Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής- Ανάπτυξη Λογισμικού και Τεχνητής Νοημοσύνης»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Αξιολόγηση τεχνολογιών αυθεντικοποίησης με χρήση σάρωσης προσώπου και ταυτοποιητικού εγγράφου** **Assessment of authentication technologies using face scanning and document id**
Ονοματεπώνυμο Φοιτητή	**Δημήτριος Κασώτης**
Πατρώνυμο	**Ιωάννης**
Αριθμός Μητρώου	**ΜΠΣΠ/ 20017**
Επιβλέπων	**Ευάγγελος Σακκόπουλος, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Απρίλιος 2022**

Μεταπτυχιακή Διατριβή Δημήτριος Κασώτης

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Ευθύμιος Αλέπης Αναπληρωτής Καθηγητής	Διονύσιος Σωτηρόπουλος Επίκουρος Καθηγητής	Ευάγγελος Σακκόπουλος Επίκουρος Καθηγητής

Σύνοψη

Η επαλήθευση ταυτότητας είναι απαραίτητη σε διάφορες πτυχές τις καθημερινότητας. Για αυτό το λόγο υπάρχει πληθώρα εφαρμογών όπου ενδεικτικά κυμαίνονται από το ξεκλείδωμα της κινητής συσκευής έως την πρόσβαση σε ηλεκτρονικό λογαριασμό. Εναλλακτικά μπορεί να έχει εφαρμογή στην καταγραφή των χρόνων άφιξης και εξόδου από την εργασία ή τον έλεγχο της πρόσβασης σε περιορισμένη περιοχή.

Η δημοφιλέστερη εκδοχή επαλήθευσης ταυτότητας είναι ο έλεγχος ταυτότητας με κωδικό πρόσβασης. Ωστόσο ο συγκεκριμένος τρόπος παρουσιάζει δυσκολίες οι οποίες χάριν παραδείγματος αφορούν σε ξεχασμένο ή κλεμμένο κωδικό πρόσβασης ή πολυπλοκότητα στη διαδικασία που δυσκολεύει τον εκάστοτε χρήστη.

Η παρούσα μεταπτυχιακή διατριβή παρουσιάζει μια εναλλακτική λύση η οποία έχει εφαρμογή σε κινητά τηλέφωνα τεχνολογίας Android και μπορεί να αποτελέσει βελτίωση στις υπάρχουσες μεθόδους επαλήθευσης ταυτότητας. Αυτή η βελτιωμένη επαλήθευση ταυτότητας είναι μια προσέγγιση μέσω του SDK που παρέχει η FaceTec.

Η εφαρμογή αποτελεί ένα συστήματα αυθεντικοποίησης που έχει ως προϋπόθεση ότι ο χρήστης έχει μια ταυτότητα την οποία καλείται να επαληθεύσει με έλεγχο προσώπου ή πληκτρολόγηση ενός username και password. Τα χαρακτηριστικά και οι ενέργειες του προσώπου του χρήστη πρέπει να ταιριάζουν με αυτά που έχουν αποθηκευτεί στο σύστημα για να περάσουν την επαλήθευση ταυτότητας. Η επαλήθευση απαιτεί την μετωπική όψη του προσώπου και επικυρώνει ταυτόχρονα τα χαρακτηριστικά και τις ενέργειες του προσώπου. Στην ουσία δημιουργεί μια ενσωμάτωση των χαρακτηριστικών και της δράσης του προσώπου σε ένα σύντομο βίντεο για αντιστοίχιση.

Με λίγα λόγια, ο χρήστης με μία βίντεο-selfie επαληθεύει το 3D liveness. Η εφαρμογή συγκρίνει το πρόσωπο του μέσω της φωτογραφίας του στο δίπλωμα, πραγματοποιείται οπτική αναγνώριση κειμένου του διπλώματος και επαληθεύει τα στοιχεία του. Εφόσον ο χρήστης ανοίξει εκ νέου την εφαρμογή ο έλεγχος ταυτότητας προσώπου αποδεικνύει και πάλι το 3D liveness το οποίο συγκρίνεται με το ήδη καταχωρημένο 3D Face Map και πραγματοποιεί είσοδο στην εφαρμογή χωρίς να απαιτείται κωδικός πρόσβασης.

Abstract

In our everyday life, identity verification is needed everywhere. There are plenty of applications where indicatively range from unlocking the mobile device to accessing an online account. Alternatively it may apply to recording arrival and exit times from work or controlling access to a restricted area.

The most popular version of authentication is password authentication. However, this way presents difficulties that for example concern a forgotten or stolen password or complexity in the process that makes it difficult for the user.

The present master's thesis presents an alternative that has application in Android technology mobile phones and can be an improvement on existing authentication methods. This improved identity verification is an approach through the SDK provided by FaceTec.

The application is an authentication system that has as a condition that the user has an identity which he is required to verify by face checking or typing a username and password. The characteristics and actions of the user's face must match those stored in the system to pass identity verification. Verification requires the frontal view of the face and validates the facial features and actions at the same time. In essence it creates an integration of facial features and facial action into a short video for matching.

In short, the user with one video-selfie verifies 3D liveness. The app compares his face through his photo on the ID, performs visual text recognition of the ID and verifies his details. Once the user re-opens the application face authentication again demonstrates the 3D liveness which is compared to the already registered 3D face Map and performs login without requiring password.

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1°

1. ΕΙΣΑΓΩΓΗ

Η ανίχνευση ζωντάνιας (3D Liveness) στα βιομετρικά στοιχεία είναι η ικανότητα ενός συστήματος να ανιχνεύει εάν ένα δακτυλικό αποτύπωμα ή πρόσωπο (ή άλλα βιομετρικά στοιχεία) είναι πραγματικό (από ένα ζωντανό άτομο που υπάρχει στο σημείο σύλληψης) ή ψεύτικο (από ένα τεχνούργημα spoof ή άψυχο μέρος του σώματος).

Περιλαμβάνει ένα σύνολο τεχνικών χαρακτηριστικών για την αντιμετώπιση των βιομετρικών επιθέσεων πλαστογράφησης, όπου ένα αντίγραφο που μιμείται τα μοναδικά βιομετρικά στοιχεία ενός ατόμου (όπως ένα καλούπι δακτυλικών αποτυπωμάτων ή μια μάσκα 3D από σιλικόνη) παρουσιάζεται στο βιομετρικό σαρωτή για να εξαπατήσει ή να παρακάμψει τα βήματα αναγνώρισης και ελέγχου ταυτότητας που δίνονται από το σύστημα.

Ο έλεγχος ζωντάνιας, χρησιμοποιεί αλγόριθμους που αναλύουν δεδομένα-αφού συλλεχθούν από βιομετρικούς σαρωτές και αναγνώστες - για να επαληθεύσουν εάν η πηγή προέρχεται από μια ψεύτικη αναπαράσταση. Η ανάγκη για σαφή και ασφαλή αναγνώριση και έλεγχο ταυτότητας έχει παρακινήσει μια μαζική ανάπτυξη βιομετρικών συστημάτων παγκοσμίως. Η αυξημένη δημόσια αποδοχή, η ευρεία προσφορά και η πτώση των τιμών των αισθητήρων, των καμερών, έξυπνων κινητών και του λογισμικού έχουν επιταχύνει αυτές τις τάσεις.

Στην παρούσα μεταπτυχιακή διατριβή θα παρουσιαστεί μια λύση 3D Liveness Authentication, η οποία έχει εφαρμογή σε κινητά τηλέφωνα τεχνολογίας Android και μπορεί να αποτελέσει βελτίωση στις υπάρχουσες μεθόδους επαλήθευσης ταυτότητας. Αυτή η βελτιωμένη επαλήθευση ταυτότητας είναι μια προσέγγιση μέσω του SDK που παρέχει η FaceTec.

Παρακάτω δίνονται βασικοί ορισμοί εννοιών όπου αναφέρθηκαν προγενέστερα:

- **FaceTec** : Παρέχει πατενταρισμένο λογισμικό ελέγχου ταυτότητας προσώπου 3D.
- **Liveness Checks** : Το πρόσωπο του χρήστη αναλύεται από το AI του FaceTec και αν οι εικόνες δεν περιέχουν ζωντανό άνθρωπο, η συνεδρία απορρίπτεται ως spoof (πλαστογράφηση).
- **Authentication** : Ταυτόχρονη ανίχνευση ζωντάνιας και 3D αντιστοίχιση προσώπου του χρήστη με τον προηγουμένως συλλεγέντα χάρτη προσώπου 3D. Πρόκειται για αντικατάσταση κωδικού πρόσβασης για σύνδεση σε μία εφαρμογή.
- **3D FaceMaps** : Το κρυπτογραφημένο αρχείο που περιέχει σχετικά βιομετρικά δεδομένα από τη συνεδρία ελέγχου ταυτότητας του χρήστη. Κάθε 3D FaceMap περιέχει δεδομένα μιας συνεδρίας. Το μέσο μέγεθος ενός πολύπλευρου χάρτη προσώπου 3D είναι περίπου 300 KB.

Στο επόμενο κεφάλαιο γίνεται αναφορά σε λύσεις που υπάρχουν διαθέσιμες σχετικά με το registration και authentication με 3D liveness. Στο 3ο κεφάλαιο, περιγράφονται οι απαιτήσεις, η ανάλυση και ο σχεδιασμός της εφαρμογής που υλοποιήθηκε. Στο 4ο κεφάλαιο, περιγράφεται η υλοποίηση και ορισμένα κρίσιμα στοιχεία του κώδικα της εφαρμογής. Στο 5ο κεφάλαιο, παρουσιάζεται η εφαρμογή με παραδείγματα. Στο 6ο κεφάλαιο, παρουσιάζονται τα συμπεράσματα που προέκυψαν από τη μελέτη αυτή, και ιδέες για περαιτέρω βελτίωση της εφαρμογής. Τέλος, ακολουθεί η παράθεση των βιβλιογραφικών πηγών που αξιοποιήθηκαν.

Κεφάλαιο 2ο

1. ΕΙΣΑΓΩΓΗ – ΑΝΑΣΚΟΠΗΣΗ ΠΕΔΙΟΥ

Η βιομετρία ως τεχνολογία για την αναγνώριση ενός ατόμου με βάση τη μέτρηση και τη στατιστική ανάλυση των μοναδικών φυσικών ή συμπεριφορικών χαρακτηριστικών του, είναι ένα φαινόμενο μεγάλης σημασίας στη σύγχρονη κοινωνία. Είναι ένα κλειδί για την εδραίωση της ψηφιακής ταυτότητας, που ενισχύεται από την ανάγκη για συστήματα διαχείρισης ταυτότητας μεγάλης κλίμακας.

Οι ειδικοί υποστηρίζουν ότι οι τάσεις ανάπτυξης στην επαλήθευση ταυτότητας μέσω κινητού τηλεφώνου θα διατηρηθούν λόγω της πρόσφατης εξάπλωσης πανδημίας που οδηγεί στην έκρηξη των αγορών που αφορούν ηλεκτρονικές ταυτότητες. Επομένως, αυτή τη στιγμή, μια τέτοια τεχνική που εξασφαλίζει ότι το βιομετρικό δείγμα υποβάλλεται από ένα πραγματικό ζωντανό άτομο, ένα σημαντικό χαρακτηριστικό ασφαλείας που μετριάζει την ευπάθεια των βιομετρικών συστημάτων σε επιθέσεις πλαστογράφησης, γίνεται ιδιαίτερα σημαντική. Αυτή η συγκεκριμένη τεχνική ονομάζεται ανίχνευση ζωντάνιας. Η βιομετρική ζωντάνια, αναφέρεται στη χρήση τεχνολογίας όρασης υπολογιστή για την ανίχνευση της πραγματικής παρουσίας ενός ζωντανού χρήστη, παρά μια αναπαράσταση όπως μια φωτογραφία ή μια μάσκα, βίντεο ή οθόνη, ένα ψεύτικο δακτυλικό αποτύπωμα ή άλλα πλαστά αντικείμενα.

Η ανίχνευση ζωντάνιας συνδέεται συνήθως με την αναγνώριση προσώπου ωστόσο μπορεί να εφαρμοστεί σε βιομετρικά στοιχεία δακτύλων και παλάμη ή στην αναγνώριση φωνής. Από τη λίστα των εταιρειών που χρησιμοποιούν liveness τεχνολογία ανίχνευσης, διαπιστώνουμε ότι η πλειοψηφία τους ειδικεύεται στην ζωντάνια του προσώπου (π. χ. 3D Face Matching από FaceTec ή SVORT, και έλεγχο ζωντάνιας προσώπου από το ID R&D και Innovatrics).

Ένας μικρός αριθμός εταιρειών παρέχει βιομετρική ζωντάνια δακτύλων ή παλάμης (π.χ. τεχνική χωρίς επαφή από την IDENTY, λογισμικό δακτυλικών αποτυπωμάτων από ακριβή βιομετρικά στοιχεία), αναγνώριση φωνής (π. χ. η τεχνολογία VSR της Liopa ελέγχει εάν τα ψηφία ομιλούνται σωστά και έτσι καθορίζει εάν υπάρχει ένα πραγματικό "ζωντανό" άτομο). Επίσης μοναδικές λύσεις αναπτύσσονται από την AuthMe, η οποία ειδικεύεται στην ανίχνευση ζωντανών καρδιακών παλμών, και το Nymi, το οποίο τα φορητά χρησιμοποιούν δακτυλικό αποτύπωμα για έλεγχο ταυτότητας και καρδιακό παλμό για ανίχνευση ζωντάνιας.

2.1.1 Πάροχοι ανίχνευσης ζωντάνιας

Acuant (ΗΠΑ)
Η Acuant παρέχει πλήρη επαλήθευση ταυτότητας. Χρησιμοποιεί μηχανική μάθηση και βιομετρικά στοιχεία για να αυτοματοποιήσει τη διαδικασία επαλήθευσης και να προσφέρει λύσεις που είναι ελεγμένες στο NIST και συμβατές με iBeta με τα βραβεία Επιπέδου 1 & 2 του Presentation Attack Detection (PAD).

ALiCE Biometrics (Γαλλία)
Το ALiCE είναι μια λύση επαλήθευσης ταυτότητας που επιτρέπει στους χρήστες να εγγράφονται στο διαδίκτυο γρήγορα, αυτόματα και με ασφάλεια.

Ariadnext (Ταϊβάν)
Η Ariadnext είναι ένας από τους παρόχους υπηρεσιών ψηφιακής ταυτοποίησης και διαθέτει πιστοποίηση FIDO για την πιστοποίηση βιομετρικών στοιχείων. Ο χρήστης πρέπει να εκτελέσει τα βήματα που ζητούνται από τη λύση κατά τη διάρκεια μιας ροής βίντεο και η λύση ανίχνευσης ζωντάνιας του Ariadnext βασίζεται στην ανάλυση κίνησης μεταξύ δύο αυτοματοποιημένων λήψεων εικόνων. Το API του Project κάνει πολλαπλές συγκρίσεις μεταξύ του βίντεο και της εξαγόμενης φωτογραφίας από το έγγραφο ταυτότητας.

AuthMe (Ταϊβάν)
Η AuthMe παρέχει λύσεις ελέγχου ταυτότητας που αξιοποιούν την αναγνώριση προσώπου και την ανίχνευση παθητικής ζωντάνιας για τον εντοπισμό επιθέσεων απάτης με τεχνητή νοημοσύνη, όπως το deepfake.

Basis ID (Εσθονία)
Η Basis ID είναι μια πλατφόρμα επαλήθευσης ταυτότητας, ενσωμάτωσης πελατών και διαχείρισης δεδομένων KYC που έχει δημιουργηθεί για την επίλυση των προκλήσεων των επιχειρηματικών εργασιών για KYC και AML.

BioID (Γερμανία)
Η BioID είναι πρωτοπόρος και ένας από τους κορυφαίους παίκτες στον εντοπισμό ζωντάνιας προσώπου βάσει λογισμικού στα βιομετρικά στοιχεία. Αξιοποιεί περισσότερα από 20 χρόνια εμπειρίας στα βιομετρικά. Η κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας ανίχνευση επίθεσης παρουσίασης επιτρέπει την επαλήθευση ταυτότητας KYC για πελάτες σε όλο τον κόσμο. Το BioID προσφέρει βιομετρικά στοιχεία ως υπηρεσία με ανίχνευση ζωντάνιας συμβατό με το ISO/IEC 30107. Ο έλεγχος ταυτότητας που βασίζεται σε λογισμικό και η τεχνολογία κατά της πλαστογράφησης επιτρέπουν μια απρόσκοπτη εμπειρία χρήστη, που απαιτεί μόνο δύο selfies.

BixeLab (Αυστραλία)
Η BixeLab εξουσιοδοτεί τους οργανισμούς να παρέχουν μια αξιόπιστη εμπειρία βιομετρίας και ταυτότητας. Οι ολοκληρωμένες δοκιμές του παρέχουν σιγουριά και βεβαιότητα όπου χρησιμοποιούνται βιομετρικές τεχνολογίες για την επαλήθευση ταυτοτήτων για τη βελτίωση των κοινωνικών, τεχνολογικών και οικονομικών αποτελεσμάτων.
Είναι το μοναδικό εργαστήριο NIST της Αυστραλίας, δοκιμάζει αυστηρά τα συστήματα σύμφωνα με εθνικά και διεθνώς αναγνωρισμένα βιομετρικά πρότυπα. Παρέχει έμπειρες και ανεξάρτητες υπηρεσίες δοκιμών για το πρόσωπο, το δακτυλικό αποτύπωμα, την ίριδα, τη φωνή, καθώς και για πολλαπλούς τρόπους με έμφαση στην τεχνολογία ανίχνευσης επίθεσης παρουσίασης και ζωντάνιας. Επιπλέον, η λύση BixeLab είναι συμβατή με το ISO-30107.

Chooch AI (ΗΠΑ)
Το Chooch AI είναι μια Visual AI υπηρεσία. Ως ολοκληρωμένη πλατφόρμα Visual AI , το Chooch περιλαμβάνει ένα API, έναν πίνακα εργαλείων και SDK. Το Chooch λύνει ένα θεμελιώδες πρόβλημα στο

Visual AI, την ικανότητα απόκτησης οπτικής τεχνογνωσίας με δομημένο τρόπο παρόμοιο με την ανθρώπινη γνώση. Συνδυάζοντας την εκπαίδευση στην όραση υπολογιστή με τη μηχανική εκμάθηση, η Chooch προσφέρει έλεγχο ταυτότητας προσώπου με ανίχνευση ζωντάνιας.

Daltrey (Αυστραλία)
Η αποστολή του Daltrey είναι να επαναπροσδιορίσει τον τρόπο με τον οποίο η ταυτότητα χρησιμοποιείται για τη δημιουργία ασφαλέστερων, πιο ασφαλών περιβαλλόντων. Χρησιμοποιώντας βιομετρική τεχνολογία, παρέχει στους οργανισμούς μια λύση ταυτότητας που οδηγεί την πολιτική ασφαλείας από μια θέση εμπιστοσύνης.

FaceTec (ΗΠΑ)
Η FaceTec ιδρύθηκε το 2013 και είναι ένας από τους παγκόσμιους ηγέτες στο λογισμικό ζωντάνιας και αντιστοίχισης προσώπου 3D. Ως η μόνη τεχνολογία που υποστηρίζεται από ένα πρόγραμμα bounty spoof και πιστοποιημένο από NIST/iBeta σχετικά με την ανίχνευση ζωντάνιας, η FaceTec είναι η παγκόσμια υπηρεσία με εκατομμύρια χρήστες σε έξι ηπείρους σε χρηματοοικονομικές υπηρεσίες, ασφάλεια συνόρων, μεταφορές, blockchain, ηλεκτρονική ψηφοφορία, κοινωνικά δίκτυα, online ραντεβού και άλλα.
Το κατοχυρωμένο με δίπλωμα ευρεσιτεχνίας, κορυφαίο στον κλάδο λογισμικό 3D ελέγχου ταυτότητας προσώπου της FaceTec εδραιώνει την ψηφιακή ταυτότητα, δημιουργώντας μια αλυσίδα εμπιστοσύνης από την ενσωμάτωση χρήστη έως τον συνεχή έλεγχο ταυτότητας σε όλες τις σύγχρονες έξυπνες συσκευές και κάμερες web. Οι τρισδιάστατοι χάρτες προσώπου της FaceTec καθιστούν δυνατή την αξιόπιστη, απομακρυσμένη επαλήθευση ταυτότητας.

ID R&D (ΗΠΑ)
Η ID R&D συνδυάζει εκτεταμένες δυνατότητες E&A με προόδους στην τεχνητή νοημοσύνη για να προσφέρει ανώτερα βιομετρικά στοιχεία φωνής και λογισμικό ανίχνευσης παθητικής φωνής και ζωντάνιας προσώπου. Είναι συμβατή με το ISO 27001 με τους ισχύοντες ελέγχους για την ποιότητα του κώδικα και τον μετριασμό του κινδύνου.

IDEMIA (Γαλλία)
Η IDEMIA είναι μια πολυεθνική εταιρεία τεχνολογίας με έδρα το Courbevoie της Γαλλίας. Παρέχει υπηρεσίες ασφαλείας που σχετίζονται με την ταυτότητα και πουλά αναγνώριση προσώπου και άλλα προϊόντα και λογισμικό βιομετρικής αναγνώρισης σε ιδιωτικές εταιρείες και κυβερνήσεις.

IDENTY (ΗΠΑ)
Το IDENTY παρέχει έλεγχο ταυτότητας πολλαπλών παραγόντων που βασίζεται σε πιστοποιημένα βιομετρικά στοιχεία υψηλής απόδοσης χωρίς αφή με ανίχνευση ζωντάνιας για κινητά τηλέφωνα και υπολογιστές με τυπικές κάμερες.

Innovatrics (Σλοβακία)
Η Innovatrics είναι ένας πάροχος πολυτροπικών βιομετρικών λύσεων με έδρα την ΕΕ. Οι αλγόριθμοί τους κατατάσσονται σταθερά μεταξύ των ταχύτερων και ακριβέστερων στην αναγνώριση δακτυλικών αποτυπωμάτων και προσώπου. Για περισσότερα από 16 χρόνια, συνεργάζεται με όλους τους τύπους οργανισμών για τη δημιουργία αξιόπιστων και ευέλικτων λύσεων βιομετρικής ταυτοποίησης.

iProov (Ηνωμένο Βασίλειο)
Η iProov είναι ένας ταχέως αναπτυσσόμενος παγκόσμιος πάροχος τεχνολογίας και ένας από τους παγκόσμιους ηγέτες στην παροχή Γνήσιας Διασφάλισης Παρουσίας σε οργανισμούς σε όλο τον κόσμο. Η Αυθεντική Διασφάλιση Παρουσίας είναι ο τρόπος για να επαληθεύσει ότι ένας διαδικτυακός χρήστης είναι το σωστό άτομο, ένα πραγματικό πρόσωπο και, κρίσιμα, ότι επαληθεύει την αυθεντικότητα αυτή τη στιγμή – όχι ένας απατεώνας ή μια επίθεση στον κυβερνοχώρο που καθοδηγείται από μηχανή.

Liopa (Ιρλανδία)
Το Liopa προέρχεται από το Queen's University Belfast και το Κέντρο Ασφαλών Τεχνολογιών Πληροφοριών (CSIT) . Ενσωματώθηκε τον Νοέμβριο του 2015 και εμπορευματοποιεί πάνω από 10 χρόνια έρευνας στον τομέα της επεξεργασίας ομιλίας και εικόνας με ιδιαίτερη έμφαση στη συγχώνευση κινήσεων ομιλίας και χειλιών για ισχυρή αναγνώριση ομιλίας σε περιβάλλοντα πραγματικού κόσμου. Το Liopa παρέχει έναν ασφαλή έλεγχο ζωής για έλεγχο ταυτότητας χρήστη στο διαδίκτυο. Χρησιμοποιώντας την τεχνολογία Visual Speech Recognition (VSR), μπορεί να επικυρώσει, μέσω ανάλυσης των κινήσεων των χειλιών, εάν ένας χρήστης επανέλαβε σωστά μια τυχαία ακολουθία ψηφίων και έτσι να επικυρώσει ότι υπάρχει ένα «ζωντανό» θέμα.

LIPS Corporation (Ταϊβάν)
Ιδρύθηκε το 2013 από μια ομάδα μελετητών του MIT και είναι πρωτοπόρος στις τεχνολογίες 3D ανίχνευσης και τεχνητής νοημοσύνης και παγκόσμιος πάροχος βιομηχανικών λύσεων ανίχνευσης 3D. Το LIPSFace AC770 είναι ένα ανέπαφο σύστημα αναγνώρισης προσώπου 3D AI που βασίζεται σε βιομετρικό έλεγχο ταυτότητας με προηγμένη ανίχνευση ζωντάνιας 3D όρασης.

NEC (Νέα Ζηλανδία)
Η NEC προσφέρει τεχνολογικές λύσεις και υπηρεσίες παγκόσμιας κλάσης σε πελάτες σε όλο τον κόσμο, για περισσότερο από έναν αιώνα. Για περισσότερα από 30 χρόνια συμβάλλει στη διατήρηση της ασφάλειας και της ασφάλειας των κοινοτήτων με έξυπνα συστήματα επιτήρησης και τεχνολογίες βιομετρικής ταυτοποίησης, καθώς και πλατφόρμες δικτύου και ασφάλειας. Το λογισμικό αναγνώρισης προσώπου της NEC, NeoFace® , παρέχει γρήγορη και ακριβή ικανότητα αντιστοίχισης και είναι το πιο ανθεκτικό σε παραλλαγές γήρανσης, φυλής και γωνίας στάσης. Η τεχνολογία αναγνώρισης προσώπου κατά της πλαστογράφησης χρησιμοποιεί τεχνητή νοημοσύνη για να ανιχνεύσει εάν ένα θέμα είναι πραγματικό πρόσωπο ή όχι. Χρησιμοποιείται σε συνδυασμό με την αναγνώριση προσώπου για να ανιχνεύσει εάν κάποιος υποδύεται δόλια ένα άλλο άτομο φορώντας, για παράδειγμα, προσθετική μάσκα ή παρουσιάζοντας μια άψυχη φωτογραφία ή εικόνα.

Nimi (Καναδάς)
Το Nymi Band, παρέχει στους οργανισμούς μια πλατφόρμα για να επιτύχουν μέγιστη ασφάλεια με εξουσιοδότηση βιομετρικών στοιχείων.

OCR Labs (Αυστραλία)
Η OCR Labs θεωρείται ως ένας από τους παγκόσμιους ηγέτες στον χώρο επαλήθευσης ψηφιακών ταυτοτήτων με διπλώματα ευρεσιτεχνίας στις διάφορες τεχνολογικές λύσεις τους.

Oz Forensics (ΗΠΑ)
Η βιομετρική πλατφόρμα Oz Forensics, που εδρεύει στις ΗΠΑ, παρέχει γρήγορη και ασφαλή αναγνώριση ανθρώπων, η οποία αποτρέπει βιομετρικές και βαθιές επιθέσεις χρησιμοποιώντας ανίχνευση ζωντάνιας.

Paravision (USA)
Η Paravision είναι μια εταιρεία που ειδικεύεται στην τεχνολογία αναγνώρισης προσώπου. Η πλατφόρμα αναγνώρισης προσώπου της Paravision είναι αξιόπιστη από παγκόσμιους κατασκευαστές συσκευών ασφαλείας, παρόχους λύσεων, ενοποιητές συστημάτων και εταιρείες χρηματοοικονομικών υπηρεσιών για την παροχή εμπειριών χωρίς τριβές και ολοκληρωμένη ασφάλεια.

Precise Biometrics (Σουηδία)
Η Precise είναι ένας παγκόσμιος πάροχος λογισμικού αναγνώρισης, που προσφέρει προϊόντα με μια σειρά εφαρμογών και διαθέτει μια κορυφαία ομάδα παγκοσμίως στην έρευνα και την ανάπτυξη με περισσότερα από 20 χρόνια εμπειρίας στην ανάπτυξη λύσεων αλγορίθμων για κινητά τηλέφωνα και έξυπνες κάρτες, η εταιρεία διαθέτει εξειδίκευση όσο λίγες άλλες στον κλάδο. Έχει τρεις τομείς προϊόντων: Ψηφιακή Ταυτότητα, Κινητό και Έξυπνες Κάρτες.

Saffe (Ηνωμένο Βασίλειο)
Η Saffe είναι ένας πάροχος αναγνώρισης προσώπου που βασίζεται στην τεχνητή νοημοσύνη και επικεντρώνεται σε πληρωμές και ασφαλείς ελέγχους ταυτότητας. Διαθέτει μια πολύ ισχυρή ανίχνευση ζωντάνιας που είναι σε θέση να ανιχνεύσει ένα ζωντανό άτομο καθώς και να εντοπίσει μια φωτογραφία από μια φωτογραφία ή ένα βίντεο και που συμβάλλει στη μείωση της απάτης και στην αύξηση της ασφάλειας.

Sensetime (Χονγκ Κονγκ)
Οι λύσεις smartphone της SenseTime υποστηρίζουν έξυπνα τερματικά με ξεκλείδωμα προσώπου, πληρωμή προσώπου, εφέ AR, εφέ VR διπλής κάμερας, έξυπνο άλμπουμ, εφέ φωτισμού πορτρέτου, αναγνώριση χειρονομιών και άλλες λειτουργίες.

Shufti Pro (Ηνωμένο Βασίλειο)
Το Shufti Pro προσφέρει λύσεις επαλήθευσης ταυτότητας με τεχνητή νοημοσύνη, όπως KYC (Know Your Customer), KYB (Know Your Business), επαλήθευση προσώπου, έλεγχος AML (Anti Money Laundering) και ελέγχου ασφαλείας αεροδρομίου χωρίς αφή.

Sumsub (Ηνωμένο Βασίλειο)
Το Sumsub είναι η λύση ταυτότητας με έδρα το Ηνωμένο Βασίλειο. Η εταιρεία παρέχει προϊόντα όπως ηλεκτρονική υπογραφή, κρυπτογραφική AML και προστασία αντιστροφής χρέωσης.

SVORT (ΗΠΑ)
Η SVORT είναι μια εταιρεία με έδρα τις ΗΠΑ που παρέχει λύσεις ασφαλείας βασισμένες σε ανώνυμα νευρο-βιομετρικά στοιχεία.

TECH5 (Ελβετία)
Η TECH5 είναι μια διεθνής εταιρεία τεχνολογίας αφιερωμένη στο σχεδιασμό, την ανάπτυξη και τη διανομή λύσεων διαχείρισης ταυτότητας που βασίζονται σε βιομετρικά στοιχεία.

Veriff (Εσθονία)
Η Veriff είναι μια εταιρεία που προσφέρει υπηρεσία επαλήθευσης ταυτότητας και ιδρύθηκε και εδρεύει στο Ταλίν της Εσθονίας. Η εταιρεία προσφέρει υπηρεσίες σε διαδικτυακές επιχειρήσεις για τον μετριασμό των προσπαθειών απάτης και την υποβοήθηση της κανονιστικής συμμόρφωσης.

VisionLabs (Ολλανδία)
Η VisionLabs ειδικεύεται στην ανάπτυξη προϊόντων και λύσεων στους τομείς της αναγνώρισης προσώπου, της αναγνώρισης αντικειμένων, της επαυξημένης πραγματικότητας και της εικονικής πραγματικότητας. Τα προϊόντα VisionLabs βασίζονται σε αλγόριθμους και τεχνολογίες αιχμής

2.1.2 Λύσεις 3D Liveness

SVORT (ΗΠΑ)

Η SVORT είναι μια εταιρεία με έδρα τις ΗΠΑ που παρέχει λύσεις ασφαλείας βασισμένες σε ανώνυμα νευρο-βιομετρικά στοιχεία. Δραστηριοποιείται στις βιομηχανίες Fintech και Crypto όπου η προστασία της ιδιωτικής ζωής των χρηστών αποτελεί προτεραιότητα.

Το SVORT μπορεί να χρησιμοποιηθεί σε οποιεσδήποτε συνηθισμένες κάμερες web για ανίχνευση ζωντάνιας, δημιουργία χαρτών 3D προσώπων και συναισθηματικές προκλήσεις, δηλαδή δεν χρειάζεται να αγοράσει κάποιος ειδικό εξοπλισμό. Ο αισθητήρας παρακολούθησης βάθους μπορεί να προσδιορίσει την ένταση της εικόνας καθιστώντας σχεδόν αδύνατη την πλαστογράφηση φωτογραφιών και βίντεο και ο αισθητήρας υπέρυθρων μπορεί να αποτρέψει την πλαστογράφηση της μάσκας καθώς παρακολουθεί το χάρτη θερμότητας του προσώπου. Κάτι τέτοιο κατέστη δυνατό με την ειδική επεξεργασία AI που αναπτύχθηκε από τη SVORT. Κατά την εγγραφή, το SVORT δημιουργεί το παραμετρικό τρισδιάστατο μοντέλο του προσώπου μέσω περιστροφικών κινήσεων. Το νευρωνικό δίκτυο μαθαίνει να ταιριάζει αυτό το τρισδιάστατο μοντέλο με ένα συγκεκριμένο κλειδί ή κωδικό πρόσβασης. Όταν ένας χρήστης περάσει τον έλεγχο ταυτότητας, καλείται να ολοκληρώσει μια σειρά από τυχαίες προκλήσεις με δισεκατομμύρια πιθανούς συνδυασμούς, κάνοντας δηλαδή αδύνατη την πρόβλεψη.

ID R&D (ΗΠΑ)

Η ID R&D συνδυάζει εκτεταμένες δυνατότητες E&A με προόδους στην τεχνητή νοημοσύνη για να προσφέρει ανώτερα βιομετρικά στοιχεία φωνής και λογισμικό ανίχνευσης παθητικής φωνής και ζωντάνιας προσώπου. Είναι συμβατό με το ISO 27001 με τους ισχύοντες ελέγχους για την ποιότητα του κώδικα και τον μετριασμό του κινδύνου.

Το IDLive™ Face αποτρέπει τις επιθέσεις πλαστογράφησης με το πρώτο προϊόν στον κόσμο μεμονωμένης εικόνας, παθητικό προϊόν ανίχνευσης ζωντάνιας προσώπου και το μοναδικό που είναι συμβατό με το iBeta Επίπεδο 1 και 2 ISO 30107-3 Presentation Attack Detection (PAD). Το IDLive Face βασίζεται στην ίδια εικόνα selfie που χρησιμοποιείται για την αντιστοίχιση βιομετρικών προσώπων, βελτιώνοντας την ασφάλεια ενώ προσθέτει μηδενική τριβή στις διαδικασίες ελέγχου ταυτότητας και ψηφιακής ενσωμάτωσης. Το προϊόν χρησιμοποιείται για την επεξεργασία εκατομμυρίων μηνιαίων συναλλαγών για πελάτες σε όλο τον κόσμο.

Innovatrics (Σλοβακία)

Η Innovatrics είναι ένας πάροχος πολυτροπικών βιομετρικών λύσεων με έδρα την ΕΕ. Οι αλγόριθμοί τους κατατάσσονται σταθερά μεταξύ των ταχύτερων και ακριβέστερων στην αναγνώριση δακτυλικών αποτυπωμάτων και προσώπου. Για περισσότερα από 16 χρόνια, συνεργάζεται με όλους τους τύπους οργανισμών για τη δημιουργία αξιόπιστων και ευέλικτων λύσεων βιομετρικής ταυτοποίησης.

Το SmartFace της Innovatrics είναι μια κλιμακούμενη πλατφόρμα αναγνώρισης προσώπου. Ο έλεγχος ζωντάνιας μπορεί να εκτελεστεί πλήρως στη συσκευή ενός χρήστη χωρίς καμία ανταλλαγή δεδομένων με τον διακομιστή και χρόνο απόκρισης 1 δευτερολέπτου. Είναι μεταξύ των πρώτων από μια χούφτα εταιρειών που προσφέρει τέτοια τεχνολογία, πλήρως εκτός σύνδεσης, με συμμόρφωση iBeta Level 2 .

2.1.3 Λύσεις 3D Liveness που χρησιμοποιούν το FaceTec

Authenteq
Η λύση επιτρέπει στους πελάτες να επαληθεύουν την ταυτότητά τους μέσω κινητού ή επιτραπέζιου υπολογιστή, διατηρώντας παράλληλα τον έλεγχο των δεδομένων τους.

Anyline
Η Anyline παρέχει ασφαλή λύση για την ψηφιοποίηση δεδομένων ταυτότητας και είναι πιστοποιημένη με ISO 27001. Κάθε σάρωση γίνεται επεξεργασία απευθείας στην κινητή συσκευή του χρήστη, εξασφαλίζοντας την ασφάλεια των δεδομένων. Η τεχνολογία σάρωσης ταυτότητας για κινητά, λειτουργεί εκτός σύνδεσης και σε όλες τις συνθήκες.

Idenfy
Η Idenfy έχει συνάψει συνεργασία με την FaceTec για να ενσωματώσει την ανίχνευση βιομετρικής ζωντάνιας 3D με την πλατφόρμα επαλήθευσης ταυτότητας Idenfy, επιτρέποντας την επιβεβαίωση ότι ο χρήστης είναι ένα πραγματικό πρόσωπο. Το Idenfy βελτιώνει την εμπειρία του χρήστη και αποτρέπει την απάτη και την κλοπή ταυτότητας χρησιμοποιώντας συσκευές πελατών ως τερματικά σάρωσης ταυτότητας.

Jumio
Η Jumio έχει προσθέσει την ανίχνευση Ζωντάνιας προσώπου ZoOm ® 3D της FaceTec στην ηλεκτρονική σουίτα επαλήθευσης ταυτότητας, παρέχοντας ένα επιπλέον επίπεδο διασφάλισης και πρόληψης απάτης για τις ψηφιακές επιχειρήσεις κατά τη διαδικασία δημιουργίας λογαριασμού.

Onfido
Η Onfido εγκαινίασε μια νέα πλατφόρμα που επεκτείνει την βιομετρική επαλήθευσης ταυτότητας που είχε. Το νέο Onfido Face Authenticate αναπτύχθηκε σε συνεργασία με το FaceTec, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε υπάρχοντες λογαριασμούς σε δευτερόλεπτα

Passbase
Το Passbase προσφέρει ασφαλή επαλήθευση ταυτότητας των πελατών τους μέσω εγγράφων ταυτότητας, selfies και κυβερνητικών βάσεων δεδομένων. Η τεχνολογία ανίχνευσης ζωντάνιας αποτρέπει τις εξελιγμένες προσπάθειες πλαστογράφησης εντοπίζοντας και ταξινομώντας τις ανακτημένες εκδόσεις ενός ατόμου από μια ζωντανή και γνήσια συνεδρία.

Yoti
Ενσωμάτωσαν το ZoOm στην έκδοση του διαδικτυακού προγράμματος εκτίμησης ηλικίας Yoti Age Scan, μια ασφαλή υπηρεσία ελέγχου ηλικίας που εκτιμά με ακρίβεια την ηλικία ενός ατόμου κοιτάζοντας το πρόσωπό του. Η ανίχνευση Ζωντανότητας του ZoOm – η οποία καθορίζει εάν ο νόμιμος χρήστης είναι πραγματικά ζωντανός και παρών κατά τη σύνδεση-είναι το κλειδί για την παροχή πραγματικά ασφαλούς πρόσβασης στο λογαριασμό.

Κεφάλαιο 3°

1. ΣΥΛΥΨΗ ΑΠΑΙΤΗΣΕΩΝ

Σε αυτό το σημείο θα ασχοληθούμε με την καταγραφή των απαιτήσεων του project και την ανάλυσή τους ώστε να δημιουργηθεί ένα αρχικό σχεδιάγραμμα το οποίο θα περιγράφει τις διάφορες λειτουργίες τις οποίες θα πρέπει το σύστημα που θα υλοποιήσουμε να εκτελεί. Για να γίνει αυτό θα πρέπει να γίνουν οι παρακάτω αναλύσεις:
• Ανάλυση αναγκών (Needs Analysis)
• Ανάλυση Χρηστών (User Analysis)
• Ανάλυση Εργασιών (Task Analysis)

2. ΑΝΑΛΥΣΗ ΑΝΑΓΚΩΝ (NEED ANALYSIS)

Το σύστημα που θέλουμε να υλοποιήσουμε, θα μπορεί να εκτελέσει κάποιες συγκεκριμένες εργασίες. Με σκοπό την ομαλή και ορθή εκτέλεση αυτών των διαδικασιών, πρέπει να προβούμε σε μία ανάλυση απαιτήσεων ως προς τον τρόπο υλοποίησης τους και των τεχνικών τις οποίες πρέπει να υλοποιήσουμε.

Αρχικά πρέπει όλα τα δεδομένα να αποθηκεύονται σε ένα σύστημα διαχείρισης το οποίο θα μας επιτρέπει με την χρήση ερωτημάτων να μπορούμε να εξάγουμε τις απαντήσεις μας. Αυτό προϋποθέτει την ύπαρξη μίας βάσης δεδομένων η οποία θα μας διευκολύνει τόσο στην καταχώρηση των δεδομένων μας όσο και στην εξαγωγή αποτελεσμάτων.

Η εφαρμογή που θα υλοποιήσουμε θα εκτελείται σε Android περιβάλλον με χρήση της γλώσσας προγραμματισμού Java και θα καταχωρούνται /αντλούνται δεδομένα από μία βάση δεδομένων στη Firebase.

3. ΑΝΑΛΥΣΗ ΧΡΗΣΤΩΝ (USER ANALYSIS)

Κατά την υλοποίηση της εφαρμογής θα έχουμε ένα είδος χρήστη ως στόχο, όσο αφορά την υλοποίηση αλλά και τις διαφορετικές λειτουργίες τις οποίες θα μπορεί να διατελέσει.
User: Ο χρήστης έχει πρόσβαση σε όλες τις λειτουργίες του συστήματος. Επιγραμματικά, αυτές οι λειτουργίες είναι:

- Εγγραφή στην εφαρμογή - Registration
- Αντιστοίχιση διπλώματος με φωτογραφία - Photo Id Match
- Προβολή & Αποθήκευση Φωτογραφιών - View & Save Photos
- Σύνδεση στην εφαρμογή - Log In
- Σύνδεση στη εφαρμογή - Face Authentication

- Προβολή Πληροφοριών χρήστη - User Information
- Προβολή Φωτογραφιών Χρήστη - User Photos

4. ΑΝΑΛΥΣΗ ΕΡΓΑΣΙΩΝ (TASK ANALYSIS)

Σε αυτό το σημείο θα οργανώσουμε την υλοποίηση του συστήματος σε διάφορες φάσεις – στάδια τα οποία θα μας βοηθήσουνε να διαχωρίσουμε σε τμήματα την όλη διαδικασία.

• Βάση Δεδομένων: Πρώτη θα πρέπει να αναλυθεί και να δημιουργηθεί η βάση δεδομένων στην οποία θα καταχωρούνται / αντλούνται δεδομένα. Η δομή της βάσης θα μας οδηγήσει εύκολα στην υλοποίηση των επιμέρους τμημάτων τα οποία τόσο θα εισάγουν, όσο και θα εξάγουν δεδομένα από αυτή με την βοήθεια διάφορων ερωτημάτων.

• Δημιουργία τάξεων: Μετά την δημιουργία της βάσης θα προχωρήσουμε στη δημιουργία τάξεων σε Java περιβάλλον όπου θα αποτελέσουν τον κορμό της εφαρμογής.

• Διασύνδεση βάσης δεδομένων με τις τάξεις: Στη συνέχεια θα υλοποιηθεί με κώδικα η διασύνδεση της βάσης δεδομένων με τις τάξεις.

Η βάση δεδομένων που θα χρησιμοποιηθεί είναι η Firebase Realtime, η οποία μας δίνει την ευκαιρία μέσω της εφαρμογής μας, για ασφαλή πρόσβαση στη βάση δεδομένων από την πλευρά του client κώδικα. Τα δεδομένα αποθηκεύονται προσωρινά τοπικά όταν γίνεται αποσύνδεση από το Διαδίκτυο, και μόλις η συσκευή ανακτά τη σύνδεση, σε πραγματικό χρόνο, η βάση δεδομένων συγχρονίζει τις τοπικές αλλαγές στοιχείων με τις απομακρυσμένες ενημερώσεις που συνέβησαν κατά την αποσύνδεση του πελάτη, ενοποιώντας κατά συνέπεια τα δεδομένα. Η βάση δεδομένων Realtime παρέχει κανόνες για το ποιος και πότε μπορεί να γράψει ή να διαβάσει τα δεδομένα που υπάρχουν στη Firebase. Πρόκειται για μια πολύ ισχυρή βάση δεδομένων NoSQL και, με αυτή την ιδιότητα, έχει μεγάλη χρησιμότητα σε σύγκριση με μια σχεσιακή βάση δεδομένων. Το API της βάσης δεδομένων επιτρέπει να πραγματοποιούνται λειτουργίες σε πραγματικό χρόνο με γρήγορη εκτέλεση των εντολών. Η βάση δεδομένων Firebase Realtime υποστηρίζει Android, iOS, web και πολλά άλλα. Όλα τα δεδομένα τίθενται σε μορφή JSON και οποιαδήποτε αλλαγή στα δεδομένα αντανακλάται αμέσως με την εκτέλεση ενός συγχρονισμού.

5. ΣΧΕΔΙΑΣΜΟΣ

Στη δραστηριότητα αυτή καταγράφεται η λειτουργικότητα του συστήματος, μέσω των αντίστοιχων Περιπτώσεων Χρήσης.

3.5.1 Εγγραφή - Registration

Τίτλος περίπτωσης χρήσης	Εγγραφή- Registration
Αναγνωριστικό περίπτωσης χρήσης	UC#1
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί εγγραφή στην εφαρμογή
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει email
Αποτέλεσμα	Ο χρήστης έκανε εγγραφή στην εφαρμογή
Βασική πορεία ενεργειών	
1.	Ο χρήστης επιθυμεί να κάνει χρήση της εφαρμογής
2.	Ο χρήστης επιλέγει την εφαρμογή από το menu
3.	Ο χρήστης συμπληρώνει Email, Password, Ονοματεπώνυμο
4.	Εφόσον συμπληρωθούν και τα τρία πεδία, η εγγραφή είναι

	επιτυχής
5.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν ο χρήστης δεν συμπληρώσει τα πεδία σωστά
2.	Εμφάνιση μηνύματος που αφορά τη συμπλήρωση του εκάστοτε πεδίου
3.	Υπάρχει περίπτωση επανάληψης μέχρι να συμπληρωθούν σωστά τα πεδία
Εναλλακτική πορεία ενεργειών (Β)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.1: Εγγραφή - Registration

3.5.2 Αντιστοίχιση διπλώματος με φωτογραφία – Photo Id Match

Τίτλος περίπτωσης χρήσης	Αντιστοίχιση διπλώματος με φωτογραφία - Photo Id Match
Αναγνωριστικό περίπτωσης χρήσης	UC#2
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί αντιστοίχιση ταυτότητας με φωτογραφία
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή ή σύνδεση στην εφαρμογή
Αποτέλεσμα	Ο χρήστης θα έχει πραγματοποιήσει αντιστοίχιση διπλώματος με φωτογραφία
Βασική πορεία ενεργειών	
1.	Ο χρήστης επιλέγει το button "Photo Id Match"
2.	Πραγματοποιείται 3D FaceScan
3.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D facescan στο FaceTec Server SDK
4.	Επιβεβαιώνεται το liveness.
5.	Πραγματοποιείται το Front Id Scan
6.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου Front ID Scan στο FaceTec Server SDK
7.	Πραγματοποιείται σάρωση του Front Id Scan
8.	Πραγματοποιείται έλεγχος ότι το 3d face scan ταιριάζει με το αναγνωριστικό (δίπλωμα)
9.	Πραγματοποιείται το Back Id Scan
10.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου Back ID Scan στο FaceTec Server SDK

11.	Ο χρήστης πραγματοποιεί έλεγχο στοιχείων του διπλώματος και επιλέγει επιβεβαίωση
12.	Πραγματοποιείται μεταφόρτωση των επιβεβαιωμένων στοιχείων στο FaceTec Server SDK και στη Firebase
13.	Πραγματοποιείται ενημέρωση ότι ολοκληρώθηκε ο έλεγχος του διπλώματος
14.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν δεν είναι ευδιάκριτο το 3D FaceScan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το 3D FaceScan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το 3D FaceScan
Εναλλακτική πορεία ενεργειών (Β)	
1.	Αν δεν είναι ευδιάκριτο το Front ID Scan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το Front ID Scan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το Front ID Scan
Εναλλακτική πορεία ενεργειών (Γ)	
1.	Αν δεν είναι ευδιάκριτο το Back ID Scan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το Back ID Scan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το Back ID Scan
Εναλλακτική πορεία ενεργειών (Δ)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.2: Αντιστοίχιση διπλώματος με φωτογραφία - Photo Id Match

3.5.3 View & Save Photos

Τίτλος περίπτωσης χρήσης	View & Save Photos
Αναγνωριστικό περίπτωσης χρήσης	UC#3
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης βλέπει τις φωτογραφίες που θα αποθηκευτούν στο Storage της Firebase

Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή ή σύνδεση στην εφαρμογή
Αποτέλεσμα	Οι φωτογραφίες του χρήστη αποθηκεύονται στο Storage της Firebase
Βασική πορεία ενεργειών	
1.	Ο χρήστης επιλέγει το button "View & Save Photos"
2.	Ο χρήστης βλέπει τις φωτογραφίες του
3.	Πραγματοποιείται αποθήκευση των φωτογραφιών στο Storage της Firebase και αποθήκευση στο κινητό
4.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.3: View & Save Photos

3.5.4 Σύνδεση - Log In

Τίτλος περίπτωσης χρήσης	Σύνδεση - Log In
Αναγνωριστικό περίπτωσης χρήσης	UC#4
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί σύνδεση στην εφαρμογή
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή
Αποτέλεσμα	Ο χρήστης συνδέθηκε επιτυχώς στην εφαρμογή
Βασική πορεία ενεργειών	
1.	Ο χρήστης επιθυμεί να κάνει χρήση της εφαρμογής
2.	Ο χρήστης επιλέγει την εφαρμογή από το menu
3.	Στη register οθόνη, ο χρήστης επιλέγει "Already registered?"
4.	Ο χρήστης συμπληρώνει Email και Password
5.	Εφόσον συμπληρωθούν τα δύο πεδία,επιτυχώς μπορεί να συνδεθεί στην εφαρμογή
6.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν ο χρήστης δεν συμπληρώσει τα πεδία σωστα
2.	Εμφάνιση μηνύματος που αφορά τη συμπλήρωση του εκάστωτε πεδίου

3.	Υπάρχει περίπτωση επανάληψης μέχρι να συμπληρωθούν σωστά τα πεδία
Εναλλακτική πορεία ενεργειών (Β)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.4: Σύνδεση - Log In

3.5.5 Σύνδεση - Face Authentication

Τίτλος περίπτωσης χρήσης	Σύνδεση - Face Authentication
Αναγνωριστικό περίπτωσης χρήσης	UC#5
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί σύνδεση στην εφαρμογή με επαλήθευση προσώπου
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή
Αποτέλεσμα	Ο χρήστης συνδέθηκε επιτυχώς στην εφαρμογή
Βασική πορεία ενεργειών	
1.	Ο χρήστης επιθυμεί να κάνει χρήση της εφαρμογής
2.	Ο χρήστης επιλέγει την εφαρμογή από το menu
3.	Στη register οθόνη, ο χρήστης επιλέγει "Already registered?"
4.	Ο χρήστης επιλέγει "Face Authentication" για να μεταφερθεί στη οθόνη που θα πραγματοποιηθεί ο έλεγχος ταυτοποίησης χρήστη
5.	Ο χρήστης επιλέγει "Authenticate User" για να πραγματοποιηθεί ο έλεγχος ταυτοποίησης χρήστη
6.	Εφόσον ολοκληρωθεί η διαδικασία επιτυχώς, επιτυγχάνεται η σύνδεση στην εφαρμογή
7.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν δεν είναι ευδιάκριτο το 3D FaceScan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το 3D FaceScan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το 3D FaceScan
Εναλλακτική πορεία ενεργειών (Β)	

1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.5: Σύνδεση - Face Authentication

3.5.6 User Information

Τίτλος περίπτωσης χρήσης	User Information
Αναγνωριστικό περίπτωσης χρήσης	UC#6
Παράγοντας	Χρήστης
Περιγραφή	Εμφάνιση πληροφορίων του διπλώματος του
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς σύνδεση στην εφαρμογή
Αποτέλεσμα	Ο χρήστης βλέπει τις πληροφορίες του διπλώματος του που έχουν καταγραφεί στη Firebase
Βασική πορεία ενεργειών	
1.	Ο χρήστης πραγματοποιεί Login στην εφαρμογή
2.	Ο χρήστης βλέπει τις πληροφορίες του διπλώματος του
3.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.6: User Information

3.5.7 User Photos

Περίπτωση χρήσης User Photos	
Τίτλος περίπτωσης χρήσης	User Photos
Αναγνωριστικό περίπτωσης χρήσης	UC#7
Παράγοντας	Χρήστης
Περιγραφή	Εμφάνιση φωτογραφιών χρήστη
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς σύνδεση στην εφαρμογή και να έχει επιλέξει το button "User Photos"
Αποτέλεσμα	Ο χρήστης βλέπει τις φωτογραφίες του (3D FaceScan, Front Id, Back Id)
Βασική πορεία ενεργειών	

1.	Ο χρήστης πραγματοποιεί Login στην εφαρμογή
2.	Ο χρήστης βλέπει τις πληροφορίες του διπλώματος του
3.	Ο χρήστης επιλέγει το button "User Photos"
4.	Ο χρήστης βλέπει τις φωτογραφίες του που έχουν αποθηκευτεί τοπικά στο κινητό
5.	Η περίπτωση χρήσης τελειώνει
Εναλλακτική πορεία ενεργειών (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.6: User Photos

Κεφάλαιο 4°

1. ΥΛΟΠΟΙΗΣΗ – ΚΩΔΙΚΑΣ

Σε αυτό το κεφάλαιο θα παρουσιαστεί το πως πραγματοποιήθηκε η υλοποίηση της εφαρμογής όπως επίσης και τα βασικά σημεία του κώδικα που αναπτύχθηκε ώστε να έχουν αποτέλεσμα οι διαδικασίες που παρέχει το sdk της FaceTec.

Τα δεδομένα του χρήστη της εφαρμογής αποθηκεύονται στη Firebase Realtime. Όλα τα δεδομένα της Firebase Realtime αποθηκεύονται ως αντικείμενα JSON. Μπορείτε να θεωρηθεί η βάση δεδομένων ως δέντρο JSON που φιλοξενείται στο σύννεφο. Σε αντίθεση με μια βάση δεδομένων SQL, δεν υπάρχουν πίνακες ή εγγραφές. Όταν προσθέτονται δεδομένα στο δέντρο JSON, γίνεται ένας κόμβος στην υπάρχουσα δομή JSON με ένα σχετικό κλειδί.

Επιπρόσθετα, λόγω του ότι επιθυμούμε η εφαρμογή να αποθηκεύει φωτογραφίες του χρήστη, χρησιμοποιήθηκε το Firebase Cloud Storage, το οποίο παρέχει έναν ασφαλή και αξιόπιστο τρόπο για την αποθήκευση και ανάκτηση αρχείων.

Σύμφωνα με την ανάλυση απαιτήσεων, προκύπτει ότι η βάση δεδομένων πρέπει να περιλαμβάνει τους παρακάτω κόμβους. Ενδεικτικά παρακάτω παραθέτονται τα δεδομένα ενός χρήστη που έχει ολοκληρώσει τη διαδικασία ταυτοποίησης:


```
"5IySfIFmNqRNjI22kByDAhyBZAq1" : {
  "auditString" : "auditString-601ed464-cbd5-491c-80c1-ad27616d5dc4",
  "backString" : "backString-f92185a1-5818-4ab1-bef0-8b51d27d2d17",
  "dateOfBirth" : "02.01.19XX",
  "expirationDate" : "27.10.20XX",
  "externalDatabaseRefId" : "android_sample_app_68bf9223-48fd-412d-a0b4-87e7bd9712be",
  "firstName" : "DIMITRIOS",
  "frontString" : "frontString-600d1824-3da6-4dd8-a02f-568778bd939e",
  "issuedDate" : "27.10.2020",
  "lastName" : "KASOTIS",
  "photoId" : "080XXXXXX",
  "secondaryId" : "07XXXXXXX"
```


Εικόνα 1. Δεδομένα χρήστη που έχουν αποθηκευτή στη Realtime Database

4.1.1 Εγγραφή χρήστη (Registration)

```
/*
 * we initialise the register button, and the actions that will handle
 */
private void InitialiseRegisterButton() {
    btn_register = findViewById(R.id.bnt_login);
    btn_register.setOnClickListener(new View.OnClickListener() {
        @Override
        public void onClick(View v) {
            if (ValidateInputFields()) {
                String email = emailId.getText().toString();
                String passwrdTxt = password.getText().toString();
                String fullName = et_fullName.getText().toString();
                mFirebaseAuth = FirebaseAuth.getInstance();
                //we register user in Firebase
                mFirebaseAuth.createUserWithEmailAndPassword(email, passwrdTxt).addOnCompleteListener(new OnCompleteListener<AuthResult>() {
                    @Override
                    public void onComplete(@NonNull Task<AuthResult> task) {
                        if (task.isSuccessful()) {
                            try {
                                // After the successfull registration we update the display name
                                FirebaseUser user = task.getResult().getUser();
                                UserProfileChangeRequest.Builder userProfileBuilder =
                                        new UserProfileChangeRequest.Builder().setDisplayName(fullName);
                                user.updateProfile(userProfileBuilder.build()).addOnCompleteListener(new OnCompleteListener<Void>() {
                                    @Override
                                    public void onComplete(Task<Void> task) {
                                        if (task.isSuccessful()) {
                                            /*
                                             * we create the custom user object and we store it to user repository
                                             */
                                            User currentUser = new User(user, null);
                                            userRepository = com.unipi.myfacetec.UserRepository.getInstance();
                                            userRepository.setCurrentUser(currentUser);
                                            //we route the user to another activity
                                            routeAfterLogin();
                                        } else {
                                            Toast.makeText(RegisterMainActivity.this, task.getException().getLocalizedMessage(), Toast.LENGTH_SHORT).show();
                                        }
                                    }

                                });

                            } catch (Exception ex) {
                                Toast.makeText(RegisterMainActivity.this, ex.getLocalizedMessage(), Toast.LENGTH_SHORT).show();
                            }
                        } else {
                            Toast.makeText(RegisterMainActivity.this, task.getException().getLocalizedMessage(), Toast.LENGTH_SHORT).show();
                        }
                    }
                });
            }
        }
    });
}
```

Εικόνα 2. Κώδικας που αφορά στο registration του χρήστη στην εφαρμογή

4.1.2 Photo ID Match

```
// Perform Photo ID Match, generating a username each time to guarantee uniqueness.
public void onPhotoIDMatchPressed(View view) {
    isSessionPreparingToLaunch = true;

    utils.fadeOutMainUIAndPrepareForFaceTecSDK(new Runnable() {
        @Override
        public void run() {
            getSessionToken(new MainActivity.SessionTokenCallback() {
                @Override
                public void onSessionTokenReceived(String sessionToken) {
                    isSessionPreparingToLaunch = false;
                    latestExternalDatabaseRefID = "android_sample_app_" + randomUUID();
                    latestProcessor = new PhotoIDMatchProcessor(sessionToken, MainActivity.this);

                }
            });
        }
    });
}
```

Εικόνα 3. Κώδικας που αφορά στη διαδικασία Photo Id Match

4.1.3 Αποτελέσματα του Photo ID Match (OCR Results)

```
String responseString = response.body().string();
response.body().close();
try {
    JSONObject responseJSON = new JSONObject(responseString);
    boolean wasProcessed = responseJSON.getBoolean("wasProcessed");
    String scanResultBlob = responseJSON.getString("scanResultBlob");
    String externalDatabaseRefId = responseJSON.getString("externalDatabaseRefID");


    new JSONObject(new JSONObject(responseJSON.getString("ocrResults")).getString("ocrResults")).getJSONObject("scanned").getJSONArray("groups");
    JSONArray details = new JSONObject(new JSONObject(responseJSON.getString("ocrResults")).getString("ocrResults"))
            .getJSONObject("scanned").getJSONArray("groups");
    JSONObject jObj = details.getJSONObject(0);
    JSONArray xxx = jObj.getJSONArray("fields");

    String lastName = xxx.getJSONObject(0).getString("value");
    String name = xxx.getJSONObject(1).getString("value");
    String dateOfbirth = xxx.getJSONObject(2).getString("value");

    JSONObject jObj2 = details.getJSONObject(1);
    JSONArray xxx2 = jObj2.getJSONArray("fields");

    String idNumber = xxx2.getJSONObject(0).getString("value");
    String idNumber2 = xxx2.getJSONObject(1).getString("value");
    String issueDate = xxx2.getJSONObject(2).getString("value");
    String expireDate = xxx2.getJSONObject(3).getString("value");
```

Εικόνα 4. Κώδικας που αφορά στα αποτελέσματα του Photo Id Match

4.1.4 Εισαγωγή των δεδομένων στη Realtime Database

```
public static void insertUserData(Data data) {
    try {

        userDataDatabase = database.getReference("UserData");
        userDataDatabase.child(data.getUserUUID()).child("lastName").setValue(data.getLastName());
        userDataDatabase.child(data.getUserUUID()).child("firstName").setValue(data.getFirstName());
        userDataDatabase.child(data.getUserUUID()).child("dateOfBirth").setValue(data.getDateOfBirth());
        userDataDatabase.child(data.getUserUUID()).child("issuedDate").setValue(data.getIssuedDate());
        userDataDatabase.child(data.getUserUUID()).child("expirationDate").setValue(data.getExpirationDate());
        userDataDatabase.child(data.getUserUUID()).child("photoId").setValue(data.getPhotoId());
        userDataDatabase.child(data.getUserUUID()).child("secondaryId").setValue(data.getSecondaryId());
        userDataDatabase.child(data.getUserUUID()).child("externalDatabaseRefId").setValue(data.getExternalDatabaseRefId());


    } catch (Exception e) {

    }

}
```

Εικόνα 5. Κώδικας που αφορά στην εισαγωγή δεδομένων στη Realtime Database

4.1.5 Upload φωτογραφιών στο Firebase Storage

```
//function to upload the image to firebase storage
private void uploadImages() {
    // Create a Cloud Storage reference from the app

    ArrayList<byte[]> myImages = new ArrayList<>();
    storage = FirebaseStorage.getInstance();


    //compress and converts to byte array
    if (this.latestIDScanResult != null && !this.latestIDScanResult.getFrontImagesCompressedBase64().isEmpty()) {
        byte[] frontString = Base64.decode(this.latestIDScanResult.getFrontImagesCompressedBase64().get(0), Base64.DEFAULT);
        uploadImage("frontString", frontString);
        doInBackground(frontString, "2");
    }

    if (this.latestIDScanResult != null && !this.latestIDScanResult.getBackImagesCompressedBase64().isEmpty()) {
        byte[] backString = Base64.decode(this.latestIDScanResult.getBackImagesCompressedBase64().get(0), Base64.DEFAULT);
        uploadImage("backString", backString);
        doInBackground(backString, "3");
    }
    int pos = this.latestSessionResult.getAuditTrailCompressedBase64().length - 1;
    if (this.latestSessionResult != null && this.latestSessionResult.getAuditTrailCompressedBase64()[pos] != null) {
        byte[] auditString = Base64.decode(this.latestSessionResult.getAuditTrailCompressedBase64()[pos], Base64.DEFAULT);
        uploadImage("auditString", auditString);
        doInBackground(auditString, "1");
    }
}

private void uploadImage(String imageName, byte[] image) {
    StorageReference storageRef = storage.getReference("Selfies");
    UUID imageId = UUID.randomUUID();
    StorageReference imageRef = storageRef.child(imageName + "-" + imageId.toString());
    StorageMetadata metadata = new StorageMetadata.Builder()
            .setContentType("image/jpg")
            .setCustomMetadata("propertyName", imageName)
            .build();

    UploadTask uploadTask = imageRef.putBytes(image, metadata);

    uploadTask.addOnFailureListener(new OnFailureListener() {
        //handle failure
        @Override
        public void onFailure(@NonNull Exception exception) {
            Toast.makeText(MainActivity.this, exception.getMessage().toString(), Toast.LENGTH_SHORT).show();
        }
    }).addOnSuccessListener(new OnSuccessListener<UploadTask.TaskSnapshot>() {
        //handle sucess

        @Override
        public void onSuccess(UploadTask.TaskSnapshot taskSnapshot) {

            StorageMetadata metaData = taskSnapshot.getMetadata();
            String imageName = metaData.getName();

            String propertyName = metadata.getCustomMetadata("propertyName");
            DatabaseReference myRef = FirebaseDatabase.getInstance().getReference();
            DatabaseReference databaseReference = myRef.child("UserData");
            databaseReference.child(getCurrentUser().getUUID()).child(propertyName).setValue(imageName);
            Toast.makeText(MainActivity.this, getText(R.string.image_uploaded_sucessfully).toString(), Toast.LENGTH_SHORT).show();
        }
    });

}
```

Εικόνα 6. Κώδικας που αφορά στο upload φωτογραφιών στο Firebase Storage

4.1.6 Login Χρήστη

```
private void isValidUser() {
    myRef = FirebaseDatabase.getInstance().getReference();

    Query query = myRef.child("UserData");
    ArrayList<Data> userDataArrayList = new ArrayList<>();
    query.addListenerForSingleValueEvent(new ValueEventListener() {
        Intent routedActivity=null;

        @Override
        public void onDataChange(@NonNull DataSnapshot dataSnapshot) {


            for (DataSnapshot snapshot : dataSnapshot.getChildren()) {

                String uuid = getCurrentUser().getUUID();
                    if(uuid.equals(snapshot.getKey())){
                        if (getCurrentUser()!=null){
                            routedActivity = new Intent(getApplicationContext(),UserDataActivity.class);
                            isValidatedUser = true;
                        } else{
                            routedActivity = new Intent(getApplicationContext(),MainActivity.class);
                        }
                        break;
                    }
            }

            if(!isValidatedUser){
                routedActivity = new Intent(getApplicationContext(),MainActivity.class);
            }

            startActivity(routedActivity);
        }

        @Override
        public void onCancelled(@NonNull DatabaseError error) {

        }
    });
}
```

Εικόνα 7. Κώδικας που αφορά στη διαδικασία Login

4.1.7 Face Authentication Χρήστη

```
//Perform Authentication
public void onAuthenticateUserPressed1(View v) {
    isSessionPreparingToLaunch = true;
    utilsLogin.fadeOutMainUIAndPrepareForFaceTecSDK(new Runnable() {
        @Override
        public void run() {
            getSessionToken(new faceAuthActivity.SessionTokenCallback() {
                @Override
                public void onSessionTokenReceived(String sessionToken) {
                    isSessionPreparingToLaunch = false;
                    latestProcessor = new AuthenticateProcessor(sessionToken, faceAuthActivity.this);
                }
            });
        }
    });
}
```

Εικόνα 8. Κώδικας που αφορά στη διαδικασία Face Authentication

4.1.8 Έλεγχος υπαρκτού RefId χρήστη

```
public void getLatestExternalDatabaseRefIDFromDB(MyCallback myCallback) {

    DatabaseReference myRef = FirebaseDatabase.getInstance().getReference();
    FirebaseAuth mAuth = FirebaseAuth.getInstance();

    Query query = myRef.child("UserData");
    ArrayList<Data> userDataArrayList = new ArrayList<>();
    query.addListenerForSingleValueEvent(new ValueEventListener() {

        @Override
        public void onDataChange(@NonNull DataSnapshot dataSnapshot) {

            String uuid = mAuth.getCurrentUser().getUid();


            for (DataSnapshot snapshot : dataSnapshot.getChildren()) {
                Data data = snapshot.getValue(Data.class);
                userDataArrayList.add(data);
                if (uuid.equals(snapshot.getKey())) {
                    myCallback.onCallback(data);

                    break;
                }
            }
        }

        @Override
        public void onCancelled(@NonNull DatabaseError error) {

        }
    });


}
```

Εικόνα 9. Κώδικας που αφορά στον έλεγχο υπαρκτότητας RefId χρήστη

4.1.9 Εμφάνιση δεδομένων χρήστη

```
Intent userIntent = getIntent();
if (userIntent.hasExtra("userdata")) {
    try {
        JSONObject jObj = new JSONObject(userIntent.getStringExtra("userdata"));
        textView_firstName.setText("First name : " + jObj.optString("firstName"));
        textView_lastName.setText("Last name : " + jObj.optString("lastName"));
        textView_dateOfBirth.setText("Date of Birth : " + jObj.optString("dateOfBirth"));
        textView_photoId.setText("Photo ID # : " + jObj.optString("photoId"));
        textView_secondaryId.setText("Secondary ID # : " + jObj.optString("secondaryId"));
        textView_issuedDate.setText("Issued Date : " + jObj.optString("issuedDate"));
        textView_expirationDate.setText("Expiration Date : " + jObj.optString("expirationDate"));
        textView_welcome.setText("Welcome" + " " + jObj.optString("lastName") + " " + jObj.optString("firstName") + " ! ");


    } catch (JSONException e) {
        e.printStackTrace();
    }
} else {
    myRef = FirebaseDatabase.getInstance().getReference();
    showUserData();
}

}
```

Εικόνα 10. Κώδικας που αφορά στην εμφάνιση δεδομένων του χρήστη

4.1.10 Εμφάνιση φωτογραφιών χρήστη

```
private void showUserPhotos(StorageReference storageRef) {
    UserRepository userRepository= UserRepository.getInstance();
    User currentUser=userRepository.getCurrentUser();

    Query query = myRef.child("UserData");
    ArrayList<Photos> userPhotosArrayList = new ArrayList<>();


    query.addListenerForSingleValueEvent(new ValueEventListener() {
        FirebaseAuth mAuth =FirebaseAuth.getInstance();
        String uuid=mAuth.getCurrentUser().getUid();

        StorageReference storageReference = FirebaseStorage.getInstance().getReference("Selfies");


        @Override
        public void onDataChange(@NonNull DataSnapshot dataSnapshot) {
            for (DataSnapshot snapshot : dataSnapshot.getChildren()) {
                Photos photos = snapshot.getValue(Photos.class);
                userPhotosArrayList.add(photos);

                Bitmap auditImage = getLocalImage(uuid + "1");
                Bitmap frontImage = getLocalImage(uuid + "2");
                Bitmap backImage = getLocalImage(uuid + "3");

                auditStringPhoto.setImageBitmap(auditImage);
                frontStringPhoto.setImageBitmap(frontImage);
                backStringPhoto.setImageBitmap(backImage);

                break;
            }
        }

        @Override
        public void onCancelled(@NonNull DatabaseError error) {

        }
    });

}
```

Εικόνα 11. Κώδικας που αφορά στην εμφάνιση φωτογραφιών του χρήστη

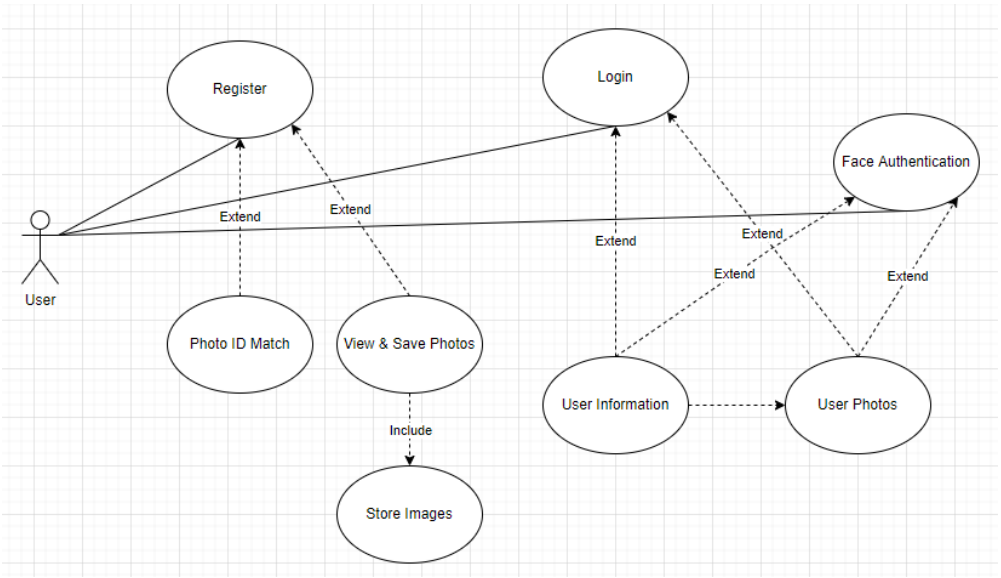
Κεφάλαιο 5°

1. ΕΦΑΡΜΟΓΗ MYFACETEC

5.1.1 Εισαγωγή

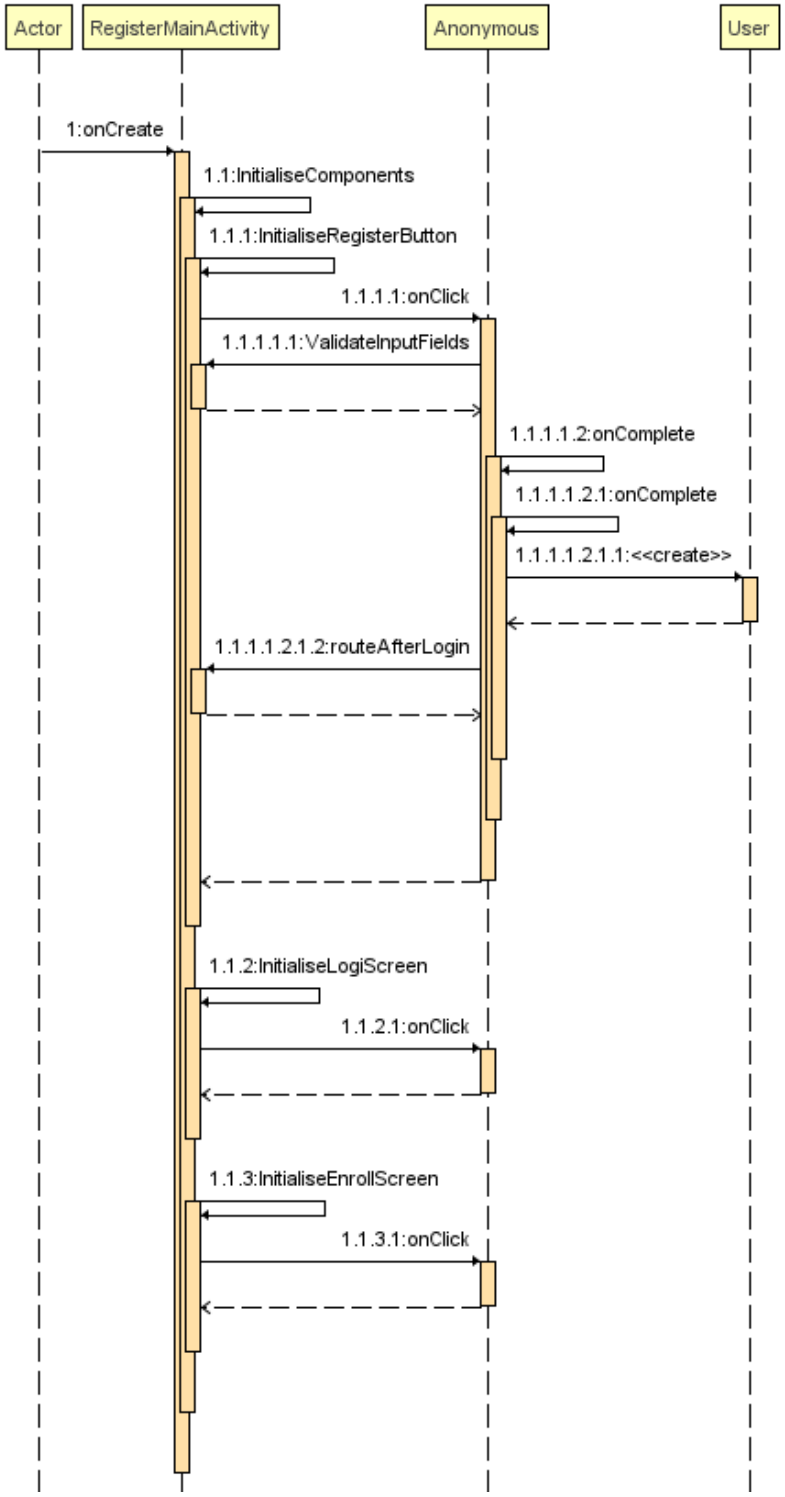
Η εφαρμογή MyFaceTec, συγκρίνει το πρόσωπο του εγγεγραμμένου χρήστη με τη φωτογραφία του στο δίπλωμα οδήγησης, πραγματοποιείται οπτική αναγνώριση κειμένου του διπλώματος, επαληθεύει τα στοιχεία του και εξάγει δεδομένα όπως το ονοματεπώνυμο, ημερομηνία γέννησης, ΑΦΜ, ημερομηνία έκδοσης και λήξης διπλώματος και αριθμός διπλώματος. Εφόσον ο χρήστης ανοίξει εκ νέου την εφαρμογή ο έλεγχος ταυτότητας προσώπου αποδεικνύεται μέσω 3D liveness το οποίο συγκρίνεται με το ήδη καταχωρημένο 3D Face Map και πραγματοποιεί είσοδο στην εφαρμογή χωρίς να απαιτείται κωδικός πρόσβασης.

5.1.2 Use Case Diagram

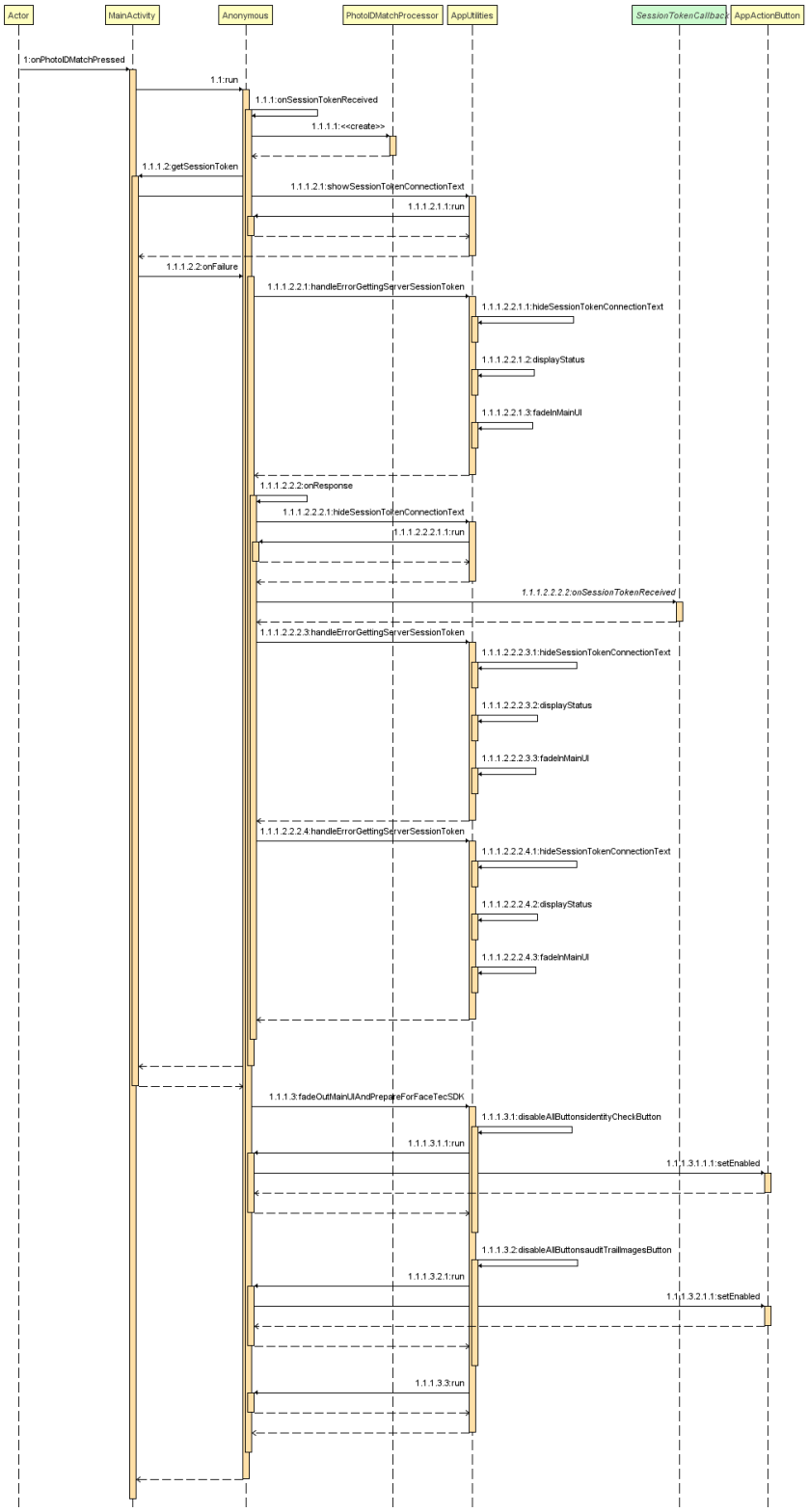


Εικόνα 12. Use Case Diagram εφαρμογής MyfaceTec

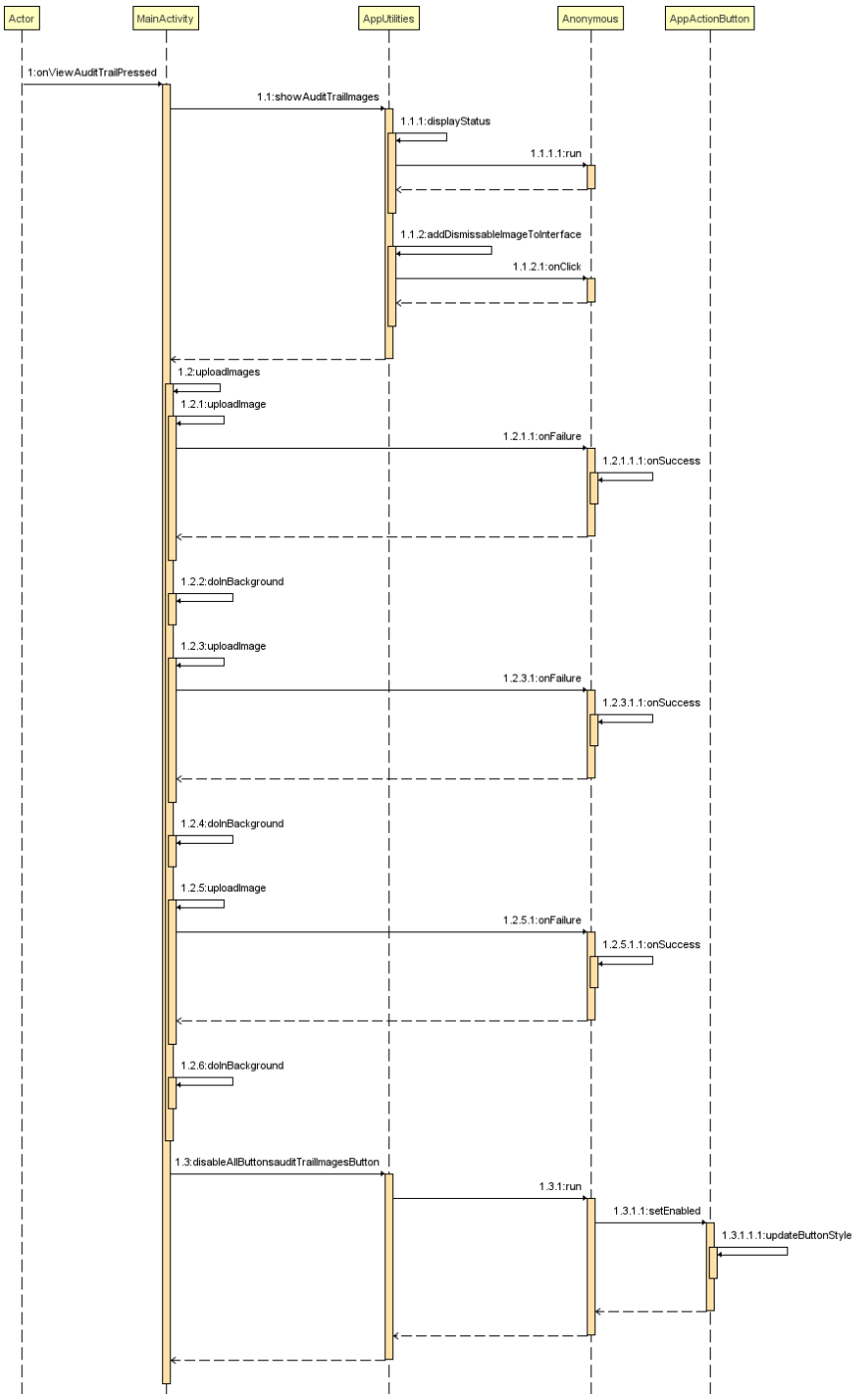
5.1.3 Sequence Diagrams



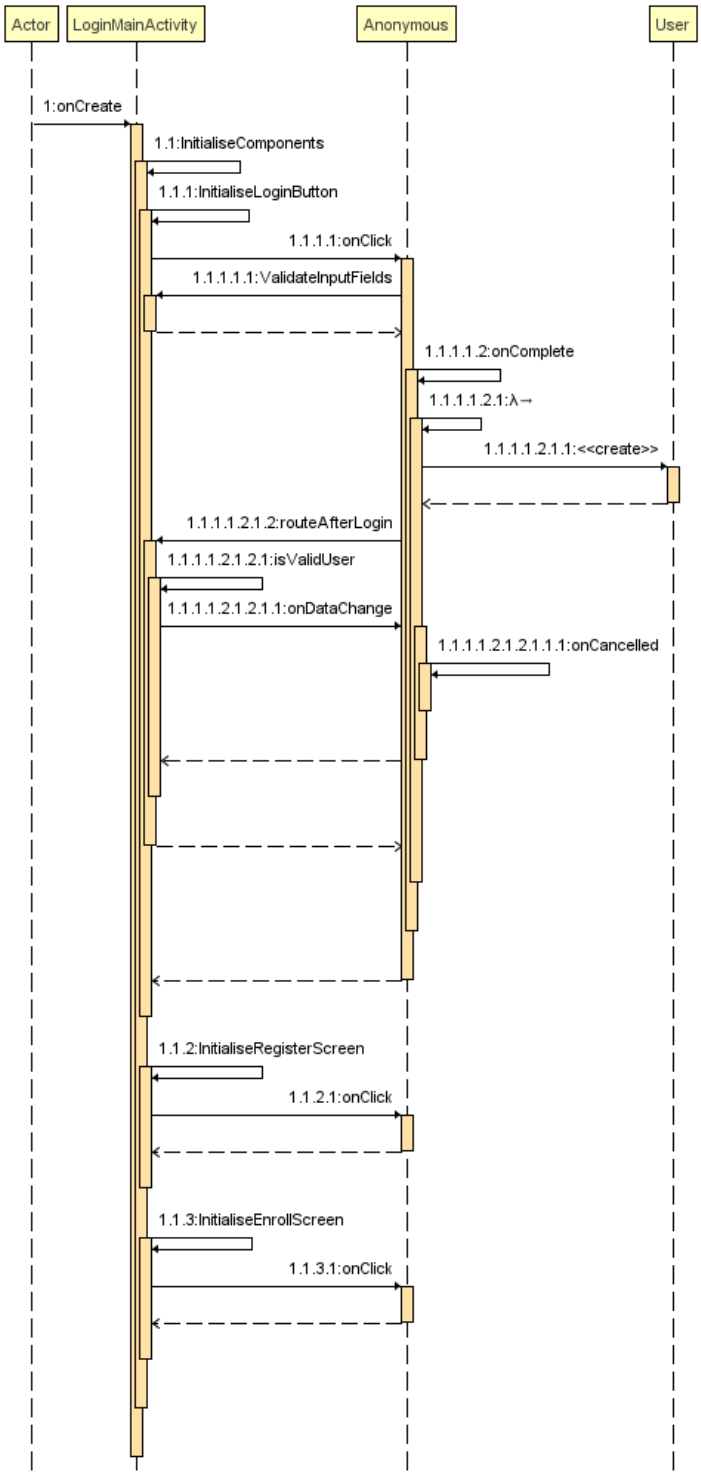
Εικόνα 13. Sequence Diagram RegisterMainActivity



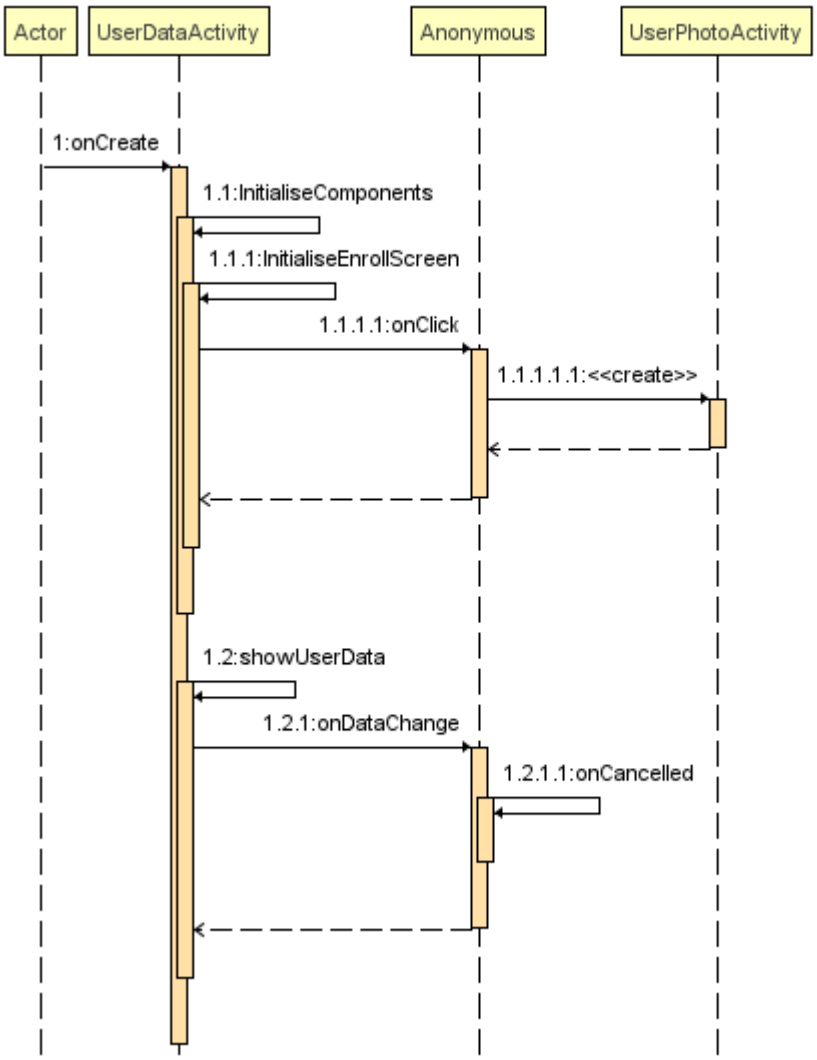
Εικόνα 14. Sequence Diagram Photo Id Match



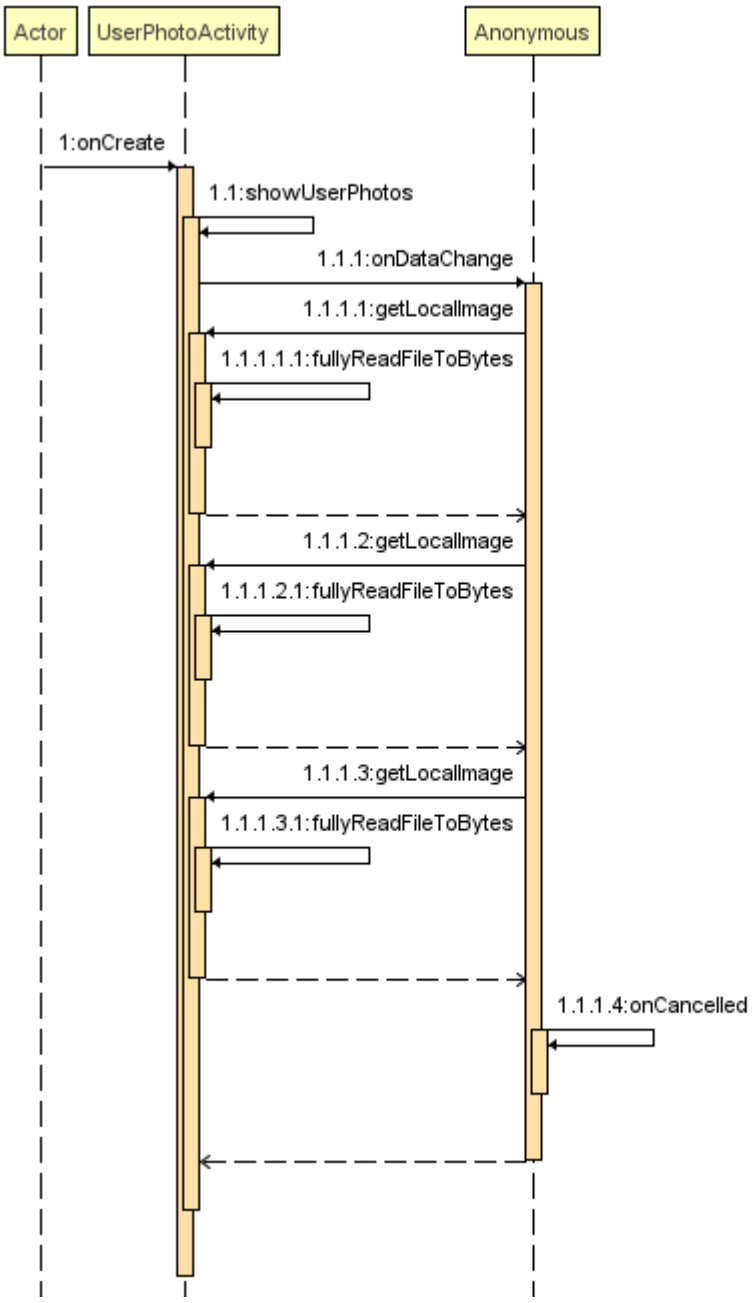
Εικόνα 15. Sequence Diagram View & Save Photos



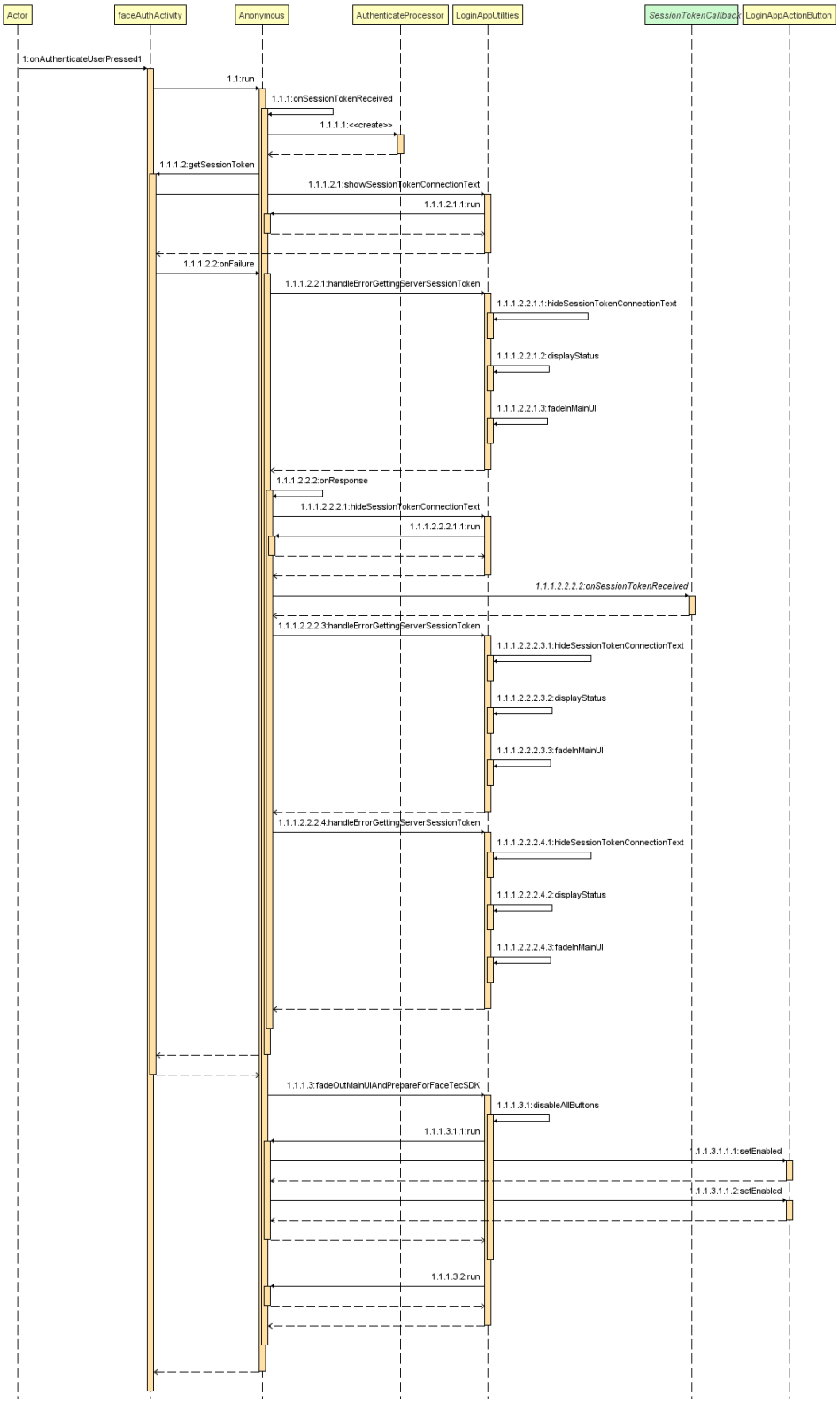
Εικόνα 16. Sequence Diagram Login



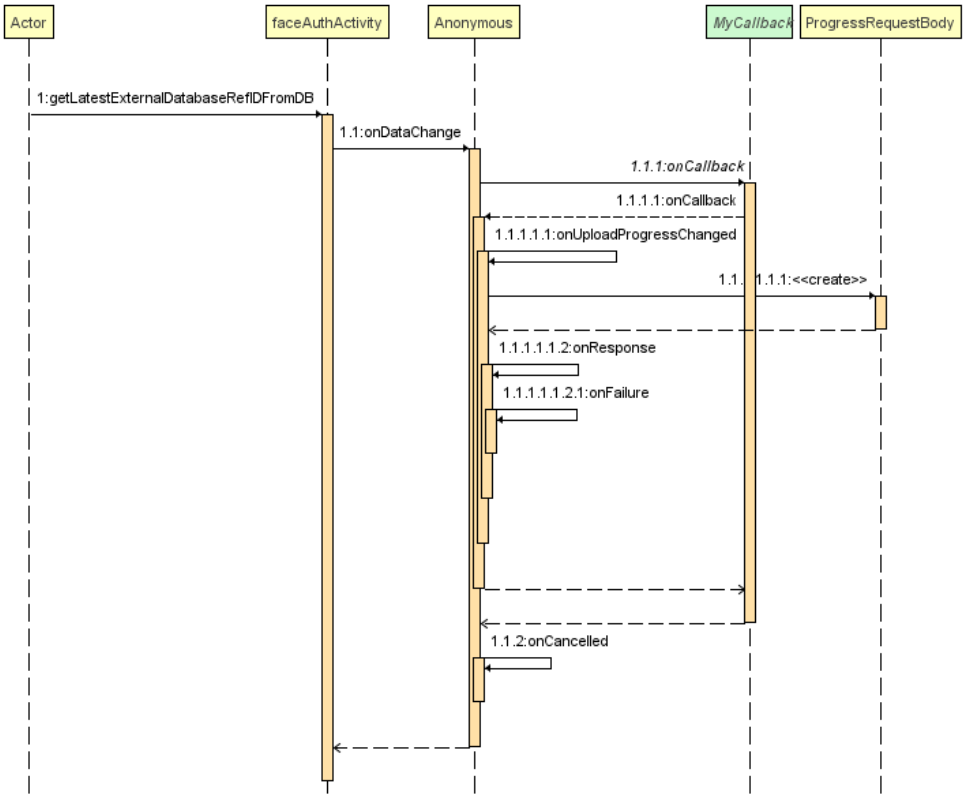
Εικόνα 17. Sequence Diagram UserDataActivity



Εικόνα 18. Sequence Diagram UserPhotoActivity



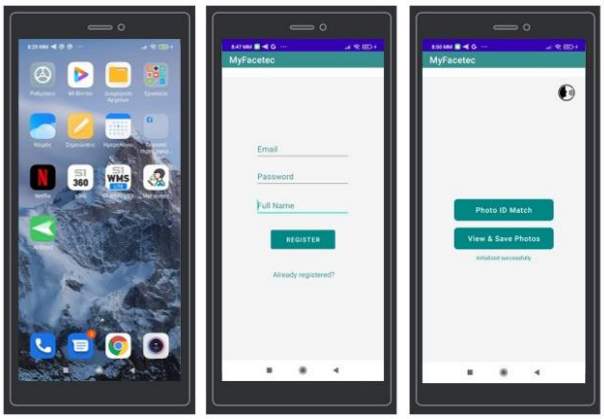
Εικόνα 19. Sequence Diagram FaceAuthActivity (Authentication)



Εικόνα 20. Sequence Diagram FaceAuthActivity (getLatestExternalRefIdFromDb)

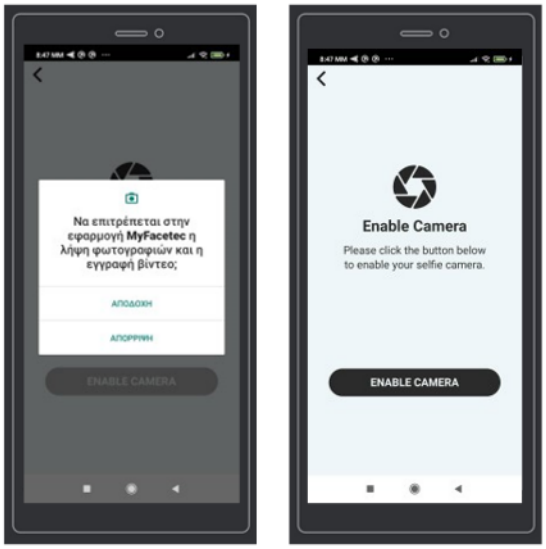
5.1.4 Ροή εφαρμογής

Ο χρήστης επιλέγει την εφαρμογή και εμφανίζεται η οθόνη που μπορεί να κάνει εγγραφή. Κατόπιν της εγγραφής ο χρήστης επιλέγει το button «Photo Id Match» ώστε να ξεκινήσει η διαδικασία ταυτοποίησης (3D FaceScan και αντιστοίχιση διπλώματος).



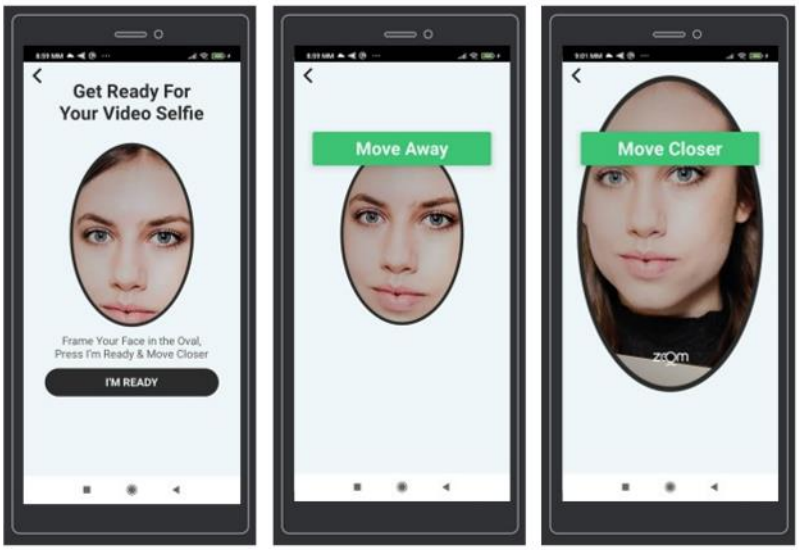
Εικόνα 21. Ροή εφαρμογής (1)

Την πρώτη φορά που θα χρησιμοποιήσει ο χρήστης την εφαρμογή, ζητούνται δικαιώματα ώστε να μπορεί να χρησιμοποιηθεί η κάμερα του κινητού τηλεφώνου.



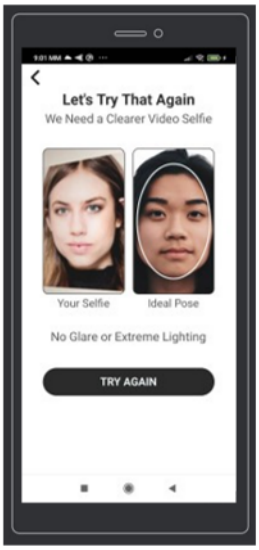
Εικόνα 22. Ροή εφαρμογής (2)

Επιλέγοντας «Enable Camera», ξεκινάει η διαδικασία όπου δίνονται οδηγίες ώστε να ολοκληρωθεί η διαδικασία «Video Selfie» που αποδεικνύει το 3D Liveness.



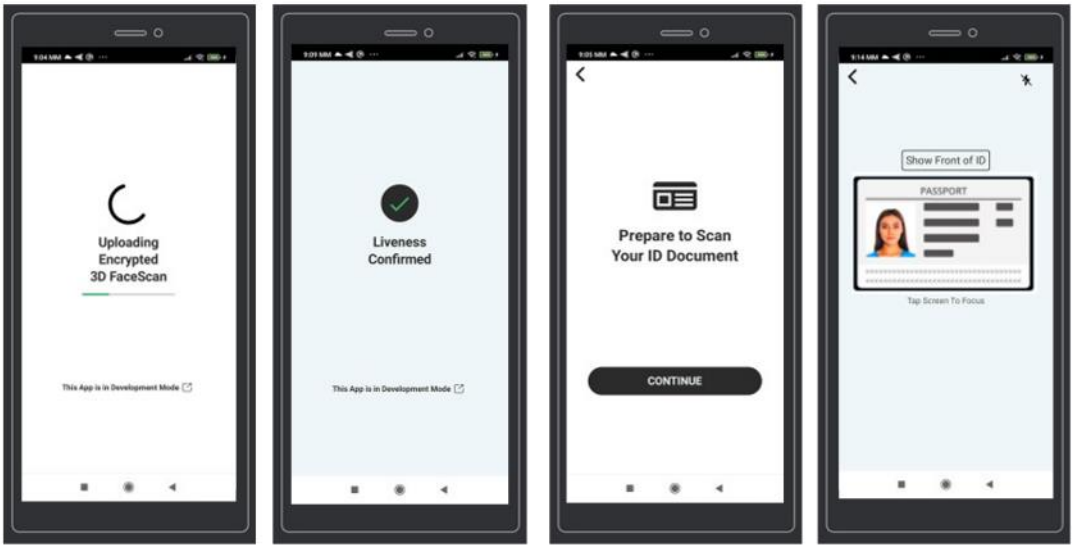
Εικόνα 23. Ροή εφαρμογής (3)

Σε περίπτωση που η «Video Selfie» δεν έχει ευκρίνεια, εμφανίζεται σχετική ενημέρωση προς το χρήστη με προτροπή να δοκιμάσει εκ νέου.



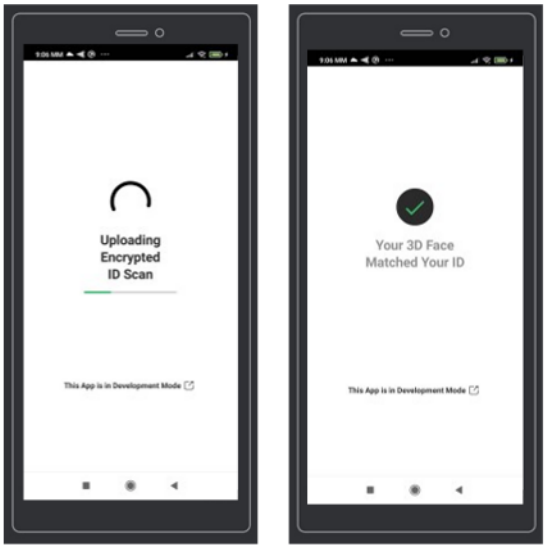
Εικόνα 24. Ροή εφαρμογής (4)

Μόλις ολοκληρωθεί επιτυχώς η λήψη της «Video Selfie» τότε αρχίζει η αποστολή της κρυπτογραφημένης 3D FaceScan στο Server της FaceTec. Έπειτα σύμφωνα με τη ροή της εφαρμογής, ενημερώνεται ο χρήστης ώστε να έχει διαθέσιμο προς σάρωση το μπροστινό μέρος του διπλώματος.



Εικόνα 25. Ροή εφαρμογής (5)

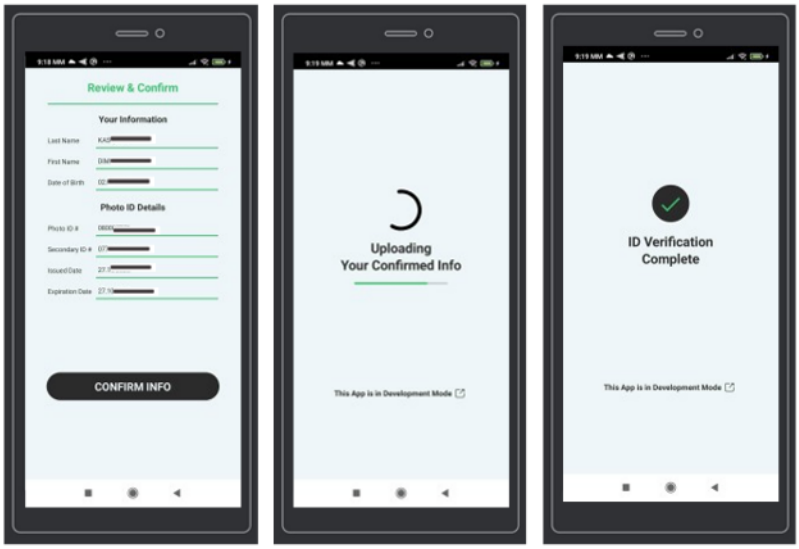
Εφόσον ολοκληρωθεί η διαδικασία, δηλαδή ανέβει το μπροστινό μέρος του διπλώματος στο server της FaceTec και επιβεβαιωθεί ότι ταιριάζει η «Video Selfie» με τη φωτογραφία προσώπου στο δίπλωμα τότε εμφανίζει ομότιτλο μήνυμα και συνεχίζεται η διαδικασία σχετικά με τη σάρωση του πίσω μέρους του διπλώματος.



Εικόνα 26. Ροή εφαρμογής (6)

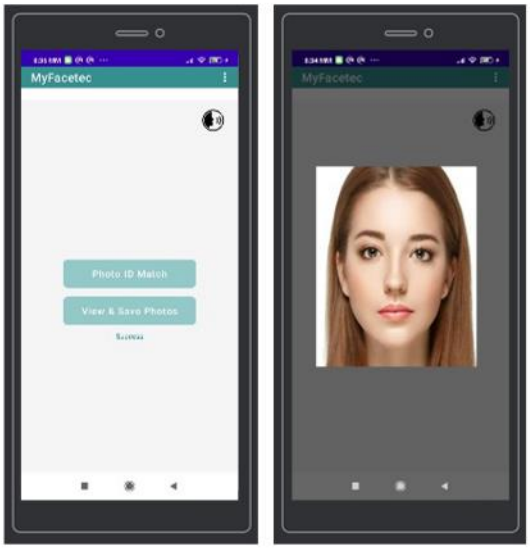
Εικόνα 27. Ροή εφαρμογής (7)

Μόλις ολοκληρωθεί η διαδικασία που αφορά τη σάρωση του πίσω μέρους του διπλώματος, εμφανίζονται τα στοιχεία χρήστη. Αν για οποιοδήποτε λόγο η διαδικασία έχει φέρει κάτι λάθος, ο χρήστης μπορεί να το αλλάξει και να επιλέξει επιβεβαίωση πληροφοριών. Έπειτα ανεβαίνουν τα στοιχεία τόσο στο server της FaceTec όσο και στη Firebase Realtime και εμφανίζεται μήνυμα ότι ολοκληρώθηκε η επιβεβαίωση «ταυτότητας».



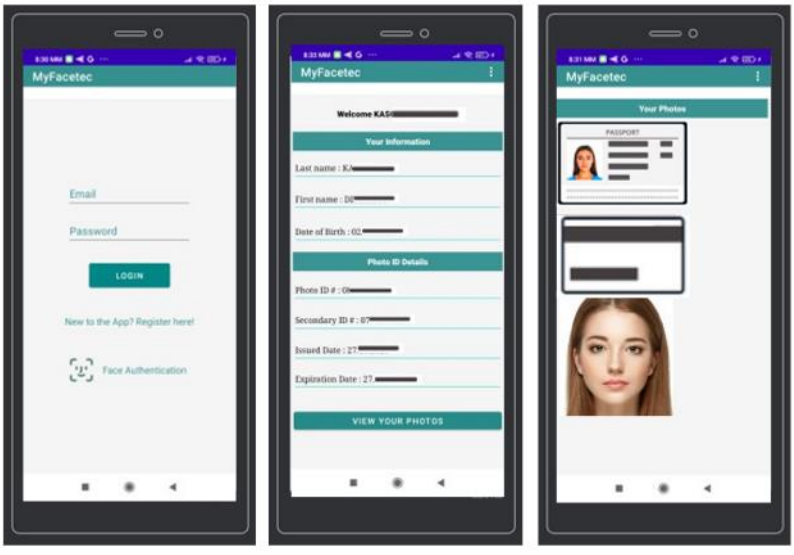
Εικόνα 28. Ροή εφαρμογής (8)

Για να δει ο χρήστης τις φωτογραφίες που έβγαλε αλλά και για να ανέβουν στο storage της Firebase πρέπει να επιλέξει το κουμπί «View & Save Photos».



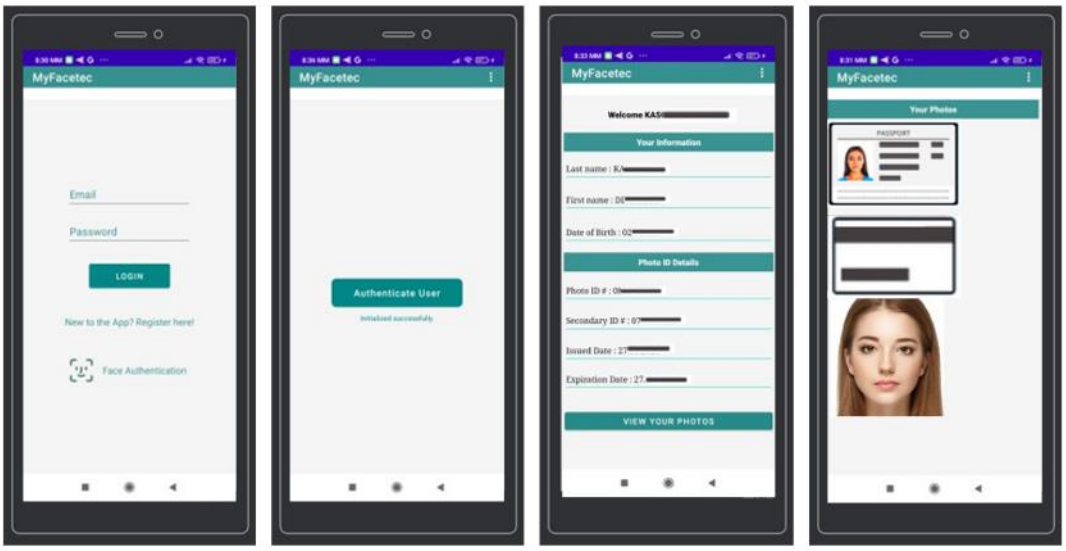
Εικόνα 29. Ροή εφαρμογής (9)

Σε εκ νέου άνοιγμα της εφαρμογής, ο χρήστης μπορεί να πραγματοποιήσει είσοδο στην εφαρμογή με τη διαδικασία Login, εισάγοντας το User Name και το Password που είχε δηλώσει κατά την αρχική εγγραφή με αποτέλεσμα να μπορεί να δει τα στοιχεία του διπλώματος και τις φωτογραφίες του.



Εικόνα 30. Ροή εφαρμογής (10)

Εκτός από τη διαδικασία Login, υπάρχει δυνατότητα για Login με Face Authentication το οποίο ελέγχει αν υπάρχει καταχωρημένο externalDatabaseRefID στη βάση δεδομένων, το οποίο αντιστοιχεί με το 3D FaceMap του χρήστη. Εφόσον υπάρχει μπορεί να δει τα στοιχεία του διπλώματος και τις φωτογραφίες του.



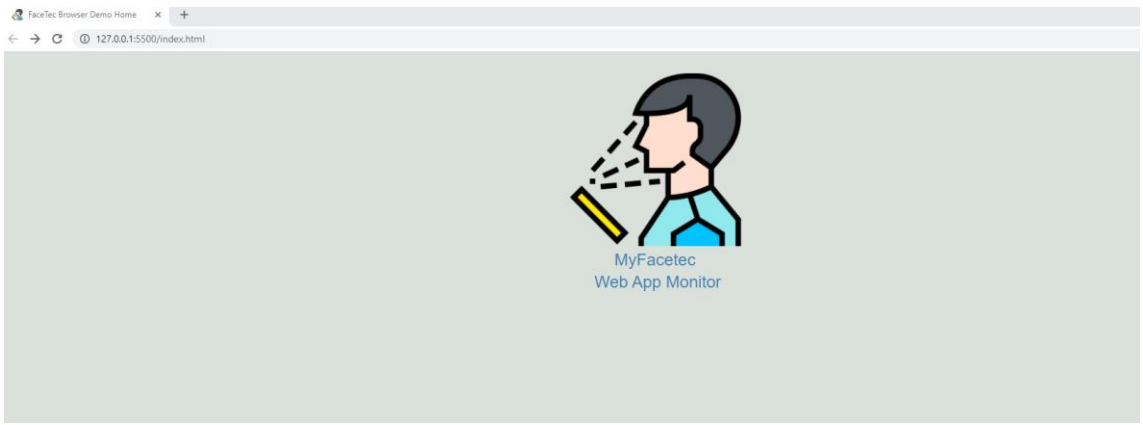
Εικόνα 31. Ροή εφαρμογής (11)

5.1.5 Web Monitor

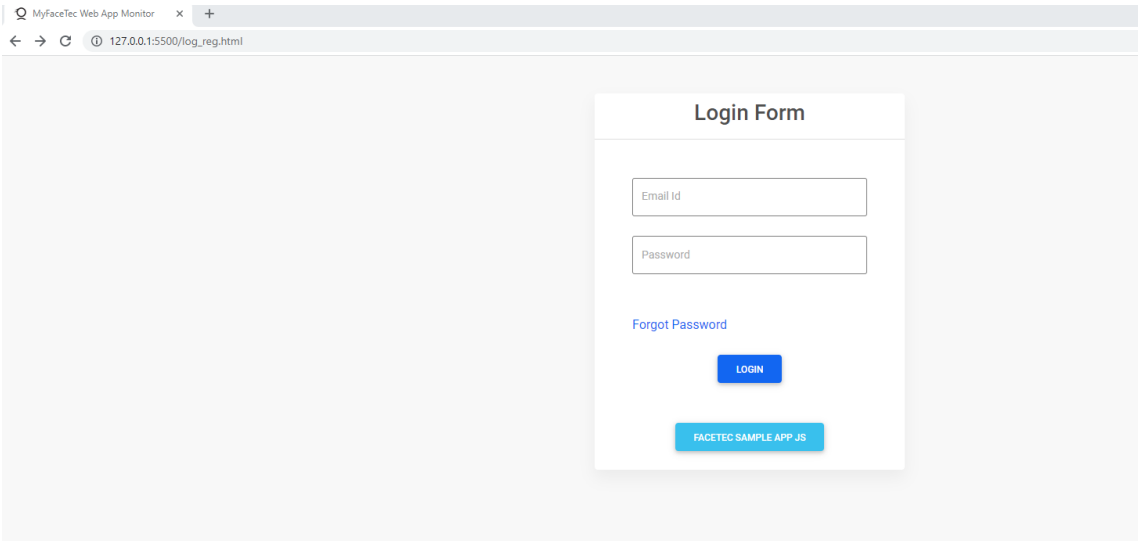
Στα πλαίσια ελέγχου των δεδομένων των καταχωρημένων χρηστών στη Realtime Database, υλοποιήθηκε ένα web application, το οποίο έχει σύνδεση με τη βάση δεδομένων και εμφανίζει στους χρήστες που έχουν κάνει login, τα στοιχεία των χρηστών (χωρίς τις φωτογραφίες τους) που υπάρχουν στη βάση.

Επιπρόσθετα ενσωματώθηκε το web sample app της Facetec ώστε να παρουσιαστούν οι demo διαδικασίες και σε web περιβάλλον.

Επιλέγοντας το λεκτικό “Web App Monitor” ο χρήστης μεταφέρεται στη login form.

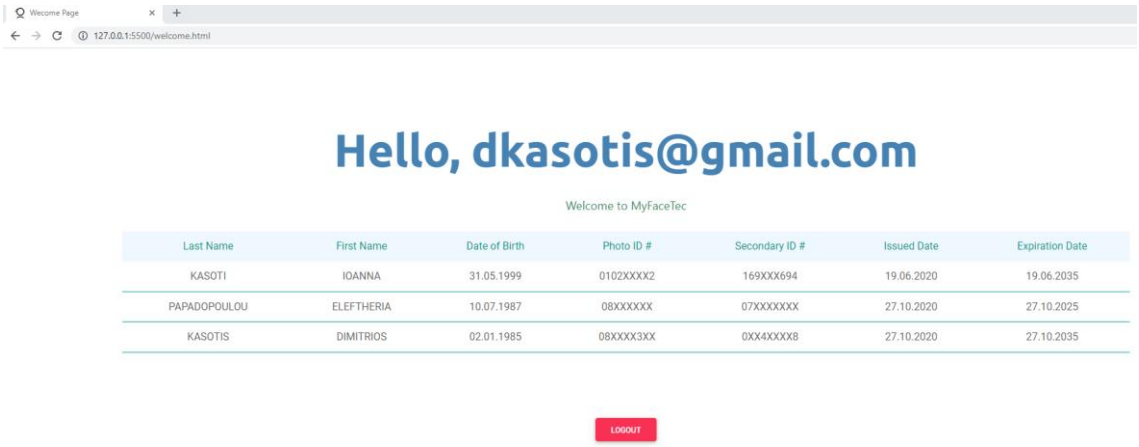


Εικόνα 32. Web App Monitor (1)

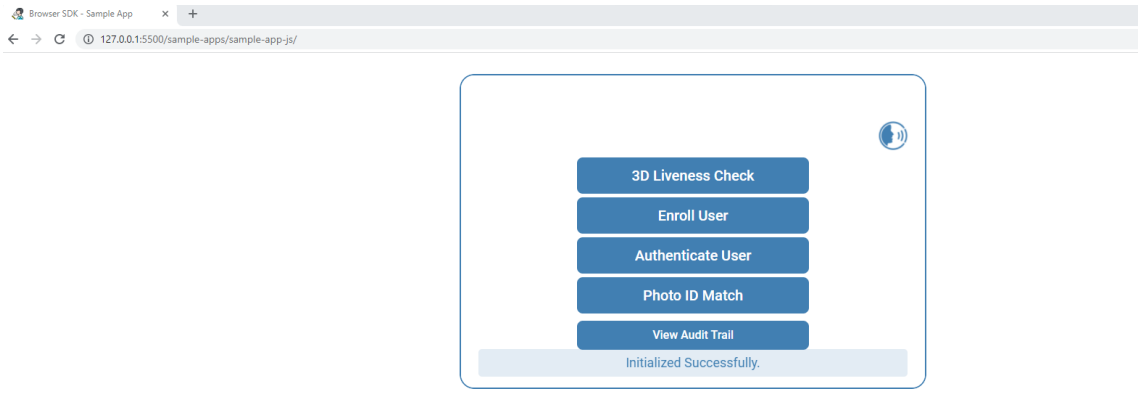


Εικόνα 33. Web App Monitor (2)

Δηλώντας email και password χρήστη που έχει κάνει εγγραφή στην εφαρμογή MyFacetec, μεταφέρεται σε οθόνη που παρουσιάζονται όλα τα δεδομένα χρηστών.

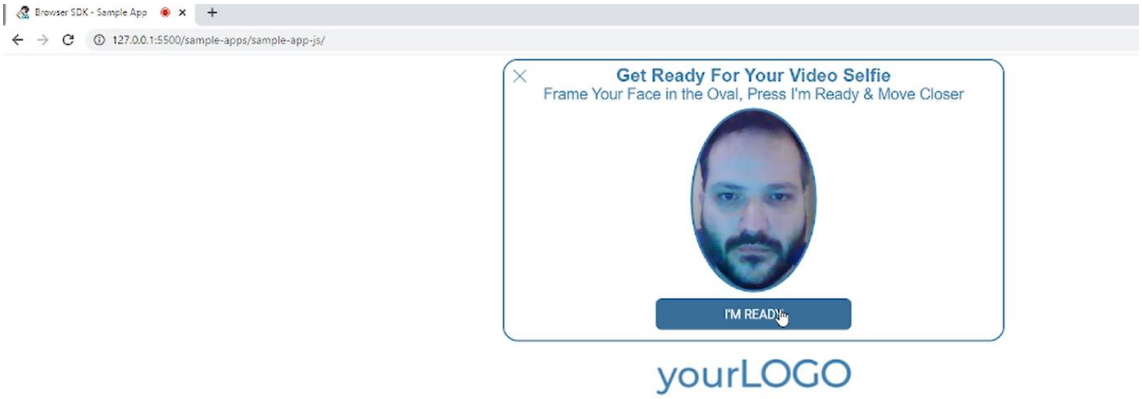


Εικόνα 34. Web App Monitor (3)

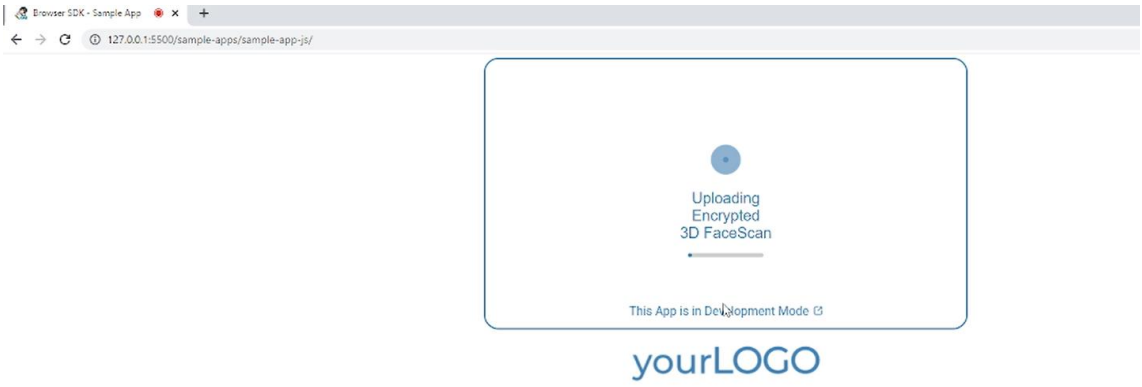


Εικόνα 35. Facetec Sample App JS

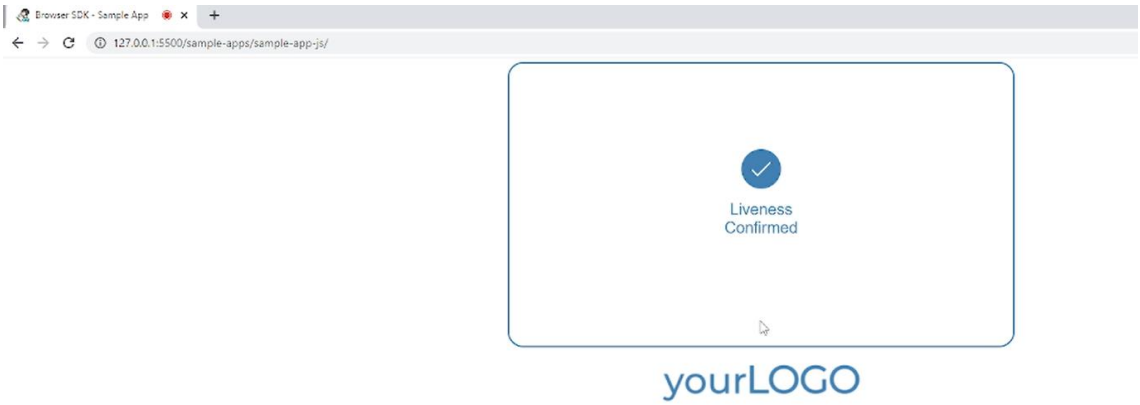
Στο menu που δίνει η FaceTec, ο χρήστης μπορεί να εκτελέσει ταυτοποίηση, να εγγραφεί στο σύστημα, να ελεγχθεί αν είναι πραγματική η εικόνα του (3D liveness) ή να τακτοποιήσει και να εγγράψει στο σύστημα την ταυτότητά του. Παρακάτω παρουσιάζονται ενδεικτικά screenshots ανά επιλογή.



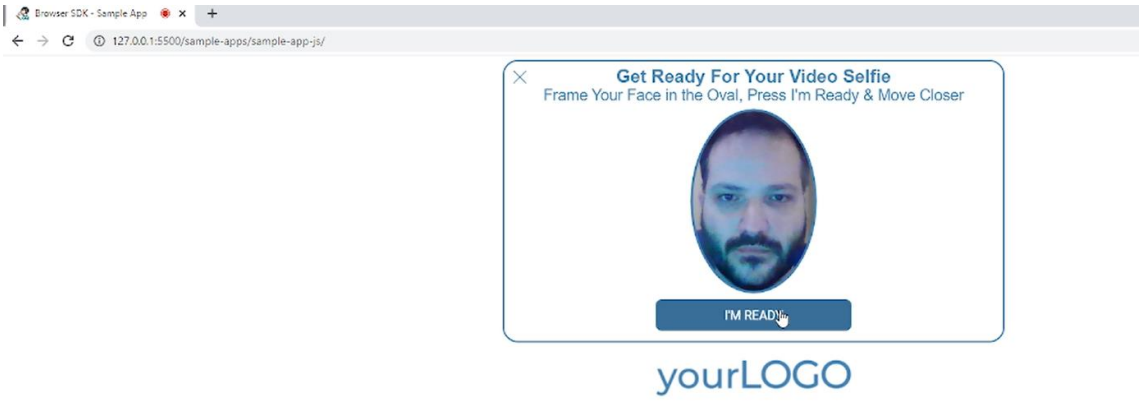
Εικόνα 36. Facetec 3D Liveness Check (1)



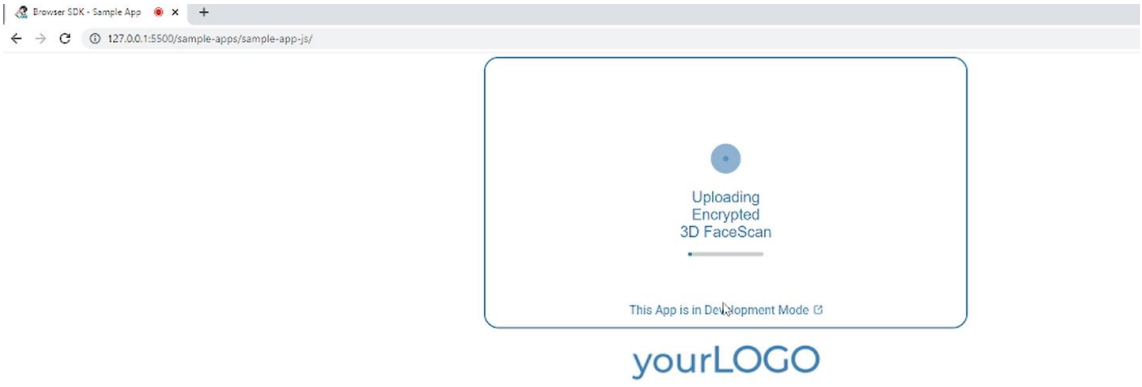
Εικόνα 37. Facetec 3D Liveness Check (2)



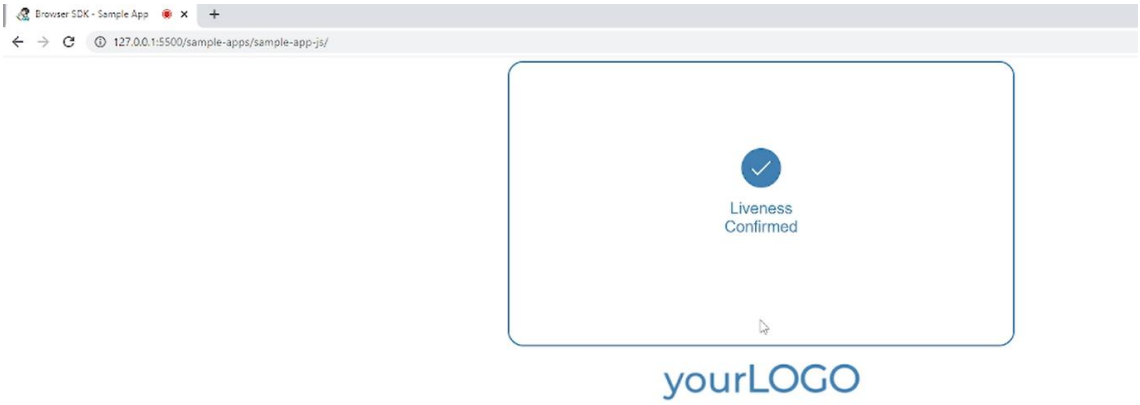
Εικόνα 38. Facetec 3D Liveness Check (3)



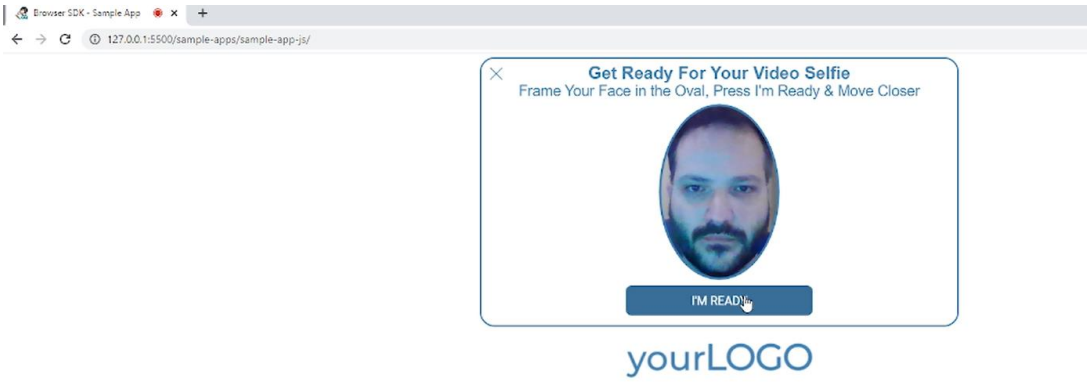
Εικόνα 39. Facetec 3D Enroll User (1)



Εικόνα 40. Facetec 3D Enroll User (2)

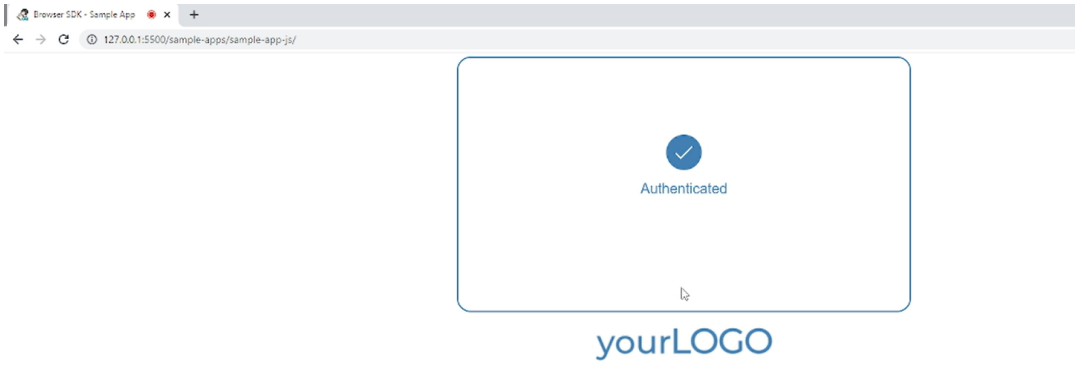


Εικόνα 41. Facetec 3D Enroll User (3)

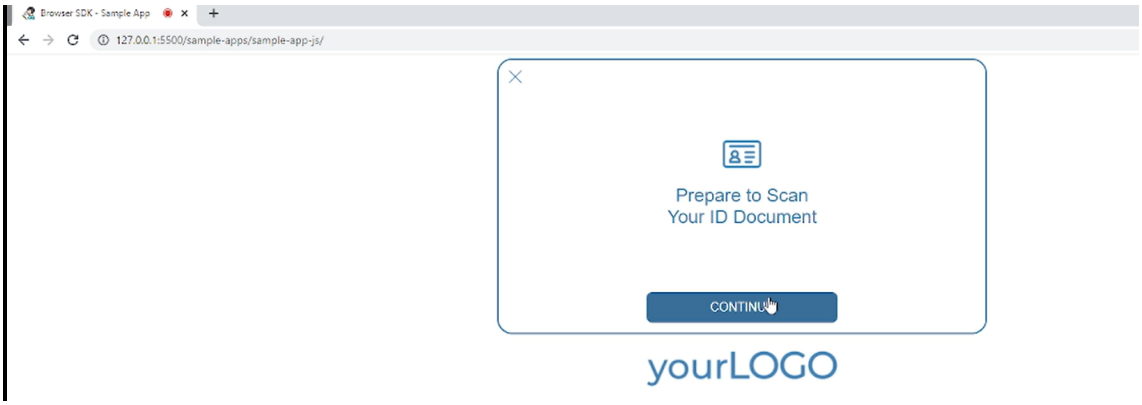


Εικόνα 42. Facetec 3D Photo Id Match (1)

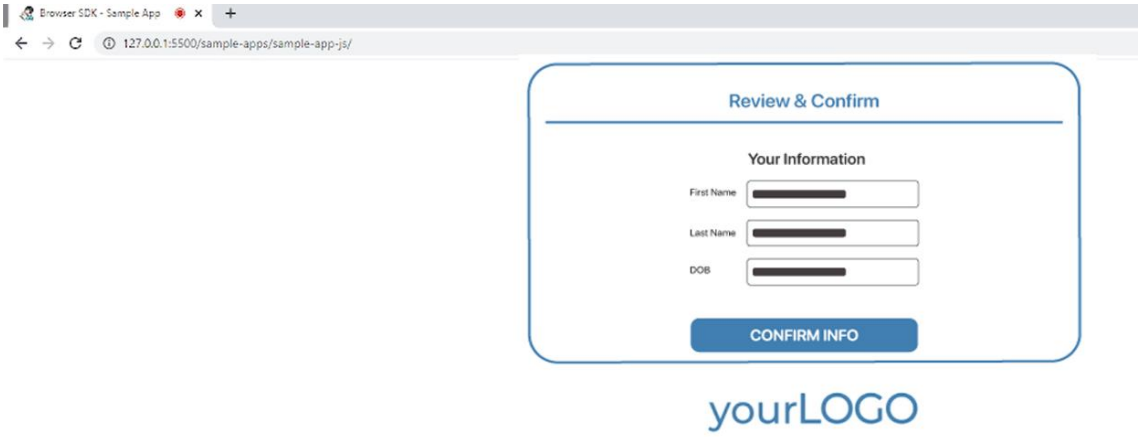
Εικόνα 43. Facetec 3D Photo Id Match (2)



Εικόνα 44. Facetec 3D Photo Id Match (3)



Εικόνα 45. Facetec 3D Photo Id Match (4)



Εικόνα 46. Facetec 3D Photo Id Match (5)

Κεφάλαιο 6°

1. ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφισβήτητα, η τεχνολογία αποτελεί ένα σημαντικό και ταυτόχρονα απαραίτητο εργαλείο στην καθημερινότητα των ανθρώπων. Η εξέλιξη της βοηθάει στην επίλυση θεμάτων όπως η επαλήθευση ταυτότητας μέσω αυθεντικοποίησης προσώπου που πραγματεύεται η μεταπτυχιακή διατριβή.

Στόχος της εργασίας είναι να παρουσιαστεί μια τεχνολογία που αφορά τη βιομετρία η οποία αποτελεί φαινόμενο μεγάλης σημασίας στη σύγχρονη κοινωνία καθότι αποτελεί κλειδί για την εδραίωση της ψηφιακής ταυτότητας, που ενισχύεται από την ανάγκη για συστήματα διαχείρισης ταυτότητας μεγάλης κλίμακας. Η παρούσα διατριβή μπορεί να αποτελέσει την αρχή για την υλοποίηση μίας ολοκληρωμένης εφαρμογής για το κοινό και να παροτρύνει τους προγραμματιστές να προχωρήσουν σε βελτιώσεις όσον αφορά τις λειτουργίες τόσο σε backend όσο και σε frontend επίπεδό.

2. ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

Η υλοποίηση της εφαρμογής έγινε με βάση τις demo λειτουργίες που παρέχει η Facetec. Οπότε συνάπτοντας εμπορική συμφωνία με την εταιρία, παρέχεται πλατφόρμα όπου μπορούν να δημιουργηθούν custom πρότυπα σε σχέση με τις ταυτότητες που γίνονται αποδεκτές. Αυτό θα έχει ως συνέπεια η εφαρμογή να μπορεί να κάνει χάριν παραδείγματος, έλεγχο φοιτητικής ή όποιου άλλου είδους ταυτότητας επιθυμεί.

Επιπρόσθετα όλες οι συνεδρίες που σε demo περιβάλλον αποθηκεύονται σε server της facetec, δύναται να αποθηκεύονται σε custom server με βάση δεδομένων (MongoDb) όπου εκεί μπορεί να υλοποιηθεί οτιδήποτε ανάλογα τις ανάγκες που υπάρχουν. Για παράδειγμα θα μπορούσαν να αντληθούν επιπρόσθετα στοιχεία από τις ταυτότητες που είναι συμβατές και να αποθηκεύονται στη βάση δεδομένων.

Ακόμη θα μπορούσε να υλοποιηθεί ένα custom REST API όπου θα ήταν υπεύθυνο για τη συλλογή όλων των πληροφοριών από τις συνεδρίες, το οποίο θα ήταν συμβατό με διαφορετικά περιβάλλοντα. Για παράδειγμα εκτός του Android, θα μπορούσε να χρησιμοποιηθεί και Web πλαφόρμα, κάτι το οποίο θα έδινε μία λειτουργικότητα όπου θα μπορούσε να τη χρησιμοποιήσει ο οποιοσδήποτε κάνει εγγραφή στην υπηρεσία από οπουδήποτε με την προϋπόθεση ότι υπάρχει σύνδεση internet.

Τέλος θα μπορούσε να υφίσταται τοπική βάση SQLite στο κινητό Android, όπου θα αποθηκεύονται τα στοιχεία των συνεδριών σε περίπτωση που δεν υπάρχει διαθέσιμο Wi-Fi ή 4G/5G δίκτυο. Σε περίπτωση που υπάρχει διαθεσιμότητα δικτύου, να γίνεται συγχρονισμός με την online βάση.

Βιβλιογραφία

[1] Michael Fairhurst, 2019, Τίτλος Biometrics: A Very Short Introduction (Very Short Introductions), Oxford University Press.

[2] Sébastien Marcel, Mark S. Nixon, Julian Fierrez, Nicholas Evans (eds.), 2019, Τίτλος: Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, Springer.

[3] Neil Smyth, 2017, Τίτλος: Firebase Essentials - Android Edition, Payload Media, Inc.

[4] Ashok Kumar S, 2018, Τίτλος: Mastering Firebase for Android Development: Build real-time, scalable, and cloud-enabled Android apps with Firebase, Packt Publishing.

[5] Neil Smyth, 2021, Τίτλος: Android Studio 4.2 Development Essentials - Java Edition: Developing Android Apps Using Android Studio 4.2, Java and Android Jetpack, eBookFrenzy.

[6] Ian F. Darwin, 2017, Τίτλος: Android Cookbook: Problems and Solutions for Android Developers, O'Reilly Media.

[7] FaceTec Competitors, URL: https://sourceforge.net/software/product/FaceTec/alternatives , προσπελάστηκε Ιανούριο 2022.

[8] Liveness detection solutions, a comparison, URL: https://blog.humanode.io/liveness-detection-solutions-a-comparison/ , προσπελάστηκε Ιανούριο 2022.

[9] What is biometrics?, URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics , προσπελάστηκε Ιανούριο 2022.

[10] How to Create Use Case Description for Your Business Analysis Report, URL: https://www.dummies.com/business/business-strategy/how-to-create-use-case-description-for-your-business-analysis-report/ , προσπελάστηκε Ιανούριο 2022.

[11] Laurence Lars Svekis (Author), Maaike van Putten (Author), Rob Percival (Author), 2021, Τίτλος: JavaScript from Beginner to Professional: Learn JavaScript quickly by building fun, interactive and dynamic web apps, games, Packt Publishing.

[12] Gunnar Overgaard, Karin Palmkvist, 2004, Τίτλος: Use cases patterns and blueprints, Addison-Wesley Professional.