

Identity & Access Management (IAM)

# Multi-Factor Authentication

for Microsoft Services



# Manual

## Microsoft Authenticator App enrolment

### Versie beheer:

Person	Date	Version
O. Oduncu	13-11-2023	v0.1

# Contents

1 Login.....	4
1.1 TU Delft services.....	4
1.2 Microsoft services.....	4
2 MFA Enrolment.....	6
2.1 New MFA registration.....	6
3 Troubleshooting.....	12
3.1 Change MFA:.....	12
3.2 MFA Device lost.....	12

# 1 Login

For all services at the TU Delft that require login, you will need a NetID account. This NetID is a personal account, which is linked to your registration at the TU Delft.

At the time of writing this manual the TU Delft environment knows 2 types of MFA services, depending on what you login: TU Delft SSO and Microsoft SSO services.

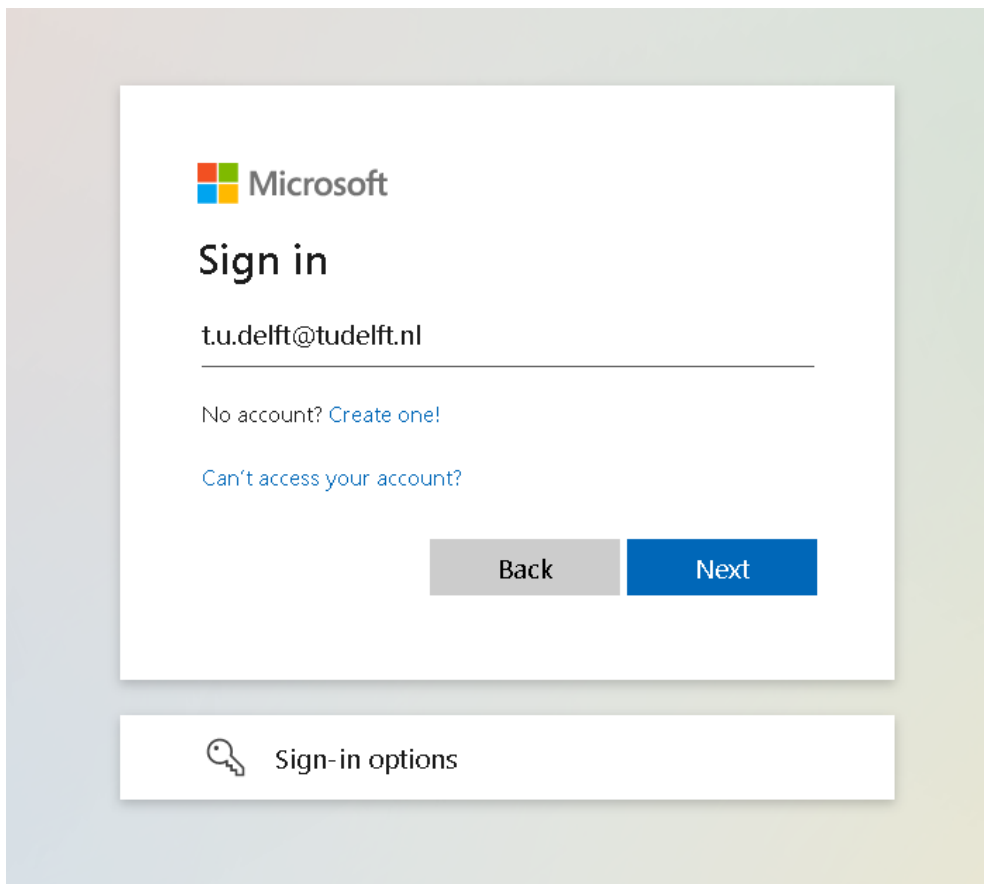
## 1.1 TU Delft services

Apart from Microsoft services and it's SSO, the TU Delft has its own SSO solution outside of the Microsoft ecosystem. The TU Delft's own SSO solution is provided via "**login.tudelft.nl**".

For more information and instruction regarding this, see the <https://www.tudelft.nl/en/it-manuals/login> and choose "Login with NetID (2FA)".

## 1.2 Microsoft services

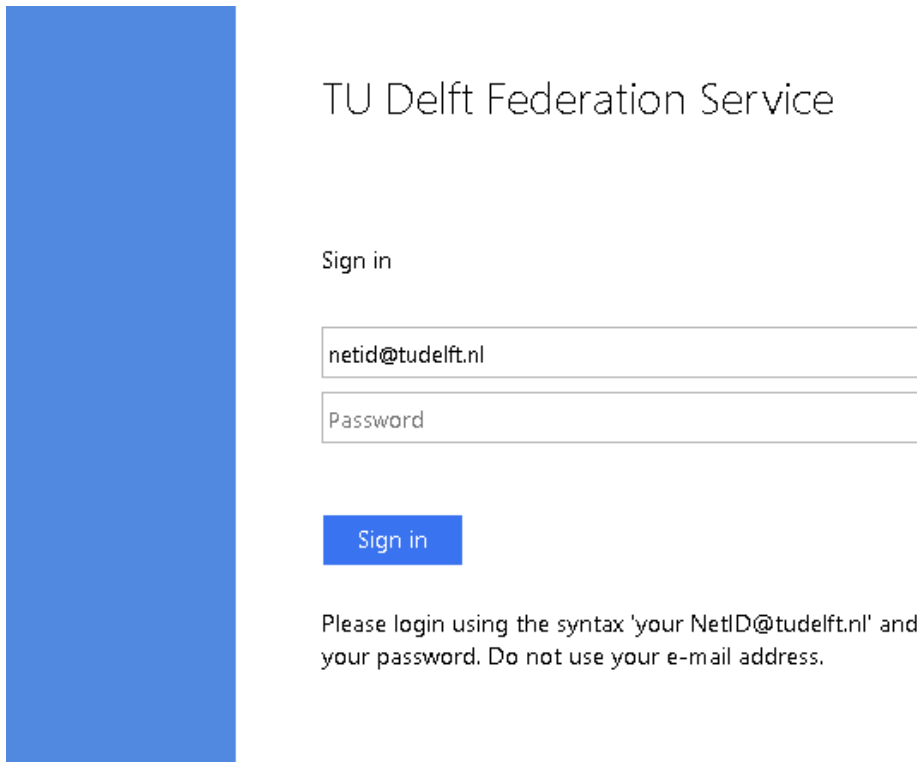
You can login with your NetID account and password at TU Delft services provided via Single Sign On (SSO). However, when trying to logon to a TU Delft service provided by **Microsoft**, you will be shown <https://login.microsoftonline.com> like the following page:



The screenshot shows the Microsoft Sign in interface. At the top is the Microsoft logo. Below it, the text "Sign in" is displayed. The email address "t.u.delft@tudelft.nl" is entered in the text box. Below the text box, there are two links: "No account? Create one!" and "Can't access your account?". At the bottom of the sign-in box are two buttons: "Back" and "Next". Below the sign-in box is a separate box with a key icon and the text "Sign-in options".



When you enter your TU Delft mailaddress, your browser will forward you to the TU Delft's own SSO Server which handles all Microsoft SSO services. You will then see the following login page from “**adfs.tudelft.nl**” or “**adfs.tudelft.net**”:

The image shows a login page for the TU Delft Federation Service. On the left is a large blue vertical rectangle. To its right, the text "TU Delft Federation Service" is displayed. Below this, the text "Sign in" is shown. There are two input fields: the first contains the text "netid@tudelft.nl" and the second is labeled "Password". Below the input fields is a blue button with the text "Sign in". At the bottom, a message reads: "Please login using the syntax 'your NetID@tudelft.nl' and your password. Do not use your e-mail address."

On this page you should enter as requested your NetID account username, and your password which have setup earlier via <https://password.tudelft.nl>.

# 2 MFA Enrolment

When using 'any' SSO service provided through and by the TU Delft, it is advised to use the "Microsoft Authenticator App" which can be found here:

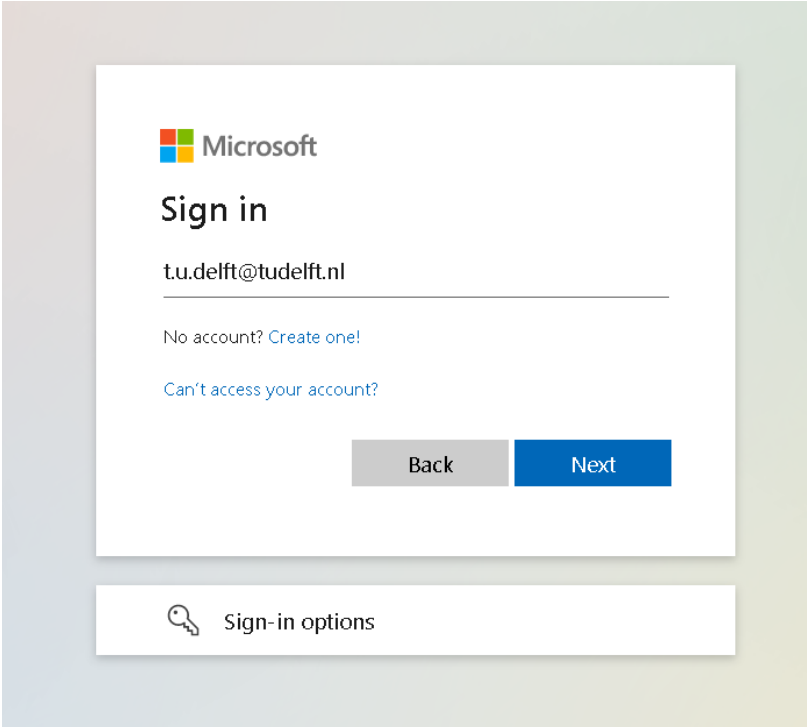
<https://www.microsoft.com/en-GB/security/mobile-authenticator-app>

If you have not yet enrolled your smartphone or smart device yet or just want to change it, then you could visit the following address to initiate an MFA enrolment process:

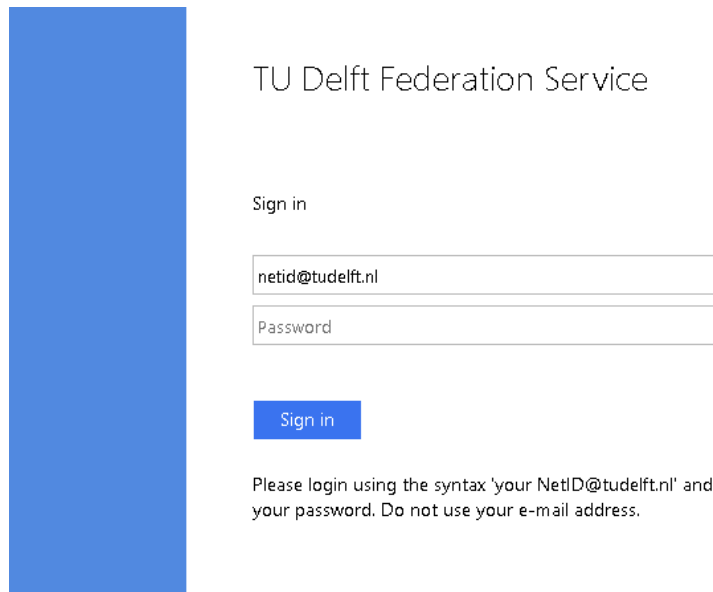
<https://aka.ms/mfasetup>

## 2.1 New MFA registration

**Step 1:** Go to <https://aka.ms/mfasetup> on a **desktop computer or laptop** and fill in your TU Delft mailaddress:

A screenshot of the Microsoft Sign in page. The page has a white background with a light gray border. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed. Underneath, the email address "t.u.delft@tudelft.nl" is entered in a text field. Below the text field, there are two links: "No account? Create one!" and "Can't access your account?". At the bottom right of the sign-in area, there are two buttons: "Back" (gray) and "Next" (blue). Below the sign-in area, there is a section titled "Sign-in options" with a key icon.

**Step 2:** Sign in using your TU Delft **NetID** Account:



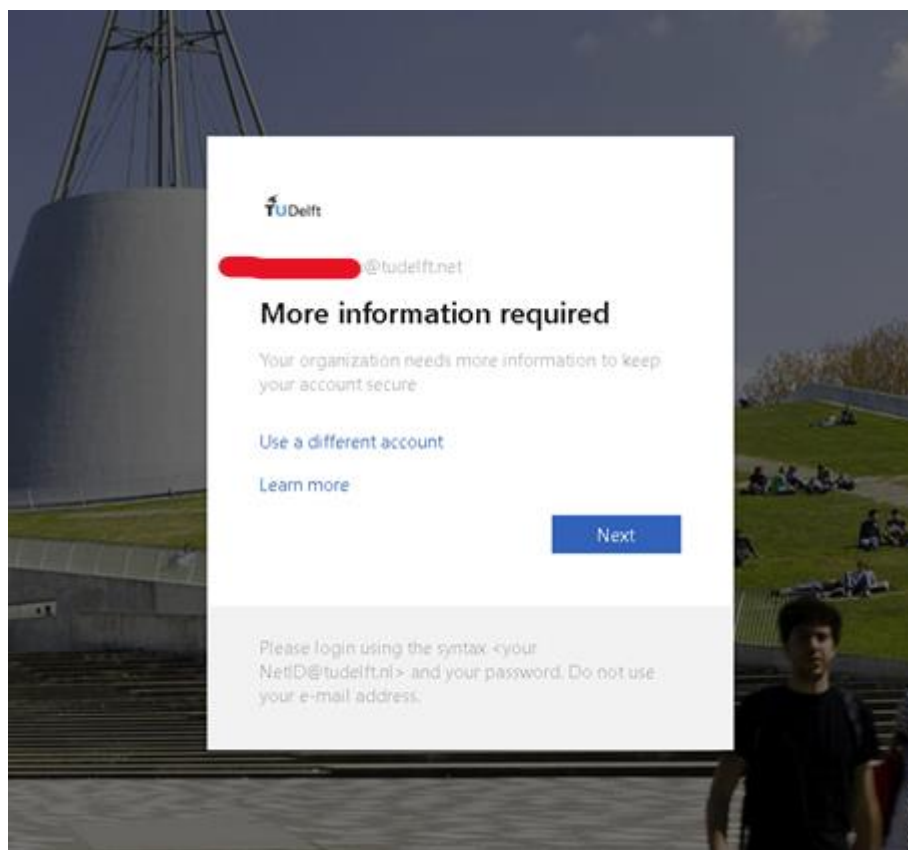
TU Delft Federation Service

Sign in

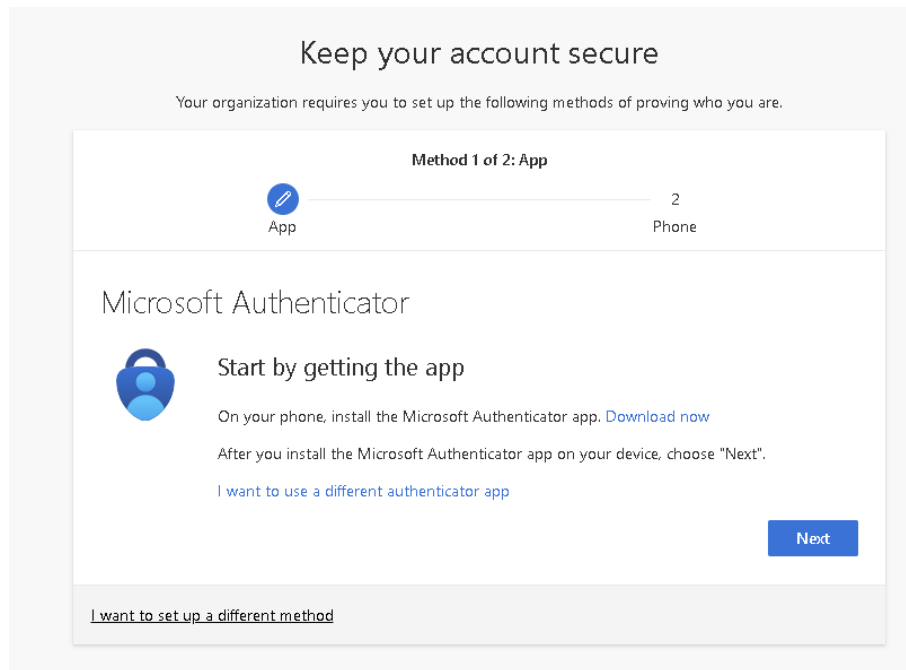
[Sign in](#)

Please login using the syntax 'your NetID@tudelft.nl' and your password. Do not use your e-mail address.

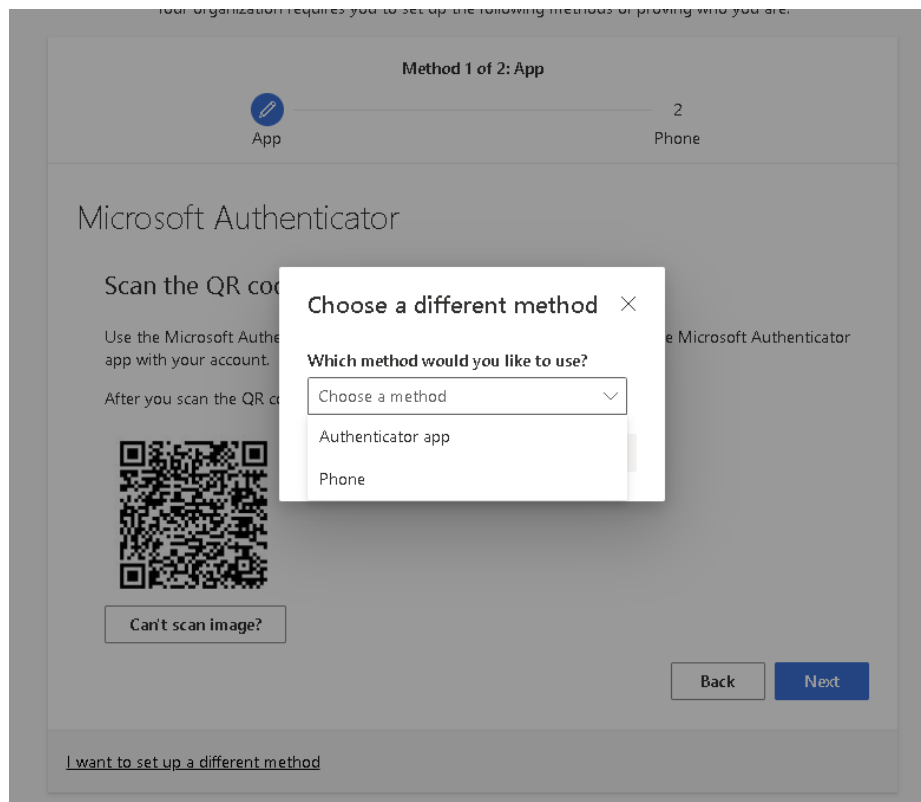
**Step 3:** You should see the following when have not yet registered any MFA device, click here on next:



**Step 4:** Follow the instructions as requested:



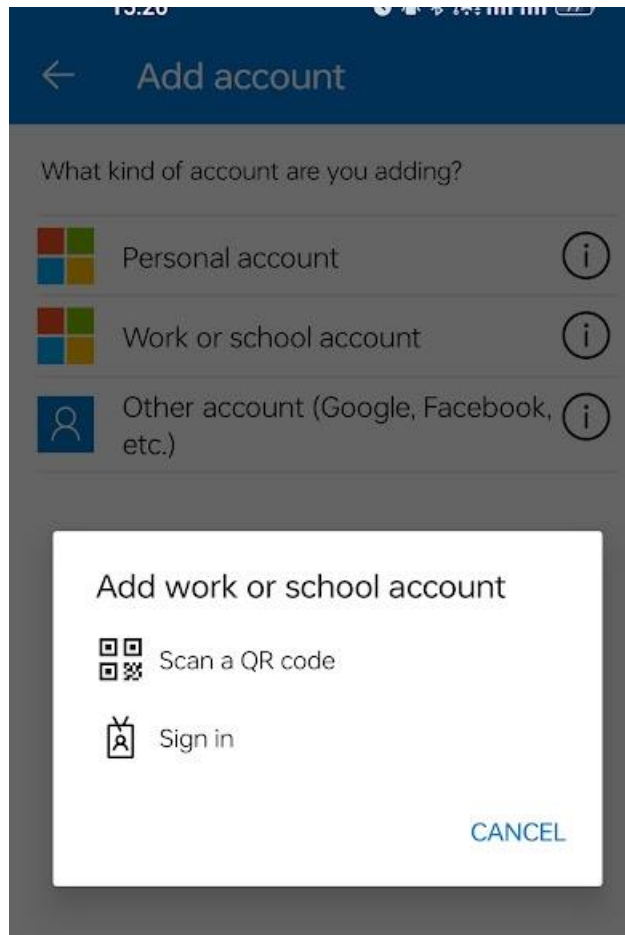
**Step 5:** Select Mobile app from the dropdown menu:



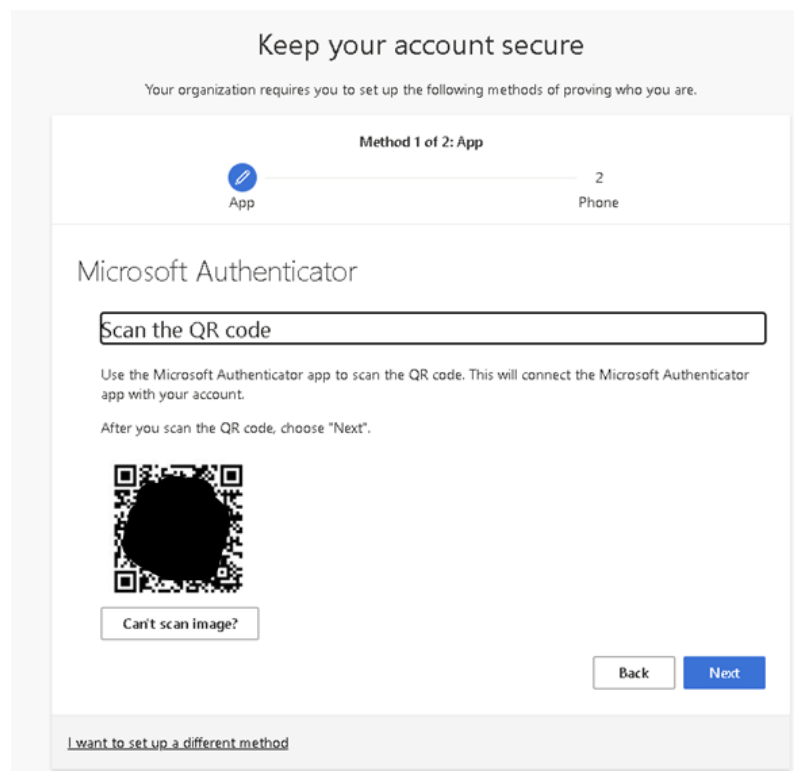
**Step 6:**

- Open the Microsoft Authenticator app on your smartphone.
- Tap the + button in the upper-right corner.
- Select Work or school account.
- You should now see a popup to scan a QR code:



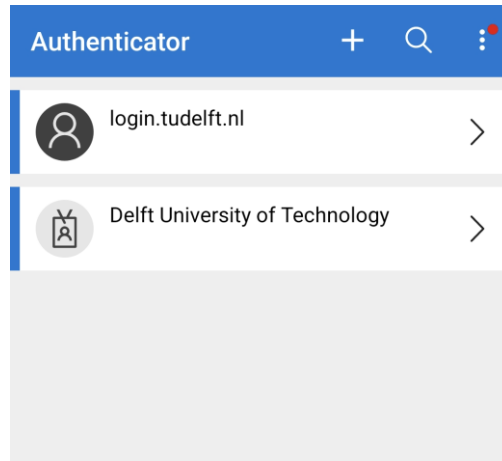


**Step 7:** Scan the QR code on your computer with your smartphone:



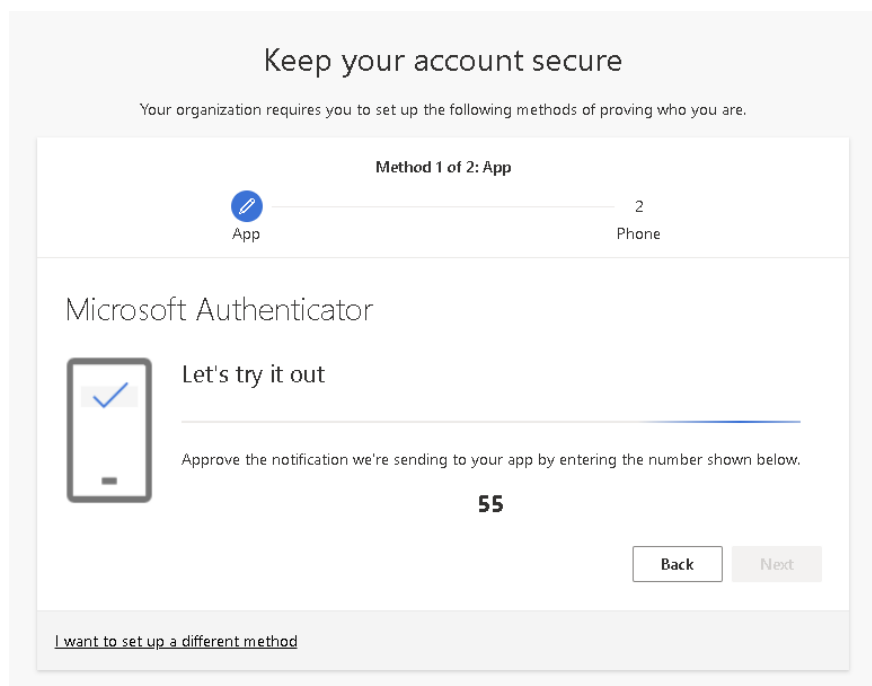
Your account will be added to the Microsoft Authenticator app automatically after you click on Next.

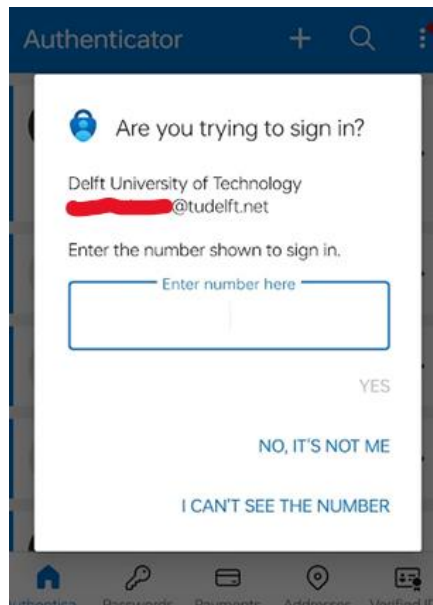
**Step 8:** To verify your account by entering the six-digit code from the Microsoft Authenticator app on your computer and click “Verify”.



Choose “**Delft University of Technology**” to see the token.

**Step 9:** Verify App by entering the number shown on your computer in the mobile app notification popup:





As shown in this example you should enter the number 55 in the Authenticator App to verify your login.

*If you do not get a notification requesting input from the authenticator app, then you should enable all notifications regarding the Microsoft Authenticator App in your smartphone settings.*

Your smartphone is now registered to <https://aka.ms/mfasetup> with the Microsoft Authenticator app. Whenever you sign in to your Microsoft work or school account, you will be prompted to enter a verification code from the Microsoft Authenticator app. This helps to protect your account from unauthorized access.

**Step 10 (optional):** In the next steps you will see the option to add a mobile number as a back-up method, follow the instructions to complete this step:

### Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Method 2 of 2: Phone

App

Phone

#### Phone

You can prove who you are by answering a call on your phone or receiving a code on your phone.

What phone number would you like to use?

Netherlands (+31)

6123123123

☒ Receive a code

☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

[I want to set up a different method](#)

# 3 Troubleshooting

## *3.1 Change MFA:*

If you have had setup a MFA Registration before, and you want to change or transfer your MFA settings to another device. Then you can visit the self-service portal of the Microsoft MFA environment at:

<https://aka.ms/mfasetup>

## *3.2 MFA Device lost*

If you have lost your smart device containing the Microsoft MFA profile, and you are not able to use your mobile number to re-enroll a new device.

Then you should contact the Service point of your faculty for requesting a MFA change.

By doing this you will be requested to verify your identity and credentials by one of our colleagues to ensure that you are the owner of the NetID account.