Display-Token (Hardware-Token) ausrollen

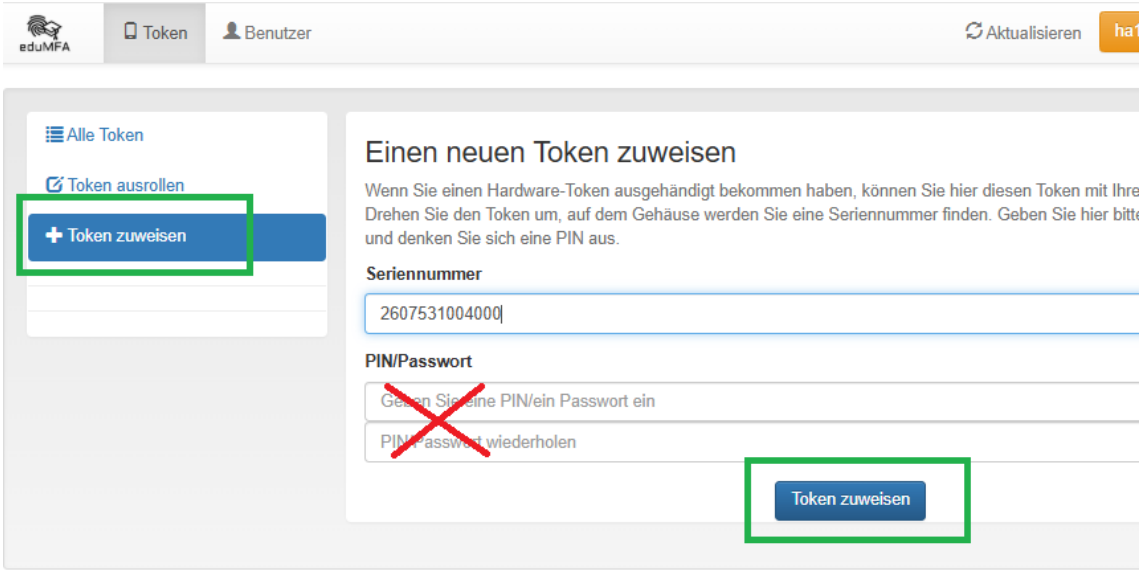
Wichtig: Diese Seite gilt nur für diesen Token-Type (Display-Token mit Anzeige)!

Sie können nach Erhalt Ihres Display-Tokens diesen im eduMFA-Portal registrieren bzw. aktivieren.



Einrichtung:

1) Melden Sie sich im eduMFA-Portal mit Ihren Hochschulzugangsdaten an
2) Klicken Sie im linken Menü auf **„Token zuweisen“**
3) Geben Sie die Seriennummer ein (diese befindet sich auf der Rückseite des Geräts)
4) Klicken Sie auf **„Token zuweisen“**



Danach ist das Display-Token erfolgreich aktiviert und kann für die Anmeldung verwendet werden.

Sicherheitsschlüssel (anhand WebAuthn) einrichten

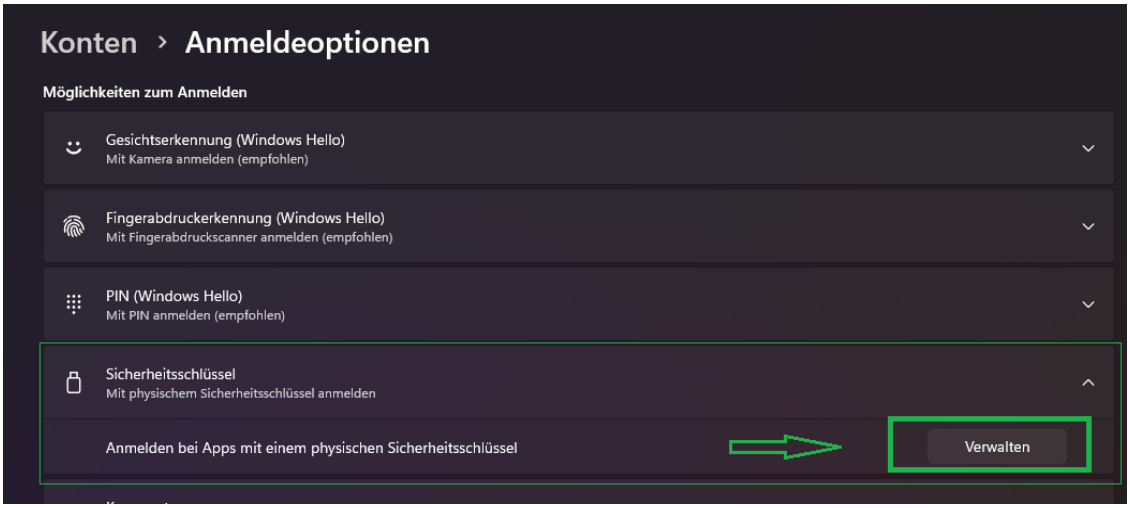
Der Token-Typ „**WebAuthn**“ im MFA-Portal ist sowohl für Sicherheitsschlüssel als auch für passwortlose Anmeldung (Biometrie, Passkey, PW-Manager) geeignet.



1. Erste Einrichtung des Hardware-Sicherheitsschlüssels

Bevor Sie mit dem Token-Ausrollen anfangen, sollten Sie zuerst Ihren Sicherheitsschlüssel auf Ihrem Gerät einrichten.

Dies können Sie in Ihren Gerät-Einstellungen unter *Konten >> Anmeldeoptionen >> Sicherheitsschlüssel* verwalten. Indem Sie eine eigene PIN festlegen.



Folgen Sie den Anweisungen zur Einrichtung.

Danach wird Ihr Sicherheitsschlüssel aktiviert und können Sie ihn für die MFA-Einrichtung nutzen.

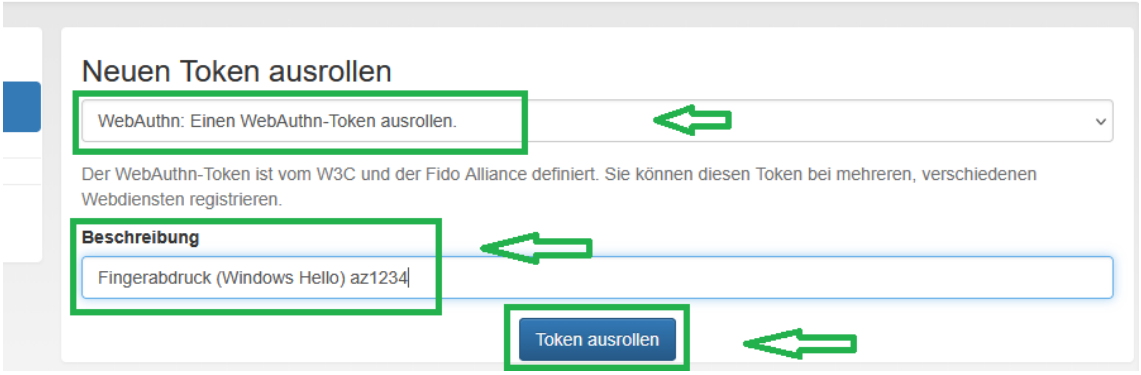
2. Das Token im eduMFA-Portal ausrollen

1) Öffnen Sie in Ihrem Browser: https://mfa.hs-woe.de/ und melden Sie sich mit Ihren Hochschuldaten an.

2) Klicken Sie links auf: **„Token ausrollen“**, unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier WebAuthn.) auswählen.

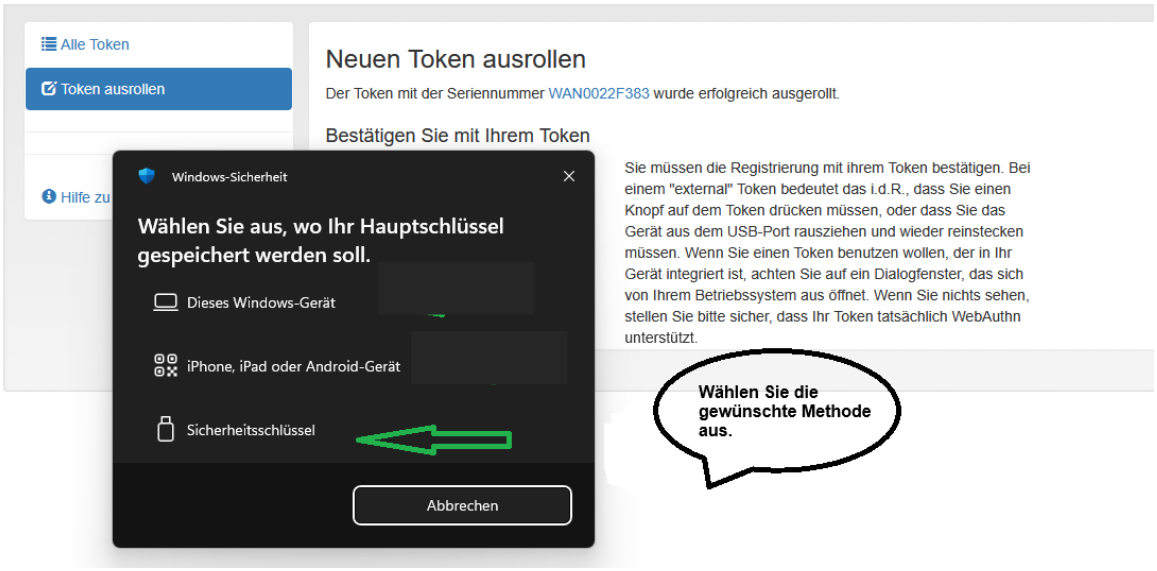
3) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Mein Sicherheitsschlüssel – Ihr Nutzername).

4) Dann klicken Sie auf „Token ausrollen“.



5) Nachdem Sie ein WebAuthn-Token ausrollen, startet im Browser im Hintergrund ein sicherer Anmeldeprozess.

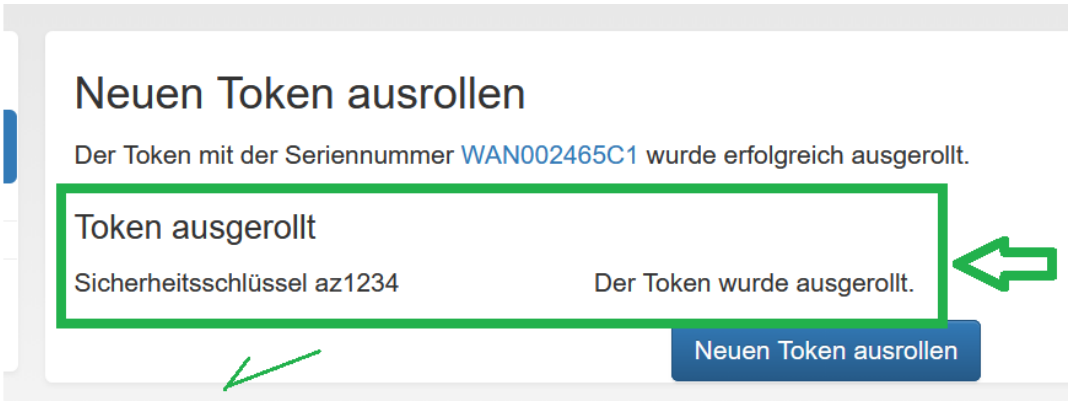
6) Je nachdem, was Sie als Authentifizierungs-Methode (Hardwareschlüssel, Biometrie oder ein Passwort Manager) hinterlegt haben, können Sie entsprechend auswählen.



7) Beim Auswählen der **Sicherheitsschlüssel-Funktion** werden Sie aufgefordert diesen Schlüssel in Ihrem Gerät einzustecken, möglicherweise zu berühren (an dem metallischen Sensor) und abschließend Ihren selbst hinterlegten PIN einzugeben.

8) Geben Sie Ihre bereits hinzugefügte Sicherheitsschlüssel-PIN ein und bestätigen Sie mit „OK“.

Hinweis: Sie müssen, abhängig vom Typ Ihres Sicherheitsschlüssels, den Finger zur Bestätigung auf die Mitte des Schlüssels oder auf den seitlichen Metallsensor legen.



Verhalten beim Verlust des Tokens oder des Gerätes?

Falls Sie mehrere Tokens eingerichtet haben, können Sie sich mit Ihrem anderen Token anmelden und das verlorene Token im Portal deaktivieren.

Falls kein weiteres Token verfügbar ist, kontaktieren Sie bitte sofort den MFA-Service des HRZ.

Bei Verdacht auf unberechtigten Zugriff (z. B. gestohlenes Token / Gerät) wenden Sie sich umgehend an den MFA-Service des HRZ.

MFA-Support kontaktieren

Haben Sie Probleme mit Ihrem Token, benötigen Sie Hilfe oder möchten Sie uns Feedback senden?

Dann können Sie ein Ticket an den MFA-ServiceCenter des HRZ über das Tickets-System

oder eine E-Mail unter einer dieser Adressen schreiben:

haya.alshahrour@jade-hs.de oder informationssicherheitsmanagement@jade-hs.de.