

Username/Email 

Username/Email

Password  

.....

URL 

Url

Notes

Note

EIKONA 20 (Edit entry)

1:09

← 

Entry Name

Name

Entry Name

Username/Email 

Username/Email

Password  

.....

URL 

Url

Notes

Note

Category 1 

Update

4.2 Password Generator

Η δεύτερη λειτουργία της εφαρμογής είναι το Password Generator, το οποίο επιτρέπει τη δημιουργία νέων, μοναδικών κωδικών με βάση τους περιορισμούς που επιλέγει ο χρήστης: μέγεθος κωδικού (16 χαρακτήρες ως προεπιλογή), χρήση μεγάλων και μικρών γραμμάτων, καθώς και συμβόλων. Για την υλοποίηση της λειτουργίας του Password Generator, χρειάστηκε η εισαγωγή Custom Code, το οποίο, με τη χρήση του custom code του FlutterFlow, λειτούργησε ομαλά και αποδοτικά.

EIKONA 21 (Password Generator)

7:05

Password Generator

Password

Length

Set Length
16

Uppercase Letters (A,B,C,D...)

Lowercase Letters (a,b,c,d...)

Numbers (1,2,3,4...)

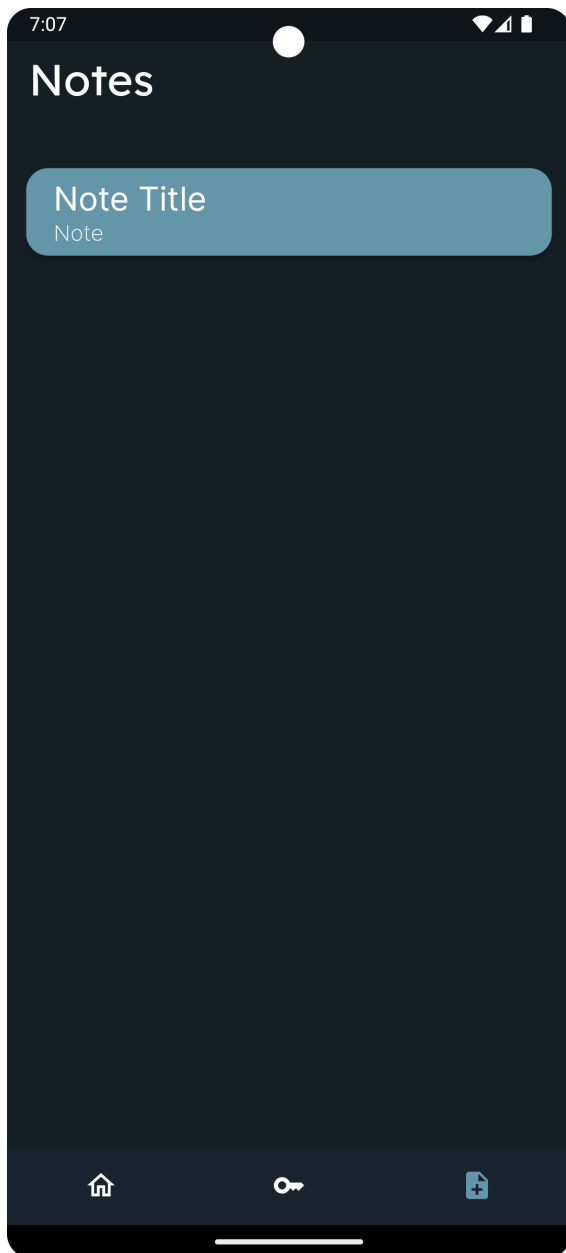
Symbols (!,@,#,\$...)

Generate

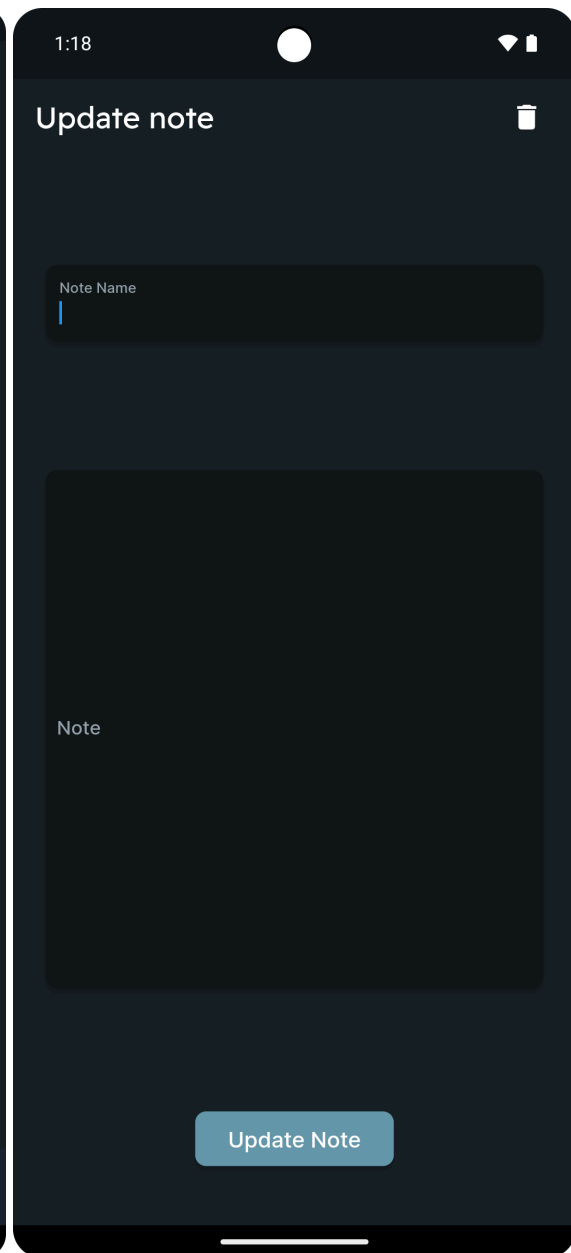
4.3 Secure Notes

Η τρίτη λειτουργία της εφαρμογής συνιστά ένα σημειωματάριο που προορίζεται για την ασφαλή αποθήκευση απλών σημειώσεων. Αποτελείται από τρεις οθόνες: την αρχική σελίδα, η οποία περιλαμβάνει τη λίστα των σημειώσεων, τη σελίδα προσθήκης και τη σελίδα τροποποίησης. Δεν υπάρχει ξεχωριστή σελίδα για την ανάγνωση των σημειώσεων, καθώς όλες οι σημειώσεις είναι ορατές στην αρχική σελίδα. Όταν ο χρήστης επιλέξει μια σημείωση, καθοδηγείται στη σελίδα τροποποίησης ή διαγραφής της αντίστοιχης σημείωσης.

EIKONA 22 (Notes Homepage)



EIKONA 23 (Add/Edit Note)



ΑΠΟΤΕΛΕΣΜΑΤΑ

Υλοποίηση εφαρμογής

Με την υλοποίηση της εργασίας,κατάφερα να αναπτύξω μια εφαρμογή Password manager με τη χρήση της υπηρεσίας Flutterflow και του flutter framework.Η επιλογή μου επέτρεψε να δημιουργήσω γρήγορα μια πλήρως λειτουργική εφαρμογή χωρίς να απαιτείται η χρήση κώδικα.Στη συνέχεια με χρήση κώδικα μετέτρεψα την βάση δεδομένων σε κρυπτογραφημένη διότι δεν το υποστηρίζει η υπηρεσία.Παρόλα αυτά,είναι σημαντικό να σημειωθεί ότι η εφαρμογή δεν προσφέρει την ίδια βαρύτητα ασφαλείας και προηγμένα χαρακτηριστικά με τις εμπορικές λύσεις.

Η σημασία της ασφάλειας των κωδικών πρόσβασης

Ένα δίδαγμα που προκύπτει από την εργασία είναι η αναγκαιότητα συνεχούς εκπαίδευσης και κατανόησης των κινδύνων ασφάλειας στο διαδίκτυο.Ο καθημερινός χρήστης πρέπει να υιοθετήσει σύγχρονες μεθόδους ασφαλείας για τους λογαριασμούς του.Αυτό σημαίνει την δημιουργία σύνθετων κωδικών που να αποτελούνται από τουλάχιστον 12 χαρακτήρες,χρησιμοποιώντας ένα μείγμα κεφαλαίων,πεζών,αριθμών και συμβόλων.Η χρήση μονών πεζών ή μόνο αριθμών είναι ιδιαίτερα επικίνδυνη,καθώς μπορούν εύκολα να παραβιαστούν.Η χρήση ταυτοποίησης δύο παραγόντων(2FA) είναι πολύ σημαντική και προσθέτει ακόμα ένα επίπεδο ασφάλειας.Η αποφυγή επαναχρησιμοποίησης κωδικών πρόσβασης σε διαφορετικούς λογαριασμούς είναι επίσης σημαντική,καθώς μια παραβίαση σε έναν λογαριασμό μπορεί να θέσει σε κίνδυνο όλους τους υπόλοιπους.

Περιορισμοί και εμπορικές λύσεις

Η εφαρμογή, λόγω της απλοϊκής αρχιτεκτονικής της, προορίζεται αποκλειστικά για ερευνητικούς σκοπούς και δεν συνιστάται η καθημερινή της εφαρμογή. Δεν παρέχει την ίδια προστασία με τις εμπορικές λύσεις που υποστηρίζονται από μεγάλες εταιρείες ασφαλείας και διαθέτουν συνεχή ανάπτυξη και βελτίωση. Η διατήρηση ενημερωμένου λογισμικού συστήματος και η χρήση αξιόπιστων εφαρμογών είναι απαραίτητες για την προστασία από κακόβουλο λογισμικό.

Ασφάλεια γενικότερα

Στον τομέα της τεχνολογίας, οι ευπάθειες στον κώδικα, τα λειτουργικά συστήματα και τις εφαρμογές ανακαλύπτονται καθημερινά. Είναι σημαντικό να παραμένετε ενημερωμένοι για τις τελευταίες απειλές σε οποιαδήποτε κατηγορία και να ακολουθείτε τις βέλτιστες πρακτικές για την προστασία των προσωπικών σας δεδομένων και των λογαριασμών σας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

A. ΞΕΝΟΓΛΩΣΣΗ

Luevanos, C., Elizarraras, J., Hirschi, K. and Yeh, J. (2017). Analysis on the Security and Use of Password Managers. *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*.

Tunio, N. (2024). Historical evolution of cryptography.

Góis, B., Matias Martinez, M., Gois Mateus, B. and Martinez, M. (2019). *An Empirical Study on Quality of Android Applications written in Kotlin language*.

B.ΣΥΝΔΕΣΜΟΙ

Bitwarden. (n.d.). *Open Source Password Manager for Individuals and Teams*. [online] <https://bitwarden.com/>

Reichl, D. (n.d.). *KeePass Password Safe*. [online] keepass.info. Available at: <https://keepass.info>

Flutterflow.io. (2024). *FlutterFlow - Build high quality, customized apps quickly!* [online] <https://www.flutterflow.io/>

Dart (2024). *Dart programming language*. [online] dart.dev. [https://dart.dev/](https://dart.dev)

Flutter (n.d.). *Flutter - Beautiful native apps in record time*. [online] [Flutter.dev](https://flutter.dev). <https://flutter.dev/>

newsroom.cisco.com. (n.d.). Passwords have a long history – how much do you know...? <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2022/m11/security-timeline.html>

Wikipedia Contributors (2019). Password. [online] Wikipedia. <https://en.wikipedia.org/wiki/Password>

Wikipedia. (2020). *Password manager*. [online] https://en.wikipedia.org/wiki/Password_manager

IBM (2023). Cryptography. [online] [IBM.com](https://www.ibm.com/think/topics/cryptography) <https://www.ibm.com/think/topics/cryptography>

Wikipedia Contributors (2019). Cryptography. [online] Wikipedia. <https://en.wikipedia.org/wiki/Cryptography>

Wikipedia Contributors (2019c). Linux kernel. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Linux_kernel

Wikipedia Contributors (2019a). Android (operating system). [online] Wikipedia. [https://en.wikipedia.org/wiki/Android_\(operating_system\)](https://en.wikipedia.org/wiki/Android_(operating_system))

Wikipedia Contributors (2019b). Android software development. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Android_software_development

Wikipedia. (2020). Android version history. [online] Available at: https://en.wikipedia.org/wiki/Android_version_history

Wikipedia. (2026). Android 16. [online] https://en.wikipedia.org/wiki/Android_16

Dart (n.d.). Dart overview. [online] dart.dev. <https://dart.dev/overview>.

harkiran78 (2019). Top Programming Languages for Android App Development -
GeeksforGeeks. [online] GeeksforGeeks. <https://www.geeksforgeeks.org/top-programming-languages-for-android-app-development/>

Mohan, M. (2024). What is SQLite? Everything about SQLite with examples. [online] codedamn news. <https://codedamn.com/news/sqlite/introduction-to-sqlite>

Sqlite.org. (2020). Distinctive Features Of SQLite. [online] <https://www.sqlite.org/different.html>

Wikipedia Contributors (2019). SQLite. [online] Wikipedia. <https://en.wikipedia.org/wiki/SQLite>

www.sqlite.org. (n.d.). How SQLite Works. [online] <https://www.sqlite.org/howitworks.html>.

Wikipedia Contributors (2019a). *Flutter (software)*. [online] Wikipedia. [https://en.wikipedia.org/wiki/Flutter_\(software\)](https://en.wikipedia.org/wiki/Flutter_(software))

Staysafeonline.org. (2025). *What About Password Manager Risks? - National Cybersecurity Alliance*. [online] Available at: <https://www.staysafeonline.org/articles/what-about-password-manager-risks>

Wikipedia. (2023). *Android SDK*. [online] Available at: https://en.wikipedia.org/wiki/Android_SDK

Karim Toubba (2022). *Security Incident December 2022 Update - LastPass - The LastPass Blog*. [online] Lastpass.com. Available at: <https://blog.lastpass.com/posts/notice-of-recent-security-incident>