

The setting and usage of the two-factor authentication in the NEPTUN system of the Hungarian University of Agriculture and Life Sciences

In accordance with the security standards of the era, and to prevent possible security incidents, the two-factor identification service has been activated in the NEPTUN Educational (study) System (NEPTUN) of the Hungarian University of Agriculture and Life Sciences.

The use of two-factor authentication is highly recommended for all users with an account in the system. Obligatory use of two-factor authentication will be imposed on all users shortly. The obligatory use of the authentication mode will be phased in gradually, but all users can join voluntarily before the obligatory introduction. Please ensure that everyone turns it on as described below!!

Two-factor authentication means that in addition to the previously used Identity + Password pair, a 6-digit code (token) is also required for each login to NEPTUN, generated by an authenticator (authentication application).

Steps to set up two-factor authentication:

1. **Download the authenticator to your smartphone/computer**
2. **Registration in the authenticator and setting up two-factor authentication in NEPTUN**
3. **Using the authenticator (entering a code every time you log in)**

Before you start the installation, we recommend that you take note of the following:

- Greater security is achieved if the system and the authenticator are running on different devices, because then both need to be accessed by an unauthorised user, which is more difficult to achieve. **For this reason, we recommend installing the authenticator on your mobile phone and logging into NEPTUN on a personal computer!** In case you have only one device, you can install the authenticator on this device.
- **Be sure to enter a unique password for your NEPTUN login, make sure that your Neptun password does not match any other password used in any other system.**
- **Do not share your password with anyone!**

1. Download Authenticator (authentication app)

To smartphone:

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>

FortiToken:

Android:

https://play.google.com/store/apps/details?id=com.fortinet.android.ftm&pcampaignid=web_share

To personal computer:

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/> macOS-only application for registering two-factor keys, similar to FortiToken.

The listed applications are free to install and use!

2. Registration in the authenticator and setting up two-factor authentication in NEPTUN

Install one of the applications listed in point 1 on your device, then launch it when the installation is complete.

If you are one of our students or lecturers, log in to the NEPTUN web interface, then go to **My data / Settings / Two-factor authentication** and click on the **Set up** button. Then, or if you are required to use two-factor authentication, you will also be greeted with this window the first time you log in:



The screenshot shows a registration window for two-factor authentication. It features a QR code at the top left, which is highlighted with a green box. To the right of the QR code, there are two numbered steps: 1. 'Nyiss meg egy Hitelesítő alkalmazást. (pl.: Google Authenticator, Microsoft Authenticator stb.)' and 2. 'Szkennezd be az alkalmazásban az itt található QR kódot.' Below the QR code, there is a text box that says 'Ha valamiért nem tudod beszkenyelni 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, there is a third step: 3. 'Add meg a Hitelesítő alkalmazásban generált 6 számjegyű kódot és a belépési jelszavadat.' This is followed by two input fields: 'Kód megadása' with the placeholder 'pl.: 123456' and 'Jelszó'. At the bottom left, there is a blue button labeled 'Beállítás'.

Two factor authentication registration window

If you have the authenticator installed on your smartphone, press the "+" sign in the app and follow the steps to select the **Scan QR code** option, which will scan the QR code from another device's screen.

If you don't have another device or you have installed the authenticator on your computer, clicking on the "Show code" button in NEPTUN will display the character string for the QR code in the field, which can be copied into the authenticator. The character string can also be saved to a file, which can be used to install the authenticator on multiple devices in succession. Be careful to delete the saved character string after each installation! Multi-device installations should be used only when justified, instead we recommend a single installation of the authenticator on a mobile phone.

The Authenticator then generates a **6-digit code** every 30 seconds. To proceed, you must enter the 6-digit code **currently generated** by the Authenticator in the "Enter code" field of the window.

In the "**Password**" field, you must enter **the password for your Neptun ID** to finalise it, then press the "**Set**" button.

3. Use the authenticator (enter a code every time you log in)

After successful registration, each time you log in to NEPTUN, you have to start the authenticator and after entering the Identifier+Password, you have to enter the current 6-digit code in the authenticator, selecting the line you registered for NEPTUN login!

Please note that if you have only a few seconds left before the code is renewed, you should wait until the new code appears, because if you start entering a code in the last seconds, the code you have entered may become obsolete. In this case, the process can be repeated.

The authentication application can be closed after the code has been entered, it is not necessary to keep it running. It is good to know that it only requires an internet connection when registering, not afterwards.

4. Other information, technical conditions, help

Terms of the two-factor authentication service:

- The **Google Authenticator** can be reached iOS 13.0 version or above, Android 4.4 version or above.
A **Microsoft Authenticator** can be reached iOS 11.0 version or above, Android 6.0 version or above.
A **FortiToken** can be reached Windows 10 version 14393.0 or above, macOS 11.0 or above.
Az **Authy** can be reached macOS 10.11 or above, Linux (Ubuntu, Linux Mint, Debian, Manjaro).
- Internet connection on a device running the NEPTUN. An internet connection is required to install the authentication application of your choice, but no internet connection is needed to generate the 6-digit token for key registration and ongoing use.
- Smart device (Device running Android or iOS operating system) or personal computer
- Existence of a validation application on the device selected in point 1
- Client privileges in MATE NEPTUN

What to look out for when using two-factor authentication:

- When purchasing a new device, if the applications are not transferred to the new device, you will need to delete the two-factor authentication and then re-register it on the new device. **If you need help, please let us know in the "Technical support" section at the end of this manual!**
- When re-registering, the previous account must be deleted in the Authenticator.
- Specify the generated token exactly! In case of a typo, you will not be able to enter.
- You can use the same two-factor registration with multiple Authenticators if you keep the copyable string associated with the QR code.

- Users who have access to several NEPTUN services at the same time (lecturer, student, client administrator) will have access to all of them with the token created when registering through one of the interfaces. The authentication registration will only need to be done once.
- After an unsuccessful registration, if the window containing the QR code has already been closed, but the corresponding account has already been created in the Authenticator application of your choice, it is necessary to delete the previously created code account in the application before re-registering, as it will no longer be valid and usable.

Technical support:

If you need technical assistance with two-factor authentication, please summarise your problem briefly in an e-mail with "**2-factor**" in the subject line and be sure to include your **Neptun ID**. Send the letter from your e-mail address recorded in NEPTUN to neptun@uni-mate.hu

Example email:



Tisztelt Ügyintéző!

A Neptun rendszerbe nem tudok bejelentkezni, mert a két faktoros bejelentkezéshez használt alkalmazást telefoncsere miatt újra kellett telepítenem. Kérem, hogy tegyék számomra regisztrálhatóvá az új alkalmazást!

Köszönettel:
Szerencsés Eugén
Neptunkódom: XYZ123

Gödöllő, 22 March 2024.

Hungarian University of Agriculture and Life Sciences
Educational Directorate