Nutzeranleitung zur Multi Faktor Authentifizierung (MFA) an der Jade Hochschule „eduMFA“

Sie möchten nur schnell MFA einrichten?

Nutzen Sie unsere kompakte MFA-Kurzanleitung mit Bildern und einfachen Schritt-für-Schritt-Anweisungen unter: **https://hrz-wiki.jade-hs.de/de/tp/uadm/mfa**

Der Zugang zu zentralen IT-Diensten der Jade Hochschule wird künftig zusätzlich abgesichert. Ab dem Sommersemester 2026 erfolgt die Anmeldung schrittweise über eine Multi-Faktor-Authentifizierung (MFA).

Dabei wird neben Benutzername und Passwort ein weiterer Faktor zur Bestätigung der Identität verwendet. Zum Einsatz kommt das Open-Source-System eduMFA, das speziell für Hochschulen entwickelt wurde.

Inhaltsverzeichnis

1. Was bedeutet MFA?

Die Multi Faktor Authentifizierung (MFA) bezeichnet ein Anmeldeverfahren, bei dem mindestens zwei unterschiedliche Kategorien (Wissen, Besitz oder Biometrie) von Authentifizierungsfaktoren kombiniert werden. Das heißt: Neben Benutzername und Passwort (Wissen) wird beim Login ein zweiter Sicherheitsfaktor abgefragt („Token“).

Damit wird verhindert, dass Unbefugte selbst bei Kenntnis des Passworts Zugriff auf Ihr Konto oder sensible Daten erhalten.

2. Warum wird MFA eingesetzt?

Benutzerkonten gehören zu den häufigsten Angriffszielen in IT-Systemen. Wird ein Passwort bspw. durch Phishing oder Datenlecks kompromittiert, können Angreifer auf geschützte Dienste zugreifen.

Durch MFA wird zusätzlich zum Passwort ein weiterer Sicherheitsfaktor („Token“) abgefragt. Somit wird ein unbefugter Zugriff erheblich erschwert und die Sicherheit der Hochschuldienste deutlich erhöht.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt den Einsatz von MFA als wesentliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten. Die Jade Hochschule orientiert sich an diesen Empfehlungen. Viele Organisationen und Hochschulen setzen daher auf MFA als wichtigen Bestandteil moderner IT-Sicherheitsstrategien.

3. Was ist ein Token?

Ein Token ist ein zusätzlicher Sicherheitsnachweis, der Ihre Identität beim Login bestätigt. Im eduMFA-System kann ein Token verschiedene Formen haben: Einmal-Sicherheitscode (TOTP, HOTP, PRR), Hardware-Token (Sicherheitsschlüssel, Yubikey) oder biometrisches Token (Passkey).

Beim Login geben Sie diesen zusätzlichen Faktor nach der Eingabe Ihres Passworts ein.

4. Was ist jetzt neu für Sie?

Bisher erfolgte die Anmeldung an den Hochschuldiensten ausschließlich über Benutzername und Passwort.

Mit der neuen eduMFA-Lösung wird zusätzlich ein zweiter Faktor (Token) abgefragt. Damit wird das Anmeldeverfahren sicherer und besser vor Passwortmissbrauch geschützt.

5. Was wird für die erste Einrichtung der MFA benötigt?

Für die Einrichtung von MFA benötigen Sie:

- Ein Gerät zur Anmeldung (z.B. Laptop, Smartphone)
- Ihre Hochschul-Login-Daten (Benutzername und Passwort)
- Ein Token, das Sie später über das eduMFA-Portal ausrollen können.
- Eine Authenticator-App, falls Sie den Token-Typ „TOTP“ nutzen möchten. Dieser Token-Typ wird besonders in Kombination mit einer TAN-Liste oder WebAuthn (Sicherheitsschlüssel/Biometrie) besonders *empfohlen*.

  Sie können eine Authenticator-App Ihrer Wahl installieren und verwenden.

  App-Beispiele:

  PrivacyIDEA: Für Android, für iOS

  2FAS Auth.: Für Android, für iOS

  Google Authenticator: Für Android, für iOS

  Authy APP: Für Android, für iOS

  Microsoft Authenticator: Für Android, für iOS

6. Welche Authentifizierungsfaktoren stehen zur Verfügung?

Im eduMFA-System können verschiedene Faktoren verwendet werden:

- **TOTP:** Zeitbasiertes Einmalpasswort, (über eine Authenticator-App).
- **WebAuthn:** Sicherheitsschlüssel, Passkey, Biometrie oder Passwortmanager.
- **PPR:** Papier-Token bzw. TAN-Liste mit einmalig nutzbaren Codes.
- **HOTP:** Ereignisbasiertes Token (App- oder Hardwarebasiert).
- **YubiKey:** ein spezieller Sicherheitsschlüssel als Hardware-Token, kein Security Key.

7. Verfügbare Sicherheitsschlüssel als Hardware-Token

Kategorie	Unterstützte Tokens	Funktionsweise	Besonderheiten
Display-Token (Hardware-Token mit Display) Preis: 13 € 	TOTP	Das Gerät erzeugt einen Code, der manuell in die MFA-Anmeldemaske eingegeben wird.	Funktioniert unabhängig vom Smartphone. Gilt als Ersatz für Authenticator-Apps.
Sicherheitsschlüssel  **iShield 2 von Firma Swissbit:** - USB-A: 24 € - USB-C: 28 € **YubiKey von Firma Yubico:** - Security Key USB-A: 35 € - Security Key USB-C: 35 €	WebAuthn.	Der Schlüssel wird per USB eingesteckt. Die Anmeldung erfolgt durch Einstecken des Schlüssels und Bestätigung (ggf. mit PIN).	Hohe Sicherheit, direkte Anmeldung ohne manuelle Codeeingabe.

Beschaffung:

Die Bestellung erfolgt über das Ticketsystem per formloser E-Mail unter Angabe von Kostenstelle, Hardware-Typ und Anschlussart (USB-A oder USB-C).

Hinweis:

Für die Nutzung mit eduMFA sind der Swissbit iShield Key 2 und der YubiKey Security Key funktional gleichwertig. Beide unterstützen die Anmeldung per WebAuthn/FIDO2 und bieten ein vergleichbares Sicherheitsniveau. Die Unterschiede liegen hauptsächlich beim Hersteller, der Bauform (USB-A/USB-C) und dem Preis.

Die angegebenen Preise können je nach Angebot und Bestellzeitpunkt geringfügig variieren.

8. Wie erfolgt die MFA-Einrichtung?

Im eduMFA-Portal können Sie bis zu 5 aktive Tokens besitzen und verwalten.

Es wird empfohlen, mehrere Tokens einzurichten, bspw. ein TOTP-Token auf dem Handy und ein zusätzliches Token auf einem anderen Gerät, in Ihrem bevorzugten Passwortmanager oder in einer anderen Form (z. B. biometrisch oder als Hardware-Token).

Dadurch können Sie sich im Notfall, etwa bei Verlust oder Defekt eines Geräts, weiterhin sicher anmelden und auf Ihre Hochschuldienste zugreifen.

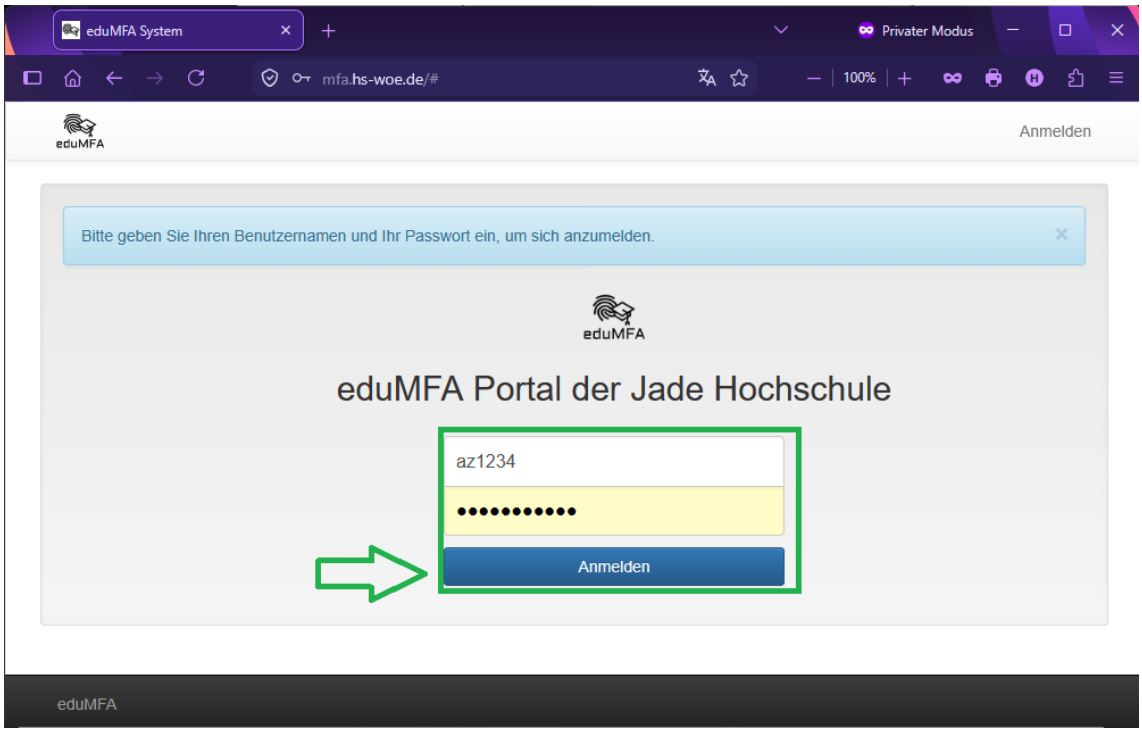
Schritt-für-Schritt-Ablauf:

1) Aufruf der eduMFA-Webseite

Öffnen Sie das eduMFA-Portal https://mfa.hs-woe.de/ im Browser.

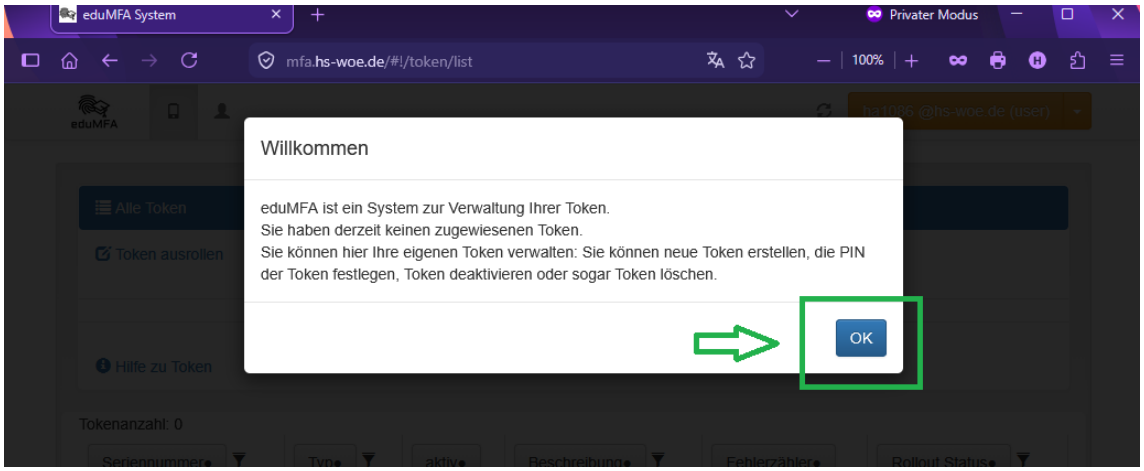
2) Anmeldung mit Hochschul-Login-Daten

Geben Sie Ihren Benutzername und Ihr Passwort ein. Dann auf „Anmelden“ klicken.

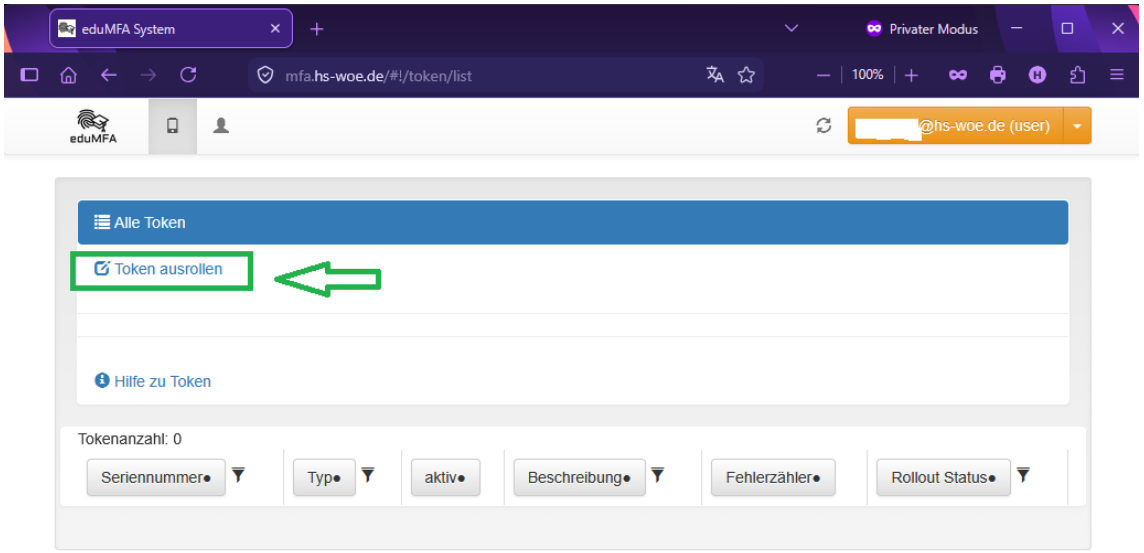


3) Erstellung des ersten Tokens

Erstmal den Willkommen-Dialog mit „OK“ bestätigen. Anschließend können Sie Ihr erstes Token ausrollen.



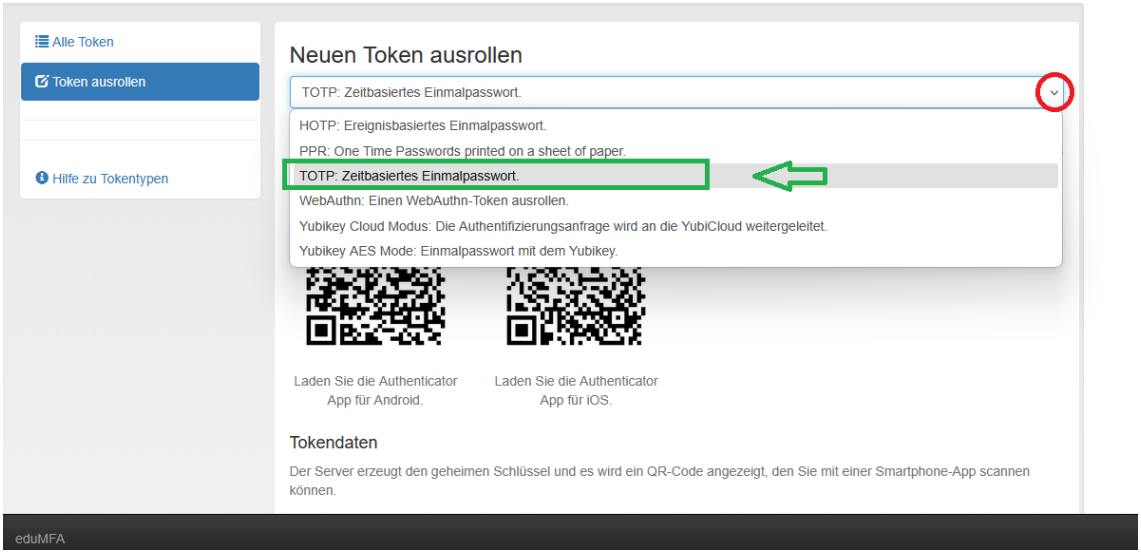
Dann klicken Sie unter dem Menü links auf das Feld „Token ausrollen“.



Es stehen Ihnen verschiedene Arten von Tokens zur Verfügung, deren Einrichtung hier im Detail beschrieben ist:

8.1 TOTP-Token ausrollen

1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier TOTP) auswählen.

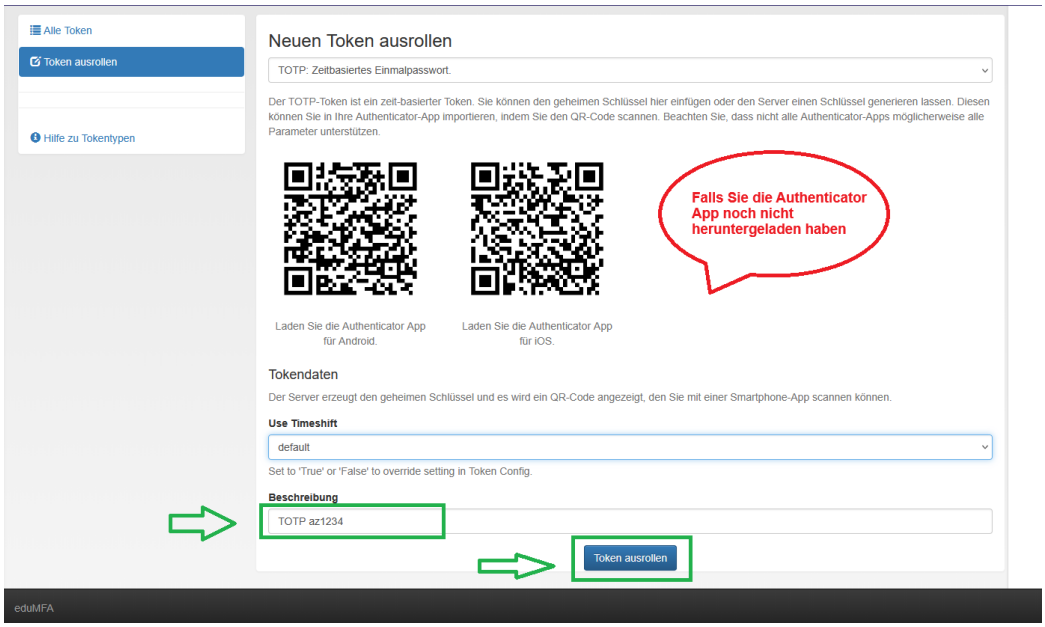


2) Falls Sie noch keine Authenticator-App auf Ihrem Handy installiert haben, werden Ihnen zwei QR-Codes angezeigt, über die Sie die App „PrivacyIDEA“ herunterladen können.

   Ignorieren Sie diese Codes, wenn Sie bereits eine App installiert haben oder keine App bzw. eine andere verwenden möchten.

3) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Token-Art & Nutzername).

4) Klicken Sie auf „Token ausrollen“.



5) **Um den Token zu aktivieren, haben Sie 3 Möglichkeiten:**

a) QR-Code scannen (empfohlen)

Scannen Sie den QR-Code mit der bereits installierten App auf Ihrem Handy. Nach dem Scannen erscheint in der App **ein 6-stelliger zeitbasierter Code**.

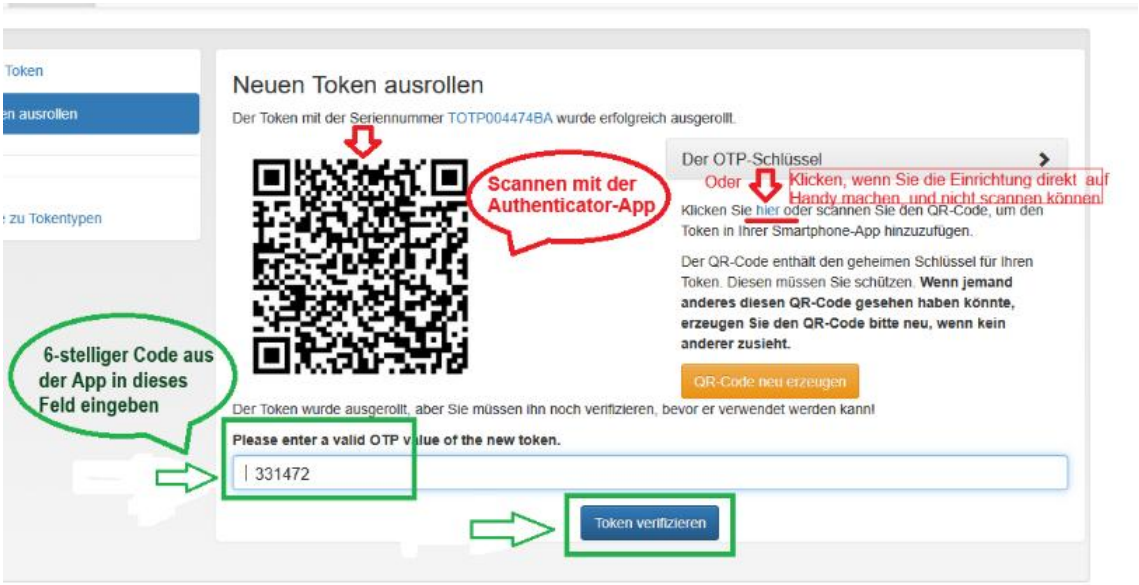
Geben Sie diesen Code aus Ihrer App in das entsprechende Feld ein und bestätigen Sie die Eingabe mit **„Token verifizieren“** *(wie auf dem Bild unten angezeigt)*.

Erst nach dieser Verifizierung ist Ihr Token aktiv und kann für die Anmeldung verwendet werden. Wie im Kapitel 9 unten beschrieben ist.

b) Oder QR-Code direkt auf dem Handy öffnen

Wenn Sie den Vorgang auf dem Handy durchführen und den QR-Code nicht scannen können, klicken Sie auf den blauen Link „hier“.

Wählen Sie anschließend Ihre Authenticator-App aus, um das Token automatisch hinzuzufügen.



Auf Ihrem Handy sollen Sie dann die entsprechende App auswählen und Ihr Token wird automatisch zur App hinzugefügt.

Geben Sie diesen Code aus Ihrer App in das entsprechende Feld ein und bestätigen Sie die Eingabe mit **„Token verifizieren“**.

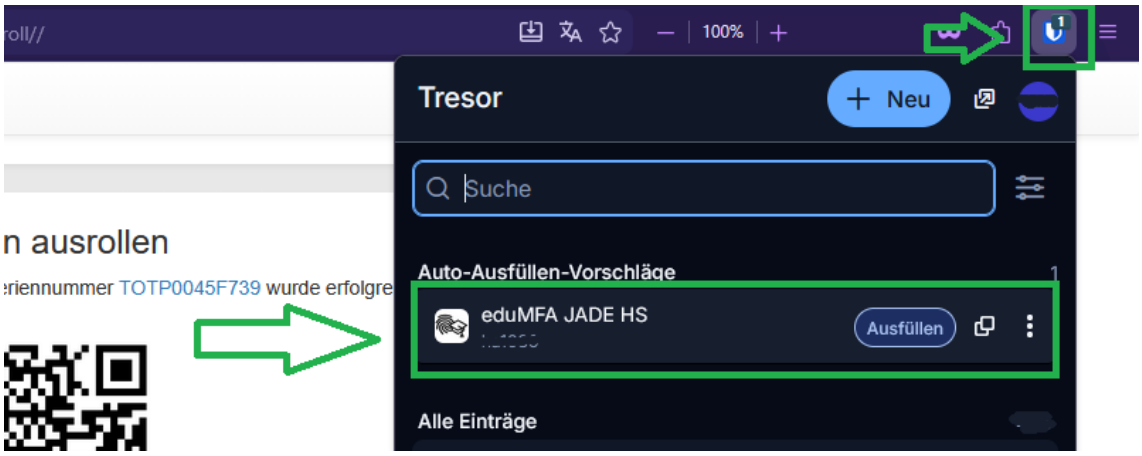
c) Browser-Erweiterung nutzen

Alternativ können Sie eine Browser-Erweiterung (Extension) eines Passwort-managers oder einer 2FA-App nutzen. Der QR-Code wird dabei automatisch erkannt, sofern die Erweiterung aktiviert ist.

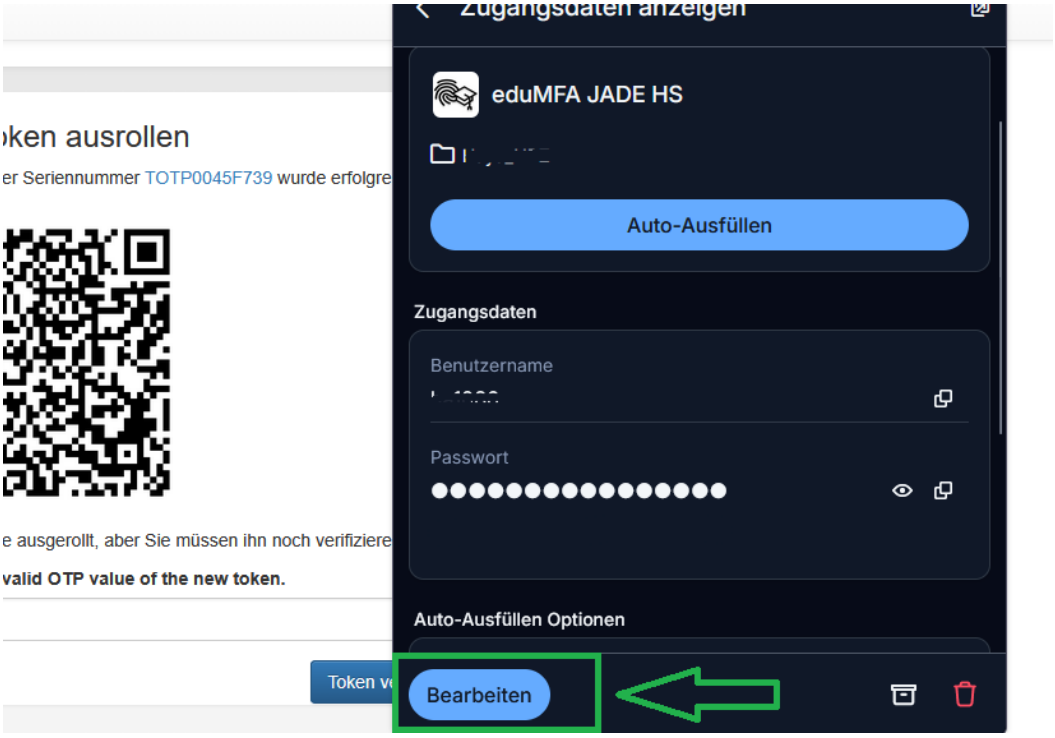
Beispielhafte Einrichtung über eine Browser-Erweiterung: (hier Bitwarden)

Hinweis: Die Bezeichnungen können je nach verwendeter Browser-Erweiterung leicht abweichen.

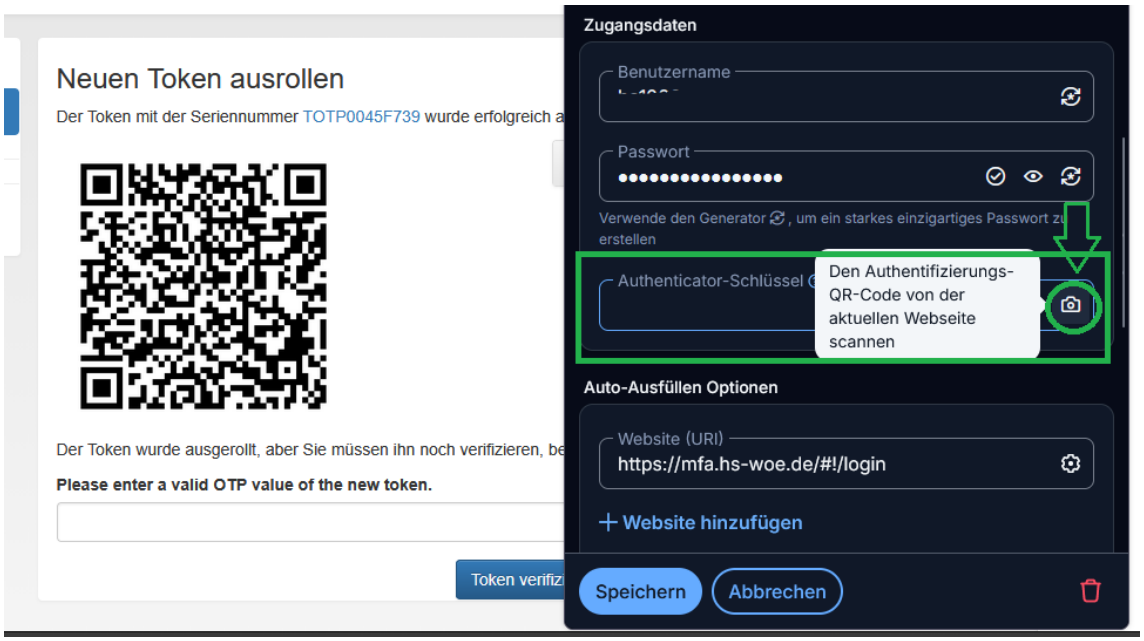
- Öffnen Sie das Symbol der Erweiterung in Ihrem Browser.
- Wählen Sie den entsprechenden Eintrag (Anmeldedaten) aus.



- Klicken Sie auf „Bearbeiten“.

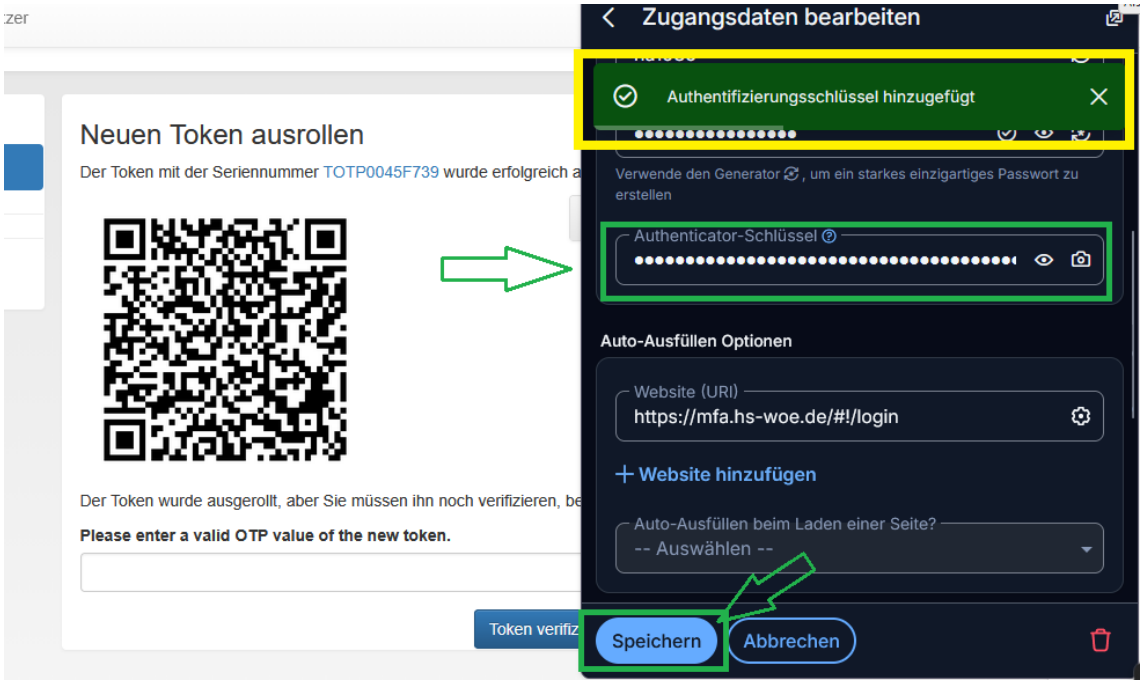


➢ Klicken Sie im Feld „Authenticator-Schlüssel hinzufügen“ auf das Kamera-Symbol.

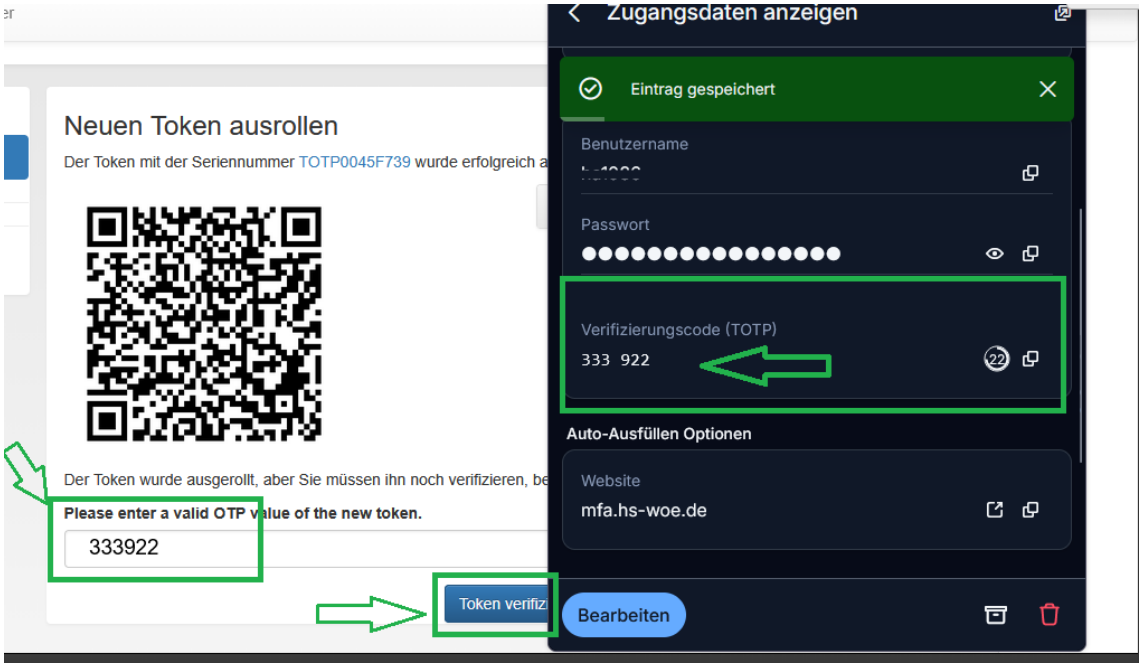


➢ Der QR-Code auf der Webseite wird dann automatisch erkannt und übernommen.

➢ Klicken Sie abschließend auf „Speichern“.



➢ Anschließend wird Ihnen der zeitbasierte Einmalcode (OTP) in der Erweiterung angezeigt.

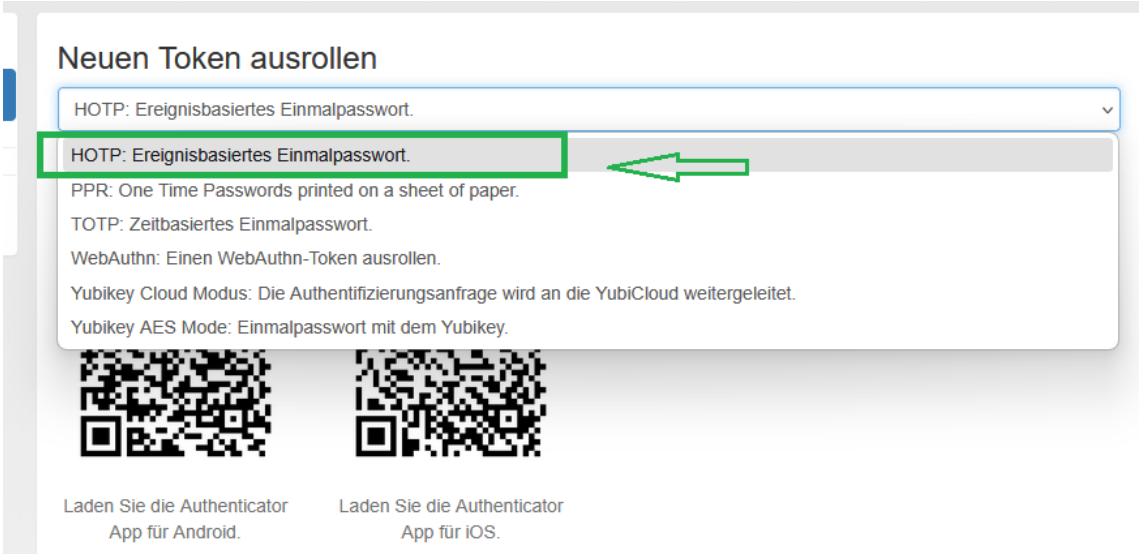


Geben Sie diesen Code aus Ihrer App in das entsprechende Feld ein und bestätigen Sie die Eingabe mit **„Token verifizieren“**.

Erst nach dieser Verifizierung ist Ihr Token aktiv und kann für die Anmeldung verwendet werden. Wie im Kapitel 9 unten beschrieben ist.

8.2 HOTP-Token ausrollen

1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier HOTP) auswählen.



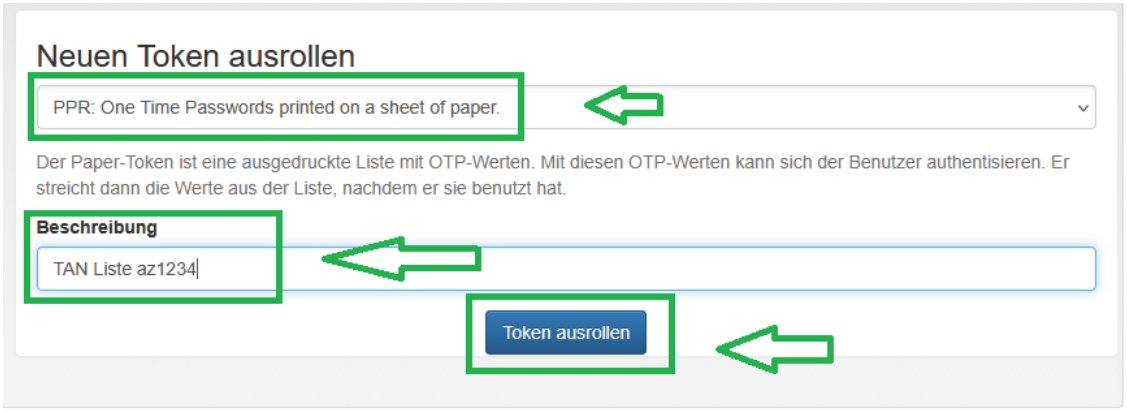
2) Falls Sie noch keine Authenticator-App auf Ihrem Handy haben. Wird Ihnen als Hilfe zwei QR-Codes angezeigt, die für das Installieren der App „PrivacyIDEA“ verwendet werden können.

   Ignorieren Sie diese Codes, wenn Sie die App bereits auf Ihrem Handy haben, oder nicht nutzen wollen.

3) Dann geht es weiter genau wie beim Token TOTP, im Kapitel 8.1 oben.

8.3 Papier-Token /TAN-Liste als PDF (PPR) ausrollen

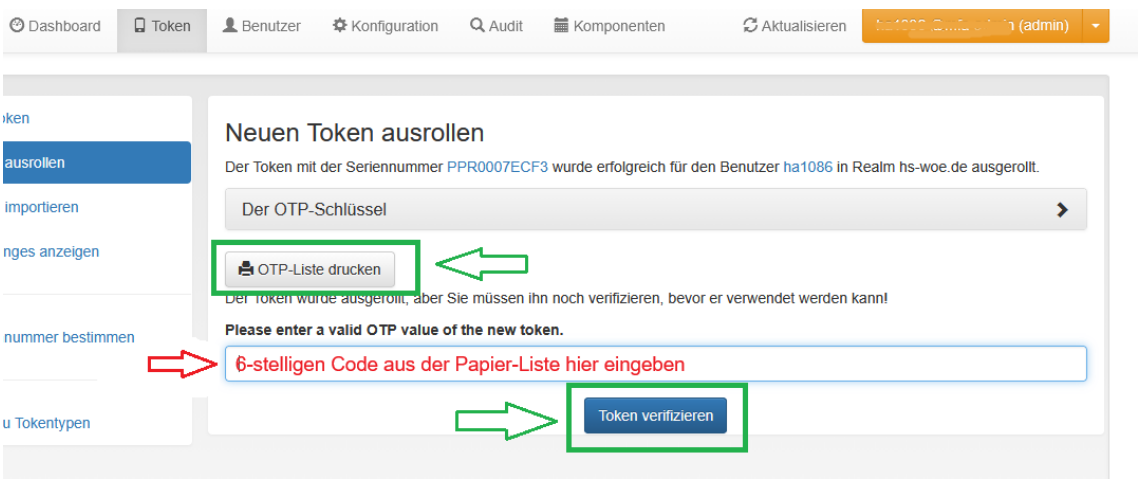
1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier PPR) auswählen.
2) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Token-Art & Nutzername).
3) Dann klicken Sie auf „Token ausrollen“.



Hierbei wird eine Liste mit ca. 100 einmaligen Codes generiert, die Sie beim Anmelden der Reihe nach einmalig verwenden können.

4) Klicken Sie auf „OTP-Liste drucken“, um die Liste als PDF-Datei zu speichern bzw. zu drucken. Dies ist nur nach dem Ausrollen möglich.
5) Dann einen Code aus der Liste in das Feld eingeben und auf „Token verifizieren“ klicken. Erst danach ist Ihr Token aktiv und kann verwendet werden.

Wichtig: Sobald Sie diese Seite verlassen haben, können Sie die Liste nicht mehr sehen bzw. herunterladen!

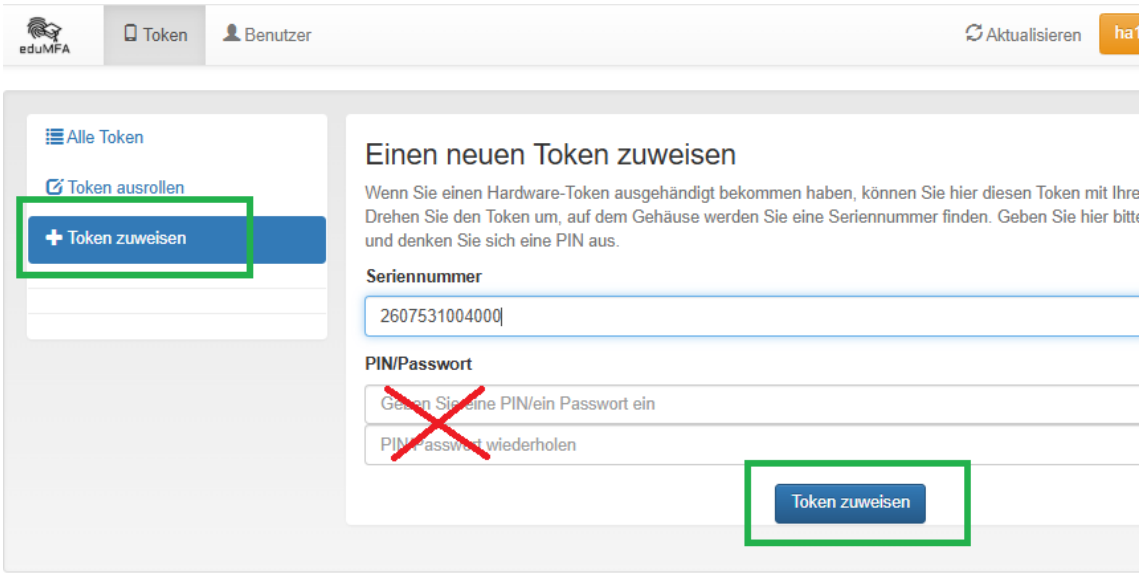


8.4 Display-Token (Hardware-Token) ausrollen

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.

8.5 Sicherheitsschlüssel / Passkey / Biometrie (WebAuthn) ausrollen

Dieser Token-Typ (WebAuthn.) ist sowohl für Sicherheitsschlüssel als auch für passwortlose Anmeldung (Biometrie, Passkey, PW-Manager) geeignet.

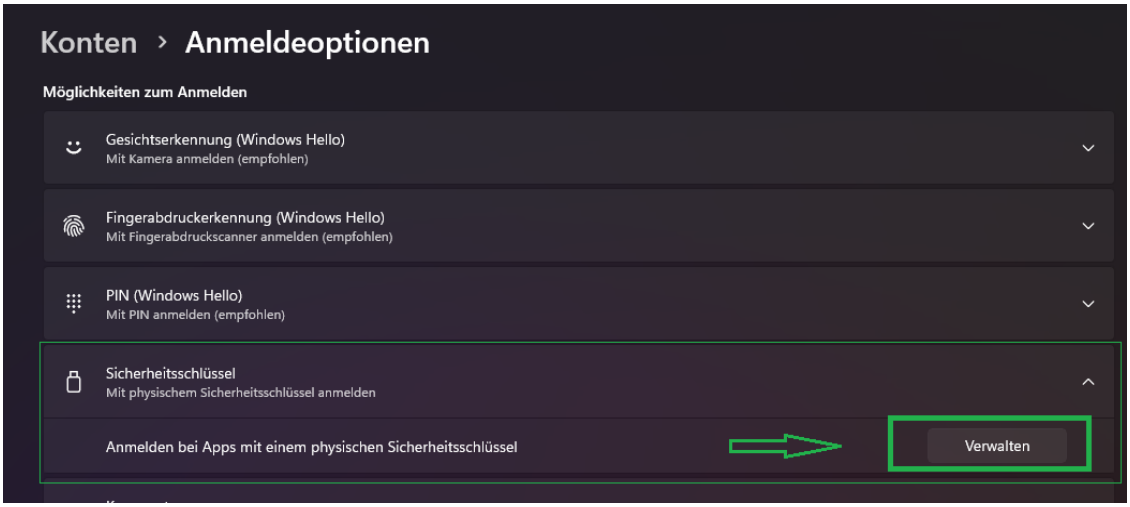
Bevor Sie mit dem Token-Ausrollen anfangen, sollten Sie zuerst die gewünschte Methode (z.B. Fingerabdruck, Gesichtserkennung, Sicherheitsschlüssel) auf Ihrem Gerät einrichten.

Dies können Sie in Ihren Gerät-Einstellungen unter *Konten >> Anmeldeoptionen* verwalten. Indem Sie Ihre biometrischen Daten hinzufügen, eine eigene PIN festlegen oder Ihren Hardware-Schlüssel einrichten.

8.5.1 Erste Einrichtung des Hardware-Sicherheitsschlüssels

Ihren Sicherheitsschlüssel können Sie folgendermaßen einrichten:

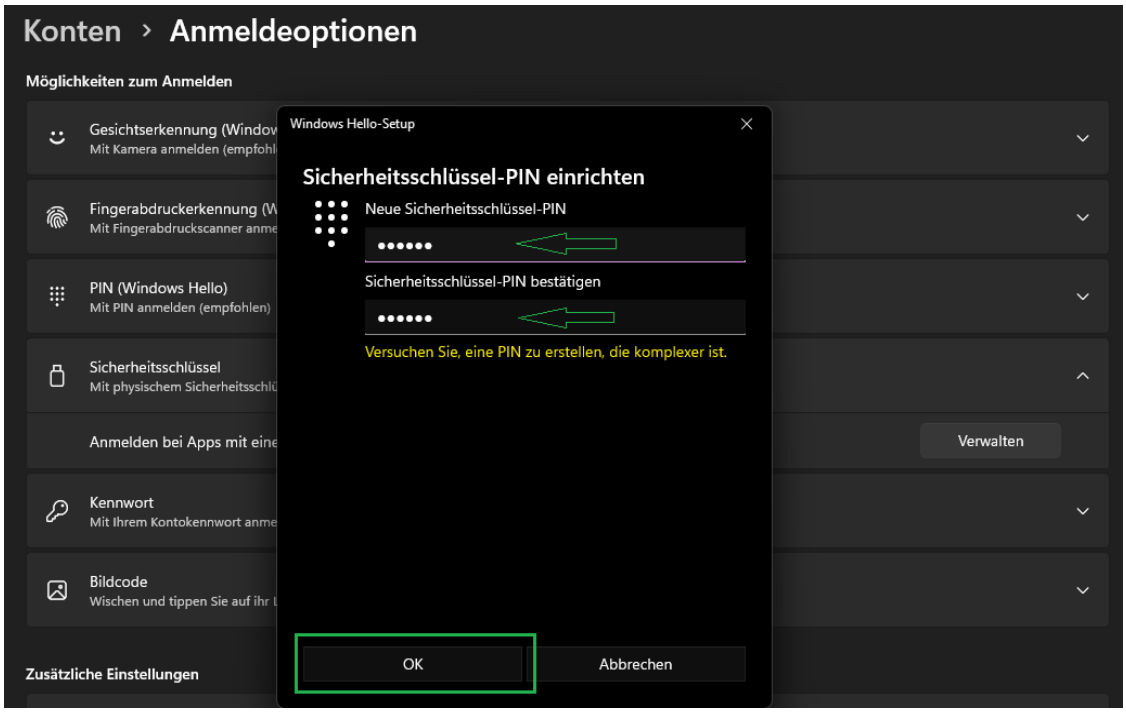
In den Einstellungen unter *Konten >> Anmeldeoptionen* beim „Sicherheitsschlüssel“ auf „Verwalten“ klicken.



Folgen Sie den Anweisungen zur Einrichtung:

Erstellen Sie eine PIN für Ihren Sicherheitsschlüssel:

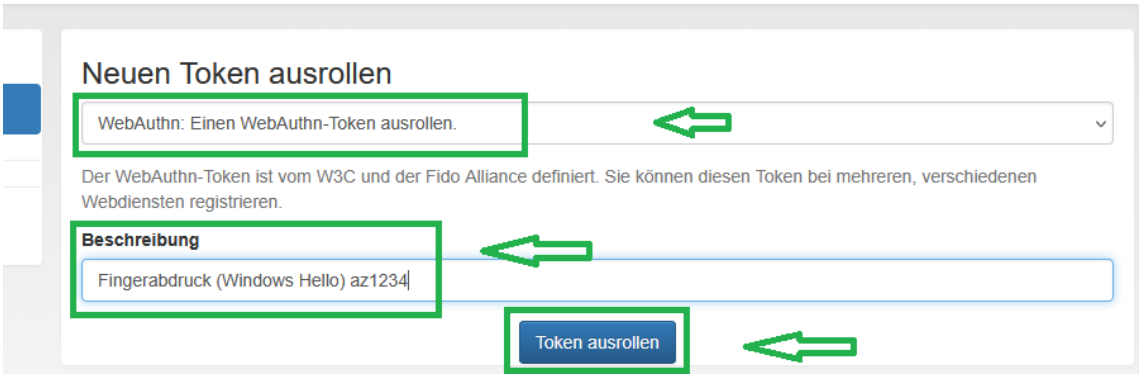
Eine komplexe 4- oder 6-stellige PIN eingeben und wiederholen und abschließend mit „OK“ bestätigen.



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

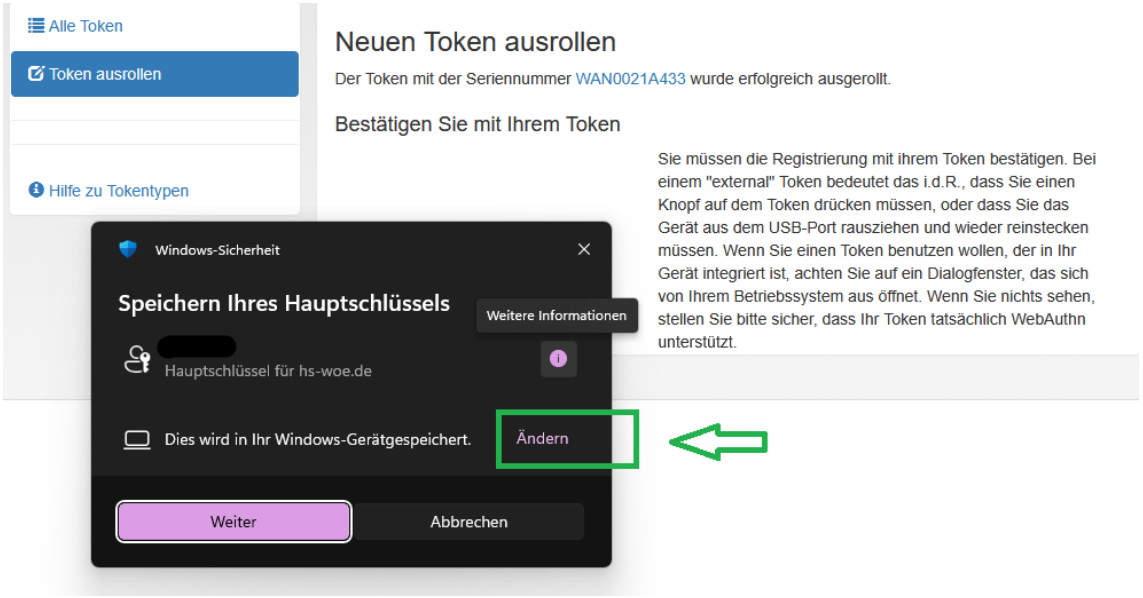
8.5.2 Das Token ausrollen

1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier WebAuthn.) auswählen.
2) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Token-Art & Nutzername).
3) Dann klicken Sie auf „Token ausrollen“.

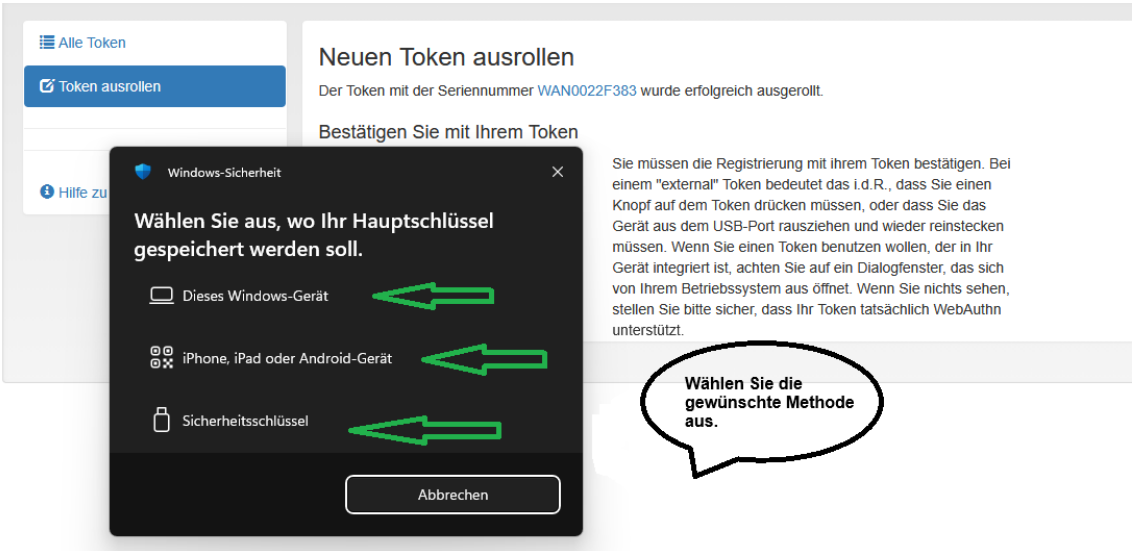


4) Nachdem Sie ein WebAuthn-Token ausrollen, startet im Browser im Hintergrund ein sicherer Anmeldeprozess.

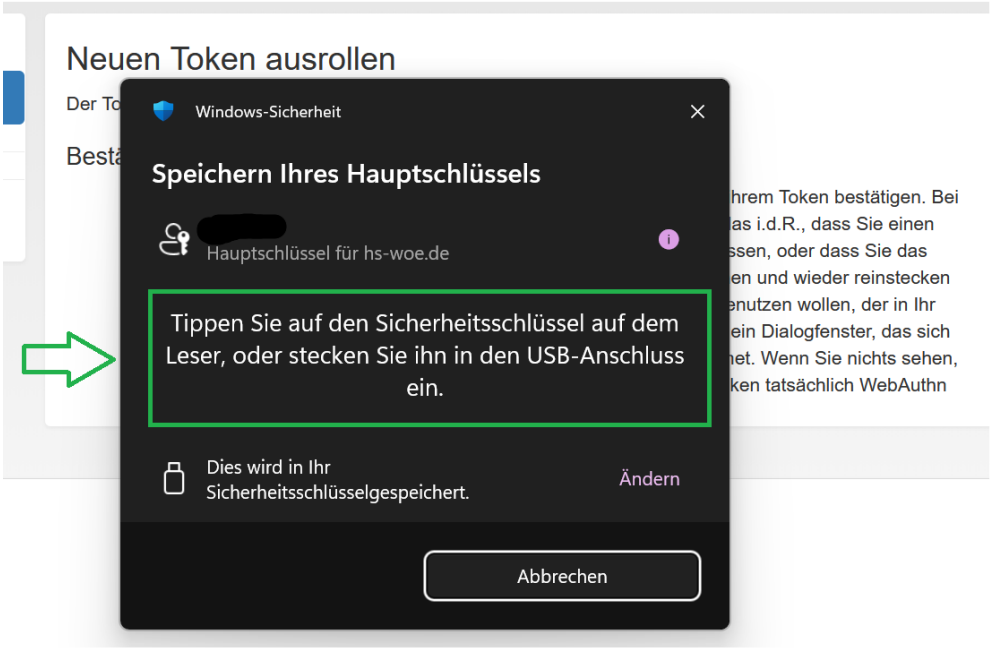
5) Über den Button „Ändern“ können Sie auswählen, wo dieser Schlüssel gespeichert ist.



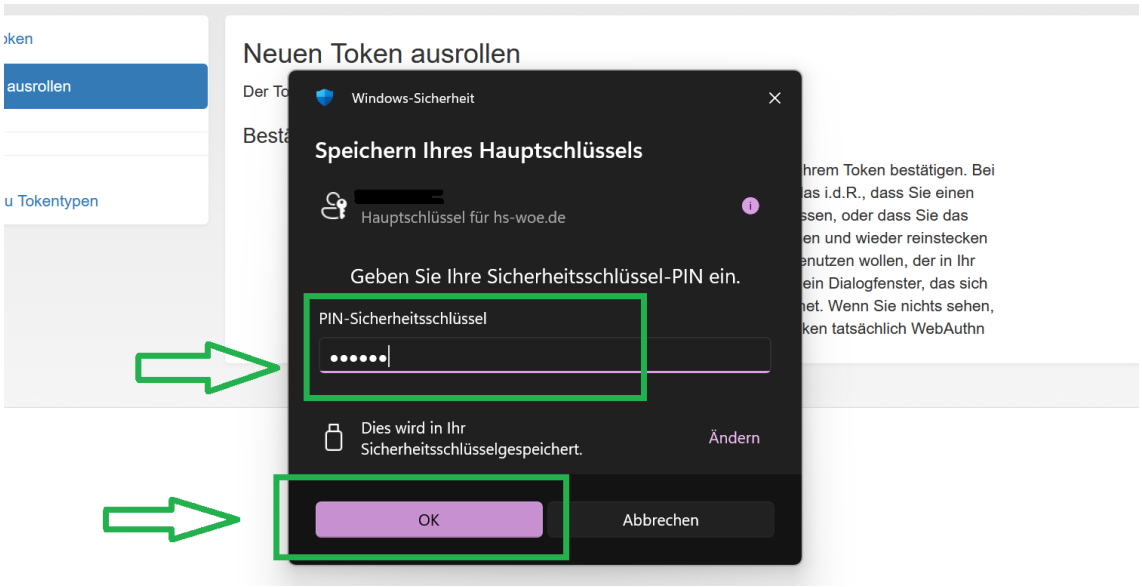
6) Je nachdem, was Sie als Authentifizierungs-Methode (Hardwareschlüssel, Biometrie oder ein Passwort Manager) hinterlegt haben, können Sie entsprechend auswählen.



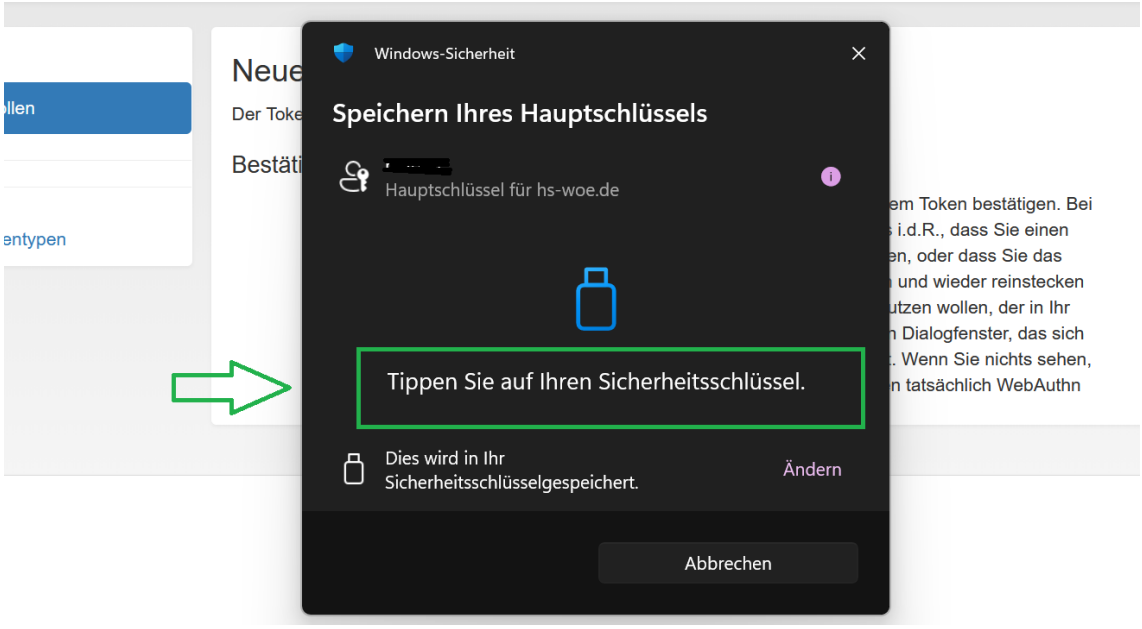
7) Beim Auswählen der **Sicherheitsschlüssel-Funktion** z.B. „USB-Hardware-Schlüssel“ werden Sie aufgefordert diesen Schlüssel in Ihrem Gerät einzustecken, möglicherweise zu berühren und abschließend Ihren selbst hinterlegten PIN einzugeben.



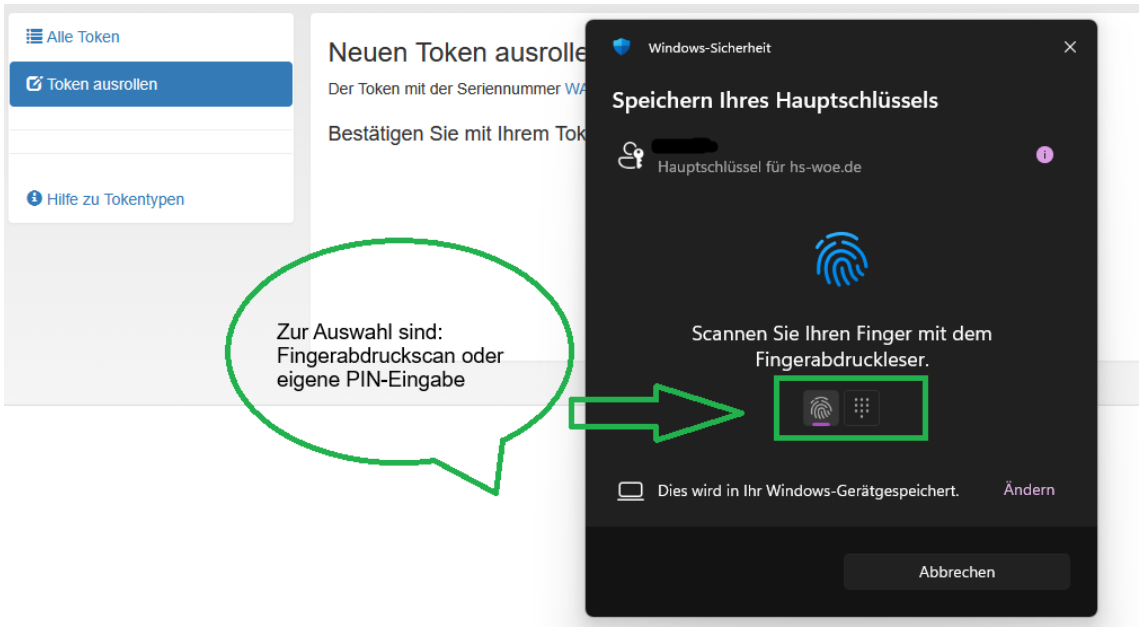
8) Geben Sie Ihre bereits hinzugefügte Sicherheitsschlüssel-PIN ein und bestätigen Sie mit „OK“.



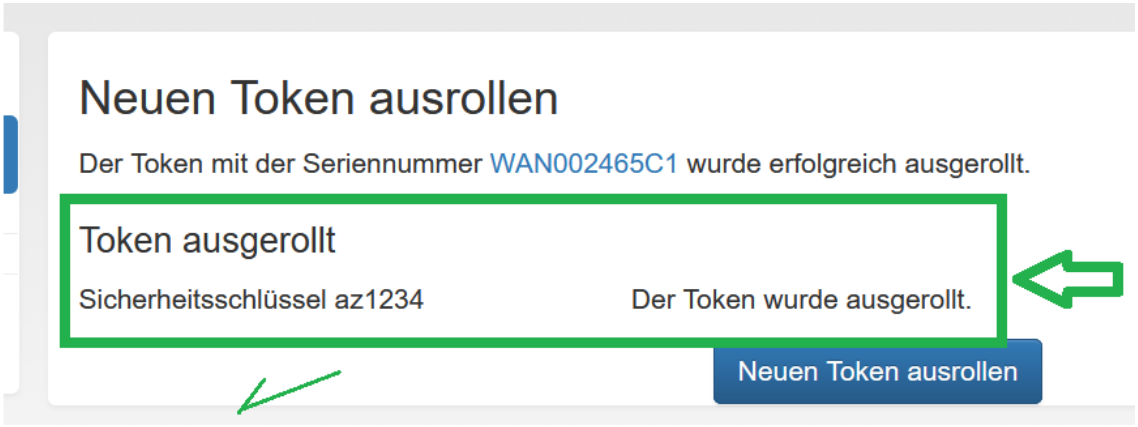
9) Möglicherweise müssen Sie, abhängig vom Typ Ihres Sicherheitsschlüssels, den Finger zur Bestätigung auf die Mitte des Schlüssels oder auf den seitlichen Metallsensor legen.



10) Beim Auswählen der **Biometrie-Funktion** hier „Windows Hello“ werden Sie aufgefordert entweder Ihre biometrischen Daten (Fingerabdruck, Gesicht) zu scannen, oder Ihren hinterlegten PIN einzugeben.



11) Vergewissern Sie sich, dass Ihnen im eduMFA-Portal angezeigt, dass das Token ausgerollt ist. Ansonsten wird das Token nicht richtig aktiviert sein.



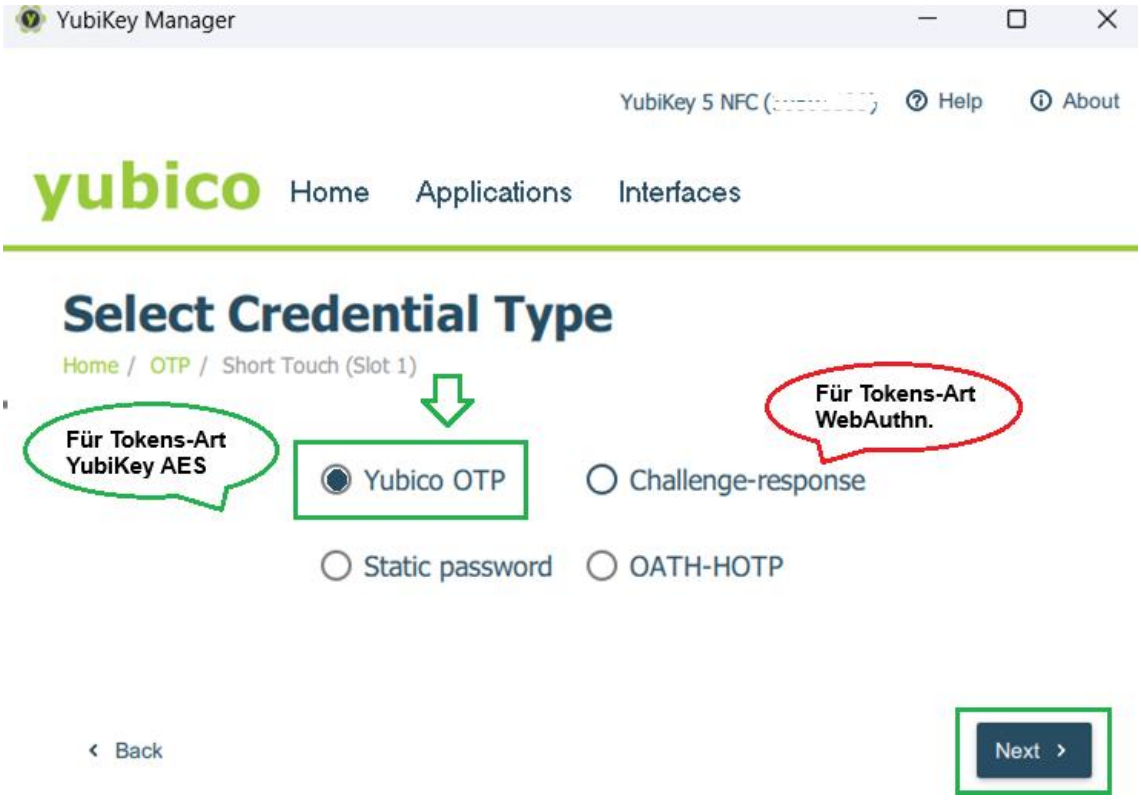
8.6 YubiKey-Token (spezieller Sicherheitsschlüssel) ausrollen

Bei diesem Token-Type sollten Sie beachten, dass der ***Security Key NFC Yubico*** **nicht als YubiKey** gilt., (für diesen genannten Security Key ist das Token WebAuthn. Geeignet, wie auf S. 15 beschrieben).

Der YubiKey sollte gängige Authentifizierungsprotokolle unterstützen (z. B. FIDO2, Yubico OTP). Der geheime Schlüssel in Hex und die gesamte Länge des OTP-Wertes werden hier benötigt.

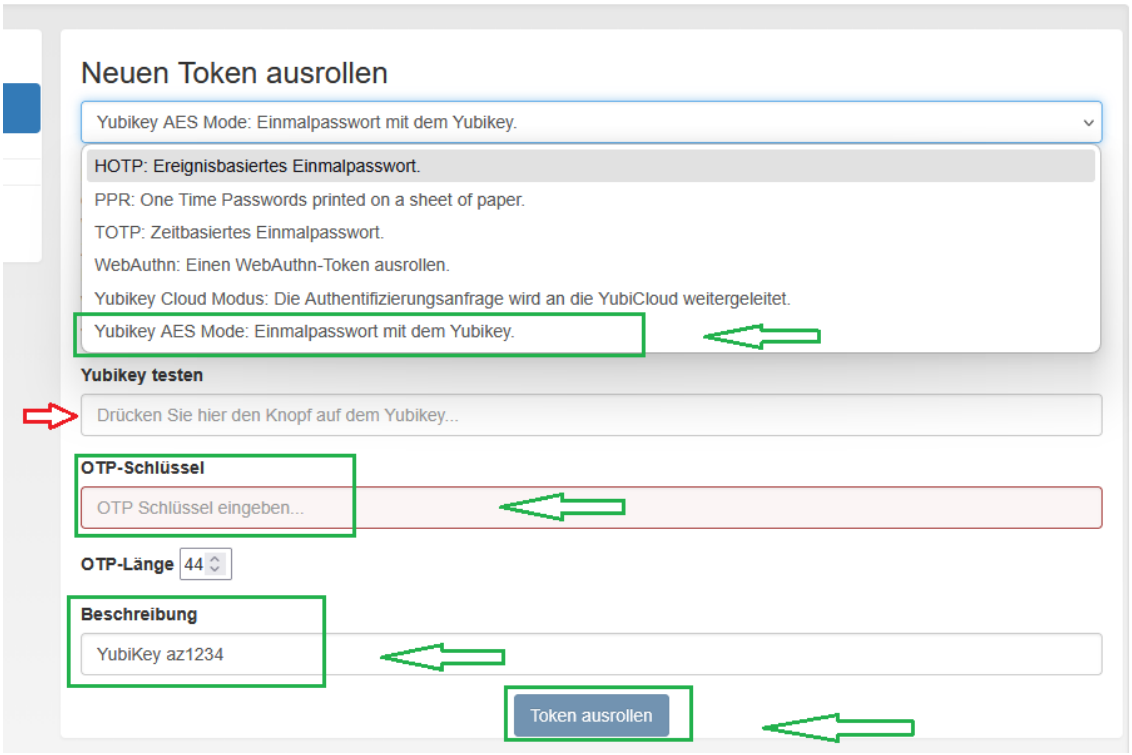
Zuerst sollen Sie Ihren Yubikey in den Gerät-Einstellungen, wie im Kapitel 8.5.1 oben beschrieben, (oder auch in der App YubiKey Manager) richtig einrichten.

Wichtig: Der passende „Credential Type“ Des YubiKeys soll für diesen Tokenart **„Yubico OTP“** im YubiKey Manager ausgewählt werden.



1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier YubiKey AES) auswählen.

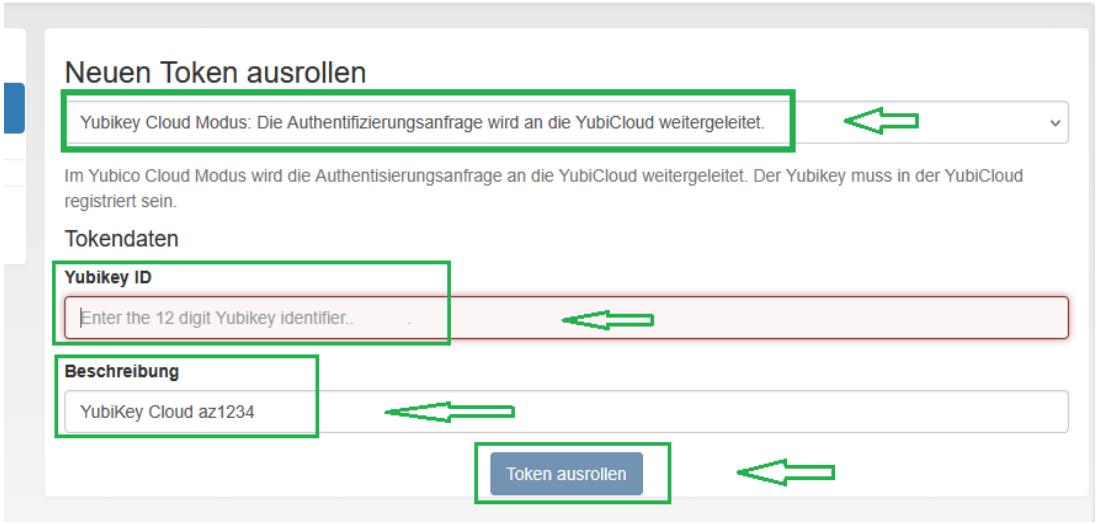
2) Im Feld Yubikey Testen können Sie den Knopf auf Ihrem Yubikey drücken und ihn testen.
3) Dann geben Sie den geheimen Schlüssel in Hex ein.
4) Dann wählen Sie die gesamte Länge des OTP-Wertes aus.
5) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Token-Art & Nutzername).
6) Abschließend auf „Token ausrollen“ klicken.



8.7 YubiKey Cloud-Token ausrollen

Im Yubikey Cloud Modus wird die Authentisierungsanfrage an die YubiCloud weitergeleitet. Der Yubikey muss in der YubiCloud registriert sein.

1) Unter dem Menü „Neuen Token ausrollen“ können Sie den gewünschten Token-Typ (hier YubiKey Cloud Modus) auswählen.
2) Dann geben Sie den 12-stelligen Yubikey ID ein.
3) Geben Sie im Feld „Beschreibung“ einen Namen für Ihr Token ein (z.B. Token-Art & Nutzername).
4) Abschließend auf „Token ausrollen“ klicken.



8.8 Unsere Empfehlung für Sie

Für die meisten Nutzer empfehlen wir die Einrichtung mehrerer Token-Arten.

Besonders sinnvoll ist die Kombination aus einem TOTP-Token (z. B. über eine Authenticator-App oder einen Passwortmanager) und einem WebAuthn-Token (Passkey bzw. Hardware-Sicherheitsschlüssel).

So können Sie Ihr zweites Token nutzen, wenn Sie das andere gerade nicht zur Hand haben.

Gleichzeitig helfen Sie dabei, Support-Anfragen zu reduzieren.

9. Wie erfolgt die Anmeldung mit MFA

Viele Hochschuldienste sind aktuell mit MFA gesichert. V.a. SSO IdP-Dienste (Moodle, Webex, und andere interne Verwaltungs-Dienste), eduVPN sowie Microsoft 365.

Die Anmeldung mit MFA erfolgt wie bisher, jedoch mit einem zusätzlichen Schritt.

Je nach Art und Anzahl Ihrer Tokens können Sie auswählen, mit welchem Token Sie authentifizieren möchten.

Sie können entweder mit Passkey (Hardware-Token, Yubikey, Biometrie) oder mit dem 6-Stelligen Einmal-Code aus der App/Liste (TOTP, HOTP, PPR) anmelden.

9.1 Mit TOTP oder PPR beim Hochschuldienst anmelden

Voraussetzung ist, dass Sie Ihr Token (TOTP/HOTP/PPR) bereits im eduMFA-Portal ausgerollt haben. Anschließend können Sie dieses als zweiten Faktor nutzen.

Nachdem Sie sich mit Ihrem Nutzername und Passwort an einem Dienst der Jade Hochschule angemeldet haben, wird Ihnen diese Anmeldemaske angezeigt.

Im unteren Eingabefeld können Sie das 6-stellige Einmalpasswort (OTP) aus Ihrer App bzw. PPR-Liste eingeben und anschließend mit „Überprüfen“ bestätigen.

Falls Sie das PPR-Token verwenden, wird Ihnen als Orientierungs-Hilfe ein Hinweis mit Nr. angezeigt, damit Sie wissen, welches OTP aus der Liste abschreiben sollen.

9.2 Mit Passkey oder Hardware-Schlüssel beim Hochschuldienst anmelden

Zunächst sollten Sie Ihr Token (WebAuthn / YubiKey) im eduMFA-Portal schon ausgerollt haben, können Sie dieses bei der Anmeldung als zweiter Faktor nutzen und damit authentifizieren.

Nachdem Sie sich mit Ihrem Nutzername und Passwort an einem Dienst der Jade Hochschule angemeldet haben, wird Ihnen diese Anmeldemaske angezeigt.

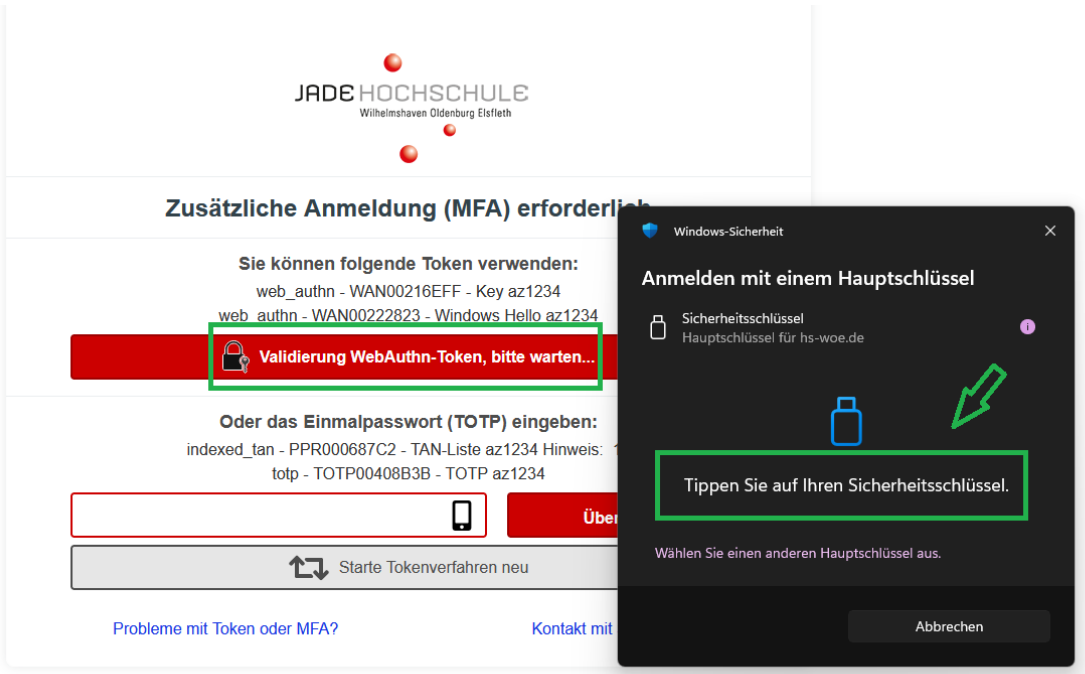
Klicken Sie auf das erste Button „Mit Passkey oder Sicherheitsschlüssel anmelden“.

Dann wählen Sie die gewünschte Methode (Biometrie oder Hardware-Schlüssel) aus.

Falls Sie die Methode „Sicherheitsschlüssel ausgewählt haben“, stecken Sie Ihren Hardware-Schlüssel und folgen Sie den Anweisungen.

Dann geben Sie Ihre PIN für den Schlüssel ein und auf „OK“ klicken.

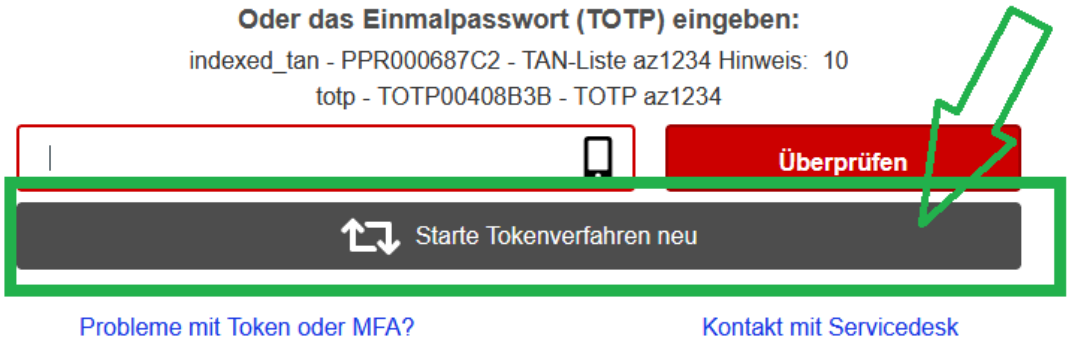
Abschließend bestätigen Sie Ihren Schlüssel mit einem Fingertipp auf dem Schlüssel.



Token-Verfahren neustarten:

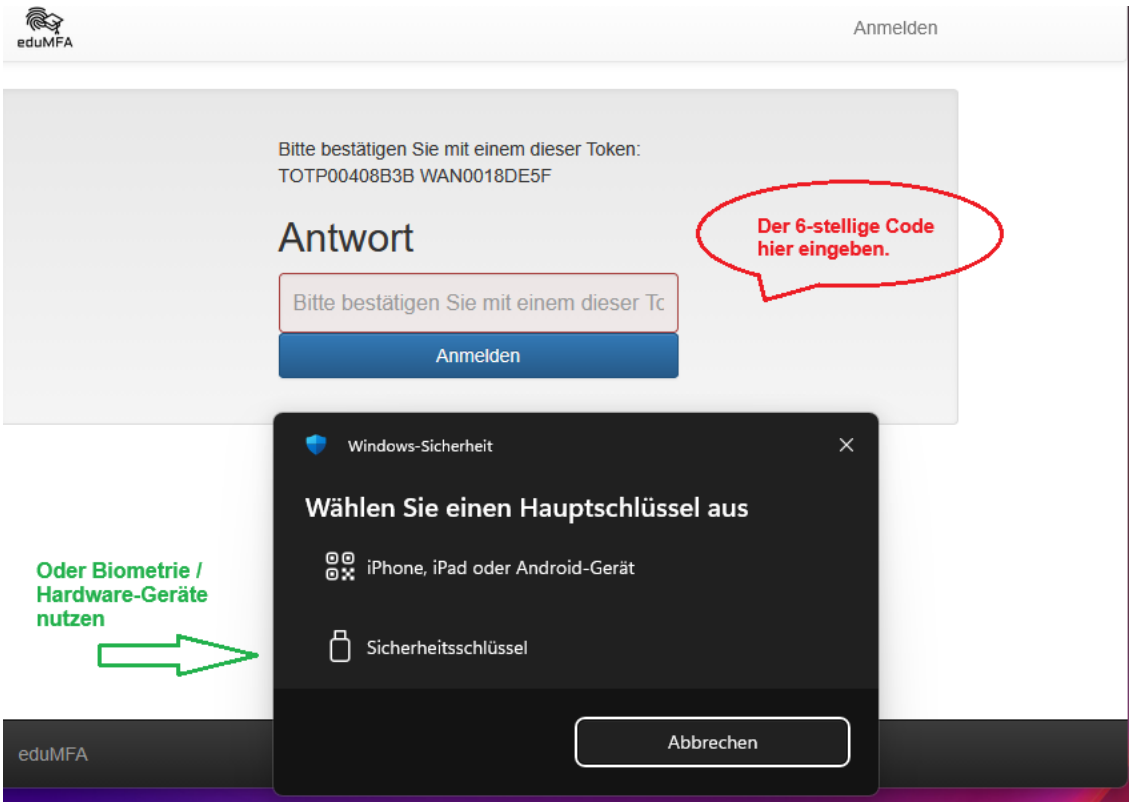
Es kann passieren, dass Sie aus einem beliebigen Grund verzögert haben, mit Ihrem Token anzumelden und somit die Zeit abgelaufen wurde.

Dabei können Sie einfach auf dem Button „Starte Tokenverfahren neu“ ganz unten klicken und nochmal versuchen, mit Ihrem Token anzumelden.



9.3 Mit MFA beim eduMFA-Portal anmelden

Oder Sie melden sich erneut im eduMFA-Portal an. Nach Eingabe der Nutzername und Passwort geben Sie den 6-stelligen Code aus der App/TAN-Liste ein oder verwenden Sie Ihren Hardware-Token, um die MFA zu bestätigen.



10. eduMFA mit Microsoft „M365“ verbinden

eduMFA kann in Ihrem Microsoft-Konto für die MFA als externe Anmeldemethode hinterlegt werden. Damit können Sie eduMFA auch für Microsoft 365-Dienste (z.B. SharePoint, Outlook, Teams) als zweiten Faktor nutzen.

Wichtiger Hinweis:

Es ist nicht möglich, die externe MFA-Methode (eduMFA) in Microsoft als bevorzugte Methode festzulegen. Wenn mehrere MFA-Methoden in Ihrem Microsoft-Konto hinterlegt sind, werden diese von Microsoft standardmäßig zuerst angezeigt.

Empfehlung:

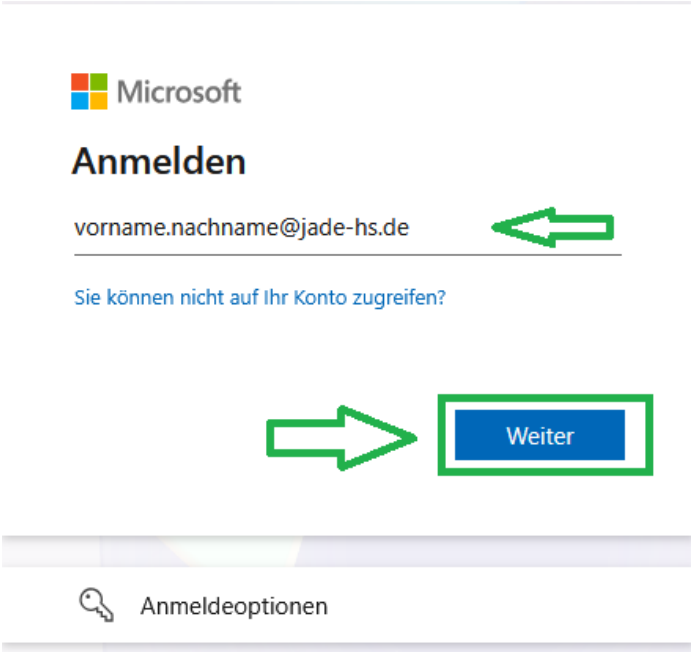
Hinterlegen Sie daher möglichst nur die eduMFA als einzige Anmeldemethode in Ihrem Hochschul- Microsoft-Konto.

So vermeiden Sie zusätzliche Schritte bei der Anmeldung und erhalten eine einheitliche Nutzererfahrung.

10.1 Einrichtung der Verbindung:

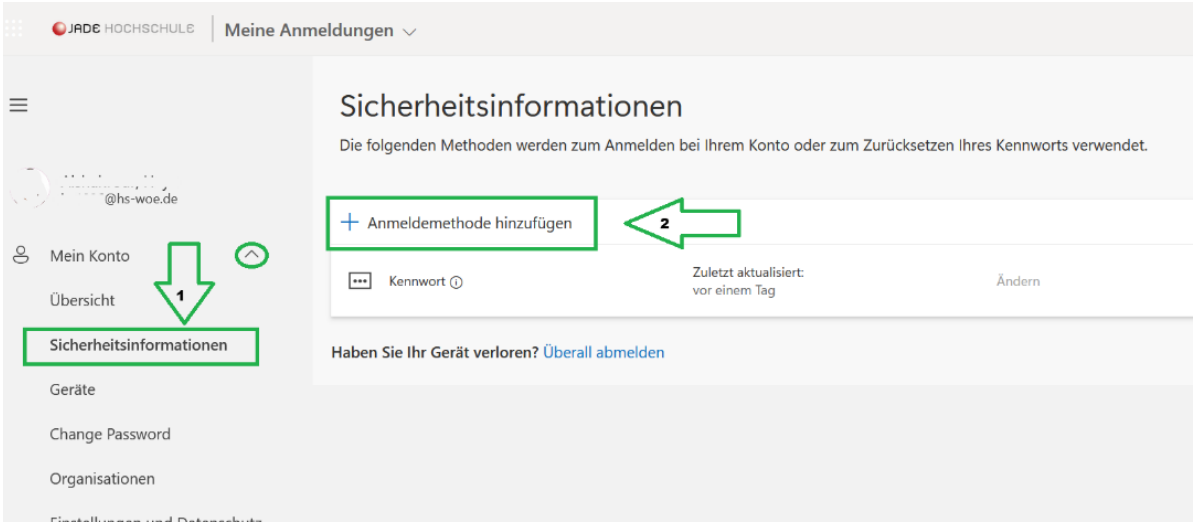
Vorausgesetzt, dass Sie im eduMFA-Portal mindestens 1 Token eingerichtet haben.

1) Öffnen Sie die Microsoft-Webseite: https://myaccount.microsoft.com/ und melden Sie sich mit Ihrer E-Mail-Adresse (vorname.nachname@jade-hs.de oder @student.jade-hs.de) oder UPN-Benutzernamen (xx9999@hs-woe.de) an.



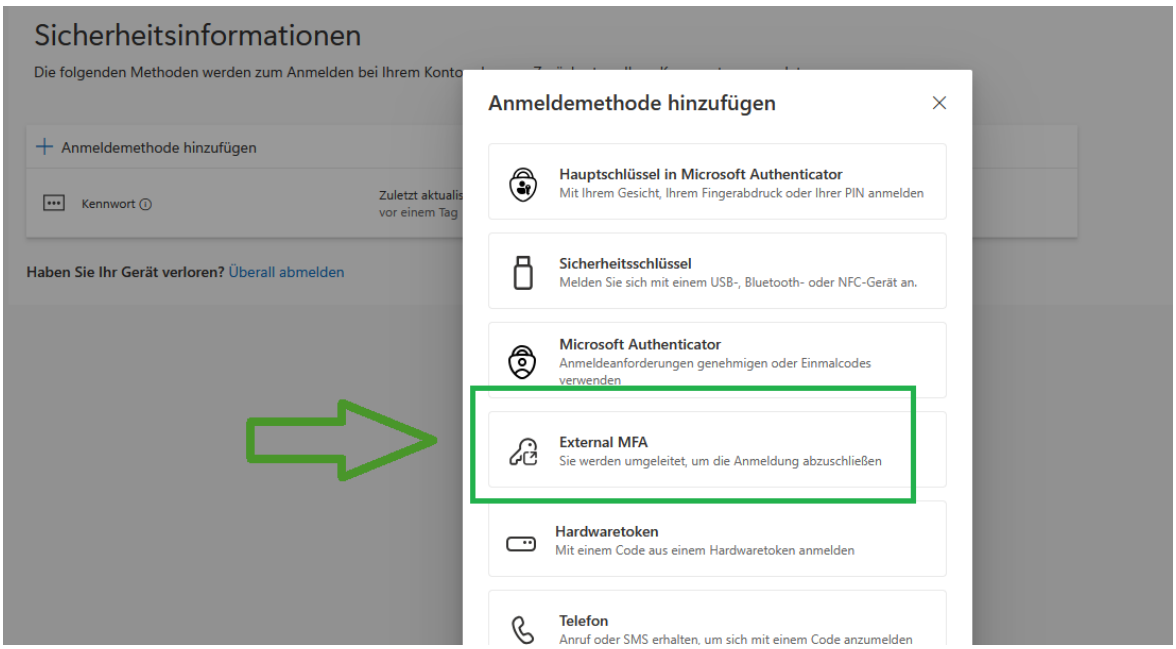
2) Wählen Sie im Menü links den Punkt „Sicherheitsinformationen“ aus.

3) Klicken Sie auf „+ Anmeldemethode hinzufügen“.



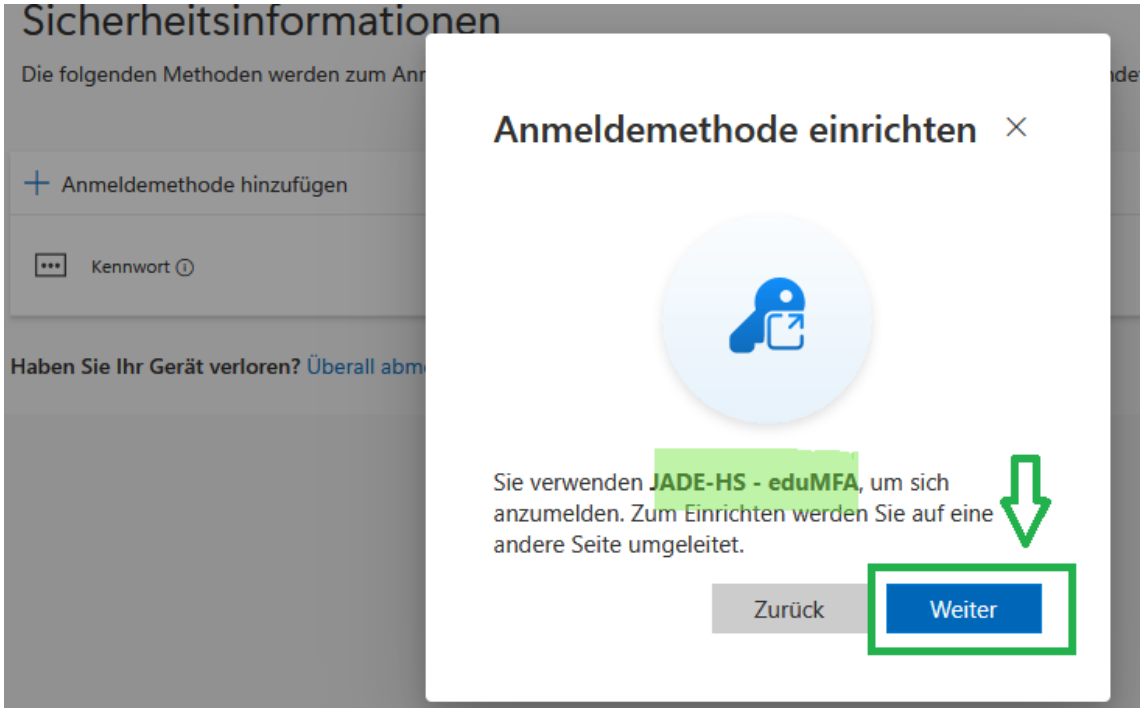
4) Es erscheint ein Fenster mit verschiedenen Methoden.

Wählen Sie die Option „External MFA“ aus.



5) Es wird ein Fenster „Anmeldemethode einrichten“ angezeigt.

Klicken Sie auf „Weiter“.

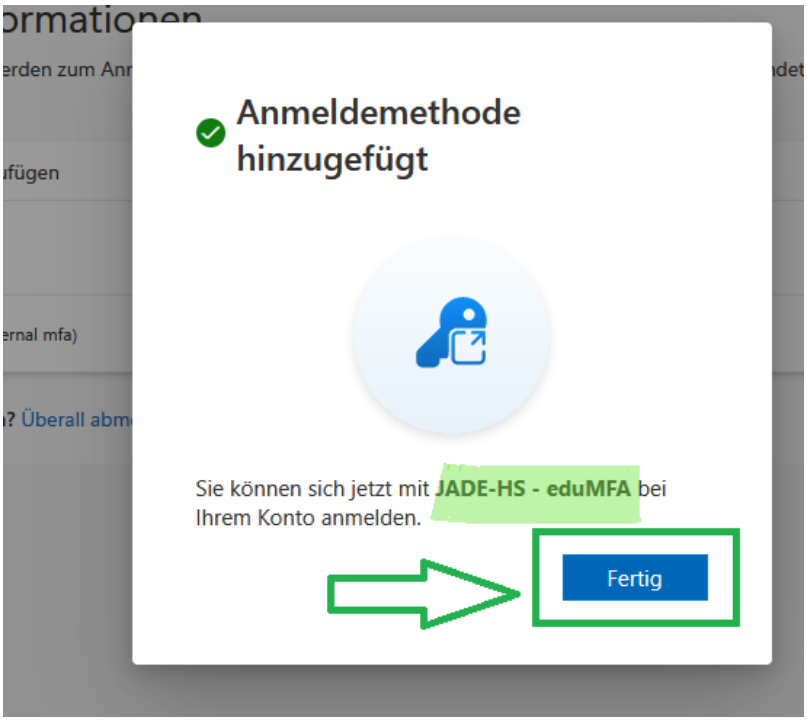


6) Bestätigen Sie ggf. Ihr bereits in eduMFA eingerichtetes Token.

7) Nach erfolgreicher Einrichtung erscheint die Meldung:

„Anmeldemethode hinzugefügt. Sie können sich jetzt mit JADE-HS - eduMFA anmelden.“

Klicken Sie auf „Fertig“.



8) Abschließend sollte die eduMFA unter Ihren Anmeldemethoden angezeigt sein.

10.2 Anmeldung mit eduMFA bei mehreren hinterlegten Methoden in M365

Wenn in Ihrem Microsoft-Konto mehrere Anmeldemethoden (z. B. Microsoft Authenticator & eduMFA) hinterlegt sind, wird die eduMFA-Anmeldung nicht automatisch angezeigt.

Gehen Sie in diesem Fall wie folgt vor:

1) Stellen Sie sicher, dass eduMFA bereits mit Ihrem Microsoft-Konto verbunden ist (siehe 10.1 oben).

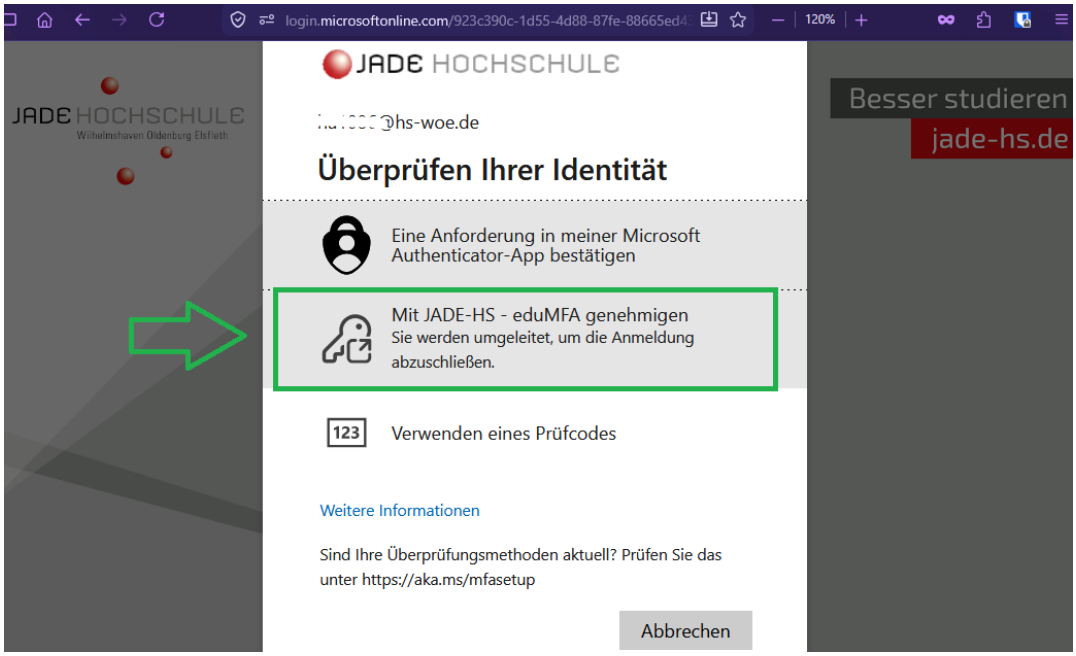
2) Melden Sie sich auf der Microsoft-Webseite mit Ihren Hochschuldaten an.

3) Wenn Sie zur MFA aufgefordert werden, erscheint möglicherweise zunächst eine Abfrage über die Microsoft Authenticator App.

   Wählen Sie unten die Option „Ich kann meine Microsoft Authenticator-App im Moment nicht verwenden“ aus.

4) Es werden Ihnen alternative Anmeldemethoden angezeigt.

Wählen Sie „Mit JADE HS – eduMFA genehmigen“ aus.



5) Sie werden zur eduMFA-Anmeldeseite der Jade Hochschule weitergeleitet. Bestätigen Sie dort Ihr Token – die Anmeldung ist damit abgeschlossen.

11. Verwaltung der Tokens im eduMFA-Portal

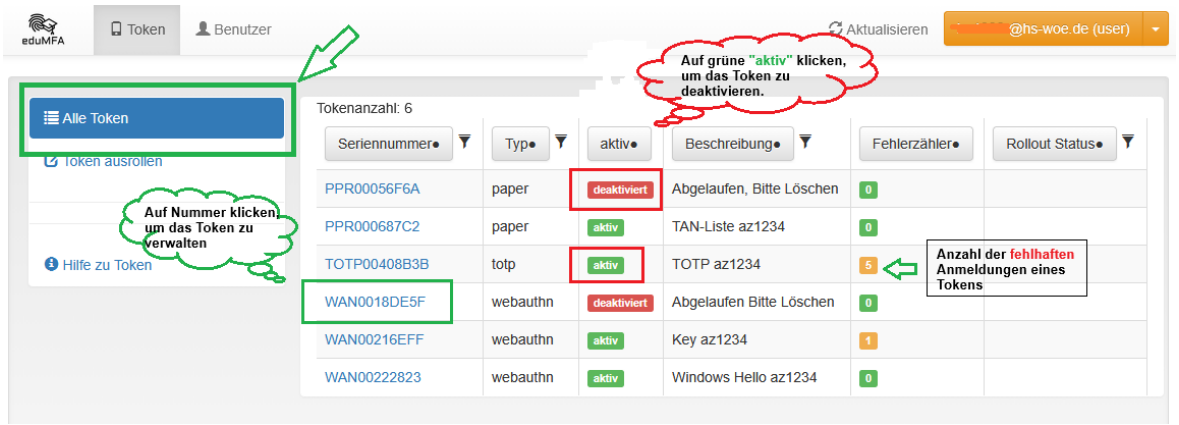
Melden Sie sich im eduMFA-Portal mit MFA. Wenn Sie auf „Alle Token“ klicken, sollten Sie alle Ihre Tokens sehen und verwalten (Deaktivieren und Umbenennen).

11.1 Ihr Token beim Verlust oder Ablauf Deaktivieren

Im Portal können Sie Ihr abgelaufenes, verlorenes oder nicht mehr benötigtes Token deaktivieren, indem Sie auf dem grünen Button **„aktiv“** des entsprechenden Tokens klicken.

Wenn Sie ein Token deaktiviert haben, können Sie es aus Sicherheitsgründen nicht selbst wieder aktivieren.

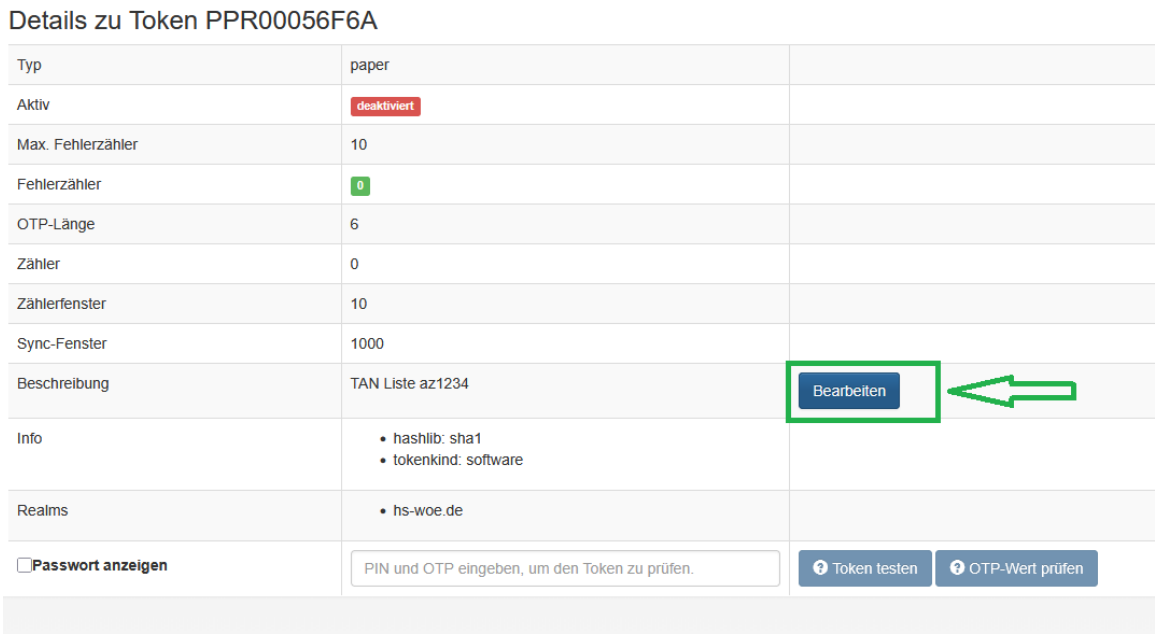
Falls Sie ein Token aus Versehen deaktiviert haben, aber Sie es noch weiternutzen wollen, wenden Sie sich in diesem Fall an den MFA-Support im HRZ.



11.2 Ihre Tokens-Beschreibung Ändern

Die Beschreibung Ihres Tokens können Sie ändern, indem Sie auf die blaue Tokens-Nummer (z.B. WAN0018DE5F) klicken.

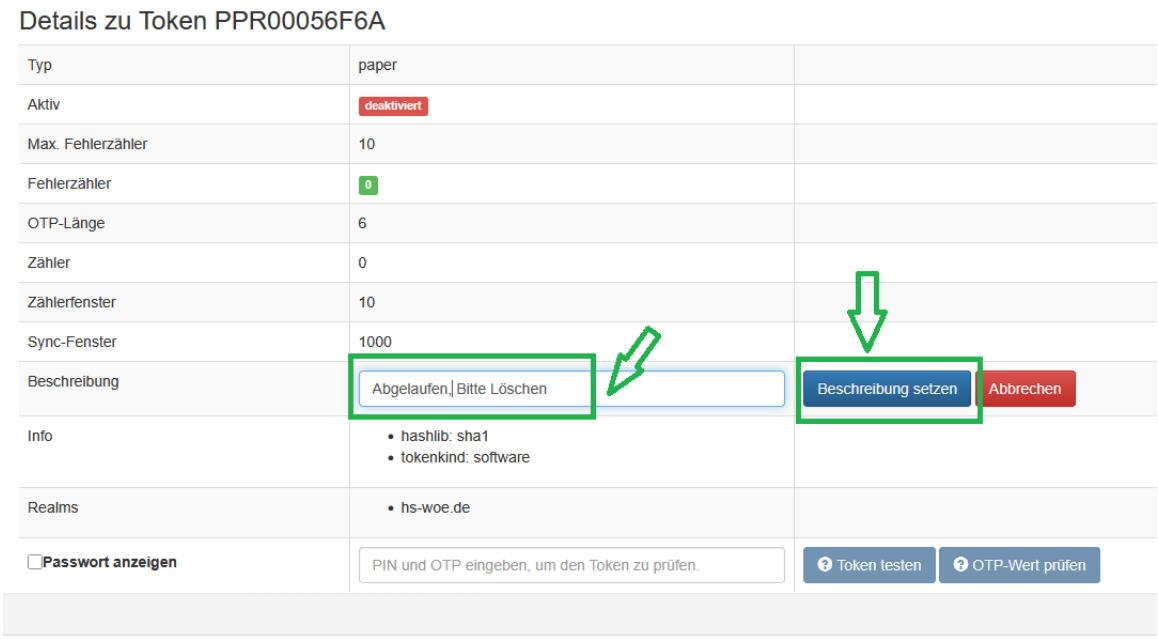
Dann wählen Sie „Bearbeiten“ aus.



Geben Sie eine neue Beschreibung in dem Feld ein und abschließend auf „Beschreibung setzen“ klicken.

Für eine besser MFA-Verwaltung:

Für Ihr nicht mehr benötigtes Token geben Sie in der Beschreibung „Löschen“ ein, damit der zuständige Mitarbeiter Ihr deaktiviertes Token löschen wird.



11.3 Ihr Token Reaktivieren oder Löschen

Aus Sicherheitsgründen können Nutzer ihre Tokens weder löschen noch reaktivieren. In solchen Fällen wenden Sie sich bitte an den MFA-Support im HRZ.

12. 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.

13. Gesperrter Zugriff nach zu vielen Fehlerversuchen

Nach zehn fehlerhaften Anmeldeversuchen wird der Zugriff automatisch gesperrt.

Wenden Sie sich bitte in diesem Fall an den MFA-Support, um den Zähler zurücksetzen zu lassen.

14. 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:

hrz-servicedesk@jade-hs.de oder informationssicherheitsmanagement@jade-hs.de.

15. Hinweise zum Datenschutz bei der MFA-Nutzung

Bei der Nutzung von MFA werden Ihre Daten sicher verarbeitet.

- Die Authentifizierung erfolgt über sichere kryptografische Verfahren, bei denen keine sensiblen Informationen (wie z. B. Ihr Passwort oder biometrische Daten) übertragen werden.

- Bei der Einrichtung eines appbasierten Tokens (TOTP/HOTP) wird lediglich ein technischer Schlüssel (TOTP-Secret mit Token-Label) zur Generierung der Einmalcodes in die App übernommen. Es werden dabei keine Passwörter oder anderen sensiblen Zugangsdaten an die verwendete App übermittelt.

  Der Schlüssel dient ausschließlich zur lokalen Erzeugung von Einmalcodes auf Ihrem Gerät.

- Bei der Verwendung von WebAuthn (z. B. Fingerabdruck oder Gesichtserkennung) verbleiben die biometrischen Daten ausschließlich auf Ihrem Endgerät und werden nicht an die Hochschule oder externe Dienste übertragen.

Hinweis:

Bei der Nutzung von Authenticator-Apps oder Passwortmanagern können anbieterabhängig Daten (z. B. im Rahmen von Backup- oder Synchronisations-Funktionen) durch den jeweiligen Dienst verarbeitet werden.

Bitte beachten Sie hierzu die Datenschutzbestimmungen des jeweiligen Anbieters.