FWF Österreichischer Wissenschaftsfonds

Aktivierung der Multifaktor-Authentifizierung für SSO

Anleitung

Gültig ab 01.06.2026, Version 1.4

Entdecken, worauf es ankommt.

FWF Österreichischer Wissenschaftsfonds

Inhalt

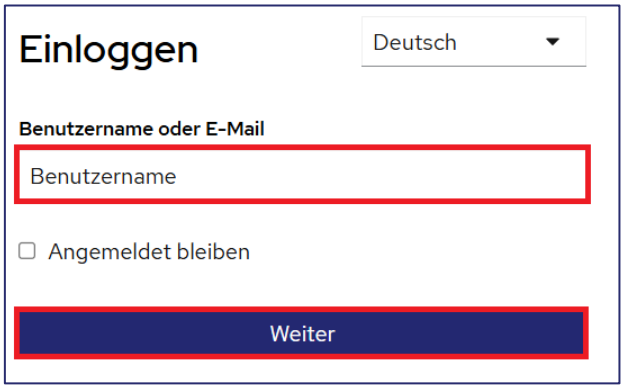
1 Einleitung

Ab dem 01.07.2026 ist am SingleSignOn-Portal (sso.fwf.ac.at) die Mehrfaktor-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.

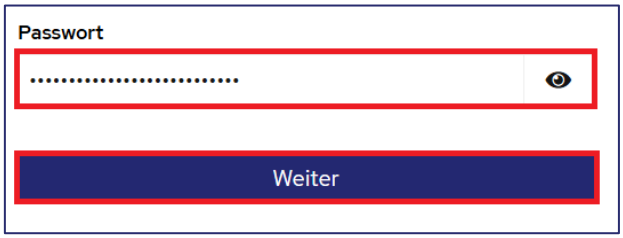
2 Multifaktor-Authentifizierung für SSO einrichten (vor dem 02.07.2026)

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

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



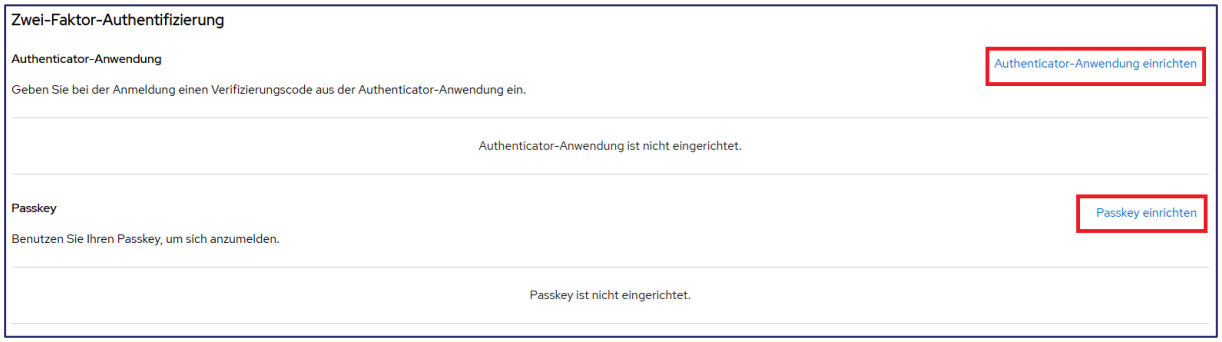
Im nächsten Schritt das Passwort eingeben und auf **„Weiter“** klicken:



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

Nun muss die gewünschte Authentifizierungsmethode ausgewählt werden:

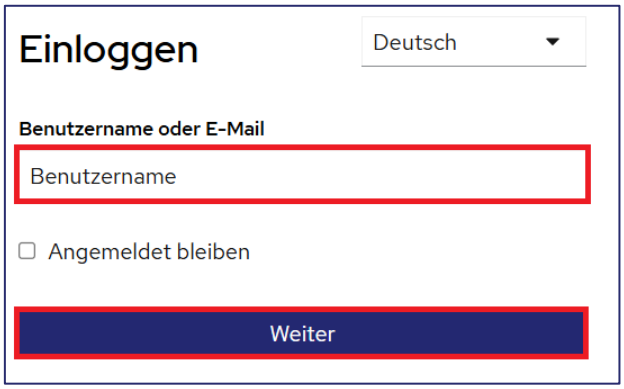
- Für die Einrichtung einer Authenticator-App mit TOTP wird **„Authenticator-Anwendung einrichten“** ausgewählt. Weitere Schritte siehe Abschnitt 4.1.
- Soll ein Passkey als zweiter Faktor hinterlegt werden, wird **„Passkey einrichten“** ausgewählt. Weitere Schritte siehe Abschnitt 5.2.



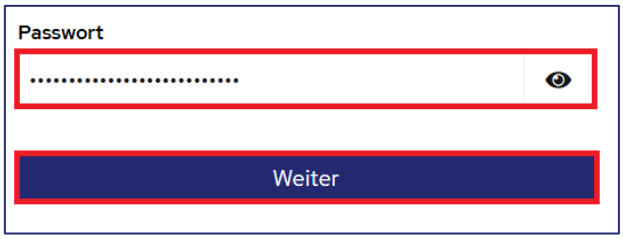
3 Multifaktor-Authentifizierung für SSO einrichten (ab dem 02.07.2026)

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

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

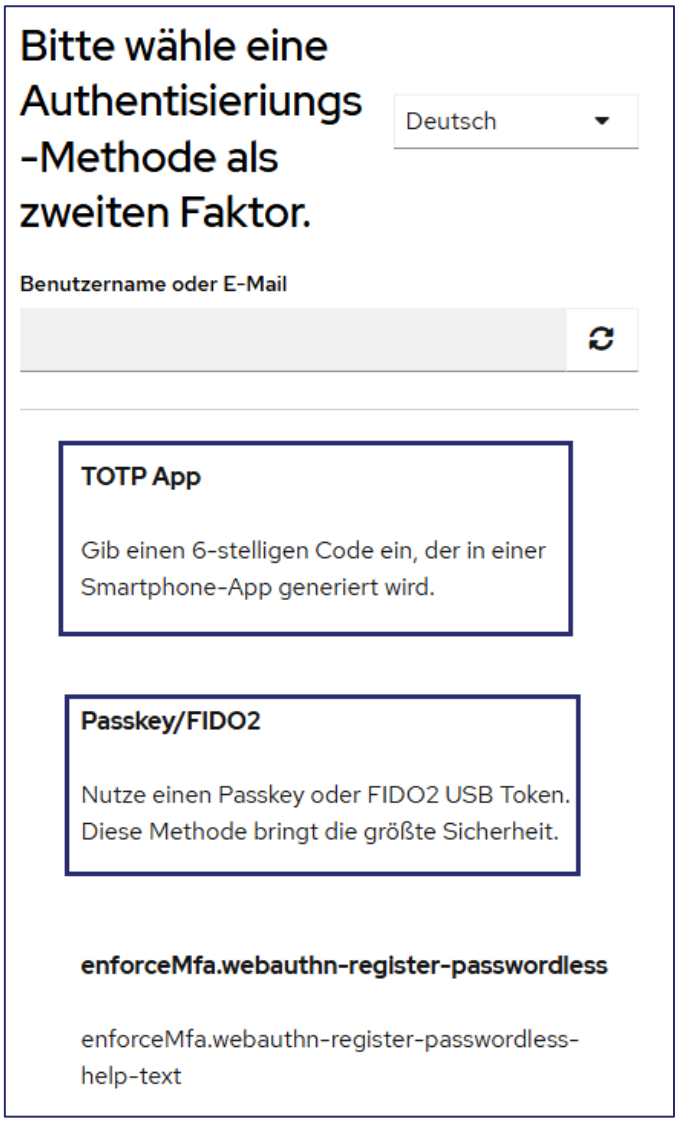


Im nächsten Schritt das Passwort eingeben und auf **„Weiter“** klicken:



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 Authentisieriungs -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-Passwort) 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.

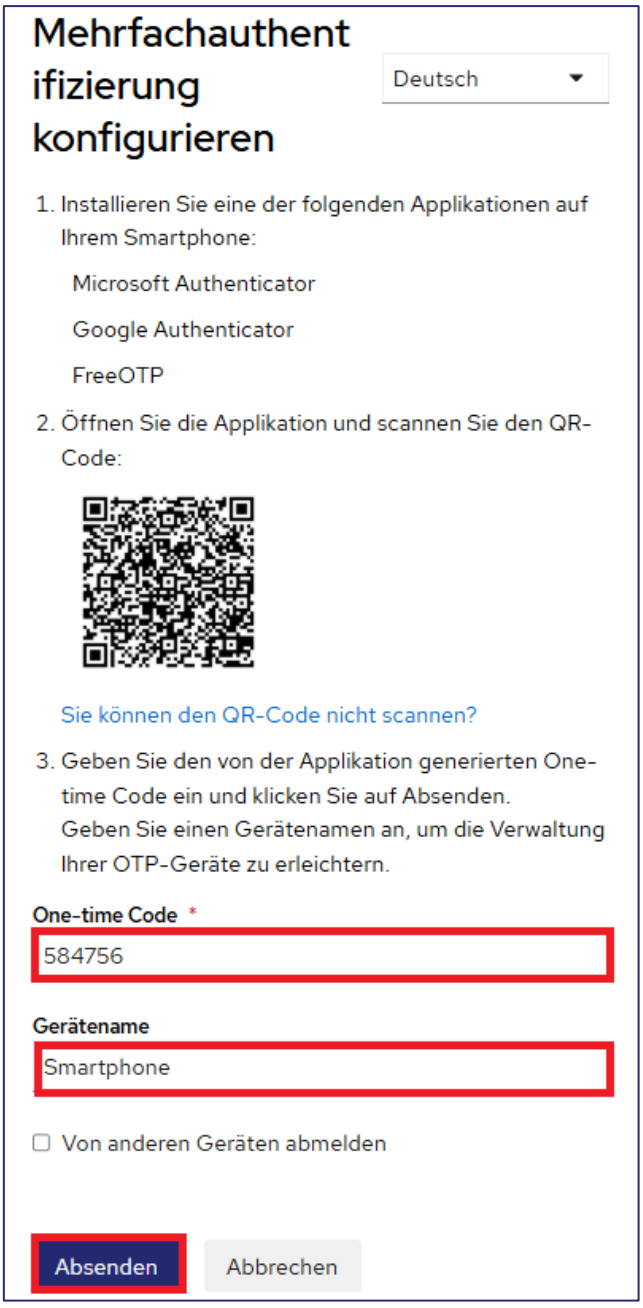
Am häufigsten verwendet werden hierzu die Apps „Google Authenticator“ oder „Microsoft Authenticator“. Alternative Apps sind zum Beispiel „FortiToken Mobile“ oder „FreeOTP“.

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.



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

5 Passkey/FIDO2

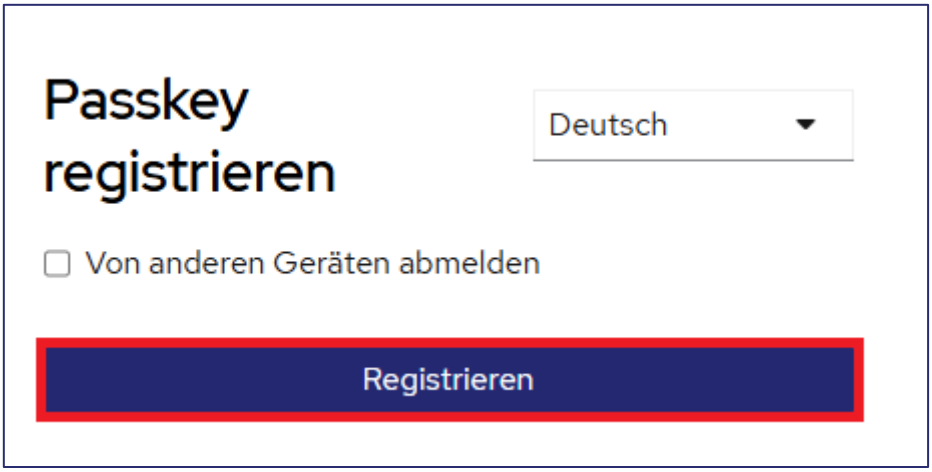
5.1 Was ist Passkey/FIDO2?

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.

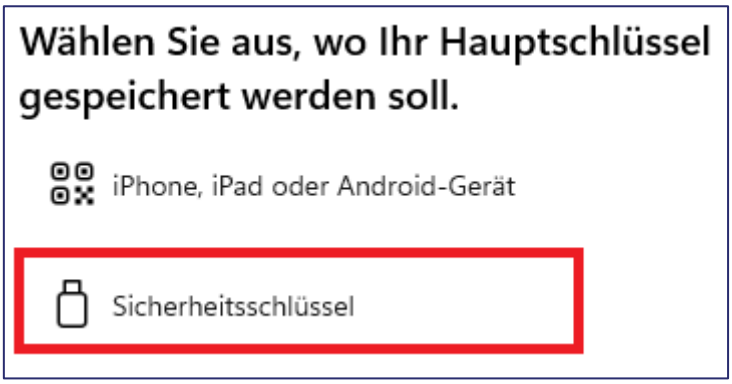
5.2 Passkey einrichten am Beispiel YubiKey

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

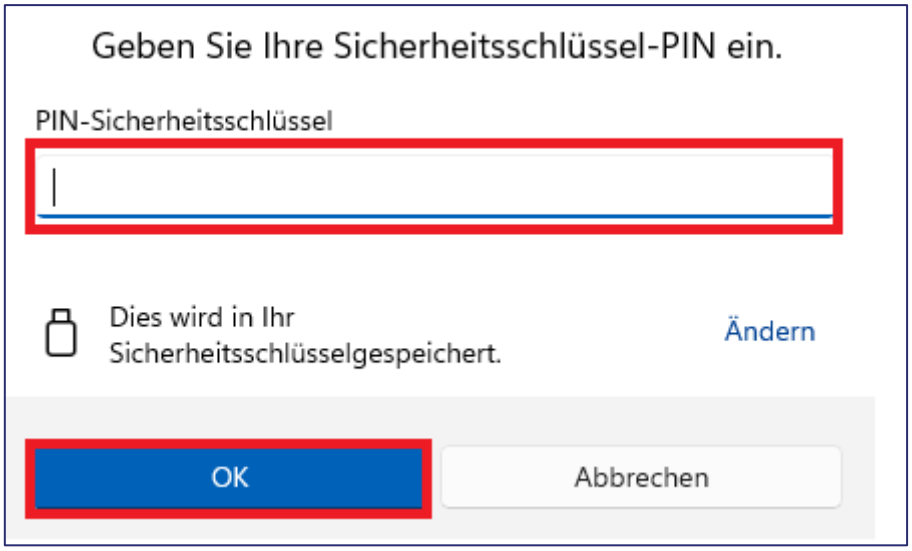


Um den Vorgang fortzusetzen, müssen im nächsten Schritt erneut die Zugangsdaten eingegeben werden (FWF-Benutzername + Passwort).

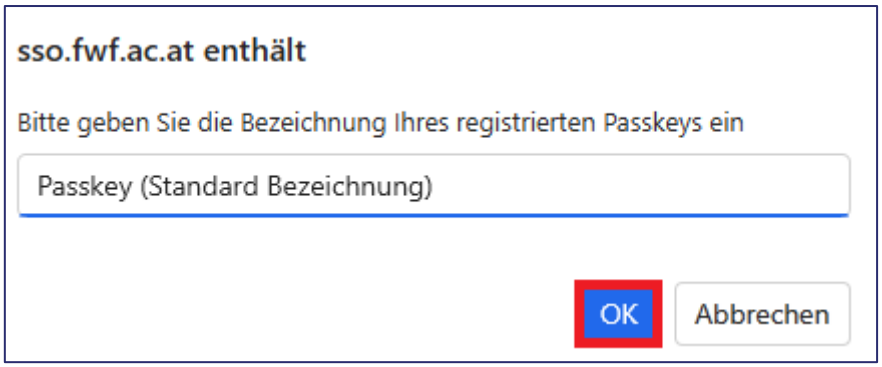
Sicherheitsschlüssel auswählen:



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



Die Bezeichnung des Passkeys (selbst zu wählender Anzeigename) eingeben und mit einem Klick auf **„OK“** bestätigen:



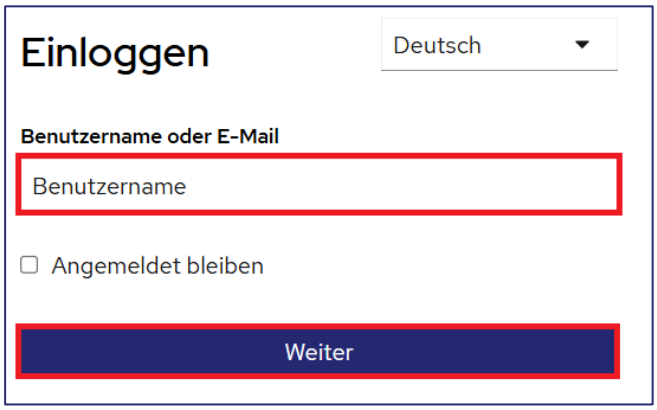
Wurde der Token erfolgreich gespeichert, ist die Einrichtung von SSO abgeschlossen und das Fenster kann geschlossen werden.

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.

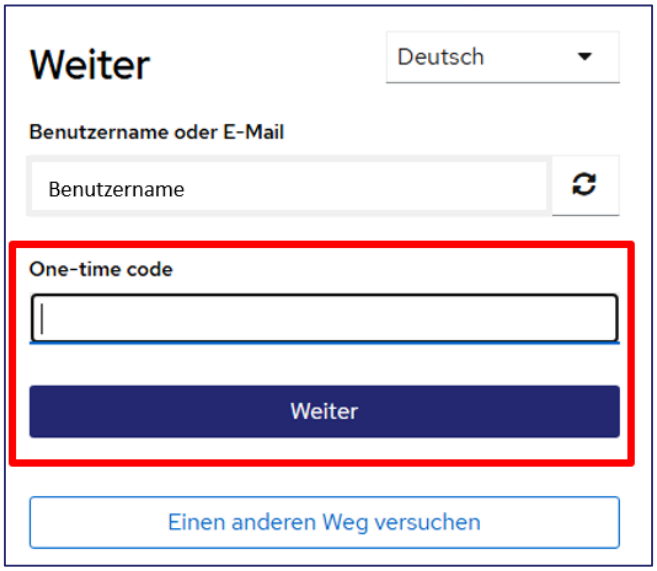
6.1 Anmeldung mit Authenticator-App

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



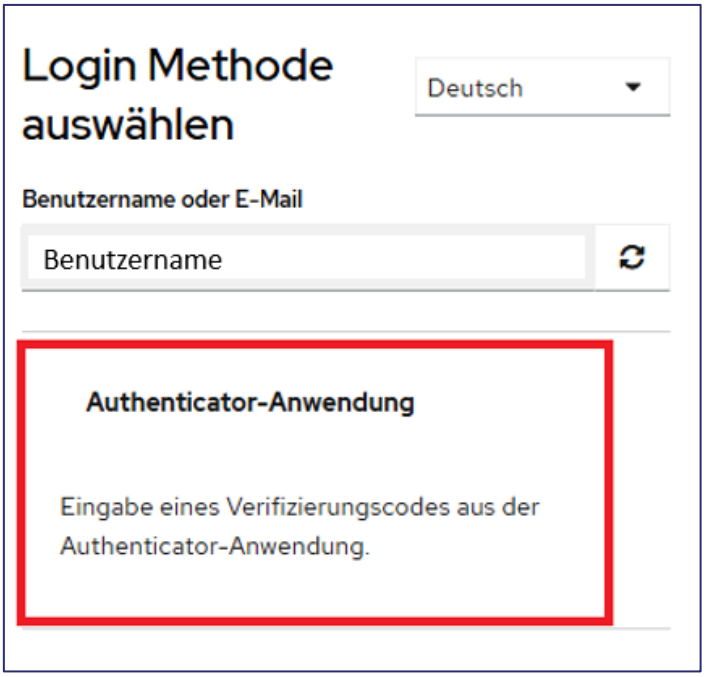
Die Authenticator-App auf dem Smartphone öffnen.

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



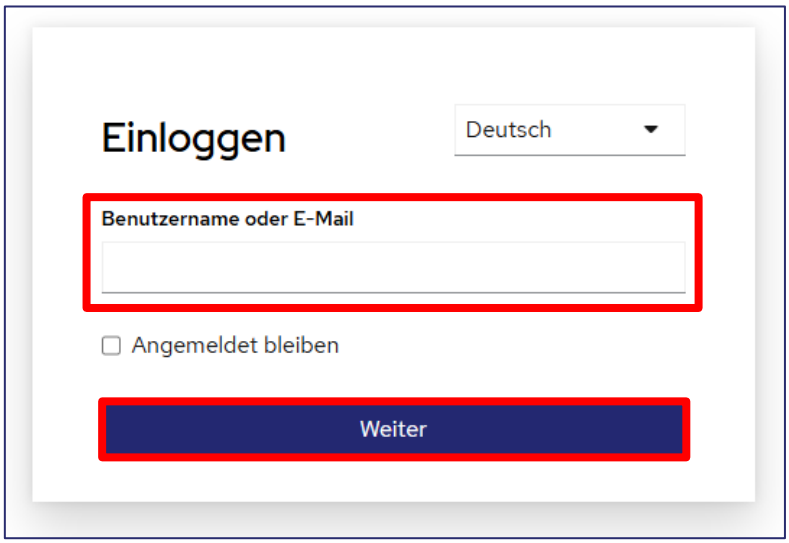
Falls das Bearbeitungsfeld **„One-time code“** nicht angezeigt wird, auf **„Einen anderen Weg versuchen“** klicken.

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

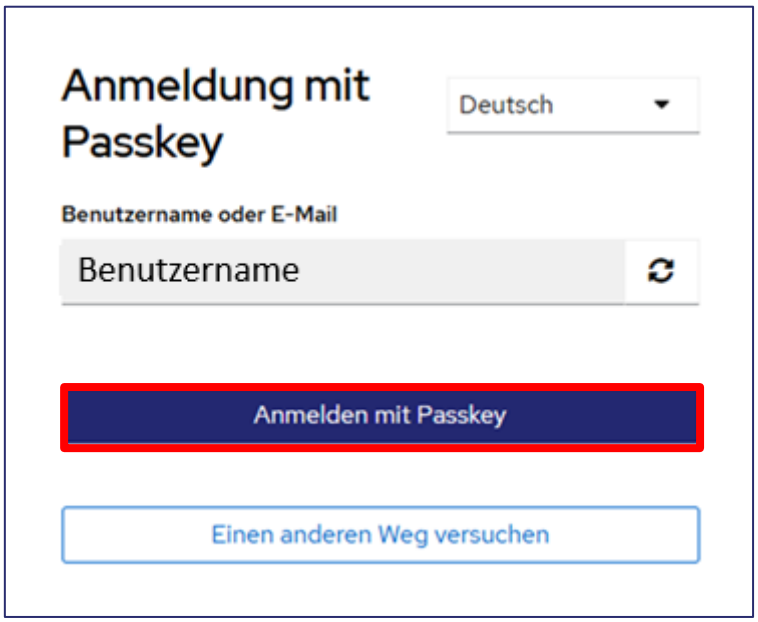


6.2 Anmeldung mit Passkey

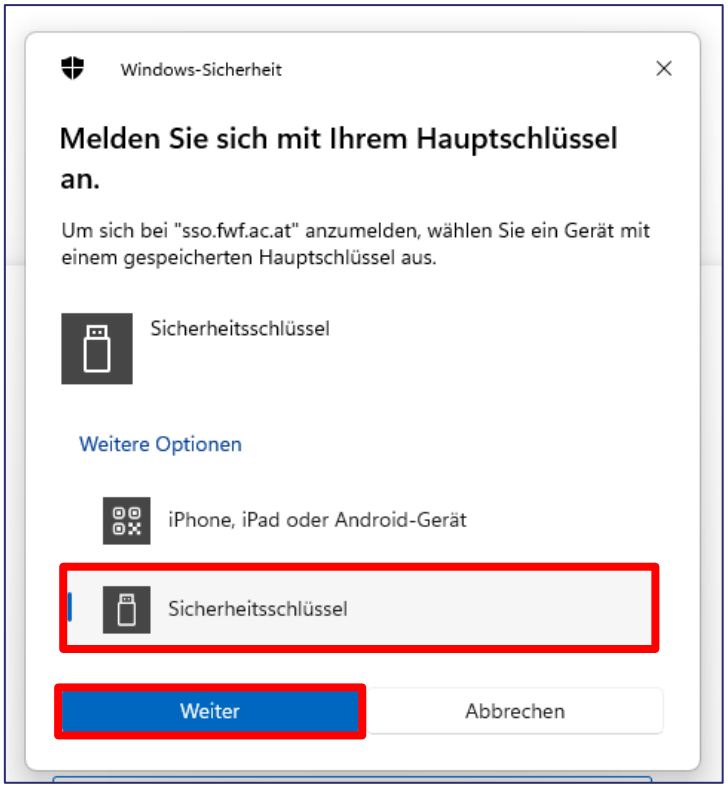
FWF-Benutzername oder E-Mail eingeben und auf **„Weiter“** klicken:



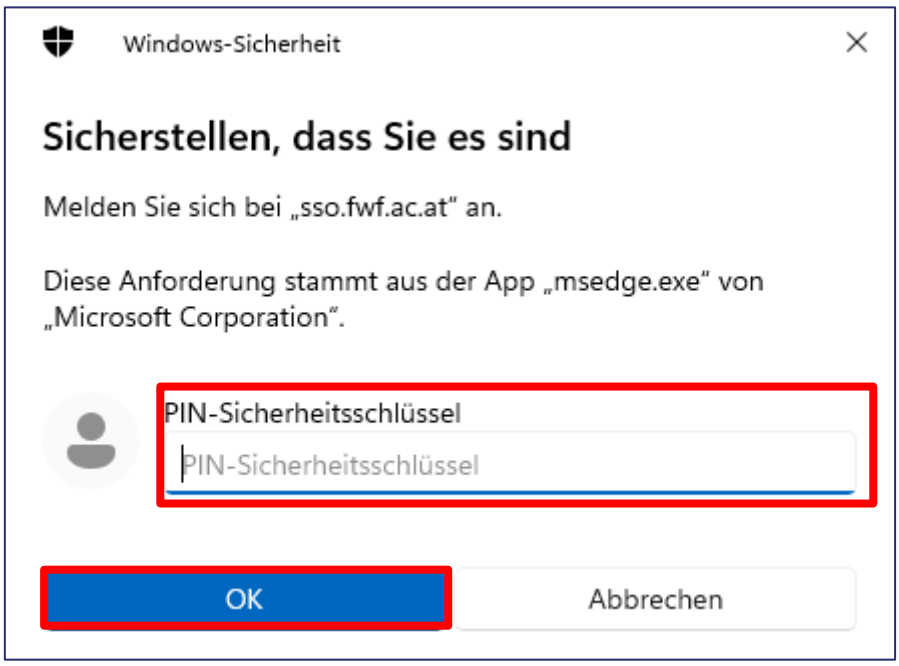
Auf **„Anmelden mit Passkey“** klicken:



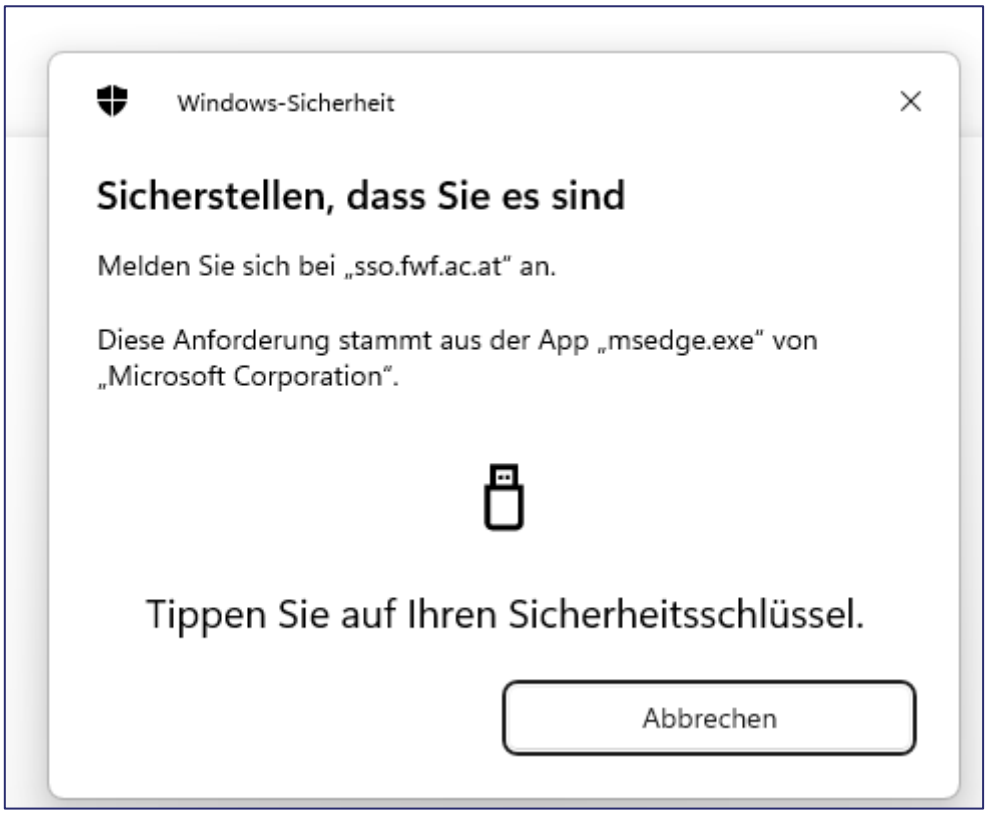
Auf **„Sicherheitsschlüssel“** und dann auf **„Weiter“** klicken:



PIN-Sicherheitsschlüssel eingeben und mit einem Klick auf **„OK“** bestätigen:



Mit Finger auf den blinkenden Yubikey-Knopf drücken.


Windows-Sicherheit
Sicherstellen, dass Sie es sind
Melden Sie sich bei „sso.fwf.ac.at“ an.
Diese Anforderung stammt aus der App „msedge.exe“ von „Microsoft Corporation“.
Tippen Sie auf Ihren Sicherheitsschlüssel.
Abbrechen