TECHNISCHE UNIVERSITÄT DARMSTADT

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

HRZ Hochschulrechenzentrum

Option 1: Verwendung einer Authenticator-App

Nach erfolgreicher Aktivierung der Zwei-Faktor-Authentifizierung können Sie einen neuen Token ausrollen. Sollten Sie noch nicht in der 2FA-Verwaltung angemeldet sein, rufen Sie sie 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.

Klicken Sie auf den Button **„Weiter“**. Sie sehen nun die folgende **Auswahlmaske** (Abbildung 1).

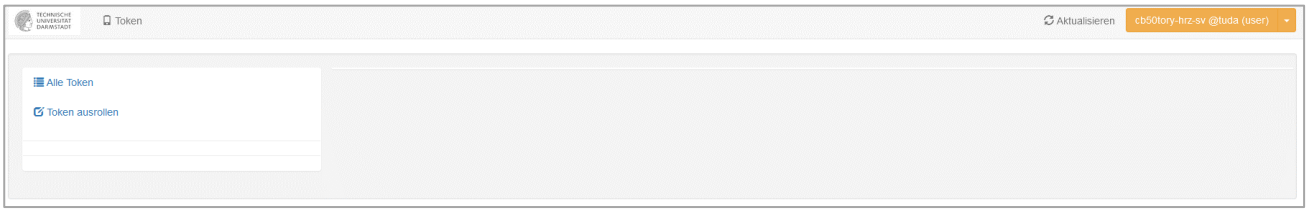

Abbildung 1: Auswahlmaske Token

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).

Nachdem Sie erfolgreich einen neuen Token erstellt haben, werden Sie bei jedem Login am SSO künftig danach gefragt.

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

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 2). 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.

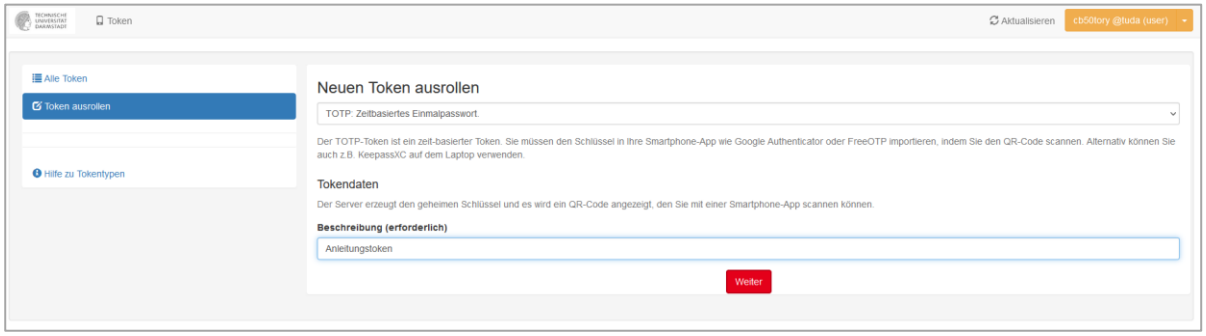

Abbildung 2: Token ausrollen Ansicht

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 3).

Abbildung 3: Erzeugtes Einmalpasswort in der *privacyIDEA Authenticator-App*

[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.

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 4). Wenn alles korrekt eingegeben wurde, haben Sie erfolgreich Ihren ersten **Software-Token** ausgerollt (Abbildung 5). Über den Button **„Alle Token“** gelangen Sie zur Übersicht Ihrer Tokens.

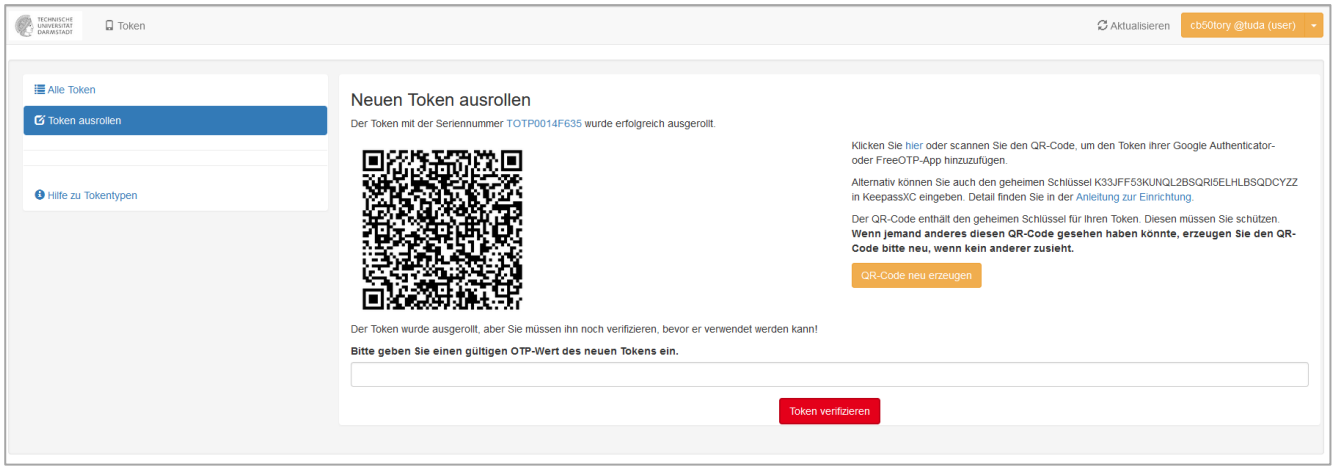

Abbildung 4: QR-Code des Tokens

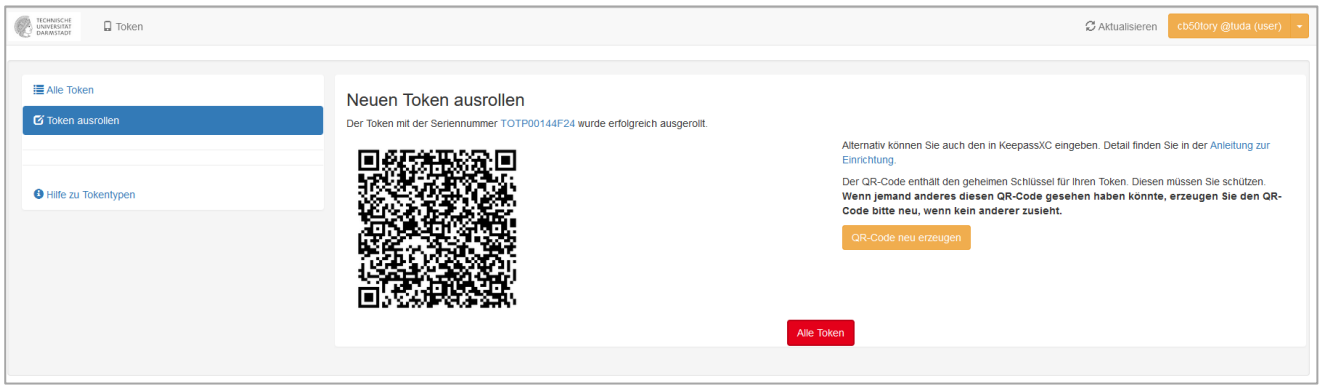

Abbildung 5: Abschluss des Registrierungsprozesses

Falls es nicht möglich ist, den QR-Code mit dem Smartphone zu scannen, können Sie alternativ den **geheimen Schlüssel** (Abbildung 6) manuell in der mobilen App – in unserem Fall *privacyIDEA Authenticator* – eintragen (Abbildung 7 und 8).

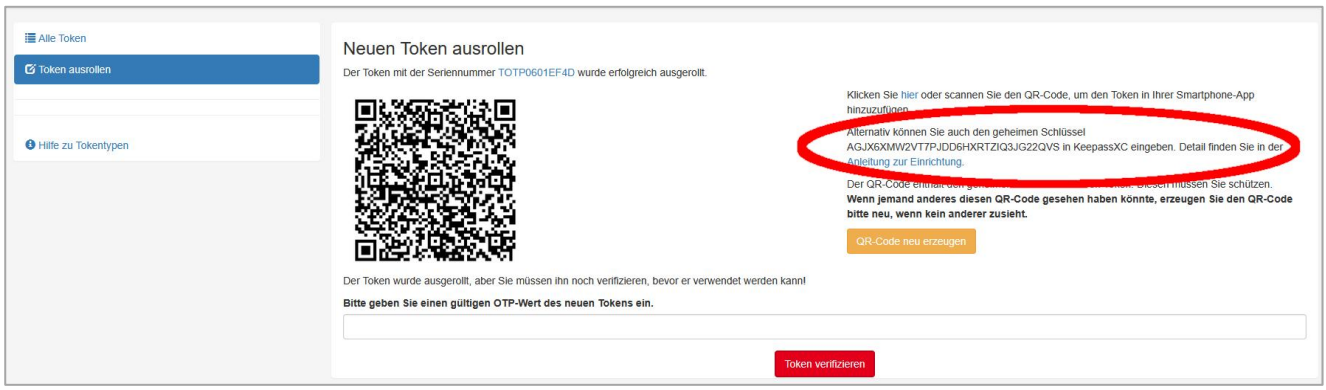

Abbildung 6: Geheimer Schlüssel

Abbildung 7: Hinzufügen des geheimen Schlüssels

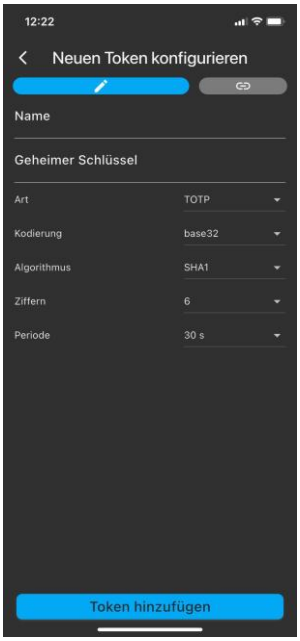

Abbildung 8: Neuen Token konfigurieren

Sie können die 2FA-Verwaltung nun verlassen.