

Multifactor authentication (MFA)

Version 1.8, 17.06.2026

To log in to online services such as OpenOlat, BigBlueButton, eduVPN, Seafile, Panopto or OWA (all services with authentication via *Shibboleth*), you need not only your HSKL login (username and password) but also an additional authentication factor for these services.

With such a *multifactor authentication (MFA)*, it is no longer possible for strangers to access all your data if your login credentials are compromised (e.g., through malware or phishing emails).

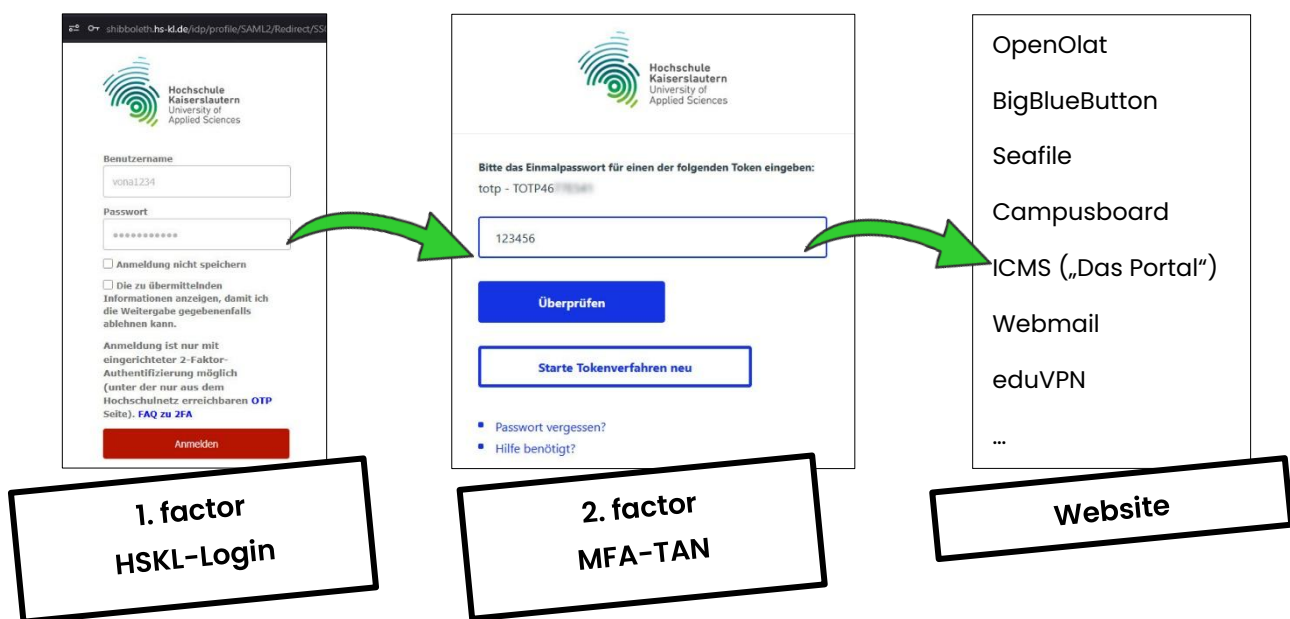


Table of contents

1. Authentication methods	3
1.1 Authenticator apps (TOTP)	4
1.2 TAN list (PPR).....	5
1.3 YubiKey	5
2. Set up or configure multifactor authentication	8
2.1 You are connected to the university's network	9
2.2 You are not connected to the university's network	12
2.3 Diagram: Setting up or changing the MFA.....	16
3. Mehrfaktor-Authentifizierung nutzen	17

1. Authentication methods

Three authentication methods are currently supported:

- **TOTP: TAN password with time limit**

With this method, a code is generated that changes every 30 or 60 seconds. To log in, you must enter the current code.

An authenticator app is required for this method!

→ see section '[Authenticator apps](#)'

- **PPR: TAN list with index**

With this method, a numbered TAN list is generated. To log in, you must enter the TAN with the corresponding number.

→ see section '[TAN list](#)'

- **YubiKey**

This method uses a USB hardware key. To log in, you must press a button on the YubiKey, which is plugged into an available USB port on your device.

Special hardware is required for this method!

→ see section '[YubiKey](#)'



We highly recommend **setting up at least two different authentication methods** in case one method is not available or does not work. **Especially if you do not have the option of logging into the university network on site**, as VPN access via eduVPN is also secured with a second factor.

For example, a printed TAN list or the YubiKey on your key ring is a good alternative if your smartphone is not at hand or is not charged.



When you get a new smartphone or after resetting your smartphone, you'll need to set up authentication via the app again. A "backup TAN list" is very useful in this situation as well.

1.1 Authenticator apps (TOTP)

An authenticator app is required for the TOTP method. There is a whole range of such apps and the multi-factor authentication we use should work with most of them.

Below we have listed a selection of popular authenticator apps that we have tried ourselves and that are available for both Android and iOS devices.

- **privacyIDEA Authenticator (*our recommendation!*)**
The authenticator app from the provider of our MFA system.
 - [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](#)

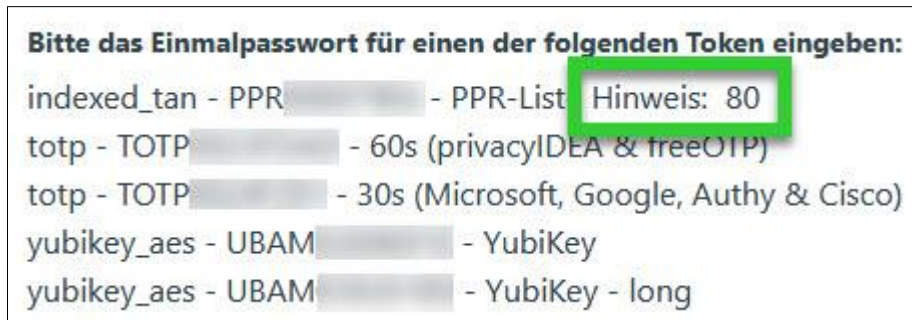
- **Cisco Duo Mobile**
 - [Google Play Store](#)
 - [Apple App Store](#)

- **FreeOTP**
 - [Google Play Store](#)
 - [Apple App Store](#)

1.2 TAN list (PPR)

A printed list of 100 one-time passwords (TANs). To log in, you must enter the TAN with the corresponding number („Hinweis: xy“).

Example: In this case, you must enter number 80 from the list to log in.



Keep the list in a safe place, and please remember to create a new list in plenty of time before all 100 TANs have been used.

1.3 YubiKey

The YubiKey is a security token from Yubico that generates an event-based one-time password. Currently, Shibboleth supports only these hardware keys; other well-known brands may be supported in the future.

The YubiKey is available in various versions with a different range of functions. You can find out more at <https://www.yubico.com/products>.

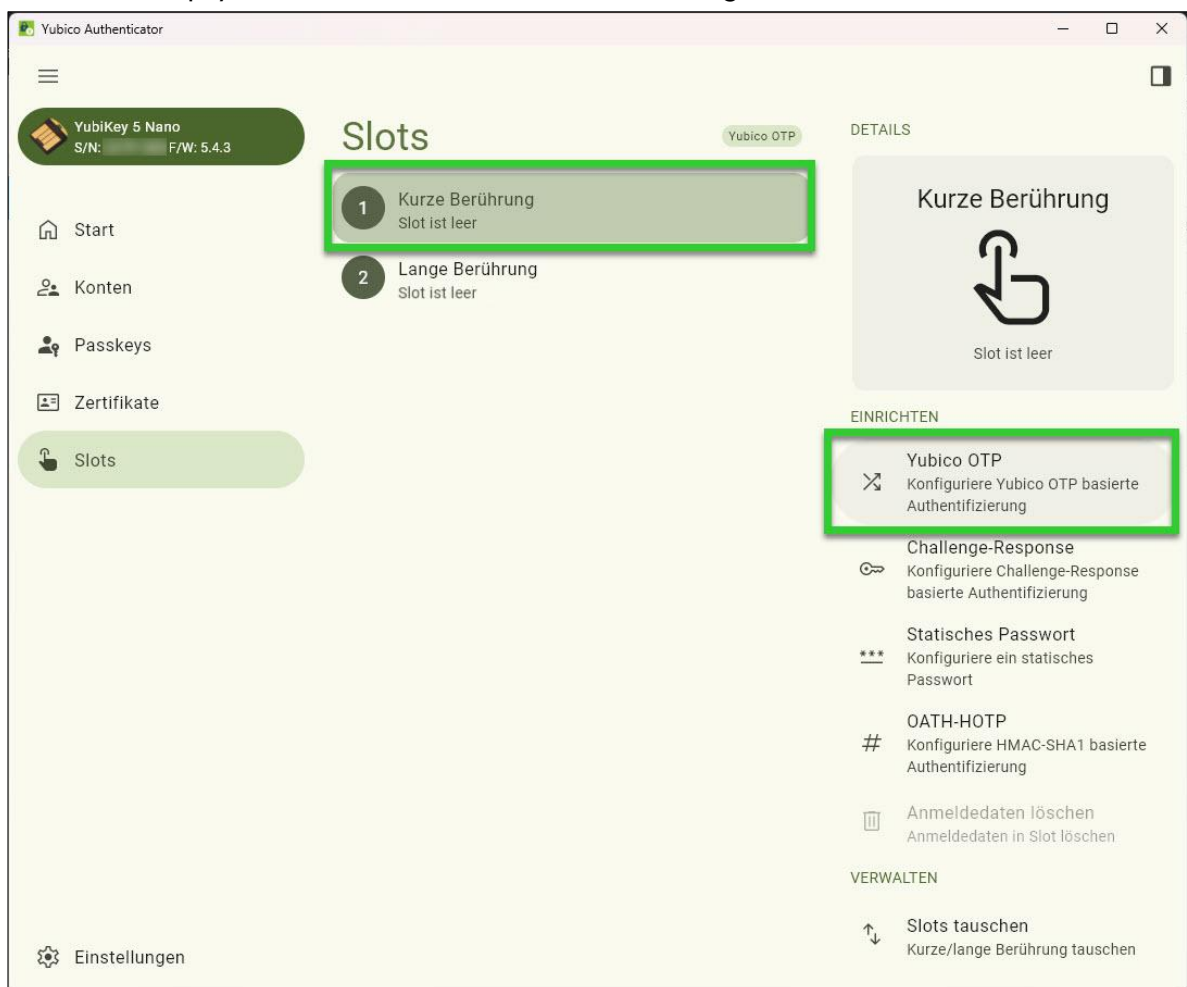


Image source: <https://www.yubico.com>

Konfiguration

1. Go to <https://www.yubico.com/products/yubico-authenticator> to download and install *Yubico Authenticator* for your operating system.
2. Plug the YubiKey into an available USB port on your device and launch the program.
3. Many YubiKeys can be configured with two different login methods, known as "slots". This allows you to use the YubiKey for other applications as well. Pressing the [Y] button on the key briefly activates the first slot, while pressing and holding it (for about 2 seconds) activates the second slot.

Select an empty slot and click „Yubico OTP“ on the right-hand side.



4. Click the three buttons on the right side of the three input fields. Leave the remaining settings unchanged.

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 hochgeladen werden

Abbrechen Speichern

5. Note down or copy the 32-digit „Schlüssel“ (or „Key“). You'll need this when setting up multi-factor authentication.

Then click „Speichern“ (or „Save“).

Yubico OTP

Öffentliche ID 12/12

Private ID 12/12

Schlüssel 32/32

anhängen Keine Datei für den E...

Exportierte Anmeldedaten können auf upload.yubico.com hochgeladen werden

Abbrechen Speichern

6. The YubiKey is now fully configured, but it must still be integrated on the OTP page before it can be used (→ see section [“Set up or configure multifactor authentication”](#)).

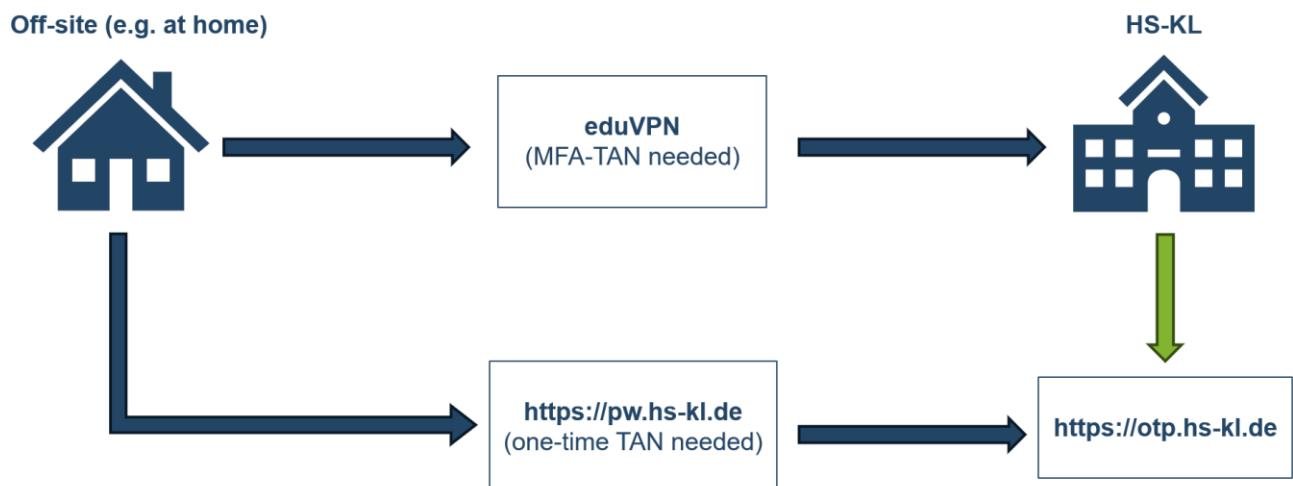
2. Set up or configure multifactor authentication

Multifactor authentication is set up and configured via the page

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

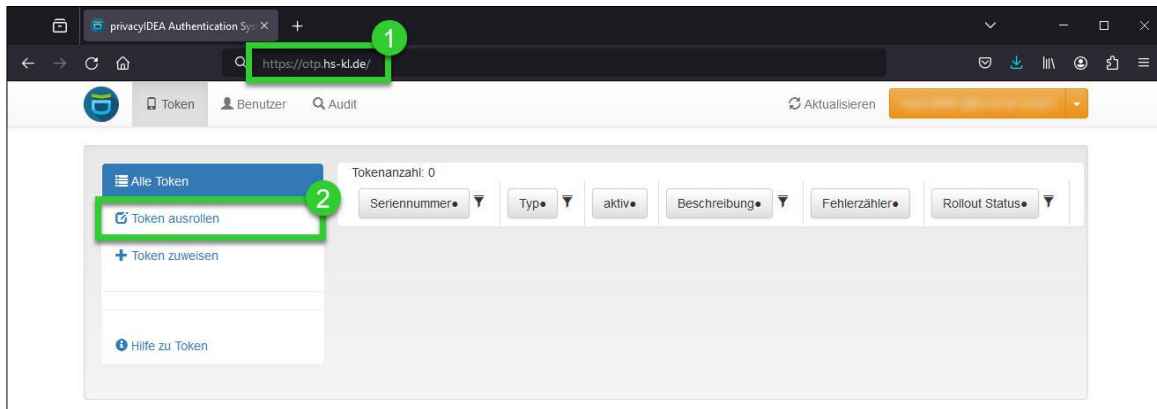
There are three ways to access this page:

1. Directly from the university network (LAN or Wi-Fi on campus).
2. Indirectly via a VPN connection to the university network using eduVPN. But a valid MFA-TAN is required for this. Information and instructions on eduVPN can be found at <https://www.hs-kl.de/hochschule/servicestellen/rechenzentrum/dienste/vpn>.
3. If you are **not** connected to the university's network, you will need a so-called *one-time TAN*. [Section 2.2](#) explains how to obtain one.

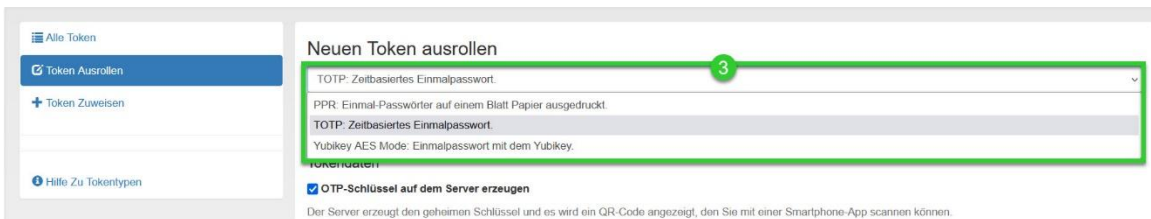


2.1 You are connected to the university's network

1. Go to <https://otp.hs-kl.de> and log in with your HSKL login.
2. Click on „Token ausrollen“.



3. Select an authentication method (→ see section '[Authentication methods](#)'). A short description is displayed below for each method.



4. Adjust the settings as needed:
 - When using the „privacyIDEA Authenticator“ app (TOTP method), you can set „Zeitschritt“ to „60 Sekunden“ verwenden. For all other apps, keep the default setting.
 - When using a YubiKey, you must enter the copied „Schlüssel“/„Key“ (→ see section „[Yubi Key](#)“) in the field „OTP-Schlüssel“.
 - To distinguish between the different methods, enter a short description of the token at „Beschreibung“ (optional).
 - Leave all other values unchanged.

☰ Alle Token

☑ Token ausrollen

+ Token zuweisen

📖 Hilfe zu Tokentypen

Neuen Token ausrollen

Der Token mit der Seriennummer TOTP [redacted] 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 [redacted] wurde erfolgreich ausgerollt.

OTP-Werte >

[🖨️ OTP-Liste drucken](#)

[Neuen Token ausrollen](#)

6. At „Alle Token“ you will find the tokens you have created so far and you can review the parameters for each token, reset the error counter, test the token or deactivate or reactivate it.

☰ Alle Token

☑ Token ausrollen

+ Token zuweisen

📖 Hilfe zu Token

Tokenanzahl: 2

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

2.2 You are not connected to the university's network

In case you are unable to connect to the university's network (e.g. distance learning students, lecturers or during a stay abroad), there is also a solution.

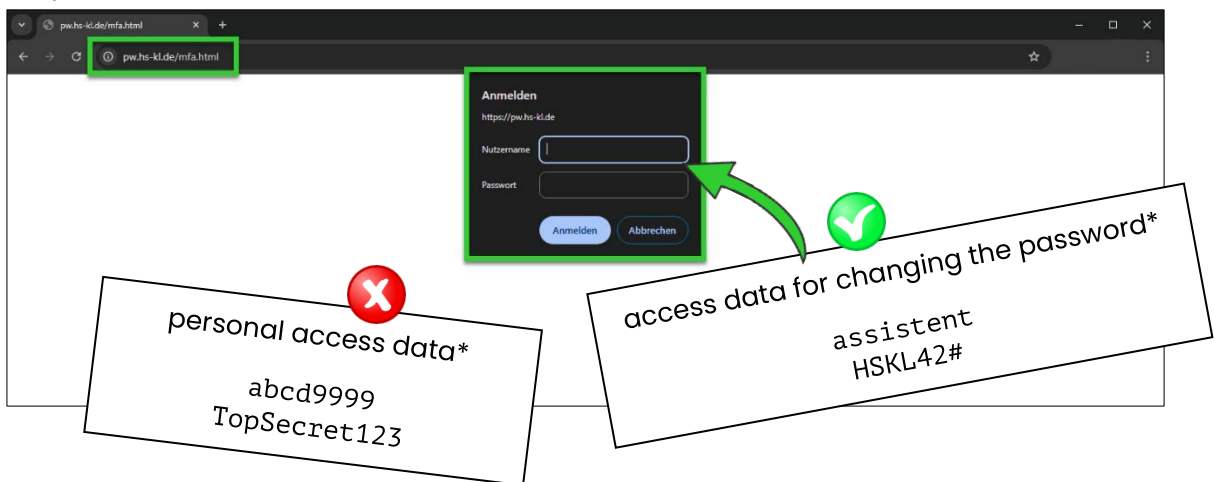
You will need:

- a so-called **one-time TAN** (a 24-digit code)
- the **access data for changing the password** (these are not your personal access data)

You will receive these data either at the beginning together with your personal access data or alternatively at the service points of the computer center and the IT representatives of your department*. In this case it is **necessary to verify your identity in a video meeting**. Otherwise, someone pretending to be you could cause a great deal of damage.

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

1. Go to <https://pw.hs-kl.de/mfa.html> and log in with the access data for changing the password.



*: These are of course examples, not real access data ;-)

2. Read the text and then click on the 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> im Abschnitt "MFA".

Der Server zur Einrichtung und Verwaltung von MFA, → <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, Fragen zum Thema Datenschutz richten Sie bitte an datenschutz@hs-kl.de.

Gelesen und verstanden → Zum Formular

3. Enter your personal access data and click on „Anmelden“.

Hochschule
Kaiserlautern
University of
Applied Sciences

Benutzername
abcd1234

Passwort
abcd9999

Anmeldung nicht speichern

Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

Anmeldung ist nur mit eingerichteter 2-Faktor-Authentifizierung möglich (unter der nur aus dem Hochschulnetz erreichbaren **OTP** Seite). [FAQ zu 2FA](#)

Anmelden

personal access data*
abcd9999
TopSecret123

4. Now enter the 24-digit one-time token and click on „Überprüfen“.
Note: The one-time TAN only works on this page!

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) | [Impressum](#) | [HochschuleKaiserslautern.de](#)

5. Confirm the transmission of your data with the 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.

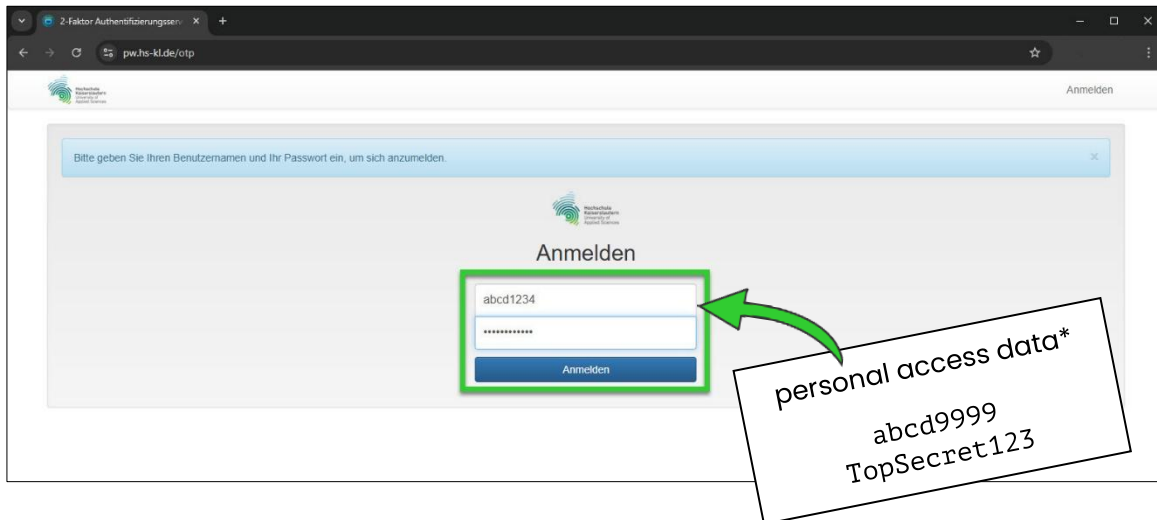
Erneut fragen, wenn sich die Informationen ändern, welche diesem Dienst weitergegeben werden.

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

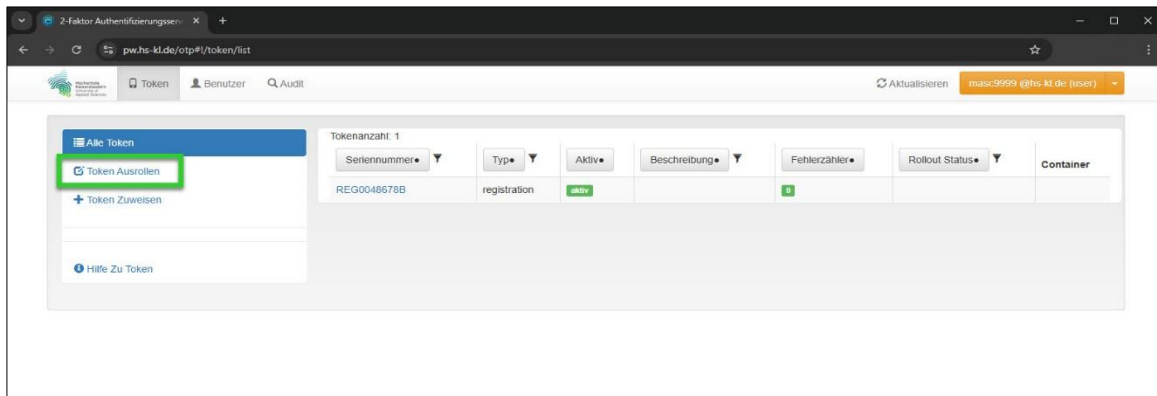
Diese Einstellung kann jederzeit mit der Checkbox auf der Anmeldeseite widerrufen werden.

Ablehnen Akzeptieren

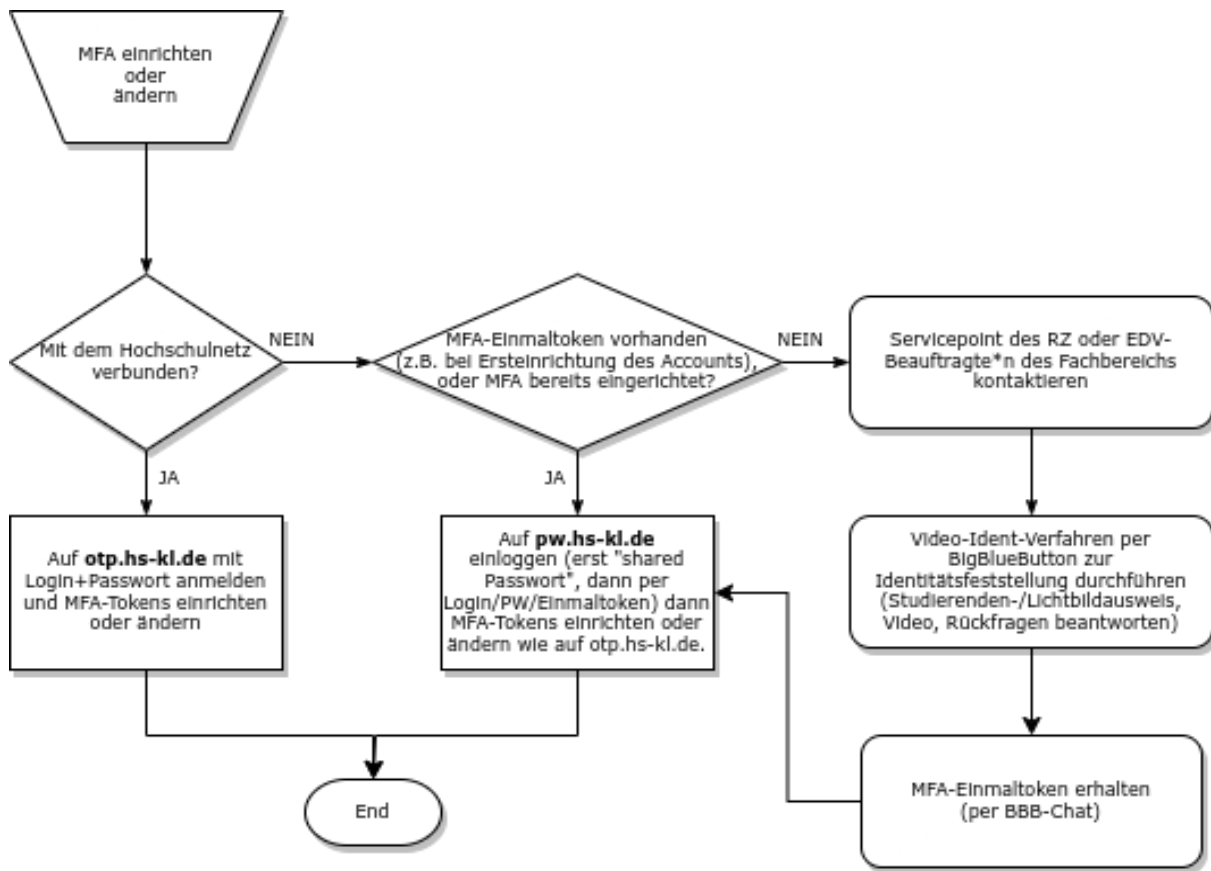
6. Enter your personal access data on this page as well and click on „Anmelden“.



7. You can now set up multifactor authentication as described in [section 2.1](#) or edit existing MFA methods.



2.3 Diagram: Setting up or changing the MFA



3. Mehrfaktor-Authentifizierung nutzen

After setting up your MFA tokens, you will first be asked for your user name and HSKL password and then for the second factor (the code of one of your tokens) each time you log in to Shibboleth (e.g. OpenOlat, BigBlueButton, eduVPN, Campusboard, Seafiler, Panopto or OWA). **If you have set up several tokens, it does not matter which code you use.**

When using the YubiKey, the code is automatically inserted into the field by pressing the [Y] button on the key. For all other methods, you must enter the code yourself.

Hochschule
Kaiserslautern
University of
Applied Sciences

Anmelden bei OpenOlat

Benutzername

Passwort

Anmeldung nicht speichern

Die zu übermittelnden
Informationen anzeigen, damit ich
die Weitergabe gegebenenfalls
ablehnen kann.

Anmelden

Hochschule
Kaiserslautern
University of
Applied Sciences

Anmelden bei Landesnetz Rheinland-Pfalz

Universitäten und Hochschulen von
Rheinland-Pfalz

Das Landesnetz Rheinland-Pfalz stellt verschiedene Dienste Zentral für die Universitäten und
Hochschulen von Rheinland-Pfalz bereit.

Bitte das Einmalpasswort für einen der folgenden Token eingeben:

tan - PITN0015C98D - TAN-Liste
totp - TOTP0022A759 - App

123456

Überprüfen

Starte Tokenverfahren neu

- Passwort vergessen?
- Hilfe benötigt?