



Kétfaktoros hitelesítés használata Oktatói Web felületen

Általános leírás

A Neptun tanulmányi rendszerben opcionálisan beállítható a kétfaktoros hitelesítés, amivel nem csak felhasználónév és jelszó párossal védhetjük meg az adatállományt, hanem egy második faktor is rendelkezésre áll, ami egy dinamikusan változó kód vagy más néven token.

Az első faktor a felhasználónév és jelszó, a második a hitelesítő kód (token), ami az okostelefonra telepített/letöltött autentikációs szoftver által generált kód.

A kétfaktoros hitelesítés hatékony módszer arra, hogy egy kiber- vagy hacker támadás elkerülhető legyen. Ez a módszer időérzékeny hitelesítő kódokat használva akadályozza meg az identitás ellopását és az adatvesztést.

Neptun rendszerben az egyetlen hátránya, hogy jelenleg **nem lehet kulcs visszaállítást készíteni, így** jogosultság hiányában **kizárólag a Tanulmányi Hivatal Neptun rendszeradminisztrátora tudja törölni a regisztrációt.**

Javasolt autentikációs alkalmazások telefonra

Az alábbi applikációk letölthetők Android operációs rendszerrel rendelkező telefonok esetén Play áruházból, IOS-szel rendelkezők esetén pedig AppStore-ból.

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:

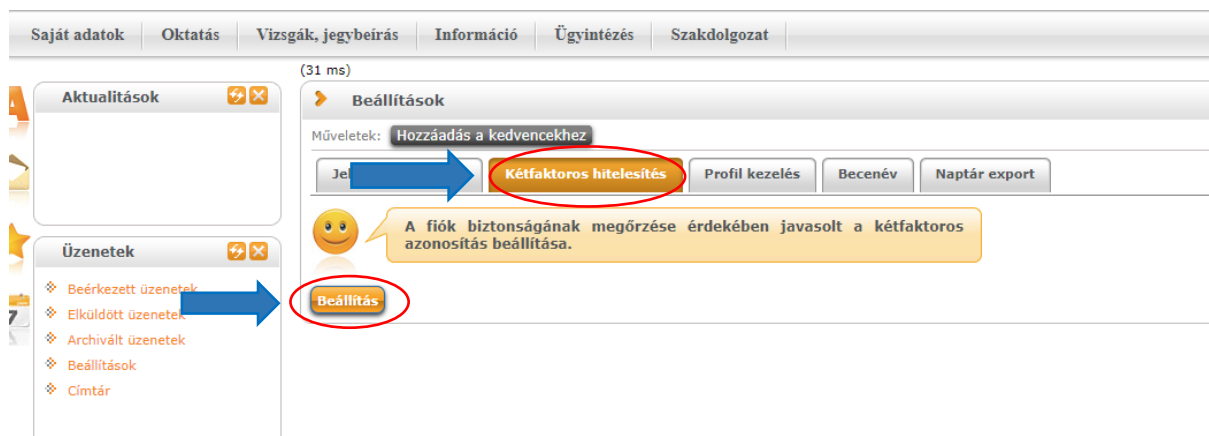
- Android: <https://play.google.com/store/apps/details?id=hu.innobile.niszauth&hl=hu>
- IOS: <https://apps.apple.com/hu/app/nisz-hiteles%C3%ADt%C5%91/id1603444961?l=hu>

Kétfaktoros hitelesítés beállítása

Oktatói webes felületen a **Saját adatok->Beállítások** menüpontban a **Kétfaktoros hitelesítés** tabulátorfül kiválasztása után, majd a **Beállítás** gombra kattintva indítható el a regisztráció.




1. ábra – Neptun rendszer – Beállítások megnyitása



2. ábra – Neptun rendszer – Kétfaktoros hitelesítés beállítása

A megjelenő „Kétfaktoros hitelesítés” ablakban be kell olvasni a QR kód autentikátor segítségével, majd a kapott 6 számjegyű kód és a jelszó megadásával a regisztráció megtörténik.

Kétfaktoros hitelesítés



1

Meg kell nyitni egy Hitelesítő alkalmazást.
(pl.: Google Authenticator, Microsoft Authenticator stb.)

2

Be kell szkennelni az itt található QR kódot.

Amennyiben nem lehetséges beszkenyelni a QR kódot, a szöveges kód megadásával is aktiválható a Hitelesítő alkalmazásban a kétfaktoros hitelesítés.

Kód megtekintése ▾

3

A hitelesítő alkalmazásban generált 6 számjegyű kód és a belépési jelszót kell megadni.

Kód megadása

pl.: 123456

Jelszó

Beállítás

Vissza

3. ábra – Neptun rendszer – Kétfaktoros hitelesítés regisztráció

Bejelentkezésnél a felhasználónév és jelszó megadását követően a „Kétfaktoros hitelesítés” felugróablakban az egyedi, 6 számjegyű token megadása szükséges a továbblépéshez.



4. ábra – Neptun rendszer – Token kód megadása bejelentkezésnél

Kétfaktoros hitelesítés megszüntetése esetén a **Kikapcsolás** gombot választva lehetséges a regisztrációt törölni:



5. ábra – Neptun rendszer – Kétfaktoros hitelesítés kikapcsolása