

A hallgatói – és az oktatói webre való belépéskor, ha a felhasználó még nem regisztrálta magát, akkor regisztrálnia kell a kulcsot az általa használt autentikátorban.



- 1 Nyiss meg egy Hitelesítő alkalmazást. (pl.: Google Authenticator, Microsoft Authenticator stb.)
- 2 Szkennezd be az alkalmazásban az itt található QR kódot.

Ha valamiért nem tudod beszkenneálni a QR kódot, akkor szöveges kód megadásával is tudod aktiválni a Hitelesítő alkalmazásban a kétfaktoros hitelesítést.

Mutasd a kódot ▾

3 Add meg a Hitelesítő alkalmazásban generált 6 számjegyű kódot és a belépési jelszavadat.

Kód megadása

Jelszó

Beállítás

A felhasználónév/jelszó megadását követően megjelenik a „*Kétfaktoros hitelesítés*” ablak. Az 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 belépési jelszavát.

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.



Kétfaktoros hitelesítés

Kérem írja be az autentikáló eszközén jelenleg érvényes 6 számjegyű token

Kód megadása:

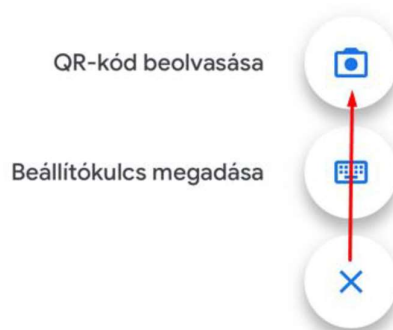
Mégsem Belépés

Token megadása

Az aktuális token kizárólag a felhasználó autentikátorjában érhető el.

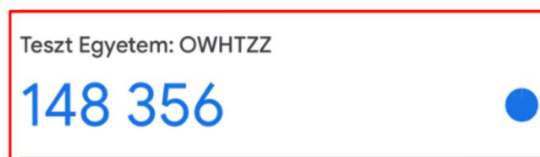
Google authenticatort használva

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.

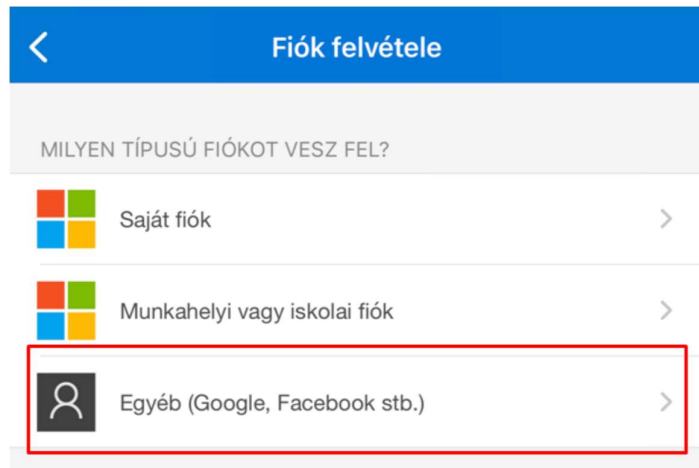


Kulcs neve és Generált kód

Microsoft Authenticatort használva

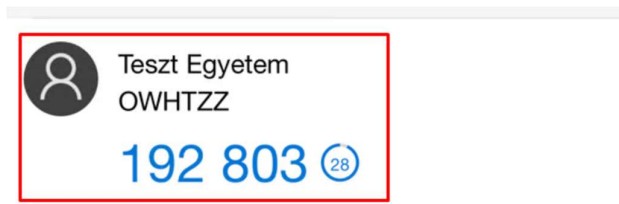
Megnyitjuk az alkalmazást, majd jobb alul a + jelre kattintva a megjelenő opcióknál az „Egyéb (Google, Facebook stb.)” opciót kell választani.





Kulcs létrehozása

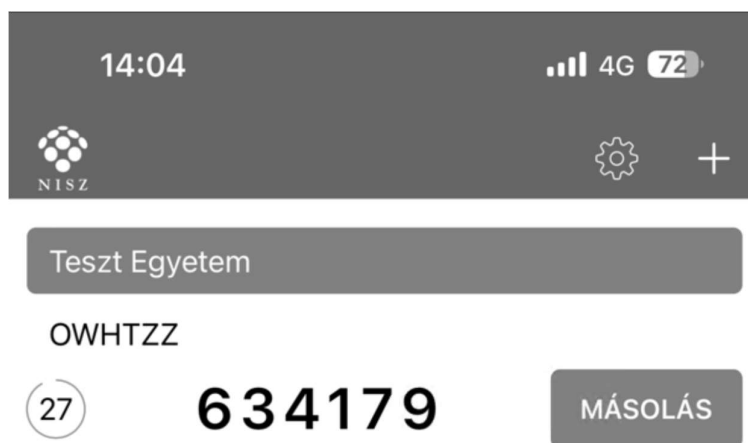
A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcs neve és Generált kód

NISZ Hitelesítőt használva

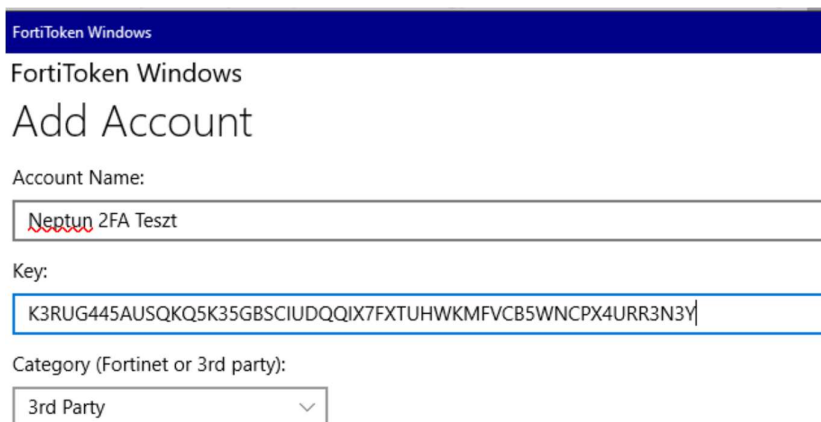
Az alkalmazást megnyitva jobb felül a + jelre kattintva csak be kell olvasni a képernyőről a QR kódot. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcs neve és Generált kód

FortiToken használva

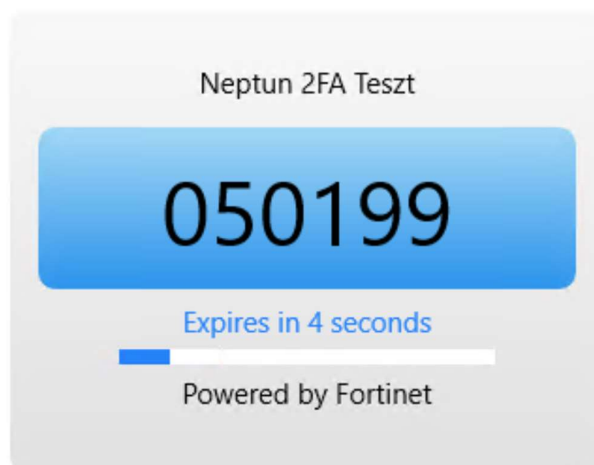
A letöltést követően meg kell nyitni az alkalmazást. Megnyitva a felület jobb alsó részén a „+” ikonnal ellátott „Add” gombra kattintva kezdhető meg a beállítás. „Account Name”-nek bármit megadhatunk, ez lesz a neve a kulcsunknak, mi nevezzük el amire szeretnénk. A „Key” mezőben azt a kulcsot kell majd 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.



The screenshot shows the 'FortiToken Windows' application window. The title bar is dark blue with the text 'FortiToken Windows'. Below the title bar, the text 'FortiToken Windows' and 'Add Account' are displayed. There are three input fields: 'Account Name' with the value 'Neptun 2FA Teszt', 'Key' with the value 'K3RUG445AUSQKQ5K35GBSCIUDQQIX7FXTUHWKMFVCB5WNC PX4URR3N3Y', and 'Category (Fortinet or 3rd party)' with a dropdown menu showing '3rd Party'.

Adatok kitöltése

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



Generált kód