MFA – Multi-Factor Authentication

What is multi-factor authentication?

Everyone is familiar with the multi-factor authentication (MFA) process from withdrawing money at an ATM: The first factor is the bank card, the second factor is the PIN. In online banking, a combination of log-in data and transaction number (TAN) is used. Customers receive the TAN, which is only valid once, as an SMS (smsTAN) or app notification (pushTAN) on their smartphone, or they generate it themselves using a TAN generator and chip card (chipTAN).

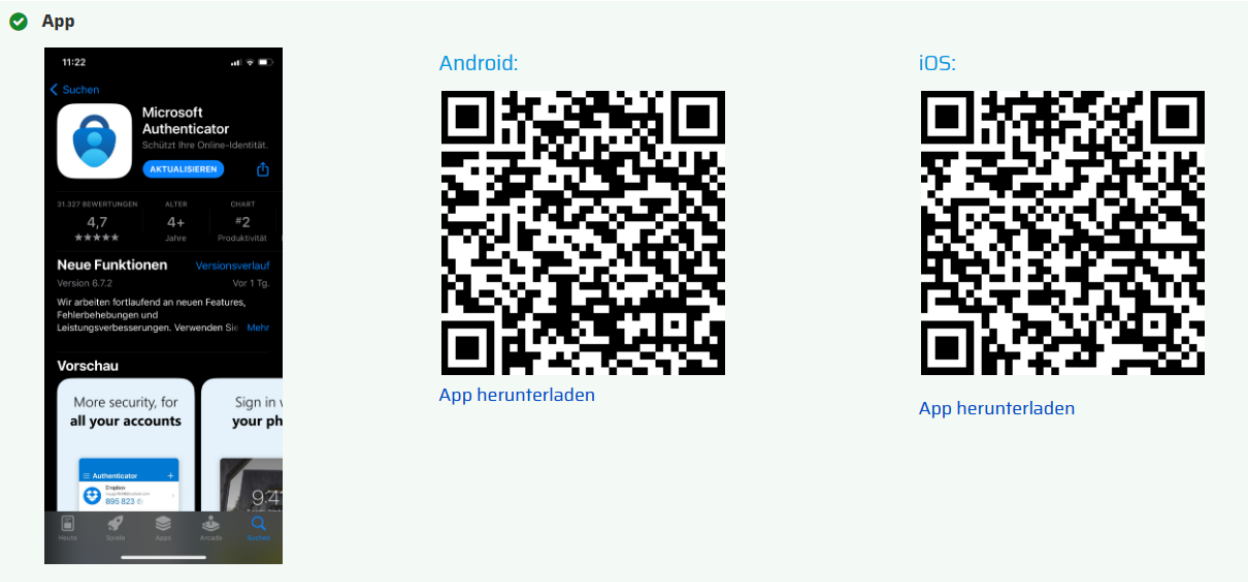
Transferred to the Deggendorf University of Technology, your first factor is the already known username-password combination, which you already needed daily to log in to Windows or to web services PLUS in the future a second factor via an app release.

How do I set up multi-factor authentication?

As a primary second factor in addition to the already known username/password combination, we recommend that students use the smartphone app **"Microsoft Authenticator"** (*or any other OATH/TOTP app such as Google Authenticator*). To avoid being locked out after changing your cell phone, it is recommended that you configure a backup for your smartphone or, as a fallback solution, configure your cell phone number as an additional second factor (TAN will then be sent via SMS). However, if you have a security key, you can of course also store it.

MFA initial setup – prompt

1. Download the app “Microsoft Authenticator” on your smartphone

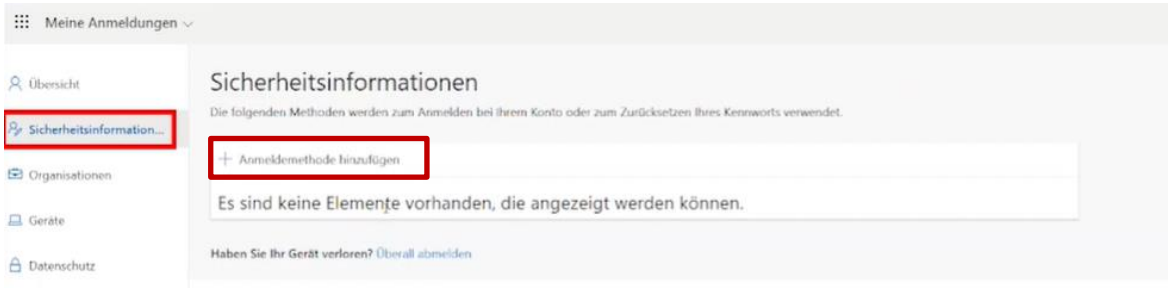


Deggendorf Institute of Technology
Dieter-Görlitz-Platz 1
94469 Deggendorf, Germany

Tel.: +49 991 3615-0
Fax: +49 991 3615-297

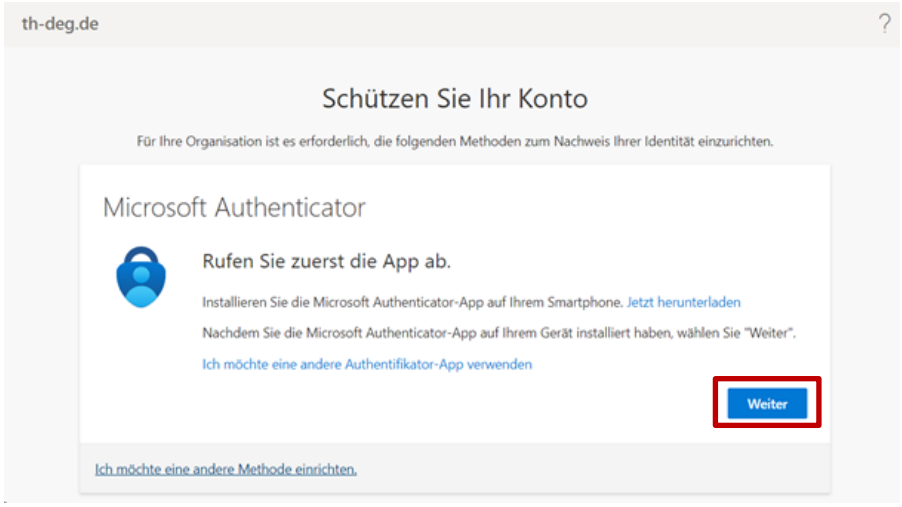
www.th-deg.de
info@th-deg.de

2. Login to MySign-Ins

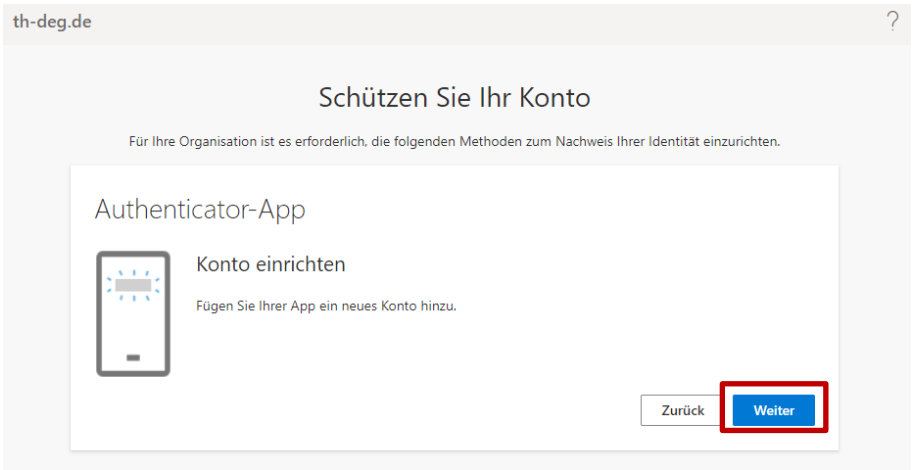


→ Select “Sicherheitsinformationen”, click on “Anmeldemethode hinzufügen“ and choose „Authenticator App”.

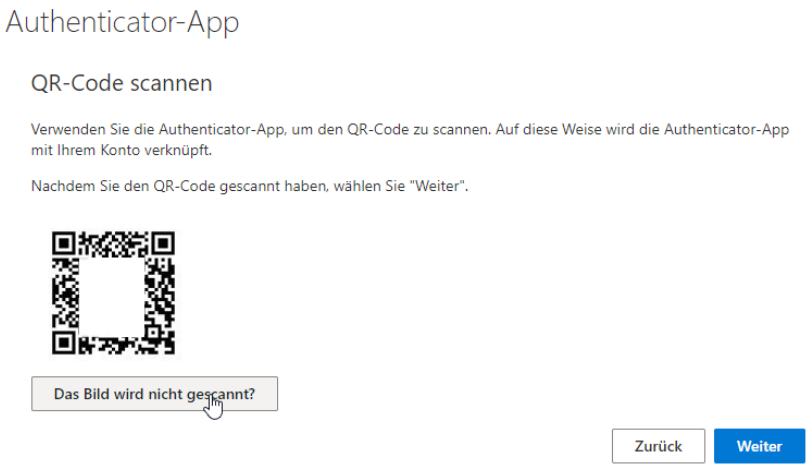
3. Request to set up the second factor



→ Click “next”.

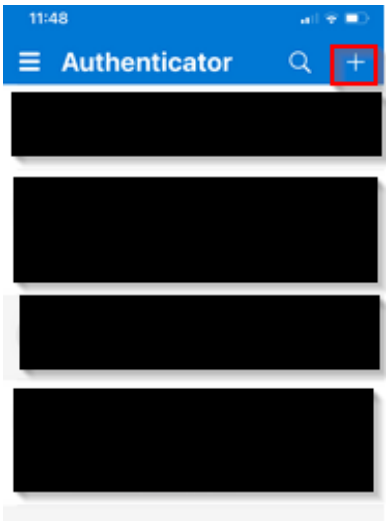


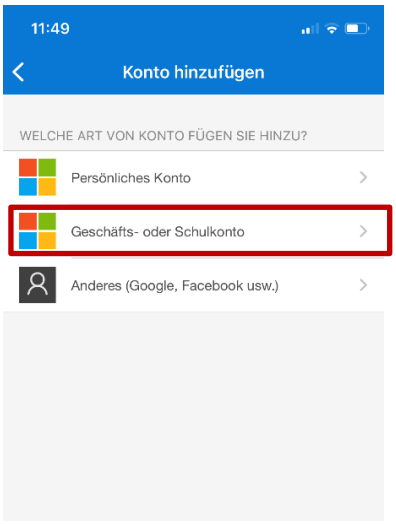
→ Click “next” again.



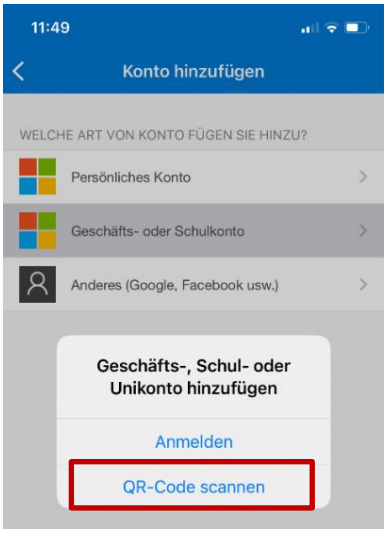
→ Leave this window open and launch the previously installed Authenticator app on your smartphone.

4. Add another “business or school account” in the Authenticator app

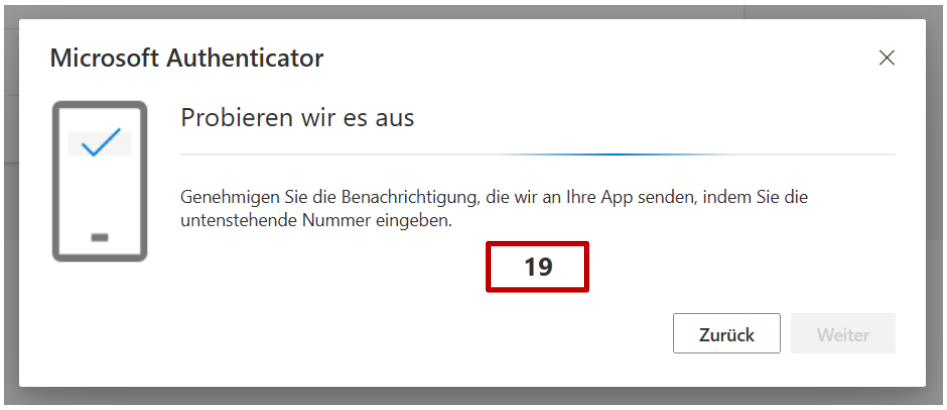




5. Select “Scan QR Code” to connect the account. Here, the previously generated QR Code from the “My-Sign Ins” portal must then be scanned



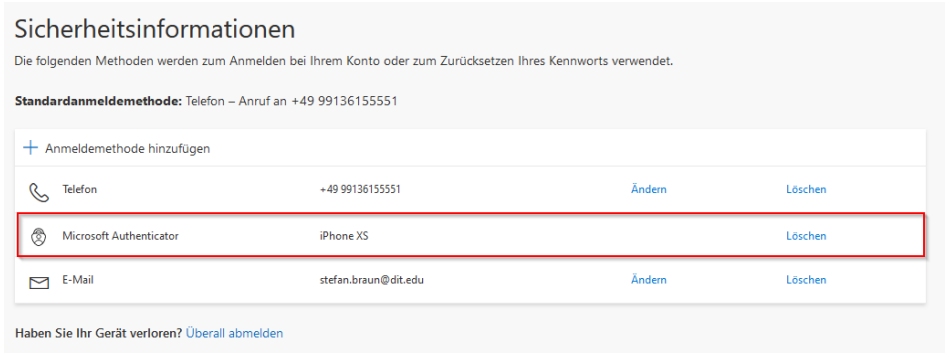
6. The following message appears – the specified code must then be entered in the app



7. App successfully filed

→ The account data will now be synchronized, and the account will be set up ready.

8. The “Authenticator App” is listed as a login method in the My Sign-Ins portal



9. You will be notified via the app for future login attempts. In the app, you then check the legitimacy of the login and approve it if necessary