Hochschule Kaiserslautern
University of Applied Sciences
Kompetenzzentrum Digitalisierung & Medien

Multifactor authentication (MFA)

Version 1.5, 25.08.2024

To log in to online services such as OpenOlat, BigBlueButton, Seafile, Panopto or OWA (all services with authentication via Shibboleth), you now need an additional factor for authentication with these services in addition to your user name and password.

With such a *multifactor authentication (MFA)*, it is no longer possible for strangers to access all your data if they gain knowledge of your password.

Authentication methods

Five authentication methods are currently supported:

- **HOTP: One-time password without time limit**
  This method generates a code that does not change automatically. If the code has been used once, a new code must be generated.
  An authenticator app is required for this method!

- **TOTP: One-time password with time limit**
  This method generates a code that changes every 30 or 60 seconds. The current code must always be used to log in.
  An authenticator app is required for this method!

- **PPR: TAN list with index**
  This method generates an indexed TAN list. Each TAN is assigned a sequential number. To log in, the TAN with the matching number must be entered.

- **TAN-Liste (ohne Index)**
  This method generates a TAN list. Any TAN from the list can be entered to log in. Such a TAN can only be used once and must then be crossed out in the list.

- **YubiKey**
  This method uses a hardware USB key. To log in, press a button on the YubiKey, which is plugged into a free USB port on your device.
  Special hardware is required for this method!

Recommendations

- We recommend using several of these authentication methods in parallel if one method is not available or does not work. 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.

- We recommend printing out TAN lists and not saving them on the device.

Authenticator apps

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

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

- **privacyIDEA Authenticator**
  The authenticator app from the manufacturer of our MFA procedure.
  - Google Play Store
  - Apple App Store

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

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

- **Twilio Authy**
  Also available as a desktop app for Windows, Mac and Linux. Registration with telephone number and e-mail address is required.
  - Google Play Store
  - Apple App Store
  - Desktop-App

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

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

Set up YubiKey

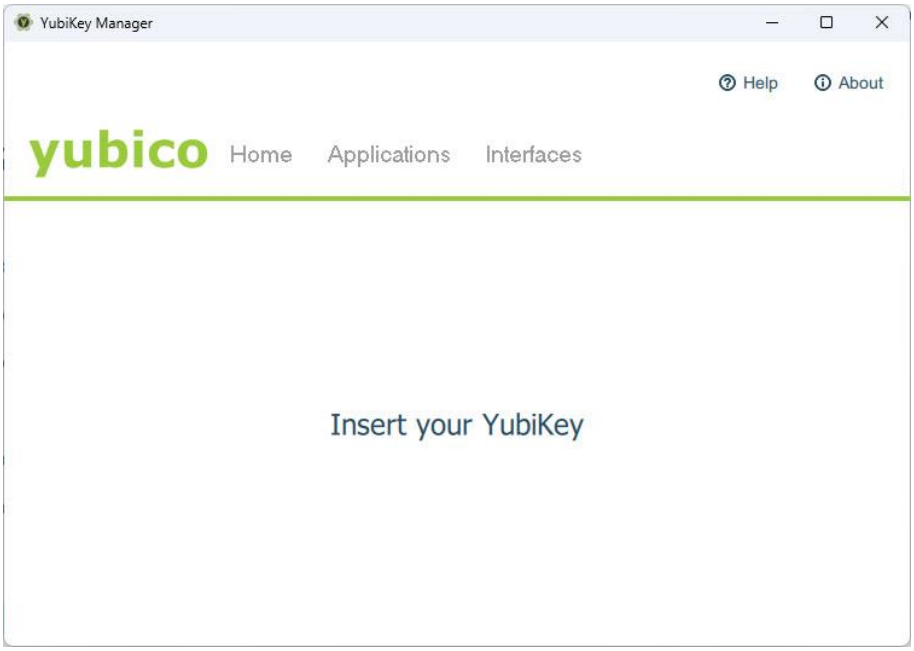
The YubiKey is a security token from the company yubico, which issues an event-based one-time password. Shibboleth currently only supports these hardware keys, but other well-known brands such as Nitrokey may also be supported in the future.

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

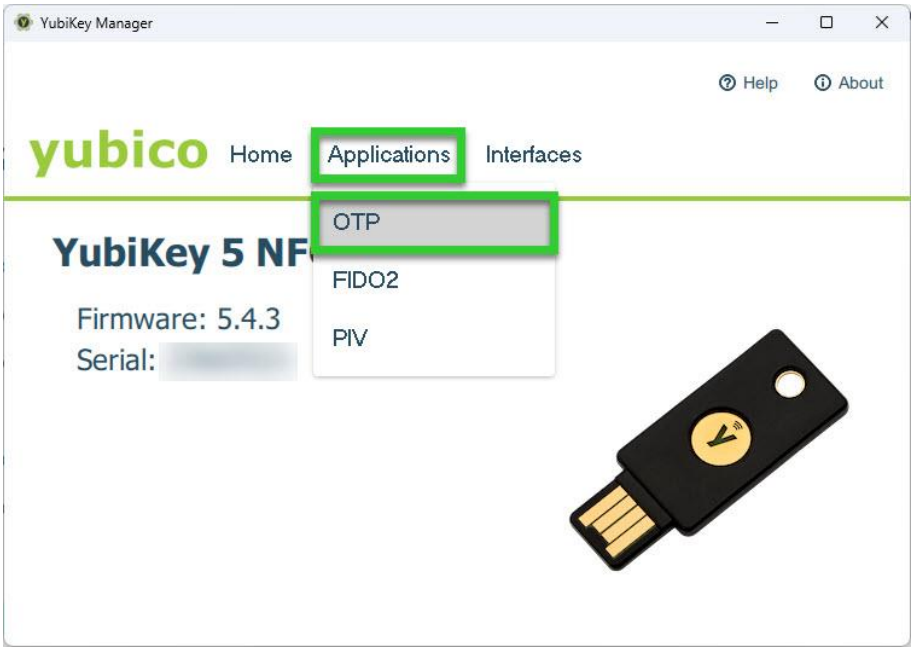
Configuration

1. Download and install the *YubiKey Manager* for your operating system from https://www.yubico.com/support/download/yubikey-manager.

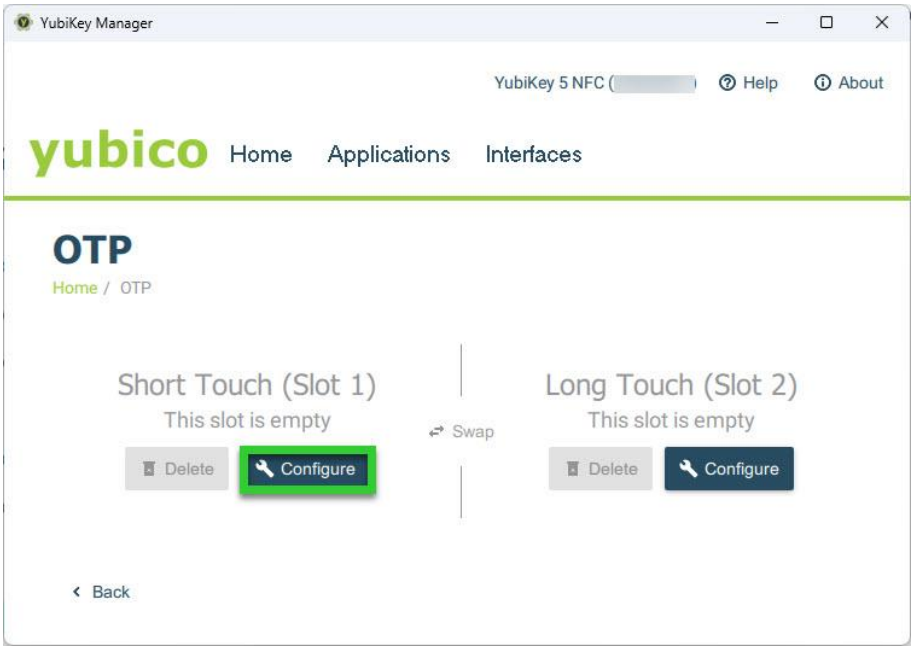
   After starting the programme, you may be asked to insert the YubiKey into a free USB port on your device.



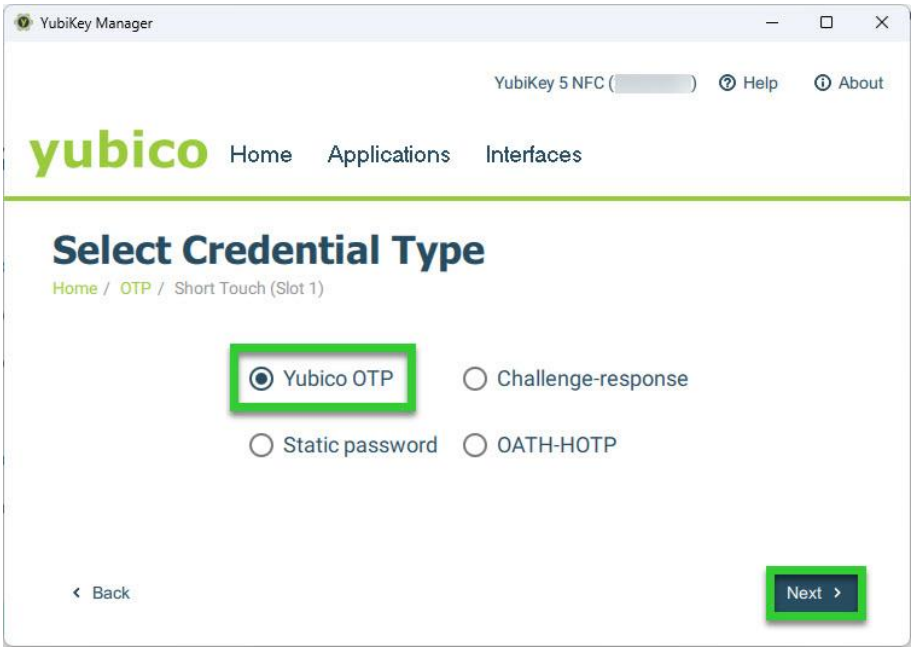
2. Click on *„Applications“* > *„OTP“* in the YubiKey Manager.



3. If you have a YubiKey with several slots, click on *„Configure“* at an unused slot or delete a configuration first with the *„Delete“* button.
   These YubiKeys distinguish between a short and a long press of the button and can therefore be used for two different applications.

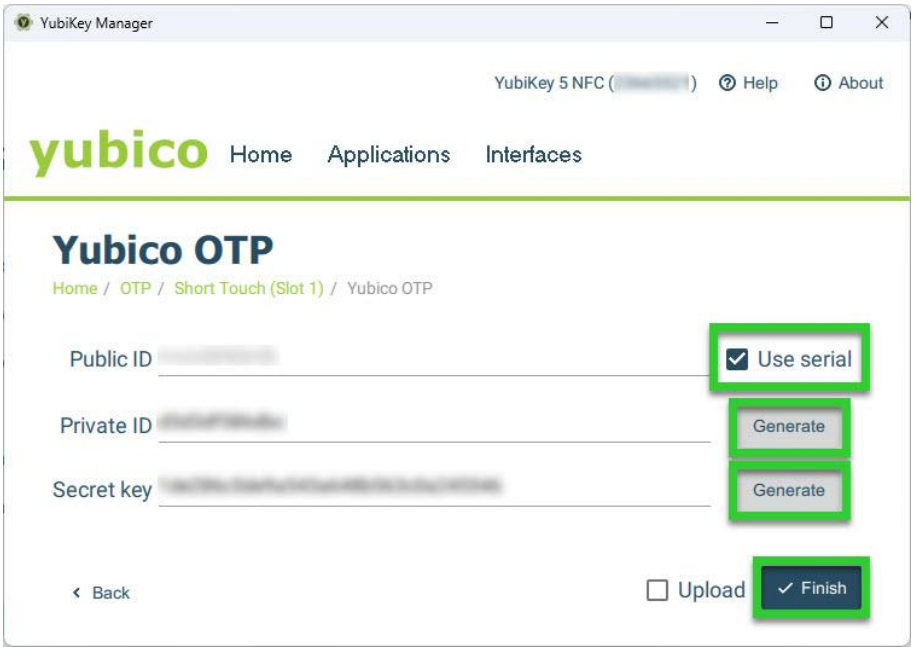


4. Select *„Yubico OTP“* and click on *„Next“*.



5. Tick the *„Use serial“* box and click on both *„Generate“* buttons.

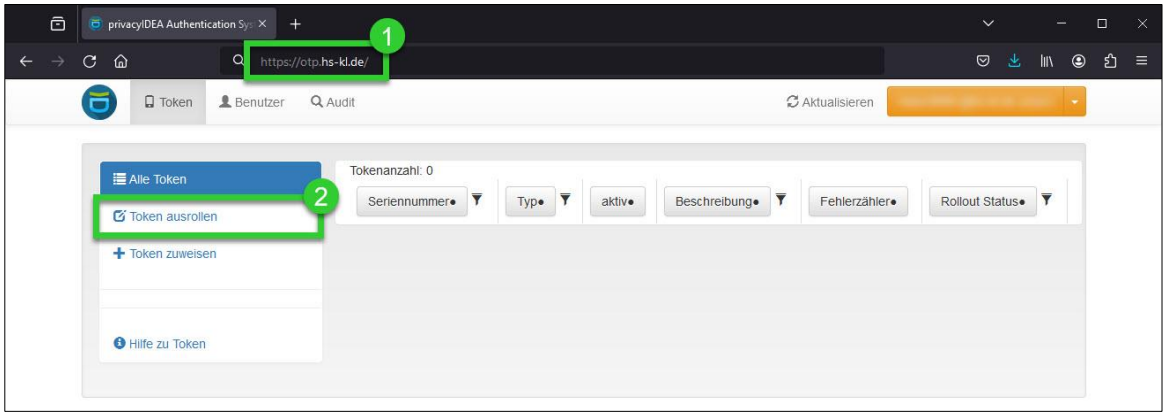
   Make a note of or copy the 32-digit *„Secret key“* before you close the window with *„Finish“* or leave the window open until you have set up multi-factor authentication.



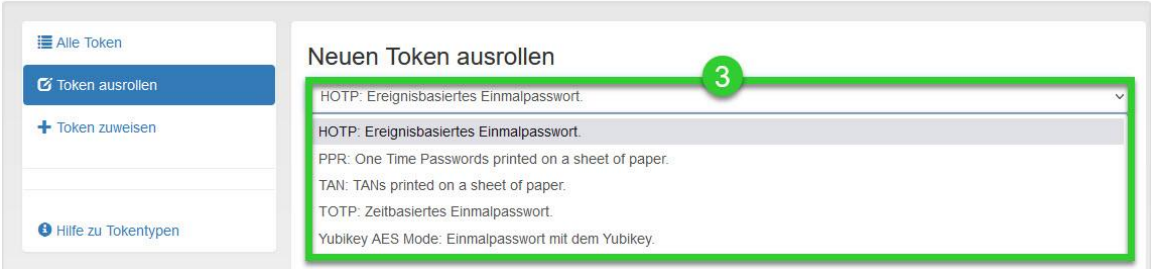
Set up multifactor authentication

1. Go to https://otp.hs-kl.de and log in with your HSKL login. This page is only accessible from the university network or via VPN connection!

2. Click on *„Token ausrollen“*.



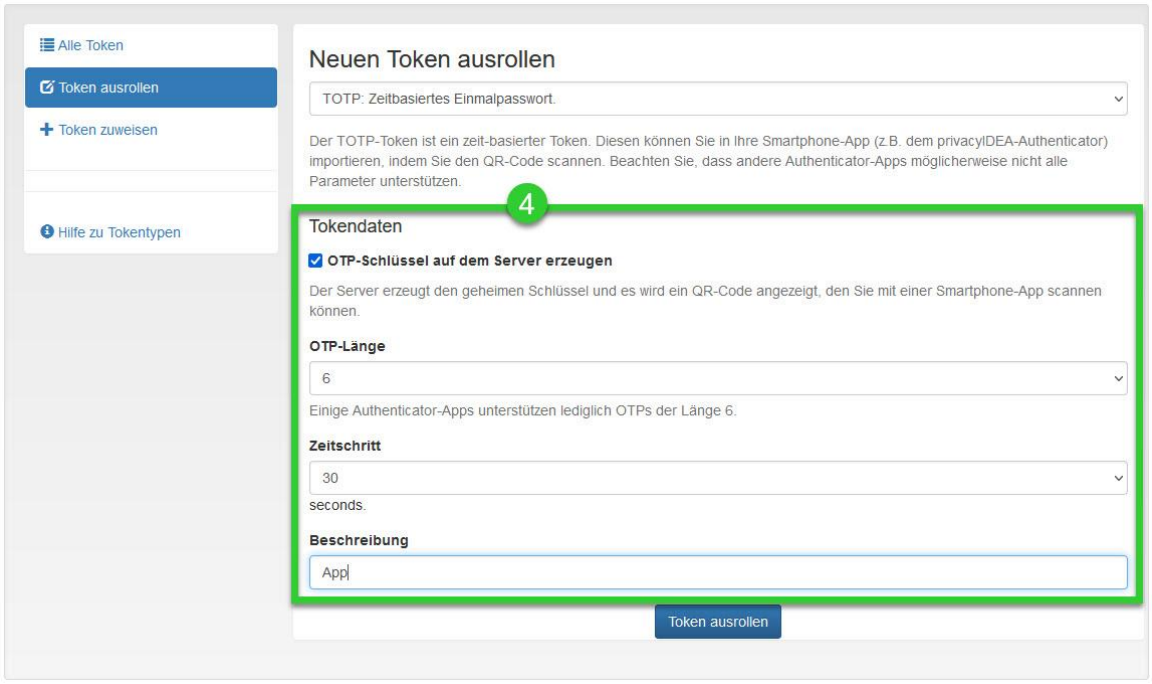
3. Select an authentication method (see section ‘Authentication methods’). A short description is displayed below for each method.

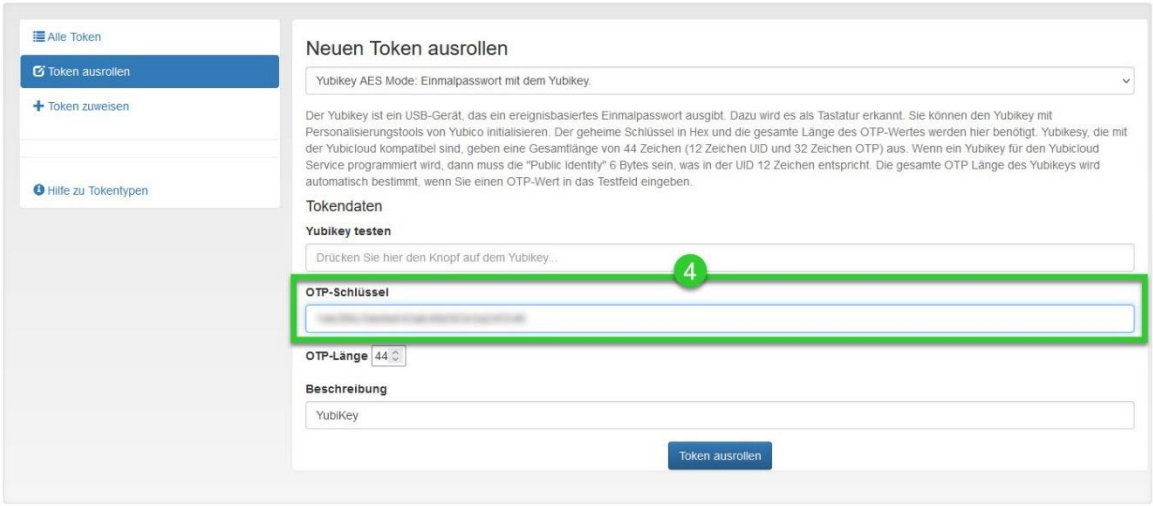


4. If necessary, adjust the settings and enter a short description of the token at *„Beschreibung“* to differentiate between the various methods. In most cases, the default settings can/should be retained.

   When using time-based one-time passwords (TOTP), the time step (*„Zeitschritt“*) must be set to 30 seconds for the apps from Google, Microsoft, Cisco and Twilio.

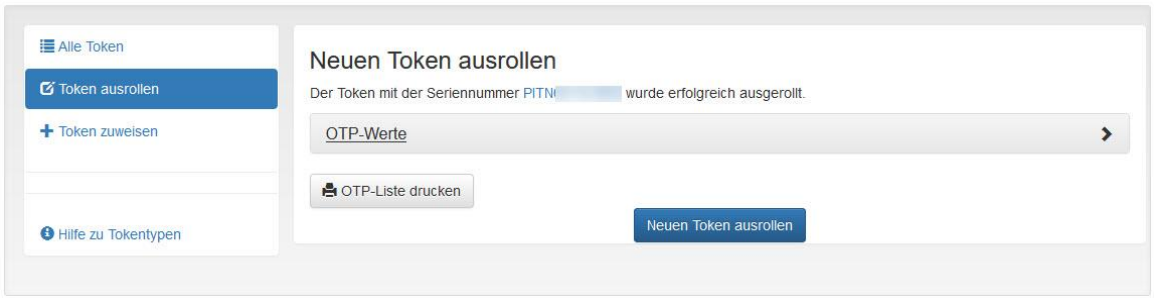
   When using a YubiKey, you must enter the *„Secret key“* (see section ‘Set up YubiKey’) in the *„OTP-Schlüssel“* field.



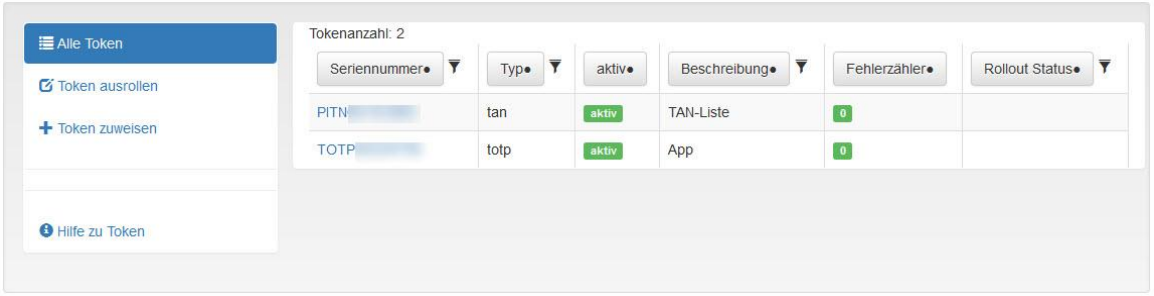


5. Click on *„Token ausrollen“*. Depending on the method selected, the setup is complete or you will be shown a QR code that you need to scan with your authenticator app or a TAN list (*„OTP-Werte“*) that you can now print out.

   Important: In all cases, this display cannot be called up again for security reasons. You must therefore scan the QR code directly or print out the list directly! Otherwise, you must roll out a new token and delete the old token if necessary.



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



Use multifactor authentication

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, Seafile, 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 button on the key. For all other methods, you must enter the code yourself.