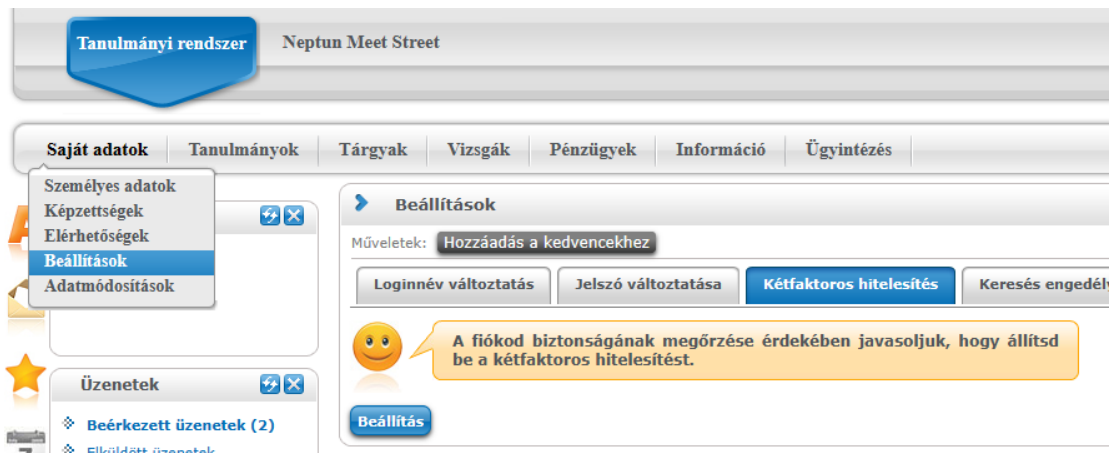


Kétfaktoros hitelesítés beállítása a Neptun webes felületén (oktatói és hallgatói web)

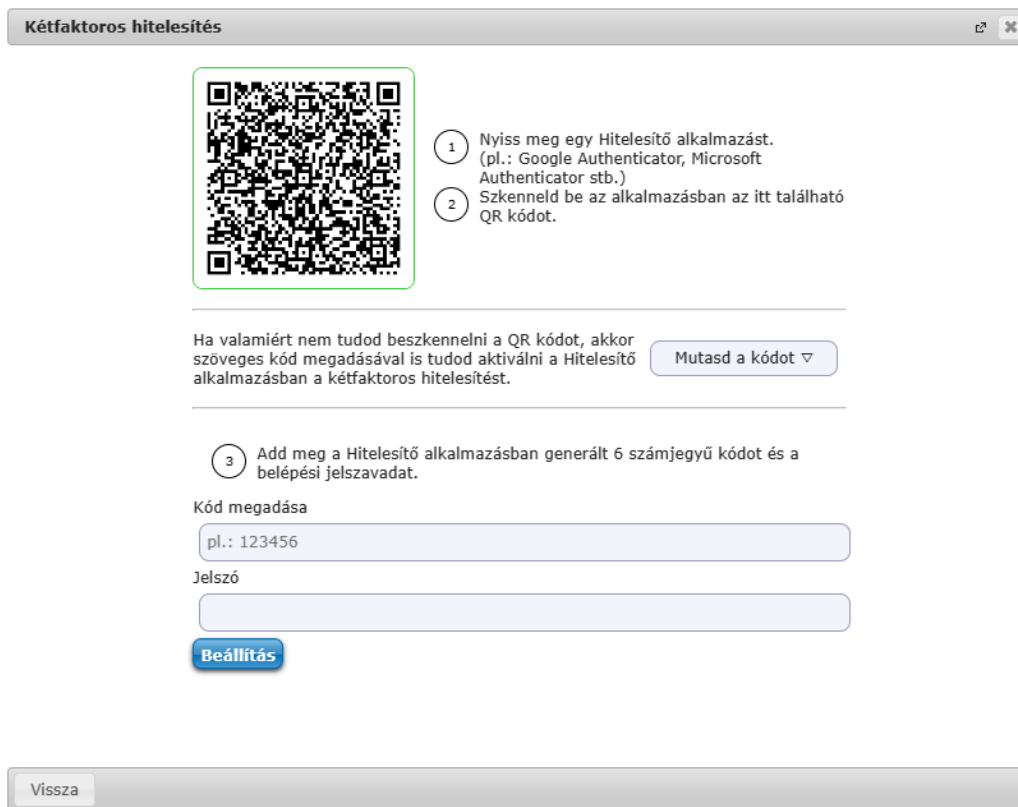
Első alkalommal a **Saját adatok/Beállítások/Kétfaktoros hitelesítés** menüpont alatt, regisztrálni kell a felhasználóhoz a kulcsot az általa használt autentikátorban.



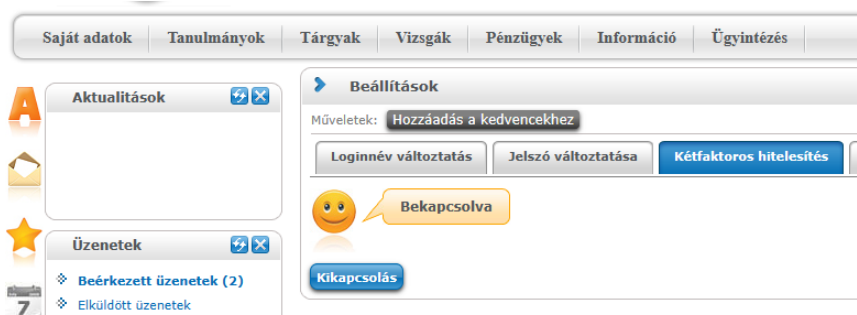
The screenshot shows the Neptun web interface. The top navigation bar includes 'Tanulmányi rendszer' and 'Neptun Meet Street'. Below it, a menu bar contains 'Saját adatok', 'Tanulmányok', 'Tárgyak', 'Vizsgák', 'Pénzügyek', 'Információ', and 'Ügyintézés'. The 'Saját adatok' dropdown menu is open, showing options like 'Személyes adatok', 'Képzettségek', 'Elérhetőségek', 'Beállítások', and 'Adatmódosítások'. The 'Beállítások' section is active, showing a 'Műveletek: Hozzáadás a kedvencekhez' and buttons for 'Loginnév változtatás', 'Jelszó változtatása', 'Kétfaktoros hitelesítés', and 'Keresés engedélyezése'. A yellow notification bubble is present with the text: 'A fiókod biztonságának megőrzése érdekében javasoljuk, hogy állítsd be a kétfaktoros hitelesítést.' Below the notification is a 'Beállítás' button.

A **Kétfaktoros hitelesítés** ablakban megjelenik egy QR kód, valamint a „Mutasd a kódot” gombra kattintva megjelenik a mezőben a QR kódhoz tartozó másolható karaktorsor.

A **Kód megadása** mezőben a sikeres regisztrálás után meg kell adni a 6 jegyű azonosítót a véglegesítéshez. A **Jelszó** mezőben a felhasználónak a véglegesítéshez meg kell adnia a Neptun belépési jelszavát, majd a Beállítás gombbal véglegesíteni a beállítást.



The screenshot shows the 'Kétfaktoros hitelesítés' (Two-factor authentication) setup window. It features a QR code and a list of instructions: 1. Nyiss meg egy Hitelesítő alkalmazást. (pl.: Google Authenticator, Microsoft Authenticator stb.) 2. Szkennd be az alkalmazásban az itt található QR kódot. Below the QR code, there is a text box for 'Kód megadása' (e.g., 123456) and a 'Jelszó' (password) field. A 'Beállítás' button is at the bottom. A 'Mutasd a kódot' button is also visible.

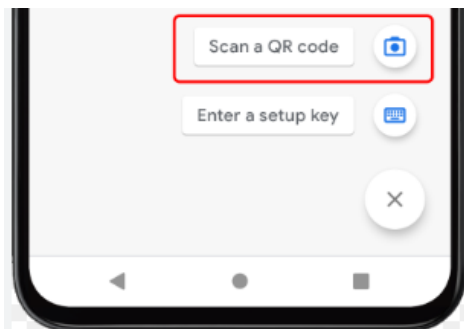


The screenshot shows the Neptun web interface. The top navigation bar includes 'Saját adatok', 'Tanulmányok', 'Tárgyak', 'Vizsgák', 'Pénzügyek', 'Információ', and 'Ügyintézés'. The 'Beállítások' section is active, showing a 'Műveletek: Hozzáadás a kedvencekhez' and buttons for 'Loginnév változtatás', 'Jelszó változtatása', 'Kétfaktoros hitelesítés', and 'Keresés engedélyezése'. A yellow notification bubble is present with the text: 'Bekapcsolva' (Enabled). Below the notification is a 'Kikapcsolás' button.

Authentikátor programok használata

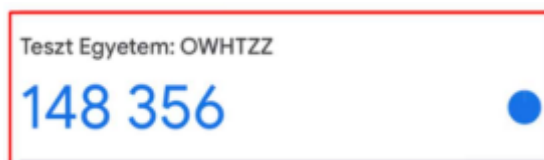
Google Authenticator:

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.

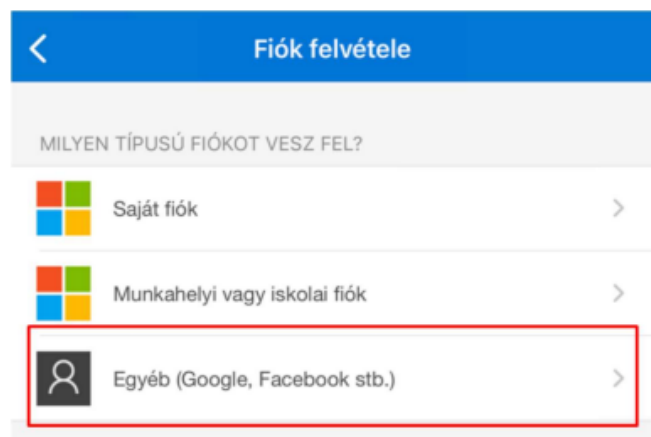


Kulcs neve és generált kód

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

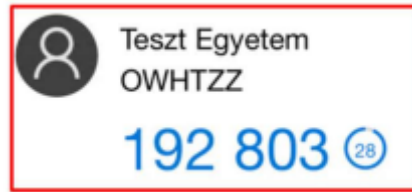
Microsoft Authenticator:

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



Kulcs létrehozása

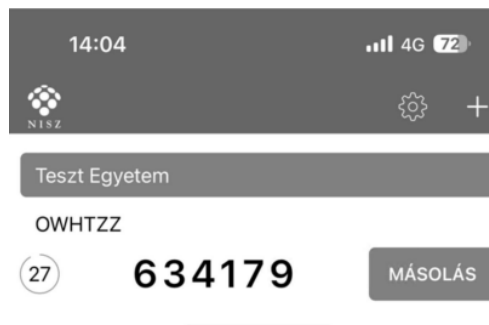
A QR kód beolvasása után azonnal elkezdődik a kódgenerálás, a kulcs neve az intézmény neve (Soproni Egyetem), és a felhasználó Neptunkódja lesz.



Kulcs neve és generált kód

NISZ Hitelesítő

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



Kulcs neve és generált kód

FortiToken (asztali alkalmazás)

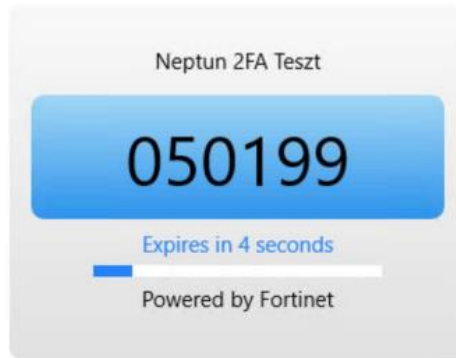
A letöltést és telepítést követően az alkalmazást megnyitva, a jobb alsó részben lévő + ikonnal megjelenő **Add gombra** kattintva kezdhető a beállítás.

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.

A screenshot of the FortiToken Windows "Add Account" form. The title bar says "FortiToken Windows". The main title is "FortiToken Windows" and "Add Account". There are three input fields: "Account Name:" with the value "Neptun 2FA Teszt", "Key:" with the value "K3RUG445AUSQKQ5K35GBSCIUDQQIX7FXTUHWKMFVCB5WNCXPX4URR3N3Y", and "Category (Fortinet or 3rd party):" with a dropdown menu showing "3rd Party".

Adatok kitöltése

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



Kulcs neve és generált kód

Belépés kétfaktoros hitelesítéssel a webes felületen:

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/token. A token a felhasználó autentikátor programjában érhető el.

✕

Kétfaktoros hitelesítés

Kérem írja be az autentikáló eszközén jelenleg érvényes 6 számjegyű token

Kód megadása:

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 autentikáló 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 autentikátor 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 autentikátor programból.
- Sikertelen regisztráció esetén, ha a QR kódot vagy a karaktersor beolvasásra került az autentikátor programban, de a QR kód ablak bezárásra került, akkor az újbóli regisztráció előtt törölni kell az autentikátor 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.