HUMBOLDT-
UNIVERSITÄT
ZU BERLIN

Zwei-Faktor-Authentisierung (2FA) - Softwaretoken

16. 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).

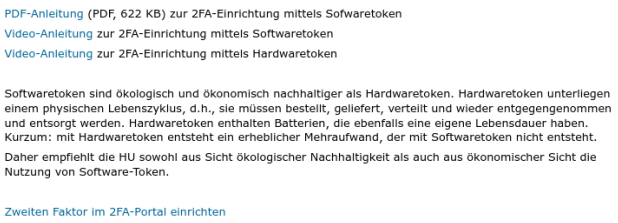
2 Vorbereitung

An der HU wird der 2. Faktor mittels TANs umgesetzt, die Mitarbeitende über eine App auf einem mobilen Endgerät oder per sogenanntem Handwaretoken generieren können. Die App kann kostenlos auf dem Smartphone oder Tablet

installiert werden und ist dann ohne Internetverbindung oder Mobilfunknetz nutzbar. Die HU empfiehlt dieses Verfahren. Im Folgenden wird beschrieben, wie Sie zu einem Software-Token der HU kommen. Als App wird dabei exemplarisch *Aegis Authentificator* genommen. Der Import des Softwaretokens funktioniert bei den anderen empfohlenen Apps ähnlich.
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).

3 HU Authentifizierungsmanager

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



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

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

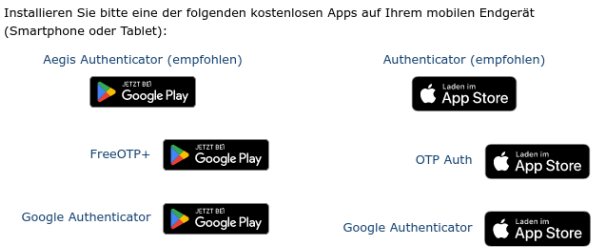
3.2 Softwaretoken auswählen

Klicken Sie auf die Schaltfläche der **Smartphone App**, um ein neues Softwaretoken anzulegen.

4 Neues Softwaretoken hinzufügen

Jetzt benötigen Sie für die weiteren Schritte Ihr mobiles Endgerät (Smartphone oder Tablet). Die folgende Seite enthält Links zu getesteten Apps und auch schon Ihr neues Software-Token in Form eines QR-Codes.

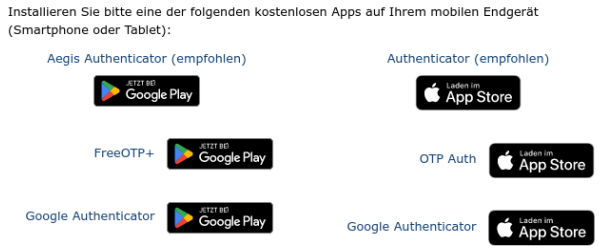
4.1 Installation der App



Falls Sie bereits eine App zum Erzeugen von OTP Token auf Ihrem Smartphone installiert haben, fahren Sie direkt mit Schritt 4.2 fort. Anderenfalls installieren Sie bitte, je nach Endgeräte-Typ z.B.

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

von GooglePlay bzw.



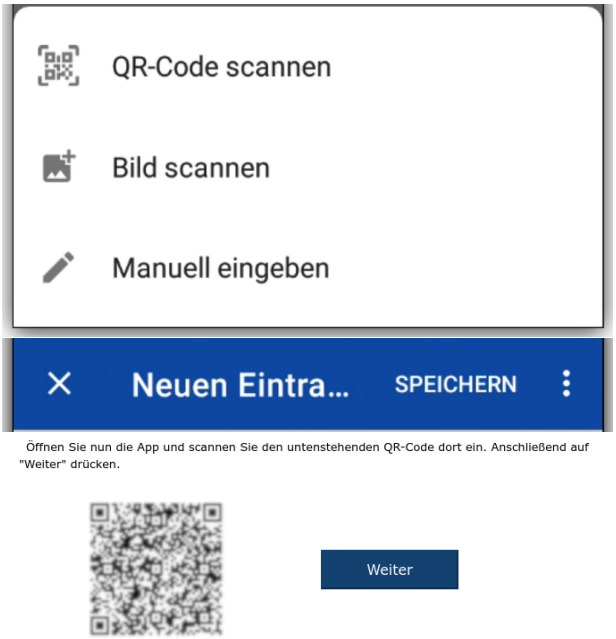
- Authenticator: https://apps.apple.com/app/authenticator/id766157276 oder
- Google Authenticator: https://apps.apple.com/app/google-authenticator/id388497605

aus dem AppStore.
Die Installation der App sollte jeweils kostenlos möglich sein.

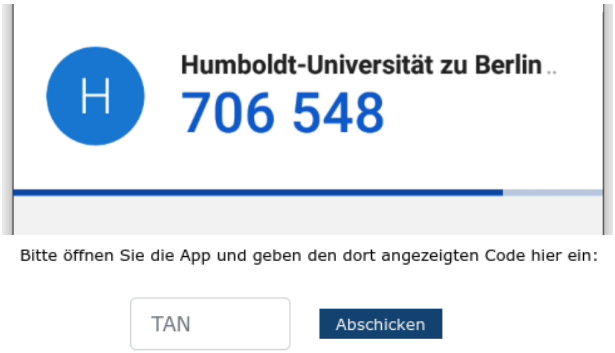
4.2 Software-Token importieren

Öffnen Sie bitte die (zuvor installierte) Authenticator-App auf Ihrem Endgerät. Hier wird beispielhaft *Aegis Authenticator* verwendet.

Bitte drücken Sie auf **+**, um einen Code hinzufügen.



Bitte tippen Sie auf dem mobilen Entgerät auf **QR-Code scannen**, um den auf der Webseite angezeigten QR-Code hinzufügen. Fokussieren Sie mit der Kamera Ihres Smartphones den im Browser angezeigten QR-Code. Hat ihr mobiles Endgerät den QR-Code erkannt, erscheint das Fenster **Neuen Eintra...** auf Ihrem mobilen Endgerät. Tippen Sie dort bitte auf **Speichern**. Anschließend könnten Sie auf der Webseite auf **Weiter** klicken.

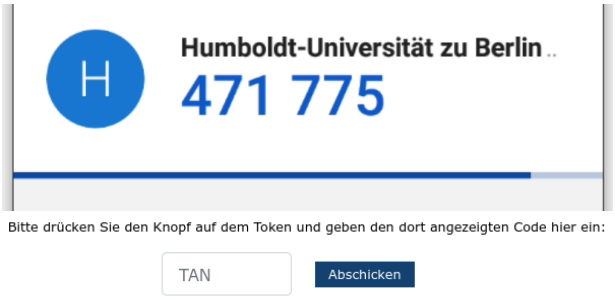


Geben Sie auf der Webseite nun die auf Ihrem mobilen Endgerät angezeigte TAN, in diesem Fall **706548**, in das Eingabefeld **TAN** ein und bestätigen Sie mit **Abschicken**.

Wenn Sie danach 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).

5 Verifizierung Ihres neuen Softwaretokens

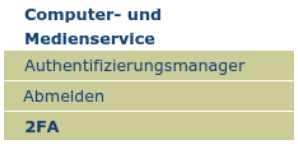
Bitte überprüfen Sie jetzt noch die Funktionalität Ihres neuen Softwaretokens und gehen dazu auf den Button **Prüfen**.



Nehmen Sie nun bitte wieder Ihr mobiles Endgerät zur Hand und öffnen Sie die Authentifizierungsapp. Geben Sie auf der Webseite nun die auf Ihrem mobilen Endgerät angezeigte TAN, in diesem Fall **471775**, in das Eingabefeld **TAN** ein und bestätigen Sie mit **Abschicken**.

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

6 Abmeldung



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.