Kétfaktoros hitelesítés beállítása a Neptun kliens felületén (dolgozók, ügyintézők részére)

1. Authentikátor (Hitelesítő alkalmazás) letöltése, telepítése

Telepítsük okoseszközünkre/számítógépünkre az alább javasolt Authentikátorok egyikét!

Okoseszközre:
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

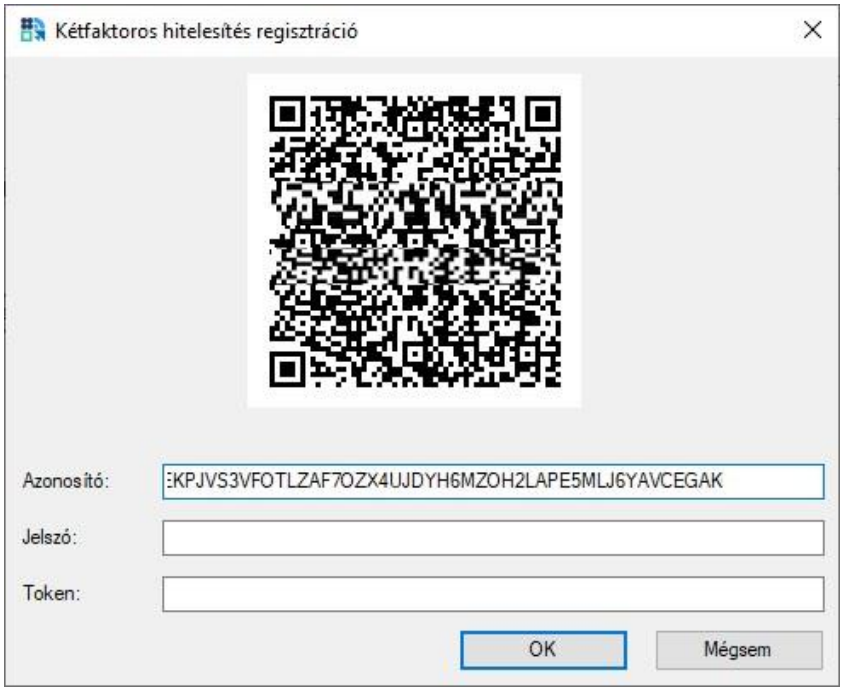
Számítógépre:
FortiToken:
Windows: https://apps.microsoft.com/store/detail/fortitokenwindows/9P0TDH1J7WFZ?hl=en-us&gl=us
macOS: https://apps.apple.com/us/app/fortitoken-mobile/id500007723

Step Two: https://steptwo.app/ csak macOS-re elérhető alkalmazás, amelyben a FortiTokenhez hasonlóan elvégezhető a kétfaktoros kulcs regisztrálása.

A felsorolt alkalmazások telepítése és használata ingyenes!

2. Kétfaktoros hitelesítés regisztráció bejelentkezést követően

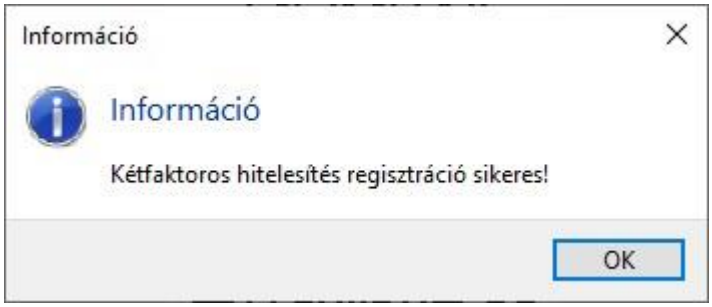
A **Kétfaktoros hitelesítés** regisztráció ablakban megjelenik egy QR kód, valamint a kódhoz tartozó Azonosító karaktersor gombra kattintva megjelenik a mezőben a QR kódhoz tartozó másolható karaktersor.



A választott Authentikátor programtól függően a **QR kód beolvasása és/vagy az Azonosító mezőben szereplő karaktersor kimásolásával** a 2. pontban szereplő lépéseknek megfelelően (Authentikátor programok használata/ kulcs létrehozása).

A **jelszó mezőbe** a Neptun belépéshez használt jelszót kell megadni.

A **Token mezőben a regisztrált Authentikátor program által generált 6 számjegyű számsort kell megadni**. Ügyelni kell az aktuális számsor megadására, mivel a számsor 30 másodpercenként változik!

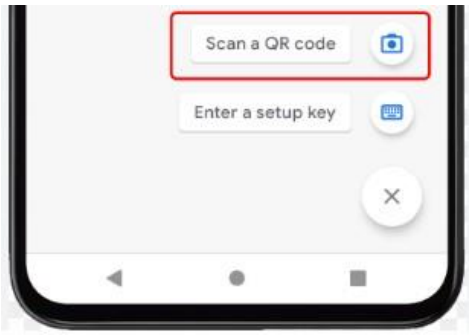


Az **Ok gombbal** véglegesíteni a beállítást, sikeres beállítás esetén a **Kétfaktoros regisztráció sikeres!** üzenet jelenik meg.

3. Authentikátor programok használata

Google Authenticator:

Az alkalmazás megnyitása után jobb oldalon alul lévő **+ jelre kattintva majd a QR-kód beolvasása (Scan a QR code)** gombbal lehet létrehozni a kulcsot a programban.



Kulcs létrehozása

A QR kód beolvasása után azonnal elkezdődik a kódgenerálás, a kulcs neve az intézmény neve (Soproni Egyetem), és a felhasználó Neptunkódja lesz.

Kulcs neve és generált kód

Az alkalmazás megnyitását követően a megjelenő kóddal lehet bejelentkezni a Neptunba.

Microsoft Authenticator:

Az alkalmazás megnyitása után jobb oldalon felül lévő **+ jelre kattintva lehet fiókot hozzáadni, az Egyéb fiók (Google, Facebook stb) opciót kiválasztva.**

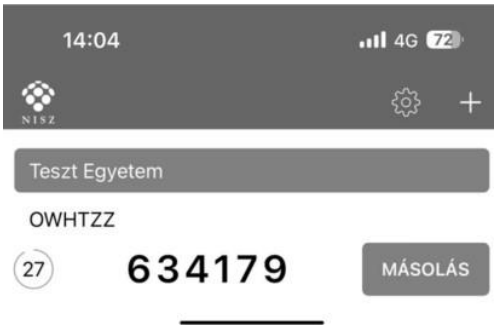
Kulcs létrehozása

A QR kód beolvasása után azonnal elkezdődik a kódgenerálás, a kulcs neve az intézmény neve (Soproni Egyetem), és a felhasználó Neptunkódja lesz.

Kulcs neve és generált kód

NISZ Hitelesítő

Az alkalmazás megnyitása után jobb oldalon felül lévő + jelre kattintva lehet QR kódot beolvasni, a a kulcs neve az intézmény neve (Soproni Egyetem), és a felhasználó Neptunkódja lesz.

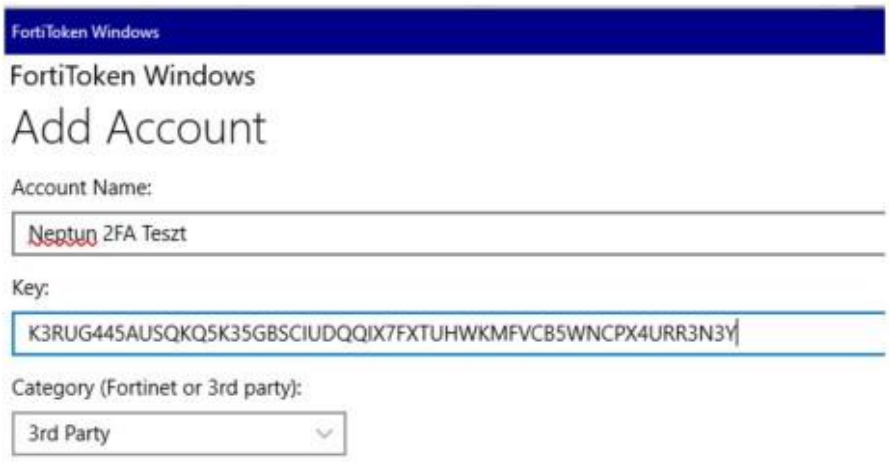


Kulcs neve és generált kód

FortiToken (asztali alkalmazás)

A letöltést és telepítést követően az alkalmazást megnyitva, a jobb alsó részen lévő **+ ikonnal megjelenő Add gombra** kattintva kezdhető a beállítás.

Account Name tetszőlegesen megadható, ez lesz a kulcs neve. A Key mezőbe a Neptunban a Mutasd a kódot gombra megjelenő kulcsot kell megadni, bemásolva az értéket, a Category mezőben a 3rd Party lehetőséget kell kiválasztani.



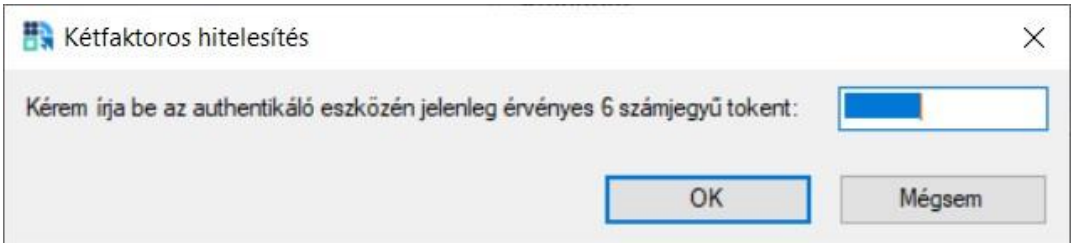
Adatok kitöltése

A kitöltést követően a jobb alul megjelenő **Done** gombbal kezdődik meg a kódgenerálás.

Kulcs neve és generált kód

4. Belépés kétfaktoros hitelesítéssel

Amennyiben sikeresen beállításra került a kétfaktoros hitelesítés, akkor az azonosító (Neptunkód) és a jelszó megadását követően megjelenik a **Kétfaktoros hitelesítés ablak, amelyben a belépéshez meg kell adni a 6 számjegyű egyszeri jelszót/tokent. A token a felhasználó authentikátor programjában érhető el.**



A token sikeres megadása után a szokásos módon a bejelentkezés megtörténik, és a korábbiaknak megfelelően használható a program. Újbóli belépés vagy újabb kliensprogram indításakor ismételten kérni fogja a rendszer az aktuális 6 számjegyű számsort, ami az authentikátor programból érhető el.

5. Egyéb Információk, segítség

A kétfaktoros hitelesítés feltételei:

- Hitelesítő alkalmazás megléte
  A Google Authenticator elérhető iOS 13.0 verzió vagy felett, Android 4.4 verzió vagy felett.
  A Microsoft Authenticator elérhető iOS 11.0 verzió vagy felett, Android 6.0 verzió vagy felett.
  A NISZ Hitelesítő elérhető iOS 11.0 verzió vagy felett, Android 4.1 verzió vagy felett.
  A FortiToken elérhető Windows 10 verzió 14393.0 vagy felett, macOS 11.0 vagy felett.
- Internetkapcsolat a Neptun Egységes Tanulmányi Rendszert futtató eszközön.
  A választott authetikáló alkalmazás telepítéséhez szükséges internetkapcsolat, viszont a kulcs regisztrációjánál és a folyamatos használatnál a 6 számjegyű token generálásához már nincs szükség internetre.
- Okoseszköz (Android vagy iOS operációs rendszerrel), vagy számítógép
- Hozzáférési jogosultság a SOE Neptun rendszeréhez

Mire kell ügyelni a kétfaktoros hitelesítéskor használatakor:

- belépéskor ügyelni kell a 6 számjegyű token pontos megadására, elírás esetén nem engedi a rendszer a belépést
- Többféle authentikátor programmal is használható ugyanaz a kétfaktoros regisztráció, ha ugyanahhoz a QR kódhoz tartozó karaktersor kerül beállításra.
- Új kétfaktoros regisztráció esetén törölni kell a korábban regisztrált fiókot az authentikátor programból.
- Sikertelen regisztráció esetén, ha a QR kódot vagy a karaktersor beolvasásra került az authentikátor programban, de a QR kód ablak bezárásra került, akkor az újbóli regisztráció előtt törölni kell az authentikátor programban létrehozott fiókot, mivel az már nem lesz érvényes.
- Új eszköz (okoseszköz vagy számítógép) beállítása esetén, ha kerülnek át a korábbi eszközről az alkalmazások, akkor a kétfaktoros hitelesítés törlése szükséges, majd az új eszközön új regisztráció szükséges. Amennyiben a korábbi regisztráció törlése nem történt meg, és segítségre van szüksége ezt kérjük a neptun-admins@uni-sopron.hu címen jelezze.
- Azok a Neptun felhasználók akik több hozzáféréssel is rendelkeznek (oktatói, hallgató, kliens ügyintézők) azoknak elegendő az egyik felületen elvégezniük a kétfaktoros regisztrációt, az érvényes lesz az összes hozzáférésükhöz, tehát a regisztrációt csak egyszer kell elvégezniük.

Technikai segítség:

- bármilyen a kétfaktoros hitelesítés beállításával használatával kapcsolatos kérését kérjük jelezze a Neptunkódja és a részletes probléma feltüntetésével a neptun-admins@uni-sopron.hu címen.