

Aktivierung der Multifaktor- Authentifizierung für SSO

Kurzanleitung

Wien, 21.07.2026, Version 5

Entdecken,
worauf es
ankommt.

Inhalt

1	Einleitung	3
2	Multifaktor-Authentifizierung für SSO einrichten	3
3	Authenticator App (OTP).....	5
3.1	Einrichtung Authenticator App	6
4	Passkey/FIDO2.....	7
4.1	Was ist FIDO2 / Passkey?	7
4.2	Einrichtung Passkey am Beispiel YubiKey	7
5	SSO Anmeldung mit Multifaktor-Authentifizierung	9
5.1	Anmeldung mit Authenticator App.....	9
5.2	Anmeldung mit Passkey	11

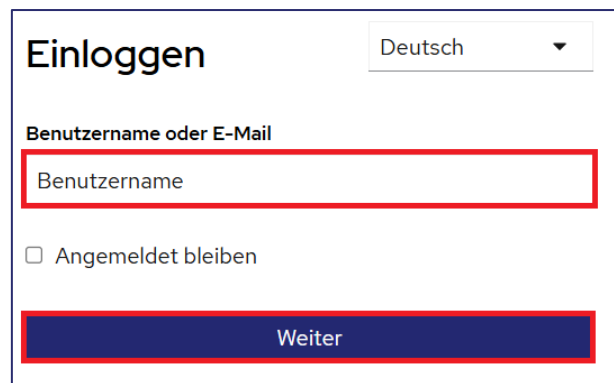
1 Einleitung

Ab dem 01.07.2026 ist am SingleSignOn-Portal (sso.fwf.ac.at) die Multifaktor-Authentifizierung (MFA) für externe User:innen verpflichtend. Das bedeutet, dass auf dem Handy und am Notebook kein Login mehr mit Passwort möglich ist. Das Passwort wird künftig nur mehr bei der **Erstregistrierung** am SingleSignOn-Portal benötigt.

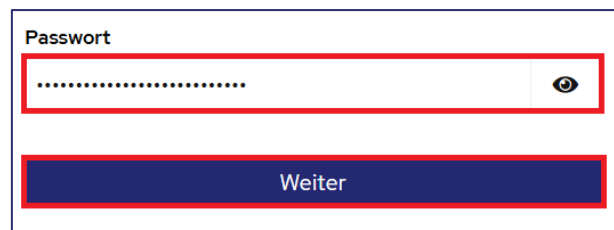
2 Multifaktor-Authentifizierung für SSO einrichten

Im Browser die URL <https://sso.fwf.ac.at/auth/realms/sso/account/#/> aufrufen.

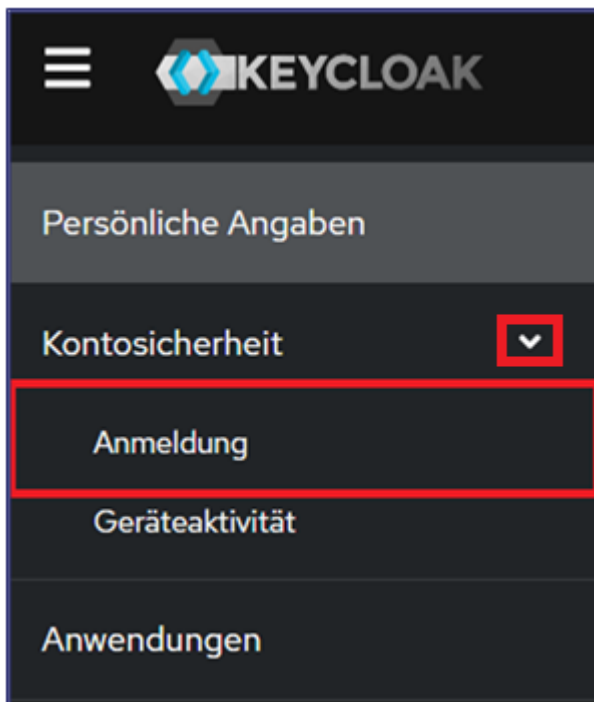
Den Benutzernamen eingeben und auf „**Weiter**“ klicken.



Im nächsten Schritt das Passwort eingeben und auf „**Weiter**“ klicken.



Im nächsten Schritt ist im Dropdown-Menü „**Kontosicherheit**“ der Punkt „**Anmeldung**“ auszuwählen.



Im nächsten Schritt muss die gewünschte Authentisierungsmethode ausgewählt werden:

- Für die Einrichtung einer Authenticator-App mit TOTP wird **„Authenticator-Anwendung einrichten“** ausgewählt. Weitere Schritte [Kapitel 4.1](#).
- Soll ein Passkey als zweiter Faktor hinterlegt werden, wird **„Passkey einrichten“** ausgewählt. Weitere Schritte [Kapitel 5.1](#).

Zwei-Faktor-Authentifizierung	
Authenticator-Anwendung	Authenticator-Anwendung einrichten
Geben Sie bei der Anmeldung einen Verifizierungscode aus der Authenticator-Anwendung ein.	
Authenticator-Anwendung ist nicht eingerichtet.	
Passkey	Passkey einrichten
Benutzen Sie Ihren Passkey, um sich anzumelden.	
Passkey ist nicht eingerichtet.	

3 Authenticator App (OTP)

Für die Aktivierung der Multifaktor-Authentifizierung muss eine Authenticator App (OTP - One-Time-Password) auf Ihrem Smartphone installiert sein.

Auf den allermeisten Smartphones ist bereits mindestens eine App dieser Art vorinstalliert.

Falls derzeit keine OTP-App auf dem Smartphone installiert ist, ist vor Beginn der Einrichtung eine entsprechende App über den App Store des jeweiligen Geräts zu beziehen.

Am häufigsten verwendet werden hierzu die Apps „Google Authenticator“ oder „Microsoft Authenticator“. Alternative Apps sind zum Beispiel „FortiToken Mobile“ oder „FreeOTP“.

Weitere Informationen zu diesem Thema finden Sie zum Beispiel hier:

<https://www.onlinesicherheit.gv.at/Services/News/Authenticator-Apps.html>

3.1 Einrichtung Authenticator App

Authenticator App am Handy öffnen und QR-Code auf dem Bildschirm scannen.

Mehrfachauthentifizierung konfigurieren Deutsch ▼

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:

- Microsoft Authenticator
- Google Authenticator
- FreeOTP

2. Öffnen Sie die Applikation und scannen Sie den QR-Code:



[Sie können den QR-Code nicht scannen?](#)

3. Geben Sie den von der Applikation generierten One-time Code ein und klicken Sie auf Absenden.
Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

One-time Code *
584756

Gerätename
Smartphone

☐ Von anderen Geräten abmelden

Absenden Abbrechen

Anschließend den von der Applikation generierten One-time Code und einen Gerätenamen eingeben und auf „**Absenden**“ klicken.

Wurde der Token erfolgreich gespeichert, ist die Einrichtung von SSO abgeschlossen und das Fenster kann geschlossen werden.

4 Passkey/FIDO2

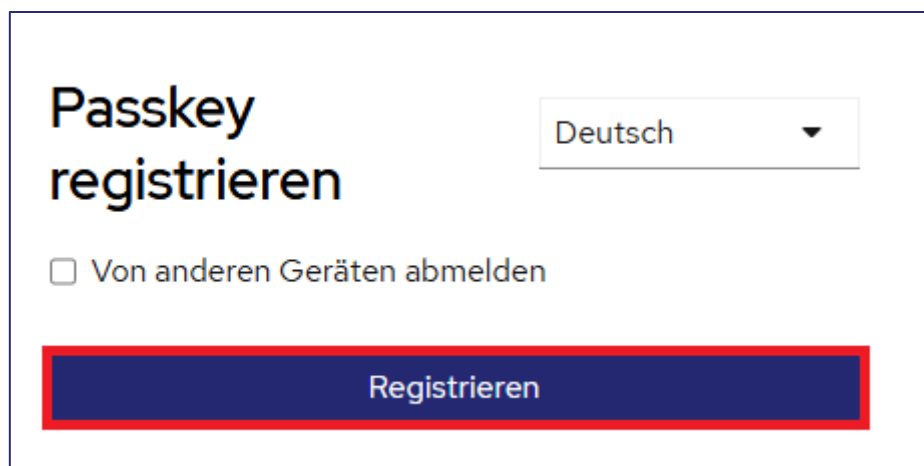
4.1 Was ist FIDO2 / Passkey?

FIDO2 ist ein moderner, besonders sicherer Anmeldestandard. Statt eines Codes wird die Identität durch einen kryptografischen Schlüssel bestätigt, der auf dem Gerät gespeichert ist. Ein Passkey kann auf einem Hardware-Token (z. B. YubiKey) oder direkt auf einem kompatiblen Gerät (z. B. Windows Hello, Face ID) hinterlegt sein.

Wichtig: FIDO2 wird nicht von allen YubiKey-Modellen unterstützt. Bei älteren Modellen (z. B. YubiKey 4) ist lediglich FIDO U2F verfügbar. Vor der Einrichtung sollte daher geprüft werden, welches Modell vorhanden ist.

4.2 Einrichtung Passkey am Beispiel YubiKey

Auf **Registrieren** klicken.



Um den Vorgang fortzusetzen müssen im nächsten Schritt erneut die Zugangsdaten eingegeben werden (FWF-Benutzername + Passwort).

Sicherheitsschlüssel auswählen.

**Wählen Sie aus, wo Ihr Hauptschlüssel
gespeichert werden soll.**



iPhone, iPad oder Android-Gerät



Sicherheitsschlüssel

Im nächsten Schritt den PIN-Sicherheitsschlüssel eingeben und diesen mit einem Klick auf **OK** bestätigen.

Geben Sie Ihre Sicherheitsschlüssel-PIN ein.

PIN-Sicherheitsschlüssel

|



Dies wird in Ihr
Sicherheitsschlüsselgespeichert.

[Ändern](#)

OK

Abbrechen

Die Bezeichnung des Passkeys (selbst zu wählender Anzeigename) eingeben und mit einem Klick auf OK bestätigen.

sso.fwf.ac.at enthält

Bitte geben Sie die Bezeichnung Ihres registrierten Passkeys ein

Passkey (Standard Bezeichnung)

OK

Abbrechen

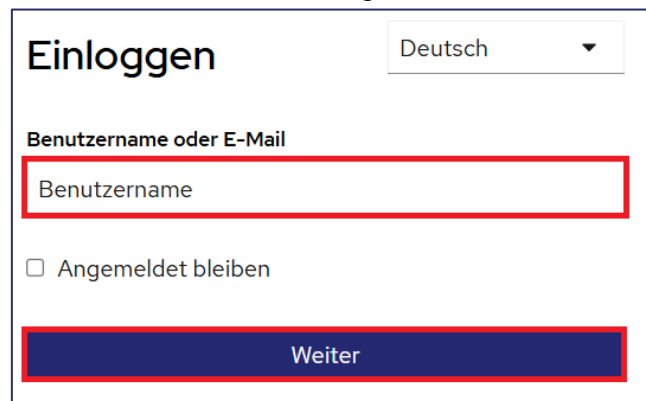
Wurde der Token erfolgreich gespeichert, ist die Einrichtung von SSO abgeschlossen und das Fenster kann geschlossen werden.

5 SSO Anmeldung mit Multifaktor-Authentifizierung

Die Anmeldung über die Login-Seite (SSO – Single Sign-On) ist nach der Erstregistrierung auf zwei Arten möglich: mittels Authenticator-App oder Passkey.

5.1 Anmeldung mit Authenticator App

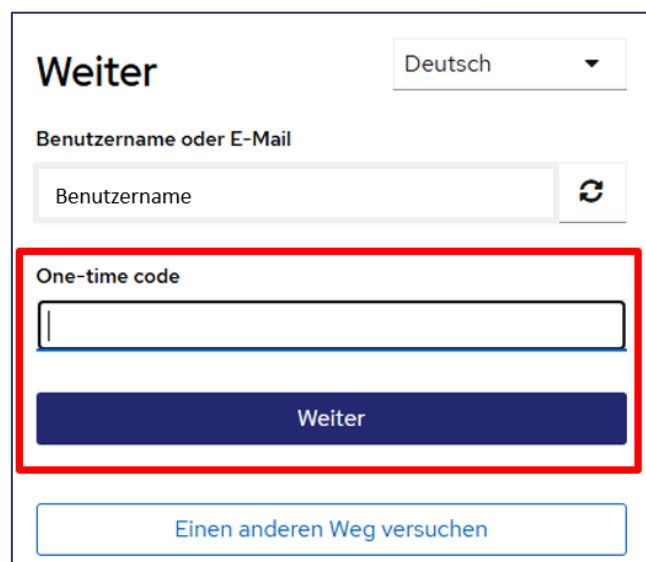
FWF-Benutzername oder Email eingeben und auf „**Weiter**“ klicken.



The screenshot shows the 'Einloggen' (Login) form. At the top right is a language dropdown menu set to 'Deutsch'. Below the title is a label 'Benutzername oder E-Mail'. Underneath is a text input field containing 'Benutzername', which is highlighted with a red rectangular border. Below the input field is a checkbox labeled 'Angemeldet bleiben'. At the bottom is a dark blue button with the text 'Weiter', also highlighted with a red rectangular border.

Die Authenticator App auf dem Smartphone öffnen.

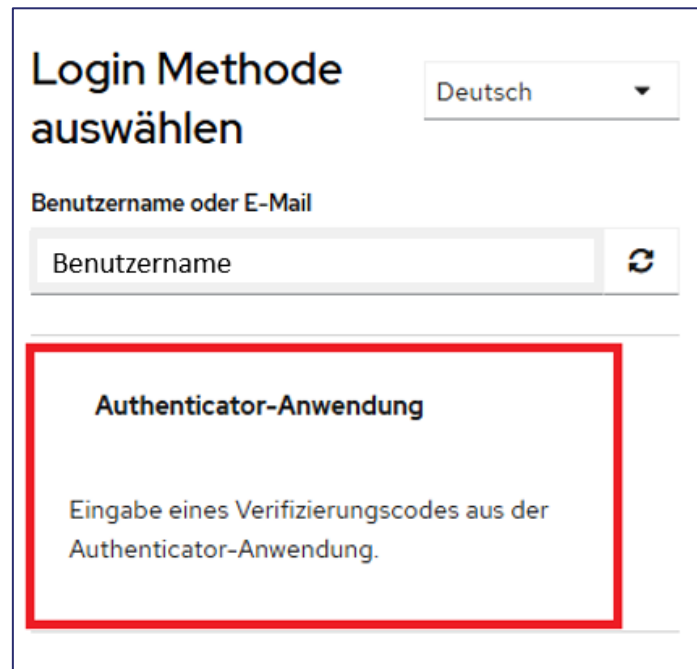
Den von der Applikation generierten One-time Code auslesen und in das Bearbeitungsfeld „**One-time code**“ eingeben. Mit einem Klick auf „**Weiter**“ bestätigen.



The screenshot shows the 'Weiter' (Continue) form. At the top right is a language dropdown menu set to 'Deutsch'. Below the title is a label 'Benutzername oder E-Mail'. Underneath is a text input field containing 'Benutzername', followed by a refresh icon (circular arrow). Below this is a label 'One-time code' above a text input field, which is highlighted with a red rectangular border. Below the input field is a dark blue button with the text 'Weiter'. At the bottom is a light blue button with the text 'Einen anderen Weg versuchen'.

Falls das Bearbeitungsfeld „One-time code“ nicht angezeigt wird auf **„Einen anderen Weg versuchen“** klicken.

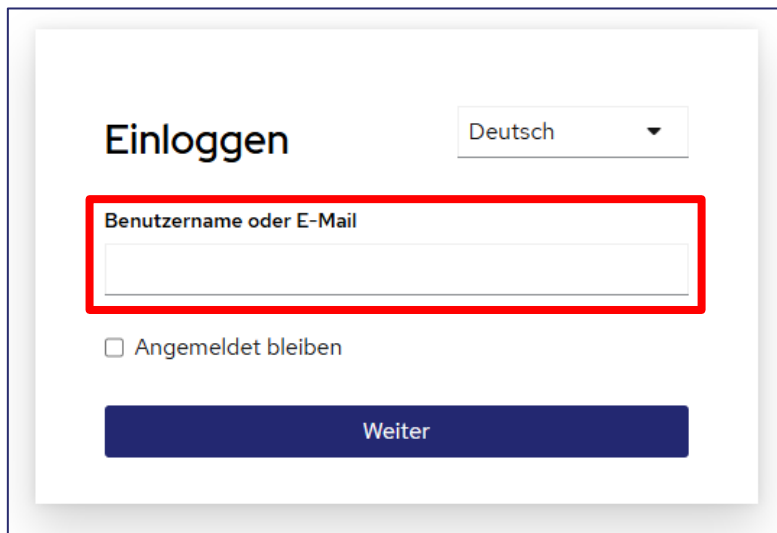
Als Login-Methode **„Authenticator-Anwendung“** auswählen.



The screenshot shows a login interface with the title "Login Methode auswählen". In the top right corner, there is a language dropdown menu set to "Deutsch". Below the title, there is a label "Benutzername oder E-Mail" and a text input field containing "Benutzername". To the right of the input field is a circular refresh icon. Below the input field, a red rectangular box highlights the "Authenticator-Anwendung" option. Under this option, the text "Eingabe eines Verifizierungscode aus der Authenticator-Anwendung." is displayed.

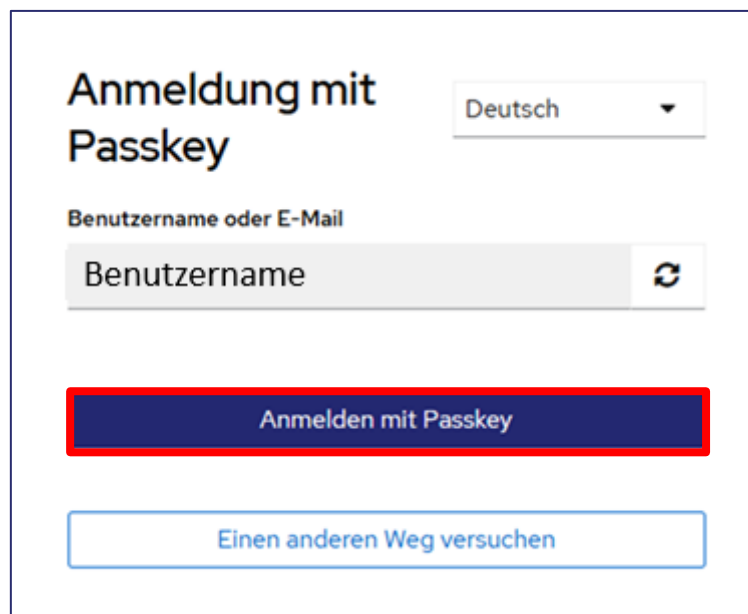
5.2 Anmeldung mit Passkey

FWF-Benutzername oder E-Mail eingeben und auf „**Weiter**“ klicken.



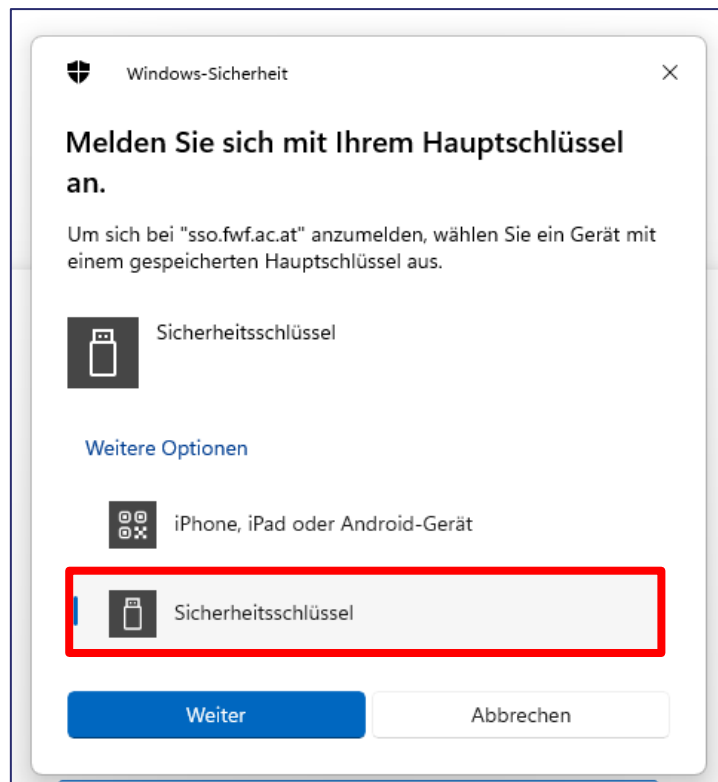
The screenshot shows a login form titled "Einloggen". In the top right corner, there is a language selector dropdown menu set to "Deutsch". Below the title, the label "Benutzername oder E-Mail" is positioned above a text input field, which is highlighted with a red rectangular border. Underneath the input field, there is a checkbox labeled "Angemeldet bleiben". At the bottom of the form, there is a dark blue button with the text "Weiter".

„Anmelden mit Passkey“ klicken.

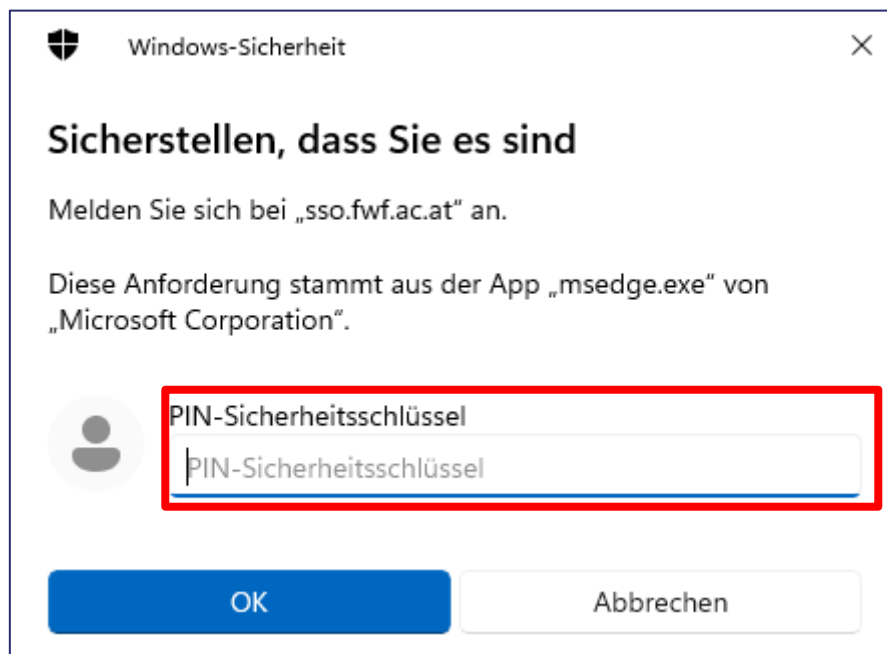


The screenshot shows a form titled "Anmeldung mit Passkey". In the top right corner, there is a language selector dropdown menu set to "Deutsch". Below the title, the label "Benutzername oder E-Mail" is positioned above a text input field. The input field contains the text "Benutzername" and has a circular refresh icon on its right side. Below the input field, there is a dark blue button with the text "Anmelden mit Passkey", which is highlighted with a red rectangular border. At the bottom of the form, there is a light blue button with the text "Einen anderen Weg versuchen".

Auf „Sicherheitsschlüssel“ und dann auf „Weiter“ klicken.



PIN-Sicherheitsschlüssel eingeben und mit einem Klick auf OK bestätigen.



Mit Finger auf den blinkenden Yubikey Knopf drücken.

