# Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung ist die anerkannte und empfohlene Methode zur Absicherung von Remote-Zugriffen auf Netzwerke und Web-Applikationen. Aktuelle Lösungen verwenden als zweiten Faktor meist sogenannte One Time Passwords bzw. Passcodes (OTP) oder Einmalpasswörter. Diese werden für jeden spezifischen Anmeldevorgang generiert und können nur zur einmaligen Authentifizierung genutzt werden.

Die Hochschule Fulda setzt die 2-Faktor-Authentifizierung für horstl-Benutzer*innen mit umfangreichen Rechten ein. Alle Beschäftigte erhalten einen **Hardware-Token (Yubikey)**. Für Lehrbeauftragte ist ein **App-Token (Smartphone-App)** vorgesehen.

## Ausgabe Hardware-Token (Yubikey) für Beschäftigte

Allen Beschäftigten, mit abgesicherten Rollen durch einen zweiten Sicherheitsfaktor, wird ein Hardware-Token zur TAN-Generierung automatisch durch das Rechenzentrum zugestellt und muss nicht beantragt werden.

Die Abfrage der TAN erscheint nach dem Login mit Ihrem FD-Benutzer.
Hierzu stecken Sie Ihren persönlichen Hardware-Token in den Rechner ein und berühren die Tastfläche des Sticks. Dadurch wird automatisch eine TAN eingegeben und die Anmeldung fortgesetzt.

Falls Sie die TAN-Eingabe abbrechen, stehen Ihnen die besonders schützenswerten Rollen (z.B. Prüfer-/in, Prüfungsausschuss, Prüfungsplaner-/in, Department-Administrator-/in, …) in horstl nicht zur Verfügung.


## Anleitung zur Einrichtung und Installation des App-Token (Smartphone) für Lehrbeauftragte

Für die Installation einer Software zur Zwei-Faktor-Authentifizierung ist es erforderlich, aus dem App-Store Ihres Betriebssystems eine spezielle Anwendung auf Ihrem Smartphone herunterzuladen. Die Hochschule Fulda empfiehlt hier die Nutzung der kostenfreien Apps **2FAS Authenticator** oder **privacyIDEA Authenticator**.

 Installationsanleitung: 2FAS Authenticator

 Installationsanleitung: privacyIDEA

Anschließend kann ein Token über die Selbstregistrierung erzeugt und in die installierte App importiert werden.

 Selbstregistrierung Zwei-Faktor-Authentifizierung (2FA)

## Kontakt

Für Fragen zur Zwei-Faktor-Authentifizierung stehen Ihnen die Kolleg*innen des Rechenzentrum Bereich Service zur Verfügung. Gerne können Sie eine E-Mail an it-support@rz.hs-fulda.de schreiben.

## Verlustmeldung

Bitte senden Sie eine E-Mail an it-support@rz.hs-fulda.de, wenn Sie Ihren Hardware-Token (Yubikey) oder Ihr Smartphone (bei Verwendung einer App) verloren haben. Der Token oder das Smartphone wird gesperrt und eine Neuausgabe in die Wege geleitet bzw. Neuregistrierung ermöglicht.

## Zusätzliche Informationen zum TAN-Verfahren

Die Hochschule Fulda setzt zur Nutzung der mit Zwei-Faktor-Authentifizierung aktivierten Diensten, folgende TAN-Verfahren ein.

### Yubico One-time Password

Jeder Yubikey enthält ab Werk bereits einen einzigartigen, geheimen Schlüssel, über den auf

Knopfdruck dynamisch ein Passwort generiert werden kann. Dieser Schlüssel wird in unserem Fall individuell neu geschrieben und per Schlüsselfile dem Authentifizierung-Server mitgeteilt. Dieser Mechanismus funktioniert ähnlich wie alle üblichen OTP Verfahren: Ein Zähler im Yubikey und auf dem Authentifizierung-Server wird bei jedem Login inkrementiert. Beide Seiten berechnen einen Soll-Schlüssel und vergleichen diesen miteinander. Der Hauptunterschied: Der Key auf dem Yubikey ist fest eingebrannt, kann nicht ausgetauscht werden und eine Authentifizierung ist nur gegenüber einem Authentifizierung-Server möglich.
Dazu kommt noch eine Komfortfunktion, dass der Yubikey das Passwort selbstständig eingibt.

Der YubiKey OTP-Schlüssel besteht aus folgenden Feldern, die mit einem eindeutigen AES-128-Bit-Schlüssel verschlüsselt sind. Das Ergebnis ist eine 32-stellige Modhex-Zeichenfolge, die an eine 12-stellige öffentliche ID angehängt wird.

| Mnemonisch | Byte-Offset | Größe | Beschreibung |
|---|---|---|---|
| uid | 0 | 6 | Private (geheime) ID |
| verwendungCtr | 6 | 2 | Verwendungszähler |
| tstp | 8 | 3 | Zeitstempel |
| sessionCtr | 11 | 1 | Sitzungsnutzungsindikator |
| rnd | 12 | 2 | Zufallszahl |

**Time-based One-time Password (TOTP)**

Zeitbasierte Algorithmen verwenden die Uhrzeit zusammen mit einem privaten Schlüssel um ein Passwort zu generieren. Daher bieten zeitbasierte Einmalpasswörter zusätzliche Sicherheit, denn selbst wenn das herkömmliche Passwort eines Anwenders gestohlen oder kompromittiert wird, kann ein Angreifer ohne das TOTP keinen Zugriff erhalten.
TOTP ist ein anerkannter Standard der Internet Engineering Task Force (IETF).

*TOTP Parameter*

- OTP-Länge = 6 Zeichen
- Zeitschritt = 30 Sekunden
- Hash-Algorithmus = SHA256