MFA

Einrichtung einer Multi-Faktor-Authentisierung (MFA) mittels KeePassXC / Setting up multi-factor authentication (MFA) using KeePassXC

03.12.2024

https://kim.uni-hohenheim.de

Die Multi-Faktor-Authentisierung (MFA) stellt ein wirksames Mittel zur Erhöhung der Sicherheit bei der Verwendung von klassischen Zugangsdaten wie Benutzername und Passwort dar. Zum Einsatz können dabei softwarebasierte oder hardwarebasierte Token kommen. Softwarebasierte Token werden beim Smartphone durch eine App realisiert. Bei einem Personal Computer (PC, Laptop, MAC etc.) durch ein Programm. Seitens der Universität wird der Passwortmanager KeePassXC empfohlen und unterstützt.

Multi-factor authentication (MFA) is an effective means of increasing security when using traditional access data such as user name and password. Software-based or hardware-based tokens can be used. Software-based tokens are implemented on smartphones using an app. On a personal computer (PC, laptop, MAC, etc.) using a program. The university recommends and supports the password manager KeePassXC.

Inhalt / Content

Voraussetzungen / Prerequisites

Falls Sie den Passwortmanager KeePassXC noch nicht installiert haben, dann laden Sie diesen von der Webseite herunter. Das Programm steht für Windows, Linux und MacOS zur Verfügung.

If you have not yet installed the KeePassXC password manager, download it from the website. The program is available for Windows, Linux and MacOS.

https://keepassxc.org/download/

Für die Installation verweisen wir auf die Webseite des Herstellers.

For the installation, please refer to the manufacturer's website.

https://keepassxc.org/docs/KeePassXC_GettingStarted#_downloading_keepassxc

Hinweis für Windows: Prüfen Sie, ob KeePassXC fehlerfrei startet. Sollte KeepassXC nicht starten oder ein „Systemfehler: VCRUNTIME140_1.dll wurde nicht gefunden" angezeigt werden, dann muss die MSVC-Laufzeitbibliothek noch installiert werden. Sie können die neueste Version von Microsoft herunterladen.

Note for Windows: Check whether KeePassXC starts without errors. If KeepassXC does not start or a "System error: VCRUNTIME140_1.dll was not found" is displayed, then the MSVC runtime library still needs to be installed. You can download the latest version from Microsoft.

https://aka.ms/vs/17/release/vc_redist.x64.exe (nur Windows)

Ein softwarebasiertes Token einrichten / Set up a software-based token

Bitte rufen Sie die Webanwendung von Ihrem Personal Computer oder Smartphone auf

Please call up the web application from your personal computer or smartphone

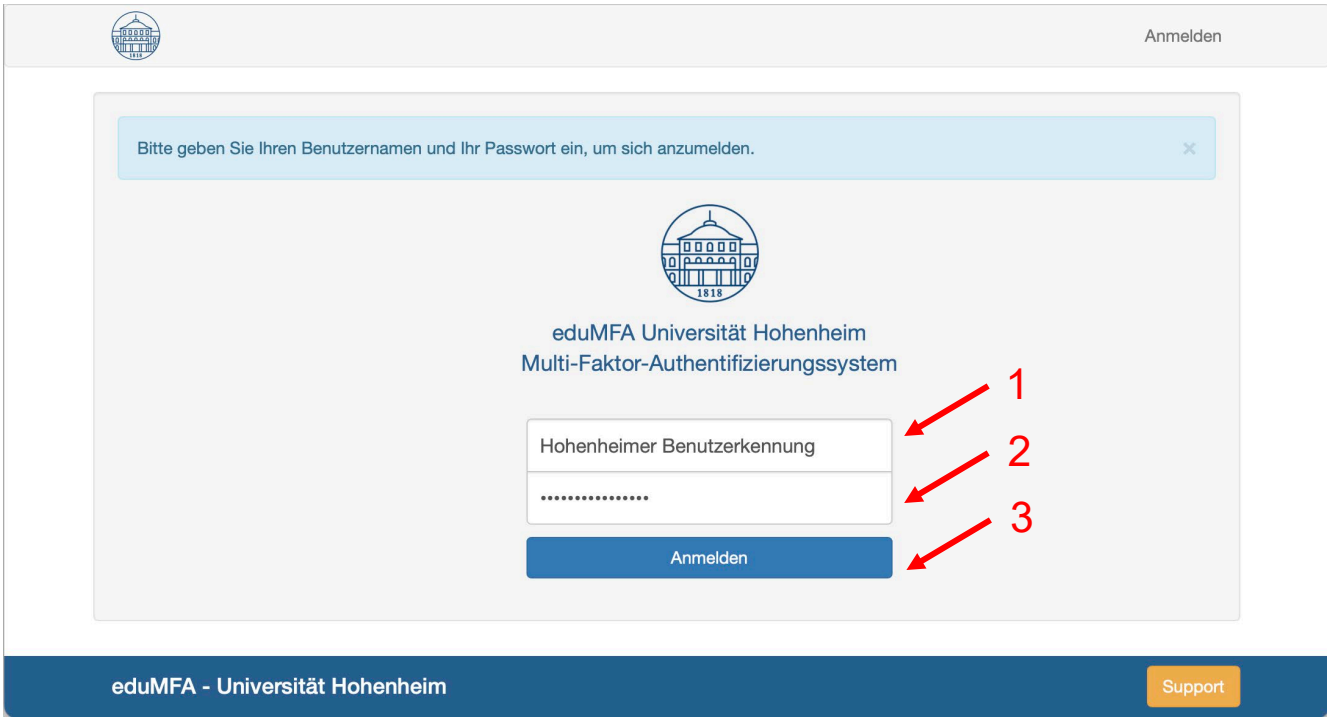
https://edumfa.uni-hohenheim.de

Dazu müssen Sie am Campus mit dem Netzwerk verbunden sein (kabelgebunden oder eduroam).

To do this, you must be connected to the network on campus (wired or eduroam).

Es erscheint die Anmeldemaske. Dort geben Sie Ihre Hohenheimer Benutzerkennung (1) und das zugehörige Passwort (2) ein.

The login screen will appear. Enter your Hohenheim user ID (1) and the corresponding password (2).

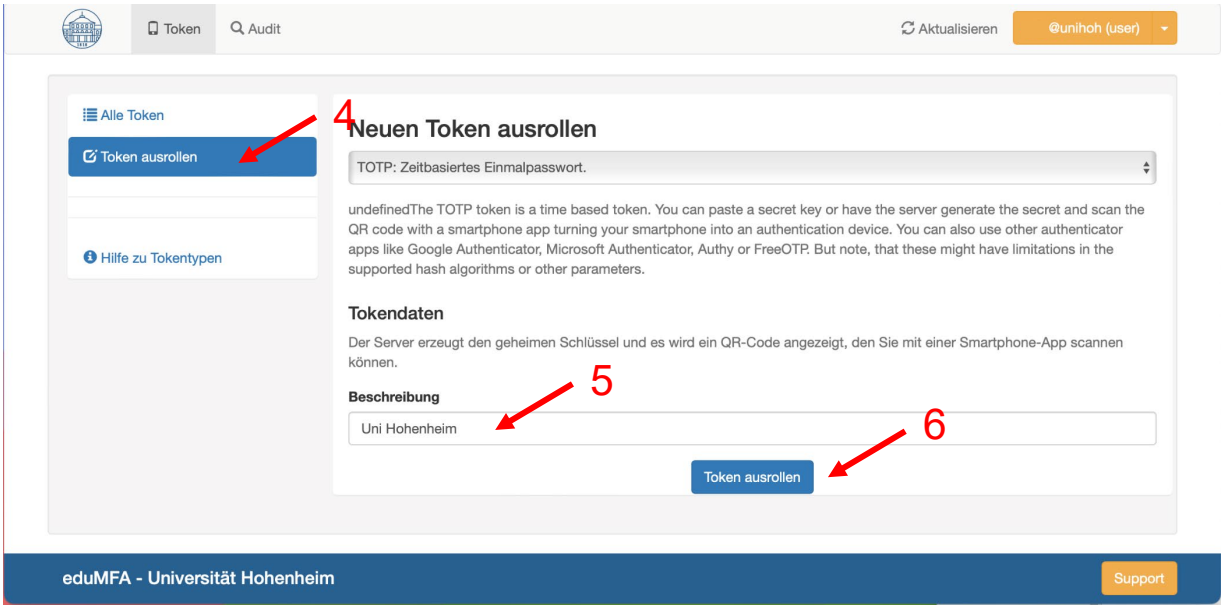


Anschließend drücken Sie mit der linken Maustaste bitte auf Anmelden (3).

Then click on Log In (3) with the left mouse button.

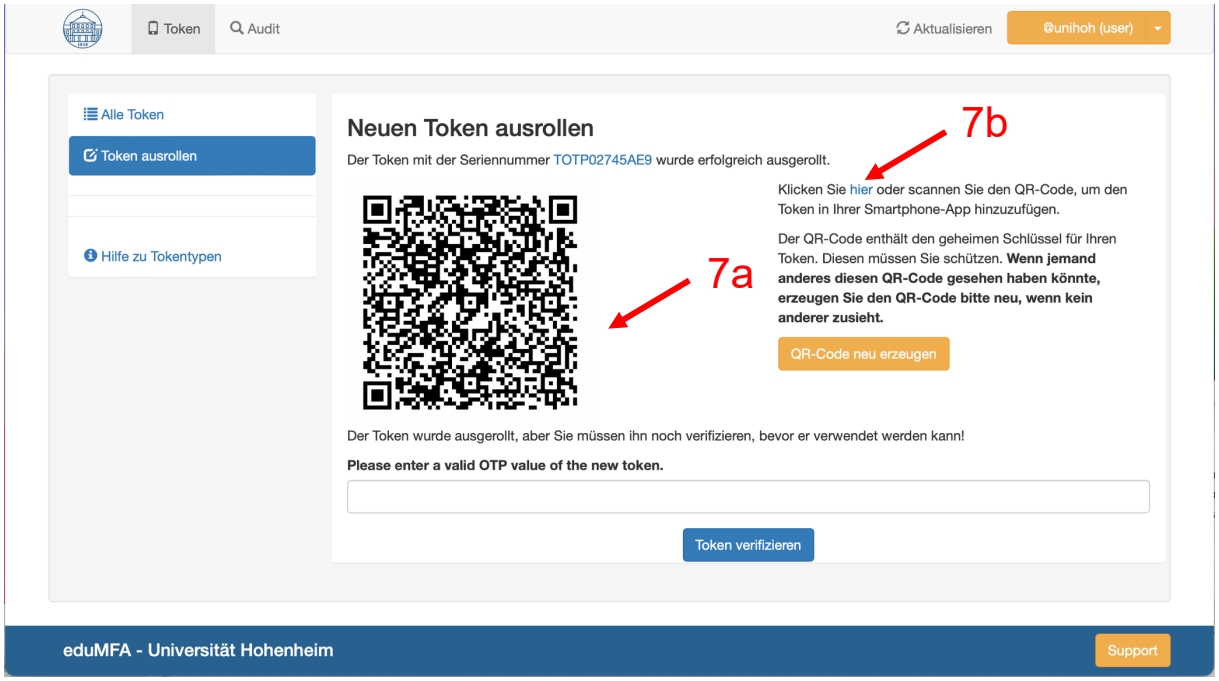
Im nächsten Schritt wählen Sie bitte im linken Bereich „Token ausrollen“ (4) aus und geben eine beliebige Beschreibung (5), z. B. Uni Hohenheim, ein.

In the next step, please select "Enroll token" (4) in the left-hand area and enter any description (5), e.g. University of Hohenheim.



Nun können Sie den „Token ausrollen“ (6) mit der linken Maustaste drücken. Im Anschluss wird der QR-Code (7a) angezeigt. Schließen Sie dieses Fenster erst, sobald Sie den Token verifiziert haben.

Now you can press the "Enroll Token" (6) with the left mouse button. The QR code (7a) is then displayed. Do not close this window until you have verified the token.

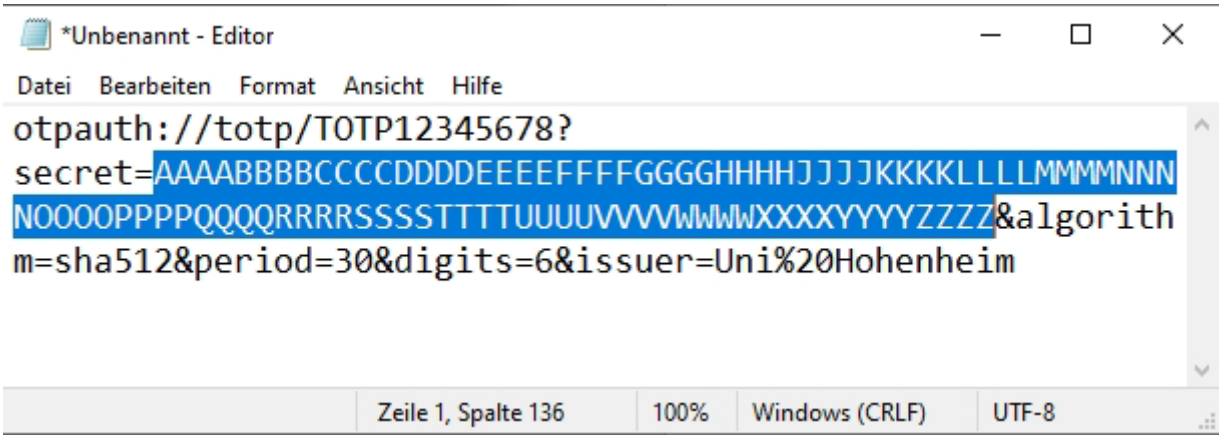


Sofern Sie Ihr PC/Notebook verwenden, können Sie den QR-Code (7a) **nicht** abscannen, sondern müssen diesen durch Klick auf „hier“ (7b) übertragen.

If you are using your PC/Notebook, you **cannot** scan the QR code (7a), but must transfer it by clicking on "here" (7b).

Neben dem QR-Code wird auch ein Link „hier“ (7b) angezeigt, der den geheimen Schlüssel enthält. Kopieren Sie den gesamten Inhalt des Links in einen Texteditor, z. B. Notepad (rechte Maustaste, bei Windows: Link-Adresse kopieren).

In addition to the QR code, a link "here" (7b) containing the secret key is also displayed. Copy the entire content of the link into a text editor, e.g. Notepad (right mouse button, for Windows: Copy link address).



Sie benötigen aus diesem Link alles nach dem „secret=“ bis ausschließlich mit nächsten „&“. Fügen Sie diesen Code später bei KeePassXC (12) als geheimen Schlüssel ein.

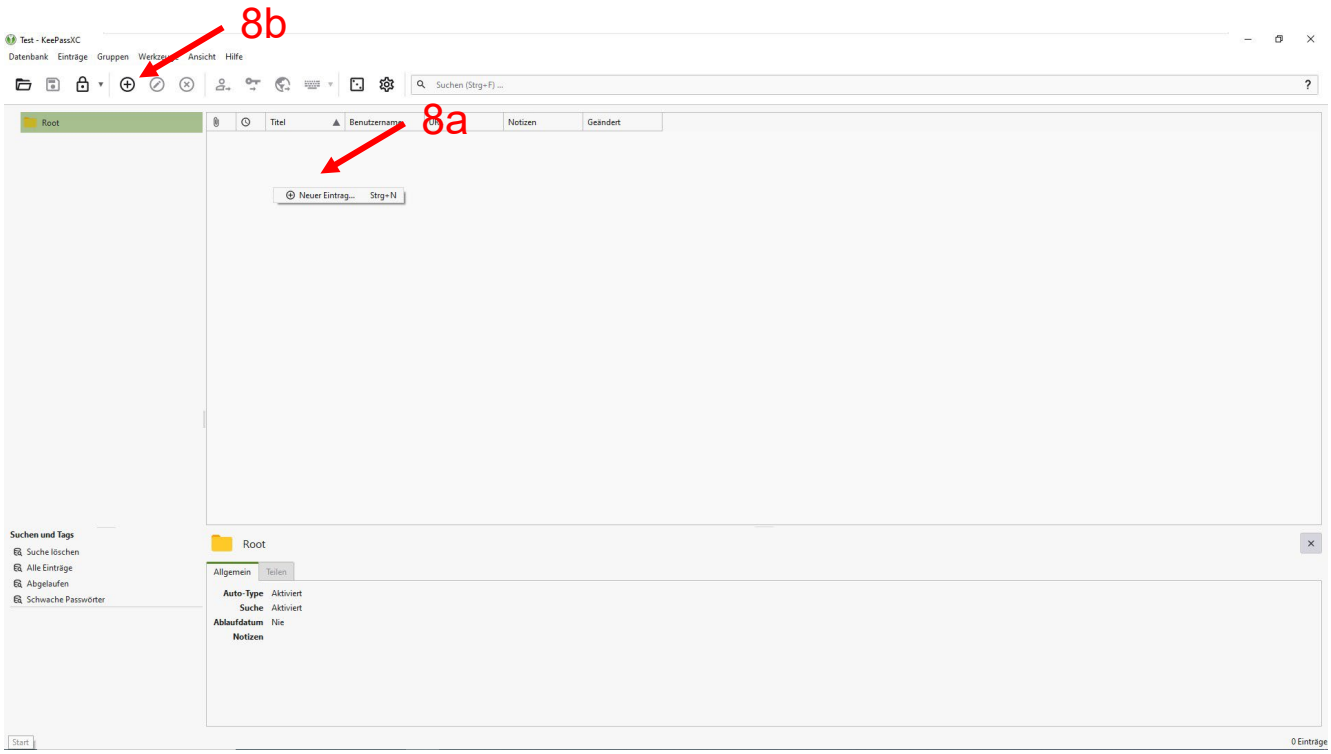
You need everything from this link after the "secret=" up to but excluding the next "&". Add this code later to KeePassXC (12) as a secret key.

Im Folgenden werden Screenshots von Windows gezeigt. Die Nutzung von KeePassXC bei Linux und MacOS weicht nur geringfügig davon ab.

Screenshots from Windows are shown below. The use of KeePassXC on Linux and MacOS differs only slightly.

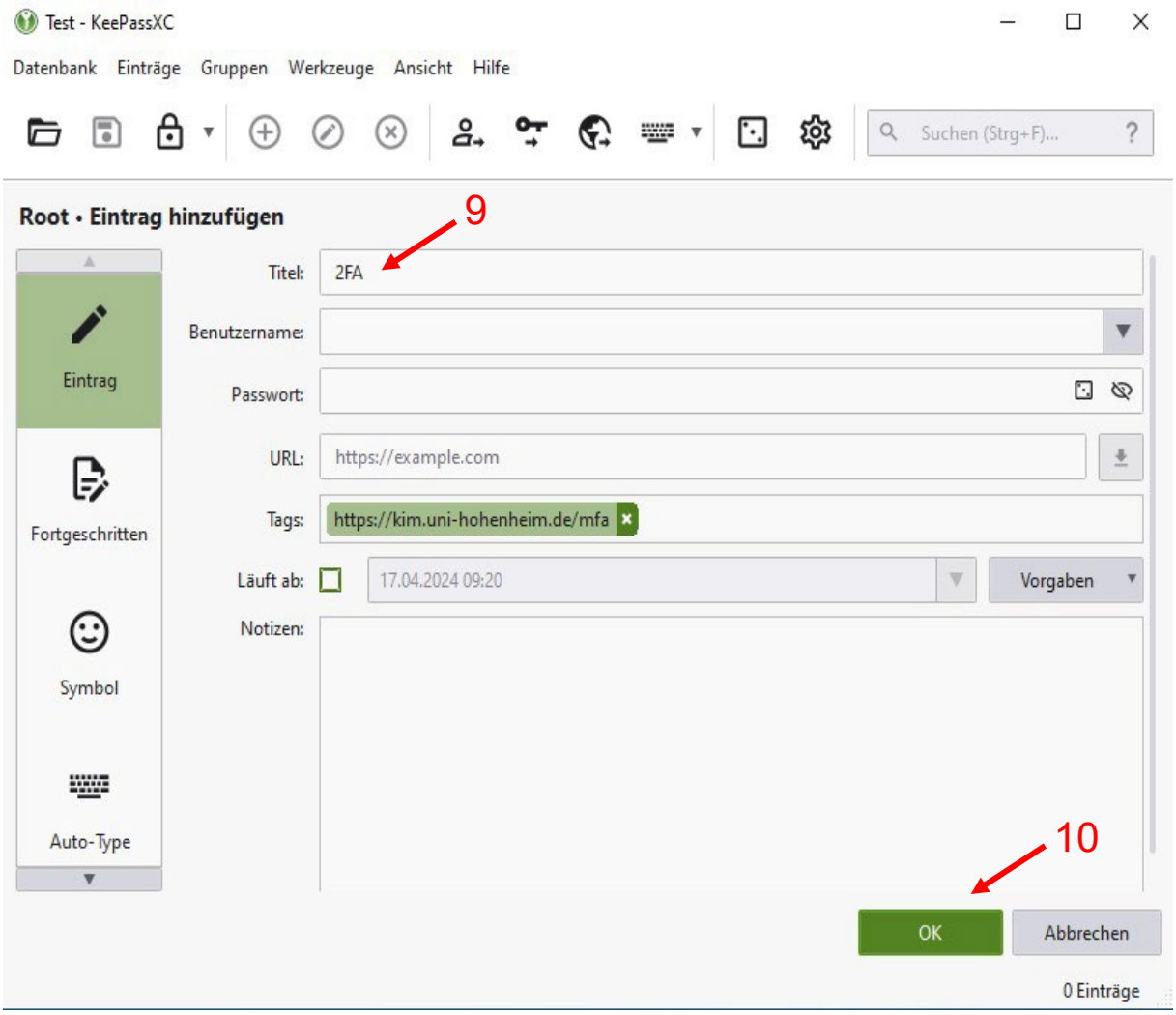
Nach dem Sie den Passwortmanager KeePassXC gestartet haben und eine Datenbank eingerichtet oder ausgewählt haben, befinden Sie sich in der Übersicht. Im Kontextmenü (Rechtsklick, 8a) oder über das Plus-Symbol (8b) können Sie einen neuen Eintrag erstellen.

After you have started the KeePassXC password manager and set up or selected a database, you will find yourself in the overview. You can create a new entry in the context menu (right-click, 8a) or via the plus symbol (8b).



Für den neuen Eintrag legen Sie bitte ein Titel (9) fest, z. B. 2FA. Benutzername und Passwort müssen nicht ausgefüllt werden. Sie können aber auch die Zugangsdaten für das Hohenheimer Benutzerkonto hier speichern.

Please define a title (9) for the new entry, e.g. 2FA. User name and password do not have to be filled in. However, you can also save the access data for the Hohenheim user account here.

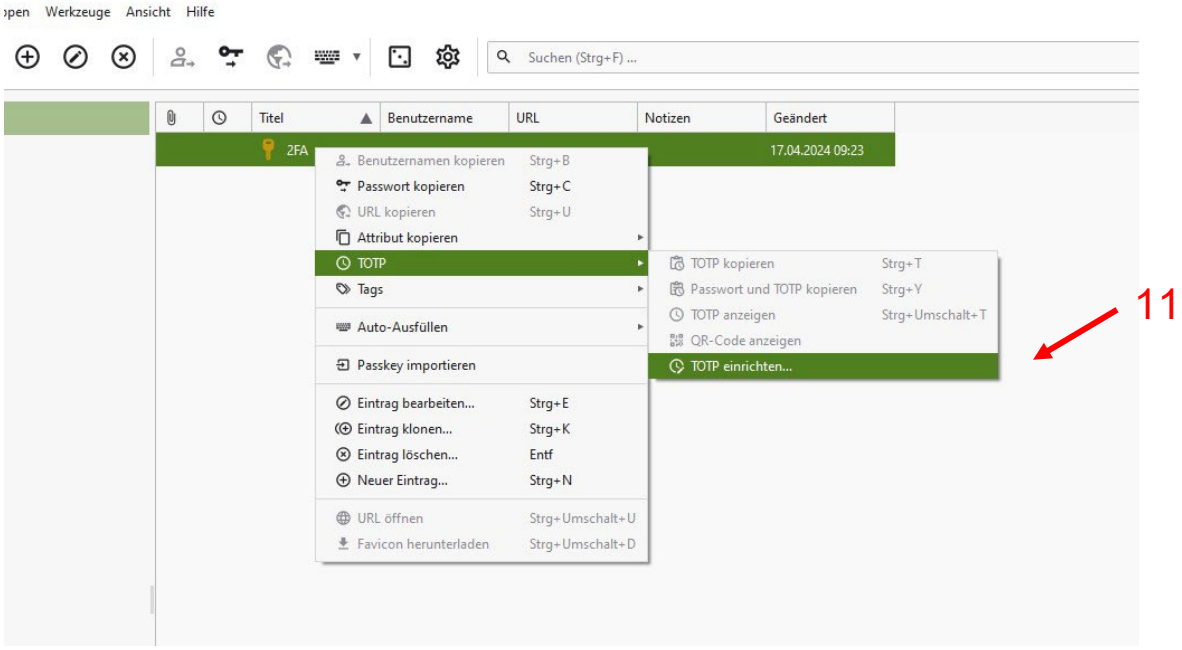


Anschließend speichern Sie den Eintrag mit „OK" (10).

Then save the entry with "OK" (10).

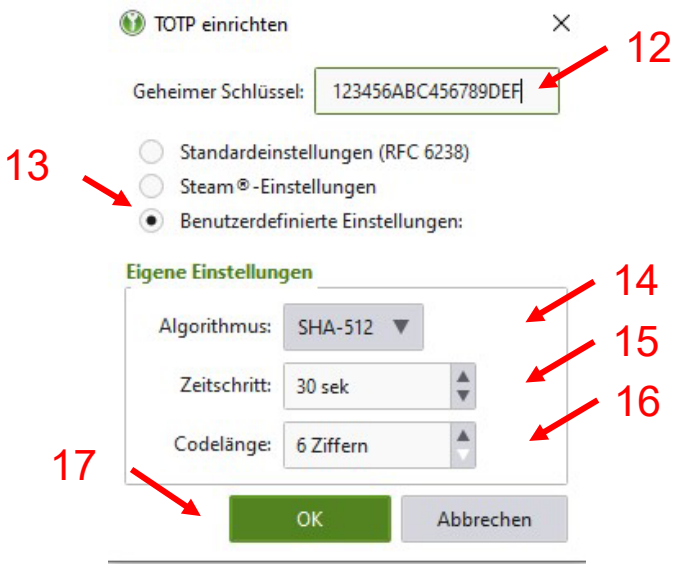
Auf dem neuen Eintrag liefert das Kontextmenü den Eintrag „TOTP“. Bitte wählen Sie den Untereintrag „TOTP einrichten“ aus (11). TOTP steht für „Time-based one-time password“.

In the new entry, the context menu provides the entry "TOTP". Please select the sub-entry "Set up TOTP" (11). TOTP stands for "Time-based one-time password".



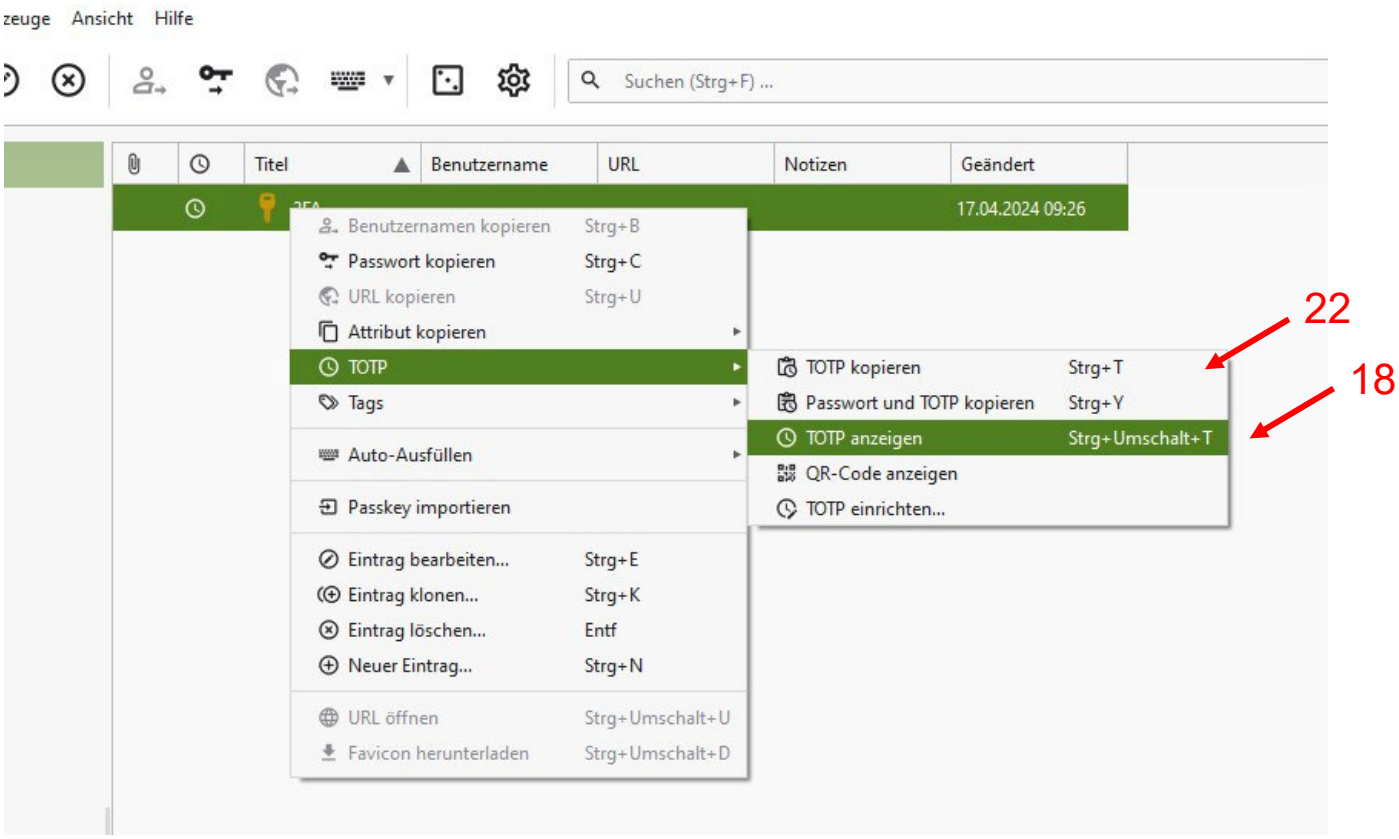
Im sich öffnenden Fenster geben Sie bitte den „Geheimer Schlüssel“ (12) aus (7b) ein und wählen „Benutzerdefinierte Einstellungen“ (13) aus. Anschließend können Sie den Algorithmus auf SHA-512 (14), den Zeitschritt auf 30 sek (15) und die Codelänge auf 6 Ziffern (16) einstellen. Mit „OK“ (17) schließen Sie die Konfiguration ab.

In the window that opens, please enter the "Secret key" (12) from (7b) and select "User-defined settings" (13). You can then set the algorithm to SHA-512 (14), the time step to 30 sec (15) and the code length to 6 digits (16). Click "OK" (17) to complete the configuration.



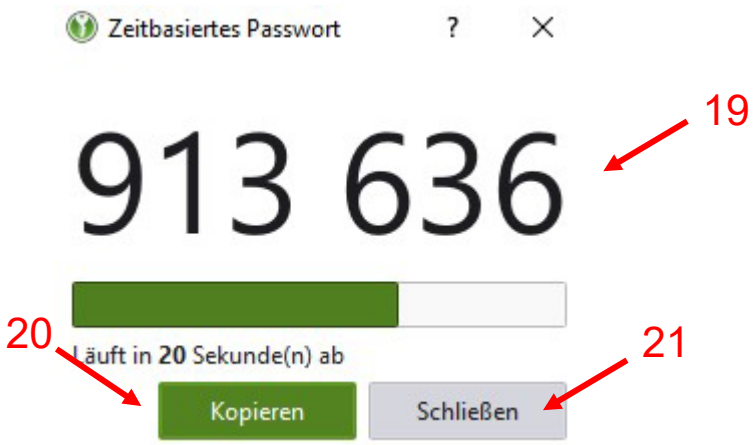
Sie gelangen wieder in der Übersicht. Auf dem eben erstellten Eintrag zeigt das Kontextmenü den Eintrag „TOTP“ an. Dort wählen Sie nun der Eintrag „TOTP anzeigen“ (18) aus.

You return to the overview. The context menu shows the "TOTP" entry on the entry you have just created. Now select the entry "Show TOTP" (18).



Es öffnet sich ein weiteres Fenster mit dem zeitbasierten Passwort (19).

Another window opens with the time-based password (19).

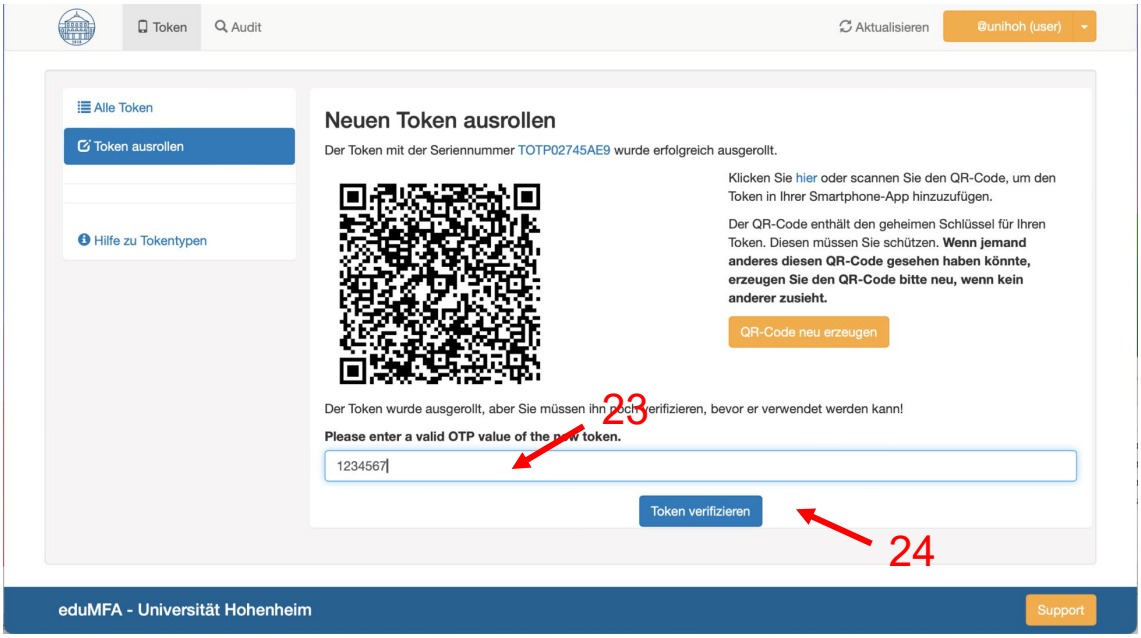


Durch Drücken auf „Kopieren“ (20) können Sie diesen Wert in den Zwischenspeicher legen. Mit „Schließen“ (21) wird das Fenster geschlossen. Alternativ können Sie auch direkt „TOTP kopieren“ (20) im Kontextmenü wählen.

Press "Copy" (20) to store this value in the temporary memory. The window is closed with "Close" (21). Alternatively, you can also select "Copy TOTP" (20) directly in the context menu.

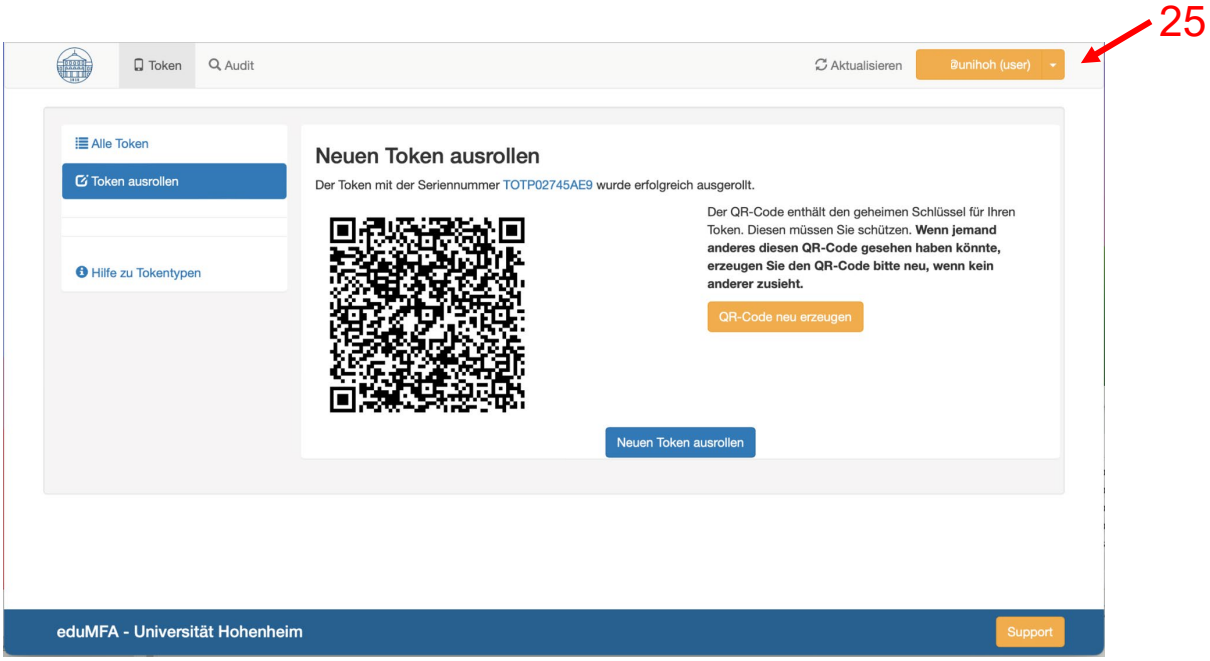
Den TOTP (19) fügen Sie nun als Bestätigung auf der Webseite ein (23) und können damit den „Token verifizieren“ (24).

Now insert the TOTP (19) as confirmation on the website (23) and you can use it to "verify the token" (24).



In der Webanwendung wird der QR-Code nochmals angezeigt.

The QR code is displayed again in the web application.

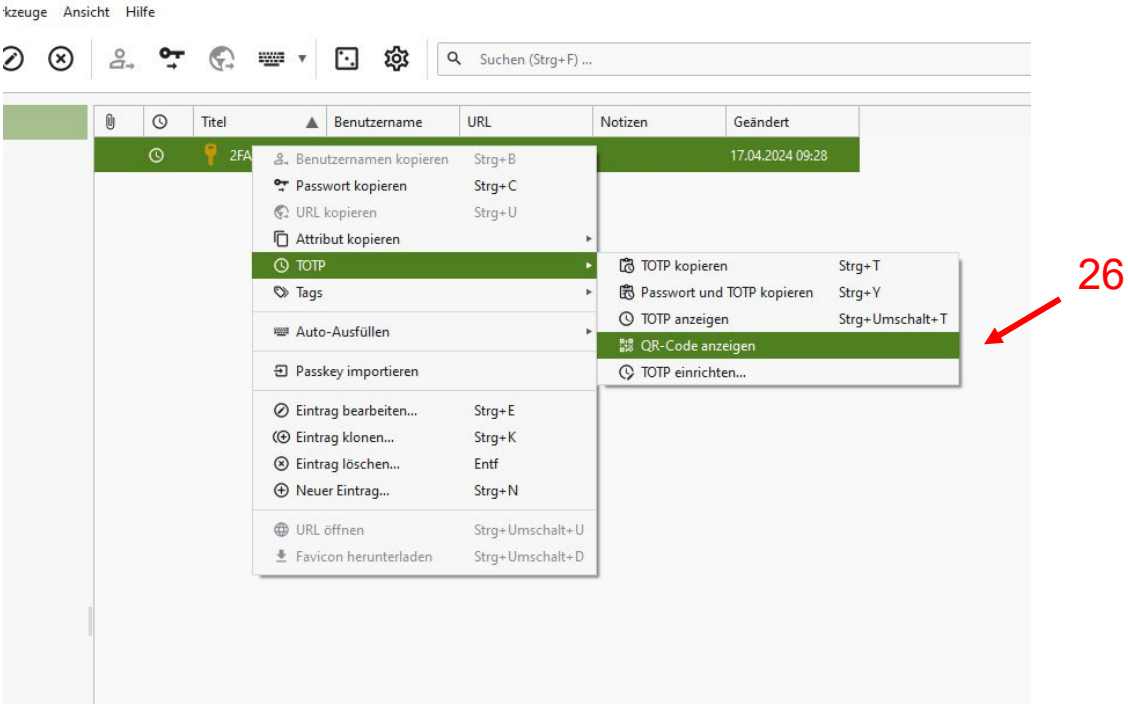


Falls Sie den Token noch auf ein anderes Gerät übertragen wollen, können Sie den QR-Code an dieser Stelle, z. B. mit einem anderen Gerät einscannen. Anschließend können Sie sich abmelden (25).

If you still want to transfer the token to another device, you can scan the QR code at this point, e.g. with another device. You can then log out (25).

KeePassXC bietet zudem die Möglichkeit den QR-Code erneut anzuzeigen. Dazu einfach im Kontextmenü auf den Eintrag „QR-Code anzeigen" klicken (26).

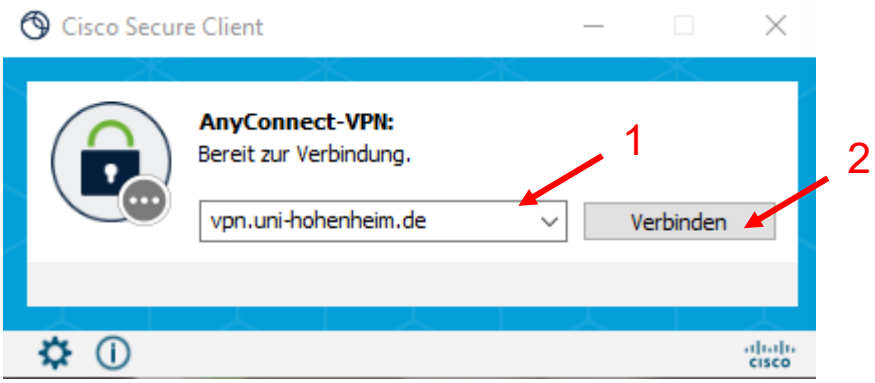
KeePassXC also offers the option of displaying the QR code again. To do this, simply click on the "Show QR code" entry in the context menu (26).



VPN-Verbindung mit MFA am Beispiel Windows / VPN connection with MFA using Windows as an example

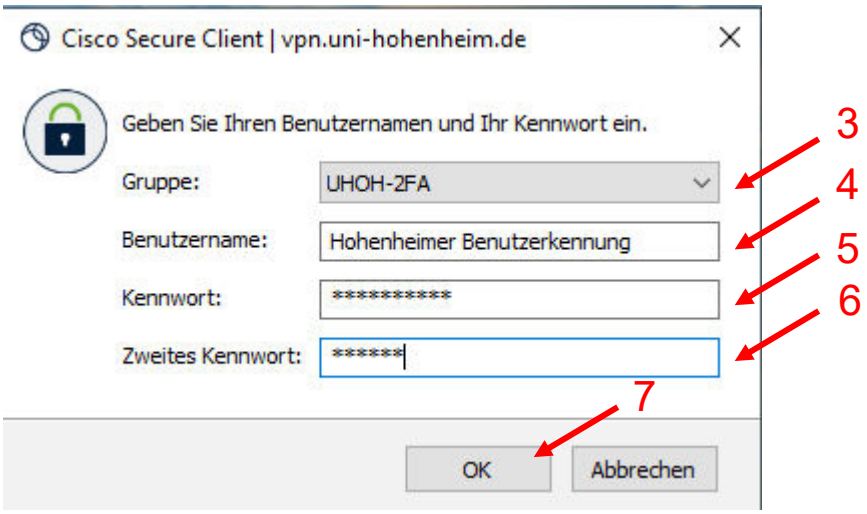
Eine praktische Anwendung findet die Multi-Faktor-Authentisierung bei der VPN-Verbindung. Die Verbindung wird wie gehabt zu vpn.uni-hohenheim.de (1) aufgebaut (2).

Multi-factor authentication is used in practice for the VPN connection. The connection is established as usual to vpn.uni-hohenheim.de (1) (2).



Sobald das softwarebasierte Token für Ihre Hohenheimer Benutzerkennung erfolgreich eingerichtet wurde, wählen Sie falls noch nicht voreingestellt die Gruppe UHOH-2FA (3) aus. Es wird ein zusätzliches Feld (Zweites Kennwort oder 2FA Token) angezeigt. Bitte geben Sie nun Ihren Hohenheimer Benutzernamen (4), das zugehörige Passwort (5) und das Token (6) ein.

As soon as the software-based token for your Hohenheim user ID has been successfully set up, select the UHOH-2FA group (3) if it has not already been set up. An additional field (Second password or 2FA token) will be displayed. Please now enter your Hohenheim user name (4), the corresponding password (5) and the token (6).



Den Token erhalten Sie aus KeePassXC.

Get the token from KeePassXC.

Die Verbindung wird mit OK (7) - wenn alle Daten korrekt sind - aufgebaut.

The connection is established with OK (7) - if all data is correct

Hinweise / Notes

- Der softwarebasierte Token kann nur aus dem Hohenheimer Netzwerk (vor Ort) initial beantragt und eingerichtet werden. Eine VPN-Verbindung ist aus Gründen der IT-Sicherheit nicht ausreichend.

- Der QR-Code kann nach der Einrichtung durch KeePassXC erneut angezeigt werden. Es empfiehlt sich trotzdem ein Backup anzulegen. Da der QR-Code nicht passwortgeschützt ist, sollte dieser QR-Code bzw. das Backup sorgfältig verwahrt werden.

- Sobald der softwarebasierte Token erfolgreich eingerichtet wurde, kann dieser beim VPN-Dienst genutzt werden. Bitte ggf. die Gruppe UHOH-2FA auswählen.

- Der softwarebasierte Token ist zeitlich beschränkt gültig (max. 30 Sekunden, beginnend zur 0-ten und 30-sten Sekunde). Möglichweise ist dieses bei Eingabe bereits ungültig. Dann bitte einen neuen Token aus KeePassXC ablesen und übernehmen.

- Wenn der softwarebasierte Token verloren geht, dann kann dieser nutzerseitig nicht zurückgesetzt werden. In diesem Fall wenden Sie sich bitte an den IT-Service-Desk. Unter Vorlage eines amtlichen Ausweises (Personalausweis oder Reisepass) wird der softwarebasierte Token gelöscht und Sie können selbst gemäß dieser Anleitung einen neuen softwarebasierten Token erstellen.

- Über die Webanwendung (https://edumfa.uni-hohenheim.de) haben Sie die Möglichkeit den softwarebasierten Token zu testen und den Fehlerzähler selbständig zurückzusetzen. Die Deaktivierung kann Ihrerseits erfolgen, aber nicht rückgängig gemacht werden. Bitte wenden Sie sich in diesem Fall an den IT-Service-Desk.

- The software-based token can only be initially requested and set up from the Hohenheim network (on site). A VPN connection is not sufficient for IT security reasons.

- The QR code can be displayed again after KeePassXC has been set up. It is nevertheless recommended to create a backup. As the QR code is not password-protected, this QR code or the backup should be stored carefully.

- As soon as the software-based token has been successfully set up, it can be used with the VPN service. Please select the UHOH-2FA group if necessary.

- The software-based token is valid for a limited time (max. 30 seconds, starting at the 0th and 30th second). It may already be invalid when you enter it. In this case, please read a new token from KeePassXC and accept it.

- If the software-based token is lost, it cannot be reset by the user. In this case, please contact the IT Service Desk. On presentation of an official ID (ID card or passport), the software-based token will be deleted and you can create a new software-based token yourself in accordance with these instructions.

- You can test the software-based token and reset the error counter yourself via the web application (https://edumfa.uni-hohenheim.de). The deactivation can be carried out by you, but cannot be reversed. In this case, please contact the IT Service Desk.

Bei Fragen stehen wir Ihnen gerne am
IT-Service-Desk des KIM
Biogebäude 1, Garbenstraße 30, 1. UG
oder per E-Mail unter
kim-it-account@uni-hohenheim.de
zur Verfügung.

If you have any questions, please contact the
IT Service Desk of the KIM
Biogebäude 1, Garbenstraße 30, 1. Basement
or send us an email
kim-it-account@uni-hohenheim.de