

Selbstregistrierung Zwei-Faktor-Authentifizierung (2FA)

Allgemein

Als Lehrbeauftragte*r der Hochschule Fulda verfügen Sie in der Regel über die zwei Rollen „Lehrbeauftragte“ und „Prüfer/-in“. Die Rolle „Prüfer/-in“ ist mit einem zweiten Sicherheitsfaktor abgesichert, um die Sicherheit des Zugriffs gegen Missbrauch zu schützen.

Den zweiten Sicherheitsfaktor können Sie selbstständig über die Selbstregistrierung einrichten.

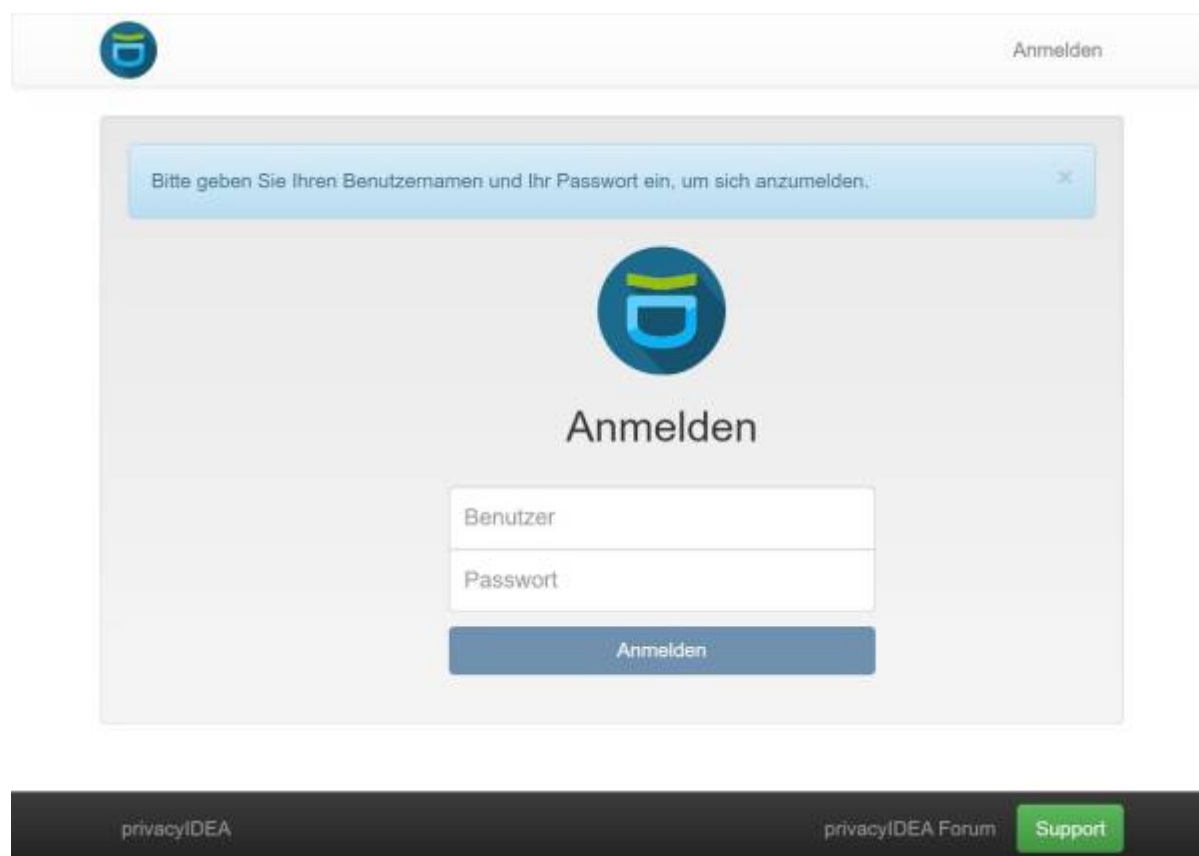
Installieren Sie dazu bereits vorher ein App zur Zwei-Faktor-Authentifizierung auf Ihrem Smartphone (z.B. [2FAS](#) oder [privacyIDEA](#)).

Selbstregistrierung Zwei-Faktor-Authentifizierung

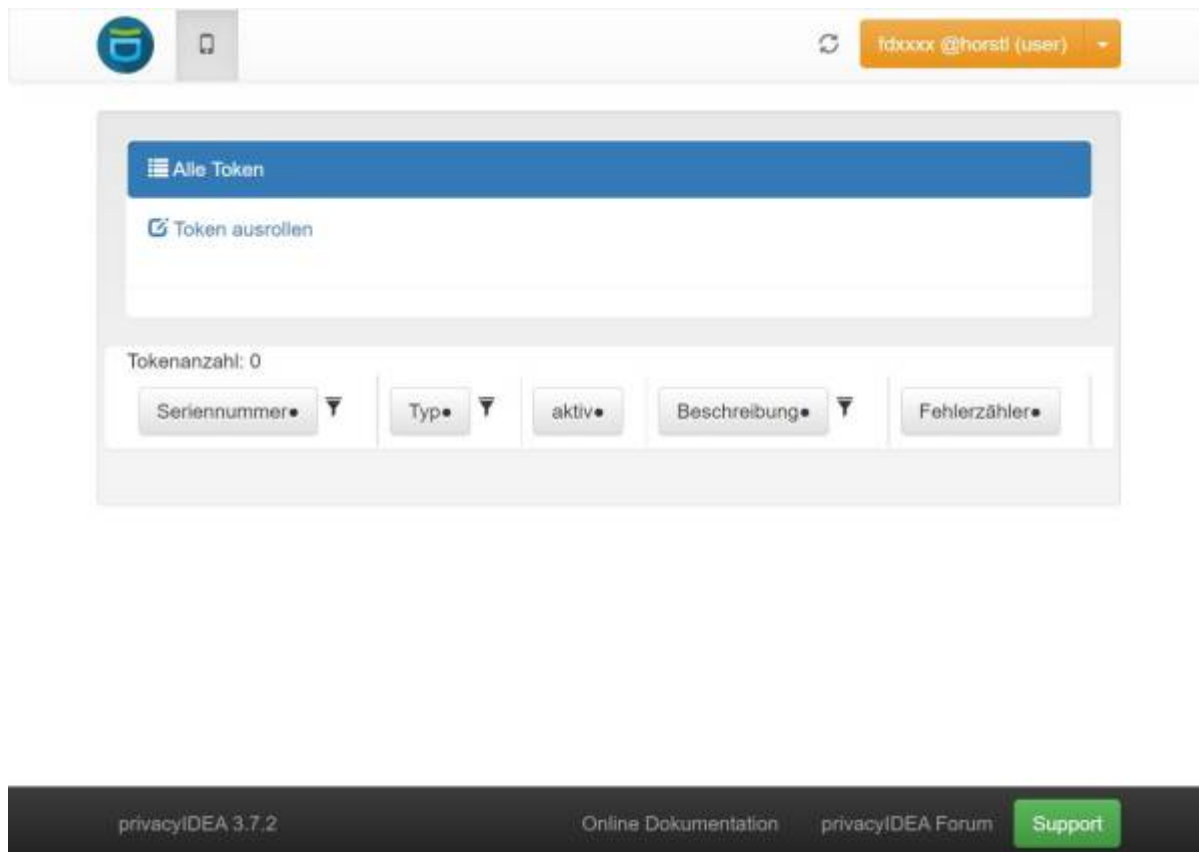
Anmeldung

Das System zur Selbstregistrierung des zweiten Sicherheitsfaktors erreichen Sie über <https://privacyidea.rz.hs-fulda.de>. Beachten Sie bitte, dass das System nur aus dem Hochschulnetzwerk (LAN oder VPN) erreichbar ist.

Auf der Anmeldeseite können Sie sich mit Ihrem FD-Benutzer anmelden.






Anschließend erhalten Sie eine Übersicht Ihrer registrierten Tokens (zweiter Sicherheitsfaktor), von denen noch keine vorhanden sein sollten.



Erzeugen eines Tokens zur Zwei-Faktor-Authentifizierung

Im nächsten Schritt können Sie über „**Token ausrollen**“ sich Ihren eigenen Token erzeugen. Die Einstellungen sind bereits mit den empfohlenen Standardeinstellungen vorbelegt, sodass Sie nur noch auf „**Token ausrollen**“ klicken brauchen.

Die Funktion „**Token ausrollen**“ ist nur für Lehrbeauftragte möglich.
Den Beschäftigten werden Hardware-Token (Yubikey) ausgegeben.

tdxxxxx @horstl (user)

Alle Token

Token ausrollen

Neuen Token ausrollen

TOTP: Zeitbasiertes Einmalpasswort.

Der TOTP-Token ist ein zeitbasierter Token. Sie können den geheimen OTP-Schlüssel hier einfügen oder den Server einen Schlüssel generieren lassen. Diesen können Sie in Ihre Smartphone-App wie Google Authenticator oder FreeOTP importieren, indem Sie den QR-Code scannen.

Tokendaten

☒ **OTP-Schlüssel auf dem Server erzeugen**

Der Server erzeugt den geheimen Schlüssel und es wird ein QR-Code angezeigt, den Sie mit einer Smartphone-App scannen können.

OTP-Länge

6

Der Google Authenticator unterstützt lediglich OTP Länge 6.

Zeitschritt

30

seconds.

Hash-Algorithmus

sha256

Der Google Authenticator unterstützt lediglich den SHA1-Algorithmus.

Token ausrollen

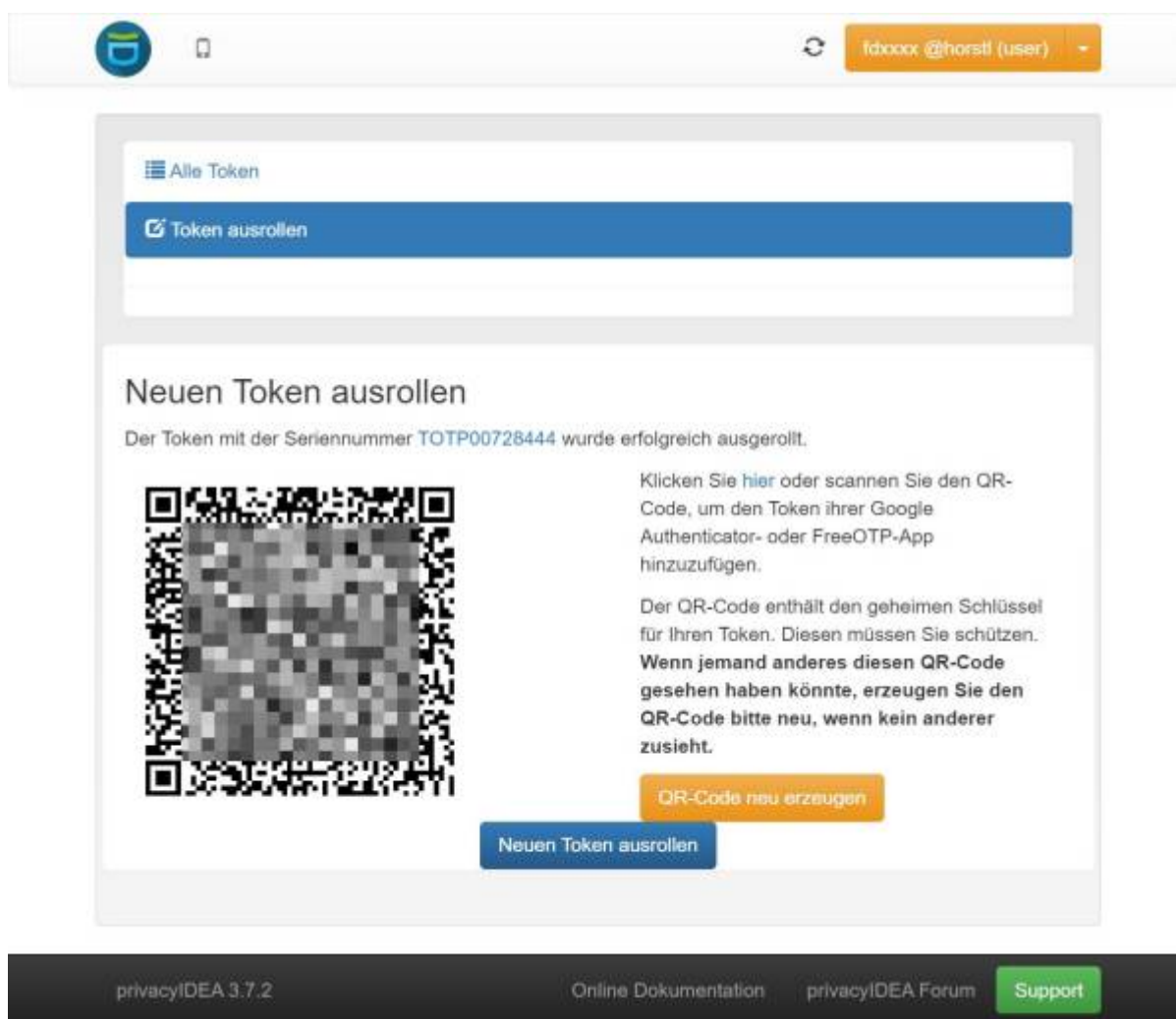
privacyIDEA 3.7.2

Online Dokumentation

privacyIDEA Forum

Support

Anschließend erhalten Sie einen QR-Code angezeigt. Der QR-Code enthält den geheimen Schlüssel für Ihren Token.



Öffnen Sie die bereits installierte App (z.B. [2FAS](#) oder [privacyIDEA](#)) zur Zwei-Faktor-Authentifizierung auf Ihrem Smartphone und importieren dort den Token über das Scannen des QR-Codes (hierzu muss der App der Zugriff auf die Kamera erlaubt werden).

Folgen Sie hierzu der Anleitung der ausgewählten App zur Zwei-Faktor-Authentifizierung.

From:

<https://doku.rz.hs-fulda.de/> - **Dokumentation des Rechenzentrums**

Permanent link:

https://doku.rz.hs-fulda.de/doku.php/docs:horstl_intern:tan:privacyidea-regstrierung

Last update: **24.01.2023 09:30**

