

## Anleitung zur Verwaltung der Zwei-Faktor-Authentifizierung (2FA)

### Login mit 2FA

Der Login beginnt wie gewohnt mit der Eingabe Ihres Benutzernamens (TU-ID) und Passworts (Abbildung 1).



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

**Identity Provider der Technischen Universität Darmstadt**

Anmelden bei Zentrales Web Content Management System (WCMS)  
der TU Darmstadt

**Benutzername**

**Passwort**

Anmeldung nicht speichern

Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

**Anmelden**

- Passwort vergessen?
- Aktivierung der TU-ID
- Regelwerke
- Hilfe benötigt?
- IDM-Portal
- 2FA-Verwaltung
- HRZ-News

**Hinweis:**  
Aus Sicherheitsgründen sollten Sie sich bei Verlassen der geschützten Bereiche explizit ausloggen und Ihren Webbrowser schließen!

Abbildung 1: Login Benutzername und Passwort

Nachdem Sie die „Anmelden“ geklickt haben, werden Sie aufgefordert Ihren 2. Faktor einzugeben. Der 2. Faktor ist der von Ihnen eingerichtete Software- oder Hardware-Token. In unserem Beispiel ist das der **Software-Token „myMobileAuthenticator“** (Abbildung 2).



Abbildung 2: Auswahl des Tokens

Wenn Sie den Token auswählen, werden Sie zur Eingabe Ihres Einmalpassworts (OTP) aufgefordert (Abbildung 3).

Dieses Einmalpasswort wird z.B. von Ihrer Authenticator-Anwendung (in unserem Fall *privacyIDEA Authenticator*) generiert und besteht aus 6 Ziffern.

Tragen Sie das Einmalpasswort ein und bestätigen Sie mit „**Überprüfen**“. Wenn Sie alles korrekt eingetragen haben, erfolgt Ihr Login mit dem 2. Faktor und Sie können den Dienst, für den Sie sich anmelden, benutzen.

Falls Sie mehrere Tokens in der 2FA-Verwaltung ausgerollt haben, können Sie auch einen anderen Token auswählen, indem Sie auf „**Anderen Token wählen**“ klicken.



Abbildung 3: Eingabe des Einmalpassworts (OTP)