When accessing the student - and tutor - web, if the user has not registered yet, they must register the key in the authenticator they use.

1. Open an Authenticator application (e.g. Google Authenticator, Microsoft Authenticator, etc.)
2. Scan the QR code here in the application.

If – for some reasons – you are not able to scan the QR code, you can activate the Two-factor authentication by entering the text code.

Show code

3. Enter the 6-digit code generated in the Authenticator application and your login password.

Enter code
Password

Setting

After entering the username/password, the *"Two-Factor Authentication"* window will appear. A QR code will be displayed in the window, and by clickng on the "Show code" button the row of copyable characters associated with the QR code will be displayed in the field. After a successful registration, the user will be asked to enter the 6-digit identifier in the *"Enter code"* field for finalization. The user must enter their login password in the "Password" field to finalize the process.

Process of entry linked to two factors

In case the user is registered with a two-factor authentication, after entering the username (identifier) and the password the *"Two-factor authenticator"* pop-up window will appear, where it is required to enter the 6-digit token to proceed.

Two-factor authentication

Please enter the 6-digit token currently valid on your authentication device.

Enter code:

No – Enter

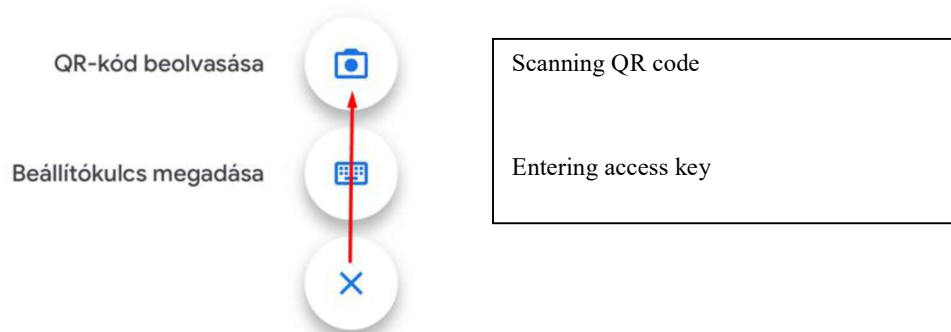*Entering token*

The current token is only available in the user's authenticator.

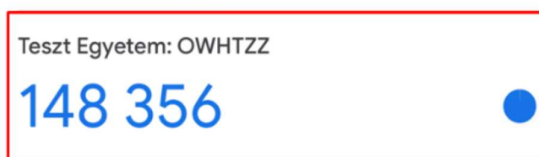**When you use Microsoft Authenticator:**

Open the application, click the + symbol at the bottom right to select the "Scan QR code" option.

Scanning QR code
Entering access key

Creating a key

After scanning the QR code, the code generation will start immediately. The name of the key will be the name of the institution and the user's Neptun code.
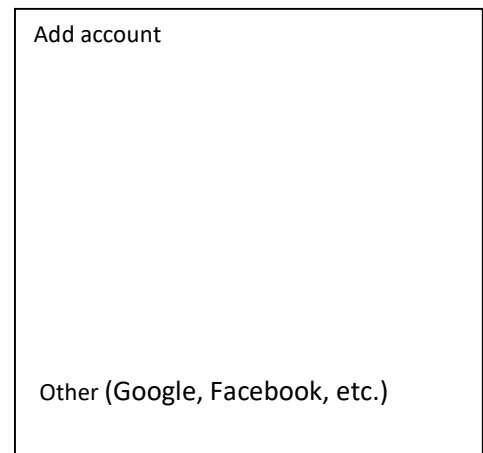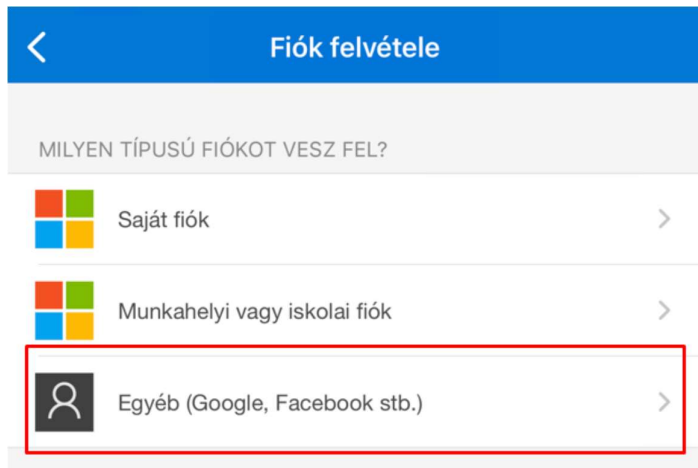

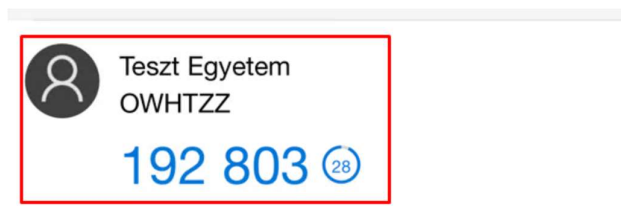*Key name and Generated code*

When you use Microsoft Authenticator:

Open the application, click the + symbol at the bottom right and select the "Other (Google, Facebook, etc.)" option from the options that appear.

Add account

Other (Google, Facebook, etc.)

Creating a key

After scanning the QR code, the code generation will start immediately. The name of the key will be the name of the institution and the user's Neptun code.

Key name and Generated code

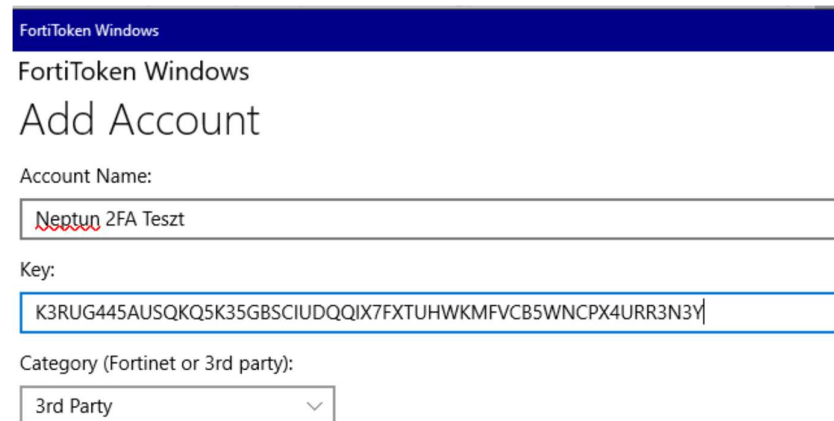**When you use NISZ (National Infocommunications Service Company Ltd.) Authenticator:**

Open the application, click on the + symbol at the bottom right and scan the QR code from the screen. The name of the key will be the name of the institution and the user's Neptun code.
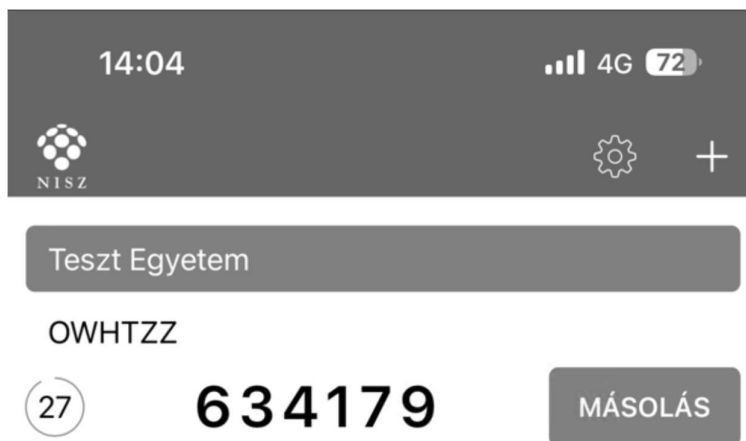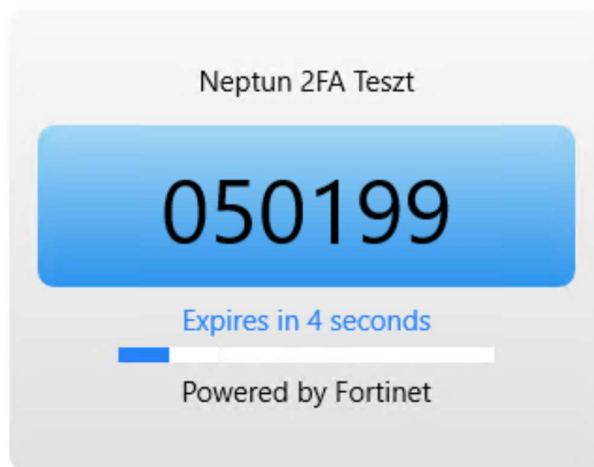

Key name and Generated code

Using FortiToken

The applcation must be opened after the download. Open it, then click on the "Add" button with the + icon at the bottom right of the interface to start the configuration. Anything can be given as "Account Name", this will be the name of our key. We can call it whatever we want. In the "Key" field the user will be asked to enter the key that will appear in the Neptun registration window when they click on the "Show code" button. In the "Category" field, select the "3rd Party" option.

Sending data

After entering the data click on the "**Done**" button with a tick in the bottom right corner of the interface.

Generated code