

Selbstregistrierung Zwei-Faktor-Authentifizierung (2FA)

Allgemein

Als Lehrbeauftragte*r der Hochschule Fulda verfügen Sie in horstl in der Regel über die zwei Rollen „Lehrbeauftragte“ und „Püfer/-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 selbständig über die Selbstregistrierung einrichten.

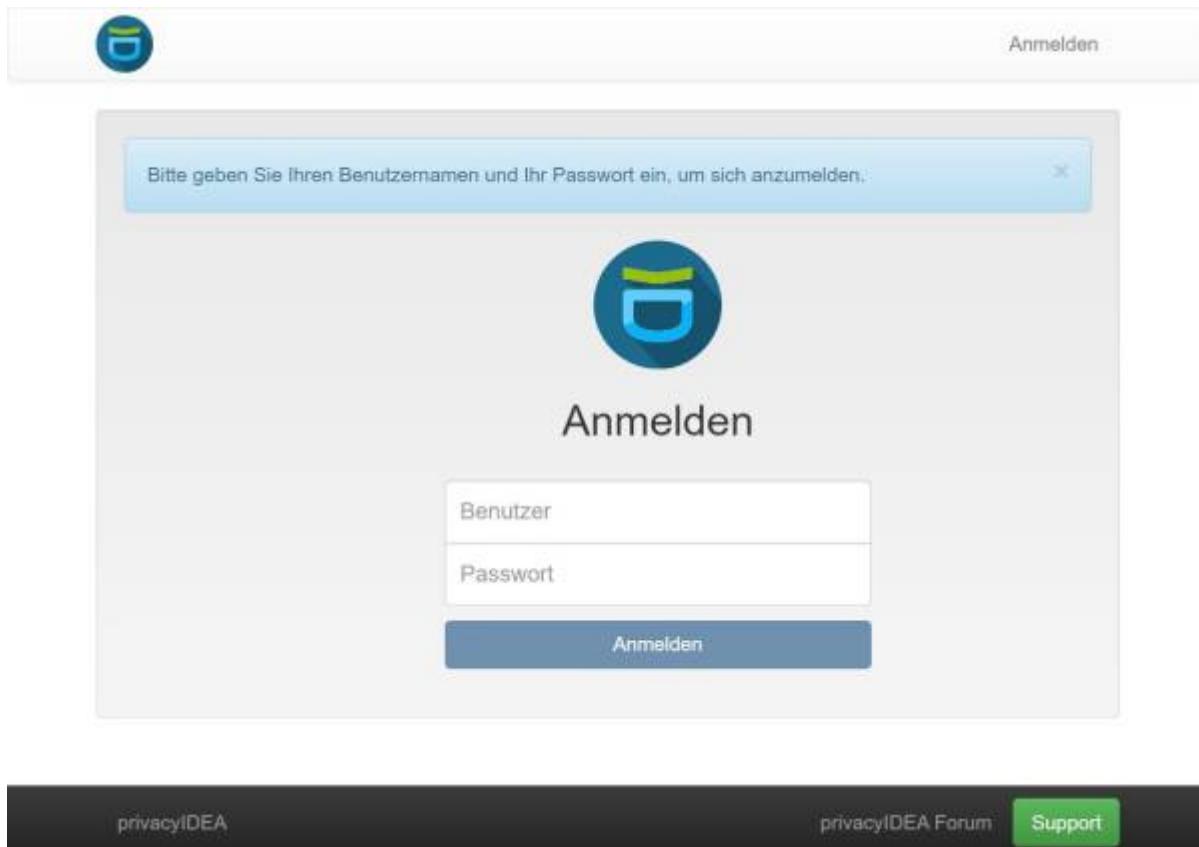
Installieren Sie dazu bereits vorher eine App zur Zwei-Faktor-Authentifizierung auf Ihrem Smartphone (z.B. [2FAS](#) oder [privacyIDEA](#)).

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.



Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich anzumelden.

Anmelden

Benutzer

Passwort

Anmelden

privacyIDEA

privacyIDEA Forum

Support

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-Tokens (Yubikey) ausgegeben.

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.

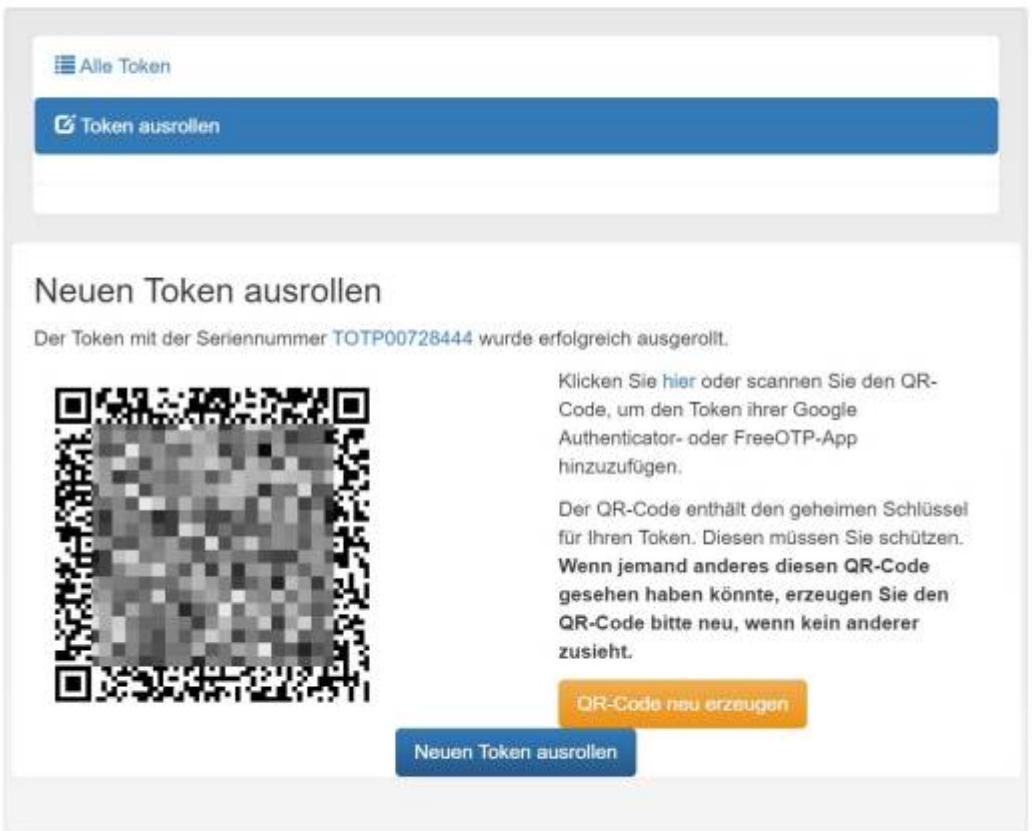
Hash-Algorithmus

sha256

Der Google Authenticator unterstützt lediglich den SHA1-Algorithmus.

Token ausrollen

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



The screenshot shows the privacyIDEA web interface. At the top, there is a navigation bar with a logo, a search bar, and a user icon labeled "tdoxx @horstl (user)". Below the navigation bar, there are two buttons: "Alle Token" and "Token ausrollen". The "Token ausrollen" button is highlighted with a blue background and white text. The main content area has a title "Neuen Token ausrollen" and a sub-instruction "Der Token mit der Seriennummer TOTP00728444 wurde erfolgreich ausgerollt.". To the left of the text is a large QR code. To the right, there are two paragraphs of text: one explaining how to use the QR code with a Google Authenticator or FreeOTP app, and another cautioning against sharing the QR code. Below the text are two buttons: "QR-Code neu erzeugen" (orange) and "Neuen Token ausrollen" (blue). At the bottom of the interface, there is a footer with links: "privacyIDEA 3.7.2", "Online Dokumentation", "privacyIDEA Forum", and "Support".

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/> - **Rechenzentrum**

Permanent link:
<https://doku.rz.hs-fulda.de/doku.php/docs:horstl:tan:privacyidea-regstrierung>

Last update: **20.10.2025 09:26**

