

Aktivierung der Multifaktor- Authentifizierung für SSO

Anleitung

Gültig ab 01.06.2026, Version 1.4

Entdecken,
worauf es
ankommt.

Inhalt

1	Einleitung	3
2	Multifaktor-Authentifizierung für SSO einrichten (vor dem 02.07.2026)	3
3	Multifaktor-Authentifizierung für SSO einrichten (ab dem 02.07.2026).....	5
4	Authenticator-App (OTP).....	7
4.1	Authenticator-App einrichten.....	8
5	Passkey/FIDO2.....	9
5.1	Was ist Passkey/FIDO2?	9
5.2	Passkey einrichten am Beispiel YubiKey	9
6	SSO-Anmeldung mit Multifaktor-Authentifizierung.....	11
6.1	Anmeldung mit Authenticator-App	11
6.2	Anmeldung mit Passkey	13

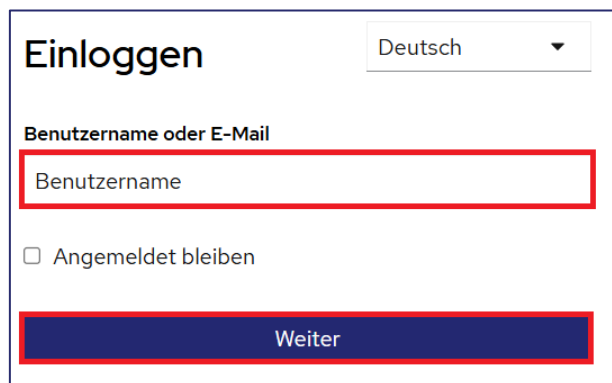
1 Einleitung

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 (vor dem 02.07.2026)

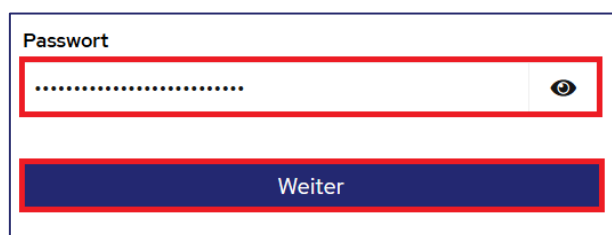
Im Browser die URL <https://sso.fwf.ac.at/auth/realms/sso/account/#/> aufrufen.

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



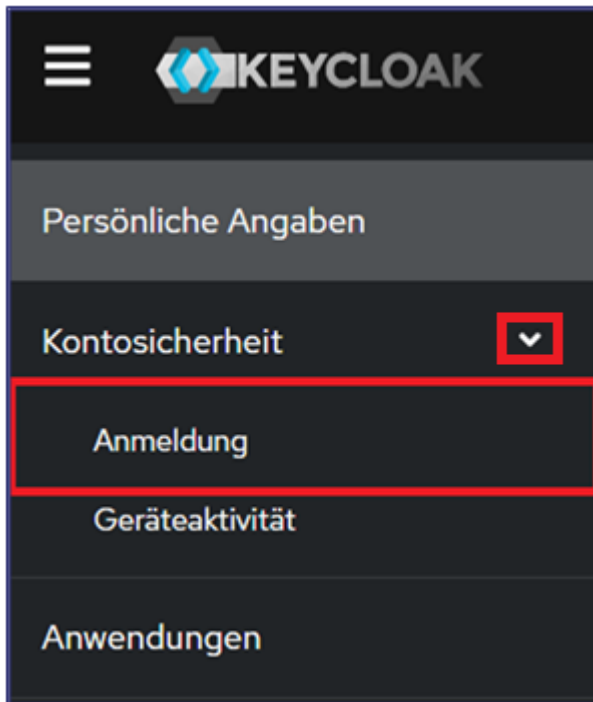
The screenshot shows a login form titled "Einloggen" with a language dropdown set to "Deutsch". Below the title is the label "Benutzername oder E-Mail" above a text input field containing "Benutzername". A red box highlights this input field. Below the input field is a checkbox labeled "Angemeldet bleiben". At the bottom of the form is a blue button labeled "Weiter", also highlighted with a red box.

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



The screenshot shows a password input field with the label "Passwort" above it. The field contains a series of dots and has a red box around it. To the right of the field is an eye icon for toggling visibility. Below the field is a blue button labeled "Weiter", also highlighted with a red box.

Im nächsten Schritt ist im Drop-down-Menü „**Kontosicherheit**“ der Punkt „**Anmeldung**“ auszuwählen:



Nun muss die gewünschte Authentifizierungsmethode ausgewählt werden:

- Für die Einrichtung einer Authenticator-App mit TOTP wird „**Authenticator-Anwendung einrichten**“ ausgewählt. Weitere Schritte siehe [Abschnitt 4.1](#).
- Soll ein Passkey als zweiter Faktor hinterlegt werden, wird „**Passkey einrichten**“ ausgewählt. Weitere Schritte siehe [Abschnitt 5.2](#).

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

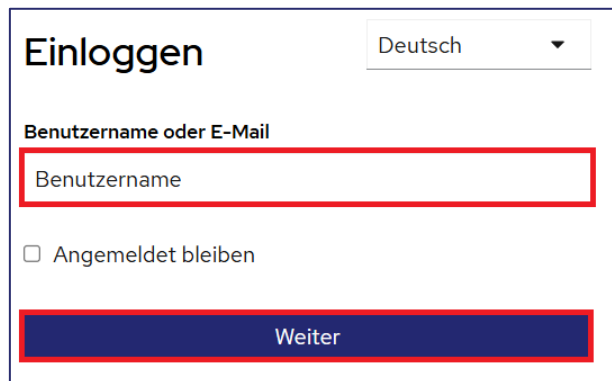
Benutzen Sie Ihren Passkey, um sich anzumelden.

Passkey ist nicht eingerichtet.

3 Multifaktor-Authentifizierung für SSO einrichten (ab dem 02.07.2026)

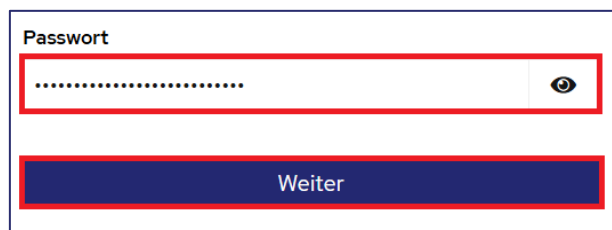
Im Browser die URL <https://sso.fwf.ac.at/auth/realms/sso/account/#/> aufrufen.

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



The screenshot shows a login form titled "Einloggen" with a language dropdown set to "Deutsch". Below the title, there is a label "Benutzername oder E-Mail" above a text input field containing "Benutzername". Below the input field is a checkbox labeled "Angemeldet bleiben". At the bottom of the form is a blue button labeled "Weiter". Red boxes highlight the input field and the "Weiter" button.

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



The screenshot shows a password entry form titled "Passwort" above a text input field containing a masked password ".....". To the right of the input field is an eye icon for toggling visibility. Below the input field is a blue button labeled "Weiter". Red boxes highlight the input field and the "Weiter" button.


Nun muss die gewünschte Authentifizierungsmethode ausgewählt werden:

- Für die Einrichtung einer Authenticator-App mit TOTP wird „**TOTP App**“ ausgewählt. Weitere Schritte siehe [Abschnitt 4.1](#).
- Soll ein Passkey als zweiter Faktor hinterlegt werden, wird „**Passkey/FIDO2**“ ausgewählt. Weitere Schritte siehe [Abschnitt 5.2](#).

Bitte wähle eine Authentisierungs- -Methode als zweiten Faktor.

Deutsch ▼

Benutzername oder E-Mail



TOTP App

Gib einen 6-stelligen Code ein, der in einer Smartphone-App generiert wird.

Passkey/FIDO2

Nutze einen Passkey oder FIDO2 USB Token. Diese Methode bringt die größte Sicherheit.

enforceMfa.webauthn-register-passwordless

enforceMfa.webauthn-register-passwordless-help-text

4 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>


4.1 Authenticator-App einrichten

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

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

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:

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

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

5 Passkey/FIDO2

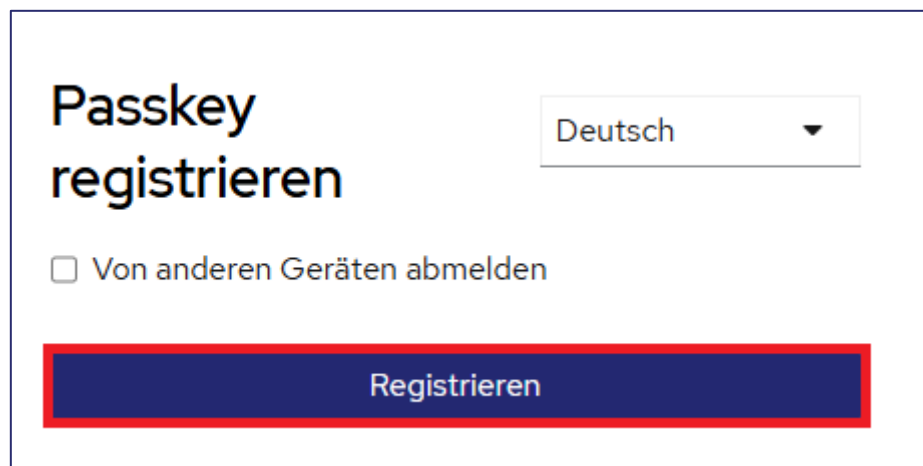
5.1 Was ist Passkey/FIDO2?

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.

5.2 Passkey einrichten am Beispiel YubiKey

Nach Auswahl von „**Passkey einrichten**“ bzw. „**Passkey/FIDO2**“ (siehe Abschnitt 2 bzw. 3) öffnet sich folgendes Fenster. Auf „**Registrieren**“ klicken:



Passkey
registrieren

Deutsch ▼


Von anderen Geräten abmelden

Registrieren

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
Sicherheitsschlüssel gespeichert.

[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

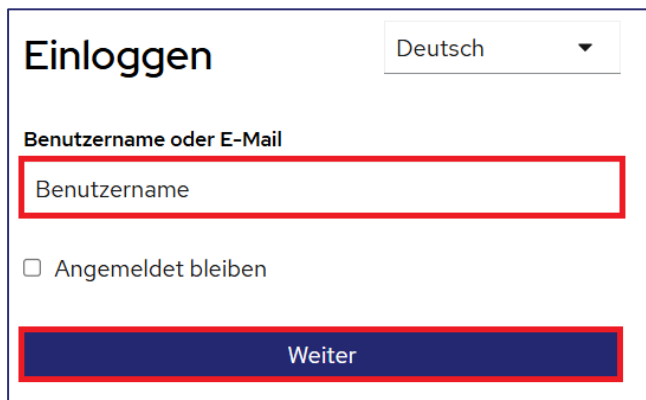
Wurde der Token erfolgreich gespeichert, ist die Einrichtung von SSO abgeschlossen und das Fenster kann geschlossen werden.

6 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.

6.1 Anmeldung mit Authenticator-App

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



Einloggen Deutsch

Benutzername oder E-Mail

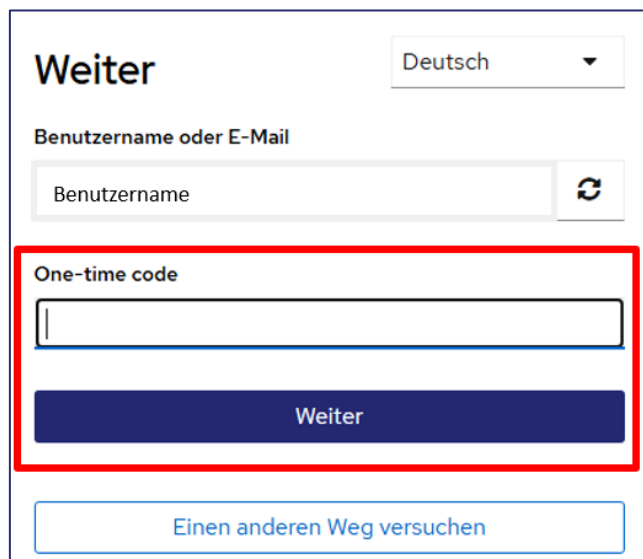
Benutzername

Angemeldet bleiben

Weiter


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:



Weiter Deutsch

Benutzername oder E-Mail

Benutzername 

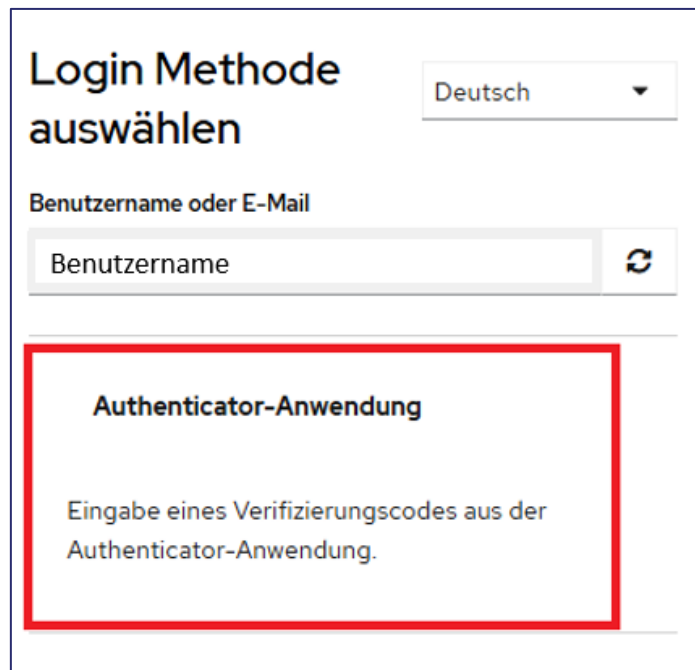
One-time code

Weiter

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:



Login Methode auswählen Deutsch ▾

Benutzername oder E-Mail

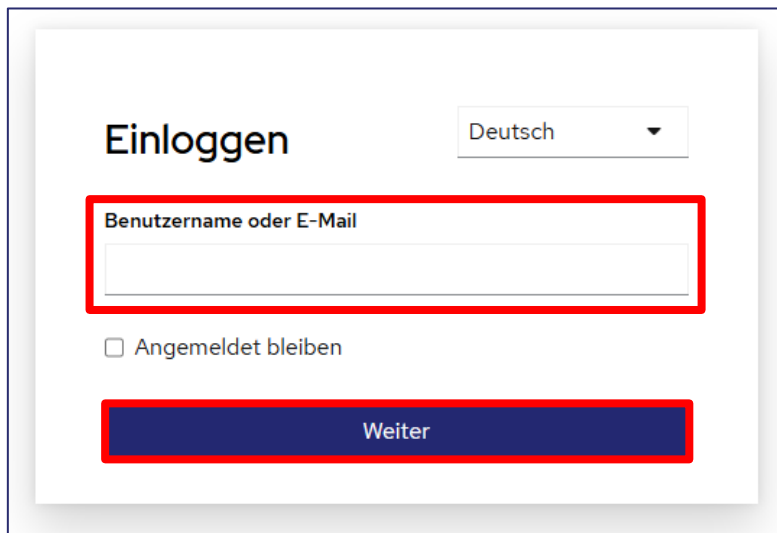
Benutzername ↻

Authenticator-Anwendung

Eingabe eines Verifizierungscodes aus der Authenticator-Anwendung.

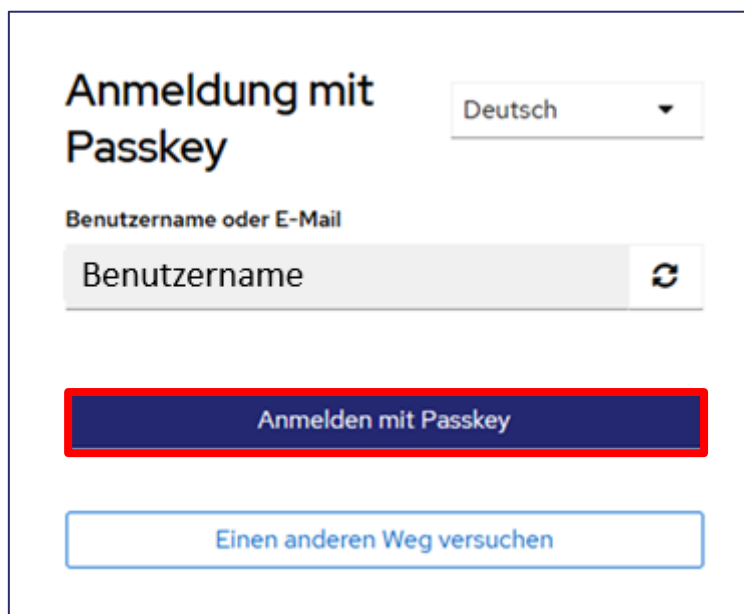
6.2 Anmeldung mit Passkey

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



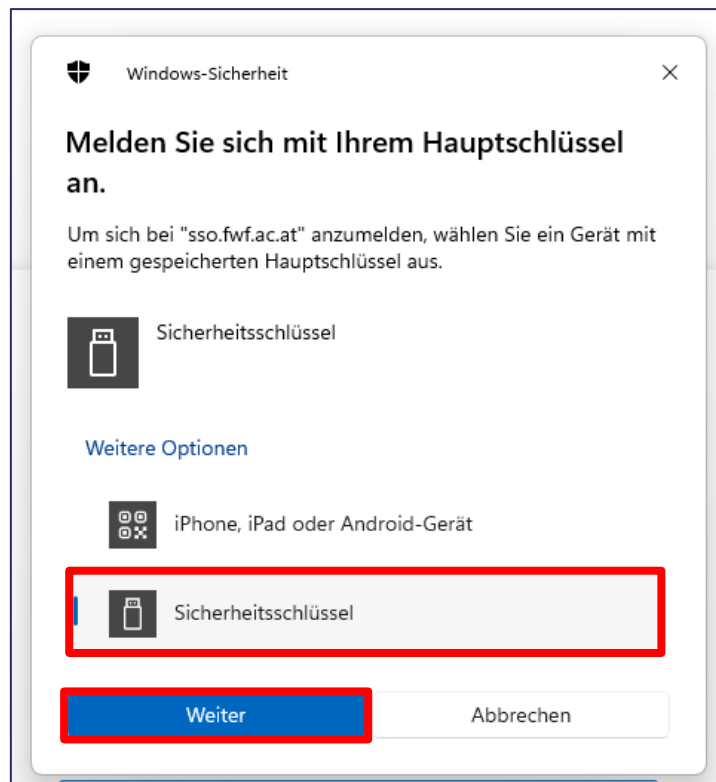
The screenshot shows a login form with the title "Einloggen" and a language dropdown menu set to "Deutsch". A red box highlights the input field labeled "Benutzername oder E-Mail". Below the input field is a checkbox labeled "Angemeldet bleiben". At the bottom, a blue button labeled "Weiter" is highlighted with a red border.

Auf „**Anmelden mit Passkey**“ klicken:

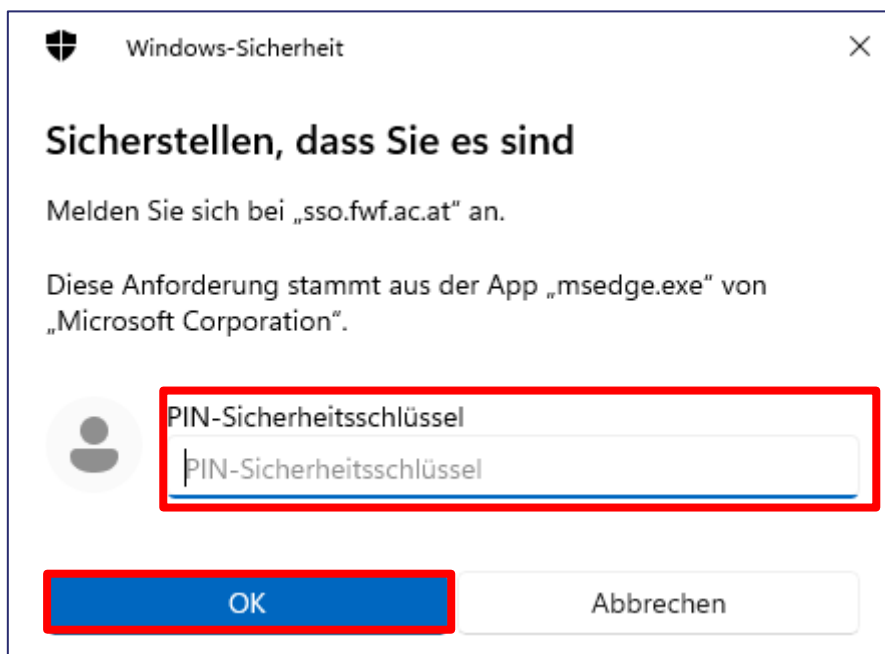


The screenshot shows a page titled "Anmeldung mit Passkey" with a language dropdown menu set to "Deutsch". Below the title is a label "Benutzername oder E-Mail" and an input field containing "Benutzername" with a refresh icon on the right. A blue button labeled "Anmelden mit Passkey" is highlighted with a red border. Below it is a light blue button labeled "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.

