

Kétfaktoros hitelesítés beállítása hallgatói webes felületen

A Debreceni Egyetem Neptun tanulmányi rendszerének hallgatói felületére való belépés biztonságának fokozása érdekében úgynevezett kétfaktoros azonosítási szolgáltatás került bevezetésre.

A kétfaktoros hitelesítő azonosítás azt jelenti, hogy a korábban megszokott Azonosító+Jelszó páros megadását követően minden egyes belépéskor egy 6 számjegyű kód megadása is szükséges, amelyet egy Authentikátor (Hitelesítő alkalmazás) generál.

A kétfaktoros hitelesítés beállításának lépései:



1. Authentikátor (Hitelesítő alkalmazás) letöltése

Telepítsük okostelefonunkra/számítógépünkre az alább javasolt Authentikátorok egyikét.

Okostelefonra:

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/fortitoken-windows/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. Regisztráció, kétfaktoros hitelesítés beállítása

2.1. Kétfaktoros azonosítás beállítása

Az 1. pont szerint a javasolt Authentikátorok egyikét szükséges telepíteni.

A Neptunba történő belépéskor, az Azonosító+Jelszó megadását követően az alábbi kétfaktoros hitelesítés regisztrációs ablak jelenik meg a hallgatói belépő oldalon:

The screenshot shows a registration window for two-factor authentication. It features a QR code on the left, which is highlighted with a green border. To the right of the QR code are two numbered instructions: 1. 'Nyiss meg egy Hitelesítő alkalmazást. (pl.: Google Authenticator, Microsoft Authenticator stb.)' and 2. 'Szkennezd be az alkalmazásban az itt található QR kódot.' Below these instructions is a text box with the message: 'Ha valamiért nem tudod beszkenneálni a QR kódot, akkor szöveges kód megadásával is tudod aktiválni a Hitelesítő alkalmazásban a kétfaktoros hitelesítést.' To the right of this text is a button labeled 'Mutasd a kódot ▾'. Below this is a third instruction: 3. 'Add meg a Hitelesítő alkalmazásban generált 6 számjegyű kódot és a belépési jelszavadat.' This is followed by a 'Kód megadása' section with a text input field containing 'pl.: 123456', a 'Jelszó' section with an empty text input field, and a blue 'Beállítás' button at the bottom left.

Kétfaktoros hitelesítés regisztrációs ablak

Az előzetesen választott és okostelefonra letöltött Authentikátorral (Hitelesítő alkalmazással) be kell olvasni a megjelenített QR kódot, ezzel regisztrálva az Authentikátorban a kulcsot. A QR kód beolvasása helyett a „**Mutasd a kódot**” gombra kattintva megjelenik a mezőben a QR kódhoz tartozó karaktersor, amely bemásolható a számítógépre letöltött Authentikátorba.

Ha okostelefonra telepített Authentikátort használunk, bármennyi eszközön/számítógépen beléphetünk a Neptunba. Ez célszerűbb megoldás, mint a számítógépes Authentikátor alkalmazás.

A számítógépes Authentikátor csak az adott számítógépen működik. Amennyiben számítógépes Authentikátort használunk, ahhoz, hogy több számítógépen is be tudjunk lépni, a „Mutasd a kódot” karaktersort szükséges elmenteni/megőrizni és bemásolni az összes olyan számítógépre feltelepített Authentikátorba, amelyen be szeretnénk lépni a Neptunba.

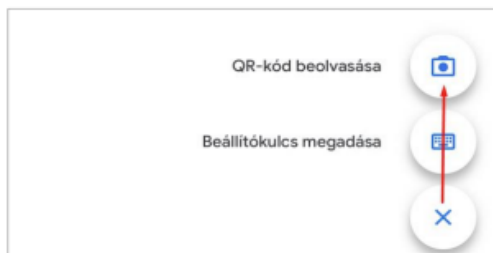
Ezután az Authentikátor félpercenként generál egy 6 számjegyből álló kódot. A „**Kód megadása**” mezőben a sikeres regisztrálás után meg kell adni az **aktuális** 6 számjegyű kódot. A „**Jelszó**” mezőben a véglegesítéshez meg kell adni a **hálózati azonosítóhoz tartozó jelszót**.

Ezt a regisztrációt egyszer szükséges elvégezni, majd ezt követően minden Neptun belépéskor az Azonosító+Jelszó beírása után az Authentikátorban kapott **aktuális** 6 számjegyű kódot is meg kell adni! Az autentikáló alkalmazás a kód megadását követően bezárható, nem szükséges, hogy folyamatosan fusson.

2.2 Authentikátorok használata, a kétfaktoros hitelesítés beállítása

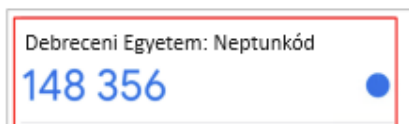
Okostelefonon Google Authenticatort használva:

Miután okostelefonunkra sikeresen telepítettük az alkalmazást, megnyitjuk azt, majd jobb oldalon alul a + jelre kattintva a „QR kód beolvasása” lehetőséget választjuk.



Kulcs létrehozása

A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve „Debreceni Egyetem” és a felhasználó Neptunkódja lesz.



Kulcs neve és Generált kód

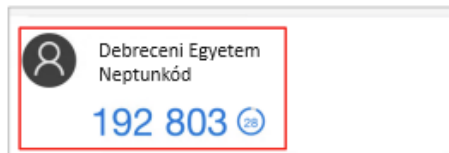
Okostelefonon Microsoft Authenticatort használva:

Megnyitjuk az alkalmazást, majd jobb oldalon a + jelre kattintva a megjelenő opcióknál az „Egyéb (Google, Facebook stb.)” opciót választjuk.



Kulcs létrehozása

A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve „Debreceni Egyetem” és a felhasználó Neptunkódja lesz.



Kulcs neve és Generált kód

Számítógépen FortiTokenet használva:

A letöltést követően meg kell nyitni a **FortiToken** alkalmazást. A felület jobb alsó részén a „+ Add” gombra kattintva kezdhető meg a beállítás. Az „Account Name” mező szabadon tölthető, ez lesz a neve a kulcsnak. A „Key” mezőben azt a másolható karaktersort kell megadnunk, ami a Neptunban a regisztrációs ablakon belül jelenik meg, amikor a „Mutasd a kódot” gombra kattintunk. A „Category (Fortinet or 3rd party)” mezőben pedig a „3rd Party” lehetőséget kell kiválasztani. Az adatok megadását követően a felület jobb alsó felén kattintsunk a „✓ Done” feliratú gombra.

A screenshot of the FortiToken Windows application interface. The title bar says "FortiToken Windows". The main window title is "FortiToken Windows" and the subtitle is "Add Account". There are three input fields: "Account Name:" with the value "Neptun 2FA Teszt", "Key:" with the value "K3RUG445AUSQKQ5K35GBSCIUDQQIX7FXTUHWKMFVCB5WNC PX", and "Category (Fortinet or 3rd party):" with a dropdown menu showing "3rd Party".

Adatok kitöltése

3. Az Authentikátor (Hitelesítő alkalmazás) használata (kód megadása minden belépéskor)

A sikeresen beállított kétfaktoros hitelesítést követően minden belépéskor a hallgatói webes belépő felületen az Azonosító+Jelszó megadása után megjelenik a „Kétfaktoros hitelesítés” felugró ablak. Itt a korábban sikeresen regisztrált Authentikátorban generált **aktuális** 6 számjegyű kódot kell megadni.

A belépéshez kattintsunk a „Belépés” gombra.

A screenshot of a dialog box titled "Kétfaktoros hitelesítés". The text inside says "Kérem írja be az autentikáló eszközén jelenleg érvényes 6 számjegyű tokent". Below this is a text input field labeled "Kód megadása:" with the value "pl.: 123456". At the bottom right, there are two buttons: "Mégsem" and "Belépés".

Kód megadása

4. Egyéb információk, technikai feltételek, segítség

A kétfaktoros hitelesítés szolgáltatás feltételei:

- 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 **FortiToken** elérhető Windows 10 verzió 14393.0 vagy felett, macOS 11.0 vagy felett.
Az **Authy** elérhető macOS 10.11 vagy felett, Linux-on (Ubuntu, Linux Mint, Debian, Manjaro).
- 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 kód generálásához már nincs szükség internetre.
- Okostelefon (Android vagy iOS operációs rendszert futtató eszköz) vagy számítógép
- Hitelesítő alkalmazás megléte az 1-es pontban választott eszközön
- A DE Neptun rendszerében hallgatói jogosultság

Mire szükséges figyelni a kétfaktoros hitelesítés használatakor:

- Új eszköz vásárlásakor, ha nem kerülnek át az alkalmazások az új készülékre, akkor a kétfaktoros hitelesítés törlése szükséges, majd újra regisztrálása az új eszközön. Amennyiben segítségre van szüksége, kérjük jelezze a neptun@unideb.hu e-mail címen.
- Újra regisztrálásakor a korábbi fiókot törölni kell az Authentikátorban.
- Pontosán adjuk meg a generált kódot! Elírás esetén nem fogunk tudni belépni.
- Bármennyi eszközön beléphetünk a Neptunba, ha okostelefonra telepített Authentikátort használunk, emiatt célszerű azt választani számítógépre telepített Authentikátor helyett, ahol a karaktersort szükséges elmenteni/megőrizni és bemásolni a számítógépre telepített Authentikátorba.
- Azon felhasználók, akik egyszerre több Neptun szolgáltatáshoz is rendelkeznek hozzáféréssel (oktatói, hallgatói, kliens adminisztrátori), az egyik felületen keresztüli regisztrációnál létrehozott kóddal mindegyik felülethez hozzá fognak férni. A hitelesítés regisztrációt csak egyszer kell elvégezni.
- Sikertelen regisztráció után, amennyiben a QR-kódot tartalmazó ablakot már bezártuk, de a választott Hitelesítő alkalmazásunkban az ehhez tartozó fiók már létrejött, akkor az újbóli regisztráció előtt a korábban létrejött kód fiókot mindenképp törölni szükséges az alkalmazásban, mivel az már nem lesz érvényes, használható.

Technikai segítség:

Amennyiben a kétfaktoros hitelesítéssel kapcsolatosan technikai segítségre van szüksége, kérjük, hogy a problémát részletezve, képernyőképet csatolva és **Neptunkódját** feltüntetve a következő e-mail címen jelezze: neptun@unideb.hu