Authentikátor-ok (hitelesítők)

A 2FA-os funkció használatához a felhasználónak rendelkeznie kell egy telepített asztali vagy telefonos alkalmazással, mely képes **TOTP** (**T**ime-based **o**ne-**t**ime **p**assword) alapú kulcsot használni. Az alkalmazást a funkció használata előtt szükséges telepíteni. A javasolt három telefonos alkalmazás elérhető Androidon a Google Play-en és iOS-en is az App Store-ban.

Authentikátor-ok (hitelesítő alkalmazás) letöltése 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

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

Authentikátor (hitelesítő alkalmazás) letöltése számítógépre:

Az egyik elterjedtebb az a „**FortiToken Windows**”, de manapság a jelszó menedzserek is képesek már ezeknek a kulcsoknak a tárolására.

FortiToken:
Windows: https://apps.microsoft.com/store/detail/fortitoken-windows/9P0TDH1J7WFZ?hl=enus&gl=us

macOS: https://apps.apple.com/us/app/fortitoken-mobile/id500007723

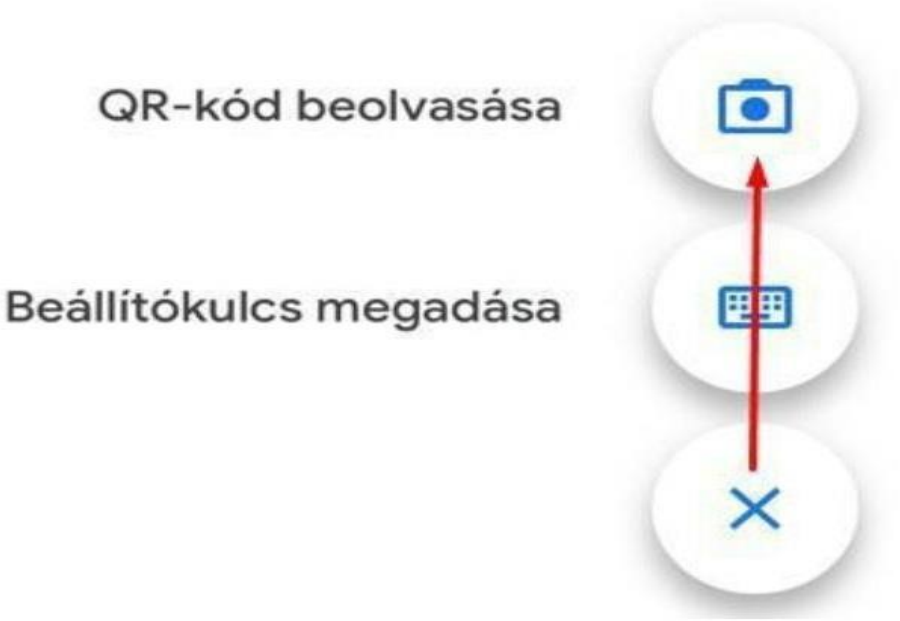
Step Two:
https://steptwo.app/
Csak macOS-re elérhető a „**Step Two**” nevű alkalmazás, amelyben hasonlóan elvégezhető a kétfaktoros kulcs regisztrálása, mint a FortiToken-nél, és ezután ugyanúgy generálni fogja a program a 6 számjegyű tokent, amivel tudja majd magát azonosítani belépéskor.

Twilio Authy:
https://authy.com/
Linux-ra elérhető a „**Twilio Authy**” nevű alkalmazás, amelyben hasonlóan elvégezhető a kétfaktoros kulcs regisztrálása, mint a FortiToken-nél, és ezután ugyanúgy generálni fogja a program a 6 számjegyű token-t, amivel tudja majd magát azonosítani belépéskor.

Példák az authentikátor-ok használatára

a. Google authenticator-t használva

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



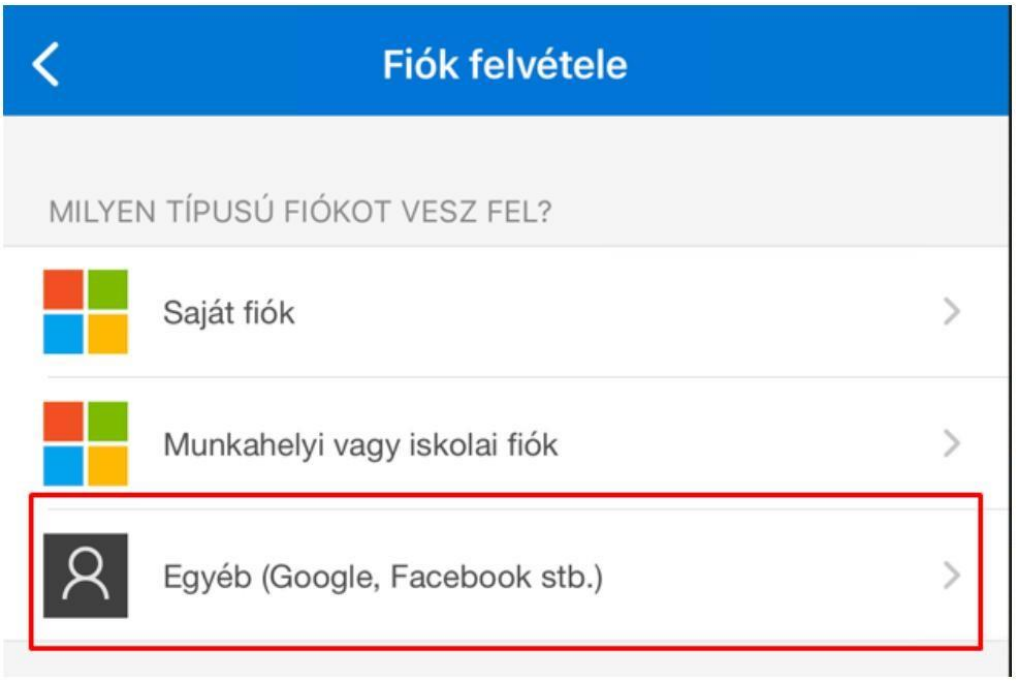
Kulcs létrehozása

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

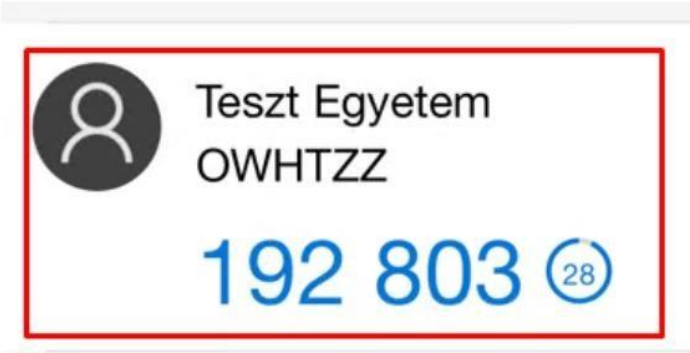
b. Microsoft Authenticator-t használva

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



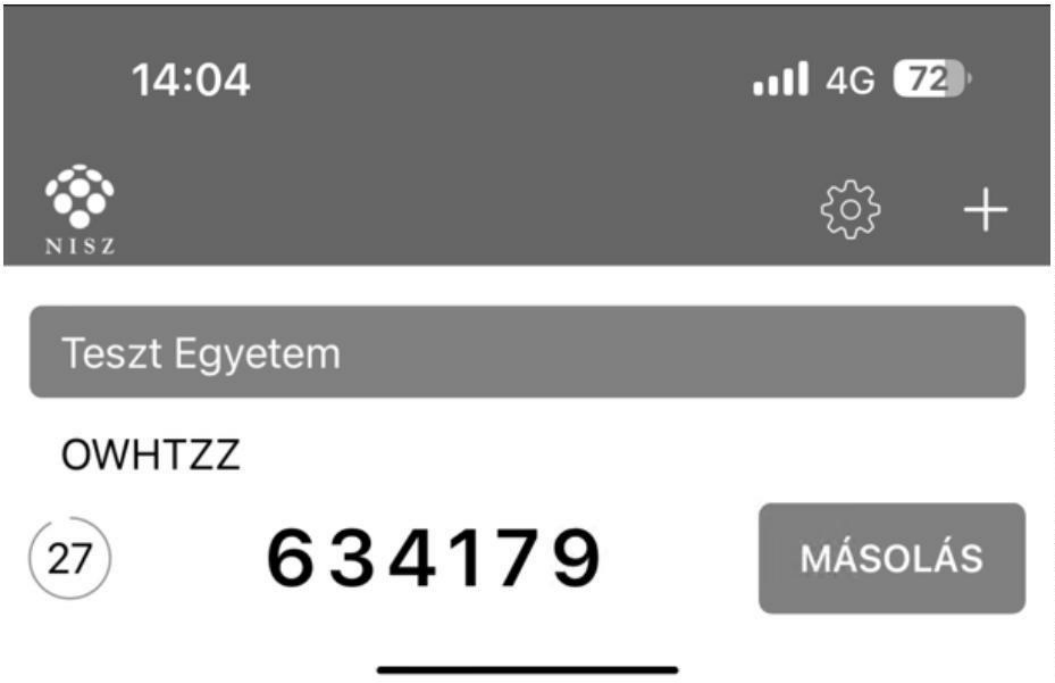
Kulcs létrehozása

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



c. NISZ Hitelesítőt használva

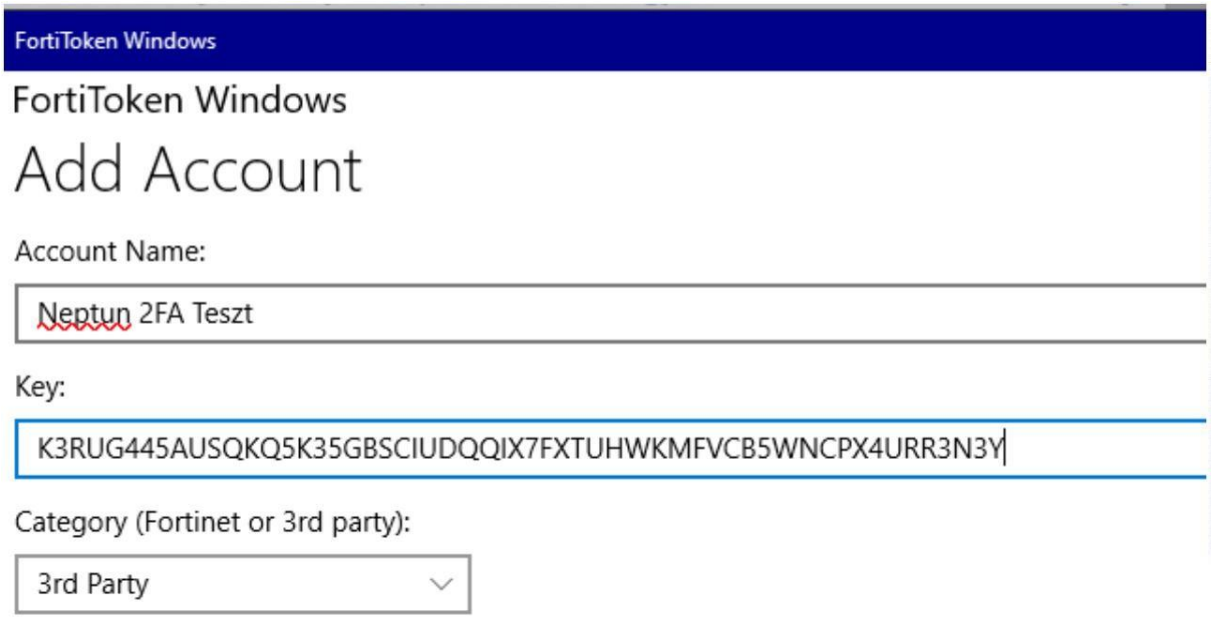
Az alkalmazást megnyitva jobb felül a **+** jelre kattintva csak bekell olvasni a képernyőről a QR kódot. A kulcs neve az intézmény neve és a felhasználóknak a Neptunkódja lesz.



Kulcsneve és Generált kód

d. FortiToken-t 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



Adatok kitöltése

Generált kód

Amennyiben nem tud belépni a 2FA-os hitelesítéssel a neptun rendszerbe, akkor kérjük jelezze a halmi.zsolt@unithe.hu e-mail címen. Az e-mail-ben mindenféleképpen legyen feltüntetve a pontos név és a pontos neptun-kód is!