Einführung Zwei-Faktor-Authentifizierung (2FA)

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 Smartphone-App erzeugt werden, oder durch sogenannte Hardware-Token (im Schlüsselanhängerformat erhältlich).

Wie erhalte ich einen zweiten Faktor?

An der HU wird der 2. Faktor mittels TANs umgesetzt, die Mitarbeitende über eine App auf einem mobilen Endgerät 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. Alternativ können die TANs mit einem Hardware-Token generiert werden, der in Sonderfällen beantragt werden kann.

Im Folgenden wird beschrieben, wie Sie zu einem Software-Token der HU kommen.

HU Software-Token

1. HU Authentifizierungsmanager starten

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

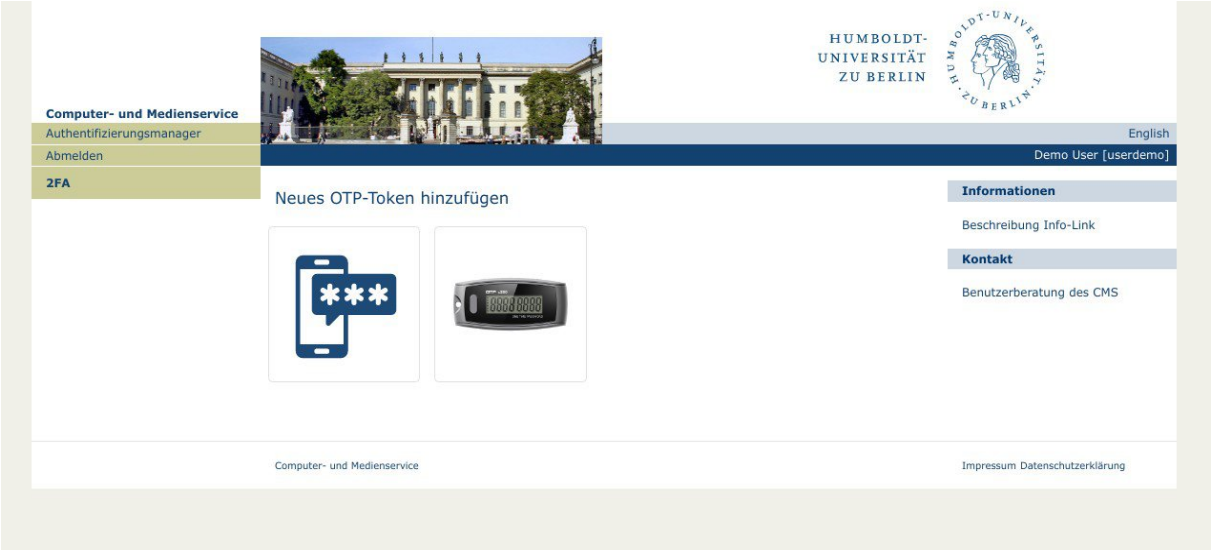
Die Anmeldung erfolgt über den HU zentralen Singe-Sign-On (SSO) Service. Sie benötigen Ihren HU-Account und das zugehörige Passwort.

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

Authentifizierungsmanager: Startseite (initial)

2. Neues Token hinzufügen

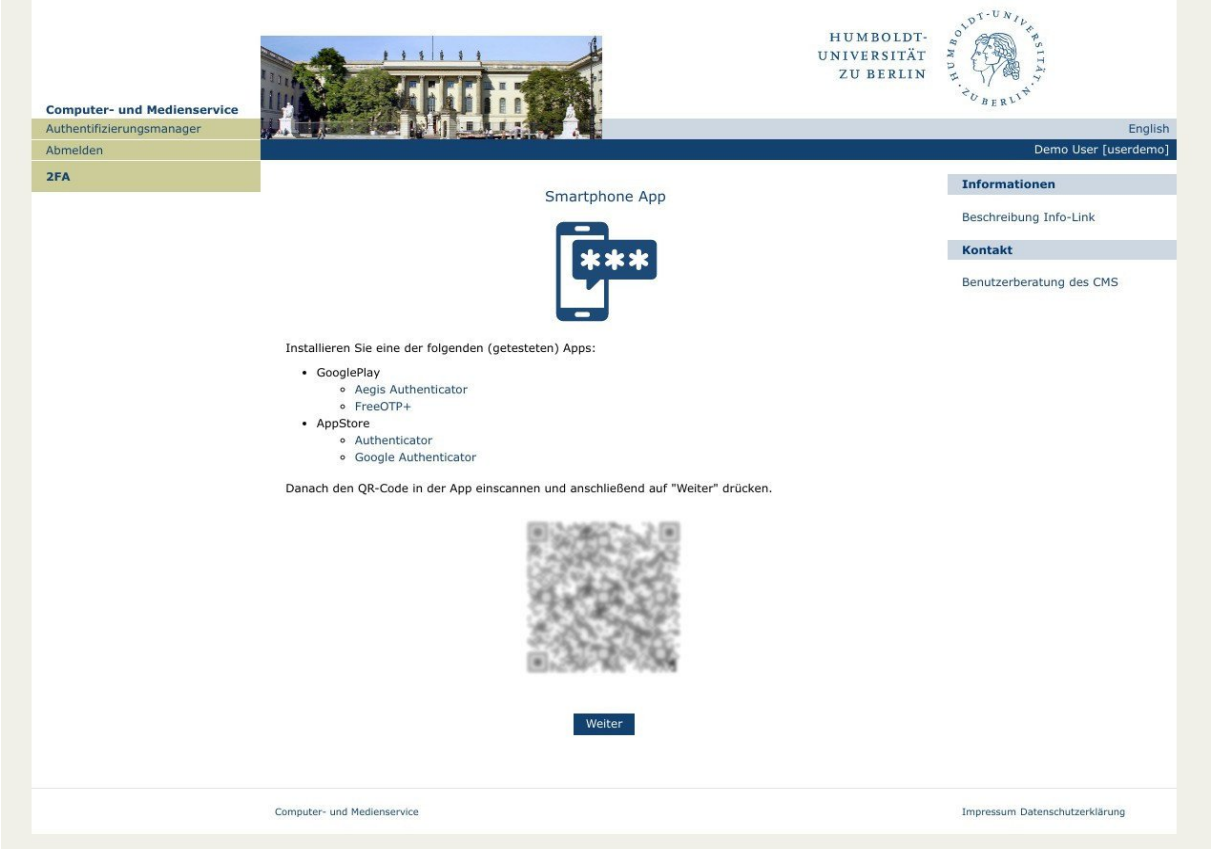
Klicken Sie auf die Schaltfläche ‚+ Neues OTP Token hinzufügen', um ein neues Token anzulegen. Auf der folgenden Seite klicken Sie auf die Graphik mit dem Handy und den Sternchen, siehe Abbildung.



Authentifizierungsmanager: Neues OTP Token hinzufügen

3. Neues Software-Token hinzufügen

Spätestens jetzt benötigen Sie für die weiteren Schritte Ihr Smartphone. Die folgende Seite enthält Links zu getesteten Apps für Ihr Smartphone und auch schon Ihr neues Software-Token in Form eines QR-Codes, siehe Abbildung.



Authentifizierungsmanager: Neues Software-Token

3.1 Smartphone-App

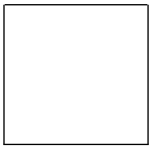
Falls Sie bereits eine App zum Erzeugen von OTP Token auf Ihrem Smartphone installiert haben, fahren Sie direkt mit Schritt 3.2 fort.

Anderen Falls installieren Sie bitte, je nach Smartphone-Typ die App FreeOTP+ oder Aegis Authenticator von GooglePlay bzw. Google Authenticator oder Authenticator aus dem AppStore. Die Installation der App sollte jeweils kostenlos möglich sein.

3.2 Software-Token importieren

Öffnen Sie bitte die (zuvor installierte) Authenticator App auf Ihrem Smartphone. Wählen Sie in den (Import) Einstellungen die Funktion ‚QR-Code scannen' und fokussieren Sie Ihr Smartphone auf den im Browser angezeigten QR-Code.

Als Ergebnis sollten Sie nun Ihren HU Token in der Liste der Token sehen:



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

Da die Generierung des Einmalpasswortes zeitgesteuert auf Basis des Tokens erfolgt, ist jedes Einmalpasswort in genau einem Zeitintervall von 30 Sekunden Länge gültig. Die

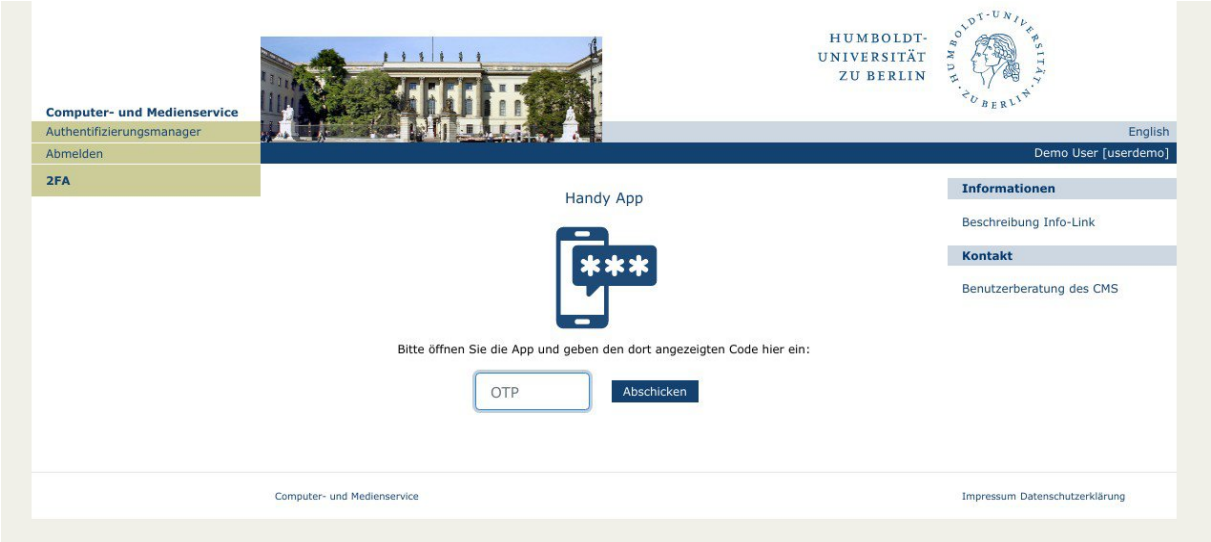
aktuelle Gültigkeitsdauer des Einmalpasswortes wird Ihnen durch ein Bild vor dem Code angezeigt. Das aktuelle Einmalpasswort wird generiert bzw. angezeigt, wenn Sie die Zeile in der Liste antippen.

Das Einmalpasswort besteht aus 6 Ziffern. Für die Generierung ist keine Internet- und auch keine Verbindung ins Mobilfunk-Netz nötig.

Falls Sie weitere Geräte für die Generierung Ihres Einmalpasswortes nutzen möchten, kann der selbe QR-Code auch auf weiteren Geräten mit einer entsprechenden Anwendung gescannt werden, z.B. Tablets.

4. Verifizierung Ihres neuen Software-Tokens

Nachdem Sie obiges Token in Ihrer Token-Liste auf dem Smartphone sehen, gehen Sie mit dem Button ‚Weiter' auf die nächste Seite, siehe Abbildung.



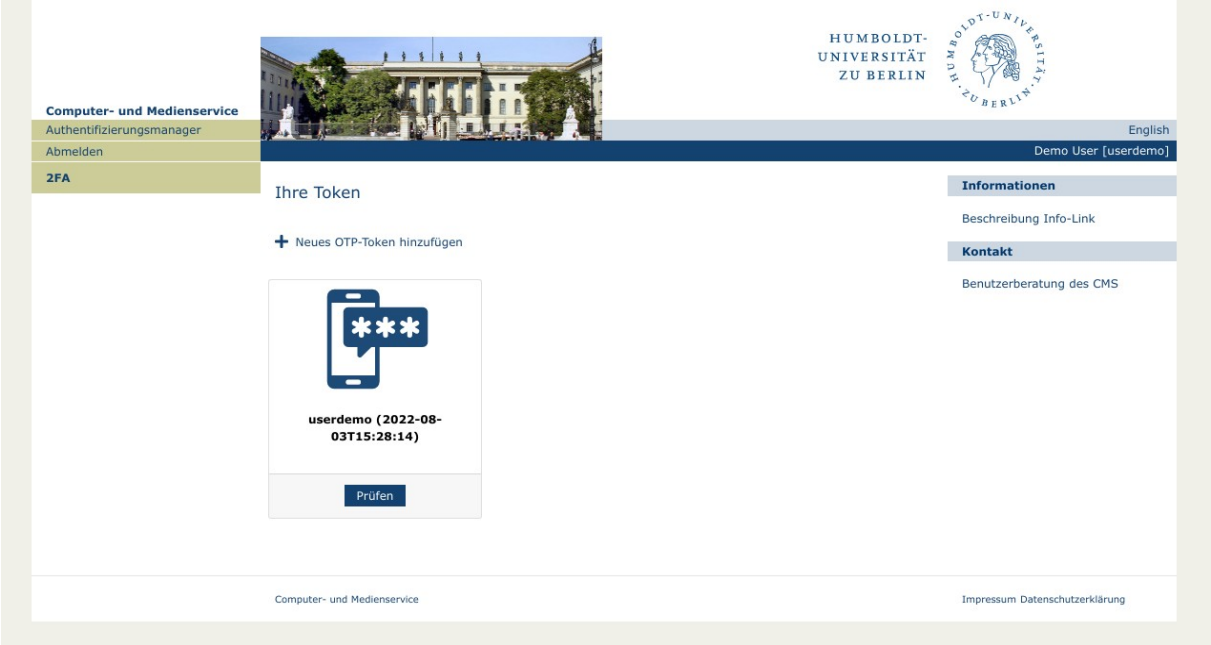
Authentifizierungsmanager: Verifizieren des neuen Software-Tokens

Lassen Sie sich nun von Ihrer Smartphone-App das aktuelle Einmalpasswort (Code: 6 Ziffern) anzeigen und geben sie es in das Eingabefeld ein. Achten Sie darauf, dass es noch gültig ist, wenn Sie die Eingabe beendet haben.

Tipp: Ist der in Ihrem Smartphone angezeigte Code nur noch wenige Sekunden gültig, warten Sie ein wenig, bis Ihnen die App einen neuen Code anzeigt.

Nach der Eingabe des Codes im Browser drücken Sie ‚Enter' oder den Button ‚Abschicken'.

War die Validierung des Codes erfolgreich, wird Ihnen im Browser jetzt die Startseite des Authentifizierungsmanagers mit Ihrem neuen Software-Token angezeigt, siehe Abbildung.



Authentifizierungsmanager: Erfolgreich erstellter, neuer Software-Token

Benannt ist das Token mit Ihrem HU-Account und in Klammern dahinter der Zeitpunkt der Erstellung.

Im Fehler-Fall wird Ihnen eine entsprechende Nachricht im Browser angezeigt. Bitte versuchen Sie es erneut ab Schritt 1. - Falls der Fehler wiederholt auftreten sollte, wenden Sie sich bitte an die Benutzerberatung des CMS:

cms-benutzerberatung@hu-berlin.de