



ERA KERETRENDSZER KÉTFAKTOROS AZONOSÍTÁS

Felhasználói kézikönyv

v1.4

Tartalom

1. Fogalomtár.....	3
2. Bevezetés.....	3
3. Előfeltétel a kétfaktoros azonosítás használatához.....	4
4. Bejelentkezés a kétfaktoros azonosítás bevezetését követően	4
4.1. Türelmi időszak	4
4.1.1. Bevezetést megelőzően regisztrált felhasználók.....	4
4.1.2. Bevezetést követően regisztrált felhasználók	6
4.2. Kétfaktoros azonosítás regisztráció.....	7
4.3. Kétfaktoros azonosítással történő bejelentkezés	12
4.4. Kétfaktoros hitelesítés visszaállítása	15
4.5. További tudnivalók a kétfaktoros azonosításról	19
4.5.1. Létrehozás/Újragenerálás funkciógomb.....	19

1. FOGALOMTÁR

ERA: a Magyar Nemzeti Bank (MNB) elektronikus rendszere hitelesített adatok fogadásához, amely a regisztrált felhasználóknak/intézményeknek lehetőséget biztosít, hogy az MNB egyes szolgáltatásait egységes felületen keresztül érhessek el.

Regisztráció típusai: az ERA egyes szolgáltatásainak elérése regisztrációhoz kötött. Az egyes szolgáltatások eltérő szintű regisztrációval érhetőek el. A különbséget a regisztrációs típusok között a hitelesítés típusa jelenti. A regisztrációs folyamat során a felhasználó számára listázásra kerül az egyes regisztráció típusokkal elérhető szolgáltatások köre.

- Központi Azonosítási Ügynökön (KAÜ) keresztüli regisztráció: ezen regisztráció típussal korlátozott körben érhetőek el az ERA szolgáltatásai. Az ERA-s regisztrációs űrlap kitöltését megelőzi a www.magyarorszag.hu portálon keresztül az Ügyfélkapuba történő bejelentkezés.
- Felhasználónév-jelszó alapú regisztráció: ezen regisztráció típussal korlátozott körben érhetőek el az ERA szolgáltatásai.
- Tanúsítvány alapú regisztráció: a regisztrációs folyamat során, a regisztrációs űrlap kitöltése előtt a regisztráció időpontjában érvényes, fokozott vagy minősített biztonságú aláíró tanúsítvány feltöltése szükséges.

Kétfaktoros azonosítás: az ERA-ba történő felhasználói bejelentkezéshez felhasználónév és jelszó megadását követően egy második hitelesítési faktor is szükséges a felhasználó azonosításához.

Türelmi időszak: a kétfaktoros azonosítás bevezetésekor meghatározásra kerül egy 60 napos időszak, melyben a már korábban regisztrált felhasználó számára nem kötelező a kétfaktoros azonosítás, illetve az arra történő regisztráció, de a lehetőség biztosított rá. Az újonnan regisztráló felhasználók számára azonban már a türelmi időszak alatt is kötelezővé válik a kétfaktoros azonosítás használata.

Előregisztráció: a kétfaktoros azonosítás bevezetése előtt regisztrált felhasználók számára biztosított a lehetőség a türelmi időszak alatt előzetes kétfaktoros azonosítás regisztrációra. Amennyiben a felhasználó él az előregisztráció lehetőségével, onnantól minden bejelentkezésnél kötelező a kétfaktoros azonosítás.

Kötelező regisztráció: a türelmi időszak lejáratát követően a kétfaktoros azonosítás bevezetése előtt regisztrált felhasználók számára is kötelező a kétfaktoros azonosítás.

2. BEVEZETÉS

Az ERA rendszerbe történő felhasználónév-jelszó alapú és tanúsítványos regisztráció esetén, a felhasználó személyes és üzleti adatainak magasabb szintű védelme érdekében a bejelentkezési folyamatba bevezetésre kerül a kétfaktoros felhasználói hitelesítés, ami azt jelenti, hogy a felhasználónév és jelszó megadása mellett egy további azonosítót is meg kell adni a bejelentkezéshez. Ezt az azonosítót egy, a felhasználó mobiltelefon (okostelefon) készülékére telepített (ingyenesen letölthető) hitelesítő alkalmazás biztosítja.

A kétfaktoros hitelesítés bevezetése előtt regisztrált felhasználók számára türelmi időszak lesz biztosítva. Ezen időszak alatt számukra még nem kötelező a kétfaktoros azonosítás alkalmazása. Az újonnan regisztráltak számára viszont már ebben az időszakban is kötelező a kétfaktoros azonosítás.

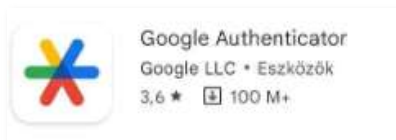
A KAÜ-s regisztrációval rendelkező felhasználók esetében a bejelentkezési folyamat nem változik.

3. ELŐFELTÉTEL A KÉTFAKTOROS AZONOSÍTÁS HASZNÁLATÁHOZ

A kétfaktoros azonosítás előfeltétele, hogy a felhasználó rendelkezzen egy Google Android vagy egy Apple iOS operációs rendszerrel rendelkező vagy egy Microsoft Windows Phone okostelefon készülékkel, valamint az arra telepített, ingyenes hitelesítő alkalmazással, amely a kétfaktoros azonosítás regisztrációjához és a bejelentkezéshez szükséges.

Az alábbi hitelesítő alkalmazások használhatóak a kétfaktoros azonosításhoz:

- *Google Authenticator* – az alkalmazás elérhető:
 - a Google Play Áruházban: Google Android készülék használata esetén:



- az Apple App Store-ban: Apple iOS operációs rendszerrel rendelkező készülék esetén:



- *Microsoft Authenticator* – az alkalmazás elérhető:
 - a Google Play Áruházban: Google Android készülék használata esetén:



- az Apple App Store-ban: Apple iOS operációs rendszerrel rendelkező készülék esetén:



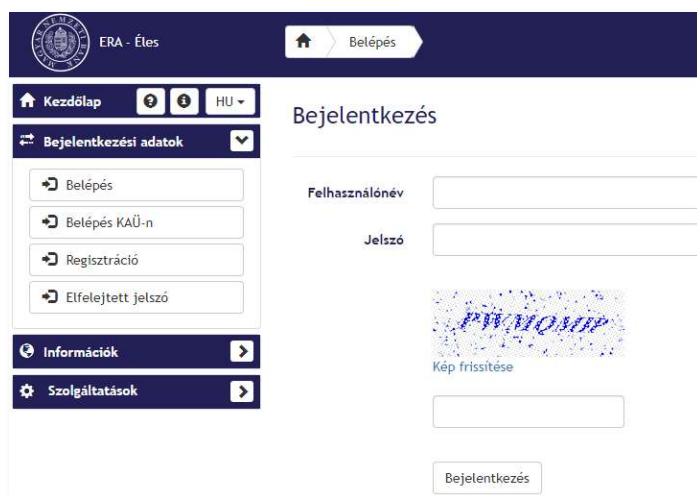
4. BEJELENTKÉZÉS A KÉTFAKTOROS AZONOSÍTÁS BEVEZETÉSÉT KÖVETŐEN

4.1. Türelmi időszak

4.1.1. Bevezetést megelőzően regisztrált felhasználók

4.1.1.1. Bejelentkezés a korábbiakkal megegyező módon

A kétfaktoros azonosítás bevezetését megelőzően regisztrált felhasználók számára a türelmi időszak végéig biztosított a korábbiakkal megegyező módon történő bejelentkezés. Azaz a felhasználónév, jelszó megadását és captcha kitöltését (sikeres bejelentkezést) követően a felhasználó számára megszokott módon elérhetőek a regisztrált intézmények és a szolgáltatások.

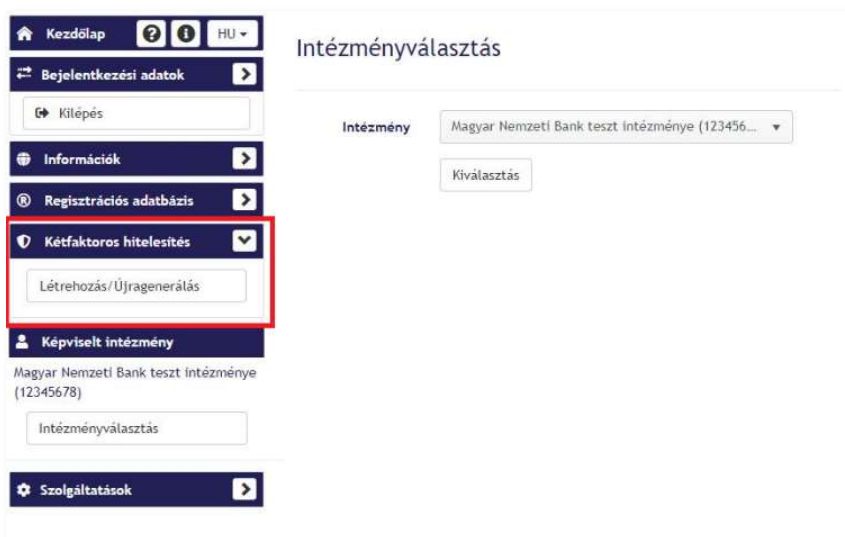


1. ábra: ERA rendszer bejelentkező felület

A türelmi időszak lejártával ezen bejelentkezési módra már nincs lehetőség, ekkor már kötelező a kétfaktoros azonosítás regisztráció a [4.2 Kétfaktoros azonosítás regisztráció](#) pontban leírtak szerint.

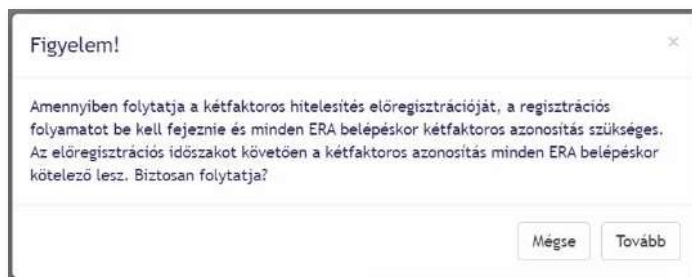
4.1.1.2. Előregisztrációs lehetőség

A kétfaktoros azonosítás bevezetését megelőzően regisztrált felhasználók számára a türelmi időszak alatt lehetőség van az előregisztrációra. Erre a bejelentkezést követően a bal oldali menülistában a *Kétfaktoros hitelesítés* menüpontban található *Létrehozás/Újragenerálás* funkciógomb segítségével van lehetőség. A menüpontra kattintva megjelenítésre kerül a regisztrációs felület. A kétfaktoros azonosítás regisztráció a [4.2 Kétfaktoros azonosítás regisztráció](#) pontban leírtak szerint történik.



2. ábra: Létrehozás/Újragenerálás funkciógomb

Fontos, hogy amennyiben a felhasználó megkezdte a kétfaktoros azonosítás regisztrációs folyamatát, addig nem tud továbblépni (vagy bejelentkezni a korábbiak szerint), ameddig be nem fejezi a regisztrációt. Erről a kétfaktoros hitelesítés létrehozásakor egy figyelmeztető üzenet is tájékoztatja a felhasználót. Ekkor lehetősége van elvetni a kétfaktoros hitelesítés regisztrációt (a *Mégse* gombra kattintva), vagy tovább folytatni (a *Tovább* gombra kattintva).



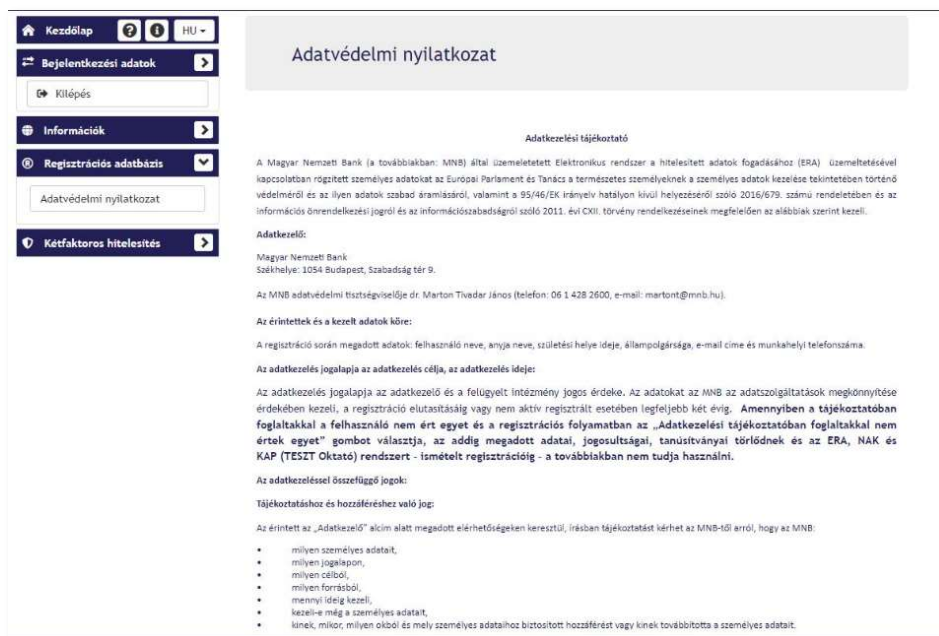
3. ábra: Kétfaktoros hitelesítés előregisztráció megerősítő üzenet

A sikeres regisztrációt követően pedig már **csak kétfaktoros hitelesítéssel történő bejelentkezésre lesz lehetősége**, a [4.3. Kétfaktoros azonosítással történő bejelentkezés](#) pontban leírtak szerint. Ezt követően abban az esetben is kötelező lesz a kétfaktoros azonosítás használata, amennyiben kétfaktoros hitelesítés visszaállítását kezdeményezi a felhasználó.

4.1.2. Bevezetést követően regisztrált felhasználók

A kétfaktoros azonosítás bevezetését követően regisztrált felhasználók számára az első bejelentkezéskor kötelező a kétfaktoros azonosítás regisztráció a [4.2 Kétfaktoros azonosítás regisztráció](#) pontban leírtak szerint. Ezt megelőzően kizárólag a „Regisztrációs adatlap” letöltésére van lehetőség.

Az első bejelentkezést és a kétfaktoros azonosítás regisztrációt követően az „Adatvédelmi nyilatkozat” elfogadásával van lehetőség az ERA rendszer használatára (a regisztrációra vonatkozó részletes leírás az [ERA útmutatók](#) között elérhető *Súgó a regisztrációs folyamathoz* dokumentumban található).



4. ábra: Adatvédelmi nyilatkozat (a regisztrációt követően)

4.2. Kétfaktoros azonosítás regisztráció

A kétfaktoros azonosítás regisztráció lépései:

1. Bejelentkezés az ERA keretrendszerbe felhasználónév és jelszó megadásával, valamint a captcha kitöltésével.
2. Az ERA felületén megjelenítésre kerül a kétfaktoros azonosítás regisztrációhoz szükséges QR kód, illetve kulcs.

ERAteszt3 - Teszt3

Kétfaktoros hitelesítés újragenerálás

Kétfaktoros hitelesítés

A felhasználónév-jelszó alapú bejelentkezés manapság már nem nyújt elég erős védelmet a felhasználó számára, ezért a személyes és üzleti adatainak védelme miatt az MNB bevezeti egy külső alkalmazás segítségével biztosított **kétfaktoros hitelesítést** az ERA-ba történő biztonságos bejelentkezés érdekében.

A hitelesítő alkalmazás használatához kövesse az alábbi lépéseket:

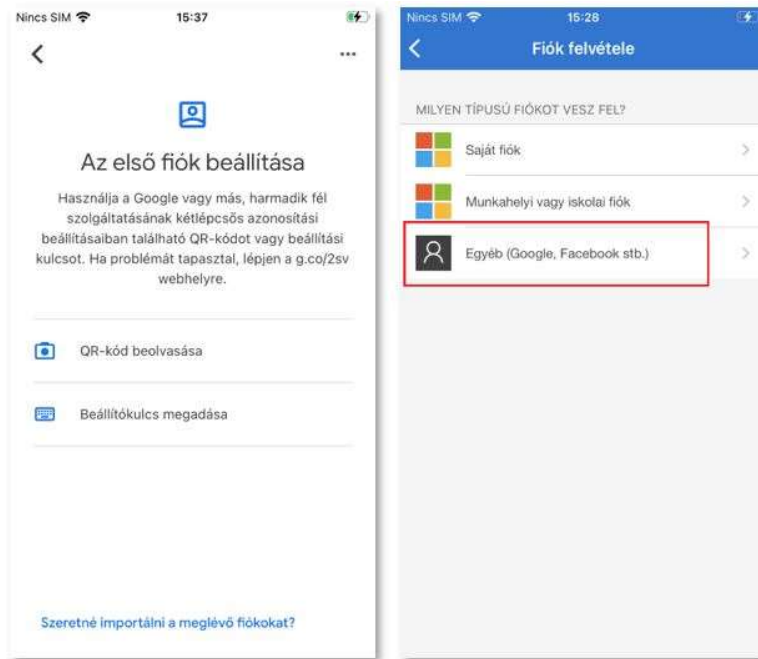
1. A kétfaktoros azonosítás előfeltétele egy Androidos, egy iOS vagy egy Windows phone mobilkészülék, valamint az arra telepített hitelesítő alkalmazás, amely a kétfaktoros azonosítás regisztrációjához és bejelentkezéséhez szükséges. Töltsön le egy ingyenes kétfaktoros hitelesítő alkalmazást, mint például a Microsoft Authenticator (Windows Phone, Android, iOS telefonra) vagy a Google Authenticator (Android, iOS telefonra).
2. Olvassa be az alábbi QR-kódot, vagy írja be ezt a kulcsot: **GVTDENDDMT2DSNLE** a telepített kétfaktoros hitelesítő alkalmazásába.
3. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg (ERA: [felhasználónév]) és egy dinamikusan változó egyedi kódot biztosít Önnek. Írja be a felületen megjelenő kódot az alábbi **Ellenőrzőkód** mezőbe, majd nyomja meg az **Ellenőrzés** gombot.

Ellenőrzőkód

Ellenőrzés

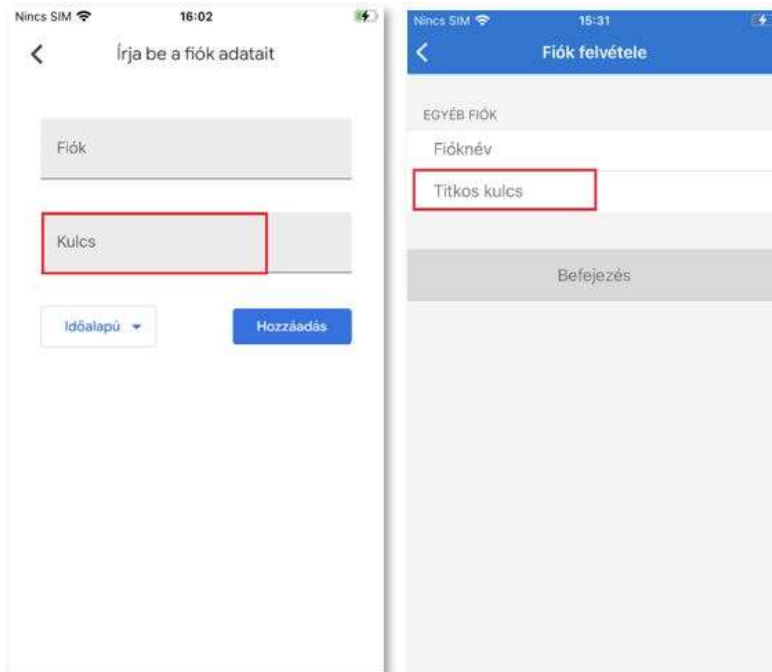
5. ábra: Kétfaktoros hitelesítés regisztrációs felülete, QR kód és kulcs

3. A mobiltelefon készülék hitelesítő alkalmazásában a QR kód beolvasásával ([3. Kétfaktoros azonosítás használatához szükséges előfeltétel](#)), vagy a beállítókulcs megadása opcióval új fiók kerül létrehozásra a hitelesítő alkalmazásban.



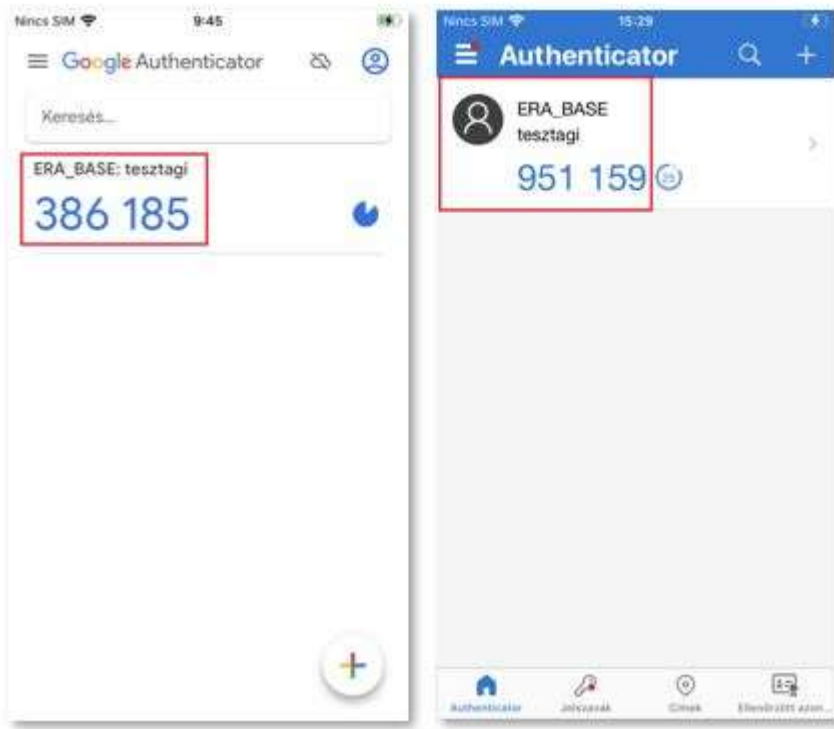
6. ábra: Hitelesítő alkalmazások, fiók beállítása

Utóbbi esetben a kulcs megadása mellett szükséges megadni mindkét hitelesítő alkalmazás esetén a „Fiók neve”-t, valamint a Google Authenticator esetén a „Kulcs típusa”-t is ki kell választani (időalapú).



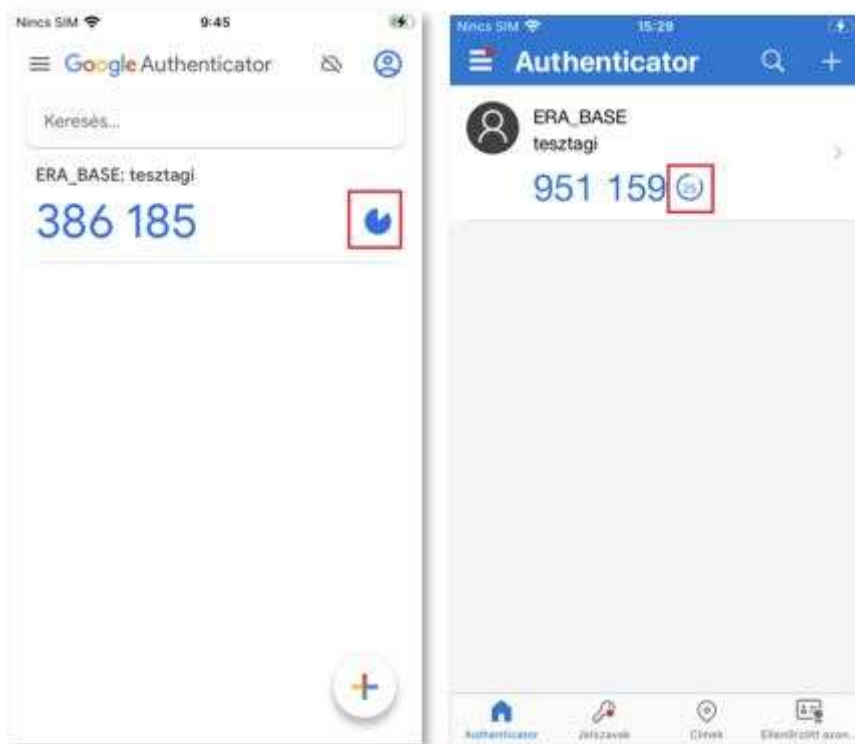
7. ábra: Hitelesítő alkalmazások, kétfaktoros hitelesítés regisztráció kulcs megadással

4. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg: *ERA: [felhasználónév] (a kulcs begépelése esetében a felhasználó által megadott fióknév).*



8. ábra: Hitelesítő alkalmazások, létrehozott fiók és generált kód

5. A létrehozott fiókhoz a hitelesítő alkalmazás automatikusan legenerálja az ellenőrzőkódot. Az ellenőrzőkód érvényességi ideje fél perc, az érvényességi idő lejártát követően az alkalmazás automatikusan új ellenőrzőkódot generál. Az ellenőrzőkód érvényességi idejének múlását az alkalmazás jelzi.



9. ábra: Hitelesítő alkalmazások, kód érvényességi ideje

6. Az ellenőrzőkód megadása az ERA *Kétfaktoros hitelesítés* felületén, majd az *Ellenőrzés* gombra szükséges kattintani.

ERAteszt3 - Teszt3

Kétfaktoros hitelesítés újragenerálás

Kétfaktoros hitelesítés

A felhasználónév-jelszó alapú bejelentkezés manapság már nem nyújt elég erős védelmet a felhasználó számára, ezért a személyes és üzleti adatainak védelme miatt az MNB bevezeti egy külső alkalmazás segítségével biztosított **kétfaktoros hitelesítést** az ERA-ba történő biztonságos bejelentkezés érdekében.

A hitelesítő alkalmazás használatához kövesse az alábbi lépéseket:

1. A kétfaktoros azonosítás előfeltétele egy Androidos, egy iOS vagy egy Windows phone mobilkészülék, valamint az arra telepített hitelesítő alkalmazás, amely a kétfaktoros azonosítás regisztrációjához és bejelentkezéséhez szükséges. Töltsön le egy ingyenes kétfaktoros hitelesítő alkalmazást, mint például a Microsoft Authenticator (Windows Phone, Android, iOS telefonra) vagy a Google Authenticator (Android, iOS telefonra).
2. Olvassa be az alábbi QR-kódot, vagy írja be ezt a kulcsot: `GVTDENDMMI2DSMLE` a telepített kétfaktoros hitelesítő alkalmazásába.
3. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg (ERA: [felhasználónév]) és egy dinamikusan változó egyedi kódot biztosít Önnek. Írja be a felületen megjelenő kódot az alábbi **Ellenőrzőkód** mezőbe, majd nyomja meg az **Ellenőrzés** gombot.

Ellenőrzőkód

Ellenőrzés

10. ábra: Kétfaktoros hitelesítés regisztrációs felülete, Ellenőrzőkód

7. A sikeres azonosítást követően az ERA kezdőképernyőre navigál a rendszer.

ERA - Étes

Kezdőlap HU

Bejelentkezési adatok

Kilépés

Regisztrációs adatbázis

Képviselet intézmény

Intézményválasztás

Szolgáltatások

Üdvözöljük az ERA oldalán!

A Magyar Nemzeti Bank (MNB) elektronikus rendszere hitelesített adatok fogadásához (ERA) lehetőséget biztosít a regisztrált felhasználóknak/intézményeknek, hogy az MNB egyes szolgáltatásait egységes felületen keresztül érhessek el.

- ERA technikai információk
- Az alkalmazással kapcsolatos kérdéseiket telefonon - munkanapokon 8-17 óráig - a **06(1) 550-1853** telefonszámon fogadjuk.
- Elektronikus levélben az mnb@1818.hu címre várjuk észrevételeiket, kérdéseiket. **Technikai hibabejelentések esetén kérjük minden esetben a képernyőképet mellékelten megküldeni részünkre.**

Az ERA használatához előzetes regisztráció szükséges az MNB Regisztrációs Adatbázisában. A regisztrációhoz szolgáltatástól függően elektronikus aláíró tanúsítvány vagy ügyfélkapus regisztráció szükséges.

Az ERA-ban a felhasználó a regisztráció során megjelölt és az MNB által jóváhagyott szolgáltatásokat használhatja. Az ERA felületéről elérhető a regisztrációval kapcsolatos adminisztrációs felület is.

Amennyiben Ön korábban már regisztrált az adatszolgáltatás illetve a közzététel szolgáltatásokhoz, nem kell ismételtan a teljes regisztrációs folyamatot újra elvégezni, hanem a már meglévő felhasználónévvel és jelszóval belépni az ERA felületére, a RegDB menüpont „Intézmények-szolgáltatások” almenü pontját kiválasztva a „Szolgáltatások bővítése” gombra kattintva regisztrálhat további szolgáltatásokhoz.

Az ERA oktatórendszerén keresztül, az ERA felületén található folyamatok kipróbálhatóak, regisztrációt követően.

Megjegyzés: Az ERA egyes szolgáltatásai olyan funkciókat használnak, amelyekhez szükséges a Ponte webes digitális aláíró alkalmazás, illetve az MNBSigner aláíró alkalmazás telepítése. A Ponte WDAP alkalmazás automatikusan települ az első bejelentkezéskor, kérjük, amennyiben a böngésző megkérdézi, engedélyezze a vezérlő telepítését. A telepítőkészletek letölthetők [ezen a linken](#).

Az ERA-val kapcsolatos technikai tudnivalókat a következő [linken](#) találja.

Technikai jellegű problémájával, kérjük forduljon a Helpdesk szolgáltatásunkhoz, a következő elérhetőségek egyikén:

- Az alkalmazással kapcsolatos kérdéseiket telefonon - munkanapokon 8-17 óráig - a **06(1) 550-1853** telefonszámon fogadjuk.
- Elektronikus levélben az mnb@1818.hu címre várjuk észrevételeiket, kérdéseiket.

Tájékoztató az ERA műtbéli és tervezett leállításairól [itt](#).

11. ábra: ERA kezdőképernyő, a bejelentkezett felhasználó

8. Sikertelen azonosítás esetén hibaüzenetet ad vissza a rendszer. A felhasználó a **Kétfaktoros hitelesítés** felületéről nem kerül elnavigálásra. A hibás ellenőrzőkódot a mezőből törölve, lehetősége van a helyes ellenőrzőkód újbóli megadására.

A sikertelen azonosítás okai lehetnek:

- Hibás ellenőrzőkód megadása
- Lejárt ellenőrzőkód megadása
- Üresen hagyott Ellenőrzőkód mező
- Újraregisztrálást követően az alkalmazásban nem kerül törlésre az alkalmazásban korábban létrejött felhasználó és QR kód beolvasás nélkül kerül az ellenőrzőkód megadásra

3. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg (ERA: [felhasználónév]) és egy dinamikusan változó egyedi kódot biztosít Önnek. Írja be a felületen megjelenő kódot az alábbi **Ellenőrzőkód** mezőbe, majd nyomja meg az **Ellenőrzés** gombot.

Ellenőrzőkód

111111

Érvénytelen az ellenőrzőkód. Kérjük, adja meg újra!

Ellenőrzés

12. ábra: Kétfaktoros hitelesítés regisztráció, érvénytelen ellenőrzőkód

3. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg (ERA: [felhasználónév]) és egy dinamikusan változó egyedi kódot biztosít Önnek. Írja be a felületen megjelenő kódot az alábbi **Ellenőrzőkód** mezőbe, majd nyomja meg az **Ellenőrzés** gombot.

Ellenőrzőkód

Érvénytelen ellenőrzőkód. Az ellenőrzőkód megadása kötelező!

Ellenőrzés

13. ábra: Kétfaktoros hitelesítés regisztráció, üresen hagyott Ellenőrzőkód mező

4.3. Kétfaktoros azonosítással történő bejelentkezés

A kétfaktoros azonosítással történő bejelentkezés lépései:

1. Bejelentkezés az ERA keretrendszerbe a felhasználónév és a jelszó megadásával, valamint a captcha kitöltésével.
2. Megjelenítésre kerül a *Kétfaktoros hitelesítés* felülete.
3. A felületen található Ellenőrzőkód mezőbe a mobilalkalmazás által, a korábban létrehozott fiókhoz (ERA: [felhasználónév]) generált aktuális, érvényes ellenőrzőkódot szükséges megadni. Az alkalmazásban az ellenőrzőkódok érvényességi idejének (fél perc) lejártát követően folyamatosan újragenerálódnak, így lehetősége van a felhasználónak az Ellenőrzőkód újbóli megadására szükség esetén.

ERAteszt3 - Teszt3

Kétfaktoros hitelesítés

Kezdőlap

Bejelentkezési adatok

Kilépés

Információk

Kétfaktoros hitelesítés

Kérem, nyissa meg a mobilkészülékén a hitelesítő alkalmazást és írja be az alábbi Ellenőrzőkód mezőbe a hitelesítő alkalmazás által, a korábban létrehozott fiókhoz (ERA: [felhasználónév]) generált aktuális, érvényes ellenőrzőkódot. Az Ellenőrzés gomb megnyomását követően, sikeres azonosítás esetén a rendszer belépteti, ezt követően elérhetők a regisztrált intézmények és szolgáltatások.

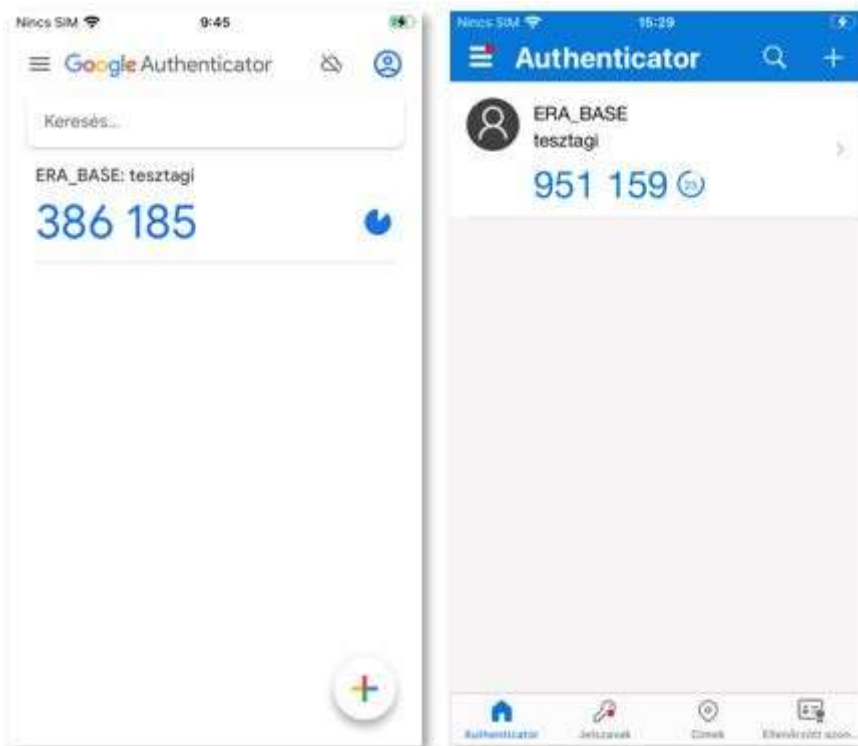
Ellenőrzőkód

Ellenőrzés

Amennyiben eszközt cserélt, elvesztette mobilkészülékét, vagy a generált kóddal nem tud belépni, kérem kattintson a **Kétfaktoros hitelesítés visszaállítás** gombra és indítsa el újra a kétfaktoros hitelesítés regisztrációját. A gombra kattintást követően automatikus e-mail kerül kiküldésre a felhasználó ERA-ban regisztrált és megerősített e-mail címére.

Kétfaktoros hitelesítés visszaállítás

14. ábra: Kétfaktoros hitelesítés bejelentkezés, ellenőrzőkód



15. ábra: Hitelesítő alkalmazások, ellenőrzőkód

4. Az *Ellenőrzés* gomb megnyomását követően, sikeres azonosítás esetén a rendszer belépteti a felhasználót, ezt követően elérhetőek a regisztrált intézmények és a szolgáltatások.



16. ábra: Kétfaktoros hitelesítés bejelentkezés, ellenőrzés gomb

ERA - Étes

Kezdőlap HU

Bejelentkezési adatok

Kilépés

Regisztrációs adatbázis

Képviselet intézmény

Intézményválasztás

Szolgáltatások

Üdvözöljük az ERA oldalán!

A Magyar Nemzeti Bank (MNB) elektronikus rendszere hitelesített adatok fogadásához (ERA) lehetőséget biztosít a regisztrált felhasználóknak/intézményeknek, hogy az MNB egyes szolgáltatásait egységes felületen keresztül érhessek el.

- ERA technikai információk
- Az alkalmazással kapcsolatos kérdéseiket telefonon - munkanapokon 8-17 óráig - a **06(1) 550-1853** telefonszámon fogadjuk.
- Elektronikus levélben az mnb@1818.hu címre várjuk észrevételeiket, kérdéseiket. **Technikai hibabejelentések esetén kérjük minden esetben a képernyőképet mellékelten megküldeni részünkre.**

Az ERA használatához előzetes regisztráció szükséges az MNB Regisztrációs Adatbázisában. A regisztrációhoz szolgáltatástól függően elektronikus aláíró tanúsítvány vagy ügyfélkapus regisztráció szükséges.

Az ERA-ban a felhasználó a regisztráció során megjelölt és az MNB által jóváhagyott szolgáltatásokat használhatja. Az ERA felületéről elérhető a regisztrációval kapcsolatos adminisztrációs felület is.

Amennyiben Ön korábban már regisztrált az adatszolgáltatás illetve a közzététel szolgáltatásokhoz, nem kell ismételt a teljes regisztrációs folyamatot újra elvégezni, hanem a már meglévő felhasználónévvel és jelszóval belépni az ERA felületére, a RegDB menüpont „Intézmények-szolgáltatások” almenü pontját kiválasztva a „Szolgáltatások bővítése” gombra kattintva regisztrálhat további szolgáltatásokhoz.

Az ERA oktatórendszerén keresztül, az ERA felületén található folyamatok kipróbálhatóak, regisztrációt követően.

Megjegyzés: Az ERA egyes szolgáltatásai olyan funkciókat használnak, amelyekhez szükséges a Ponte webes digitális aláíró alkalmazás, illetve az MNBSigner aláíró alkalmazás telepítése. A Ponte WDAP alkalmazás automatikusan települ az első bejelentkezéskor, kérjük, amennyiben a böngésző megkérdézi, engedélyezze a vezérlő telepítését. A telepítőkészletek letölthetők ezen a linken.

Az ERA-val kapcsolatos technikai tudnivalókat a következő [linken](#) találja.

Technikai jellegű problémájával, kérjük forduljon a Helpdesk szolgáltatásunkhoz, a következő elérhetőségek egyikén:

- Az alkalmazással kapcsolatos kérdéseiket telefonon - munkanapokon 8-17 óráig - a **06(1) 550-1853** telefonszámon fogadjuk.
- Elektronikus levélben az mnb@1818.hu címre várjuk észrevételeiket, kérdéseiket.

Tájékoztató az ERA műtbéli és tervezett leállításairól [itt](#).

17. ábra: ERA kezdőképernyő, bejelentkezett felhasználó

5. Amennyiben az azonosítás sikertelen, az ERA rendszer hibaüzenetet ad vissza.

A sikertelen azonosítás okai lehetnek:

- Érvénytelen ellenőrzőkód megadása
- Lejárt ellenőrzőkód megadása
- Üresen hagyott Ellenőrzőkód mező
- A hitelesítő alkalmazásban több, azonos felhasználónévvel rendelkező fiókhoz (amennyiben újraregisztálást követően nem került törlésre a korábbi felhasználói fiók) is generálódnak ellenőrzőkódok, a felhasználó nem az aktív fiókhoz generálódó ellenőrzőkódot adja meg.

Kezdőlap HU

Bejelentkezési adatok

Kilépés

Információk

Kétfaktoros hitelesítés

Kérem, nyissa meg a mobilkészülékén a hitelesítő alkalmazást és írja be az alábbi **Ellenőrzőkód** mezőbe a hitelesítő alkalmazás által, a korábban létrehozott fiókhoz (ERA: [felhasználónév]) generált aktuális ellenőrzőkódot. Az **Ellenőrzés** gomb megnyomását követően, sikeres azonosítás esetén a rendszer belépteti, ezt követően elérhetők a regisztrált intézmények és szolgáltatások.

Ellenőrzőkód 1111111

Érvénytelen az ellenőrzőkód. Kérjük, adja meg újra!

Ellenőrzés

18. ábra: Kétfaktoros hitelesítés bejelentkezés, sikertelen azonosítás, érvénytelen vagy lejárt ellenőrzőkód

The screenshot shows a web interface for two-factor authentication. On the left is a dark blue sidebar with navigation links: 'Kezdőlap' (Home), 'Bejelentkezési adatok' (Login data), 'Kilépés' (Logout), and 'Információk' (Information). The main content area is titled 'Kétfaktoros hitelesítés' (Two-factor authentication). Below the title, there is a paragraph of instructions in Hungarian. A red box highlights the 'Ellenőrzőkód' (Verification code) input field, which is empty. Below the input field, a red error message reads: 'Érvénytelen ellenőrzőkód. Az ellenőrzőkód megadása kötelező!' (Invalid verification code. Providing the verification code is mandatory!). At the bottom of the highlighted area is an 'Ellenőrzés' (Verify) button.

Kezdőlap ? i HU

Bejelentkezési adatok

Kilépés

Információk

Kétfaktoros hitelesítés

Kérem, nyissa meg a mobilkészülékén a hitelesítő alkalmazást és írja be az alábbi **Ellenőrzőkód** mezőbe a hitelesítő alkalmazás által, a korábban létrehozott fiókhoz (ERA: [felhasználónév]) generált aktuális ellenőrzőkódot. Az **Ellenőrzés** gomb megnyomását követően, sikeres azonosítás esetén a rendszer belépteti, ezt követően elérhetők a regisztrált intézmények és szolgáltatások.

Ellenőrzőkód

Érvénytelen ellenőrzőkód. Az ellenőrzőkód megadása kötelező!

Ellenőrzés

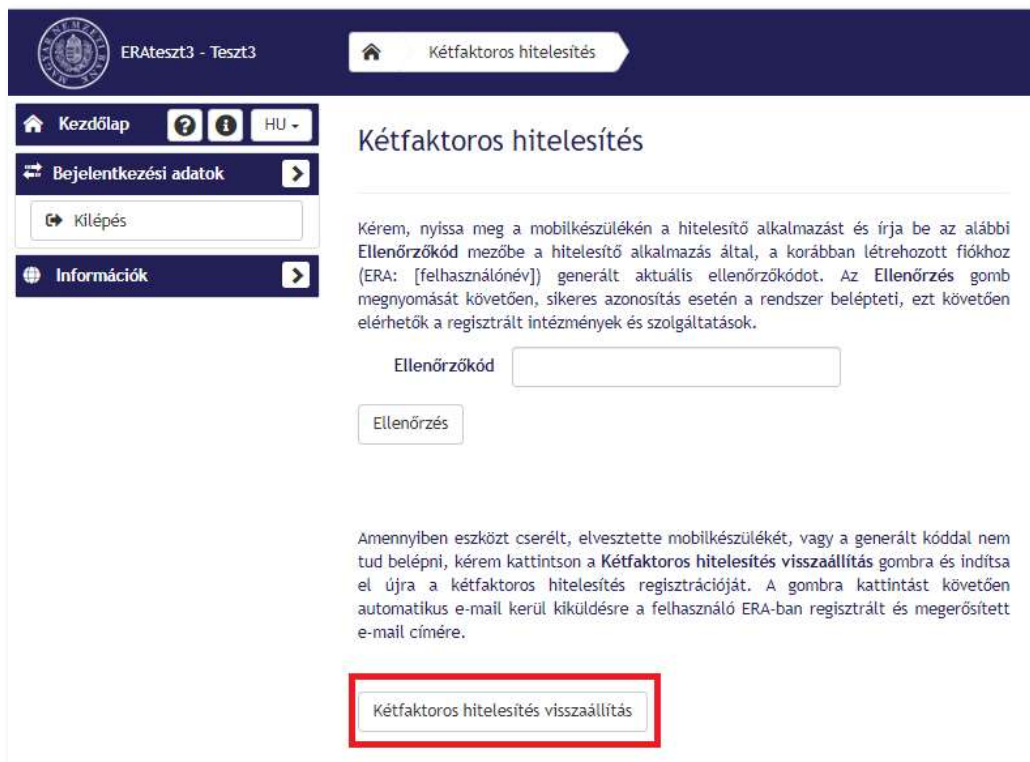
19. ábra: Kétfaktoros hitelesítés bejelentkezés, sikertelen azonosítás, üresen hagyott Ellenőrzőkód mező

4.4. Kétfaktoros hitelesítés visszaállítása

Amennyiben a felhasználó a kétfaktoros azonosítás regisztrációját követően elveszíti vagy lecseréli mobiltelefon készülékét, vagy a generált kóddal nem tud belépni, biztosított a lehetőség a kétfaktoros azonosítás visszaállítására, valamint egy új kétfaktoros hitelesítés regisztráció elindítására.

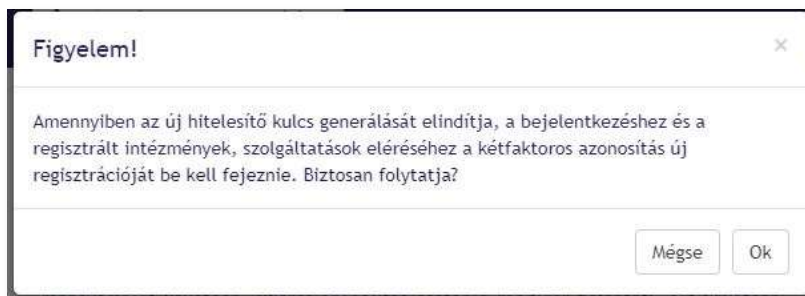
A kétfaktoros azonosítás visszaállításának lépései:

1. Bejelentkezés az ERA keretrendszerbe felhasználónév és jelszó megadásával, valamint a captcha kitöltésével.
2. Megjelenítésre kerül a Kétfaktoros hitelesítés felülete.
3. A felületen található *Kétfaktoros hitelesítés visszaállítás* gombra kattintással kezdeményezhető a kétfaktoros hitelesítés visszaállítása.



20. ábra: Kétfaktoros hitelesítés visszaállítása

4. A gombra kattintást követően felugró ablakban a felhasználónak meg kell erősítenie, hogy valóban vissza kívánja állítani a kétfaktoros hitelesítést.



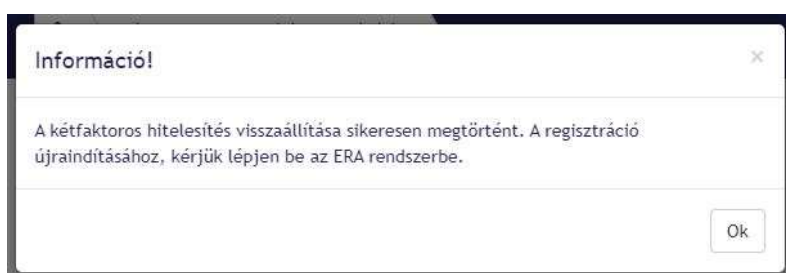
21. ábra: Kétfaktoros hitelesítés visszaállítása, figyelmeztető üzenet

5. Amennyiben elveti a lehetőséget (a *Mégse* gombra kattintással), a felületen folytathatja a kétfaktoros bejelentkezést az Ellenőrzőkód megadásával.
6. A visszaállításra vonatkozó figyelemfelhívó üzenet megerősítése esetén (*Ok* gombbal) a felhasználó számára tájékoztató üzenet kerül megjelenítésre, a visszaállításhoz szükséges e-mail kiküldésére vonatkozóan. Ezt jóváhagyva (az *OK* gombra kattintással) „Kétfaktoros hitelesítés visszaállítása” tárgyú, automatikus e-mail kerül kiküldésre a felhasználó korábban, az ERA regisztráció során megadott e-mail címére.



22. ábra: Kétfaktoros hitelesítés visszaállítása, tájékoztató az e-mail küldésről

7. Az automatikus e-mail egy linket tartalmaz, melyre (az e-mailben szereplő érvényességi időn belül) kattintva a kétfaktoros azonosítás regisztrációja alaphelyzetbe (nem regisztrált állapotba) állítható.
8. A linkre kattintva, amennyiben nem talál hibát a rendszer, a *Kétfaktoros hitelesítés visszaállítás* felületen felugró ablakban kerül megjelenítésre a sikeres visszaállításra vonatkozó tájékoztató. Ezt jóváhagyva (az *OK* gombra kattintással) a rendszer az ERA kezdőoldalára navigálja a felhasználót.



23. ábra: Kétfaktoros hitelesítés sikeres visszaállítása, tájékoztató üzenet

9. Sikeres bejelentkezést követően megjelenítésre kerül a Kétfaktoros azonosítás regisztrációs felülete, ahol a felhasználó újra elvégezheti a regisztrációt.

Az automatikus e-mailben lévő linkre kattintva, ha hibát talál a rendszer, hibaüzenet kerül megjelenítésre a felugró ablakban.

A sikertelenség okai lehetnek:

- a. a felhasználó korábban már felhasználta a linket:



24. ábra: Kétfaktoros hitelesítés, link újra felhasználása, tájékoztató üzenet

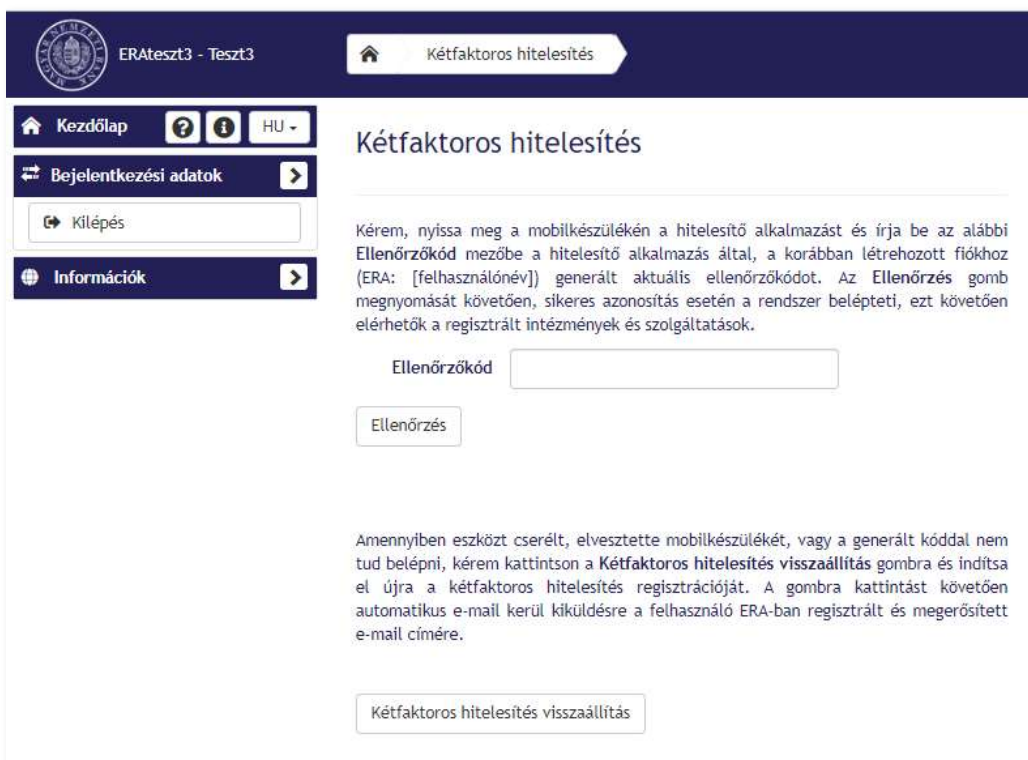
A tájékoztató üzenet jóváhagyását követően (az *OK* gombra kattintással), az ERA kezdőoldala kerül megjelenítésre, ahol a felhasználó be tud jelentkezni az ERA rendszerbe. Sikeres bejelentkezést követően megjelenítésre kerül a *Kétfaktoros azonosítás regisztrációs* felülete, ahol a felhasználó újra elvégezheti a kétfaktoros azonosításra történő regisztrációt.

- b. a felhasználó az érvényességi időn túl szeretné felhasználni a visszaállító linket – lejárt érvényességi idő hiba:



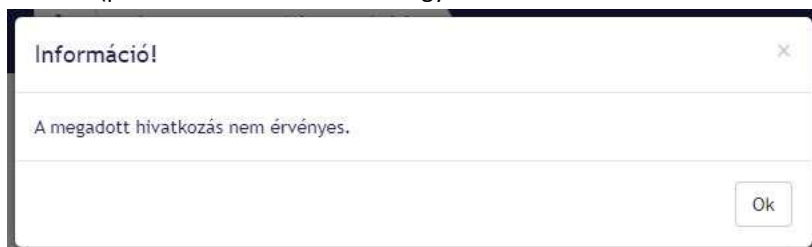
25. ábra: Kétfaktoros hitelesítés, link érvényességi idejének lejárata, tájékoztató üzenet

A tájékoztató üzenet jóváhagyását követően (az *OK* gombra kattintással), az ERA kezdőoldal kerül megjelenítésre, ahol a felhasználó be tud jelentkezni az ERA rendszerbe. A sikeres bejelentkezést követően a *Kétfaktoros hitelesítés* felületére navigálja a rendszer, ahol lehetősége van újabb visszaállítást kérni a *Kétfaktoros hitelesítés visszaállítás* gomb megnyomásával.



26. ábra: Kétfaktoros hitelesítés felülete

- c. hibás a link (például véletlenül törlésre vagy beírásra kerülnek az eredeti linkbe karakterek):



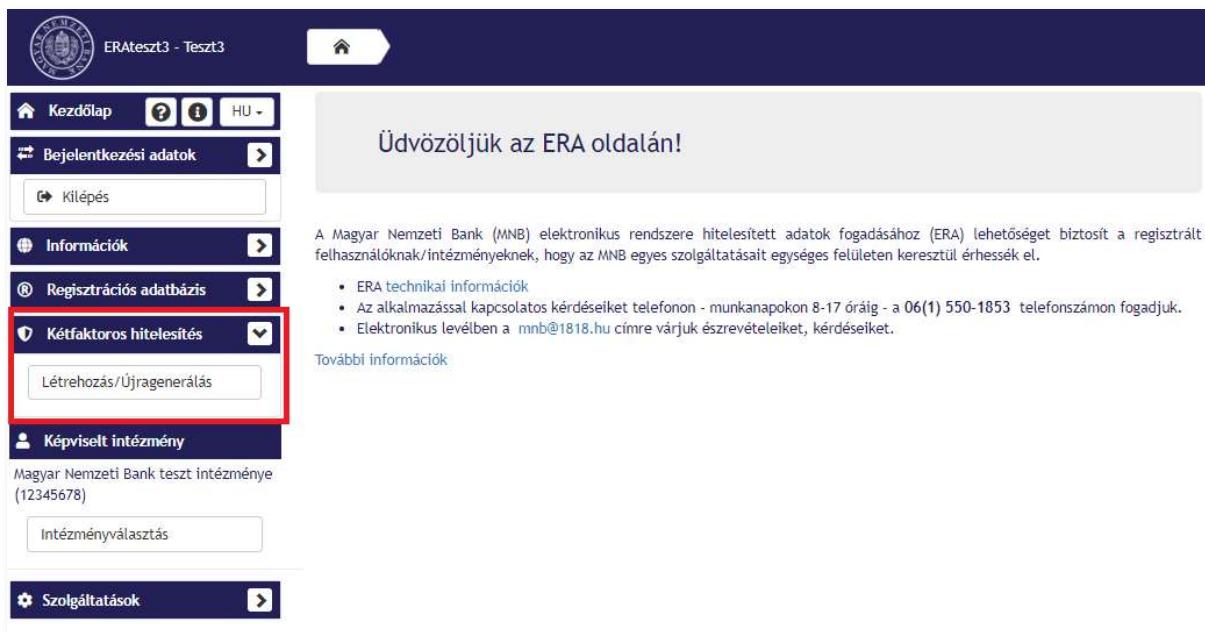
27. ábra: Kétfaktoros hitelesítés, érvénytelen link, tájékoztató üzenet

A tájékoztató üzenet jóváhagyását követően (az *OK* gombra kattintással), az ERA kezdőoldal kerül megjelenítésre, ahol a felhasználó be tud jelentkezni az ERA rendszerbe. Sikeres bejelentkezést követően a *Kétfaktoros hitelesítés* felületére navigálja a felhasználót a rendszer, ahol lehetősége van újabb visszaállítást kérni a *Kétfaktoros hitelesítés visszaállítás* gomb megnyomásával.

4.5. További tudnivalók a kétfaktoros azonosításról

4.5.1. Létrehozás/Újragenerálás funkciógomb

A kétfaktoros azonosítással történő bejelentkezést követően is bármikor elérhető a felhasználó számára a bal oldali menüben a *Kétfaktoros hitelesítés* menüpont *Létrehozás/Újragenerálás* funkciógomb. Amennyiben a kétfaktoros hitelesítéssel bejelentkezett felhasználó a *Létrehozás/Újragenerálás* gombra kattint, a rendszer jelzi számára, hogy már rendelkezik kétfaktoros hitelesítéssel.

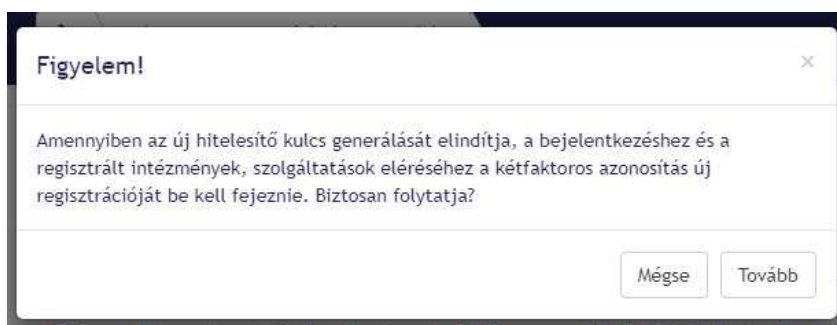


28. ábra: Kétfaktoros hitelesítés Létrehozás/Újragenerálás funkciógomb



29. ábra: Kétfaktoros hitelesítés új hitelesítő kulcs kérése gomb

Az *Új hitelesítő kulcs kérés* gombra kattintva, megjelenik egy felugró ablak, melyben a felhasználónak szükséges megerősíteni az újragenerálási szándékát:



30. ábra: Kétfaktoros hitelesítés új hitelesítő kulcs kérése, figyelmeztető üzenet

Amennyiben elveti a lehetőséget (*Mégse* gombbal), a felhasználó a Létrehozás/Újragerálás felületen marad, innen tud tovább navigálni.

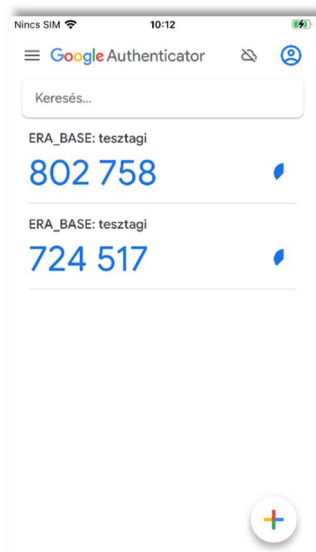
Az újragerálási szándék megerősítését (A *Tovább* gombra kattintást) követően pedig biztosított a lehetőség új hitelesítő kulcs generálásra. Megjelenik a *Kétfaktoros hitelesítés regisztráció* felülete, ahol a [4.2 Kétfaktoros azonosítás regisztráció](#) pontban leírtak szerint újra tud regisztrálni a felhasználó a kétfaktoros hitelesítésre.

Fontos, hogy amennyiben az új hitelesítő kulcs generálását elindítja a felhasználó, a bejelentkezéshez és a regisztrált intézmények, szolgáltatások eléréséhez a kétfaktoros azonosítás regisztrációját be kell fejeznie.



31. ábra: Kétfaktoros hitelesítés regisztrációs felülete

Abban az esetben, ha a mobilalkalmazásban a korábban regisztrált felhasználó nem került törlésre (az alkalmazásban továbbra is megjelenik a korábban létrehozott fiók (ERA: [felhasználónév]) és generálódnak az ellenőrzőkódok), szükséges a QR kód újra beolvasása, nem elegendő a korábbi felhasználóhoz generált ellenőrzőkód megadása. Amennyiben ezen ellenőrzőkód kerül megadásra, hibaüzenetet jelenít meg a rendszer:



32. ábra: Hitelesítő alkalmazás, korábban és újonnan regisztrált fiók is megjelenik

3. A hitelesítő alkalmazás a sikeres QR kód beolvasását vagy a kulcs megadást követően új fiókot jelenít meg (ERA: [felhasználónév]) és egy dinamikusan változó egyedi kódot biztosít Önnek. Írja be a felületen megjelenő kódot az alábbi Ellenőrzőkód mezőbe, majd nyomja meg az Ellenőrzés gombot.

Ellenőrzőkód

072915

Érvénytelen az ellenőrzőkód. Kérjük, adja meg újra!

Ellenőrzés

33. ábra: Korábban regisztrált fiókhoz generált ellenőrzőkód megadását követően hibaüzenet jelenik meg, új hitelesítő kulcs kérését követően

A mobilalkalmazásban, amennyiben a korábban regisztrált felhasználó nem került törlésre, továbbra is megjelenik a korábban létrehozott fiók (ERA: [felhasználónév]). Ekkor a QR kód beolvasását követően a két hitelesítő alkalmazásban a következőket tapasztalja a felhasználó:

- Google Authenticator:
 - Újabb fiókot hoz létre az alkalmazás (ERA: [felhasználónév]).
 - A korábbi fióko(ka)t a felhasználónak lehetősége van törölni az alkalmazásból. A törlési szándékot a felhasználónak szükséges megerősíteni.
- Microsoft Authenticator: „Ez a művelet felülírja „felhasználónév” fiókjának meglévő biztonsági adatait. A fiókjából való kizárás elkerülése érdekében csak akkor folytassa, ha megbízható forrásból kezdeményezte a műveletet.”). A felhasználó két opció közül választhat:
 - Angolul: Cancel/magyarul: Megszakítás – ebben az esetben a felhasználó elveti az új fiók létrehozását. Azonban a régi fiókhoz generálódó ellenőrzőkódok már nem lesznek érvényesek.
 - Angolul: Continue/magyarul: Folytatás:

- Apple iOS esetében az alkalmazásban létrejön a felhasználó új fiókja, az ehhez generálódó ellenőrzőkód segítségével tud a felhasználó bejelentkezni
- Google Android esetében az alkalmazásban manuálisan szükséges a fióknevet és kulcsot megadni, ahhoz, hogy az új fiók létrejöhön. A korábbi felhasználói fiók törlése és a szándék megerősítése szükséges.

Fontos, hogy amennyiben a felhasználó az alkalmazásban manuálisan adta meg korábban a kulcsot és egyedi elnevezésű fiókot hozott létre, majd a kétfaktoros hitelesítés újragenerálása során beolvassa a QR kódot, a hitelesítő alkalmazások a fiókok egyezőségét nem ismerik fel, így megőrzik a korábban létrehozott fiókot is. A korábbi fiókhoz generálódó kódok, azonban már a bejelentkezéshez nem lesznek érvényesek, a korábbi fiók törlése szükséges.

Amennyiben az alkalmazásban újonnan létrehozott fiókhoz generált ellenőrzőkód megadását követően a felhasználó újregisztrációja sikeres, a felhasználó a kezdőképernyőre navigál.