Kétfaktoros hitelesítés Neptunban

Tartalomjegyzék:

A kétfaktoros hitelesítés (2FA, azaz Two Factor Authentication) egy olyan biztonsági beállítás, amely lehetővé teszi a felhasználók számára, hogy második biztonsági réteget adhassanak a fiókjukhoz, ezzel erősítve adataik védelmét. Ez a módszer két különböző információs elemből áll. Az első része minden esetben a felhasználónév és a jelszó megadására épít, a második része egy dinamikusan változó elem, mely maga a 2FA token. Ezen két elem kombinálása biztosítja a rendszerbe történő bejelentkezést. Ebben a folyamatban, ha egy tényező hibás vagy hiányzik, akkor a felhasználót nem lehet hitelesíteni, és sikertelen lesz a bejelentkezése a rendszerbe.

Használatának előnye, hogy abban az esetben, ha illetéktelen személy hozzá jut a felhasználó jelszavához, akkor a kétlépcsős azonosítás megakadályozza a rendszerbe való belépést. Ezen lehetőség használatával a felhasználók jobban tudják védeni adataikat.

A lehetőség opcionálisan elérhető bármely felhasználó számára a tanulmányi rendszerben.

1. Authentikátorok

A funkció használatához a felhasználónak rendelkeznie kell egy telepített asztali/telefonos alkalmazással, mely képes TOTP alapú kulcsot használni. Az alkalmazást a funkció használata előtt érdemes telepíteni. A javasolt három telefonos alkalmazás elérhető Androidon a Google Play-en és IOS-en is az App Storeban.

A regisztráció folyamata a kapcsolódó fejezetekben kerül ismertetésre.

2. Javasolt telefonos alkalmazások

Google Authenticator:

• Android: https://play.google.com/store/search?q=google+authenticator&c=apps&hl=hu

• IOS: https://apps.apple.com/hu/app/google-authenticator/id388497605

Microsoft Authenticator

• Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=hu

• IOS: https://apps.apple.com/hu/app/microsoft-authenticator/id983156458?l=hu

NISZ Hitelesítő:

• Android: https://play.google.com/store/apps/details?id=hu.innobile.niszauth&hl=hu

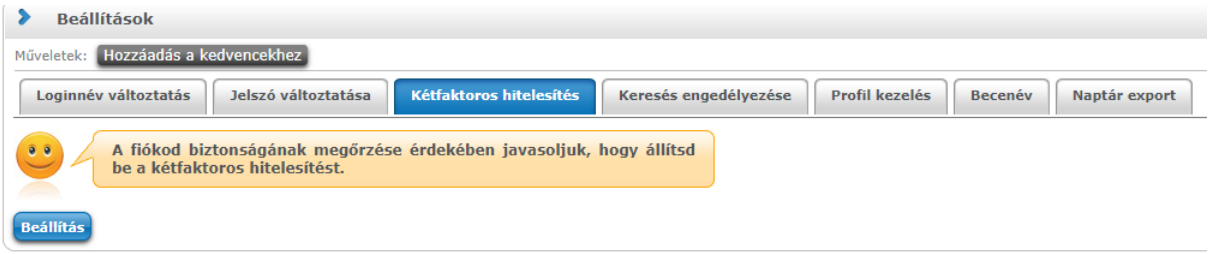
• IOS: https://apps.apple.com/hu/app/nisz-hiteles%C3%ADt%C5%91/id1603444961?l=hu

3. Javasolt asztali alkalmazás

Az egyik elterjedtebb az a „*FortiToken Windows*”, de manapság a jelszó menedzserek is képesek már ezeknek a kulcsoknak a tárolására. A „*FortiToken Windows*”-t a Microsoft Storeból lehet letölteni.

4. Regisztráció folyamata

Neptun belépést követően a *„Saját adatok/Beállítások”* menüponton a *„Kétfaktoros hitelesítés”* tabulátorfülön az alábbi információ jelenik meg, ha a felhasználónak nincs beállítva a kétfaktoros regisztrációja: *„A fiókod biztonságának érdekében javasoljuk, hogy állítsd be a kétfaktoros hitelesítést.”* A **„Beállítás”** gombra kattintva az alábbi ablak jelenik meg:



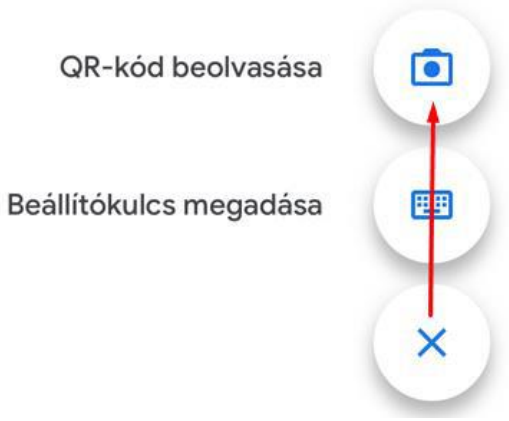
Még nem regisztrált kétfaktor

Belépést követő kétfaktor regisztráció

5. Példák az authentikátorok használatára

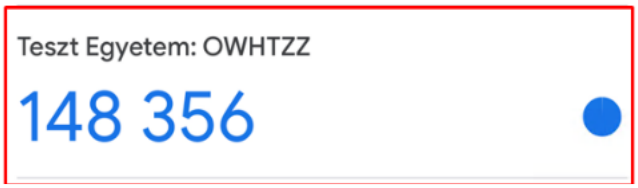
a. Google authenticatort használva

Megnyitjuk az alkalmazást, majd jobb alul a + jelre kattintva a *„QR kód beolvasása”* lehetőséget szükséges választani.



Kulcs létrehozása

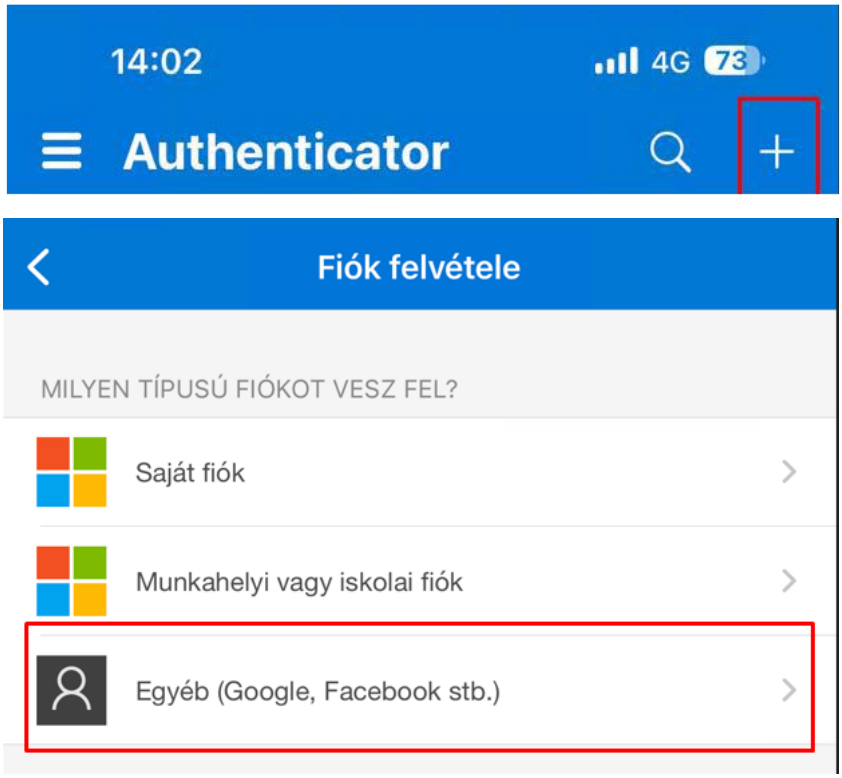
A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcs neve és Generált kód

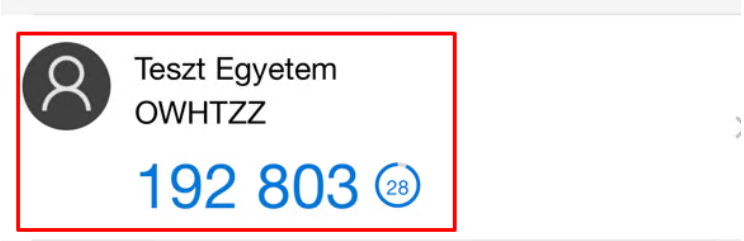
b. Microsoft Authenticatort használva

Megnyitjuk az alkalmazást, majd jobb alul a + jelre kattintva a megjelenő opcióknál az *„Egyéb (Google, Facebook stb.)”* opciót kell választani.



Kulcs létrehozása

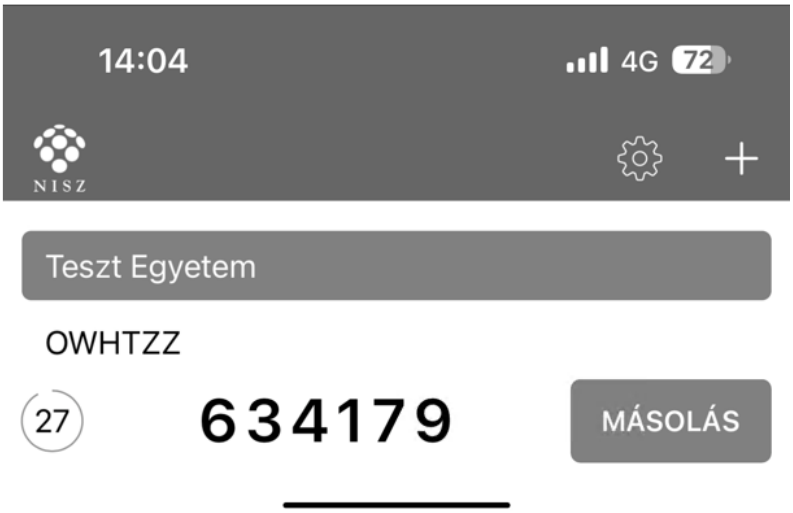
A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcs neve és Generált kód

c. NISZ Hitelesítőt használva

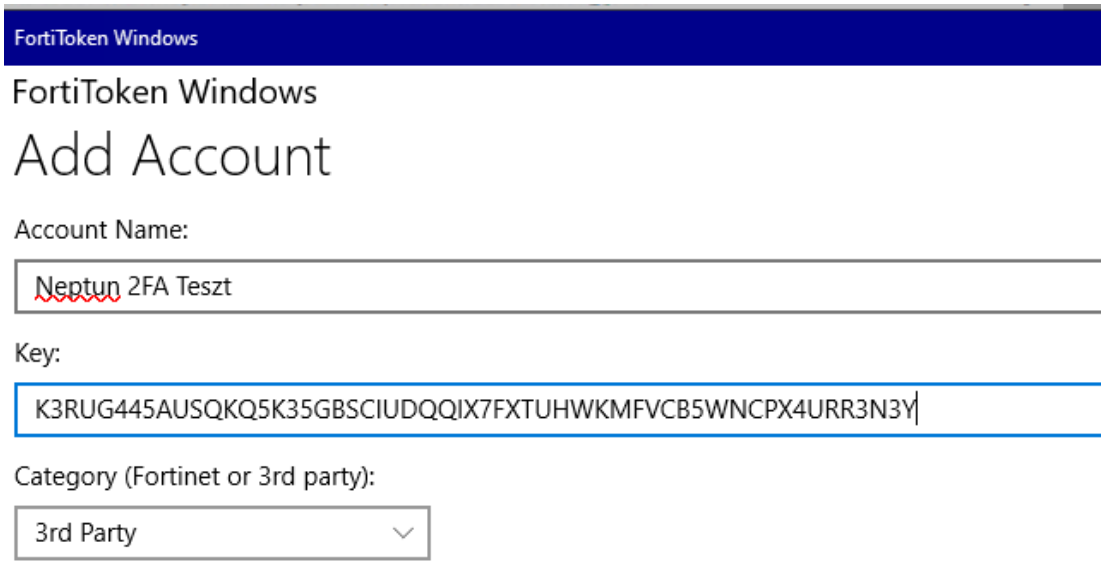
Az alkalmazást megnyitva jobb felül a + jelre kattintva csak bekell olvasni a képernyőről a QR kódot. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcs neve és Generált kód

d. FortiTokent használva

A letöltést követően meg kell nyitni az alkalmazást. Megnyitva a felület jobb alsó részén a „+” ikonnal ellátott **„Add”** gombra kattintva kezdhető meg a beállítás. *„Account Name”*-nek bármit megadhatunk, ez lesz a neve a kulcsunknak, mi nevezzük el amire szeretnénk. A *„Key”* mezőben azt a kulcsot kell majd megadnunk, ami a Neptunban a regisztrációs ablakban jelenik meg, ha a **„Mutasd a kódot”** gombra kattintunk. A *„Category”* mezőben pedig a *„3rd Party”* lehetőséget kell kiválasztani.



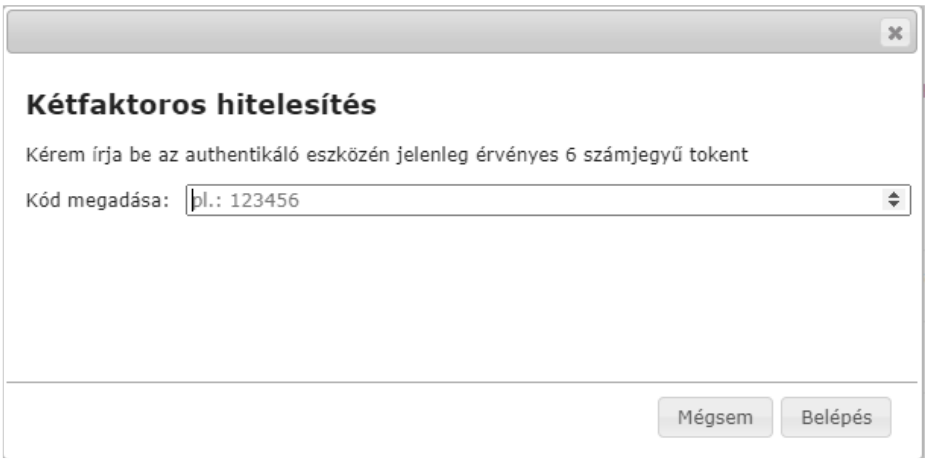
Adatok kitöltése

Az adatok megadását követően a felület jobb alsó felén rákattintunk a jobb alul megnyomjuk a pipával ellátott **„Done”** feliratú gombra.

Generált kód

6. Belépés menete kétfaktorhoz kötötten

Amennyiben a felhasználó rendelkezik regisztrált kétfaktoros hitelesítéssel, akkor a felhasználónév (azonosító) és jelszó megadását követően megjelenik a „*Kétfaktoros hitelesítés*” felugróablak, melyben az egyedi, 6 számjegyű token megadása szükséges a továbblépéshez.



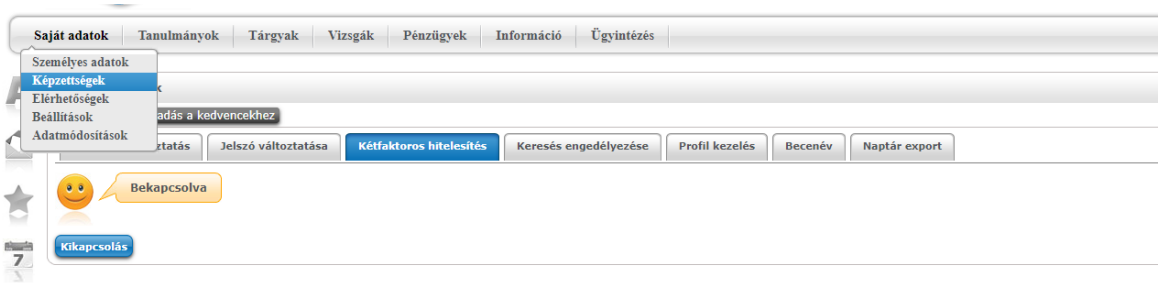
Token megadása

Az aktuális token kizárólag a felhasználó auhentikátorjában érthető el.

7. Kétfaktoros hitelesítés használatának kikapcsolása

a. Saját részre

A hallgatói- és az oktatói weben a belépést követően a „*Saját adatok/Beállítások*” menüponton a „*Kétfaktoros hitelesítést*” tabulátorfülön a **„Kikapcsolás”** gombra kattintva kapcsolható ki. A kikapcsoláshoz egyik esetben sincs szükség második faktoros azonosításra.



Kikapcsolás

b. Saját kérésre intézmény által

Abban az esetben, ha a felhasználó nem tud belépni a rendszerbe, akkor az intézmény felé jelezve a problémát kérheti a kikapcsolást.

Hallgatók a KTH-ban fogadási időben személyesen, vagy a neptun@bme.hu email címen jelezve a problémát, online személyazonosítás után tehetik ezt meg.

Oktatók az adott Kar Dékáni Hivatalában az adminisztrátor munkatársakat tudják keresni ez ügyben.