Hochschule Kaiserslautern
University of Applied Sciences
Kompetenzzentrum Digitalisierung & Medien

Mehrfaktor-Authentifizierung (MFA)

Version 1.5, 25.08.2024

Zur Anmeldung bei Online-Diensten wie OpenOlat, BigBlueButton, Seafile, Panopto oder OWA (alle Dienste mit einer Authentifizierung über *Shibboleth*) benötigen Sie neben Ihrem Benutzernamen und Passwort nun auch einen weiteren Faktor für die Authentifizierung bei diesen Diensten.

Mit einer solchen *Mehrfaktor-Authentifizierung (MFA)* ist es Fremden dann nicht mehr möglich, bei Bekanntwerden Ihres Passworts auf alle Ihre Daten zuzugreifen.

Authentifizierungs-Methoden

Derzeit werden fünf Authentifizierungs-Methoden unterstützt:

- **HOTP: Einmal-Passwort ohne Zeitbegrenzung**
  Bei dieser Methode wird ein Code erzeugt, der sich nicht automatisch ändert. Wurde der Code einmal verwendet, muss ein neuer Code generiert werden.
  Für diese Methode wird eine Authentifikator-App benötigt!

- **TOTP: Einmal-Passwort mit Zeitbegrenzung**
  Bei dieser Methode wird ein Code erzeugt, der sich alle 30 bzw. 60 Sekunden ändert. Zur Anmeldung muss immer der aktuelle Code verwendet werden.
  Für diese Methode wird eine Authentifikator-App benötigt!

- **PPR: TAN-Liste mit Index**
  Bei dieser Methode wird eine indizierte TAN-Liste erzeugt. Jede TAN ist mit einer laufenden Nummer versehen. Zur Anmeldung muss die TAN mit der passenden Nummer eingegeben werden.

- **TAN-Liste (ohne Index)**
  Bei dieser Methode wird eine TAN-Liste erzeugt. Zur Anmeldung kann eine beliebige TAN der Liste eingegeben werden. Eine solche TAN ist nur einmal verwendbar und muss anschließend in der Liste abgestrichen werden.

- **YubiKey**
  Bei dieser Methode kommt ein Hardware-USB-Schlüssel zum Einsatz. Zur Anmeldung

muss eine Taste auf dem YubiKey gedrückt werden, der in einen freien USB-Port Ihres Gerätes eingesteckt ist.
Für diese Methode wird eine spezielle Hardware benötigt!

Empfehlungen

- Wir empfehlen, mehrere dieser Authentifizierungs-Methoden parallel zu verwenden, falls eine Methode nicht verfügbar ist oder nicht funktioniert. So ist beispielsweise eine ausgedruckte TAN-Liste oder der YubiKey am Schlüsselbund eine gute Alternative wenn das Smarthone gerade nicht zur Hand oder leer ist.

- Wir empfehlen, TAN-Listen auszudrucken und nicht auf dem Gerät zu speichern.

Authentifikator-Apps

Für die Methoden HOTP und TOTP wird eine sog. Authentifikator-App benötigt. Es gibt eine ganze Reihe solcher Apps und die bei uns verwendete Mehrfaktor-Authentifizierung sollte mit den meisten davon funktionieren.

Im Folgenden haben wir Ihnen eine Auswahl an verbreiteten Authentifikator-Apps zusammengestellt, die wir selbst ausprobiert haben und die sowohl für Android- als auch für iOS-Geräte erhältlich sind.

- **privacyIDEA Authenticator**
  Die Authentifikator-App vom Hersteller unseres MFA-Verfahrens.
  - Google Play Store
  - Apple App Store

- **Google Authenticator**
  - Google Play Store
  - Apple App Store

- **Microsoft Authenticator**
  - Google Play Store
  - Apple App Store

- **Twilio Authy**
  Zusätzlich als Desktop-App für Windows, Mac und Linux erhältlich. Eine Registrierung mit Telefonnummer und E-Mailadresse ist nötig.
  - Google Play Store
  - Apple App Store
  - Desktop-App

- **Cisco Duo Mobile**
  - Google Play Store
  - Apple App Store

- **FreeOTP**
  - Google Play Store
  - Apple App Store

YubiKey einrichten

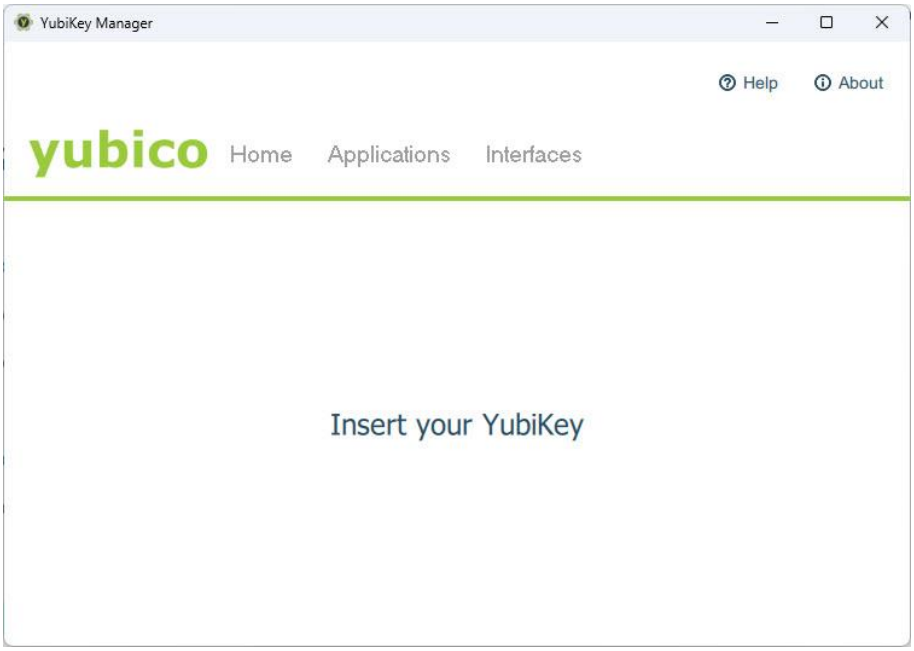
Der YubiKey ist ein Security-Token der Firma yubico, der ein ereignisbasiertes Einmalpasswort ausgibt. Derzeit werden von Shibboleth nur diese Hardware-Keys unterstützt, zukünftig ggf. auch andere bekannte Marken wie Nitrokey.

Der YubiKey ist in verschiedenen Ausführungen mit unterschiedlichem Funktionsspektrum erhältlich. Mehr dazu finden Sie unter https://www.yubico.com/der-yubikey/?lang=de.

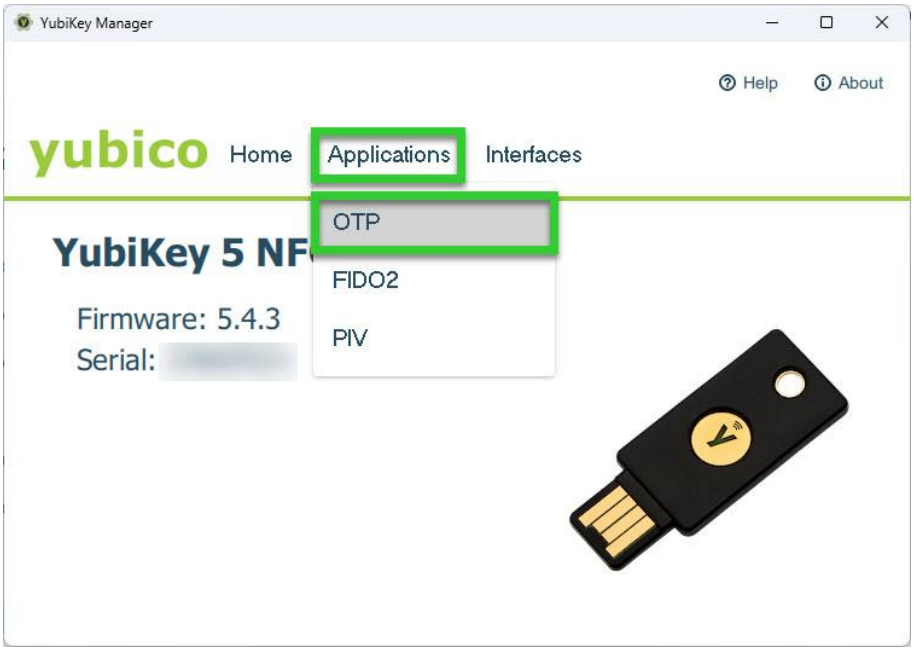
Konfiguration

1. Laden Sie sich unter https://www.yubico.com/support/download/yubikey-manager den *YubiKey Manager* für Ihr Betriebssystem herunter und installieren Sie ihn.

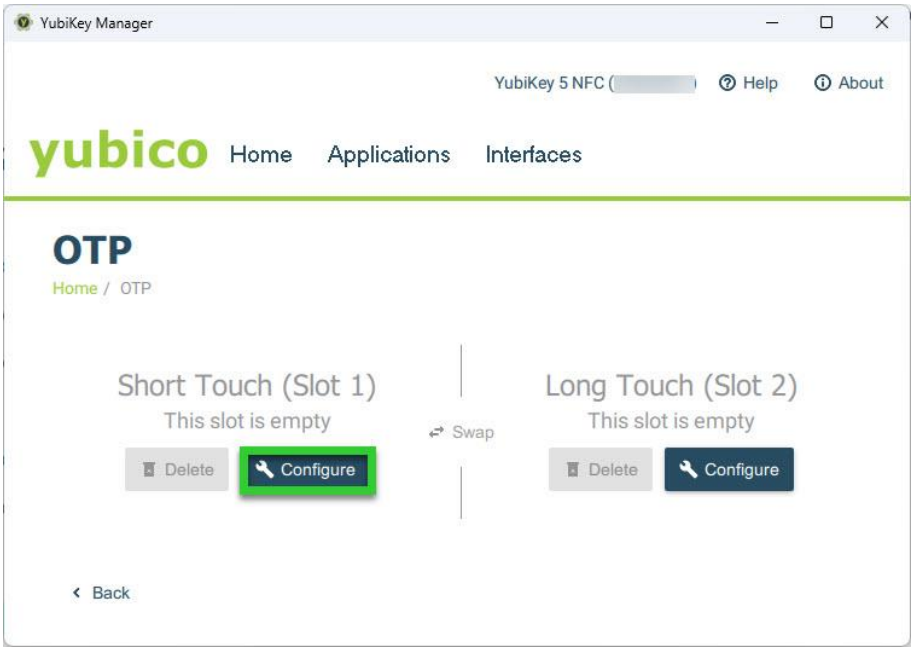
   Nach dem Start des Programms werden Sie ggf. aufgefordert, den YubiKey in einen freien USB-Port Ihres Gerätes einzustecken.



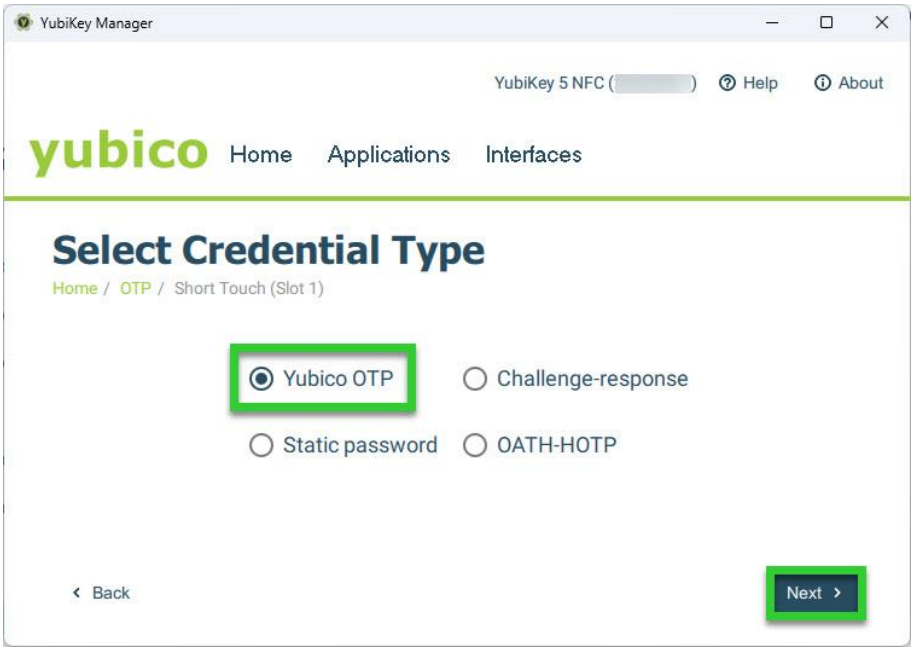
2. Klicken Sie im YubiKey Magager auf *„Applications“* > *„OTP“*



3. Wenn Sie einen YubiKey mit mehreren sog. *Slots* besitzen, klicken Sie bei einem unbenutzten Slot auf den Button *„Configure“*. Oder löschen Sie zuvor eine Konfiguration mit dem *„Delete“*-Button.
   Diese YubiKeys unterscheiden zwischen einem kurzen und einem langen Drücken des Knopfes und können so für zwei verschiedene Anwendungen genutzt werden.

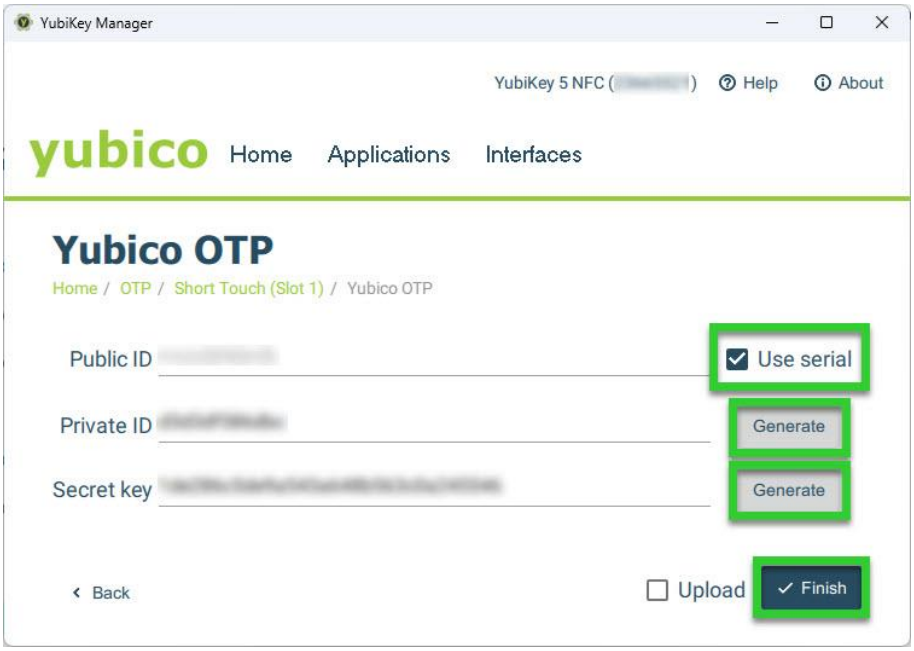


4. Wählen Sie *„Yubico OTP“* und klicken Sie auf *„Next“*.



5. Setzen Sie das Häkchen bei *„Use serial“* und klicken Sie auf beide *„Generate“*-Buttons.

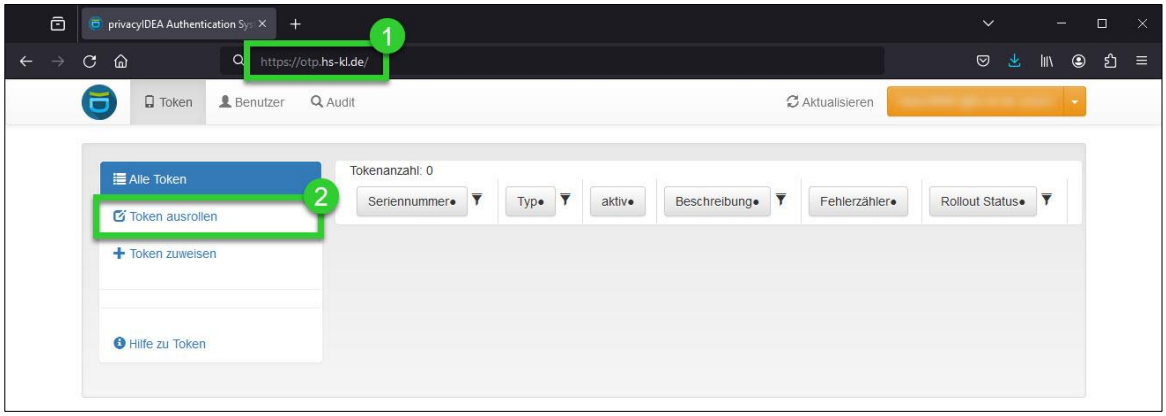
   Notieren oder kopieren Sie sich den 32-stelligen *„Secret key“* bevor Sie mit *„Finish“* das Fenster schließen oder lassen Sie das Fenster noch bis zur Einrichtung der Mehrfaktor-Authentifizierung geöffnet.



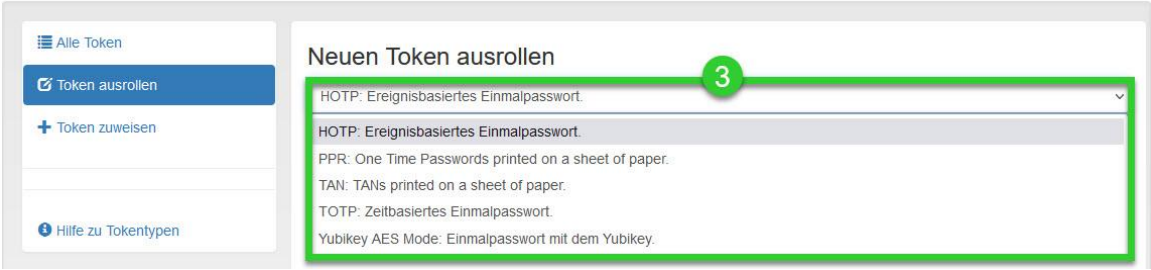
Mehrfaktor-Authentifizierung einrichten

1. Rufen Sie die Seite https://otp.hs-kl.de auf und melden Sie sich mit Ihrem HSKL-Login an. Diese Seite ist nur aus dem Hochschul-Netz bzw. per VPN-Verbindung erreichbar!

2. Klicken Sie auf *„Token ausrollen“*.



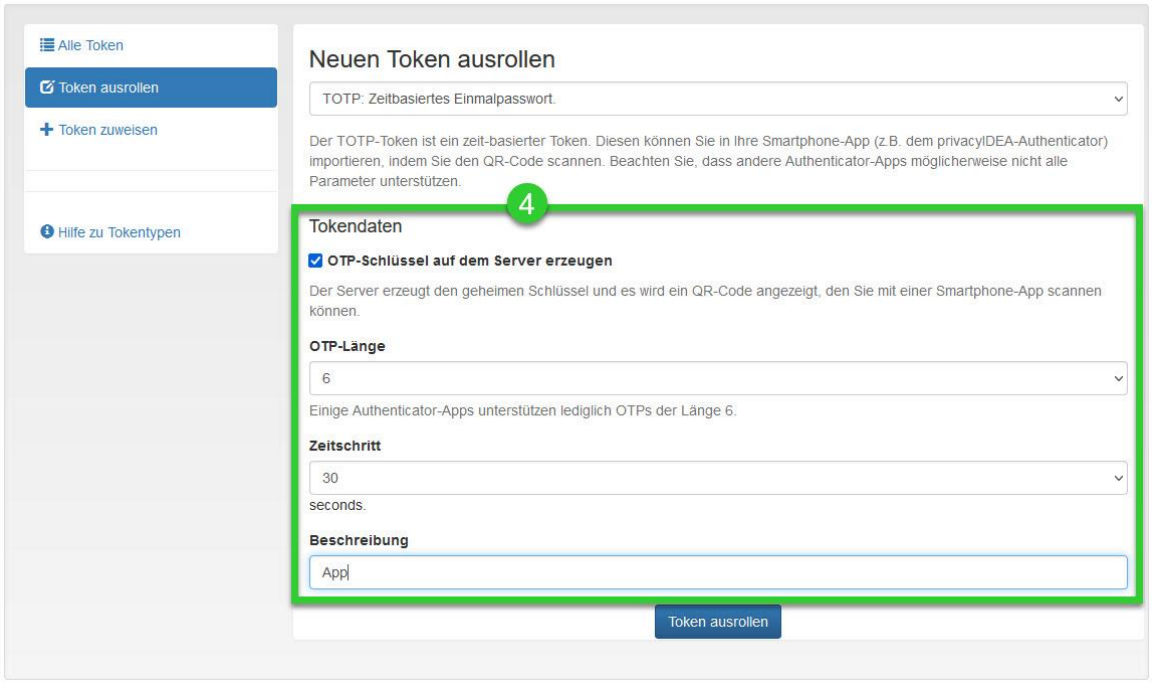
3. Wählen Sie eine Authentifizierungs-Methode aus (siehe Abschnitt „Authentifizierungs-Methoden“). Für jede Methode wird darunter eine kurze Beschreibung angezeigt.

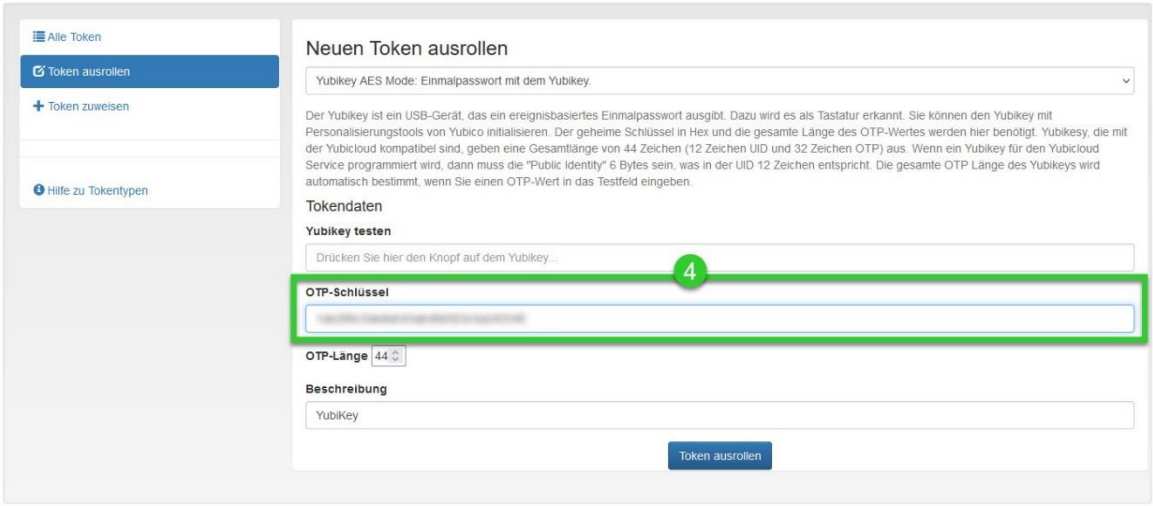


4. Passen Sie ggf. die Einstellungen an und tragen Sie zur Unterscheidung der verschiedenen Methoden eine kurze *„Beschreibung“* des Tokens ein. In den meisten Fällen können/sollten die Standardeinstellungen beibehalten werden.

   Bei der Verwendung der zeitbasierten Einmalpasswörter (TOTP) muss für die Apps von Google, Microsoft, Cisco und Twilio der *„Zeitschritt“* auf 30 Sekunden eingestellt werden.

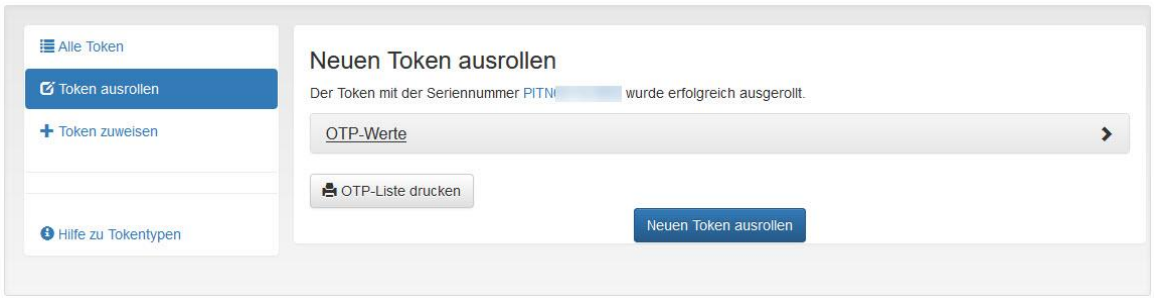
   Bei der Verwendung eines YubiKey müssen Sie den *„Secret key“* (siehe Abschnitt „Yubi Key einrichten“) in das Feld *„OTP-Schlüssel“* eintragen.



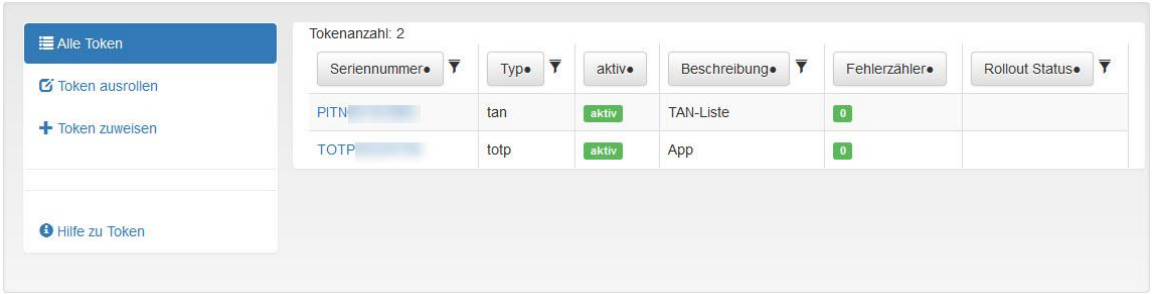


5. Klicken Sie auf *„Token ausrollen“*. Je nach gewählter Methode ist die Einrichtung abgeschlossen oder es wird Ihnen ein QR-Code, den Sie mit Ihrer Authentifikator-App scannen müssen, oder eine TAN-Liste (*„OTP-Werte“*), die Sie nun ausdrucken können, angezeigt.

   Wichtig: In allen Fällen kann diese Anzeige aus Sicherheitsgründen nicht noch einmal aufgerufen werden. Sie müssen also den QR-Code direkt scannen oder die Liste direkt ausdrucken! Andernfalls müssen Sie einen neuen Token ausrollen und ggf. den alten Token löschen.



6. Unter *„Alle Token“* finden Ihre bislang erstellten Token und können für jeden Token u.a. die Parameter einsehen, den Fehlerzähler zurücksetzen, den Token testen oder deaktivieren bzw wieder aktivieren.



Mehrfaktor-Authentifizierung nutzen

Nach der Einrichtung Ihrer MFA-Token, werden Sie bei jeder Shibboleth-Anmeldung (z.B. OpenOlat, BigBlueButton, Seafile, Panopto oder OWA) zuerst nach Ihrem Benutzernamen und HSKL-Passwort und anschließend nach dem zweiten Faktor, dem Code von einem Ihrer Token, gefragt. Haben Sie mehrere Token eingerichtet ist es egal, welchen Code Sie verwenden.

Bei der Verwendung des YubiKey wird der Code durch Drücken der *[Y]*-Taste auf dem Key automatisch in das Feld eingefügt. Bei allen anderen Methoden müssen Sie den Code selbst eingeben.