TECHNISCHE UNIVERSITÄT DARMSTADT

# Anleitung zur Verwaltung der Zwei-Faktor-Authentifizierung (2FA)

HRZ Hochschulrechenzentrum

## Einleitung

Das HRZ bietet eine zusätzliche Sicherheitsmaßnahme für Ihre TU-ID an: Bisher loggen Sie sich mit Ihrer TU-ID und einem Passwort ein. Zusätzlich zum Passwort kann ein zweites Sicherheitsmerkmal abgefragt werden. Dieses kann ein einmalig gültiger Zahlencode (Einmalpasswort) oder ein physischer Schlüssel sein. Dieser zweite Sicherheitsfaktor wird als „Token“ bezeichnet. Sie können verschiedene Arten von Tokens – wie TAN- oder TOTP-Codes und WebAuthn-Token – in der 2FA-Verwaltung erstellen und nach Bedarf verwalten.

Um Ihren Token einzurichten, benötigen Sie mindestens eines der folgenden Geräte:

1. **Dienstrechner mit eingerichtetem Passwortmanager**
   Verwenden Sie einen Dienstrechner mit einem bereits eingerichteten Passwortmanager wie beispielsweise **KeePassXC** oder **KeePass**. Wenn Sie den Passwortmanager KeePassXC verwenden möchten, finden Sie eine Anleitung auf unserer Webseite rechts unter Links & Downloads.
   Falls Sie KeePassXC noch nicht nutzen, führen Sie idealerweise die Schritte 1 bis 3 vollständig durch, bevor Sie mit der Einrichtung der Zwei-Faktor-Authentifizierung beginnen.
2. **Smartphone mit Authenticator-App**
   Nutzen Sie ein Smartphone mit einer Authenticator-App, z. B. **privacyIDEA Authenticator** oder **Google Authenticator**.
3. **Hardware-Token**
   Alternativ können Sie einen Hardware-Token verwenden. Eine Übersicht über unterstützte Hardware-Token finden Sie in den FAQ.

**Empfehlung:**
Wir empfehlen Ihnen einen TOTP-Token in einem Passwortmanager (wie *KeePassXC*) in Kombination mit einem TOTP-Token auf dem Smartphone via Authenticator-App (wie *privacyIDEA Authenticator*).

**In dieser Anleitung** erklären wir Ihnen die notwendigen Schritte zur Einrichtung der **Zwei-Faktor-Authentifizierung mit dem Smartphone via Authenticator-App *privacyIDEA Authenticator***.

**Hinweis:**
Es ist auch möglich, einen WebAuthn-Token auszurollen und zu verwenden – zum Beispiel mit Hardware-Tokens oder in Kombination mit Windows Hello. So lässt sich der 2. Faktor bequem per Fingerabdruck oder Gesichtserkennung aktivieren.

Weitere Details zu den verschiedenen Tokens und den unterstützten Einmalpasswortverfahren finden Sie auch in den FAQ auf unseren Webseiten.

## Zwei-Faktor-Authentifizierung einrichten und benutzen

### Schritt 1: Anmeldung an der 2FA-Verwaltung

Rufen Sie die 2FA-Verwaltung in einem Browser unter https://login.tu-darmstadt.de/2fa auf. Sie finden diesen Link auch im IDM-Portal (unter „Persönliche Accountverwaltung“ → „Account / Passwort“) und unter „2FA-Verwaltung“ rechts neben der Login-Maske des SSO (Single-Sign-On). Melden Sie sich mit Ihrer TU-ID und dem zugehörigen Passwort an.

Nach dem Aufruf der 2FA-Verwaltung gelangen Sie auf eine **Begrüßungsseite** (Abbildung 1). Klicken Sie dort auf **„Weiter“**, um eine kurze **Einführung** zu erhalten (Abbildung 2).

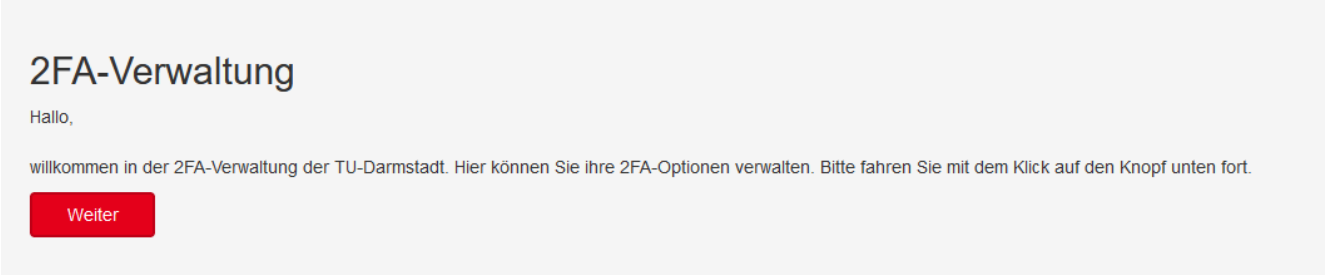


Abbildung 1: Begrüßungsseite

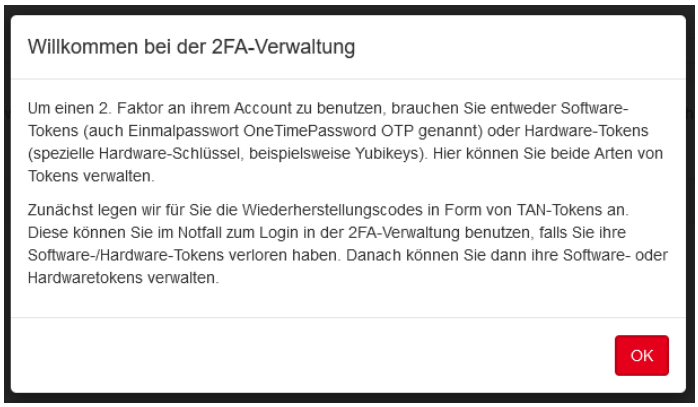


Abbildung 2: Kleiner Erklärungstext

## Schritt 2: Erstellung des Wiederherstellungscodes

Nachdem Sie auf **„OK“** geklickt haben, gelangen Sie zunächst auf eine weitere **Informationsseite** zum Erstellen Ihrer Wiederherstellungscodes (Abbildung 3).


Abbildung 3: Informationsseite

**Wichtig:** Speichern oder drucken Sie Ihre **Wiederherstellungscodes** unbedingt aus!

**Falls Ihre anderen Tokens defekt oder verloren sind** – sei es durch Verlust oder Beschädigung eines Hardware-Tokens oder durch Verlust eines Geräts bzw. zurücksetzen des Betriebssystems bei einem Software-Token –, **benötigen Sie diese Codes zwingend, um sich in die 2FA-Verwaltung einzuloggen. Ohne die Wiederherstellungscodes ist ein Zugriff nicht mehr möglich, und Sie könnten dauerhaft ausgesperrt werden.**

**Was tun bei Verlust meines Tokens?**
Falls Sie Ihren Token trotz größter Sorgfalt verlieren sollten, können Sie wie folgt vorgehen:

- Melden Sie sich mit dem **Wiederherstellungscode**, den Sie bei der Registrierung erstellt haben, in der **2FA-Verwaltung** an.
- Löschen Sie dort den verlorenen oder ungültigen Token.
- Anschließend können Sie in der 2FA-Verwaltung einen neuen Token einrichten.

Nachdem Sie auf **„Weiter“** geklickt haben, wird eine durchnummerierte Liste mit genau **5 Wiederherstellungscodes** generiert, die in Form von einem Einmalpasswort (OTP) dargestellt sind. Jedes Einmalpasswort besteht aus 6 aufeinanderfolgenden Ziffern (Abbildung 4).

Die Wiederherstellungscodes können ausschließlich für den Login in die 2FA-Verwaltung verwendet werden.

Um die Liste auszudrucken, klicken Sie auf den Button „OTP-Liste drucken“.


Abbildung 4: Liste mit generierten Wiederherstellungscodes

Sobald Sie diesen Schritt erreicht haben, ist automatisch 2FA für Sie aktiviert. Daher ist es besonders wichtig, dass Sie die Wiederherstellungscodes gut aufbewahren, damit Sie diese im Notfall verwenden können.

Zur Bestätigung der Aktivierung erhalten Sie auch eine E-Mail.

**Hinweis**:

Solange Sie außer die **Wiederherstellungscodes** keine weiteren Tokens erstellt haben, ist die **Zwei-Faktor-Authentifizierung** nur in der **2FA-Verwaltung** selbst aktiviert.

Das bedeutet: Wenn Sie die **2FA-Verwaltung** jetzt beenden, können Sie sich nur mit einem **Wiederherstellungscode** wieder anmelden.

Wenn Sie auf den Button **„Weiter“** klicken, sehen Sie die folgende **Auswahlmaske** (Abbildung 5).

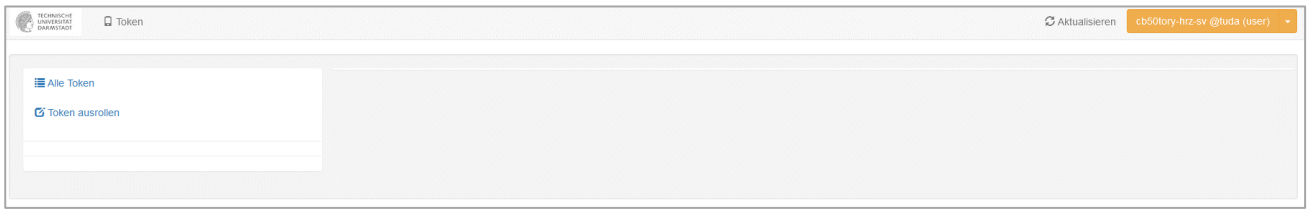


Abbildung 5: Auswahlmaske Token

An dieser Stelle haben Sie zwei Optionen:

1. Wenn Sie bereits Tokens haben, können Sie diese bearbeiten, indem Sie auf den Button **„Alle Token“** klicken.
2. Wenn Sie noch keinen Token haben, können Sie hier Ihren ersten Token **„ausrollen“** (erstellen).

Fahren Sie jetzt mit dem *Schritt 3: Token erstellen* fort. Nachdem Sie diesen erfolgreich erstellt haben, werden Sie bei jedem Login am SSO künftig danach gefragt.

## Schritt 3: Token erstellen

Ein Token wird dadurch erstellt, dass er zunächst ausgerollt und dann verifiziert wird.

### 1. Token ausrollen

Zum Erstellen eines neuen TOTP-Tokens klicken Sie auf „Token ausrollen“ und wählen TOTP.

Es gibt zwei Felder, von denen das erste Feld mit dem Wert „TOTP: Zeitbasiertes Einmalpasswort“ vorausgefüllt ist (Abbildung 6). Sie können dieses Feld so lassen und direkt fortfahren.[1]

Das zweite Feld ist für die Beschreibung[2] des Tokens vorgesehen und ist ebenfalls ein Pflichtfeld. Tragen Sie hier eine passende Beschreibung ein, z. B. **„myMobileAuthenticator“**.

Anschließend wählen Sie **„Weiter“** aus.

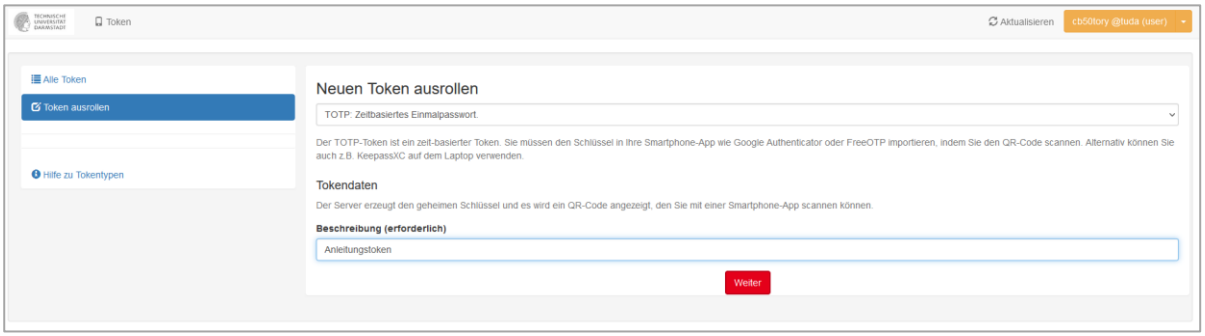


Abbildung 6: Token ausrollen Ansicht

### 2. Token verifizieren

Nun erhalten Sie einen **QR-Code**, den Sie mit dem **Authenticator** auf Ihrem Mobiltelefon einscannen können (in unserem Fall *privacyIDEA Authenticator*). Der Authenticator auf Ihrem Mobiltelefon wird daraufhin ein **Einmalpasswort (TOTP)** erzeugen, bestehend aus aufeinanderfolgenden Ziffern (Abbildung 7).

[1] Es gibt noch zwei weitere Varianten (HOTP und WebAuthn) auf die hier nicht eingegangen wird.

[2] Die Beschreibung erlaubt Ihnen beim Login am SSO die Tokens zu unterscheiden, sollten Sie mehrere konfiguriert haben.


Abbildung 7: Erzeugtes Einmalpasswort in der *privacyIDEA Authenticator-App*

Tragen Sie dieses Einmalpasswort in das dafür vorgesehene Eingabefeld in der **2FA-Verwaltung** unterhalb des QR-Codes ein. Klicken Sie anschließend auf **„Token verifizieren“** (Abbildung 8). Wenn alles korrekt eingegeben wurde, haben Sie erfolgreich Ihren ersten **Software-Token** ausgerollt (Abbildung 9). Über den Button **„Alle Token“** gelangen Sie zur Übersicht Ihrer Tokens.

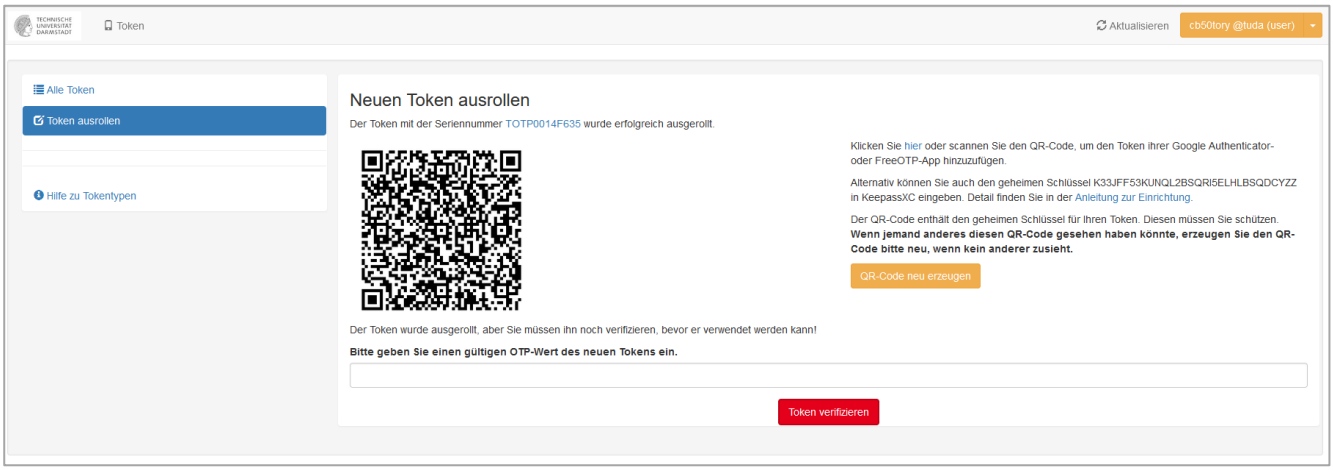


Abbildung 8: QR-Code des Tokens

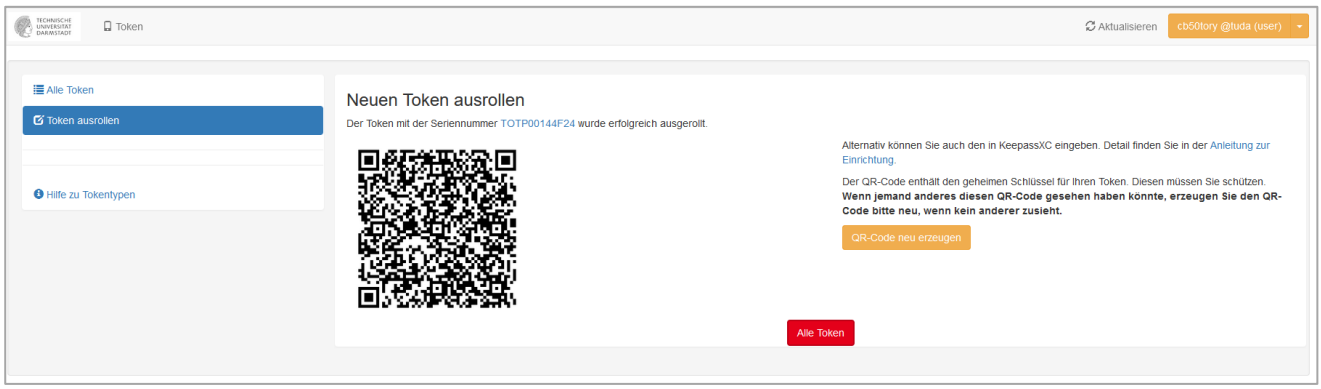


Abbildung 9: Abschluss des Registrierungsprozesses

Falls es nicht möglich ist, den QR-Code mit dem Smartphone zu scannen, können Sie alternativ den **geheimen Schlüssel** (Abbildung 10) manuell in der mobilen App – in unserem Fall *privacyIDEA Authenticator* – eintragen (Abbildung 11 und 12).

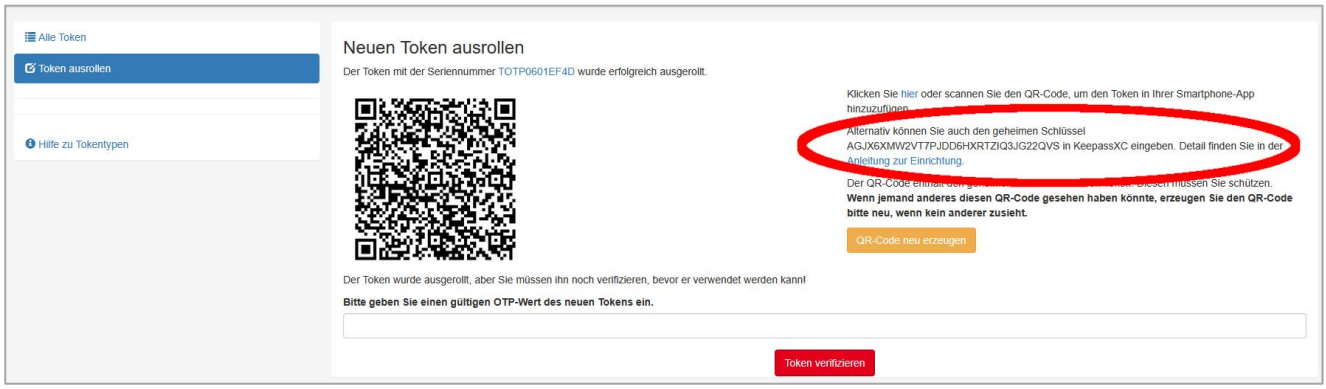


Abbildung 10: Geheimer Schlüssel


Abbildung 11: Hinzufügen des geheimen Schlüssels

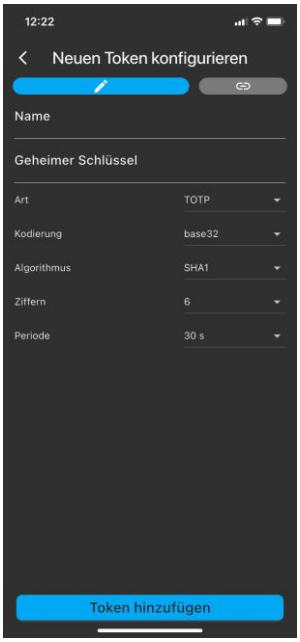


Abbildung 12: Neuen Token konfigurieren

**Hinweis**:

Sie können den geheimen Schlüssel auch in einem Passwortmanager wie beispielsweise KeePassXC auf Ihrem Dienstrechner nutzen. Eine Anleitung zu KeePassXC finden Sie auf unserer Webseite rechts unter Links & Downloads.

Alternativ oder zusätzlich können Sie auch einen eigenen Hardware-Token eintragen oder einen Hardware-Token vom HRZ registrieren und bestätigen lassen. Wenn letzteres gewünscht ist, kontaktieren Sie uns gerne per E-Mail an service@hrz.tu-darmstadt.de.

Sie können die 2FA-Verwaltung nun verlassen.

Nachdem Sie die **2FA-Verwaltung** verlassen haben, können Sie sich nun per **SSO** an einem Dienst anmelden. Was genau passiert, wenn Sie sich anmelden, wird im *Schritt 4: Login* beschrieben.

## Schritt 4: Login

Der Login beginnt wie gewohnt mit der Eingabe Ihres Benutzernamens (TU-ID) und Passworts (Abbildung 13).


Abbildung 13: Login Benutzername und Passwort

Nachdem Sie die **„Anmelden“** geklickt haben, werden Sie aufgefordert Ihren 2. Faktor einzugeben. Der 2. Faktor ist der von Ihnen eingerichtete Software- oder Hardware-Token. In unserem Beispiel war das der **Software-Token „myMobileAuthenticator“** (Abbildung 14).


Abbildung 14: Auswahl des Tokens

Wenn Sie den Token auswählen, werden Sie zur Eingabe Ihres Einmalpassworts (OTP) aufgefordert.

Dieses Einmalpasswort wird von Ihrer Authenticator-Anwendung (in unserem Fall *privacyIDEA Authenticator*) generiert und besteht aus 6 Ziffern (Abbildung 7).

Tragen Sie das Einmalpasswort ein und bestätigen Sie mit **„Überprüfen“.** Wenn Sie alles korrekt eingetragen haben, erfolgt Ihr Login mit dem 2. Faktor und Sie können den Dienst, für den Sie sich anmelden, benutzen.

Falls Sie mehrere Tokens in der 2FA-Verwaltung ausgerollt haben, können Sie auch einen anderen Token auswählen, indem Sie auf **„Anderen Token wählen“** klicken.


Abbildung 15: Eingabe des Einmalpassworts (OTP)