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).

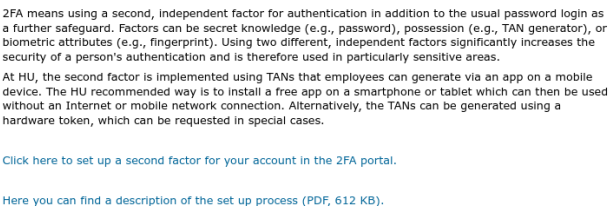
2 Preparation

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

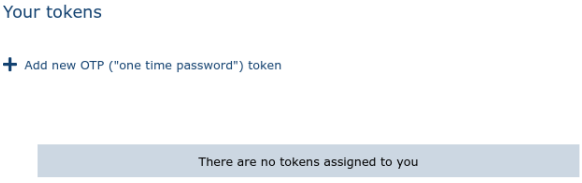
Open HU Authentication Manager (https://hu.berlin/2FA) in the browser or use



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



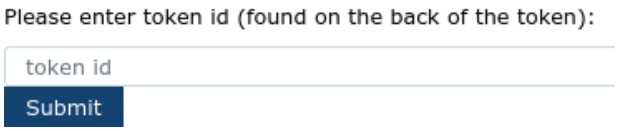
Click the **+ Add new OTP ("one time password") token** button to create a new token.

3.2 Select Hardware Token

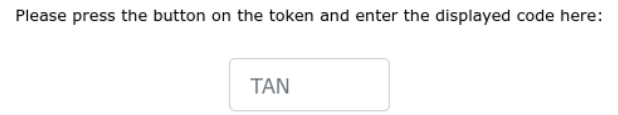
Click on the **Hardware token** button to create a new hardware token.

4 Add a New Hardware Token

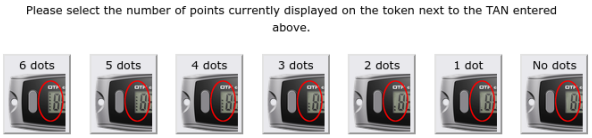
Please pick up the token given to you by the service counter now. On the back of the token is the ID of your token outlined here in red.



Please enter this ID into the input field **token id** and confirm with **Submit**.



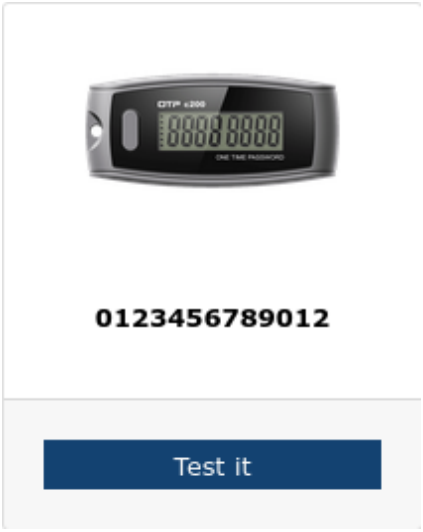
Then press the button on your token and enter the code shown there, outlined in red here, into the **TAN** input field.



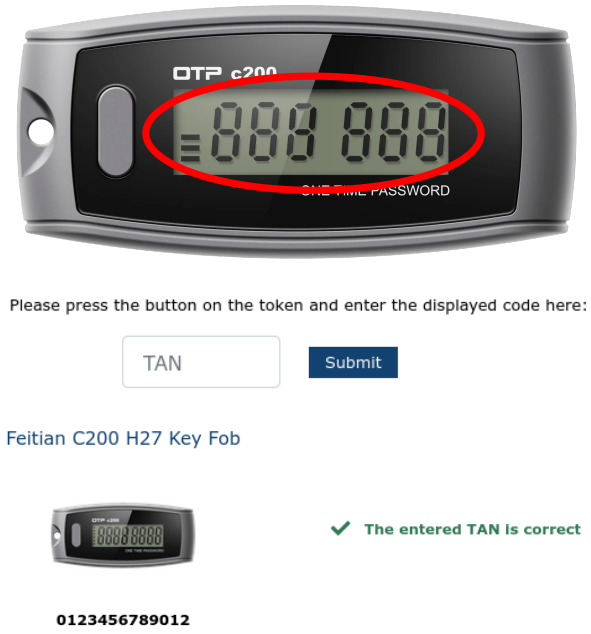
Right after that, you still click the image that shows the same number of dashes as your token. The dashes on the token are highlighted here in red, in the picture on the left the token shows e.g. three dashes.

If you are back on the overview page, then the registration of the token has been completed successfully. In case of an error, a corresponding message will be displayed in your browser. In this case, please try it 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 Hardware Token



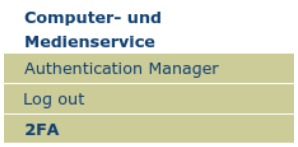
Now please check the functionality of your new hardware token by clicking on the button **Test it**.



Then please press the button on your token and enter the code shown there, outlined here in red, into the input field **TAN**. Please confirm your entry with **ENTER** or by clicking on **Submit**. The number of dashes displayed does not matter in the verification process.

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.