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

Allgemeines

2FA-Token werden in der 2FA-Verwaltung erstellt. Dort können Sie sich eine beliebige Anzahl von Tokens erstellen und diese verwalten.

In der 2FA-Verwaltung können Sie TAN-, TOTP- und Webauthn-Token verwalten.

Zwei-Faktor-Authentisierung einrichten

In die 2FA-Verwaltung gelangen Sie durch einen Klick auf „2FA-Verwaltung“ in der Login-Maske des SSO.

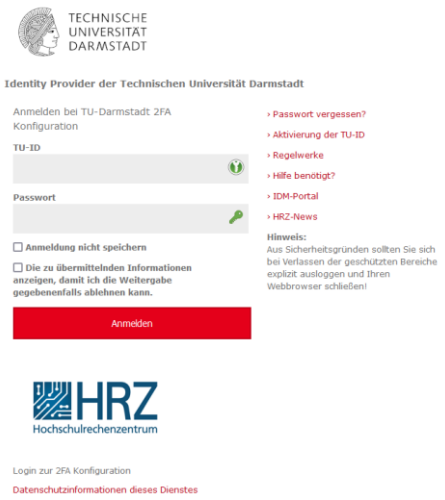


Abbildung 1: SSO-Login Maske > „2FA-Verwaltung“

Sie gelangen auf eine Begrüßungsseite und erhalten nach dem Klick auf „Weiter“ eine kurze Einführung.

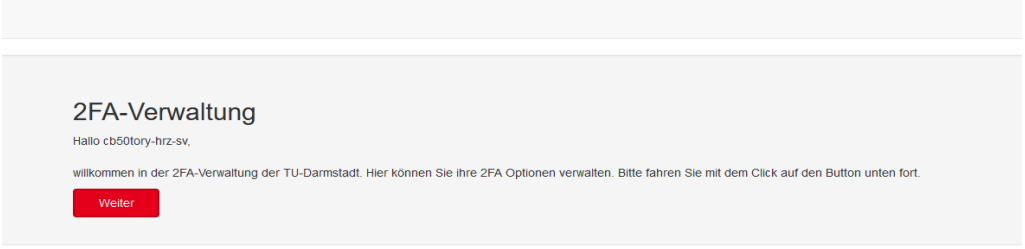


Abbildung 2: Begrüßungsseite

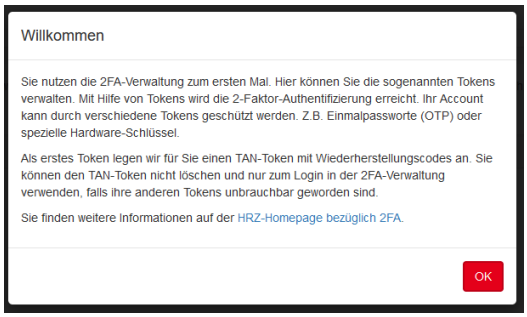


Abbildung 3: Kleiner Erklärungstext

Nach dem Klick auf „OK“ werden Sie zur Erstellung mehrerer TAN-Tokens weitergeleitet. Diese benötigen Sie, falls die anderen Token abhandenkommen. Sie können nur zum Login in der 2FA-Verwaltung verwendet werden.

Abbildung 4: Beim Klick von „Weiter“ werden die Token generiert

Im Anschluss erhalten Sie die TAN-Liste.

Wichtig: Diese TAN-Liste müssen Sie speichern oder ausdrucken. Sollten Ihre anderen Tokens defekt sein, benötigen Sie diese zum Login in die 2FA-Verwaltung.

Sie erhalten zur Bestätigung der Aktivierung auch noch eine E-Mail.

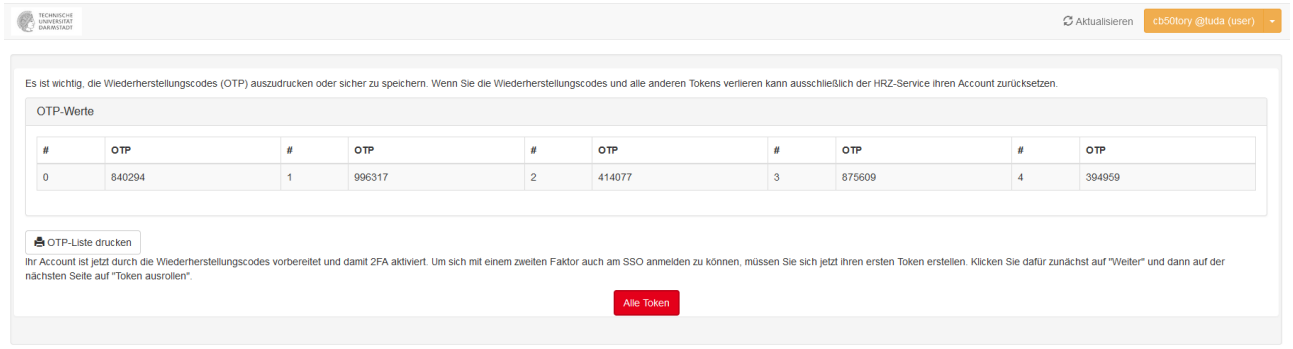
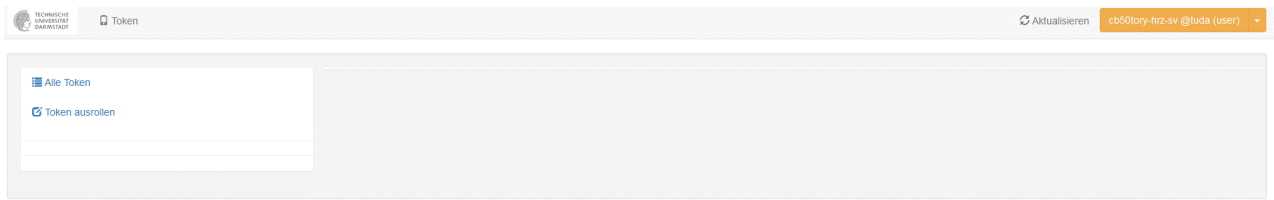


Abbildung 5: Liste mit generierten Einmalpasswörtern (OTP)

Nach dem Klicken auf „Alle Token“ gelangen Sie in die Verwaltung, wo Sie entweder Ihren bereits existierenden Token verwalten oder neue anlegen können.



Hinweis: Solange Sie außer Ihren TAN-Token keine weiteren Token konfiguriert haben, ist die Zwei-Faktor-Authentisierung nur an der 2FA-Verwaltung aktiv.

Fahren Sie jetzt mit dem Schritt „TOTP-Token erstellen“ fort, um Ihren ersten Token zur Nutzung am SSO zu erstellen.

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

TOTP-Token erstellen

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

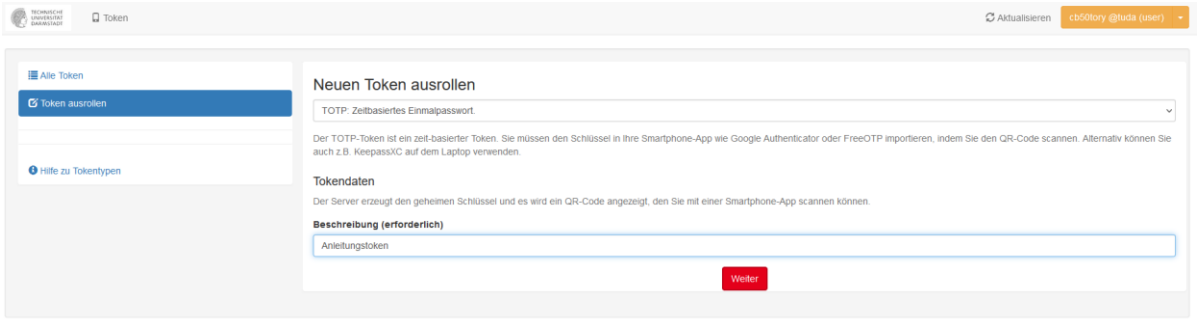


Abbildung 6: Token ausrollen Ansicht

Die Beschreibung (in Beispiel „Anleitungstoken“) ist erforderlich und erlaubt ihnen beim Login am SSO die Tokens zu unterscheiden, sollten Sie mehrere konfiguriert haben.

Anschließend wählen Sie „Weiter“ aus. Nun erhalten Sie einen QR-Code, den Sie beispielsweise mit der PrivacyIDEA Authenticator (Android oder iOS) auf ihrem Diensttelefon einscannen können. Sie können aber auch den *geheimen Schlüssel* in KeePassXC auf ihrem Dienstrechner verwenden. Eine Anleitung dazu finden Sie auf unserer Webseite. Der Schlüssel und der QR-Code wird nur hier einmalig angezeigt. Sollte das gewählte Gerät nicht mehr funktionieren, können Sie aber jederzeit einen neuen TOTP-Token anlegen und den defekten löschen.

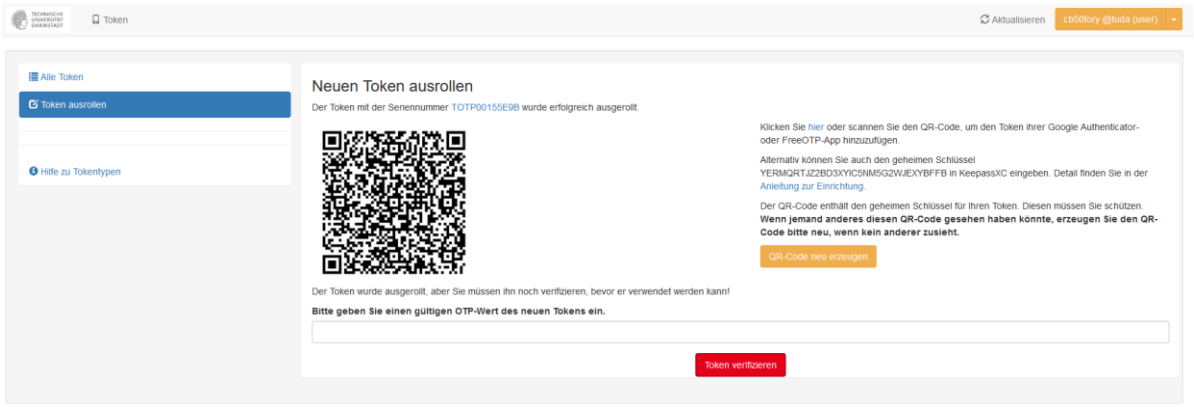


Abbildung 7: QR-Code des Tokens

Die Anwendung erzeugt nun alle 30 Sekunden ein neues 6-stelliges Einmalpasswort (OTP). Zur Bestätigung müssen Sie das aktuelle OTP in dem Feld eingeben und „Token verifizieren“ auswählen. Damit ist ihr erster TOTP Token registriert. Mit „Alle Token“ kommen Sie zurück auf die Liste Ihrer Token.

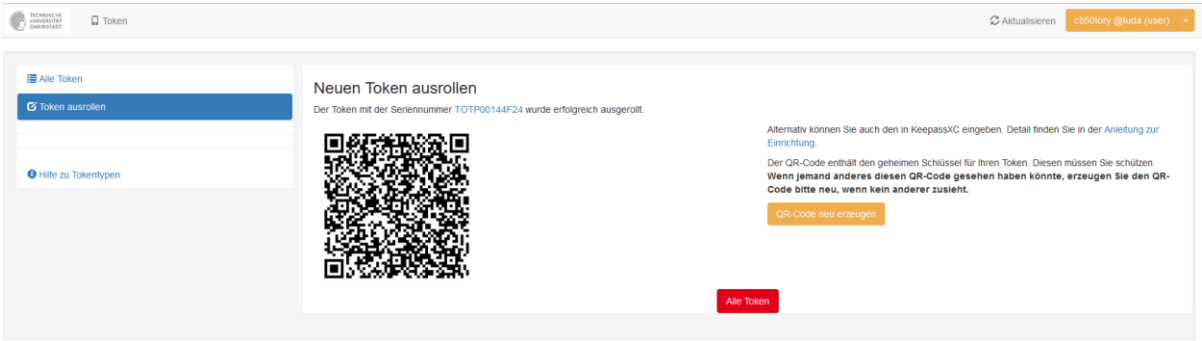


Abbildung 8: *Abschluss des Registrierungsprozesses*

Login mit 2FA

Der Login beginnt wie gewohnt mit der Eingabe von Nutzernamen und Passwort.

Nachdem diese bestätig werden, wird geprüft, ob ein oder mehrere für die Anwendung passende Token zur Verfügung stehen. Sollten mehrere zur Auswahl stehen, können Sie den passenden Token anhand der Beschreibung auswählen.

Abbildung 9: Auswahl der passenden Tokens

Danach werden Sie um die Eingabe ihres Einmalpassworts (OTP) gebeten. Dieses finden Sie in der konfigurierten Anwendung (z.B. Authenticator oder KeepassXC). Tragen Sie die 6 Ziffern hier ein und bestätigen Sie durch „Überprüfen“. Sollten Sie einen anderen Token auswählen wollen, können Sie das mit „Anderen Token wählen“ tun.

Abbildung 10: Eingabe des Einmalpassworts (OTP)