Introduction into Two-Factor-Authentication (2FA)

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 a smartphone app, or by so-called hardware tokens (available in keychain format).

How do I get a second factor?

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.

The following describes how to obtain a HU software token.

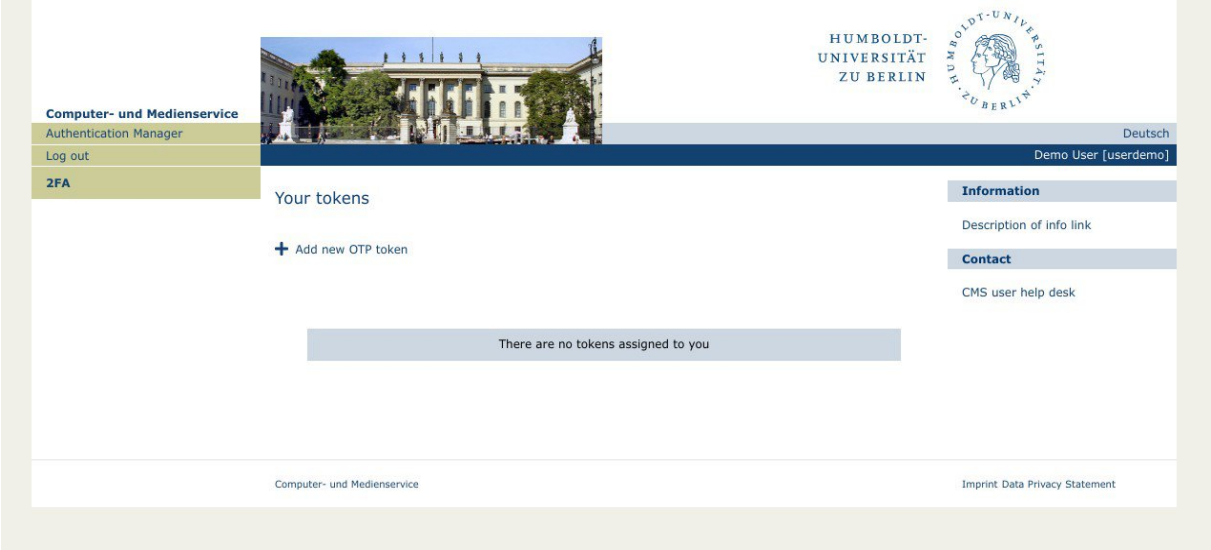
HU Software-Token

1. Launch HU Authentication-Manager

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

The login is done via the HU central Singe-Sign-On (SSO) service. You need your HU account and the corresponding password.

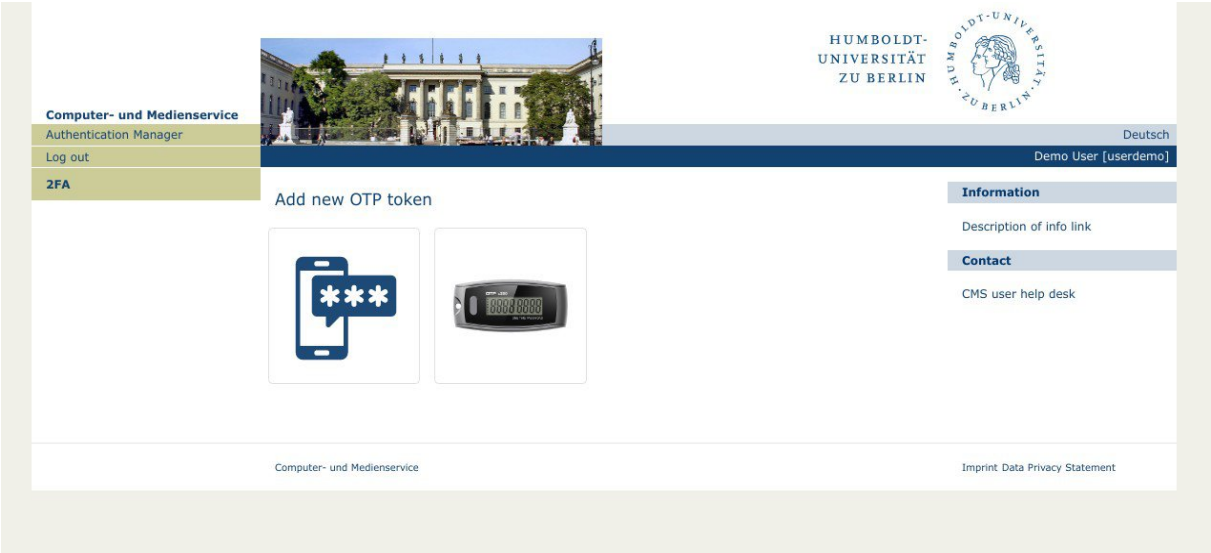
The authentication manager displays an overview of the tokens assigned to you on the start page. Initially, you should not have any assigned tokens (see figure).



Authentication manager: start page (initially)

2. Add new token

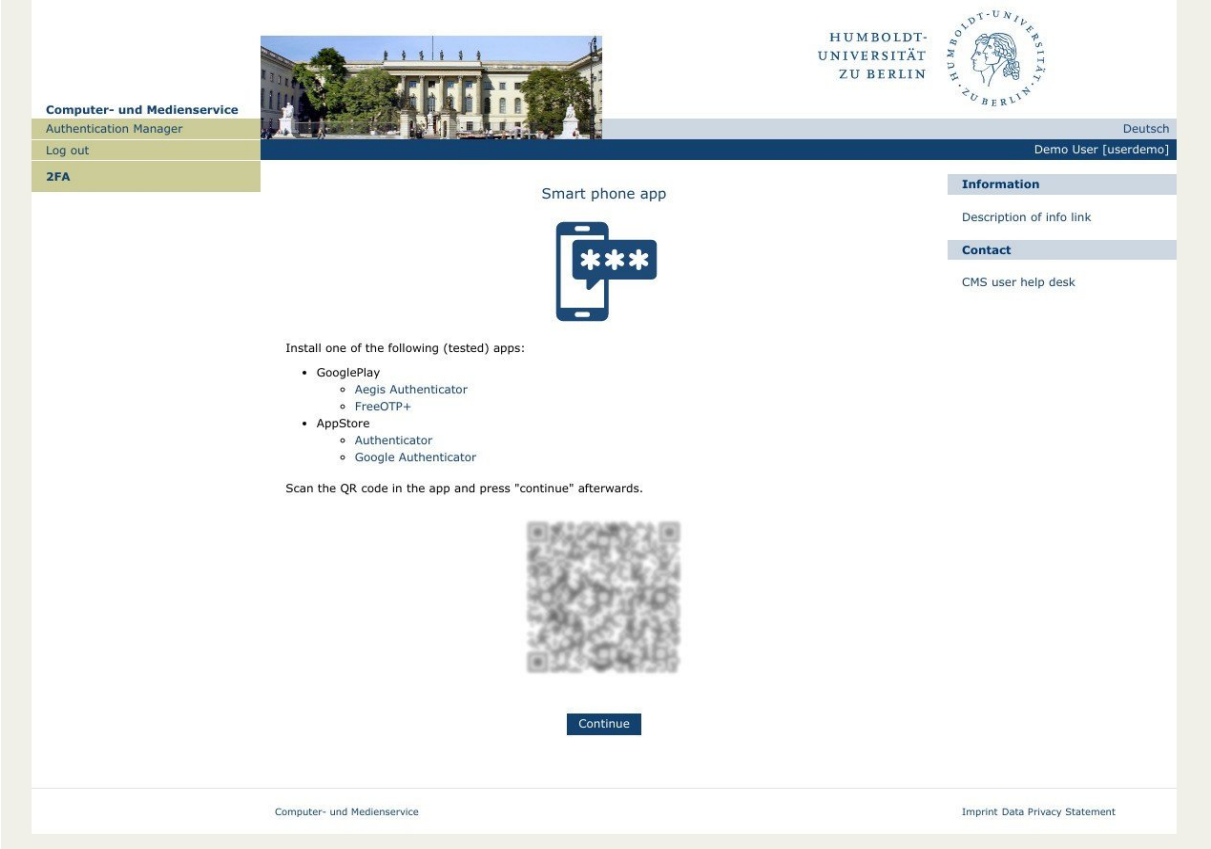
Click the '+ Add new OTP token' button to create a new token. On the following page click on the graphic with the cell phone and the asterisks, see the figure.



Authentication manager: add new OTP token

3. Add new software token

At the latest now you need your smartphone for the further steps. The following page contains links to tested apps for your smartphone and also already your new software token in the form of a QR code, see figure.



Authentication manager: add new software token

3.1 Smartphone-App

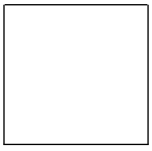
If you have already installed an app for generating OTP tokens on your smartphone, proceed directly to step 3.2.

Otherwise, depending on your smartphone type, please install the app FreeOTP+ or Aegis Authenticator from GooglePlay or Google Authenticator or Authenticator from AppStore. The installation of the app should be possible free of charge in each case.

3.2 Import software Token

Please open the (previously installed) Authenticator app on your smartphone. In the (import) settings, select the function 'Scan QR code' and focus your smartphone on the QR code displayed in the browser.

As a result, you should now see your HU token in the list of tokens:



_ _ _ _ _ _
Humboldt-Universität zu Berlin
Account-name (*YYYY-MM-DDThh:mm:ss*)

Since the generation of the one-time password is time-controlled based on the token, each one-time password is valid in exactly one time interval of 30 seconds length. The

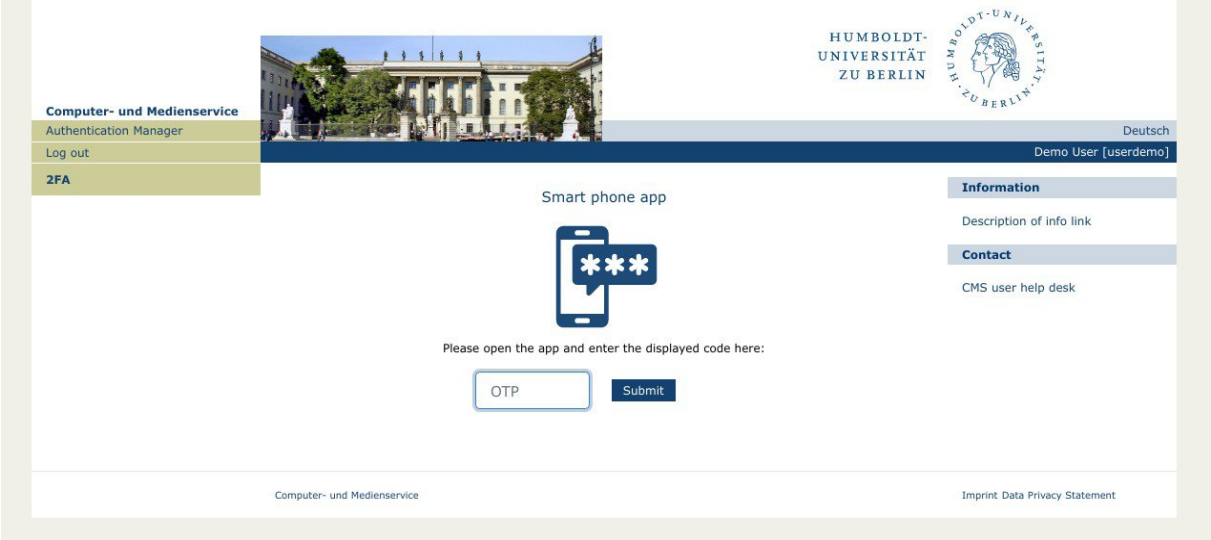
current validity period of the one-time password is indicated by an image in front of the code. The current one-time password is generated or displayed when you tap the line in the list.

The one-time password consists of 6 digits. For the generation no internet and also no connection to the mobile network is necessary.

If you want to use other devices for generating your one-time password, the same QR code can also be scanned on other devices with a corresponding application, e.g. tablets.

4. Verify your new software token

After you see above token in your token list on smartphone, go to the next page with 'Continue' button, see figure.



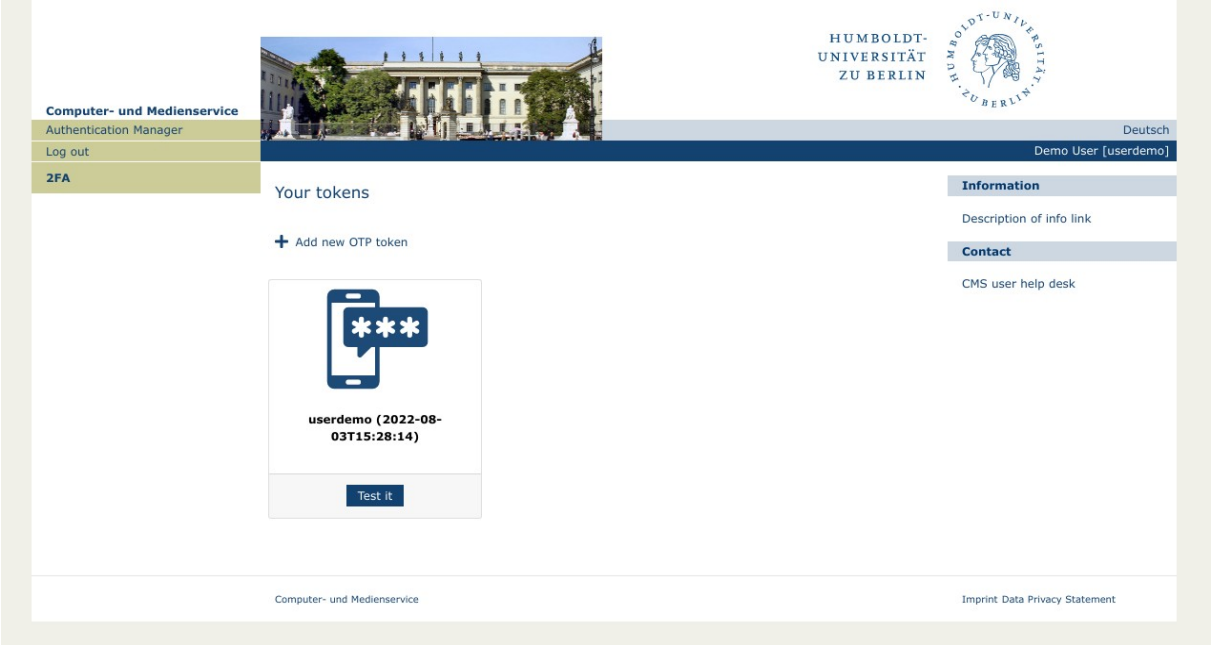
Authentication manager: verify new software token

Now have your smartphone app display the current one-time password (code: 6 digits) and enter it in the input field. Make sure that it is still valid when you have finished entering it.

Tip: If the code displayed in your smartphone is only valid for a few seconds, wait a little while until the app shows you a new code.

After entering the code in the browser, press 'Enter' or the 'Submit' button.

If the validation of the code was successful, you will now see the start page of the authentication manager in the browser with your new software token, see figure.



Authentication manager: successfully installed, new software token

The token is named with your HU account and in brackets behind it the time of creation.

In the event of an error, a corresponding message will be displayed in the browser. Please try again from step 1 - If the error occurs repeatedly, please contact the CMS user support:

cms-benutzerberatung@hu-berlin.de