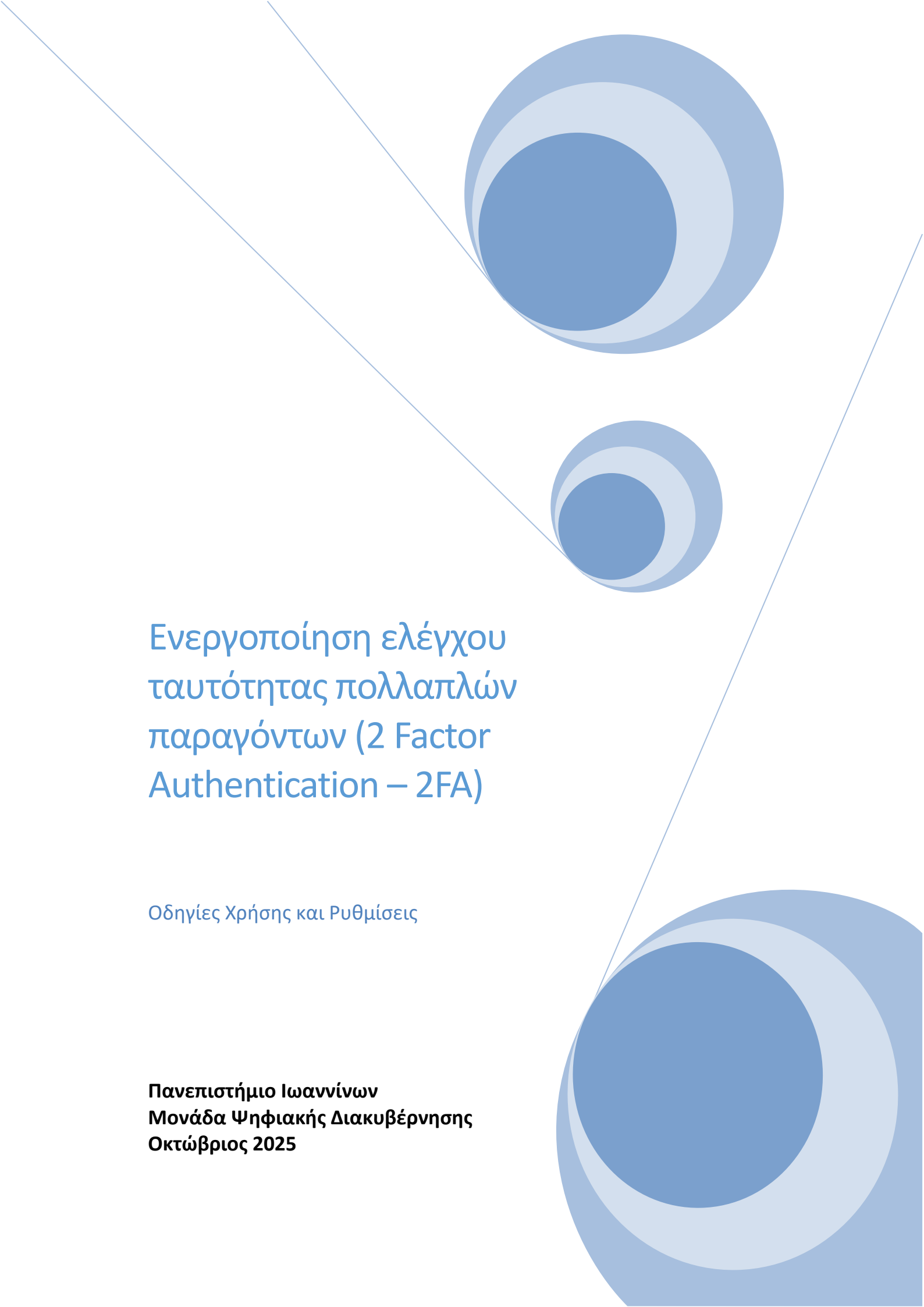




# Ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων (2 Factor Authentication – 2FA)

Οδηγίες Χρήσης και Ρυθμίσεις

**Πανεπιστήμιο Ιωαννίνων**  
**Μονάδα Ψηφιακής Διακυβέρνησης**  
**Οκτώβριος 2025**

# Ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων (2 Factor Authentication -2FA)

Ο «έλεγχος ταυτότητας πολλαπλών παραγόντων/2 Factor Authentication – 2FA» είναι ένα επιπλέον επίπεδο ασφάλειας που χρησιμοποιείται για να εισέλθουμε σε μια υπηρεσία και συνδέεται με τον λογαριασμό που διατηρούμε σε αυτή. Αρχικά, θα εισάγουμε το όνομα χρήστη και τον κωδικό πρόσβασης και στη συνέχεια, αντί να αποκτήσουμε αμέσως πρόσβαση, θα πρέπει να εισάγουμε ένα επιπλέον κωδικό (OTP) που παράγει μια εγκατεστημένη εφαρμογή στο κινητό μας τηλέφωνο (smartphone). Σε πολλές υπηρεσίες οι οποίες διαχειρίζονται δεδομένα προσωπικού χαρακτήρα (π.χ τράπεζες, πάροχοι υπηρεσιών εμπιστοσύνης) είναι υποχρεωτική η χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων.

Στις οδηγίες που ακολουθούν περιγράφεται η διαδικασία ενεργοποίησης ελέγχου ταυτότητας πολλαπλών παραγόντων/2 Factor Authentication – 2FA, με χρήση 2 προτεινόμενων εφαρμογών παραγωγής κωδικών One -Time Password (OTP).

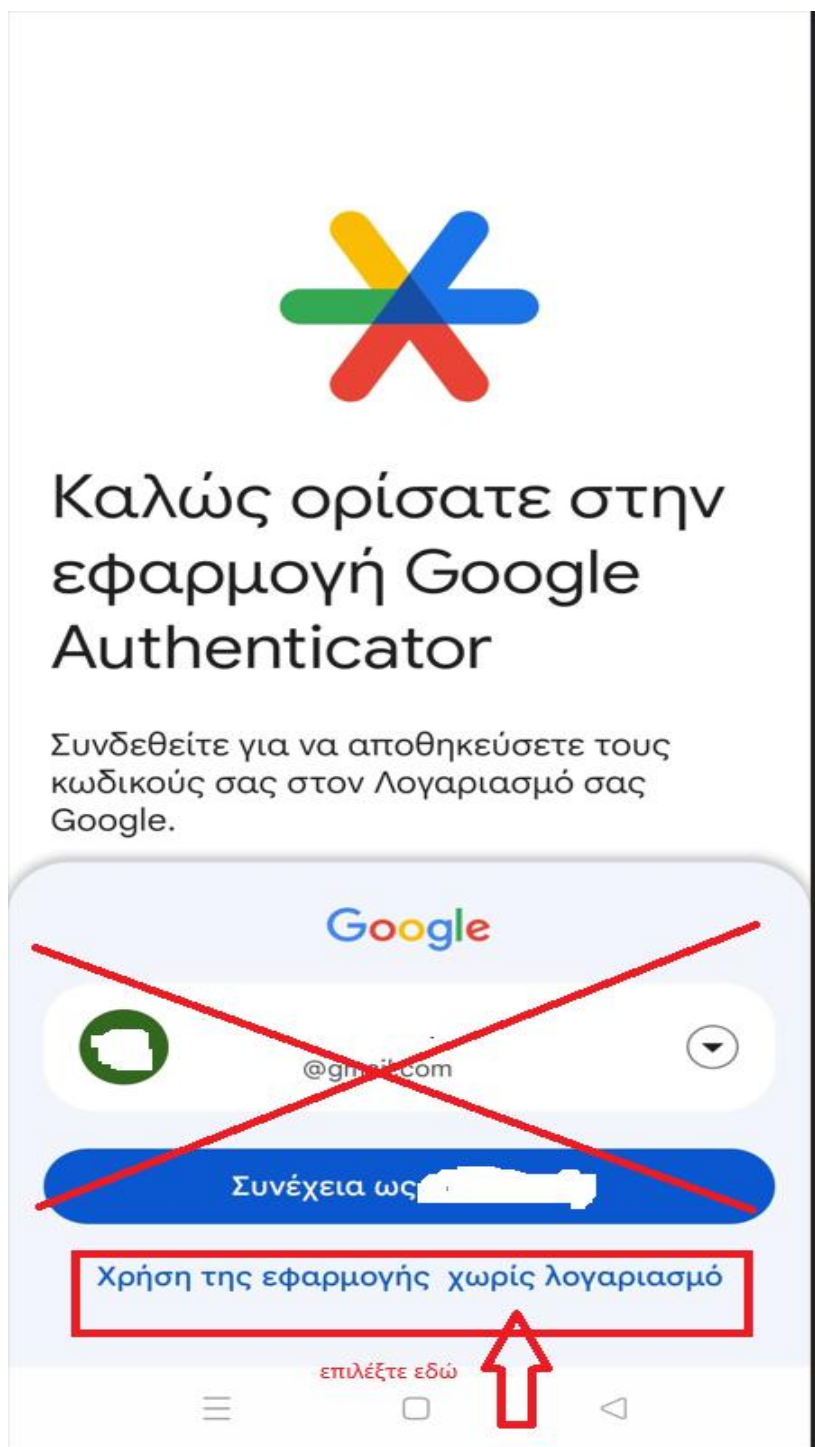
**Microsoft Authenticator** ([Google Play](#) / [Apple App Store](#))

**Google Authenticator** ([Google Play](#) / [Apple App Store](#))

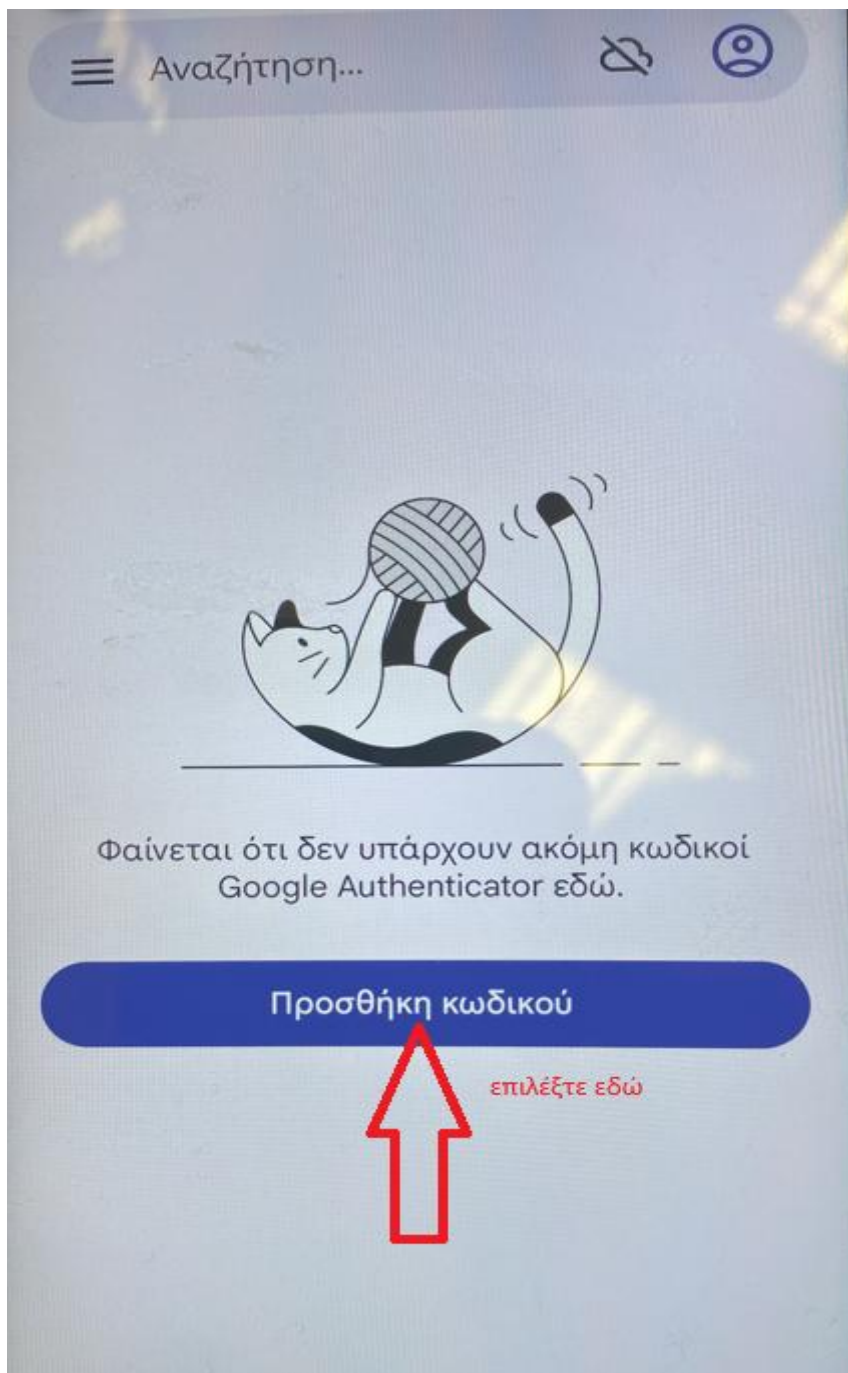
Από το Play Store ή App Store της κινητής συσκευής, ο χρήστης αναζητά έναν από τους δύο προαναφερθέντες προτεινόμενους επαληθευτές (Google Authenticator ή Microsoft Authenticator). Τον εγκαθιστά στην κινητή συσκευή.

Στη συνέχεια, ο χρήστης ανοίγει την εφαρμογή **Google Authenticator** ή **Microsoft Authenticator** που έχει εγκαταστήσει στη συσκευή του και επιλέγει **προσθήκη λογαριασμού**.

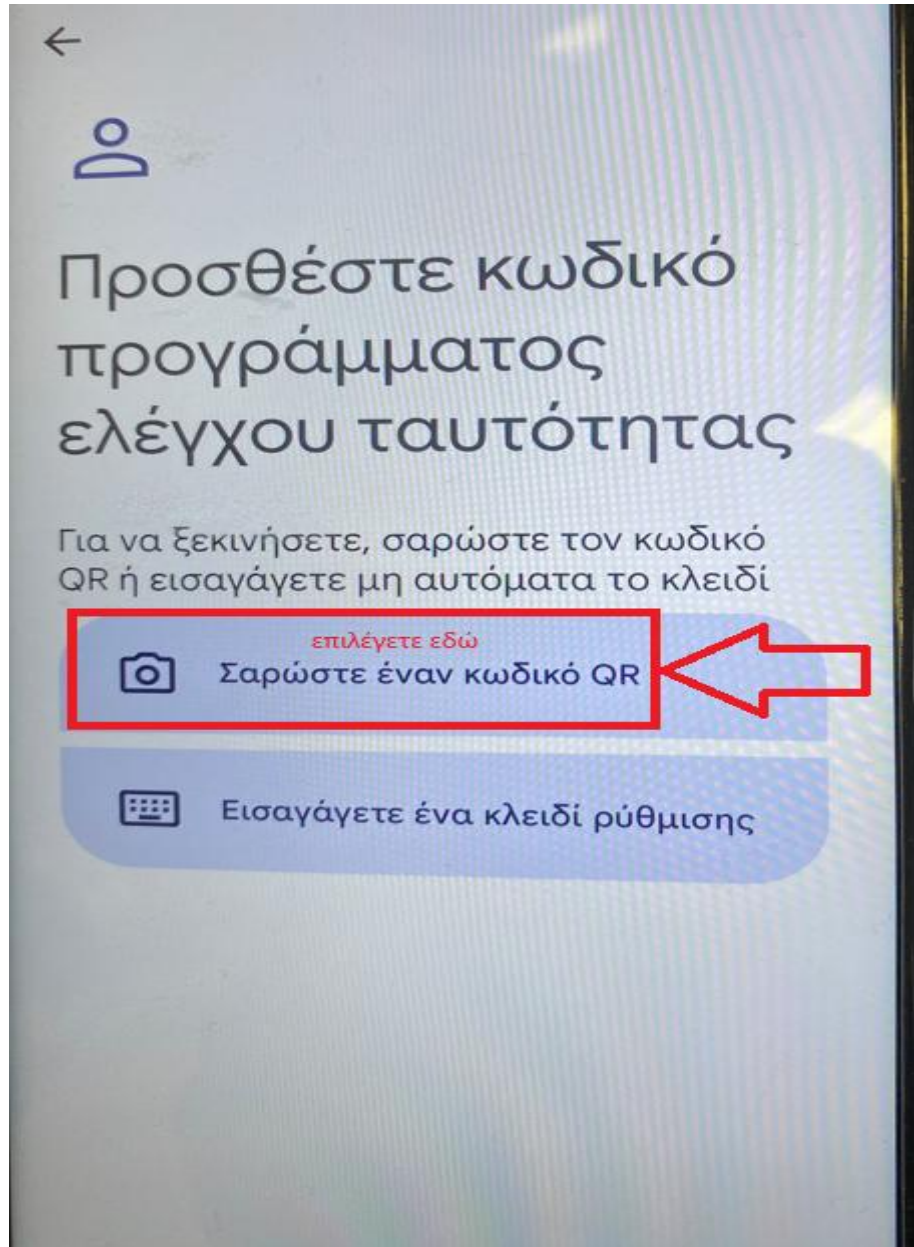
2. Έπειτα ο χρήστης επιλέγει «Χρήση της εφαρμογής χωρίς λογαριασμό» όπως φαίνεται στην ακόλουθη εικόνα



3. Στο επόμενο βήμα όπως φαίνεται στην επόμενη εικόνα ο χρήστης επιλέγει «Προσθήκη κωδικού»



3. Στο επόμενο βήμα ο χρήστης επιλέγει «**Σαρώστε ένα QR Code**» το οποίο εμφανίζεται στην ιστοσελίδα της υπηρεσίας που χρειάζεται ενεργοποίηση. **Προσοχή**, ίσως να ζητηθεί και πρέπει να δοθεί έγκριση χρήσης της κάμερας της συσκευής από την εφαρμογή.



4. Ανοίγει η κάμερα της κινητής συσκευής και στη συνέχεια ο χρήστης πρέπει να γυρίσει την κάμερα της συσκευής του προς την οθόνη του υπολογιστή και να σκανάρει το QR code που φαίνεται μέσα στο τετράγωνο ώστε να το αντιγράψει μέσα στη συσκευή του.



5. Αυτόματα προστίθεται ο λογαριασμός και ξεκινάει η παραγωγή κωδικών OTP (One Time Password) που ανανεώνονται ανά 30 δευτερόλεπτα.

