HUMBOLDT-
UNIVERSITÄT
ZU BERLIN

Two-factor Authentication (2FA) - Hardware Token

December 12, 2022

1 Preface

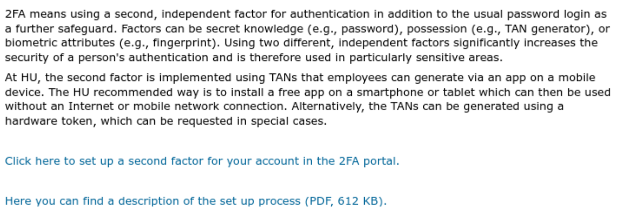
What is 2FA? 2FA means using a second factor as a further safeguard in addition to the usual password login, e.g. one-time passwords (similar to a TAN).
For security-critical application areas, 2FA has been recommended for some time, e.g. by the German Federal Office for Information Security. In banking, it was made mandatory in 2018. Stiftung Warentest also recommends using 2FA for as many web services as possible.
One-time passwords can be generated simply and easily via an app (for smartphone or tablet). In special cases, so-called hardware tokens can be provided (available in key fob format).

2 Preparation

At HU, the second factor is implemented using TANs that employees can generate via an app on a mobile device or via a so-called hardware tokens. You will receive a hardware token in person at the service counters of the User help desk in Adlershof or in the Grimm Center after a prior authorization check (check your employee status). Please inform yourself in advance about the locations and opening hours of the service counters (https://www.cms.hu-berlin.de/de/dl/oecap/locations). The authorization check is performed by presenting a valid, official photo ID. You will also need a valid HU employee account. If you do not have one or it is no longer usable, please contact User help desk (https://www.cms.hu-berlin.de/de/dl/beratung/anmeld_html) beforehand.

3 HU Authentication Manager

Open HU Authentication Manager (https://hu.berlin/2FA) in the browser or use



2FA means using a second, independent factor for authentication in addition to the usual password login as a further safeguard. Factors can be secret knowledge (e.g., password), possession (e.g., TAN generator), or biometric attributes (e.g., fingerprint). Using two different, independent factors significantly increases the security of a person's authentication and is therefore used in particularly sensitive areas.

At HU, the second factor is implemented using TANs that employees can generate via an app on a mobile device. The HU recommended way is to install a free app on a smartphone or tablet which can then be used without an Internet or mobile network connection. Alternatively, the TANs can be generated using a hardware token, which can be requested in special cases.

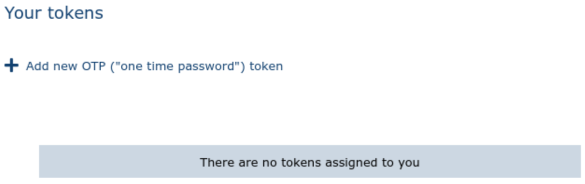
Click here to set up a second factor for your account in the 2FA portal.

Here you can find a description of the set up process (PDF, 612 KB).

Please go to **Click here to set up a second factor for your account in the 2FA portal.** to start the actual authentication manager. The login is done through the central HU Single-Sign-On (SSO) service. You will need your HU account and the associated password.

The authentication manager displays an overview of the tokens assigned to you on the start page. Initially, you should not have any tokens assigned.

3.1 Add a New Token



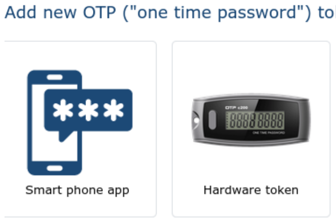
Your tokens

+ Add new OTP ("one time password") token

There are no tokens assigned to you

Click the **+ Add new OTP ("one time password") token** button to create a new token.

3.2 Select Software Token



Add new OTP ("one time password") token

Click on the **Smart phone app** button to create a new software token.

4 Add new software token

Now you need your mobile device (smartphone or tablet) for the further steps. The following page contains links to tested apps and also already your new software token in the form of a QR code.

4.1 Installing the App

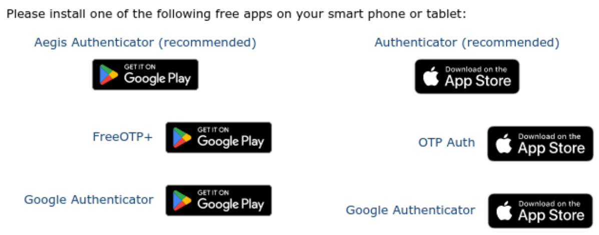
If you already have an app for generating OTP tokens installed on your smartphone, proceed directly with step 4.2. Otherwise, depending on the device type, please install e.g.

- Aegis Authenticator: https://play.google.com/store/apps/details?id=com.beemdevelopment.aegis or
- FreeOTP+: https://play.google.com/store/apps/details?id=org.liberty.android.freeotpplus

from GooglePlay resp.

- Authenticator: https://apps.apple.com/app/authenticator/id766157276 or
- Google Authenticator: https://apps.apple.com/app/google-authenticator/id388497605

from the AppStore.
You should be able to install the app for free in each case.



Please install one of the following free apps on your smart phone or tablet:

Aegis Authenticator (recommended)

Authenticator (recommended)

FreeOTP+

OTP Auth

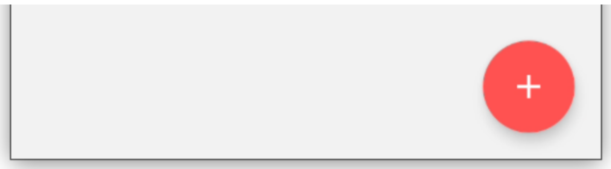
Google Authenticator

Google Authenticator

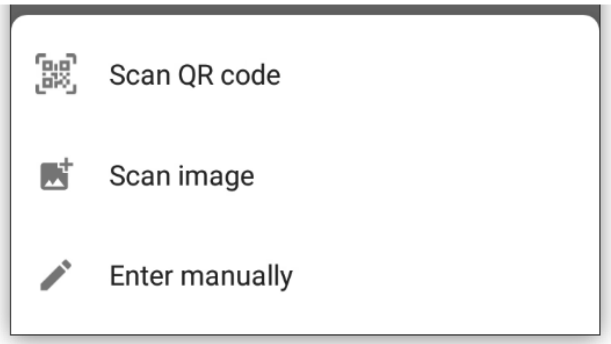
GET IT ON Google Play
Download on the App Store
GET IT ON Google Play
Download on the App Store
GET IT ON Google Play
Download on the App Store

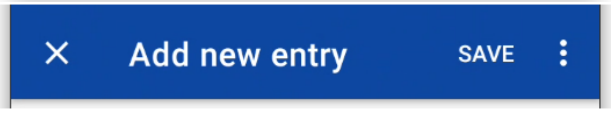
4.2 Import a Software Token

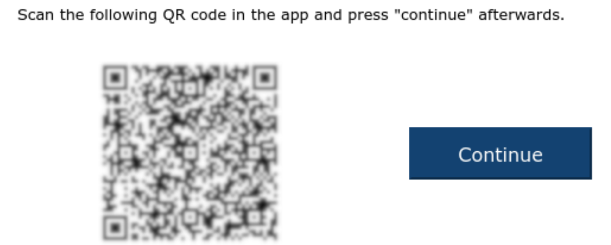
Please open the Authenticator app (previously installed) on your end device. Here *Aegis Authenticator* is used as an example.



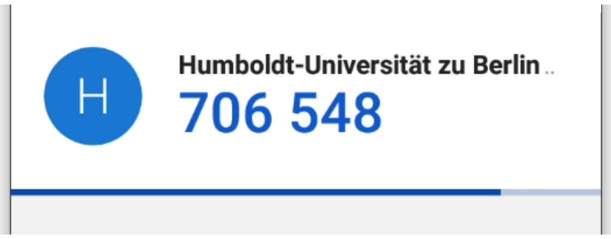
Please press **+** to add a code.

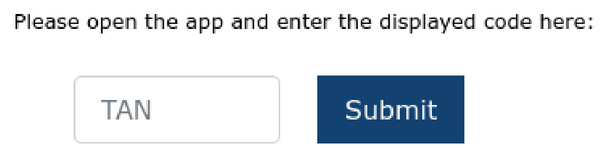





Scan the following QR code in the app and press "continue" afterwards.

Please tap **Scan QR Code** on the mobile device to add the QR code displayed on the webpage. Focus the camera of your mobile device on the QR code displayed in the browser. If your mobile device has recognized the QR code, the **Add new entry...** window appears on your mobile device. Please tap on **Save** there. After that, please click **Continue** on the webpage.

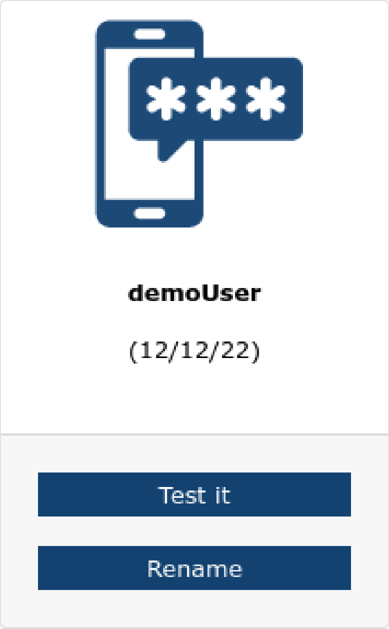



Please open the app and enter the displayed code here:

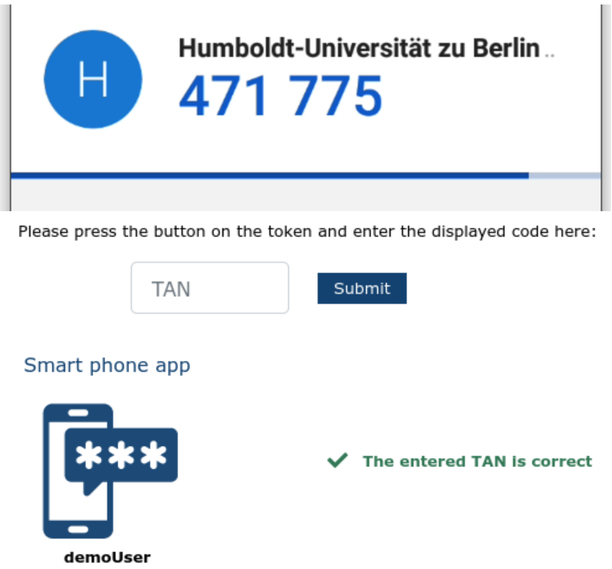
On the web page, now enter the TAN displayed on your mobile device, in this case **706548**, into the **TAN** input field and confirm with **Submit**.

If you are back on the overview page afterwards, the token registration has been completed successfully. In case of an error, a corresponding message will be displayed in your browser. In this case, please try again with a different TAN. If the error occurs repeatedly, please contact CMS User help desk (cms-benutzerberatung@hu-berlin.de).

5 Verifying Your New Software Token



Now please check the functionality of your new software token by clicking on the button **Test it**.



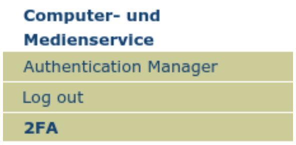
Please press the button on the token and enter the displayed code here:

✓ The entered TAN is correct

Now please pick up your mobile device again and open the authentication app. On the website, now enter the TAN displayed on your mobile device, in this case **471775**, into the input field **TAN** and confirm with **Submit**.

If you finally see the success message **The entered TAN is correct**, then you have successfully tested the functionality of your new hardware token.

6 Log out



After using the HU Authentication Manager, please log out by clicking **Log out** and close your browser to terminate all internet activity.