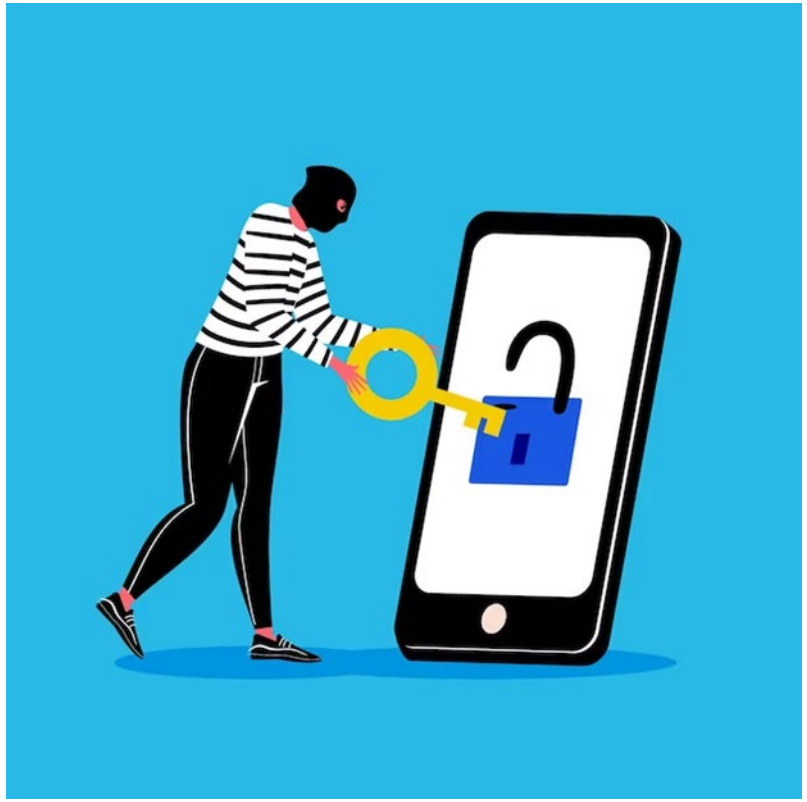
Kétfaktoros hitelesítés

Jelszavak védelme

Tippek a biztonságosabb jelszóhasználathoz



Mit tudunk tenni?

- Válasszunk erős jelszavakat!
  - a használt jelszónak **legalább 8 karakter** hosszúnak kell lennie, tartalmaznia kell **legalább 2 kis-** és **1 nagybetűt**, valamint **1 számot.**
- Az előre beállított jelszavakat mindig változtassuk meg!
- Használjunk fiókonként eltérő, egyedi jelszavakat!
- Nem szabad megosztani a jelszavakat másokkal, ne kerüljenek mentésre a számítógépen vagy papírra felírásra!

Kétfaktoros hitelesítés

2FA (Two Factor Authentication)

Mi is ez?

- Egy olyan biztonsági beállítás, amely lehetővé teszi a felhasználók számára, hogy második biztonsági réteget adhassanak a fiókjukhoz, ezzel erősítve adataik védelmét.

- Előnyei:
  - abban az esetben, ha illetéktelen személy hozzá jut a felhasználó jelszavához → a kétlépcsős azonosítás megakadályozza a rendszerbe való belépést
  - felhasználók jobban tudják védeni adataikat

Kétfaktoros hitelesítés

2FA (Two Factor Authentication)

Mi is ez?

Két különböző elemből áll:

- **1. rész**: felhasználónév és a jelszó megadása (statikus)
- **2. rész**: 2FA token (dinamikus)

A két elem kombinálása biztosítja a rendszerbe történő bejelentkezést:

- Ha valamelyik hibás/ hiányzik → a felhasználót nem lehet hitelesíteni
- Sikertelen bejelentkezés

Kétfaktoros hitelesítés

Használati feltételek

Authentikátorok

- Telepített asztali/telefonos alkalmazás → **TOTP** (idő) alapú kulcsot kezelő
- Javasolt:
  - Asztali alkalmazásként: **FortiToken Windows**
  - Telefonos alkalmazásként: **Google authenticator, Microsoft Authenticator, NISZ Hitelesítő**

Figyelem! Egyszerre csak egy alkalmazás használata lehetséges

Kétfaktoros hitelesítés

Regisztráció folyamata

Kötelező használat esetén belépéskor (web)

Regisztráció

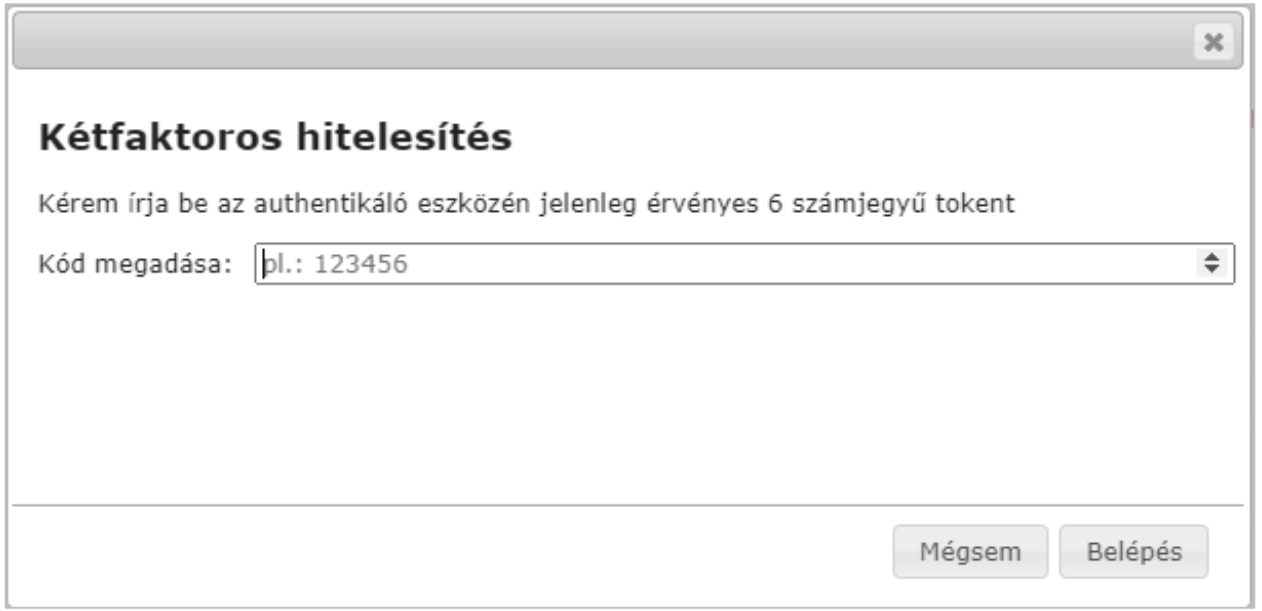
- QR kód beolvasása vagy **„Mutasd a kódot”** gombra elérhető azonosító másolása az authentikátorba
- **„Kód megadása”:** Authentikátorban megjelenő 6 számjegyű azonosító megadása
- **„Jelszó”:** újból meg kell adni

Kétfaktoros hitelesítés

Belépés folyamata

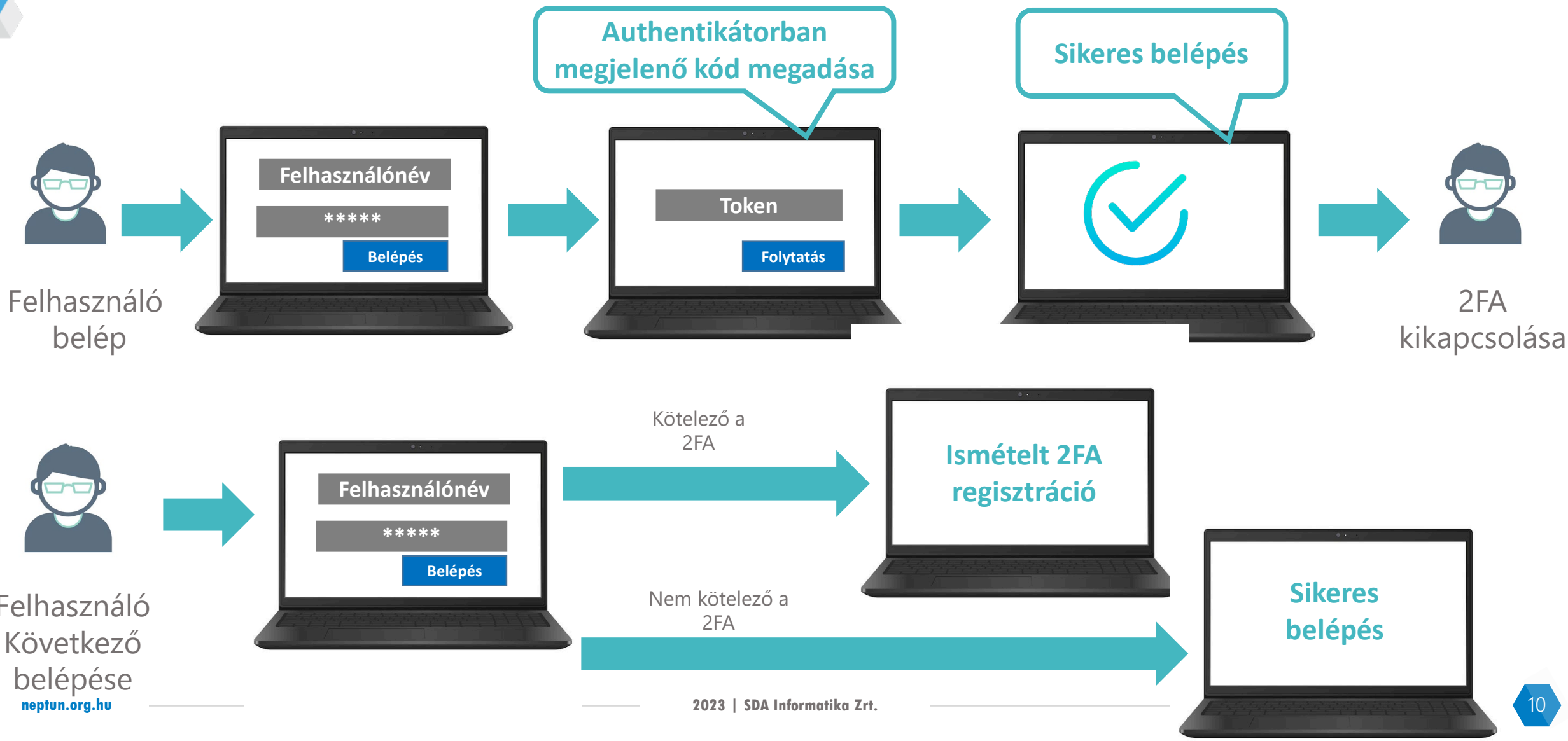
Belépés folyamata

Belépéskor token megadása (web)



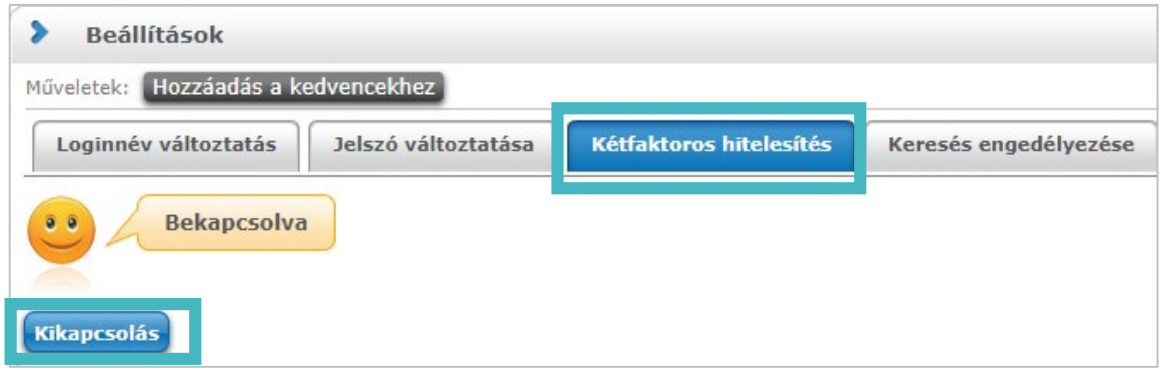
Kétfaktoros hitelesítés

Kikapcsolás folyamata - saját részre



Kétfaktoros hitelesítés kikapcsolása

Saját részre (web)



Kikapcsolás

- **„Saját adatok/Beállítások”** menüpont, **„Kikapcsolás”** gomb
- Nem szükséges 2FA a kikapcsoláshoz
- A következő belépéskor a felhasználónév (azonosító) és jelszó megadását követően megjelenik a regisztrációra szolgáló ablak. Ameddig nem végzi el ismét a regisztrációt, nem tud belépni a rendszerbe.

Javasolt telefonos alkalmazások

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 (csak Ügyfélkapu-val rendelkező felhasználóknak):

- 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

Javasolt asztali alkalmazások

FortiToken Windows

- Windows: https://apps.microsoft.com/detail/9p0tdh1j7wfz?hl=hu-hu&gl=HU

Twilio Authy

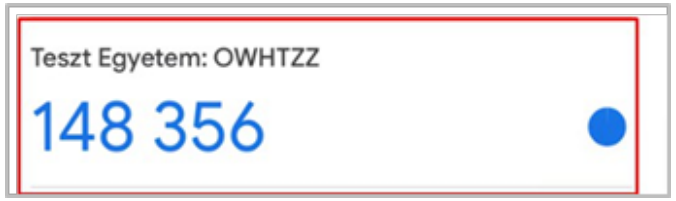
- Mac/Linux: https://authy.com/

Példák az authentikátorok használatára

Google authenticator

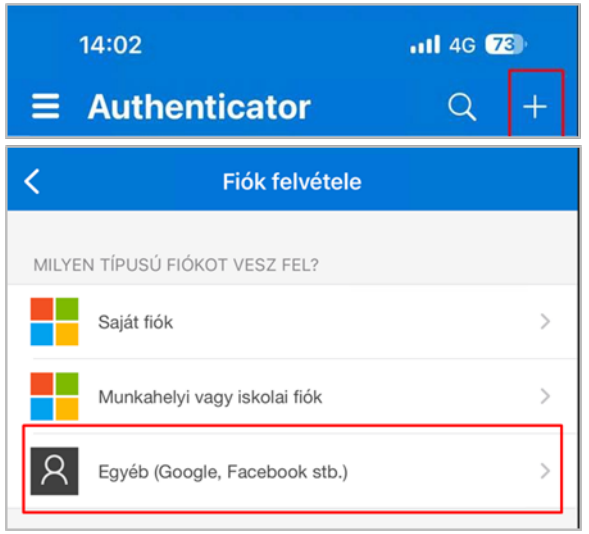
Megnyitjuk az alkalmazást, majd jobb alul a + jelre kattintva a „QR kód beolvasása” lehetőséget szükséges választani.

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

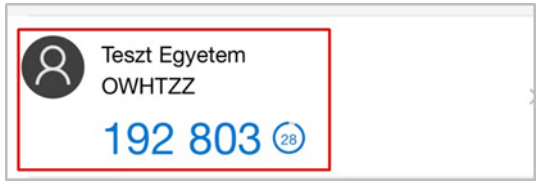


Microsoft authenticator

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

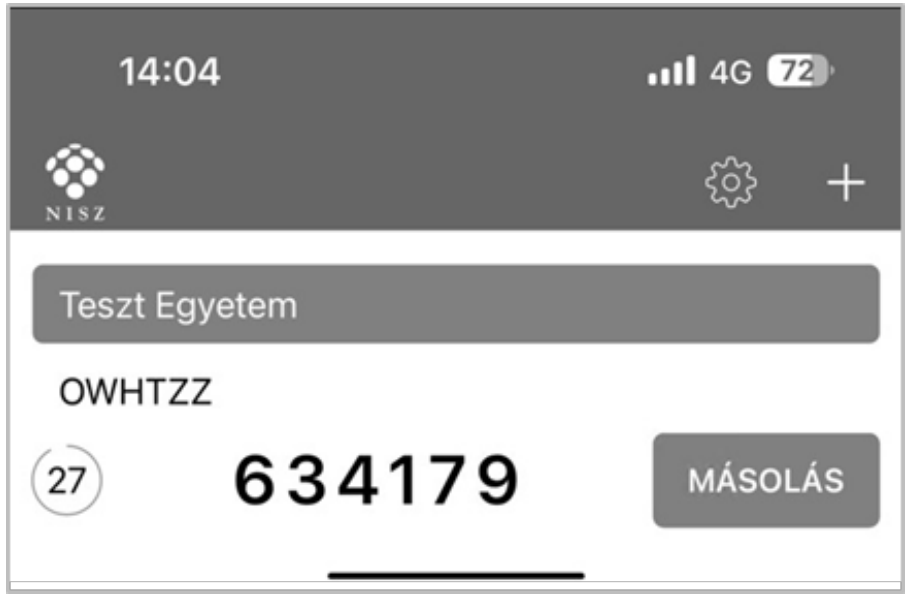


A QR kód beolvasása után azonnal megkezdődik a kódgenerálás. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



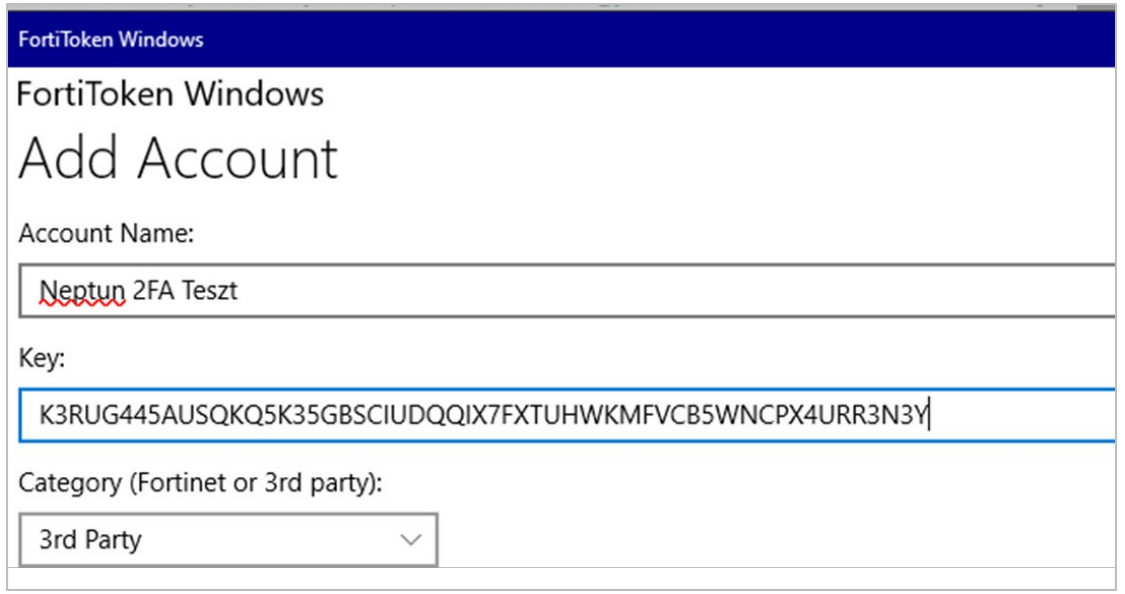
NISZ hitelesítő (csak Ügyfélkapu-val rendelkező felhasználóknak)

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



FortiToken (asztali alkalmazás)

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.



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