

Zwei-Faktor-Authentifizierung (2FA) - Hardwaretoken

5. Dezember 2022

1 Vorwort

Was ist 2FA? 2FA bedeutet, zusätzlich zum üblichen Passwort-Login als weitere Sicherung einen zweiten Faktor zu verwenden, z.B. Einmalpasswörter (ähnlich einer TAN).

Für sicherheitskritische Anwendungsbereiche wird bereits seit längerem 2FA empfohlen, z.B. vom Bundesamt für Sicherheit in der Informationstechnik. Im Bankwesen wurde sie 2018 verpflichtend eingeführt. Auch die Stiftung Warentest empfiehlt, 2FA für möglichst viele Webdienste zu nutzen.

Einmalpasswörter können einfach und unkompliziert über eine App (auf dem Smartphone oder Tablet) erzeugt werden. In Sonderfällen können sogenannte Hardware-Token zur Verfügung gestellt werden (im Schlüsselanhängerformat erhältlich).

2 Vorbereitung

An der HU wird der 2. Faktor mittels TANs umgesetzt, die Mitarbeitende über eine App auf einem mobilen Endgerät oder per sogenanntem Hardwaretoken generieren können. Sie bekommen einen Hardwaretoken nach zuvor durchgeführter

Berechtigungsprüfung (Überprüfung auf Mitarbeitenden-Status) an den Servicetheken der Benutzerberatung in Adlershof oder im Grimm-Zentrum persönlich überreicht. Bitte informieren Sie sich vorab über die Standorte und Öffnungszeiten der [Servicetheken](https://www.cms.hu-berlin.de/de/dl/oecap/locations) (<https://www.cms.hu-berlin.de/de/dl/oecap/locations>).

Die Berechtigungsprüfung wird durch Vorlage eines gültigen, amtlichen Lichtbildausweises durchgeführt.

Sie benötigen ebenfalls einen gültigen HU-Mitarbeiter-Account. Sollten Sie keinen haben oder dieser nicht mehr nutzbar sein, wenden Sie sich bitte zuvor an die [Benutzeranmeldung](https://www.cms.hu-berlin.de/de/dl/beratung/anmeld_html) (https://www.cms.hu-berlin.de/de/dl/beratung/anmeld_html).

3 HU Authentifizierungsmanager

Öffnen Sie den [HU Authentifizierungsmanager](https://hu.berlin/2FA) (<https://hu.berlin/2FA>) im Browser bzw. nutzen Sie



[PDF-Anleitung](#) (PDF, 622 KB) zur 2FA-Einrichtung mittels Softwaretoken
[Video-Anleitung](#) zur 2FA-Einrichtung mittels Softwaretoken
[Video-Anleitung](#) zur 2FA-Einrichtung mittels Hardwaretoken

Softwaretoken sind ökologisch und ökonomisch nachhaltiger als Hardwaretoken. Hardwaretoken unterliegen einem physischen Lebenszyklus, d.h., sie müssen bestellt, geliefert, verteilt und wieder entgegengenommen und entsorgt werden. Hardwaretoken enthalten Batterien, die ebenfalls eine eigene Lebensdauer haben. Kurzum: mit Hardwaretoken entsteht ein erheblicher Mehraufwand, der mit Softwaretoken nicht entsteht. Daher empfiehlt die HU sowohl aus Sicht ökologischer Nachhaltigkeit als auch aus ökonomischer Sicht die Nutzung von Software-Token.

[Zweiten Faktor im 2FA-Portal einrichten](#)

Bitte gehen Sie zum Starten des eigentlichen Authentifizierungsmanager auf **Zweiten Faktor im 2FA-Portal einrichten**. Die Anmeldung erfolgt über den zentralen HU Single-Sign-On (SSO) Service. Sie benötigen Ihren HU-Account und das zugehörige Passwort.

Der Authentifizierungsmanager stellt auf der Startseite eine Übersicht der Ihnen zugeordneten Token dar. Initial sollten Sie keine zugeordneten Token besitzen.

3.1 Neues Token hinzufügen

Ihre Token

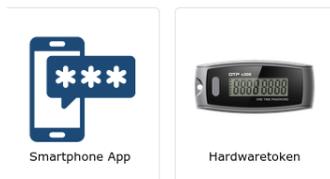
+ Neues OTP („One-Time-Password“)-Token hinzufügen

Sie haben aktuell keine Token aktiviert

Klicken Sie auf die Schaltfläche **+ Neues OTP („One-Time-Password“)-Token hinzufügen**, um ein neues Token anzulegen.

3.2 Hardwaretoken auswählen

Neues OTP ("One-Time-Password")-Token hinzufügen



Klicken Sie auf die Schaltfläche des **Hardwaretokens**, um ein neues Hardwaretoken anzulegen.

4 Neues Hardwaretoken hinzufügen



Bitte die Token ID eingeben (finden Sie auf der Rückseite des Tokens):

Token ID

Bitte nehmen Sie jetzt das von der Servicetheke ausgehängigte Token zur Hand. Auf der Rückseite des Tokens befindet sich die hier rot umrandete ID Ihres Tokens.

Bitte geben Sie diese ID in das Eingabefeld **Token ID** ein und bestätigen Sie die Eingabe mit **Abschicken**.



Bitte drücken Sie den Knopf auf dem Token und geben den dort angezeigten Code hier ein:

Anschließend drücken Sie bitte den Knopf auf Ihrem Token und geben den dort angezeigten, hier rot umrandeten Code in das Eingabefeld **TAN** ein.



Bitte wählen Sie nun die aktuell auf dem Token neben der oben eingegebenen TAN angezeigte Anzahl von Punkten.

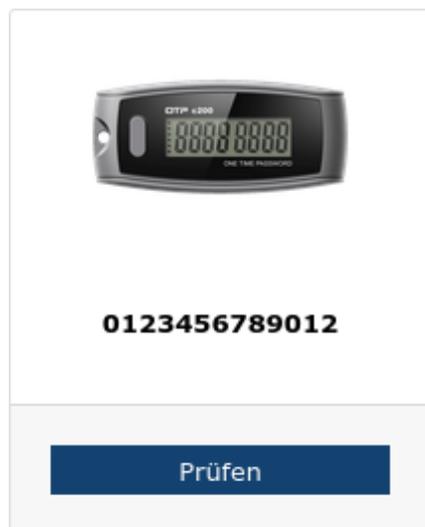


Direkt danach klicken Sie noch das Bild an, das die gleiche Anzahl an Strichen zeigt wie Ihr Token. Die Striche auf dem Token sind hier rot hervorgehoben, in der Abbildung links zeigt der Token z.B. drei Striche.

Wenn Sie wieder auf der Übersichtseite sind, dann ist die Registrierung des Tokens erfolgreich abgeschlossen. Im Fehlerfall wird Ihnen eine entsprechende Nachricht

im Browser angezeigt, bitte versuchen Sie es in diesem Fall noch einmal mit einer anderen TAN. Falls der Fehler wiederholt auftreten sollte, wenden Sie sich bitte an die [Benutzerberatung des CMS \(cms-benutzerberatung@hu-berlin.de\)](mailto:cms-benutzerberatung@hu-berlin.de).

5 Verifizierung Ihres neuen Hardwaretokens



Bitte überprüfen Sie jetzt noch die Funktionalität Ihres neuen Hardwaretokens und gehen dazu auf den Button **Prüfen**.



Anschließend drücken Sie bitte den Knopf auf Ihrem Token und geben den dort angezeigten, hier rot umrandeten Code in das Eingabefeld **TAN** ein. Bitte bestätigen Sie Ihre Eingabe mit **ENTER** oder durch Klick auf **Abschicken**. Die Anzahl der angezeigten Striche spielt bei der Prüfung keine Rolle.

Bitte drücken Sie den Knopf auf dem Token und geben den dort angezeigten Code hier ein:

Feitian C200 H27 Schlüsselanhänger



0123456789012

✓ Eingebene TAN ist korrekt

Wird Ihnen abschließend die Erfolgsmeldung **Eingegebene TAN ist korrekt** angezeigt, dann haben Sie die Funktionalität Ihres neuen Hardwaretokens erfolgreich geprüft.

6 Abmeldung

Computer- und
Medienservice

Authentifizierungsmanager

Abmelden

2FA

Bitte melden Sie sich nach der Benutzung des HU Authentifizierungsmanager mit Klick auf **Abmelden** ab und schließen Sie Ihren Browser, um alle Internet-Aktivitäten sicher zu beenden.