



## Οδηγός Χρήσης Δεύτερου Παράγοντα Ταυτοποίησης (2FA) Authentik & Google Authenticator σε Android

---

### 1. Εισαγωγή

#### Σκοπός

Αυτός ο οδηγός εξηγεί πώς να ρυθμίσετε και να χρησιμοποιείτε τον **Δεύτερο Παράγοντα Ταυτοποίησης (2FA)** για να συνδέεστε με ασφάλεια στα πληροφοριακά συστήματα του Πανεπιστημίου Πελοποννήσου.

---

#### Τι είναι ο Δεύτερος Παράγοντας Ταυτοποίησης (2FA);

Όταν συνδέεστε σε έναν λογαριασμό, συνήθως χρησιμοποιείτε μόνο έναν κωδικό πρόσβασης. Αυτό σημαίνει ότι αν κάποιος μάθει τον κωδικό σας, μπορεί να μπει στον λογαριασμό σας.

Ο **Δεύτερος Παράγοντας Ταυτοποίησης** προσθέτει ένα επιπλέον βήμα ασφαλείας: εκτός από τον κωδικό πρόσβασής σας, χρειάζεστε και έναν **μοναδικό, προσωρινό κωδικό** που παράγεται στο κινητό σας τηλέφωνο.

#### Παράδειγμα από την καθημερινή ζωή:

Σκεφτείτε το σαν ένα ATM: χρειάζεστε και την κάρτα σας (κωδικός πρόσβασης) και το PIN σας (δεύτερος παράγοντας). Ακόμα και αν κάποιος βρει την κάρτα σας, δεν μπορεί να κάνει ανάληψη χωρίς το PIN.

---

#### Τι είναι το Authentik;

Το **Authentik** είναι η πλατφόρμα διαχείρισης ταυτότητας που χρησιμοποιεί το Πανεπιστήμιο Πελοποννήσου. Μέσω του Authentik συνδέεστε σε επιλεγμένες εφαρμογές και τα πληροφοριακά συστήματα με έναν ενιαίο λογαριασμό.

---



### Τι είναι το Google Authenticator;

Το **Google Authenticator** είναι μια δωρεάν εφαρμογή για κινητό τηλέφωνο. Παράγει αυτόματα τον προσωρινό κωδικό ασφαλείας (OTP) που χρειάζεστε για τη σύνδεση.

---

### Τι είναι ο κωδικός OTP;

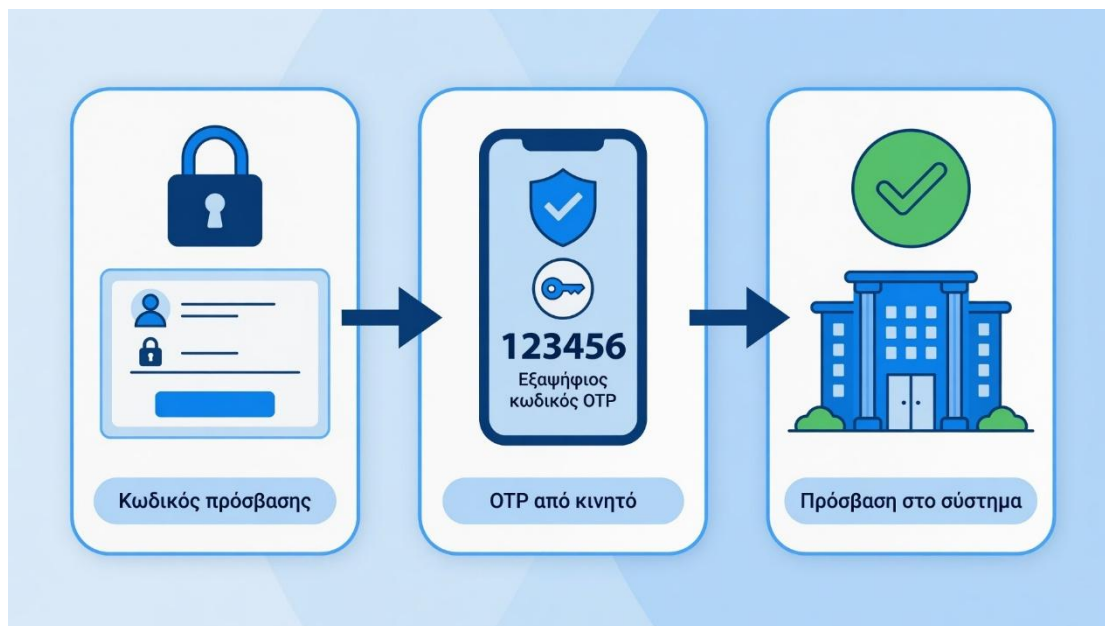
Το **OTP** (One-Time Password, δηλαδή «Κωδικός Μίας Χρήσης») είναι ένας **εξαψήφιος αριθμός** που:

- Παράγεται αυτόματα από το Google Authenticator.
  - Αλλάζει κάθε **30 δευτερόλεπτα**.
  - Είναι έγκυρος μόνο μία φορά.
  - **Δεν πρέπει ποτέ να κοινοποιείται** σε κανέναν.
- 

**Σημείωση:** Ορισμένες εικόνες που χρησιμοποιούνται στον παρόντα οδηγό είναι ενδεικτικές και έχουν δημιουργηθεί με τη βοήθεια τεχνητής νοημοσύνης. Ενδέχεται να μην απεικονίζουν πιστά την πραγματική εμφάνιση των εφαρμογών, αλλά αποσκοπούν αποκλειστικά στην υποστήριξη της κατανόησης των βημάτων εγκατάστασης.

### Πώς λειτουργεί το 2FA

Διάγραμμα ροής σύνδεσης με 2FA



*Εικόνα 1 Η διαδικασία σύνδεσης με Δεύτερο Παράγοντα Ταυτοποίησης (2FA) απαιτεί δύο βήματα: τον κωδικό πρόσβασης και τον προσωρινό κωδικό OTP.*

Διάγραμμα που απεικονίζει τρία διαδοχικά βήματα:

1. Χρήστης εισάγει όνομα χρήστη και κωδικό πρόσβασης στην οθόνη σύνδεσης.
2. Το σύστημα ζητά τον κωδικό OTP και ο χρήστης ανοίγει το Google Authenticator στο κινητό του.
3. Ο χρήστης εισάγει τον OTP και αποκτά πρόσβαση στο σύστημα.

## 2. Προαπαιτούμενα

Πριν ξεκινήσετε, βεβαιωθείτε ότι διαθέτετε τα εξής:

1. **Συσκευή Android** (smartphone ή tablet) με Android 5.0 ή νεότερη έκδοση.
2. **Σύνδεση στο Internet** (Wi-Fi ή κινητά δεδομένα) για την εγκατάσταση της εφαρμογής.
3. **Πρόσβαση στο QR Code** που εμφανίζει η πλατφόρμα Authentik κατά τη ρύθμιση.

**Σημείωση:** Το Internet χρειάζεται μόνο για την εγκατάσταση της εφαρμογής. Μετά την εγκατάσταση, ο κωδικός OTP παράγεται χωρίς σύνδεση στο Internet.



## Απαιτούμενη συσκευή

Συσκευή Android με σύνδεση στο Internet



*Εικόνα 2: Χρειάζεστε συσκευή Android με σύνδεση στο Internet για την εγκατάσταση του Google Authenticator.*

Εικόνα smartphone Android που εμφανίζει εικονίδιο Wi-Fi ή σήματος κινητής τηλεφωνίας στη γραμμή κατάστασης, με ένα κλειδωμένο λουκέτο για να υποδηλώνεται η ασφάλεια.

### 3. Εγκατάσταση Google Authenticator

#### Σκοπός

Εγκατάσταση της εφαρμογής Google Authenticator στη συσκευή Android σας.



---

## Βήμα 1 — Ανοίξτε το Google Play Store

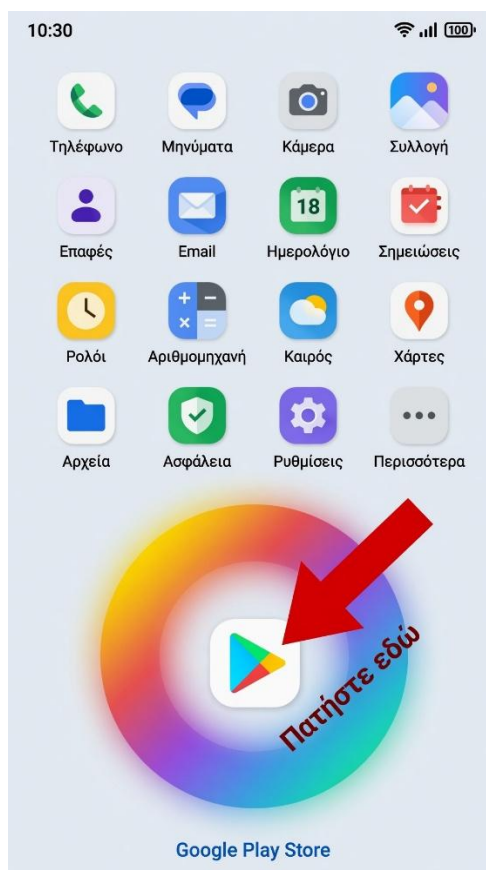
Βρείτε και πατήστε το εικονίδιο **Google Play Store** στην αρχική οθόνη ή στο μενού εφαρμογών της συσκευής σας. Το εικονίδιό του μοιάζει με τρίγωνο σε λευκό φόντο.

**Αναμενόμενο αποτέλεσμα:** Ανοίγει η αρχική οθόνη του Google Play Store.

---

## Αρχική οθόνη Android με Play Store

Εικονίδιο Google Play Store στην οθόνη Android



*Εικόνα 3: Εντοπίστε και πατήστε το εικονίδιο Google Play Store στην αρχική οθόνη.*

Στιγμιότυπο οθόνης (screenshot) της αρχικής οθόνης Android. Το εικονίδιο Google Play Store είναι επισημασμένο με έναν έγχρωμο κύκλο ή βέλος.

---

## Βήμα 2 — Αναζητήστε «Google Authenticator»

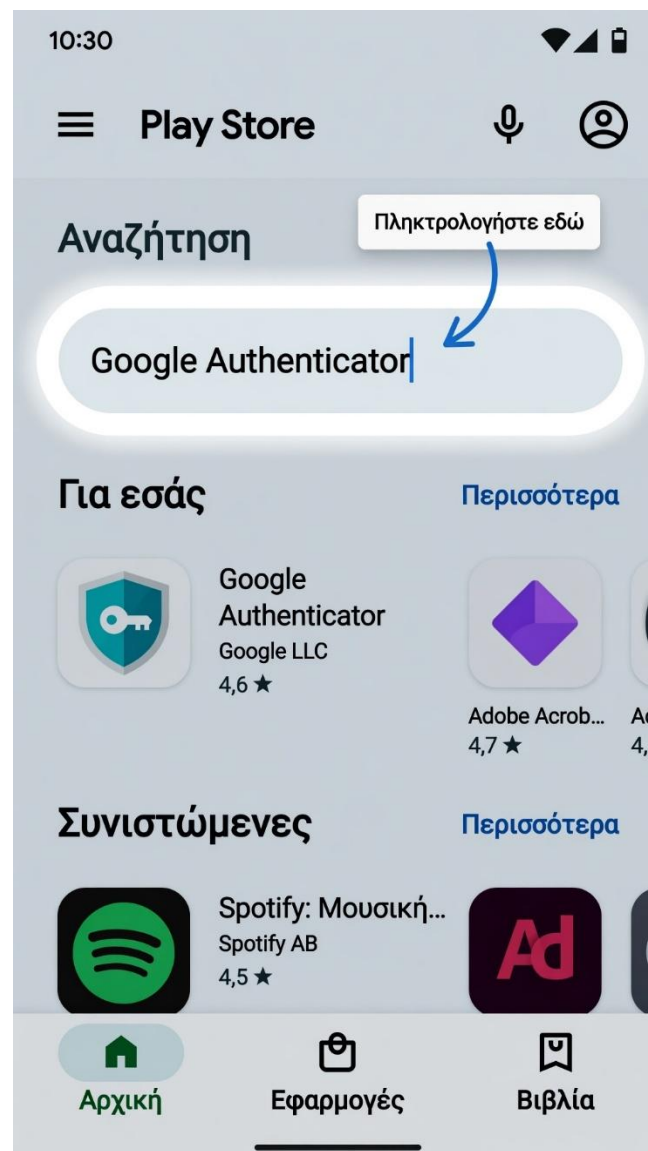


Πατήστε στο πεδίο αναζήτησης στην κορυφή της οθόνης και πληκτρολογήστε:  
**Google Authenticator**

**Αναμενόμενο αποτέλεσμα:** Εμφανίζονται αποτελέσματα αναζήτησης.

## Αναζήτηση στο Play Store

Πεδίο αναζήτησης Google Play Store



Εικόνα 4: Πληκτρολογήστε «Google Authenticator» στο πεδίο αναζήτησης.

Στιγμιότυπο του πεδίου αναζήτησης Play Store με την πληκτρολογημένη φράση «Google Authenticator».



### Βήμα 3 — Επιλέξτε την εφαρμογή

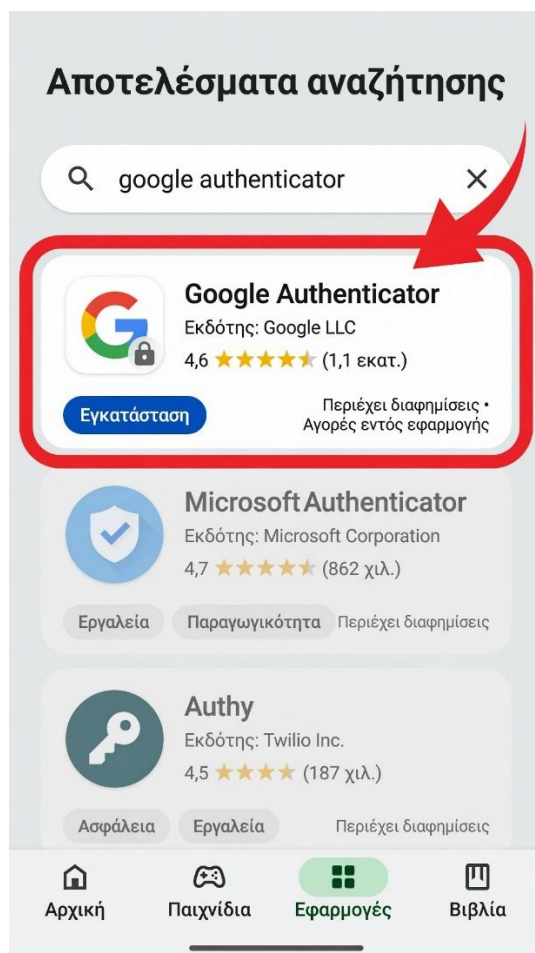
Στα αποτελέσματα, αναζητήστε την εφαρμογή **Google Authenticator** με εκδότη **Google LLC**. Βεβαιωθείτε ότι επιλέγετε τη σωστή εφαρμογή — ο εκδότης πρέπει να αναγράφει «Google LLC».

**⚠ Προσοχή:** Υπάρχουν παρόμοιες εφαρμογές με παρεμφερή ονόματα. Επιλέξτε μόνο την εφαρμογή που φέρει ως εκδότη **Google LLC**.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται η σελίδα της εφαρμογής Google Authenticator.

### Σωστή εφαρμογή στο Play Store

Google Authenticator στο Play Store — επιλογή σωστής εφαρμογής



Εικόνα 5: Επιλέξτε την εφαρμογή «Google Authenticator» με εκδότη «Google LLC».



Στιγμιότυπο αποτελεσμάτων αναζήτησης Play Store. Η σωστή εφαρμογή Google Authenticator είναι επισημασμένη, με εμφανή τα στοιχεία: εικονίδιο, όνομα «Google Authenticator» και εκδότης «Google LLC».

#### Βήμα 4 — Εγκαταστήστε την εφαρμογή

Πατήστε το κουμπί «Εγκατάσταση» (Install).

**Αναμενόμενο αποτέλεσμα:** Η εφαρμογή κατεβαίνει και εγκαθίσταται αυτόματα (διαρκεί συνήθως 1–2 λεπτά).

#### Κουμπί Εγκατάστασης

Κουμπί «Εγκατάσταση» στη σελίδα εφαρμογής



Εικόνα 6: Κουμπί «Εγκατάσταση» στη σελίδα Google Authenticator του Play Store.



Στιγμιότυπο της σελίδας Google Authenticator στο Play Store. Το κουμπί «Εγκατάσταση ή Install» (πράσινο ή μπλε) είναι επισημασμένο.

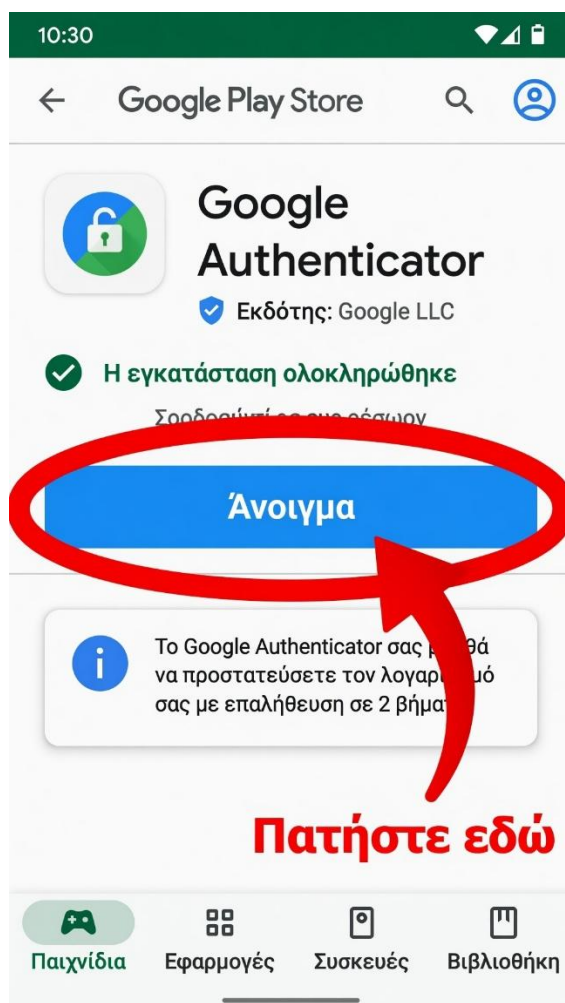
## Βήμα 5 — Ανοίξτε την εφαρμογή

Μόλις ολοκληρωθεί η εγκατάσταση, πατήστε **«Άνοιγμα»** (Open).

**Αναμενόμενο αποτέλεσμα:** Ανοίγει η εφαρμογή Google Authenticator για πρώτη φορά.

### Κουμπί Ανοίγματος

Κουμπί «Άνοιγμα/Open» μετά την εγκατάσταση



Εικόνα 7: Πατήστε «Άνοιγμα/Open» για να εκκινήσετε την εφαρμογή.



Στιγμιότυπο που δείχνει το κουμπί «Άνοιγμα/Όpen» μετά την ολοκλήρωση της εγκατάστασης.

---

#### 4. Πρώτη Ρύθμιση Google Authenticator

##### Σκοπός

Προσθήκη λογαριασμού στο Google Authenticator.

---

##### Βήμα 1 — Ανοίξτε την εφαρμογή

Πατήστε το εικονίδιο **Google Authenticator** στη συσκευή σας για να την ανοίξετε.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται η αρχική οθόνη της εφαρμογής.

---

##### Βήμα 2 — Επιλέξτε «Προσθήκη λογαριασμού»

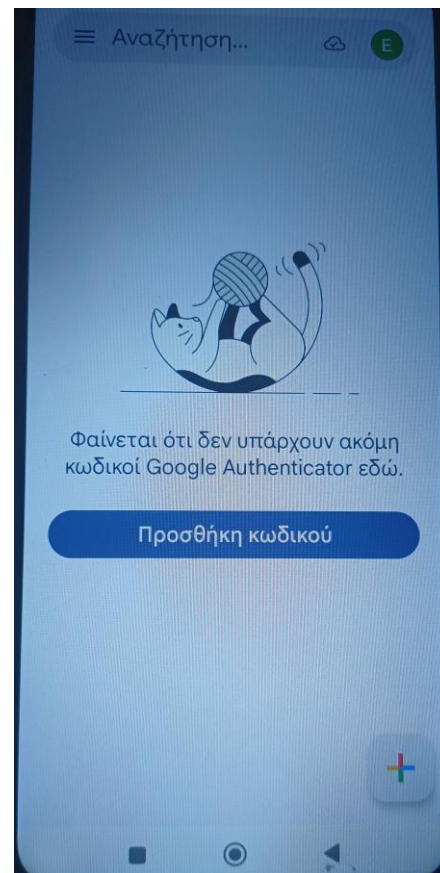
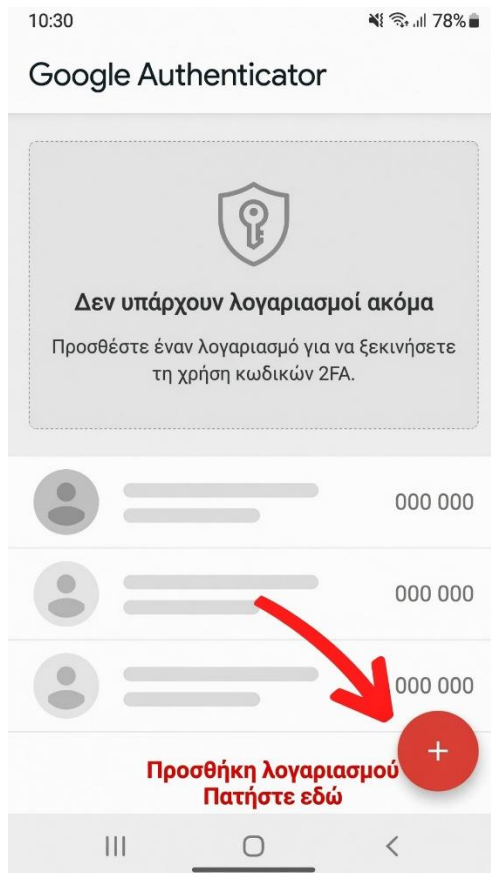
Πατήστε το εικονίδιο «+» ή το κουμπί «**Προσθήκη λογαριασμού**» (Get started / Add an account).

**Αναμενόμενο αποτέλεσμα:** Εμφανίζονται επιλογές για τον τρόπο προσθήκης λογαριασμού.

---

##### Προσθήκη κωδικού

Κουμπί «Προσθήκη Κωδικού» ή κλικ στο κουμπί  στο Google Authenticator



Εικόνα 8: Πατήστε το «+» ή «Προσθήκη λογαριασμού» για να ξεκινήσετε τη ρύθμιση.

Στιγμιότυπο της αρχικής οθόνης Google Authenticator με επισημασμένο κουμπί «+» ή «Προσθήκη κωδικού».



### Βήμα 3 — Σάρωση κωδικού

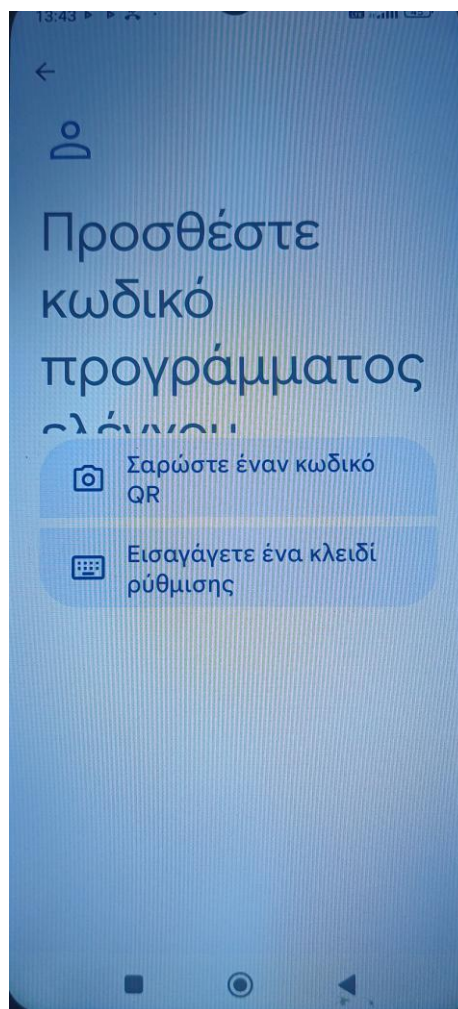
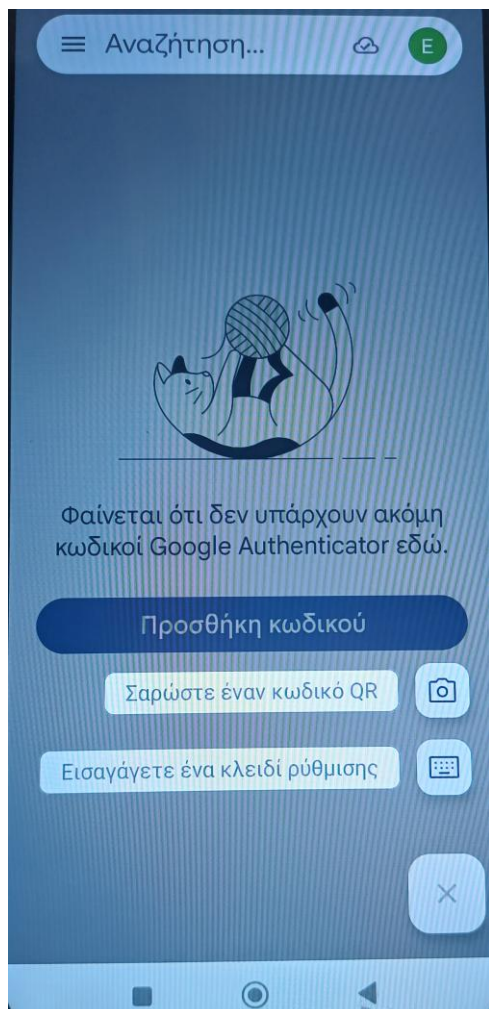
α) με κλικ στο κουμπί «+» εμφανίζεται η παρακάτω αριστερή οθόνη ενώ

β) με κλικ στο κουμπί «Προσθήκη κωδικού» εμφανίζεται η παρακάτω δεξιά οθόνη

Και δύο ροές στοχεύουν στην ίδια ενέργεια σάρωσης QR κωδικού.

**💡 Τι είναι το QR Code;** Είναι ένα τετράγωνο γραφικό με μαύρες και άσπρες κουκκίδες, παρόμοιο με barcode. Περιέχει κρυπτογραφημένες πληροφορίες που η εφαρμογή διαβάζει αυτόματα με την κάμερα.

**Αναμενόμενο αποτέλεσμα:** Ανοίγει η κάμερα της συσκευής.



Εικόνα 9: Επιλέξτε «Σαρώστε έναν κωδικό QR για να συνδέσετε τον λογαριασμό σας.



---

#### Βήμα 4 — Παραχωρήστε πρόσβαση στην κάμερα

Αν η εφαρμογή ζητήσει άδεια πρόσβασης στην κάμερα, πατήστε «**Αποδοχή**» ή «**Να επιτρέπεται**» (Allow).

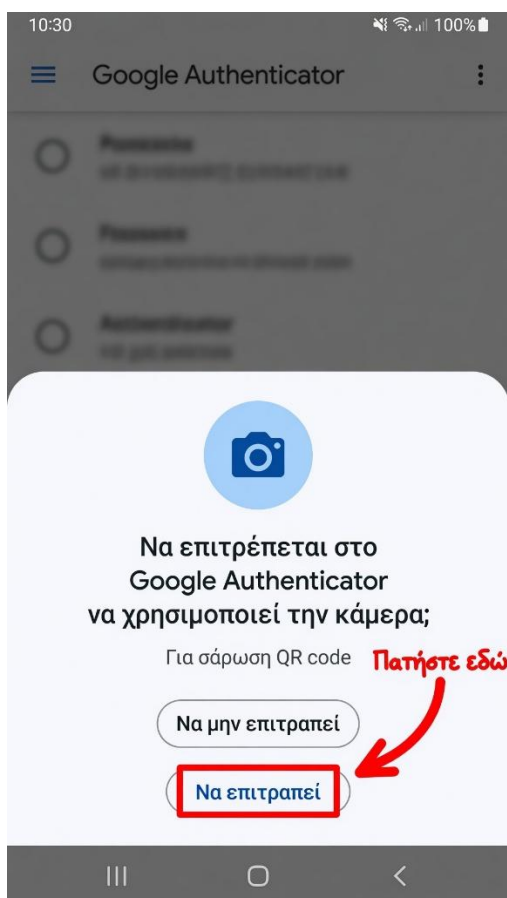
**⚠ Σημαντικό:** Χωρίς πρόσβαση στην κάμερα, η εφαρμογή δεν μπορεί να σαρώσει το QR Code.

**Αναμενόμενο αποτέλεσμα:** Ανοίγει ο σαρωτής QR Code.

---

#### Άδεια πρόσβασης κάμερας

Αίτημα άδειας πρόσβασης στην κάμερα



Εικόνα 10: Πατήστε «Να επιτρέπεται» για να δώσετε πρόσβαση στην κάμερα.



Στιγμιότυπο αναδύομένου παραθύρου Android που ζητά άδεια στην κάμερα για την εφαρμογή Google Authenticator.

---

## 5. Σύνδεση στην Πλατφόρμα Authentik

### Σκοπός

Είσοδος στο σύστημα Authentik για να λάβετε το QR Code ρύθμισης.

---

### Βήμα 1 — Μεταβείτε στη σελίδα σύνδεσης <https://auth.uop.gr>

Ανοίξτε τον περιηγητή ιστού (browser) στον υπολογιστή σας και μεταβείτε στη διεύθυνση <https://auth.uop.gr>.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται η οθόνη σύνδεσης του Authentik.

---

### Βήμα 2α — Εισάγετε τα στοιχεία σύνδεσης – όνομα χρήστη

Συμπληρώστε:

- **Όνομα χρήστη (Username):** το όνομα χρήστη (username) που έχετε.

Πατήστε «Σύνδεση» ή «Login».

---

### Οθόνη σύνδεσης Authentik – όνομα χρήστη

Φόρμα σύνδεσης πλατφόρμας Authentik για καταχώρηση ονόματος χρήστη



ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΠΕΛΟΠΟΝΝΗΣΟΥ  
University of the Peloponnese

Welcome to authentik!

Email ή Username \*

Email ή Username

Log in

Or

Use a security key

Εικόνα 11: Εισάγετε τα στοιχεία σύνδεσής σας στην πλατφόρμα Authentik.

Στιγμιότυπο της οθόνης σύνδεσης Authentik με πεδία για όνομα χρήστη (username) και κουμπί «Log in».

---

## Βήμα 2β — Εισάγετε τα στοιχεία σύνδεσης – κωδικός πρόσβασης

Συμπληρώστε:

- **Κωδικός πρόσβασης (Password):** τον κωδικό του λογαριασμού σας.

Πατήστε «Continue».

**Αναμενόμενο αποτέλεσμα:** Το σύστημα ανιχνεύει ότι δεν έχετε ρυθμίσει ακόμα 2FA και σας οδηγεί αυτόματα στη ρύθμιση.

---

## Οθόνη σύνδεσης Authentik – κωδικός πρόσβασης

Φόρμα σύνδεσης πλατφόρμας Authentik για καταχώρηση κωδικού πρόσβασης



Welcome to authentik!

[Not you?](#)

**Password**

[Continue](#)

Εικόνα 12: Εισάγετε το κωδικό (password) στην πλατφόρμα Authentik.

Στιγμιότυπο της οθόνης σύνδεσης Authentik με πεδία για κωδικό πρόσβασης και κουμπί «Continue».

### Βήμα 3 — Εμφάνιση QR Code από το Authentik

Μετά την είσοδο, το Authentik εμφανίζει αυτόματα μια **οθόνη ρύθμισης 2FA** που περιέχει ένα **QR Code**.

**💡 Τι πρέπει να κάνετε τώρα;** Κρατήστε ανοιχτή αυτή την οθόνη στον υπολογιστή σας. Στο επόμενο βήμα θα χρησιμοποιήσετε το κινητό σας για να σαρώσετε το QR Code.

**⚠ Προσοχή:** Μην κλείσετε αυτή την οθόνη και μην φωτογραφίσετε το QR Code για να το κοινοποιήσετε. Αφορά αποκλειστικά τον λογαριασμό σας.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται QR Code στην οθόνη του υπολογιστή.

### Οθόνη Authentik με QR Code

Οθόνη ρύθμισης 2FA στο Authentik — QR Code



Welcome to authentik!

IK

[Not you?](#)



[Copy TOTP Config](#)

[Copy Secret](#)

Please scan the QR code above using the Microsoft Authenticator, Google Authenticator, or other authenticator apps on your device, and enter the code the device displays below to finish setting up the MFA device.

**TOTP Code \***

Type your TOTP code...

[Continue](#)

*Εικόνα 12: Το Authentik εμφανίζει ένα QR Code για τη σύνδεση με το Google Authenticator. Κρατήστε αυτή την οθόνη ανοιχτή.*

Στιγμιότυπο της οθόνης ρύθμισης 2FA στο Authentik. Εμφανίζεται QR Code στο κέντρο με οδηγίες σάρωσης. Το QR Code είναι επισημασμένο με ένα πλαίσιο.

---

## 6. Σάρωση QR Code

### Σκοπός

Σύνδεση του Google Authenticator με τον λογαριασμό σας μέσω σάρωσης QR Code.

**Αναμενόμενο αποτέλεσμα:** Ο λογαριασμός του οργανισμού εμφανίζεται στο Google Authenticator.

- 
1. Βεβαιωθείτε ότι ο υπολογιστής και το κινητό σας βρίσκονται δίπλα-δίπλα.



2. Στο κινητό, το Google Authenticator πρέπει να έχει ανοιχτό τον **σαρωτή QR Code** (από το Βήμα 3 της ενότητας 4).
3. Κρατήστε το κινητό **μπροστά στην οθόνη του υπολογιστή** ώστε να φαίνεται το QR Code.
4. Η εφαρμογή **αναγνωρίζει αυτόματα** το QR Code — δεν χρειάζεται να πατήσετε κανένα κουμπί.
5. Μετά την επιτυχή σάρωση, ο λογαριασμός **προστίθεται αυτόματα** στο Google Authenticator.

**💡 Συμβουλή:** Αν η κάμερα δεν αναγνωρίζει το QR Code, δοκιμάστε να απομακρύνετε ελαφρώς το κινητό ή να μειώσετε τη φωτεινότητα του περιβάλλοντος.

---

## Σάρωση QR Code

Σάρωση QR Code από τον υπολογιστή με το κινητό



Εικόνα 13: Στρέψτε την κάμερα του κινητού προς το QR Code στον υπολογιστή.

Εικόνα που δείχνει χέρι που κρατά smartphone μπροστά σε οθόνη υπολογιστή. Στην οθόνη του υπολογιστή φαίνεται το QR Code του Authentik. Στην οθόνη του κινητού φαίνεται ο σαρωτής του Google Authenticator να εντοπίζει το QR Code.

---

## Επιτυχής προσθήκη λογαριασμού



## Επιτυχής προσθήκη λογαριασμού στο Google Authenticator



*Εικόνα 14: Μετά τη σάρωση, ο λογαριασμός εμφανίζεται στο Google Authenticator με ενεργό κωδικό OTP.*

Στιγμιότυπο του Google Authenticator μετά την επιτυχή σάρωση. Εμφανίζεται ο λογαριασμός του οργανισμού με ένα εξαψήφιο OTP και μια κυκλική μπάρα προόδου.

---

## 7. Λήψη Κωδικού OTP

### Σκοπός

Κατανόηση και χρήση του κωδικού OTP για τη σύνδεση.

---

Αφού προστεθεί ο λογαριασμός, το Google Authenticator εμφανίζει:

- **Ένα εξαψήφιο νούμερο** (π.χ. 482 915) — αυτός είναι ο κωδικός OTP.
- **Μια κυκλική μπάρα** που δείχνει πόσος χρόνος απομένει πριν αλλάξει ο κωδικός.

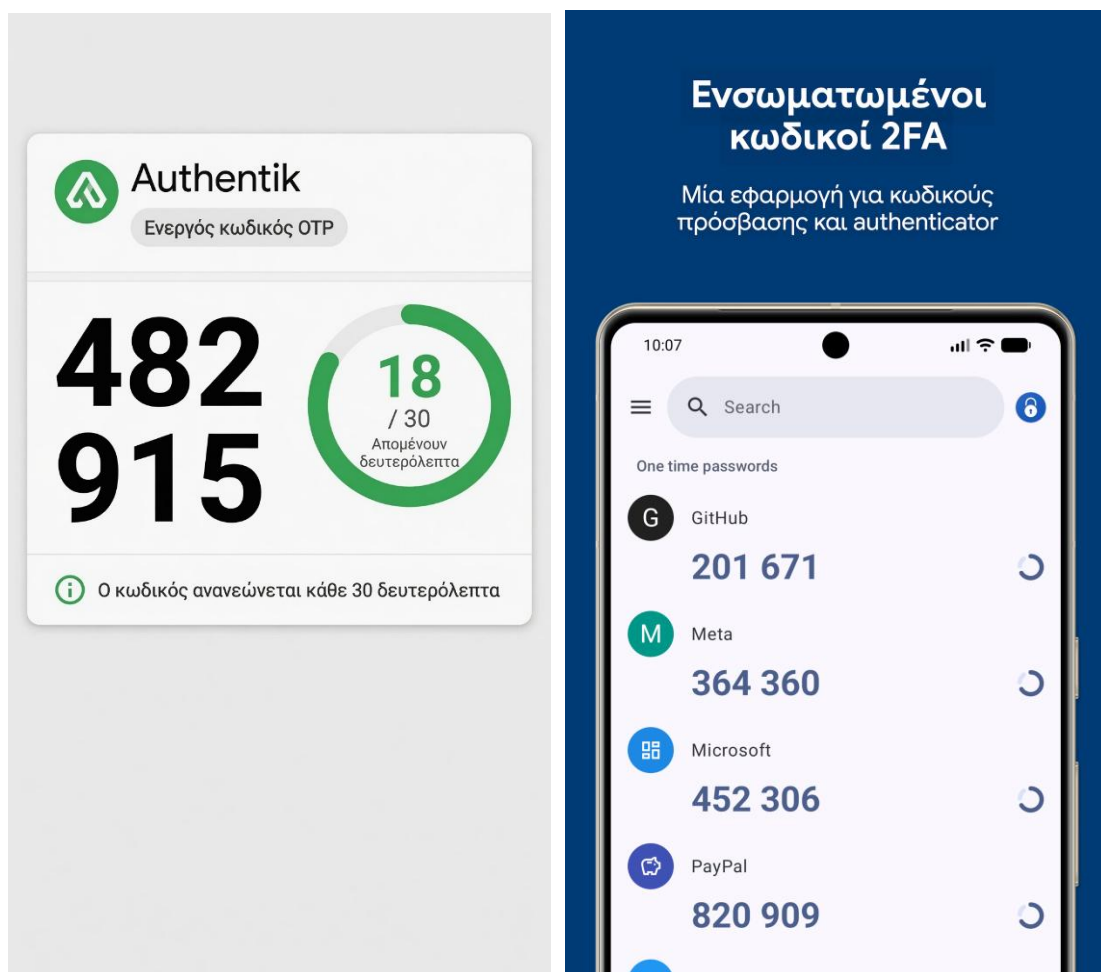
**Σημαντικό να θυμάστε:**



- Ο κωδικός **αλλάζει αυτόματα κάθε 30 δευτερόλεπτα**.
- Αν ο κωδικός αλλάξει ενώ τον πληκτρολογείτε, χρησιμοποιήστε τον νέο.
- **Μην κοινοποιείτε ποτέ** τον κωδικό OTP σε κανέναν — ούτε σε συναδέλφους, ούτε σε υποστήριξη πληροφορικής.

## Ενεργός κωδικός OTP

Οθόνη Google Authenticator με ενεργό κωδικό OTP



*Εικόνα 15: Ο εξαψήφιος κωδικός OTP αλλάζει αυτόματα κάθε 30 δευτερόλεπτα. Ο κύκλος δείχνει τον χρόνο που απομένει.*

Στιγμιότυπο της εφαρμογής Google Authenticator που δείχνει τον λογαριασμό του οργανισμού με εξαψήφιο κωδικό OTP (π.χ. 482 915) και κυκλική μπάρα προόδου που δείχνει τα δευτερόλεπτα που απομένουν.



## 8. Χρήση OTP κατά τη Σύνδεση

### Σκοπός

Ολοκλήρωση της διαδικασίας σύνδεσης χρησιμοποιώντας τον κωδικό OTP.

---

### Βήμα 1 — Εισάγετε τα στοιχεία σύνδεσης

Μεταβείτε στη σελίδα σύνδεσης του Authentik και εισάγετε το **όνομα χρήστη** και τον **κωδικό πρόσβασης** σας.

**Αναμενόμενο αποτέλεσμα:** Το σύστημα δέχεται τα στοιχεία και ζητά τον κωδικό OTP.

---

### Βήμα 2 — Εμφανίζεται αίτημα εισαγωγής OTP

Μετά την εισαγωγή κωδικού, το Authentik εμφανίζει νέα οθόνη που ζητά τον **κωδικό επαλήθευσης** (verification code).

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται πεδίο εισαγωγής 6-ψήφιου κωδικού.

---

### Εικόνα 16 — Αίτημα OTP από Authentik

**Τίτλος:** Οθόνη εισαγωγής κωδικού OTP στο Authentik



Welcome to authentik!

IK  [Not you?](#)

**Authentication code \***  
*Type an authentication code...*

Open your authenticator app to retrieve a one-time use code.

[Continue](#)

*Εικόνα 16: Το Authentik ζητά τον κωδικό επαλήθευσης μετά την εισαγωγή κωδικού πρόσβασης.*

Στιγμιότυπο της οθόνης Authentik που εμφανίζει πεδίο για εισαγωγή 6-ψήφιου κωδικού επαλήθευσης.

---

### Βήμα 3 — Ανοίξτε το Google Authenticator

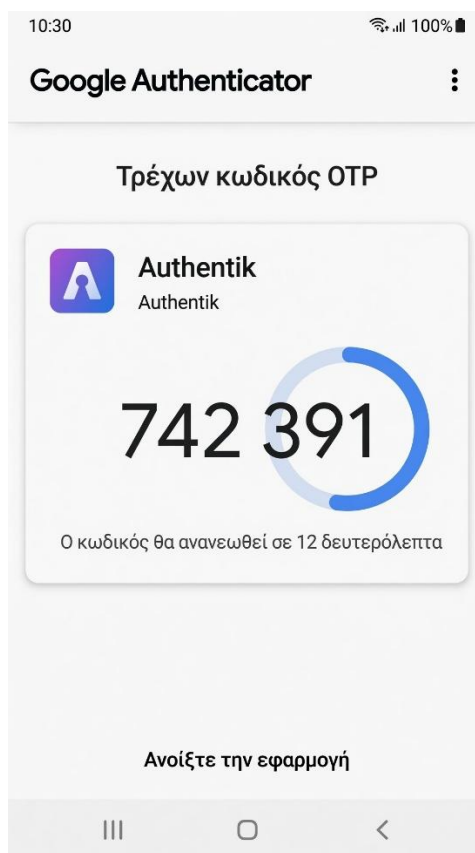
Πάρτε το κινητό σας και ανοίξτε την εφαρμογή **Google Authenticator**.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται ο ενεργός κωδικός OTP για τον λογαριασμό σας.

---

### Άνοιγμα Google Authenticator

Εφαρμογή Google Authenticator με ενεργό κωδικό



*Εικόνα 17: Ανοίξτε το Google Authenticator για να δείτε τον τρέχοντα κωδικό OTP.*

Στιγμιότυπο εφαρμογής Google Authenticator με εμφανή τον εξαψήφιο κωδικό OTP.

---

#### **Βήμα 4 — Διαβάστε τον εξαψήφιο κωδικό**

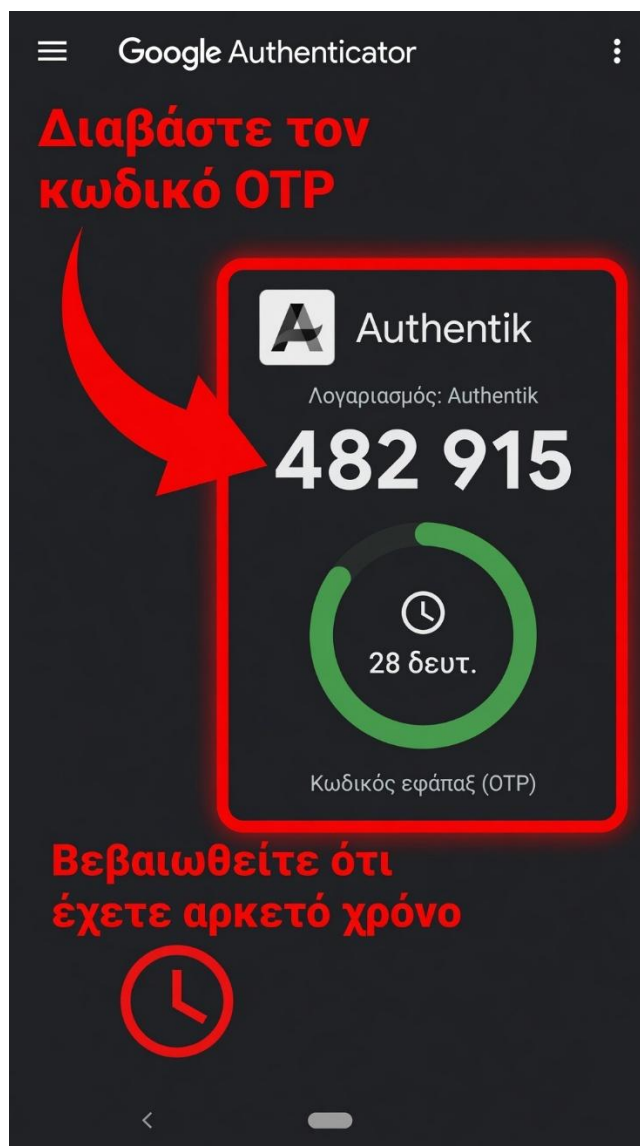
Δείτε τον εξαψήφιο κωδικό που εμφανίζεται στην εφαρμογή. Βεβαιωθείτε ότι ο κωδικός δεν είναι κοντά στη λήξη (όταν η κυκλική μπάρα είναι σχεδόν άδεια).

**💡 Συμβουλή:** Αν ο κωδικός πρόκειται να αλλάξει σε λιγότερο από 5 δευτερόλεπτα, περιμένετε τον νέο.

---

#### **Ανάγνωση κωδικού OTP**

Ανάγνωση εξαψήφιου κωδικού OTP



Εικόνα 18: Διαβάστε τον εξαψήφιο κωδικό OTP. Βεβαιωθείτε ότι έχετε αρκετό χρόνο να τον εισάγετε.

Στιγμιότυπο Google Authenticator με ευκρινή εξαψήφιο κωδικό OTP. Ο κωδικός είναι επισημασμένος.

---

### Βήμα 5 — Εισάγετε τον OTP στο Authenticik

Επιστρέψτε στον υπολογιστή σας και πληκτρολογήστε τον **εξαψήφιο κωδικό** στο πεδίο που εμφανίζει το Authenticik. Πατήστε «**Continue**».

**Αναμενόμενο αποτέλεσμα:** Το σύστημα επαληθεύει τον κωδικό.



## Εισαγωγή OTP στο Authentik

Καταχώρηση κωδικού OTP στο Authentik.

**Σημείωση:** Εάν δεν εμφανίζεται το πλαίσιο καταχώρησης OTP κάνετε κύλιση με την κατακόρυφη ράβδο κύλισης μέχρι να εμφανιστεί.



Welcome to authentik!

IK  Not you?

**Authentication code \***  
123456

Open your authenticator app to retrieve a one-time use code.

Continue

*Εικόνα 19: Εισάγετε τον εξαψήφιο κωδικό OTP και πατήστε «Continue».*

Στιγμιότυπο οθόνης Authentik με συμπληρωμένο πεδίο OTP και επισημασμένο κουμπί «Continue».

---

## Βήμα 6 — Επιτυχής είσοδος

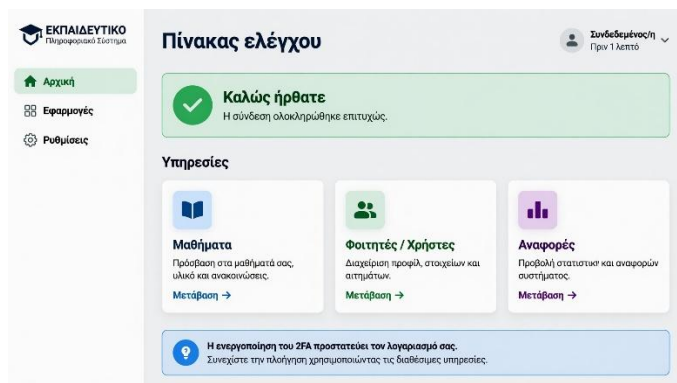
Αν ο κωδικός είναι σωστός, εισέρχεστε αυτόματα στο σύστημα.

**Αναμενόμενο αποτέλεσμα:** Εμφανίζεται η αρχική οθόνη του συστήματος ή η σελίδα καλωσορίσματος.

---

## Επιτυχής είσοδος

Επιτυχής είσοδος στο σύστημα μετά τον έλεγχο 2FA



*Εικόνα 20: Η επιτυχής εισαγωγή OTP οδηγεί στην είσοδο στο σύστημα*

Στιγμιότυπο της αρχικής οθόνης του συστήματος μετά την επιτυχή σύνδεση με 2FA.

---

## 9. Συχνές Ερωτήσεις (FAQ)

---

### **E1: Τι κάνω αν αλλάξω κινητό τηλέφωνο;**

Πρέπει να ενημερώσετε την Μονάδα Ψηφιακής Διακυβέρνησης του Πανεπιστημίου Πελοποννήσου πριν αλλάξετε συσκευή. Ο λογαριασμός θα επαναρυθμιστεί και θα σας σταλεί νέο QR Code. Μην απεγκαταστήσετε την εφαρμογή πριν ολοκληρωθεί η μεταφορά.

---

### **E2: Τι κάνω αν χάσω το κινητό μου;**

Επικοινωνήστε αμέσως με την Μονάδα Ψηφιακής Διακυβέρνησης. Ο λογαριασμός σας θα απενεργοποιηθεί προσωρινά και θα ορίσετε νέο 2FA σε νέα συσκευή.

---

### **E3: Τι γίνεται αν ο κωδικός OTP δεν λειτουργεί;**

Βεβαιωθείτε ότι:

- Εισαγάγατε τον σωστό 6-ψήφιο κωδικό (χωρίς κενά).
- Ο κωδικός δεν έχει λήξει (ο κύκλος δεν είναι άδειος).
- Η ημερομηνία/ώρα της συσκευής Android είναι σωστή.



Αν το πρόβλημα συνεχίζεται, επικοινωνήστε με την Μονάδα Ψηφιακής Διακυβέρνησης.

---

**E4: Χρειάζομαι Internet για να πάρω κωδικό OTP;**

Όχι. Μόλις εγκατασταθεί η εφαρμογή και προστεθεί ο λογαριασμός, ο κωδικός OTP παράγεται τοπικά στη συσκευή σας χωρίς σύνδεση στο Internet.

---

**E5: Μπορώ να έχω περισσότερους λογαριασμούς στο Google Authenticator;**

Ναι. Το Google Authenticator υποστηρίζει πολλούς λογαριασμούς ταυτόχρονα. Κάθε λογαριασμός εμφανίζεται ξεχωριστά στη λίστα με διαφορετικό OTP.

---

**E6: Μπορώ να χρησιμοποιήσω Microsoft Authenticator αντί για Google Authenticator;**

Η Μονάδα Ψηφιακής Διακυβέρνησης καθορίζει ποιες εφαρμογές Authenticator υποστηρίζονται. Μεταξύ αυτών και Microsoft Authenticator.

---

**E7: Γιατί αλλάζει συνεχώς ο κωδικός OTP;**

Ο κωδικός αλλάζει κάθε 30 δευτερόλεπτα για λόγους ασφαλείας. Έτσι, ακόμα και αν κάποιος δει τον κωδικό, δεν μπορεί να τον χρησιμοποιήσει μετά τη λήξη του.

---

**E8: Πόσο ασφαλές είναι το σύστημα 2FA;**

Το 2FA αυξάνει σημαντικά την ασφάλεια του λογαριασμού σας. Ακόμα και αν κάποιος γνωρίζει τον κωδικό πρόσβασής σας, δεν μπορεί να εισέλθει χωρίς πρόσβαση στο κινητό σας. Η ασφάλεια εξαρτάται επίσης από το πόσο καλά προστατεύετε τη φυσική πρόσβαση στη συσκευή σας.

---

**E9: Πού απευθύνομαι αν αντιμετωπίσω πρόβλημα;**

Επικοινωνήστε με την **Μονάδα Ψηφιακής Διακυβέρνησης** του Πανεπιστημίου Πελοποννήσου. Θα βρείτε τα στοιχεία επικοινωνίας στον ιστότοπο ή στο εσωτερικό δίκτυο του οργανισμού.



---

## 10. Συμβουλές Ασφαλείας

**⚠️ Η ασφάλεια εξαρτάται από εσάς.** Ακολουθήστε τις παρακάτω οδηγίες για να προστατέψετε τον λογαριασμό σας.

1. **Μην κοινοποιείτε ποτέ τον κωδικό OTP.** Κανείς — ούτε η υπηρεσία πληροφορικής, ούτε συνάδελφοί σας — δεν έχει ανάγκη να γνωρίζει τον κωδικό σας. Αν κάποιος τον ζητήσει, αρνηθείτε και αναφέρετέ το.
2. **Μην φωτογραφίζετε ή αποθηκεύετε το QR Code.** Το QR Code ρύθμισης αντιστοιχεί αποκλειστικά στον λογαριασμό σας. Αν πέσει σε λάθος χέρια, κάποιος μπορεί να αποκτήσει πρόσβαση.
3. **Μην στέλνετε OTP μέσω email, SMS ή μηνυμάτων.** Αν σας ζητηθεί να στείλετε κωδικό OTP με οποιονδήποτε τρόπο, αρνηθείτε αμέσως.
4. **Προστατεύστε τη συσκευή σας με PIN ή βιομετρικά.** Ορίστε κλειδωμα οθόνης (PIN, μοτίβο, δακτυλικό αποτύπωμα ή αναγνώριση προσώπου) για να αποτρέψετε μη εξουσιοδοτημένη πρόσβαση στο κινητό σας.
5. **Ενεργοποιήστε αντίγραφα ασφαλείας όπου επιτρέπεται.** Ρωτήστε την υπηρεσία πληροφορικής αν επιτρέπεται η χρήση λειτουργίας backup του Google Authenticator για να μην χάσετε τους κωδικούς σε περίπτωση αλλαγής συσκευής.
6. **Ενημερώνετε τακτικά το λειτουργικό σύστημα Android.** Οι ενημερώσεις ασφαλείας προστατεύουν τη συσκευή σας από γνωστές ευπάθειες. Εγκαταστήστε τις ενημερώσεις μόλις γίνουν διαθέσιμες.

---

## Ασφαλής χρήση 2FA

Ορθή πρακτική ασφαλείας — Τι να κάνετε και τι να αποφεύγετε



Εικόνα 21: Ακολουθήστε τις ορθές πρακτικές ασφαλείας για να προστατέψετε τον λογαριασμό σας

Εικονογράφηση δύο στηλών: Αριστερά (✓ Σωστό): Κλείδωμα οθόνης, εισαγωγή OTP μόνο στη σωστή σελίδα, αποσύνδεση μετά τη χρήση. Δεξιά (✗ Λάθος): Αποστολή OTP μέσω email, φωτογράφιση QR Code, κοινοποίηση κωδικού.

## 11. Αντιμετώπιση Προβλημάτων

Πρόβλημα	Πιθανή Αιτία	Λύση
Ο κωδικός OTP δεν γίνεται αποδεκτός	Ο κωδικός έχει λήξει	Χρησιμοποιήστε τον νέο κωδικό που εμφανίζεται στην εφαρμογή
Ο κωδικός OTP δεν γίνεται αποδεκτός	Λανθασμένος χρόνος στη συσκευή	Ελέγξτε ότι η ώρα και η ζώνη ώρας στο Android είναι σωστές (Ρυθμίσεις → Γενικά → Ημερομηνία & Ώρα → Αυτόματη ρύθμιση)
Δεν μπορώ να σαρώσω το QR Code	Κακός φωτισμός ή απόσταση	Δοκιμάστε σε καλύτερο φωτισμό. Απομακρύνετε ή πλησιάστε ελαφρώς το κινητό
Δεν μπορώ να σαρώσω το QR Code	Η εφαρμογή δεν έχει άδεια κάμερας	Μεταβείτε στις Ρυθμίσεις Android → Εφαρμογές → Google Authenticator → Άδειες → Ενεργοποίηση κάμερας
Η εφαρμογή δεν ανοίγει	Σφάλμα εφαρμογής	Επανεκκινήστε τη συσκευή Android. Αν επιμένει, απεγκαταστήστε και επανεγκαταστήστε



Πρόβλημα	Πιθανή Αιτία	Λύση
Δεν εμφανίζεται το QR Code στο Authentic	Πρόβλημα σύνδεσης ή περιόδου σύνδεσης	Αποσυνδεθείτε και επανασυνδεθείτε στο Authentic. Δοκιμάστε διαφορετικό browser
Έχασα το κινητό μου	Φυσική απώλεια ή κλοπή	Επικοινωνήστε αμέσως με την Μονάδα Ψηφιακής Διακυβέρνησης
Άλλαξα κινητό και έχασα τους κωδικούς	Δεν υπήρχε backup	Επικοινωνήστε με την υπηρεσία πληροφορικής για επαναρύθμιση 2FA
Ο λογαριασμός δεν εμφανίζεται στο Authenticator	Διαγράφηκε κατά λάθος	Επικοινωνήστε με την Μονάδα Ψηφιακής Διακυβέρνησης για νέο QR Code ρύθμισης
Το Authentic εμφανίζει «Λανθασμένος κωδικός»	Πολλαπλές αποτυχημένες προσπάθειες	Περιμένετε 5 λεπτά και δοκιμάστε ξανά. Αν επιμένει, επικοινωνήστε με την Μονάδα Ψηφιακής Διακυβέρνησης
Δεν έχω πρόσβαση στο Play Store	Περιορισμοί οργανισμού ή χωρίς Google Play	Επικοινωνήστε με την Μονάδα Ψηφιακής Διακυβέρνησης για εναλλακτικές επιλογές εγκατάστασης

---

Για περαιτέρω βοήθεια, επικοινωνήστε με την **Μονάδα Ψηφιακής Διακυβέρνησης / Helpdesk** του οργανισμού σας.

---

**Τέλος Οδηγού**