Guide to managing two-factor authentication (2FA)

Login with 2FA

As usual, you start the login process by entering your username (TU ID) and password (Figure 1).
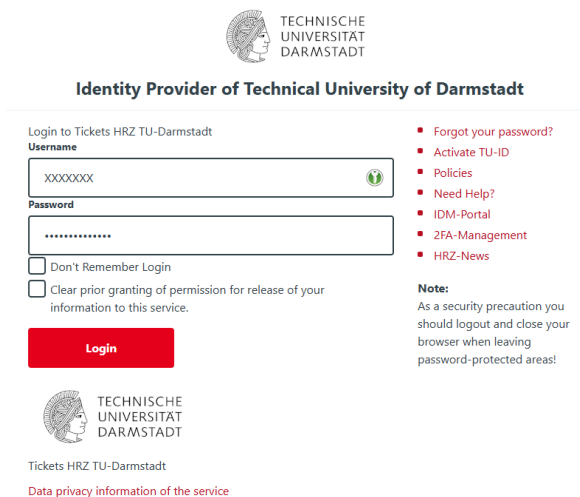

Figure 1: Login username and password

After clicking on '**Login**', you will be asked to enter your second factor. The second factor is the software or hardware token you have set up. In our example, this is the software token 'myMobil-Authenticator' (Figure 2).
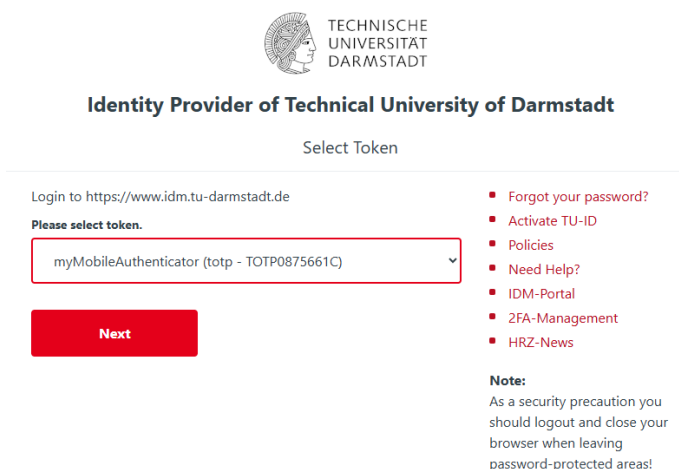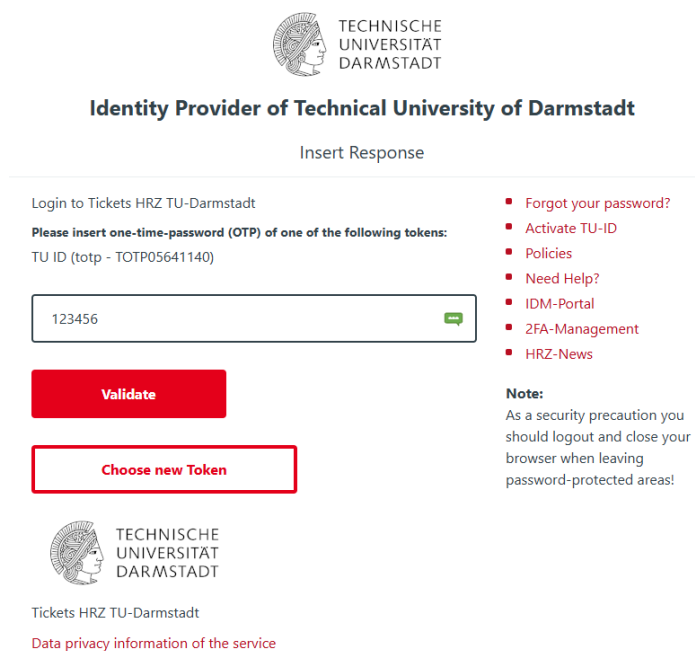

Figure 2: Selection of the token

When you select the token, you will be prompted to enter your one-time password (OTP) (Figure 3).

This one-time password is generated by your authenticator application (in our case, privacyIDEA Authenticator) and consists of 6 digits.

Enter the one-time password and confirm with '**Verify**'. If you have entered everything correctly, you will be logged in with the second factor and can use the service you are logging in to.

If you have rolled out multiple tokens in 2FA management, you can also select a different token by clicking on '**Choose new token**'.

Figure 3: Enter one-time password (OTP)