

# KÉTFAKTOROS AZONOSÍTÁS KEZELÉSE

-

## KRÉTA Tankönyvigénylő Rendszer

Felhasználói kézikönyv

## Tartalomjegyzék

1	Bevezetés.....	3
2	A Kétfaktoros azonosítás beállítása .....	3
2.1	A Kétfaktoros azonosítás beállításához szükséges követelmények .....	3
2.2	A Kétfaktoros azonosítás beállításának elérése .....	3
2.3	A Kétfaktoros azonosítás beállításának lépései .....	3
2.4	Kétfaktoros azonosítás beállítása felületen helytelen adatok megadása.....	7
2.4.1	Helytelen jelszó megadása .....	7
2.4.2	Helytelen hitelesítő kód megadása.....	7
2.5	Kétfaktoros azonosítás beállítás folyamatának megszakítása .....	7
2.5.1	Kétfaktoros azonosítás beállítása felületről kijelentkezés .....	8
2.5.2	Kétfaktoros azonosítás beállítása felületről elnavigálás.....	8
2.5.3	Kétfaktoros azonosítás beállításakor képernyő frissítése .....	8
2.5.4	Kétfaktoros azonosítás beállításakor a rendelkezési idő lejárata .....	9
2.6	Sikeres beállítást követő bejelentkezés .....	9
2.7	Hitelesítő alkalmazás módosítása .....	10
	Ábrajegyzék.....	11

## 1 Bevezetés

Jelen dokumentum célja ismertetni a Kétfaktoros azonosítás (Two-Factor Authentication, 2FA) funkcionalitás használatát a KRÉTA Tankönyvigénylő Modulban. Ezen biztonsági eljárással történő azonosítás során két különböző módon történik a felhasználó azonosságának ellenőrzése, így csökkentve az rendszerbe történő illetéktelen belépés kockázatát.

## 2 A Kétfaktoros azonosítás beállítása

### 2.1 A Kétfaktoros azonosítás beállításához szükséges követelmények

A Kétfaktoros azonosítás beállításához elengedhetetlen egy iOS vagy Android operációs rendszerű okostelefon vagy más mobil eszköz.

Az eszközre szükséges letölteni és telepíteni egy hitelesítő alkalmazást, amely egy időalapú (Time-based One-time Password, TOTP) egyszer használatos hitelesítőkódot generál. A TOTP alkalmazások (pl.: Google Authenticator, Microsoft Authenticator, Duo Mobile, NISZ Autentikátor) egyedi, időben korlátozott hozzáférési kódokat generálnak, amelyek néhány másodpercig vagy percig érvényesek.


(A KRÉTA Tankönyvigénylő rendszerben második faktoros azonosításra sem az e-mail, sem pedig az SMS nem használható.)

### 2.2 A Kétfaktoros azonosítás beállításának elérése

Amennyiben a rendszerben még nem végezte el a Kétfaktoros azonosítás beállítását, úgy a következő bejelentkezéskor szükséges ezt megtennie a rendszerbe történő belépéshez.

### 2.3 A Kétfaktoros azonosítás beállításának lépései

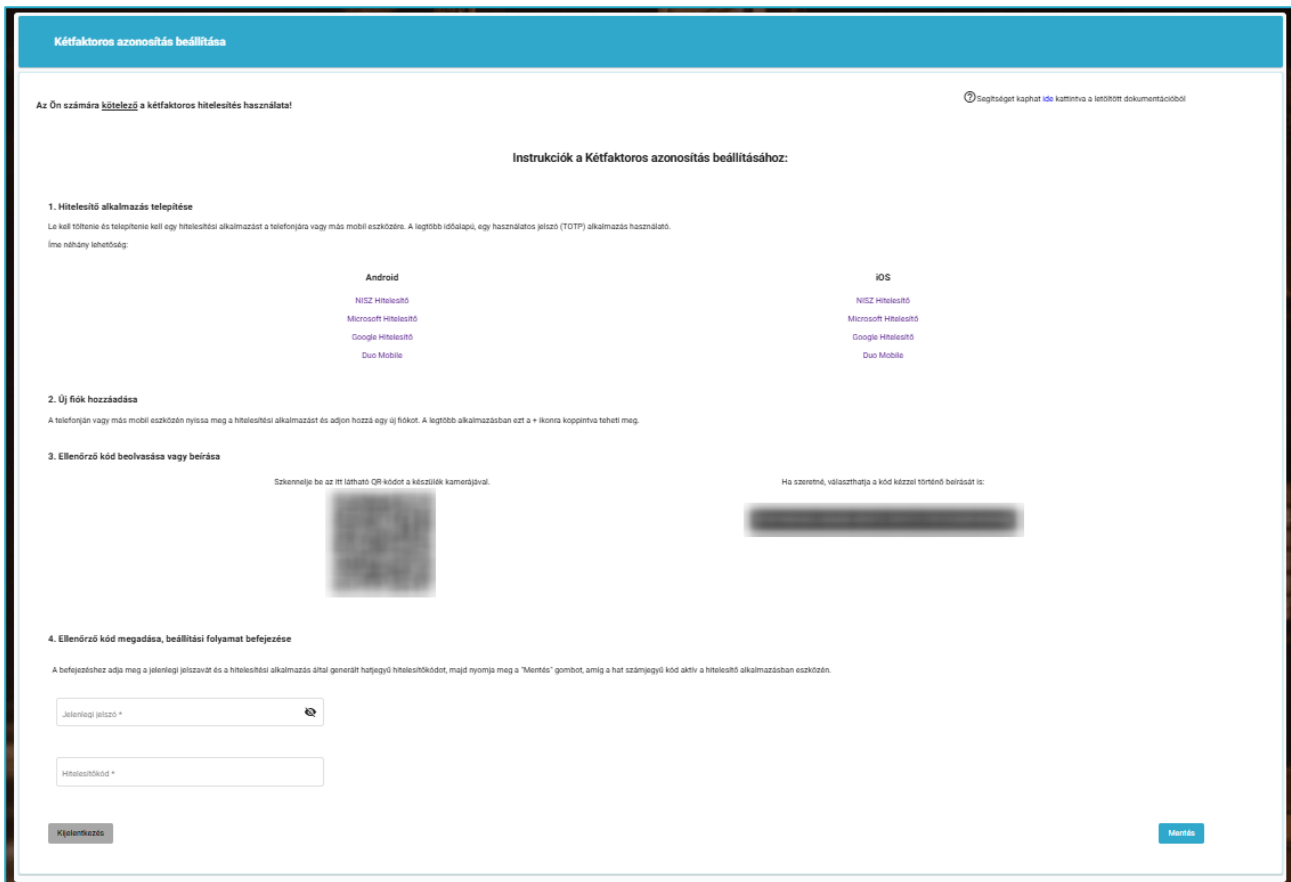
**1. lépés:** A Kétfaktoros azonosítás beállításának megkezdéséhez nyissa meg a KRÉTA Tankönyvigénylő Rendszert.

**2. lépés:** A bejelentkező felületen írja be a helyes bejelentkezési adatokat (*Felhasználónév, Jelszó*), majd kattintson a  gombra.




1. ábra – Bejelentkezés felület

A helyes bejelentkezési adatokkal történő belépés után megjelenik a *Kétfaktoros azonosítás beállítása* felület, amely a felhasználónak segítséget nyújt a Kétfaktoros azonosítás beállításában.







2. ábra – „Kétfaktoros azonosítás beállítása” felület

**3. lépés:** Az útmutató szerinti lépéseket szükséges elvégezni:





- ▶ Tájékoztató üzenetek:
  - *Az Ön számára kötelező a kétfaktoros hitelesítés használata!*
  -  *Segítséget kaphat ide kattintva a letöltött dokumentációból*
    - Az „ide” szóra kattintva letöltésre kerül a „pdf” kiterjesztésű felhasználói kézikönyv, melyben részletesen bemutatásra kerül a funkció beállítása és annak használata.
- ▶ *Instrukciók a Kétfaktoros azonosítás beállításához:*
  - **1. Hitelesítő alkalmazás telepítése**
    - Le kell töltenie és telepítenie egy hitelesítési alkalmazást a hivatalos áruházak egyikéből a telefonjára vagy más mobil eszközére (Android eszközökre a Google Play Áruházból, iOS eszközökre az App Store-ból)

- A legtöbb időalapú, egy használatos jelszó (TOTP) alkalmazás használható, pl.: a felsoroltak közül:

**Android:**

-  NISZ Hitelesítő:  
<https://play.google.com/store/apps/details?id=hu.innobile.niszauth>
-  Microsoft Hitelesítő:  
<https://play.google.com/store/apps/details?id=com.azure.authenticator>
-  Google Hitelesítő:  
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>
-  Duo Mobile  
<https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

**iOS:**

-  NISZ Hitelesítő  
<https://apps.apple.com/hu/app/nisz-hiteles%C3%ADt%C5%91/id1603444961?l=hu>
-  Microsoft Hitelesítő  
<https://apps.apple.com/hu/app/microsoft-authenticator/id983156458?l=hu>
-  Google Hitelesítő  
<https://apps.apple.com/hu/app/google-authenticator/id388497605?l=hu>
-  Duo Mobile  
<https://apps.apple.com/hu/app/duo-mobile/id422663827?l=hu>


**o 2. Új fiók hozzáadása**

- A telefonján vagy más mobil eszközén nyissa meg a telepített hitelesítési alkalmazást, majd adjon hozzá egy új fiókot. (A legtöbb alkalmazásban ezt a + ikonra koppintva teheti meg.)
- A fiókba belépve fog megjelenni a jövőben a hitelesítési kód, mely segítségével tudja majd a hitelesítést elvégezni a bejelentkezési folyamatnál.
- Ezt a beállítást egyszer szükséges elvégezni.

o 3. **Ellenőrző kód beolvasása vagy beírása**

- A hitelesítő alkalmazásban szükséges beolvasnia vagy beírnia a KRÉTA Tankönyvigénylő Rendszer Kétfaktoros azonosítást beállító képernyőjén szereplő kódok egyikét:
  - Szkenelje be a képernyőn látható egyedi QR kódot a készülék kamerájával
  - Ha szeretné, választhatja az azonosító kód kézzel történő beírását is
- A beolvasás/beírás után megtörténik a fiók hozzáadása az alkalmazásban.
- Megjelenik az eszközére telepített alkalmazásban a hatjegyű hitelesítő egyedi, időben korlátozott hozzáférési kód, amely néhány másodpercig vagy percig érvényes.


o 4. **Ellenőrző kód megadása, beállítási folyamat befejezése**

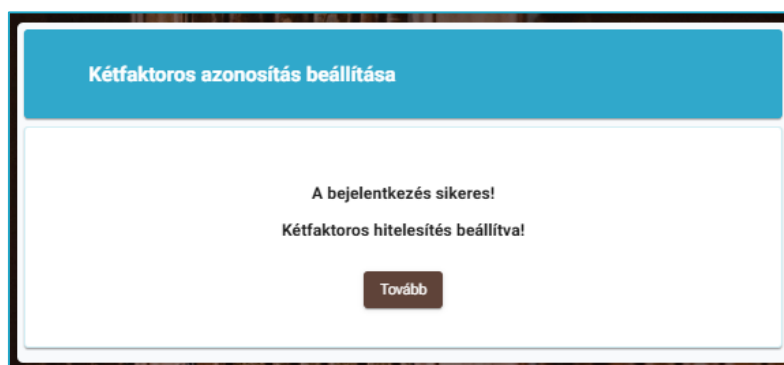
A befejezéshez adja meg a jelenlegi jelszavát és a hitelesítési alkalmazás által generált hatjegyű hitelesítő kódot a megfelelő mezőben, majd nyomja meg a  gombot, amíg a hat számjegyű kód aktív a hitelesítő alkalmazásban eszközén.

- *Jelenlegi jelszó\** (szabad szöveges beviteli mező) – a mező kitöltése kötelező
- *Hitelesítő kód\** (szabad szöveges beviteli mező) – a mező kitöltése kötelező

▶ **Funkciógombok:**

- o *Kijelentkezés*
- o *Mentés*

A  gombra kattintás után megjelenik egy új ablak, ahol visszaigazolást kap, hogy sikeresen beállításra került a Kétfaktoros azonosítás a fiókjához és megtörtént a bejelentkezés a rendszerbe.




3. ábra – Sikeres Kétfaktoros azonosítás beállítás és bejelentkezés visszaigazolása ablak

Amikor megjelent az ablak, akkor kattintson a  gombra, hogy a rendszerbe tovább tudjon navigálni, és a korábbiak szerint tudja használni.

A Kétfaktoros azonosítás beállítását egyszer szükséges megtennie!

## 2.4 Kétfaktoros azonosítás beállítása felületen helytelen adatok megadása



A *Kétfaktoros azonosítás beállítása* felületen, a beállítás véglegesítéséhez a szükséges kötelezően kitöltendő „*Jelenlegi jelszó*” és „*Hitelesítő kód*” mezőkben a  gombra kattintva a rendszer ellenőrzi a beállítás előtt a már meglévő jelszavának és az alkalmazásban megtalálható hitelesítő kód helyességét.

### 2.4.1 Helytelen jelszó megadása

Amennyiben a *Jelenlegi jelszó* mezőben helytelen jelszót adott meg, és megpróbálta elmenteni a beállítást, akkor az alábbi hibaüzenetet tapasztalja:



4. ábra – „Hibás jelszó” hibaiüzenet

Kérjük, ebben az esetben ellenőrizze az áthúzott szem  ikonra kattintás után a megjelenített jelszót, hogy biztosan a jelenlegi jelszavát írta be a mezőbe! Amennyiben nem megfelelően írta be, úgy javítsa azt ki, majd kattintson ismét a  gombra!


### 2.4.2 Helytelen hitelesítő kód megadása

Amennyiben a *Hitelesítő kód* mezőbe nem megfelelően adta meg az alkalmazás által generált hatszámjegű kódot, és megpróbálta elmenteni a beállítást, akkor az alábbi hibaüzenetet tapasztalja:



5. ábra – „Hibás hitelesítő kód” hibaiüzenet

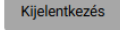

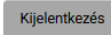
Kérjük, ebben az esetben ellenőrizze, hogy az alkalmazásból beírt generált kód (amely néhány másodpercig vagy percig érvényes), még ugyanaz-e, mint amit beírt a képernyőre és megfelelően írta be!

Ha lejárt ennek az ideje és megváltozott, vagy elírta, akkor kérjük, hogy az új kódot írja be, majd kattintson ismét a  gombra!

## 2.5 Kétfaktoros azonosítás beállítás folyamatának megszakítása

A Kétfaktoros azonosítás beállításának megszakítása többféle módon tud megtörténni, melyek után egyes folyamatokat szükséges lehet újra elvégeznie, esetlegesen a teljes beállítást újratekintenie, ezért kérjük, hogy körültekintően járjon el ezek végrehajtásakor!


### 2.5.1 Kétfaktoros azonosítás beállítása felületről kijelentkezés

A Kétfaktoros azonosítás beállítását megszakíthatja a *Kétfaktoros azonosítás beállítás* felületen a  gombra kattintva. (Ezt a  gombra kattintás előtt bármikor megteheti.) Ha a  gombra kattint, akkor megszakad a beállítás folyamata és visszanavigálja a rendszer a bejelentkezési felületre, ahol a mezők kitöltetlen állapotban jelennek meg.

Amennyiben a kijelentkezés előtt már sikeresen összekötötte a hitelesítő alkalmazást a KRÉTA Tankönyvigénylő rendszerrel (az alkalmazásban megjelent a hatjegyű kódja), akkor az alkalmazásban megjelent azonosítót szükséges törölnie. Ha ezt megtette, akkor a következő alkalommal, amikor a Kétfaktoros azonosítás beállítás végzi, az instrukcióban leírtaknak megfelelően újra szükséges beolvasnia/beírnia a hitelesítő alkalmazásban a QR kódot vagy a kézzel bevihető kódot.

Ezt követően már be tudja fejezni a beállítást a rendszerben.

### 2.5.2 Kétfaktoros azonosítás beállítása felületről elnavigálás


A *Kétfaktoros azonosítás beállítás* felületen amennyiben a böngészőből visszanavigál az előző oldalra, esetleg bezárja a böngészőt, ahol már elkezdte a beállítási folyamatot a  gombra kattintás előtt, akkor a bejelentkezési felületen ismételtelen szükséges lesz a bejelentkezési adatokat megadnia és újrakezdenie a beállítási folyamatot.

Amennyiben az elnavigálás előtt már sikeresen összekötötte a hitelesítő alkalmazást a KRÉTA Tankönyvigénylő rendszerrel (az alkalmazásban megjelent a hatjegyű kódja), akkor az alkalmazásban megjelent azonosítót szükséges törölnie. Ha ezt megtette, akkor a Kétfaktoros azonosítás beállításakor az instrukcióban leírtaknak megfelelően újra szükséges beolvasnia/beírnia a hitelesítő alkalmazásba a QR kódot vagy a kézzel bevihető kódot.

Ezt követően már be tudja fejezni a beállítást a rendszerben.

### 2.5.3 Kétfaktoros azonosítás beállításakor képernyő frissítése

A *Kétfaktoros azonosítás beállítása* felületen a böngésző frissítése esetén a megjelenő QR kód és a manuálisan bevihető egyedi azonosító is frissülni fog.


Amennyiben már sikeresen összekötötte a hitelesítő alkalmazást a KRÉTA Tankönyvigénylő rendszerrel (az alkalmazásban megjelent a hatjegyű kódja), de még nem véglegesítette a  gombbal a Tankönyvigénylő Rendszer felületén ennek a beállítását, mert frissítette felületet, akkor az alkalmazásban megjelent azonosítót szükséges törölnie. Ha ezt megtette, akkor a lefrissült felületen lévő új QR kódot vagy a kézzel bevihető kódot újra szükséges beolvasnia/beírnia a hitelesítő alkalmazásba.

Ezt követően már be tudja fejezni a beállítást a rendszerben.



## 2.5.4 Kétfaktoros azonosítás beállításakor a rendelkezési idő lejárata

A *Kétfaktoros azonosítás beállítása* felületen biztonsági okokból csak egy meghatározott időkeret áll rendelkezésére, hogy a folyamatot befejezze, és a beállítást elvégezze. Amennyiben ez az idő lejár, úgy a rendszer automatikusan visszanavigálja a bejelentkező felületre, kitöltetlen adatokkal. Ha szeretné a beállítást befejezni, úgy kezdje előlről a folyamatot!


Amennyiben már a rendelkezési idő lejárata előtt sikeresen összekötötte a hitelesítő alkalmazást a KRÉTA Tankönyvigénylő rendszerrel (az alkalmazásban megjelent a hatjegyű kódja), de még nem véglegesítette a  gombbal a Tankönyvigénylő Rendszer felületén ennek a beállítását, akkor az alkalmazásban megjelent azonosítót szükséges törölnie. Ha ezt megtette, akkor az ismételt beállítás során az új QR kódot vagy a kézzel bevihető kódot újra szükséges beolvasnia/beírnia a hitelesítő alkalmazásba.

Ezt követően már be tudja fejezni a beállítást a rendszerben.

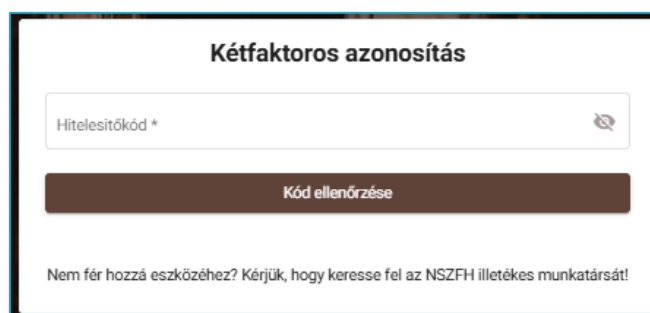
## 2.6 Sikeres beállítást követő bejelentkezés

Amennyiben sikeresen beállította a Kétfaktoros azonosítást, úgy a következő bejelentkezés alkalmával a Bejelentkezési felületen a helyes *Felhasználónév, Jelszó* megadását követően a *Kétfaktoros azonosítás* oldalon szükséges megadja a hitelesítő alkalmazásban megjelent *hitelesítő kódot*.

- ▶ *Hitelesítő kód\** (szabad szöveges beviteli mező) – a mező kitöltése kötelező

A *hitelesítő kód* beírását követően az áthúzott szem  ikonra kattintás után a megtekintheti a beírt kódot, amely alapértelmezetten a beíráskor kipontozottan jelenik meg.

A helyes hitelesítő kód megadását követően a  gombra kattintás után a rendszer bejelentkezteti, melyet a korábbiaknak megfelelő módon tud használni.



A képen látható a "Kétfaktoros azonosítás" felület egy részlete. A cím "Kétfaktoros azonosítás". Alatta egy "Hitelesítő kód \*" című szövegmező van, mellette egy áthúzott szem ikon. A mező alatt egy sötétbarna "Kód ellenőrzése" gomb található. Az alján egy kisebb szöveg olvasható: "Nem fér hozzá eszközehez? Kérjük, hogy keresse fel az NSZFH illetékes munkatársát!"

6. ábra – „Kétfaktoros azonosítás” hitelesítő kód ellenőrzése ablak

## 2.7 Hitelesítő alkalmazás módosítása

Egy felhasználói fiókhoz csak egy beállított Kétfaktoros azonosítás lehet egyidejűleg!

Amennyiben készüléket vagy hitelesítő alkalmazást szeretne változtatni, úgy kérjük, hogy a Nemzeti Szakképzési és Felnőttképzési Hivatal (NSZFH) illetékes munkatársát keresse fel és a beazonosítását követően kérje, hogy kerüljön törlésre a már korábban beállított Kétfaktoros azonosítás az Ön fiókjához!

Ha ennek a törlése megtörtént és visszaigazolták Önnek, akkor a beállítást egy másik készüléken vagy másik alkalmazásban újra el tudja végezni a korábbiaknak megfelelően.

## Ábrajegyzék

1. ábra – Bejelentkezés felület .....	3
2. ábra – „Kétfaktoros azonosítás beállítása” felület.....	4
3. ábra – Sikeres Kétfaktoros azonosítás beállítás és bejelentkezés visszaigazolása ablak.....	6
4. ábra – „Hibás jelszó” hibaüzenet .....	7
5. ábra – „Hibás hitelesítő kód” hibaüzenet .....	7
6. ábra – „Kétfaktoros azonosítás” hitelesítő kód ellenőrzése ablak.....	9