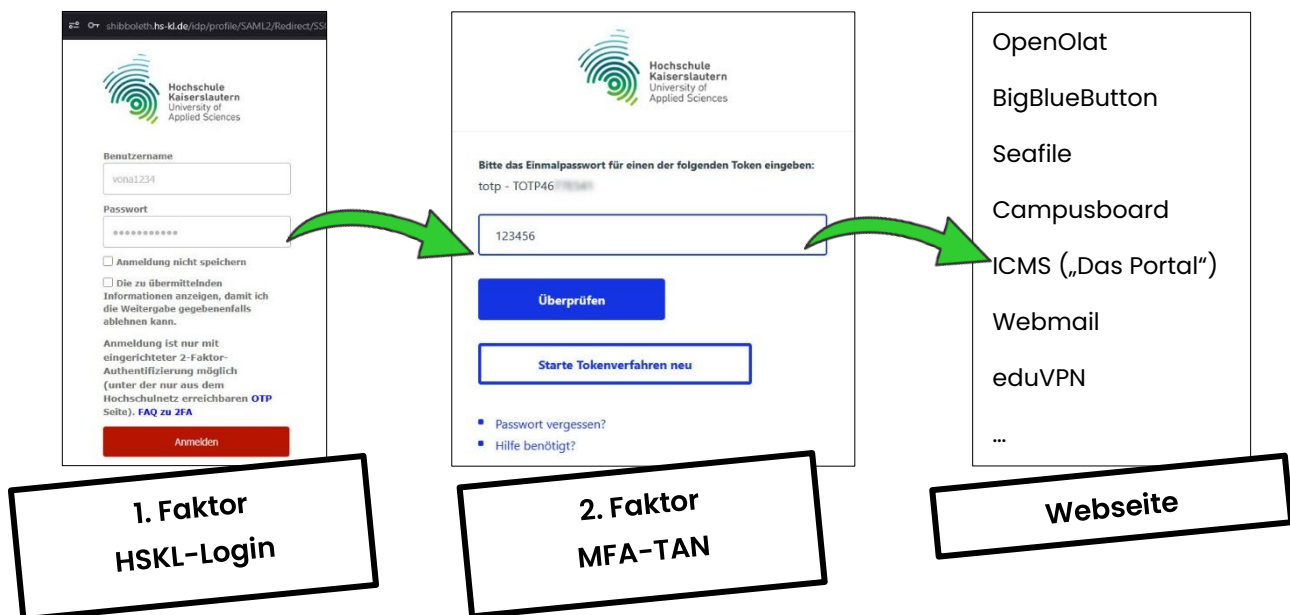


# Mehrfaktor-Authentifizierung (MFA)

Version 1.8, 18.06.2026

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

Mit einer solchen *Mehrfaktor-Authentifizierung (MFA)* ist es Fremden dann nicht mehr möglich, bei Bekanntwerden Ihrer Login-Daten (z.B. durch Schadsoftware oder Phishing-Mails) auf alle Ihre Daten zuzugreifen.



# Inhalt

1. Authentifizierungs-Methoden.....	3
1.1 Authentifikator-Apps (TOTP).....	4
1.2 TAN-Liste (PPR).....	5
1.3 YubiKey .....	5
2. Mehrfaktor-Authentifizierung einrichten oder konfigurieren.....	8
2.1 Sie sind mit dem Netzwerk der Hochschule verbunden.....	9
2.2 Sie sind mit nicht dem Netzwerk der Hochschule verbunden.....	12
2.3 Diagramm: MFA einrichten oder ändern.....	16
3. Mehrfaktor-Authentifizierung nutzen.....	17

# 1. Authentifizierungs-Methoden

Es werden drei Authentifizierungs-Methoden unterstützt:

- **TOTP: TAN 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!**

→ siehe Abschnitt „[Authentifikator-Apps](#)“

- **PPR: TAN-Liste mit Index**

Bei dieser Methode wird eine nummerierte TAN-Liste erzeugt. Zur Anmeldung muss die TAN mit der passenden Nummer eingegeben werden.

→ siehe Abschnitt „[TAN-Liste](#)“

- **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!**

→ siehe Abschnitt „[YubiKey](#)“



Wir empfehlen sehr, **mindestens zwei verschiedene Authentifizierungs-Methoden einzurichten**, falls eine Methode nicht verfügbar ist oder nicht funktioniert.

**Insbesondere wenn Sie keine Möglichkeit haben, sich im Hochschulnetz vor Ort anzumelden**, da der VPN-Zugang über eduVPN auch mit einem zweiten Faktor gesichert ist.

So ist beispielsweise eine ausgedruckte TAN-Liste oder der YubiKey am Schlüsselbund eine gute Alternative wenn das Smartphone gerade nicht zur Hand, defekt oder leer ist.



Bei einem neuen Smartphone oder nach dem Zurücksetzen des Smartphones muss die Authentifizierung mittels App neu eingerichtet werden. Auch für diesen Fall ist eine „Backup-TAN-Liste“ sehr sinnvoll.

## 1.1 Authentifikator-Apps (TOTP)

Für die TOTP-Methode 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.

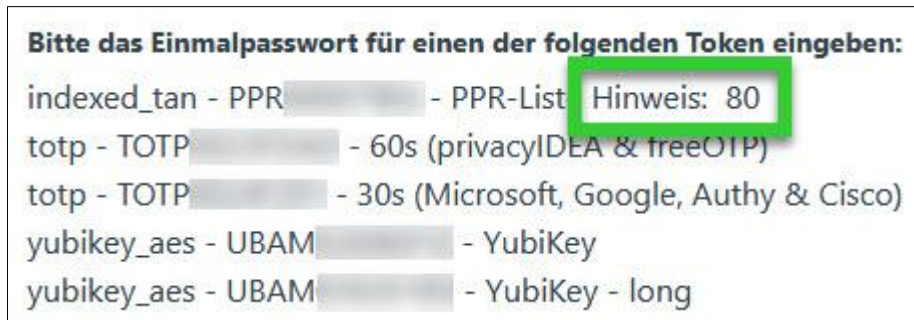
Im Folgenden haben wir Ihnen eine Auswahl an verbreiteten Authentifikator-Apps zusammengestellt, die wir selbst ausprobiert haben und die sowohl für Android- als auch für iOS-Geräte erhältlich sind.

- **privacyIDEA Authenticator (*unsere Empfehlung!*)**  
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**
  - [Google Play Store](#)
  - [Apple App Store](#)
  
- **Cisco Duo Mobile**
  - [Google Play Store](#)
  - [Apple App Store](#)
  
- **FreeOTP**
  - [Google Play Store](#)
  - [Apple App Store](#)

## 1.2 TAN-Liste (PPR)

Eine gedruckte Liste mit 100 Einmalpasswörtern (TANs). Zur Anmeldung muss die TAN mit der passenden Nummer („Hinweis: xy“) eingegeben werden.

Beispiel: In diesem Fall muss zur Anmeldung die Nummer 80 der Liste eingegeben werden.



Verwahren Sie die Liste an einem sicheren Ort auf und denken Sie bitte rechtzeitig daran, eine neue Liste zu erstellen, bevor alle 100 TANs verwendet wurden.

## 1.3 YubiKey

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.

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

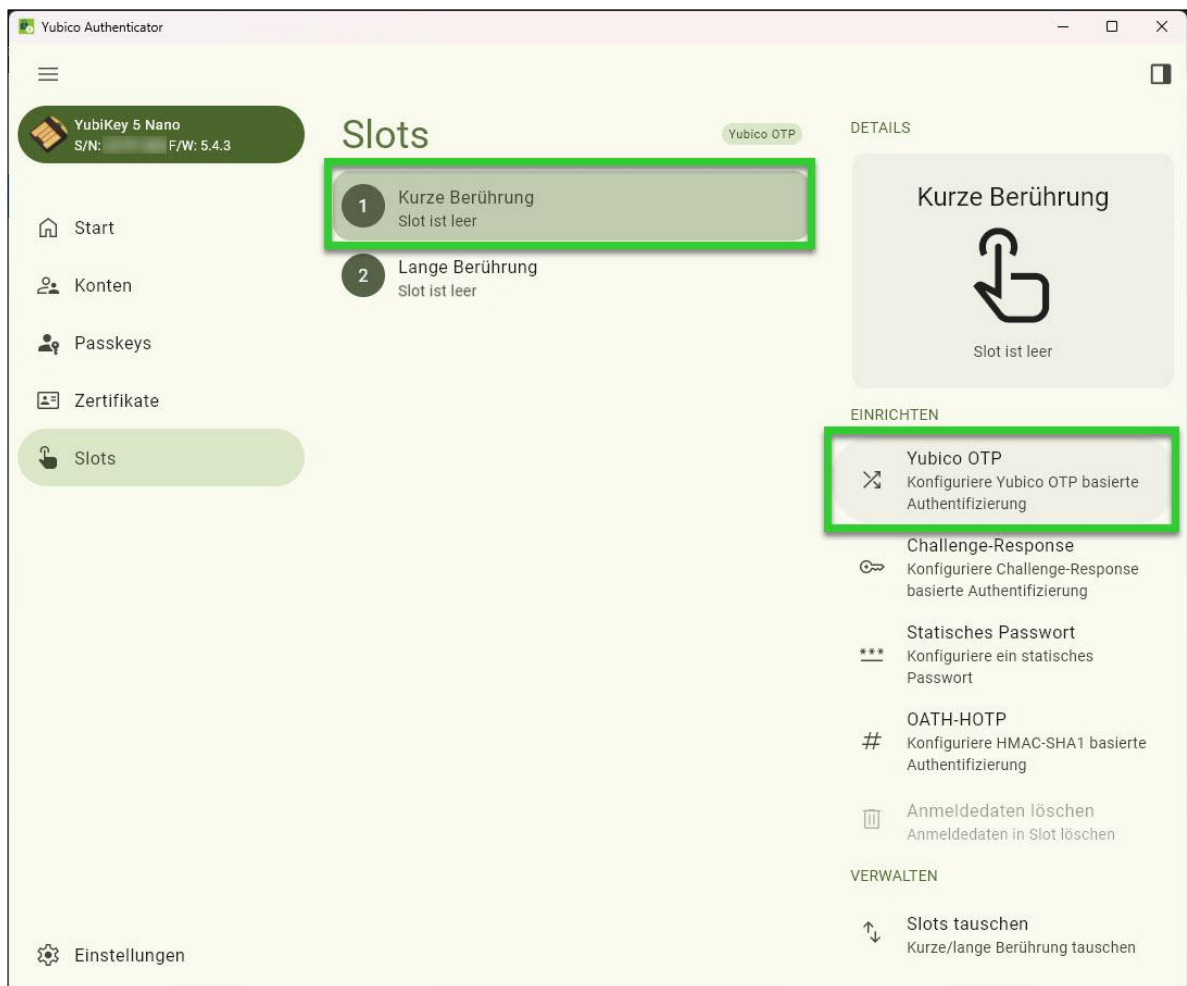


Bildquelle: <https://www.yubico.com>

## Konfiguration

1. Laden Sie sich unter <https://www.yubico.com/products/yubico-authenticator> das Programm *Yubico Authenticator* für Ihr Betriebssystem herunter und installieren Sie es.
2. Stecken Sie den YubiKey in einen freien USB-Port Ihres Gerätes und starten Sie das Programm.
3. Viele YubiKeys können mit zwei verschiedenen Login-Verfahren, sog. *Slots*, konfiguriert werden. So kann man den YubiKey auch für andere Anwendungen verwenden. Durch ein kurzes Drücken des [Y]-Knopfes auf dem Key wird der erste Slot benutzt, durch langes Drücken (ca. 2 Sekunden) der zweite Slot.

Wählen Sie einen leeren Slot aus und klicken Sie auf „Yubico OTP“ auf der rechten Seite.



4. Klicken Sie auf die drei Buttons am rechten Rand der drei Eingabefelder. Lassen Sie die restlichen Einstellungen unverändert.

Yubico OTP

Öffentliche ID  0/12

Private ID  0/12

Schlüssel  0/32

anhängen Keine Datei für den E...

Exportierte Anmeldedaten können auf [upload.yubico.com](http://upload.yubico.com) hochgeladen werden

Abbrechen Speichern

5. Notieren oder kopieren Sie sich den 32-stelligen „Schlüssel“. Dieser wird bei der Einrichtung der Mehrfaktor-Authentifizierung benötigt.

Klicken Sie anschließend auf „Speichern“.

Yubico OTP

Öffentliche ID  12/12

Private ID  12/12

Schlüssel  0/32

anhängen Keine Datei für den E...

Exportierte Anmeldedaten können auf [upload.yubico.com](http://upload.yubico.com) hochgeladen werden

Abbrechen Speichern

6. Jetzt ist der YubiKey fertig konfiguriert, muss aber vor der Verwendung noch auf der OTP-Seite eingebunden werden (→ siehe Abschnitt „[Mehrfaktor-Authentifizierung einrichten oder konfigurieren](#)“).

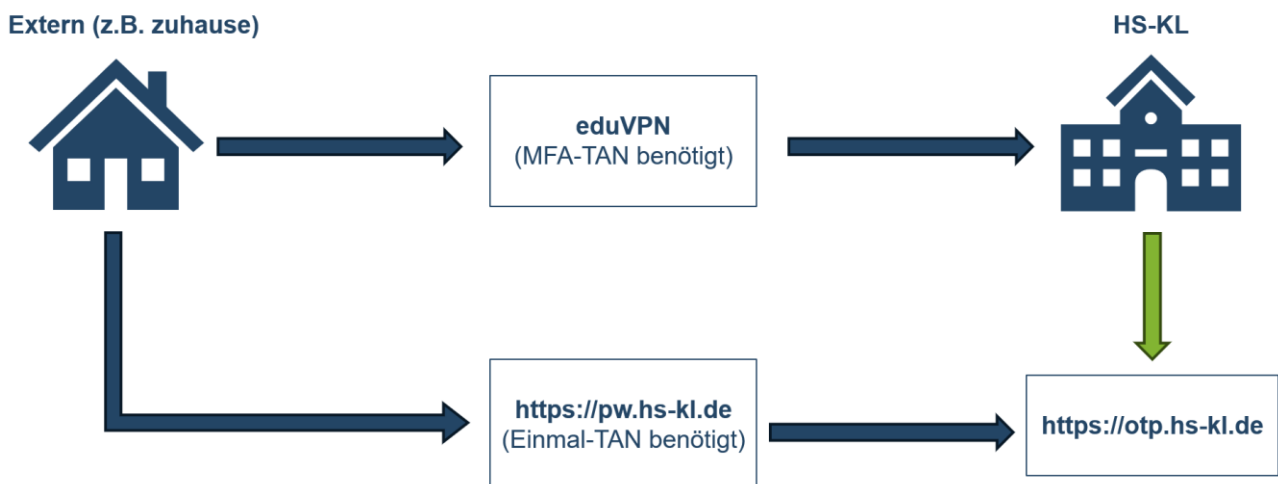
## 2. Mehrfaktor-Authentifizierung einrichten oder konfigurieren

Die Einrichtung bzw. Konfiguration der Mehrfaktor-Authentifizierung erfolgt über die Seite

<https://otp.hs-kl.de>.

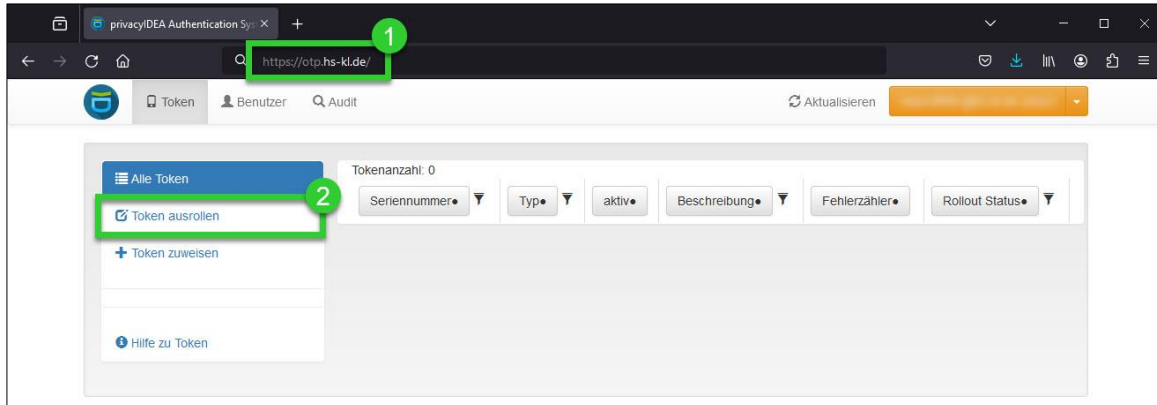
Diese Seite ist auf drei Wegen erreichbar:

1. Direkt aus Netzwerk der Hochschule (LAN oder WLAN am Campus vor Ort).
2. Indirekt über eine VPN-Verbindung mit dem Hochschulnetzwerk über eduVPN. Hier ist jedoch ein gültiger MFA-TAN nötig. Informationen und Anleitungen zu eduVPN finden Sie unter <https://www.hs-kl.de/hochschule/servicestellen/rechenzentrum/dienste/vpn>
3. Wenn Sie **nicht** mit dem Netzwerk der Hochschule verbunden sind, benötigen Sie eine sog. *Einmal-TAN*. Wie Sie diesen erhalten wird im [Abschnitt 2.2](#) beschrieben.

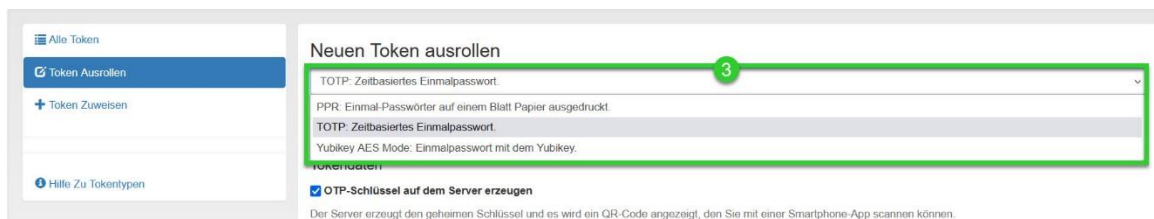


## 2.1 Sie sind mit dem Netzwerk der Hochschule verbunden

1. Rufen Sie die Seite <https://otp.hs-kl.de> auf und melden Sie sich mit Ihrem HSKL-Login an.
2. Klicken Sie auf „Token ausrollen“.



3. Wählen Sie die gewünschte Authentifizierungs-Methode aus (→ siehe Abschnitt „[Authentifizierungs-Methoden](#)“). Für jede Methode wird nach der Auswahl darunter eine kurze Beschreibung angezeigt.



4. Passen Sie ggf. die Einstellungen an:
  - Bei der Verwendung der App „*privacyIDEA Authenticator*“ (TOTP-Verfahren) können Sie bei „*Zeitschritt*“ den Wert „*60 Sekunden*“ verwenden. Behalten Sie bei allen anderen Apps die Standardeinstellung bei.
  - Bei der Verwendung eines YubiKey müssen Sie nun den kopierten „*Schlüssel*“ (→ siehe Abschnitt „[Yubi Key](#)“) in das Feld „*OTP-Schlüssel*“ eintragen.
  - Tragen Sie zur Unterscheidung der verschiedenen Methoden eine kurze „*Beschreibung*“ des Tokens ein (optional).
  - Lassen Sie alle anderen Werte unverändert.

Alle Token

Token ausrollen

Token zuweisen

Hilfe zu Tokentypen

### Neuen Token ausrollen

TOTP: Zeitbasiertes Einmalpasswort

Der TOTP-Token ist ein zeit-basierter Token. Diesen können Sie in Ihre Smartphone-App (z.B. dem privacyIDEA-Authenticator) importieren, indem Sie den QR-Code scannen. Beachten Sie, dass andere Authenticator-Apps möglicherweise nicht alle Parameter unterstützen.

**Tokendaten**

OTP-Schlüssel auf dem Server erzeugen

Der Server erzeugt den geheimen Schlüssel und es wird ein QR-Code angezeigt, den Sie mit einer Smartphone-App scannen können.

**OTP-Länge**

6

Einige Authenticator-Apps unterstützen lediglich OTPs der Länge 6.

**Zeitschritt**

30

seconds.

**Beschreibung**

App

Token ausrollen

Alle Token

Token ausrollen

Token zuweisen

Hilfe zu Tokentypen

### Neuen Token ausrollen

Yubikey AES Mode: Einmalpasswort mit dem Yubikey

Der Yubikey ist ein USB-Gerät, das ein ereignisbasiertes Einmalpasswort ausgibt. Dazu wird es als Tastatur erkannt. Sie können den Yubikey mit Personalisierungstools von Yubico initialisieren. Der geheime Schlüssel in Hex und die gesamte Länge des OTP-Wertes werden hier benötigt. Yubikeys, die mit der Yubicloud kompatibel sind, geben eine Gesamtlänge von 44 Zeichen (12 Zeichen UID und 32 Zeichen OTP) aus. Wenn ein Yubikey für den Yubicloud Service programmiert wird, dann muss die "Public Identity" 6 Bytes sein, was in der UID 12 Zeichen entspricht. Die gesamte OTP Länge des Yubikeys wird automatisch bestimmt, wenn Sie einen OTP-Wert in das Testfeld eingeben.

**Tokendaten**

**Yubikey testen**

Drücken Sie hier den Knopf auf dem Yubikey...

**OTP-Schlüssel**

**OTP-Länge** 44

**Beschreibung**

YubiKey

Token ausrollen

- Klicken Sie auf „Token ausrollen“. Je nach gewählter Methode ist die Einrichtung abgeschlossen oder es wird Ihnen ein QR-Code, den Sie mit Ihrer Authenticator-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.

Alle Token

Token ausrollen

Token zuweisen

Hilfe zu Tokentypen

### Neuen Token ausrollen

Der Token mit der Seriennummer TOTP wurde erfolgreich ausgerollt.

Klicken Sie [hier](#) oder scannen Sie den QR-Code, um den Token in Ihrer Smartphone-App hinzuzufügen.

Der QR-Code enthält den geheimen Schlüssel für Ihren Token. Diesen müssen Sie schützen. **Wenn jemand anderes diesen QR-Code gesehen haben könnte, erzeugen Sie den QR-Code bitte neu, wenn kein anderer zusieht.**

[QR-Code neu erzeugen](#)

[Neuen Token ausrollen](#)

Alle Token

Token ausrollen

Token zuweisen

Hilfe zu Tokentypen

### Neuen Token ausrollen

Der Token mit der Seriennummer PITN wurde erfolgreich ausgerollt.

OTP-Werte >

[OTP-Liste drucken](#)

[Neuen Token ausrollen](#)

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.

Alle Token

Token ausrollen

Token zuweisen

Hilfe zu Token

Tokenanzahl: 2

Seriennummer	Typ	aktiv	Beschreibung	Fehlerzähler	Rollout Status
PITN	tan	aktiv	TAN-Liste	0	
TOTP	totp	aktiv	App	0	

## 2.2 Sie sind mit nicht dem Netzwerk der Hochschule verbunden

Für den Fall, dass Sie sich nicht mit dem Hochschulnetzwerk verbinden können (z.B. Fernstudierende, Lehrbeauftragte oder bei einem Auslandsaufenthalt) gibt es auch eine Lösung.

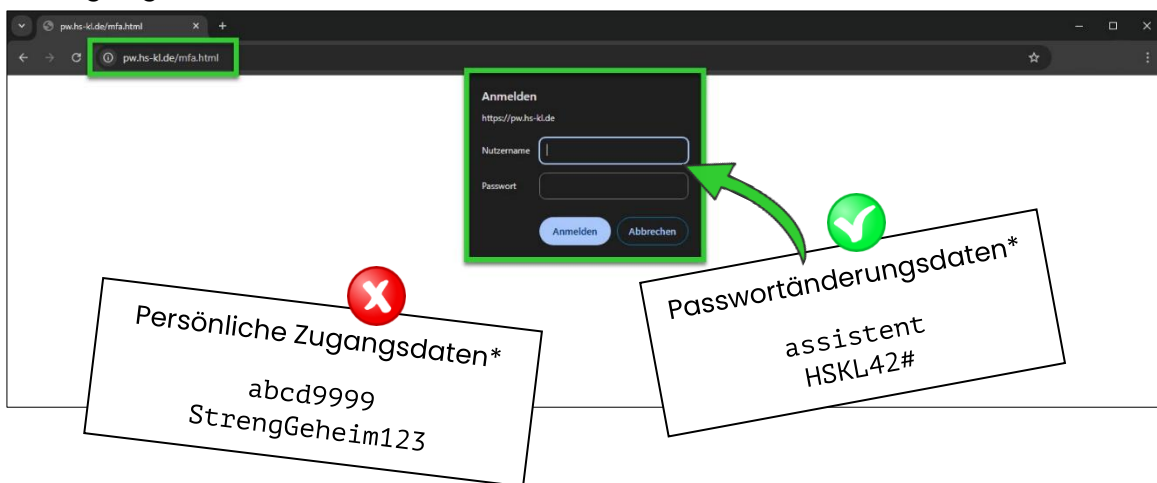
Dazu benötigen Sie:

- eine sog. **Einmal-TAN** (ein 24-stelliger Code)
- die **Zugangsdaten zum Ändern des Passworts** (das sind nicht Ihre persönlichen Zugangsdaten)

Diese Daten erhalten Sie entweder zu Beginn zusammen mit Ihren persönlichen Zugangsdaten oder alternativ bei den Servicestellen des Rechenzentrums und den EDV-Beauftragten Ihres Fachbereichs\*. In diesem Fall ist es jedoch notwendig, **Ihre Identität in einem Video-Meeting sicherzustellen**. Sonst könnte jemand, der sich für Sie ausgibt, sehr großen Schaden anrichten.

\*: <https://www.hs-kl.de/hochschule/servicestellen/rechenzentrum/support>

1. Rufen Sie die Seite <https://pw.hs-kl.de/mfa.html> auf und melden Sie sich mit den Zugangsdaten zum Ändern des Passworts an.



\*: Das sind natürlich Beispiele, keine echten Zugangsdaten ;-)

2. Lesen Sie sich den Text durch und klicken Sie anschließend auf den Button „Gelesen und verstanden → Zum Formular“.

**Mehrfaktor-Authentifizierung einrichten** ([-- go to english version](#))

**Hinweise:**

Die Mehrfaktor-Authentifizierung ist für viele, v.a. außerhalb der Hochschule zugängliche Netzwerk-Dienste, zwingend erforderlich, d.h. neben Login/Passwort wird ein zusätzlicher persönlicher Zugangs-Code (sog. "Token") benötigt. Eine Anleitung zur Einrichtung finden Sie unter [→ https://hs-kl.de/digital](https://hs-kl.de/digital) im Abschnitt "MFA".

Der Server zur Einrichtung und Verwaltung von MFA, [→ https://otp.hs-kl.de](https://otp.hs-kl.de), ist grundsätzlich **nur innerhalb des Hochschulnetzes** erreichbar.

Auf dieser Seite können Sie mit Hilfe eines **zeitbegrenzt gültigen Initial-Tokens**, das Sie ggf. bei der Einrichtung Ihrer Nutzerkennung, oder auf Anfrage mit Identifikation bei den Servicestellen des Rechenzentrums erhalten haben, die Mehrfaktor-Authentifizierung auch von außerhalb des Hochschulnetzes einrichten. Hierzu müssen Sie sich auf der folgenden Seite mit Login/Passwort und anschließend Eingabe des 24-stelligen Initialtokens anmelden.

Allgemeine Fragen zum Thema IT-Sicherheit richten Sie bitte an [informationssicherheit@hs-kl.de](mailto:informationssicherheit@hs-kl.de), Fragen zum Thema Datenschutz richten Sie bitte an [datenschutz@hs-kl.de](mailto:datenschutz@hs-kl.de).

**Gelesen und verstanden → Zum Formular**

3. Geben Sie Ihre persönlichen Zugangsdaten ein und klicken Sie auf „Anmelden“.

Benutzername  
abcd1234

Passwort  
abcd9999

**Persönliche Zugangsdaten\***  
abcd9999  
StrengGeheim123

Anmelden

4. Geben Sie nun den 24-stelligen Einmaltoken ein und klicken Sie auf „Überprüfen“.  
Hinweis: Der Einmal-TAN funktioniert nur auf dieser Seite!

Code eingeben

shibboleth.hs-kl.de/idp/profile/SAML2/Redirect/SSO?execution=e1s3

Hochschule Kaiserslautern  
University of Applied Sciences

Bitte das Einmalpasswort für einen der folgenden Token eingeben:  
registration\_code - REG004742F6  
registration\_code - REG0048678B

Überprüfen

Starte Tokenverfahren neu

Passwort vergessen?  
Hilfe benötigt?

© Hochschule Kaiserslautern 2025 (U1)

5. Bestätigen Sie die Übermittlung der Daten mit dem Button „Akzeptieren“.

Informationsweitergabe

shibboleth.hs-kl.de/idp/profile/SAML2/Redirect/SSO?execution=e1s4

Hochschule Kaiserslautern  
University of Applied Sciences

Sie sind dabei auf diesen Dienst zuzugreifen:  
pw.hs-kl.de

An den Dienst zu übermittelnde Informationen	
Targeted ID (pseudonyme Kennung)	s9+rd+UoD/9HD8UL0fGqz2ewBM-@hs-kl.de
Berechtigung	urn:mace:dir:entitlement:common-lib-terms
Persönliche ID	mas:9999@hs-kl.de
Zugehörigkeit	student@hs-kl.de member@hs-kl.de
E-Mail	mas:9999@stud.hs-kl.de
Organisationsname	Hochschule Kaiserslautern
Nachname	mas:9999
userPrincipalName	mas:9999@stud.hs-kl.de

Die oben aufgeführten Informationen werden an den Dienst weitergegeben, falls Sie fortfahren. Sind Sie einverstanden, dass diese Informationen bei jedem Zugriff auf diesen Dienst an ihn weitergegeben werden?

Wählen Sie die Dauer, für die Ihre Entscheidung zur Informationsweitergabe gültig sein soll:

Bei nächster Anmeldung erneut fragen.

- Ich bin einverstanden, meine Informationen dieses Mal zu senden.

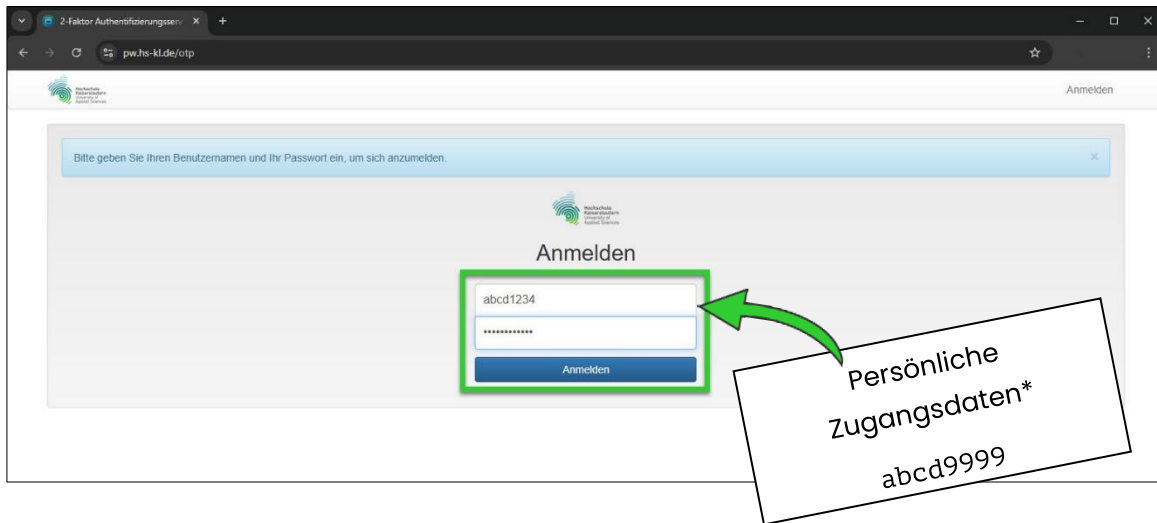
Erneut fragen, wenn sich die Informationen ändern, welche diesem Dienst weitergegeben werden.

- Ich bin einverstanden, dass dieselben Informationen in Zukunft automatisch an diesen Dienst weitergegeben werden.

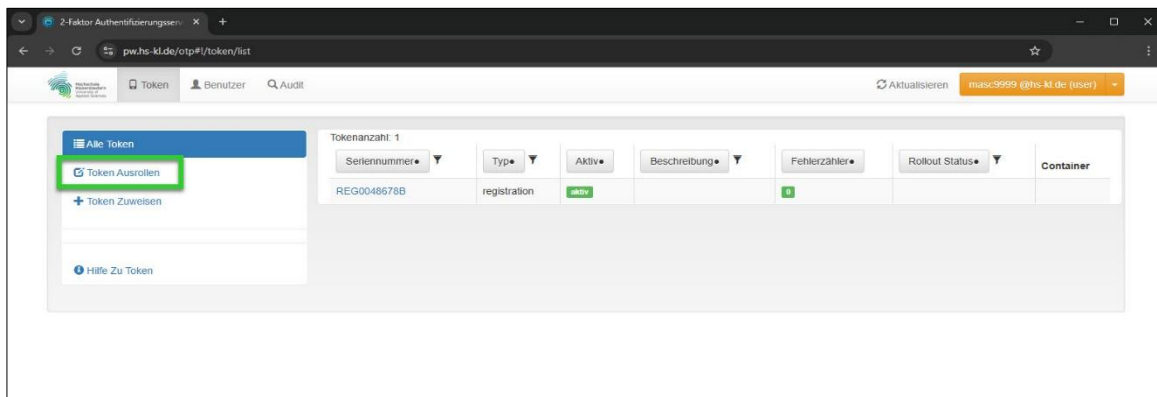
Diese Einstellung kann jederzeit mit der Checkbox auf der Anmeldeseite widerrufen werden.

Ablehnen Akzeptieren

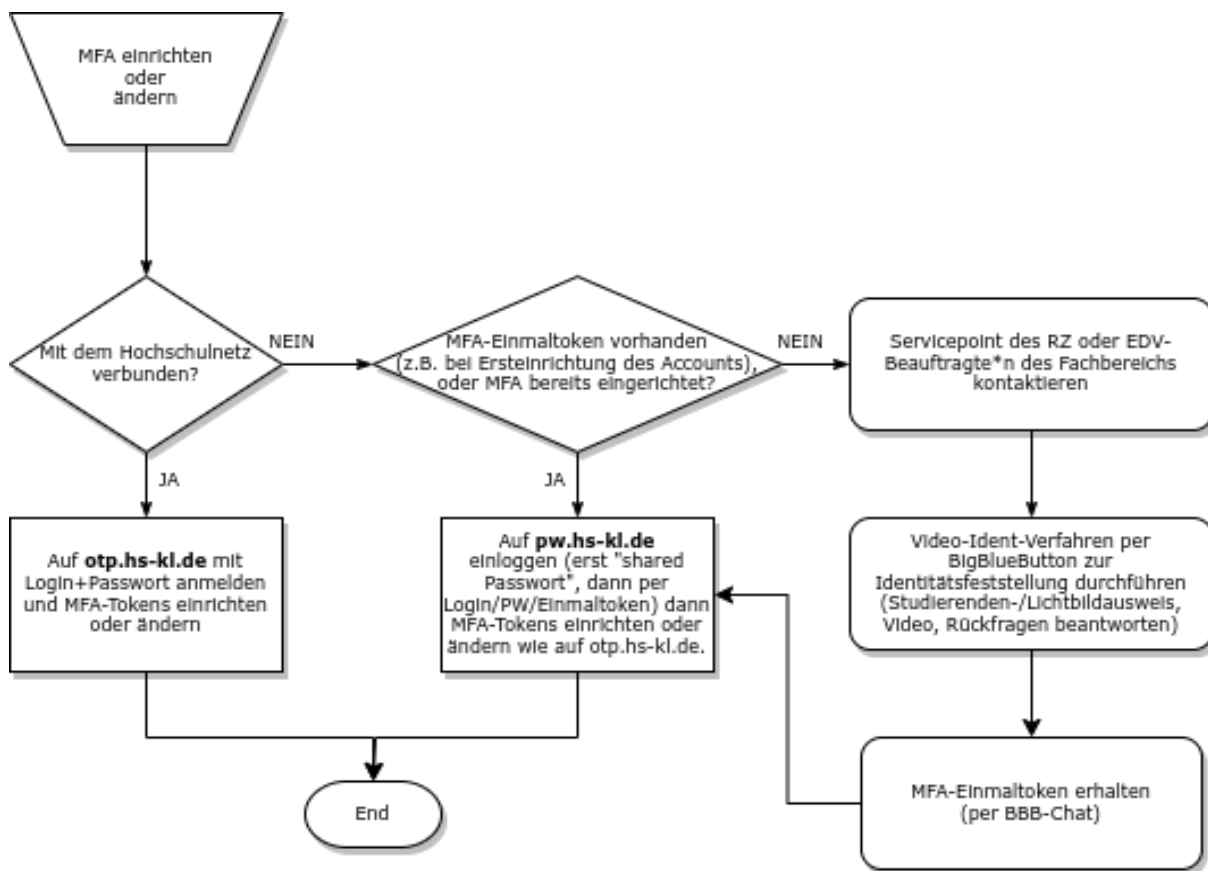
6. Geben Sie auch auf dieser Seite Ihre persönlichen Zugangsdaten ein und klicken Sie auf „Anmelden“.



7. Jetzt können Sie die Mehrfaktor-Authentifizierung wie in [Abschnitt 2.1](#) beschrieben einrichten bzw. bereits existierende MFA-Methoden bearbeiten.



## 2.3 Diagramm: MFA einrichten oder ändern



### 3. Mehrfaktor-Authentifizierung nutzen

Nach der Einrichtung Ihrer MFA-Token, werden Sie bei jeder Shibboleth-Anmeldung (z.B. OpenOlat, BigBlueButton, eduVPN, Campusboard, Seafire, 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.

The image illustrates the two-step login process for MFA. The first step (marked with a green '1') is the initial login form at Hochschule Kaiserslautern, where the user enters their username and password. The second step (marked with a green '2') is the Landesnetz Rheinland-Pfalz authentication page, where the user enters a one-time token code (e.g., 123456) and clicks 'Überprüfen' to complete the login.