

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

Οδηγίες Χρήσης και Ρυθμίσεις

Πανεπιστήμιο Ιωαννίνων
Διεύθυνση Μηχανοργάνωσης & Δικτύων
Φεβρουάριος 2021

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.

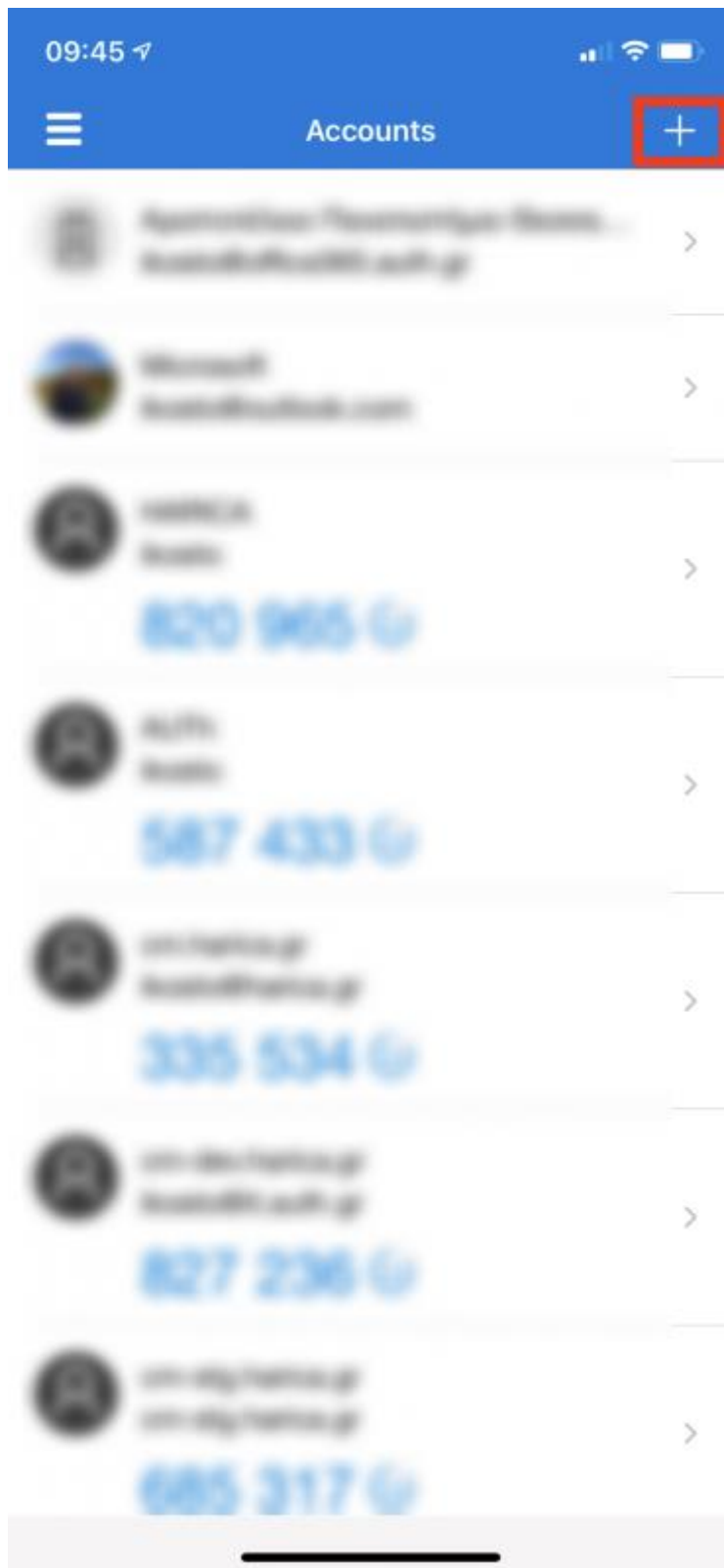
Στις οδηγίες που ακολουθούν περιγράφεται η διαδικασία ενεργοποίησης ελέγχου ταυτότητας πολλαπλών παραγόντων/2 Factor Authentication – 2FA, με χρήση 2 προτεινόμενων εφαρμογών παραγωγής κωδικών One-Time Password (OTP).

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

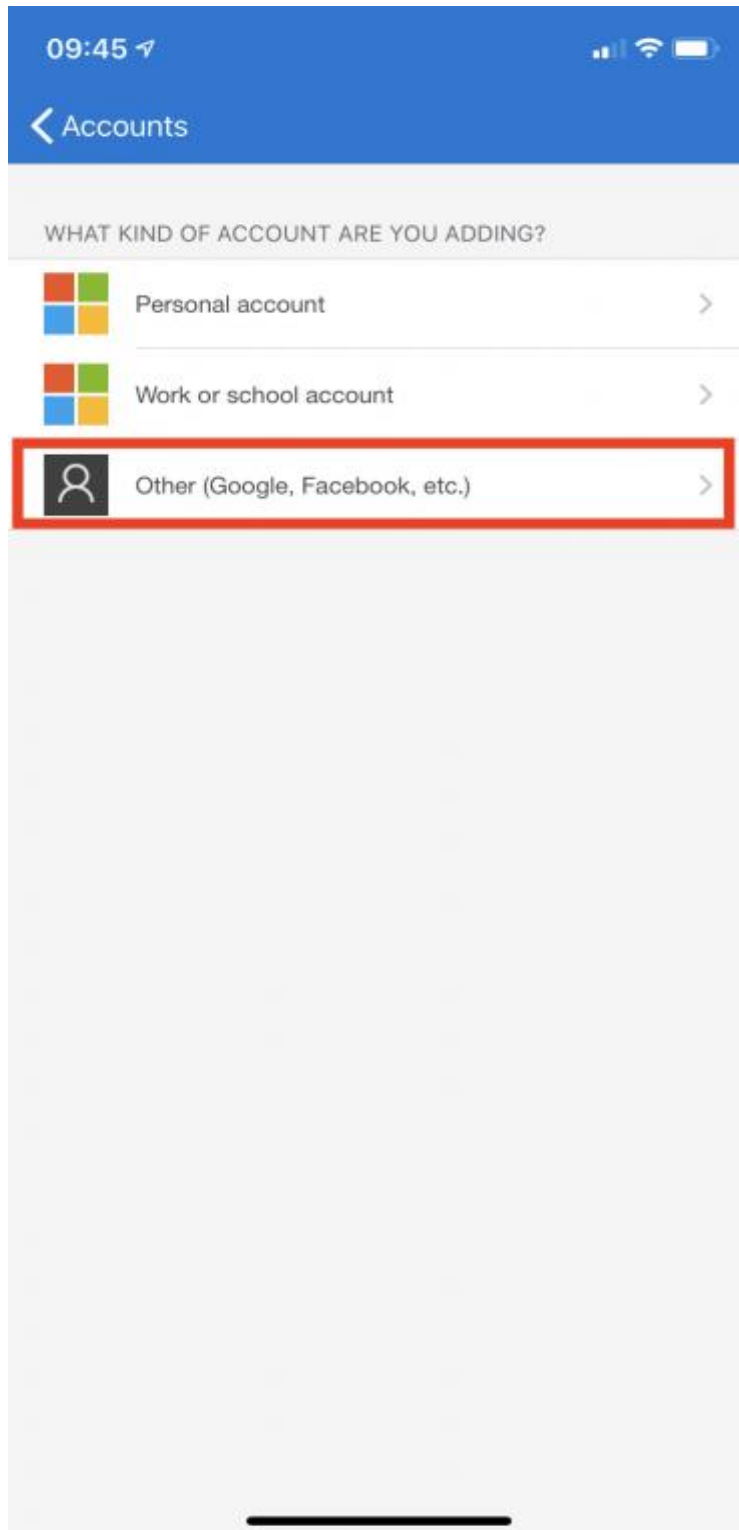
Google Authenticator ([Google Play](#) / [Apple App Store](#))

Microsoft Authenticator

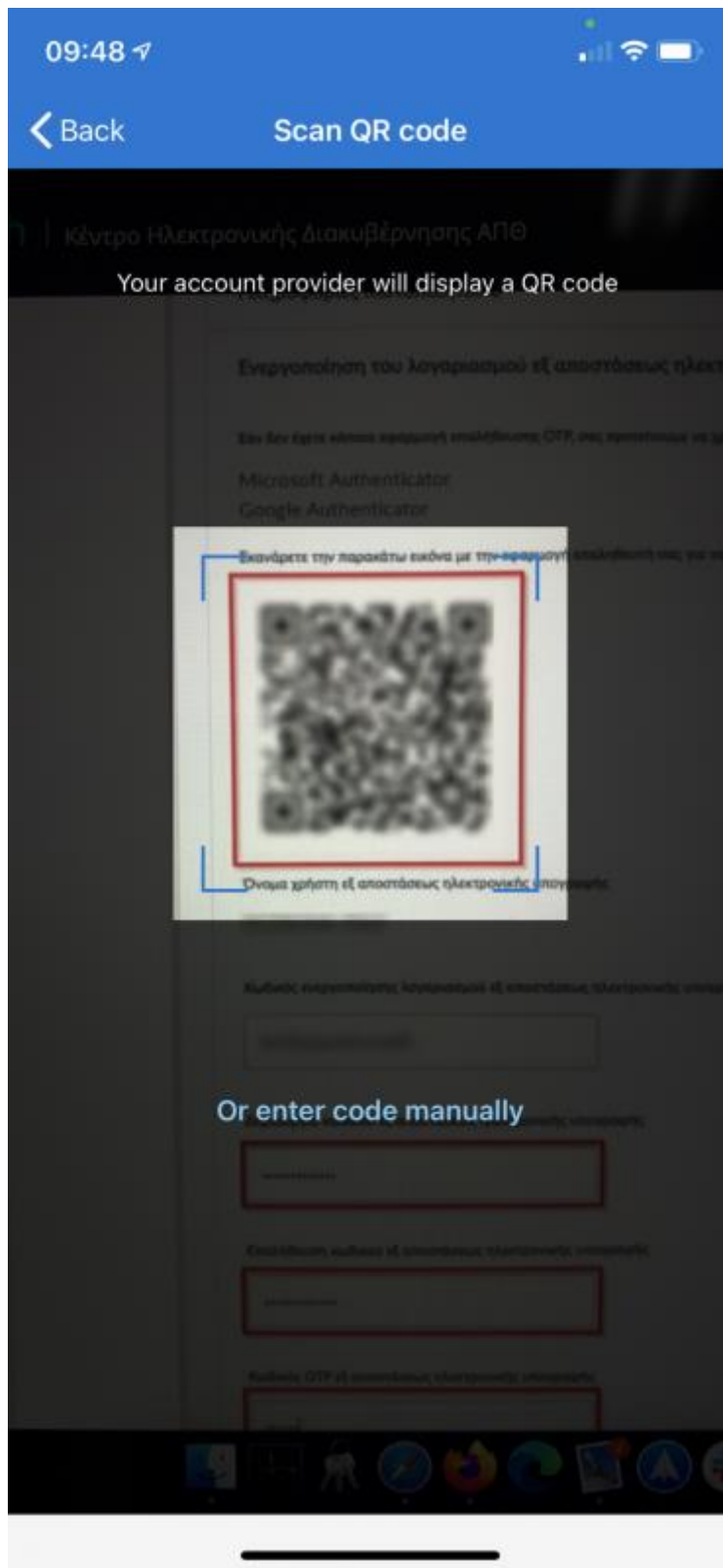
1. Ανοίγουμε την εφαρμογή **Microsoft Authenticator** που έχουμε εγκαταστήσει στη συσκευή μας και επιλέγουμε **προσθήκη λογαριασμού**.



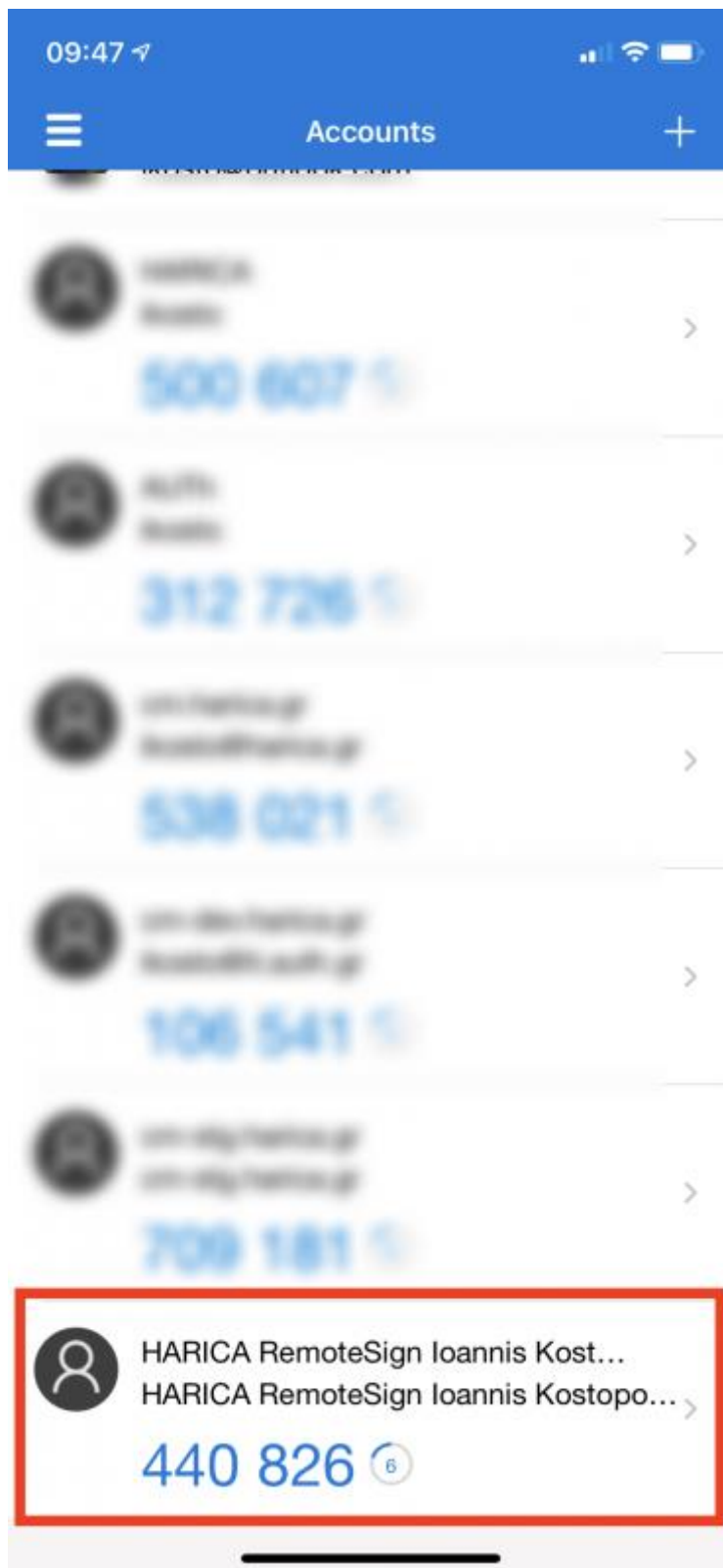
2. Επιλέγουμε **Other**.



3. Ανοίγει η κάμερα της συσκευής και σκανάρουμε το QR Code που εμφανίζεται στην ιστοσελίδα της υπηρεσίας που θέλουμε να ενεργοποιήσουμε. **Προσοχή**, μπορεί να μας ζητηθεί και πρέπει να δώσουμε έγκριση χρήσης της κάμερας της συσκευής από την εφαρμογή.

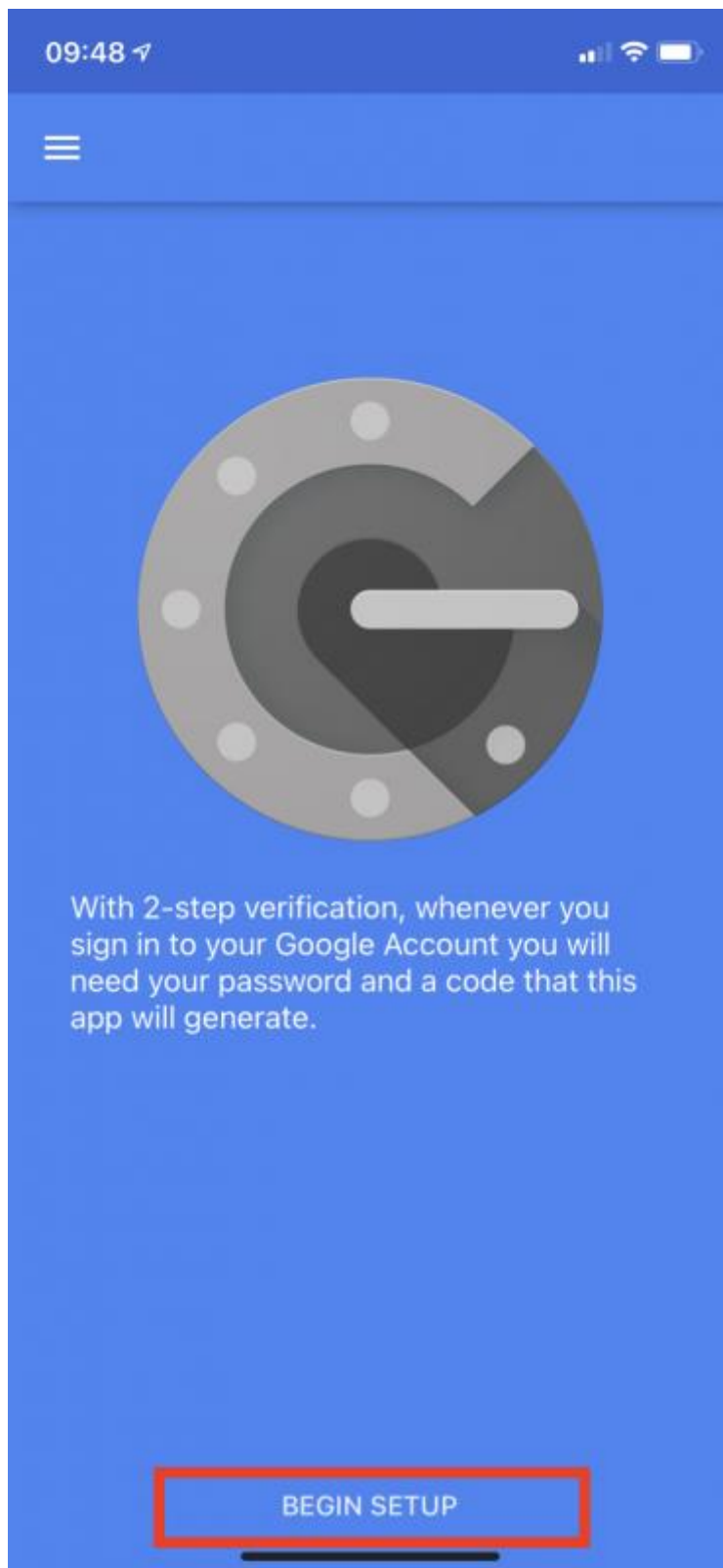


4. Αυτόματα προστίθεται ο λογαριασμός και ξεκινάει η παραγωγή κωδικών OTP που ανανεώνονται ανά 30 δευτερόλεπτα.

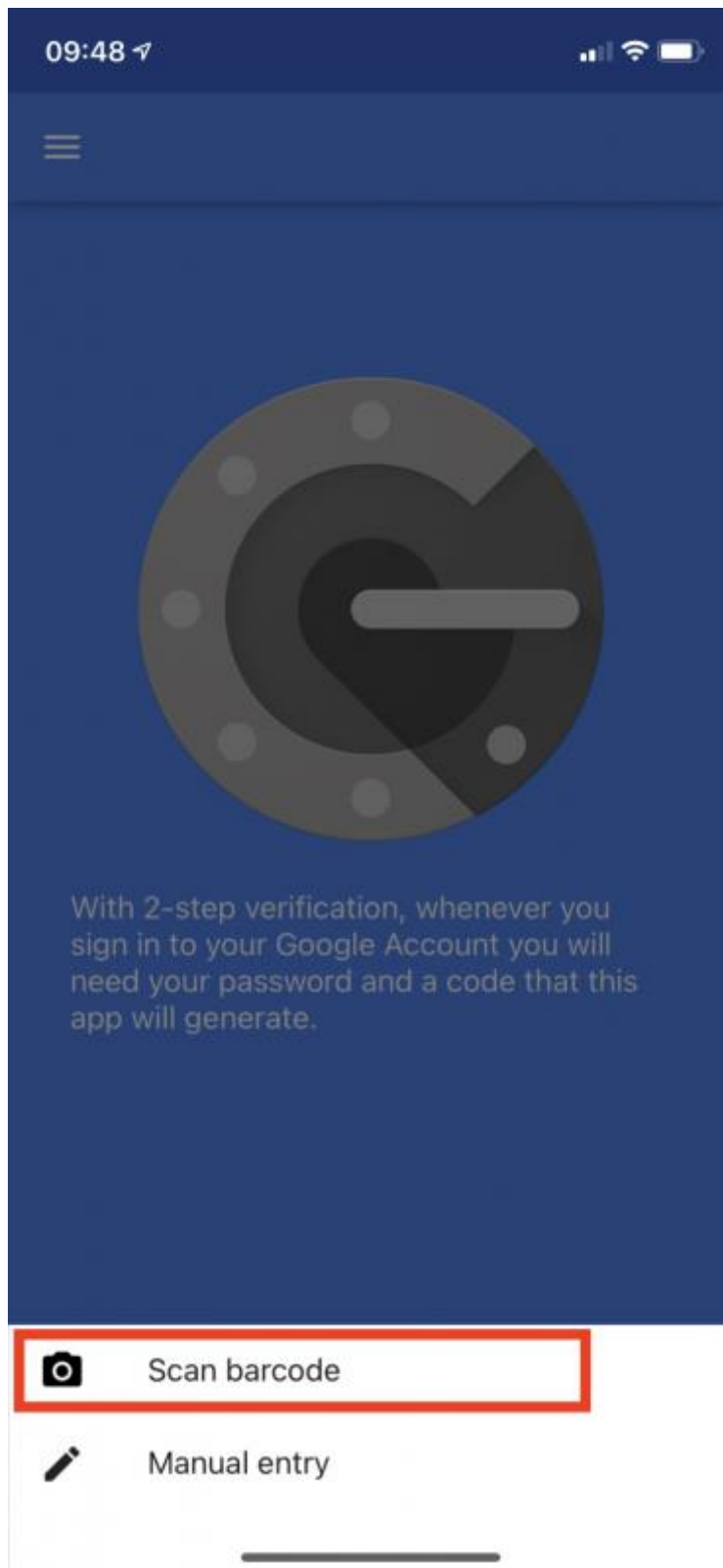


Google Authenticator

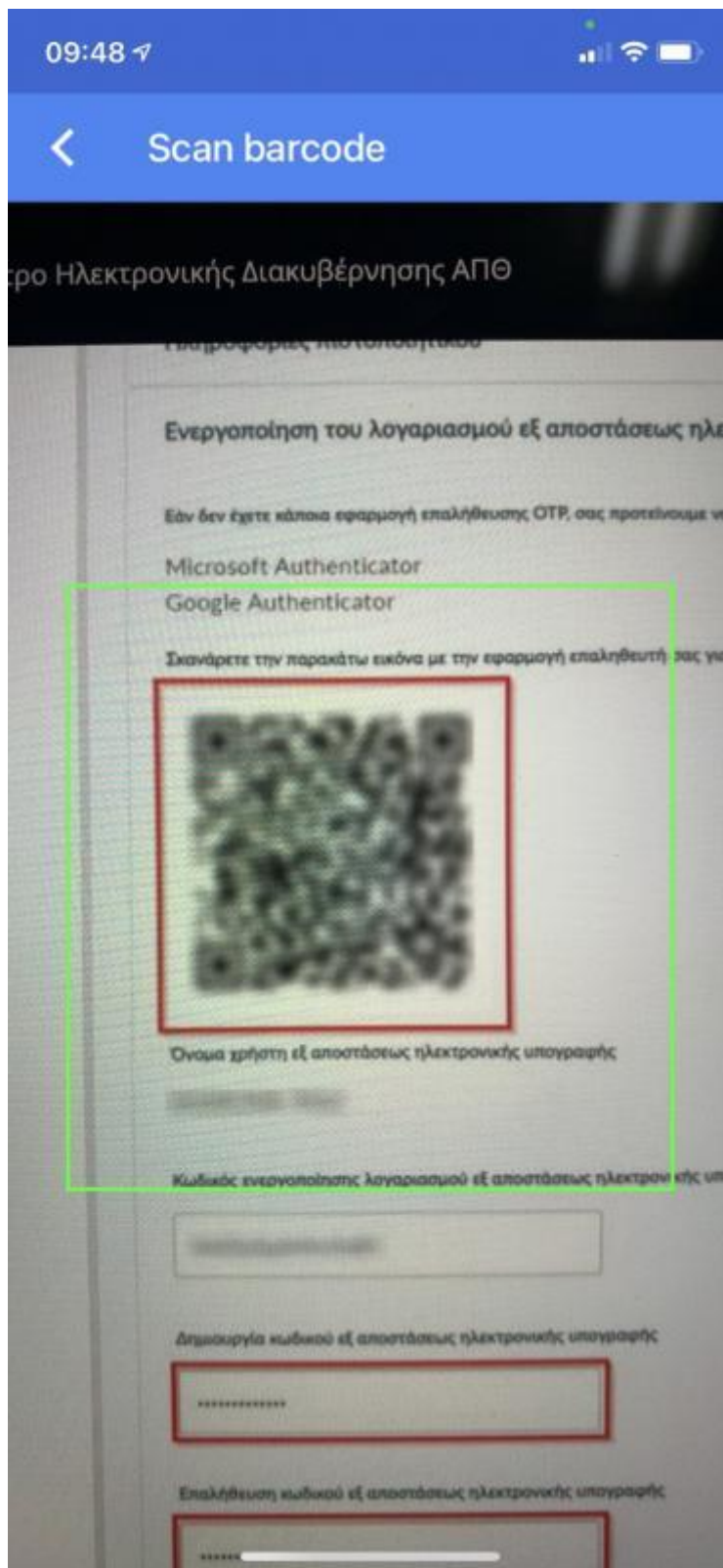
1. Ανοίγουμε την εφαρμογή Google Authenticator που έχουμε εγκαταστήσει στη συσκευή μας και επιλέγουμε **BEGIN SETUP**.



2. Επιλέγουμε **Scan barcode**.



3. Ανοίγει η κάμερα της συσκευής και σκανάρουμε το QR Code που εμφανίζεται στην ιστοσελίδα της υπηρεσίας που θέλουμε να ενεργοποιήσουμε.
Προσοχή, μπορεί να μας ζητηθεί και πρέπει να δώσουμε έγκριση χρήσης της κάμερας της συσκευής από την εφαρμογή.



4. Αυτόματα προστίθεται ο λογαριασμός και ξεκινάει η παραγωγή κωδικών OTP που ανανεώνονται ανά 30 δευτερόλεπτα.

09:54



Authenticator



731 072

HARICA RemoteSign

