Anleitung Einrichtung und Nutzung eduMFA

Version 1.1

Stand vom: 31. Oktober 2025

Inhaltsverzeichnis

1 Token ausrollen **2**

2 TOTP-Token ausrollen **3**

3 TAN-Liste ausrollen **4**

4 PUSH-Token ausrollen **5**

5 YubiKey 5 / 5C NFC für OTP einrichten **6**

5.1 Einrichtung des YubiKey mit dem Yubico Authenticator 6

5.2 Hinzufügen des YubiKey im eduMFA-Portal 8

Um die Zugänge zu Diensten der Universität sicherer zu gestalten, wird in Zukunft neben dem Passwort, das Sie für Ihr ZIMT- oder ZV-Konto hinterlegt haben, ein weiterer Schlüssel, der sogenannte zweite Faktor oder Token, notwendig sein. Dieser zweite Faktor kann in verschiedenen Formen vorliegen. Beispielsweise als zeitbasiertes Einmalpasswort (erfordert eine beliebige Authenticator-App), als Push-Bestätigung mit einer App (erfordert die `eduMFA Authenticator`-App), als ereignisbasiertes Einmalpasswort (erfordert eine private E-Mail-Adresse) oder auch als spezieller USB-Stick (erfordert einen YubiKey).

Die folgende Anleitung soll Ihnen dabei helfen, einen oder im Idealfall mehrere solcher zweiten Faktoren für Ihre Zugänge einzurichten und zu aktivieren. Die Verwaltung dieser zusätzlichen Schlüssel geschieht über die webbasierte Plattform `eduMFA`[1].

Die vorliegende Anleitung führt Sie durch die Konfiguration von eduMFA (siehe Kap. 1 *Token ausrollen*).

Die Einrichtung und Testung nimmt circa 10 Minuten in Anspruch.

1 Token ausrollen

Um eduMFA zu konfigurieren, gehen Sie zunächst in Ihrem Webbrowser auf die folgende Website: `https://mfa.uni-siegen.de/`.

In Abbildung 1 sehen Sie auf der linken Seite die Anmeldemaske in der Sie Ihre ZIMT- oder ZV-Kennung und Ihr Passwort eintragen und mit einem Klick auf `Anmelden` bestätigen.

Um einen neuen Token festzulegen, klicken Sie in der linken Menüleiste des Portals auf den Eintrag `Token ausrollen` (in Abbildung 1 rechts dargestellt).

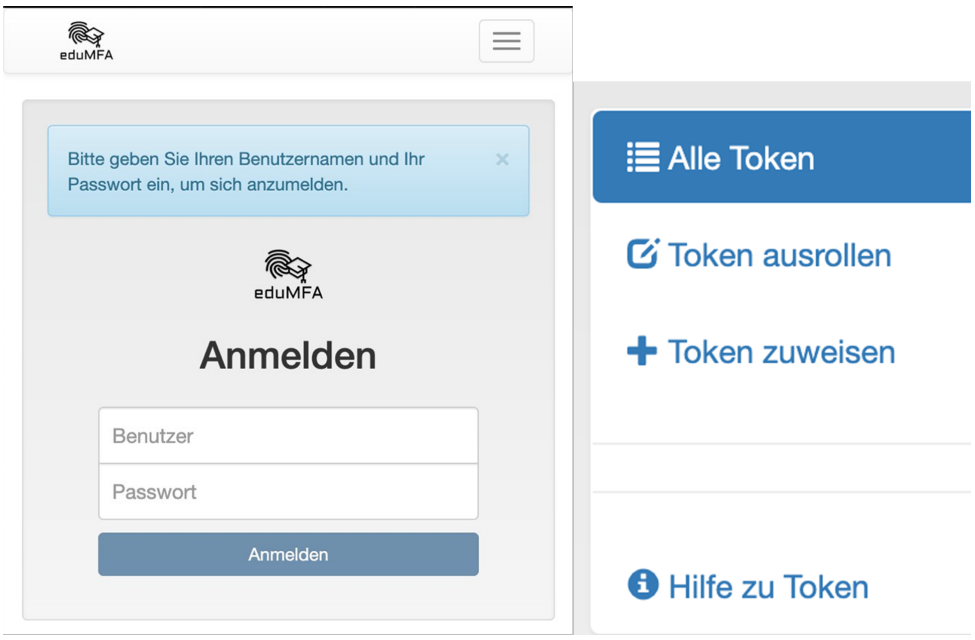

Abbildung 1: Anmeldemaske eduMFA (links) und Menüausschnitt (rechts).

[1] `https://mfa.uni-siegen.de/`

Die nun erscheinende Eingabemaske dient dem Erstellen eines zweiten Schlüssels. Im ersten ausklappbaren Menü ist standardmäßig ein `PUSH-Token` ausgewählt. Wenn Sie die Menüliste ausklappen, sehen Sie alle verfügbaren Schlüssel (siehe Abbildung 2).

Hinweis: Aktuell werden folgende Schlüssel unterstützt:

- *PUSH: Sendet eine Push-Benachrichtigung an ein Smartphone.*
  Nutzbar durch die `eduMFA Authenticator`-App.
- *TAN: TANs printed on a sheet of paper. Klassische TAN-Liste.*
  Nur für den Notfallzugang zu empfehlen.
- *TOTP: Zeitbasiertes Einmalpasswort.*
- *Yubikey AES Mode: Einmalpasswort mit dem Yubikey.*

Nach dem Ausrollen eines Tokens wird bei der nächsten Anmeldung auf der Login-Seite des ZIMT – beispielsweise für den Zugang über eduVPN – dieser zweite Faktor von Ihnen eingegeben werden müssen. Ohne diesen zweiten Faktor ist ein Anmelden am Dienst (hier eduVPN) nicht mehr möglich.

Es wird daher dringend empfohlen, dass Sie mindestens zwei Schlüssel, z. B. in Form eines TOTP-Tokens und einer TAN-Liste, generieren, sodass Sie im Notfall Zugang zu Ihrem Konto erhalten können. Wie Sie eine TAN-Liste erstellen, wird in Kap. 3 *TAN-Liste ausrollen* beschrieben.

2 TOTP-Token ausrollen

Um einen TOTP-Token auszurollen, klicken Sie in der linken Menüleiste des Portals auf den Eintrag `Token ausrollen` (in Abbildung 1 rechts dargestellt). Wählen Sie anschließend, wie in Abbildung 2 dargestellt, `TOTP` aus der Liste aus.

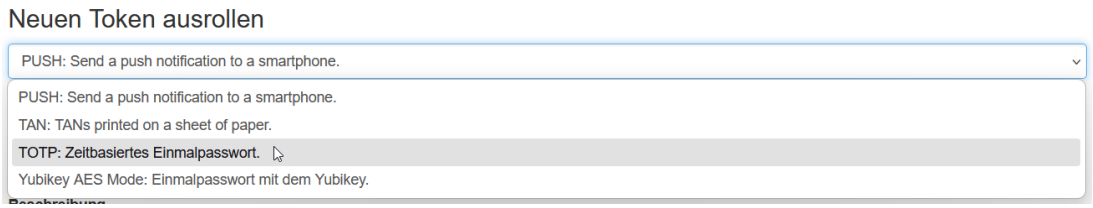

Abbildung 2: Auswahlmenü der Schlüsselarten (TOTP-Token).

Als nächstes definieren Sie die gewünschten Tokendaten (Abbildung 3). Hierbei handelt es sich zum einen um den `Zeitschritt`, der angibt, wie lange die verbleibende Gültigkeitsdauer des aktuellen Codes ist (30 s oder 60 s). Zum anderen der `Hash-Algorithmus` (sha1 oder sha256). Standardmäßig sind als Zeitschritt 60 s und der sha256 Hash-Algorithmus eingestellt. Die meisten Authenticator-Apps unterstützen diese Einstellungen. Sollten Sie einen Authenticator nutzen, der nur sha1 (z. B. der Microsoft Authenticator) und/oder nur 30 Zeitschritte unterstützt, wählen Sie dies vor dem Ausrollen entsprechend aus.

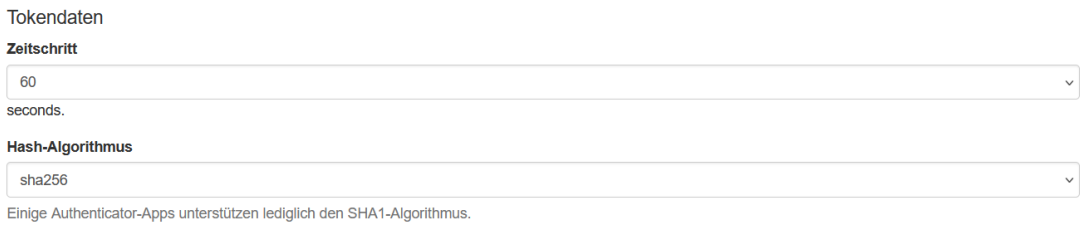

Abbildung 3: Auswahl der TOTP-Tokendaten.

Um die Schlüsselerstellung abzuschließen, muss noch eine Beschreibung vergeben werden. Tragen Sie hier einen für Sie identifizierbaren Namen ein.
Beispielsweise: `TOTP LastPass Authenticator App`

Ein Klick auf den Knopf `Token ausrollen` schließt den Einrichtungsprozess ab.

Auf der nun folgenden Seite (siehe auch Abbildung 4) wird ein sogenannter QR-Code angezeigt, den Sie mit einer beliebigen Authenticator-App (z. B. FreeOTP Authenticator oder LastPass Authenticator) und der Smartphone-Kamera abscannen müssen. Die entsprechenden Anwendungen finden Sie im Softwareportal (Google PlayStore für Android, AppStore für iOS) Ihres mobilen Geräts.

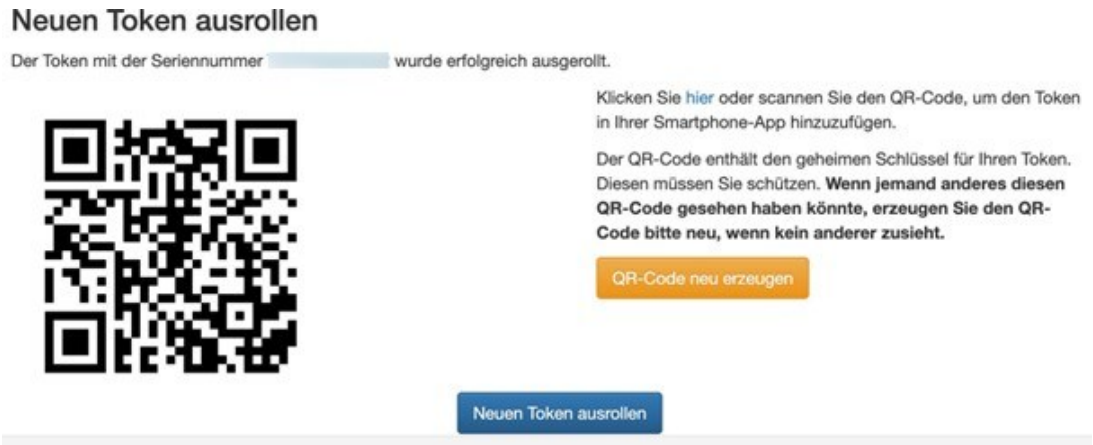

Abbildung 4: QR-Code für einen TOTP-Schlüssel der mit einer App gescannt werden muss.

Von diesem Moment an wird die App auf dem Smartphone in festgelegten Intervallen einen zweiten Faktor, bestehend aus einer 6-stelligen PIN, für Sie generieren.

3 TAN-Liste ausrollen

Um eine TAN-Liste auszurollen, klicken Sie in der linken Menüleiste des Portals auf den Eintrag `Token ausrollen` (in Abbildung 1 rechts dargestellt).

Die nun erscheinende Eingabemaske dient dem Erstellen eines weiteren Schlüssels. Im ersten ausklappbaren Menü ist standardmäßig ein `PUSH-Token` ausgewählt. Wenn Sie die Menüliste ausklappen, sehen Sie alle verfügbaren Schlüssel (siehe Abbildung 2).

Wählen Sie wie in Abbildung 5 dargestellt `TAN` aus der Liste aus.

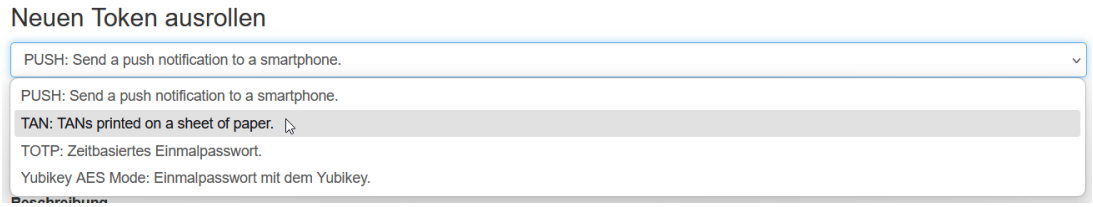

Abbildung 5: Auswahlmenü der Schlüsselarten (TAN-Liste).

Um die Schlüsselerstellung abzuschließen, muss noch eine Beschreibung vergeben werden. Tragen Sie hier einen für Sie identifizierbaren Namen ein.
Beispielsweise: `TAN-Liste November 2025`

Ein Klick auf den Knopf `Token ausrollen` schließt den Einrichtungsprozess ab.

Zuletzt klicken Sie auf die `OTP-Liste drucken` Schaltfläche (siehe Abbildung 6), um die TAN-Liste auszudrucken und anschließend an einem sicheren Ort (z. B. abschließbarer Schrank oder Rollcontainer) abzulegen. Bitte speichern Sie die TAN-Liste nicht auf Ihrem Gerät ab.

Abbildung 6: TAN-Liste ausdrucken.

Achtung: Nach dem Verlassen der Seite (siehe Abbildung 6) besteht keine Möglichkeit mehr, die TAN-Liste nachträglich auszudrucken. Schließen Sie die Seite also erst nachdem Sie die Liste ausgedruckt haben.

4 PUSH-Token ausrollen

Um einen PUSH-Token auszurollen, klicken Sie in der linken Menüleiste des Portals auf den Eintrag `Token ausrollen` (in Abbildung 1 rechts dargestellt). Wählen Sie wie in Abbildung 7 dargestellt `PUSH` aus der Liste aus.

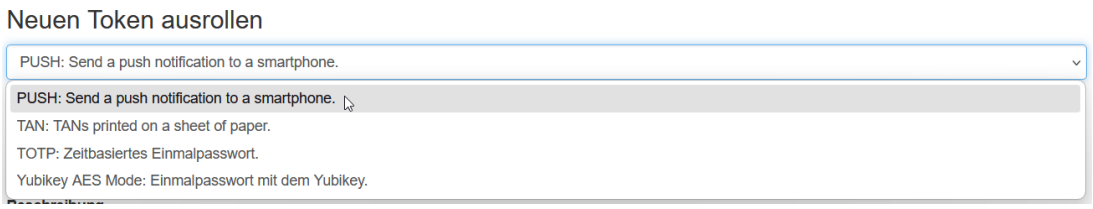

Abbildung 7: Auswahlmenü der Schlüsselarten (PUSH-Token).

Um die Schlüsselerstellung abzuschließen, muss noch eine Beschreibung vergeben werden. Tragen Sie hier einen für Sie identifizierbaren Namen ein.
Beispielsweise: `PUSH eduMFA Authenticator App`

Ein Klick auf den Knopf `Token ausrollen` schließt den Einrichtungsprozess ab.

Auf der nun folgenden Seite (siehe auch Abbildung 8) wird ein sogenannter QR-Code angezeigt, den Sie mit der `eduMFA Authenticator`-App und der Smartphone-Kamera abscannen müssen. Die entsprechende Anwendung finden Sie im Softwareportal (Google PlayStore für Android, AppStore für iOS) Ihres mobilen Geräts.

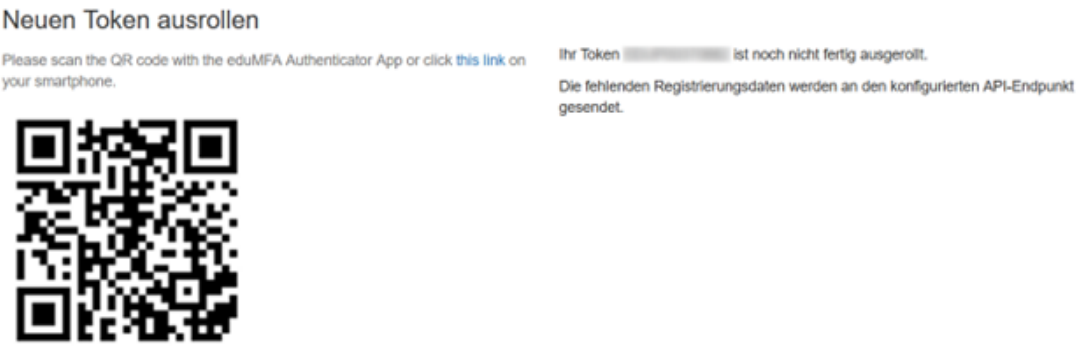

Abbildung 8: QR-Code für einen PUSH-Token.

Von diesem Moment an wird die App auf dem Smartphone eine PUSH-Benachrichtigung für Sie generieren, wenn ein zweiter Schlüssel abgefragt wird.

5 YubiKey 5 / 5C NFC für OTP einrichten

Falls Sie sich dafür entschieden haben, einen YubiKey als zweiten Faktor zu verwenden, sind die folgenden Schritte notwendig. Neben dem physischen YubiKey benötigen Sie das Programm `Yubico Authenticator`. Dieses können Sie auf der Herstellerseite[2] für Ihr Betriebssystem herunterladen.

5.1 Einrichtung des YubiKey mit dem Yubico Authenticator

Für die Authentisierung in eduMFA wird ein vom YubiKey generiertes Einmalpasswort (OTP) verwendet. Dieses muss zunächst von Ihnen eingerichtet werden. Öffnen Sie hierfür den `Yubico Authenticator` und gehen Sie auf `Slots` –> `Yubico OTP` (Abbildung 9).

Sie können im Yubico Authenticator zwei Speicherplätze konfigurieren:

Slot 1 - Short Touch (Kurze Berührung) oder **Slot 2 - Long Touch** (Lange Berührung).

Je nachdem, für welchen Slot Sie sich entscheiden, ist entweder eine kurze (1 – 2,5 Sekunden) oder eine lange (3 – 5 Sekunden) Berührung der in der Mitte des YubiKey liegenden goldenen Fläche nötig, um das Einmalpasswort zu generieren.

[2] https://www.yubico.com/products/yubico-authenticator/

Abbildung 9: Programmoberfläche des Yubico Authenticators.

Anschließend müssen Sie folgende drei Felder ausfüllen (Abbildung 10):

- `Öffentliche ID`: 12 Zeichen (6 Bytes) Modhex-Wert (nur Buchstaben).
- `Private ID`: 12 Zeichen (6 Bytes) Hex-Wert.
- `(Geheimer) Schlüssel`: 32 Zeichen (16 Bytes) Hex-Wert.

Abbildung 10: Festlegung der individuellen Werte auf den YubiKey. Der Wert des unteren `Schlüssel`-Felds wird später im eduMFA-Portal benötigt.

Klicken Sie im Feld `Öffentliche ID` auf das Symbol rechts (*Tooltip:* `Seriennummer verwenden`), um die Seriennummer Ihres YubiKey zu verwenden. Alternativ können Sie auch eigene Hex- und Dezimalwerte über den Modhex-Converter[3] von Yubico eingeben und anschließend den Modhex-Wert kopieren.

[3] https://developers.yubico.com/OTP/Modhex_Converter.html

Die Werte für die Felder `Private ID` und `Schlüssel` können einfach über die `Zufällig generieren`-Schaltflächen erstellt werden. Sie können diese beliebig oft verwenden.

Bitte dokumentieren Sie sich Ihre Werte in einer Form Ihrer Wahl (z. B. als Screenshot oder in einem Passwort-Manager) und bewahren Sie diese an einem sicheren Ort auf. Nach Abschluss der Einrichtung können Sie Ihre Werte nicht mehr einsehen.

Die Einrichtung des Einmalpasswortverfahrens auf dem YubiKey ist damit abgeschlossen.

5.2 Hinzufügen des YubiKey im eduMFA-Portal

Im nächsten Schritt muss der YubiKey in eduMFA hinterlegt werden. Melden Sie sich hierzu wie in Kap. 1 `Token ausrollen` im eduMFA-Portal an und rollen einen neuen Token aus.

Im Dropdown-Menü wählen Sie anschließend die Option `Yubikey AES Mode` aus (siehe Abbildung 11).

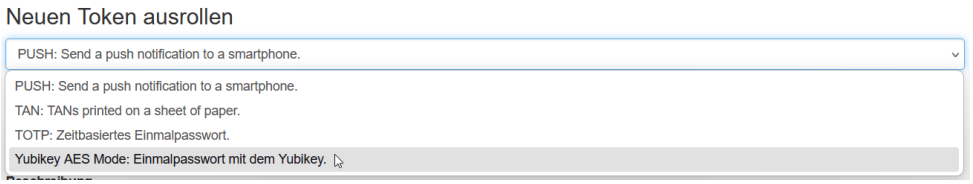

Abbildung 11: Auswahlmenü der Schlüsselarten (Yubikey AES Mode).

Nun müssen Sie im Feld `OTP-Schlüssel` (siehe Abbildung 12) Ihren zuvor generierten `Schlüssel` (siehe Abbildung 10, Nr. 2) eingeben. Außerdem sollten Sie eine Beschreibung festlegen (z. B. `YubiKey Kurze Berührung`).

Abbildung 12: Ausrollen eines YubiKey-Tokens.

Bestätigen Sie Ihre Eingabe über die Schaltfläche `Token ausrollen`. Ihr YubiKey kann ab sofort für die MFA-Abfrage verwendet werden.