Freie Universität Berlin

{tip4u://188} Version 2

Zentraleinrichtung für Datenverarbeitung (ZEDAT)
www.zedat.fu-berlin.de

Anmeldung mit Multifaktor-Authentifizierung

Diese Anleitung erklärt die Einrichtung der sicheren Anmeldeverfahren mit Multifaktor-Authentifizierung (MFA).

zedat

Zentraleinrichtung für Datenverarbeitung
Fabeckstraße 32 / 14195 Berlin
Hotline (030) 838 77777 / hilfe@zedat.fu-berlin.de

Einrichtung der sicheren Anmeldeverfahren (Multifaktor-Authentifizierung) für FU-Accounts

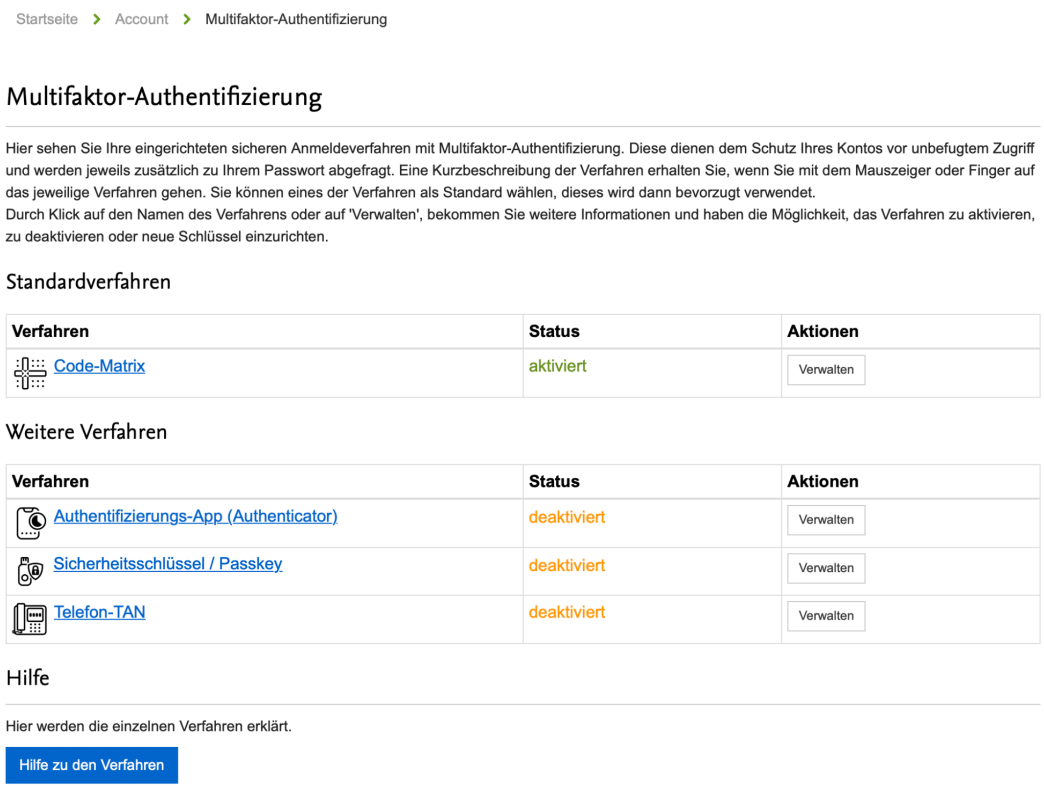
Einführung

Der Schutz Ihrer persönlichen und akademischen Daten an der Freien Universität Berlin ist uns ebenso wichtig wie Ihnen. Deshalb haben wir die **Multifaktor-Authentifizierung (MFA)** für alle FU-Accounts eingeführt. Neben Ihrem Passwort wird ein zweiter Sicherheitsfaktor benötigt, um sich anzumelden. Dieser Schritt erhöht die Sicherheit Ihrer Daten erheblich, da ein potenzieller Angreifer nun sowohl Ihr Passwort als auch einen davon unabhängigen zweiten Faktor benötigt, um auf Ihr Konto zuzugreifen.

Sie können mehrere verschiedene Anmeldeverfahren gleichzeitig als Ihren zweiten Faktor aktivieren (daher: *Multifaktor*). Es reicht zur Anmeldung aus, wenn Sie immer eins Ihrer aktivierten Verfahren zusätzlich zu Ihrem Passwort nutzen können – es ist jedoch sinnvoll, mehrere der Verfahren einzurichten, falls Sie den Zugriff auf eines verlieren sollten.

In den folgenden Abschnitten erklären wir die Einrichtung der Anmeldeverfahren. Bitte denken Sie daran, dass Sie Ihren **zweiten Faktor** (Code-Matrix, Authentifizierungs-App, Sicherheitsschlüssel / Passkey oder Telefon-PIN) **niemals mit jemandem teilen** sollten – ebenso wenig wie Ihr Passwort. Auch unser IT-Personal wird Sie niemals nach Ihrem zweiten Faktor oder Ihrem Passwort fragen.

Um die sicheren Anmeldeverfahren vollständig einzurichten und zu verwalten, navigieren Sie bitte zunächst zum Abschnitt *Account* ▸ *Multifaktor-Authentifizierung* im ZEDAT-Portal: https://portal.zedat.fu-berlin.de/



Portal-Seite für die sicheren Anmeldeverfahren

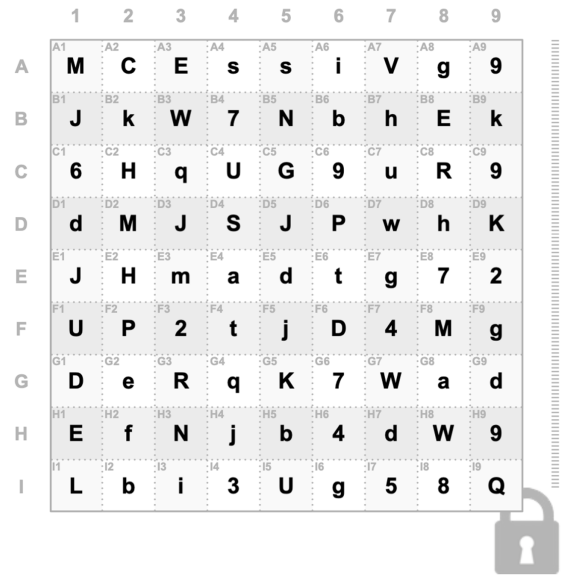
Hier finden Sie die Übersicht zu Ihren Anmeldeverfahren. In der Tabelle werden die einzelnen Verfahren aufgelistet. Wenn Sie auf den Namen eines Verfahrens oder in der Spalte *Aktionen* auf *Verwalten* klicken, kommen Sie anschließend zur speziellen Konfigurationsseite des jeweiligen Verfahrens, um es einrichten zu können. In der Spalte *Status* erkennen Sie den aktuellen Status der einzelnen Verfahren – z.B. ob ein Verfahren aktiviert, deaktiviert oder gesperrt ist. Wie Sie ein Verfahren **sperren, löschen oder deaktivieren** können und was dies bedeutet, erläutern wir weiter unten in dieser Anleitung in einem eigenen Abschnitt.

Initial ist lediglich das Verfahren „Code-Matrix" aktiviert und als Standard festgelegt. Wenn Sie ein anderes Verfahren als Ihr Standardverfahren nutzen wollen, können Sie dies nach der Aktivierung des Verfahrens in der Spalte *Aktionen* über den Button *Als Standard* festlegen.

Unter *Hilfe zu den Verfahren* finden Sie außerdem eine Kurzübersicht zu den einzelnen Anmeldeverfahren.
Im Bereich *E-Mail-Benachrichtigung* können Sie einstellen, ob Sie bei Anmeldeversuchen eine Sicherheits-Benachrichtigung per Mail erhalten wollen.

Verfahren 1: Code-Matrix (Standard / Backup)

Das Verfahren „Code-Matrix" ist immer aktiviert und für die initiale Einrichtung sowie als Backup vorgesehen. Bei Verwendung dieses Verfahrens werden Sie nach sechs zufälligen Positionen aus Ihrer individuellen Code-Matrix gefragt. Die Code-Matrix wird Ihnen üblicherweise zunächst per Post zugesandt. Es ist immer nur **eine** Code-Matrix aktiv. Bei Neuausstellung wird die vorherige ungültig.



Beispiel einer Code-Matrix

- Die individuelle 9x9 Code-Matrix enthält zufällige Klein- und Großbuchstaben sowie Ziffern.
- Im Anmeldevorgang mit diesem Verfahren werden Sie nach 6 zufällig gewählten Feldern aus dieser Matrix gefragt.

- Die Felder sind dabei nach ihrer Reihe und Spalte benannt. Die Bezeichnungen der Positionen setzen sich jeweils zusammen aus einem Buchstaben (A-I), der die Reihe angibt, sowie einer Ziffer (1-9), die die Spalte angibt.
- Wenn aufgefordert, geben Sie bitte die abgefragten Positionen aus Ihrer Matrix in der richtigen Reihenfolge ohne Leerzeichen sowie unter Beachtung von Groß- und Kleinschrift ins Eingabefeld ein und bestätigen Sie so Ihre Anmeldung.
- *Beispiel (nach obiger Beispiel-Matrix): Werden Sie etwa nach dem Inhalt des Feldes* G8 *gefragt, so müssen Sie den Buchstaben* a *eingeben.*

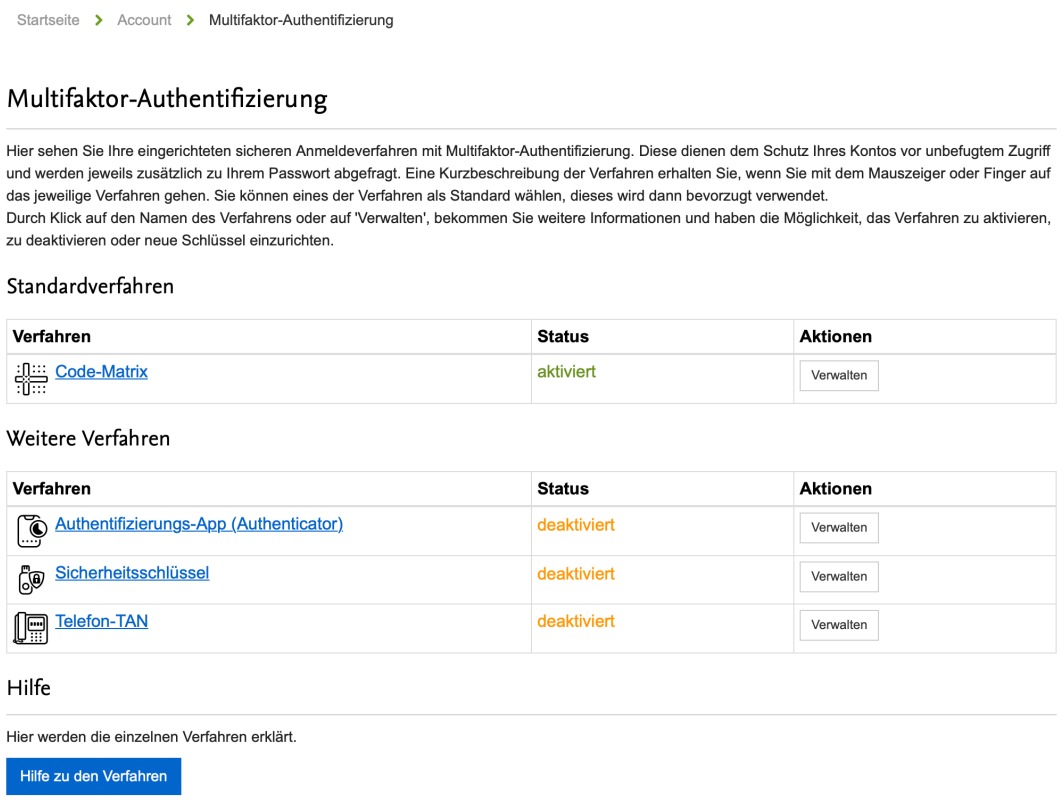
Beispiel einer Code-Matrix-Abfrage

- Bewahren Sie die Code-Matrix sicher auf und teilen Sie diese mit niemandem.
- Falls Sie eines der anderen Anmeldeverfahren aktiviert haben, können Sie sich selbst bei Bedarf eine neue Code-Matrix im Portal ausstellen lassen (*Portal* ▸ *Account* ▸ *Multifaktor-Authentifizierung* ▸ *Code-Matrix* ▸ *Neue Matrix ausstellen*). Dabei verliert die alte Matrix ihre Gültigkeit und kann nicht mehr verwendet werden. Falls Sie keines der anderen Anmeldeverfahren aktiviert haben, wenden Sie sich bei Verlust der Matrix bitte an den Benutzerservice.

Portal-Seite zur Verwaltung der Code-Matrix

Hinzufügen von weiteren Anmeldeverfahren

Die Einrichtung mindestens eines der nachfolgenden zusätzlichen Verfahren erleichtert den Anmeldevorgang erheblich. Navigieren Sie dazu zunächst im ZEDAT-Portal zu *Account* ▸ *Multifaktor-Authentifizierung* und klicken Sie dort auf das entsprechende Verfahren.



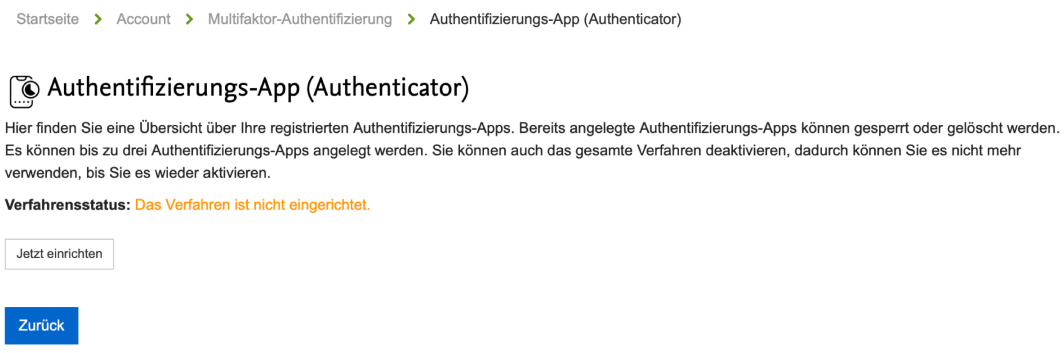
Portal-Seite für die sicheren Anmeldeverfahren

Verfahren 2: Authentifizierungs-App (Authenticator) *(Empfohlen)*

Beim Anmeldeverfahren „Authentifizierungs-App“ wird beim Anmeldevorgang ein zeitbasierter, einmaliger Bestätigungscode in Ihrer App generiert (TOTP / Time-based One-time Password). Diesen geben Sie beim Anmeldevorgang, wenn aufgefordert, zusätzlich zu Ihrem Passwort mit ein. Eine Authentifizierungs-App ist ein schneller und einfacher Weg der sicheren Anmeldung im Alltag. Sie können eine beliebige TOTP-Authentifizierungs-App nutzen (z.B. Google Authenticator, Microsoft Authenticator). Sie können bis zu **drei** Apps auf verschiedenen Geräten einrichten und alternativ verwenden.

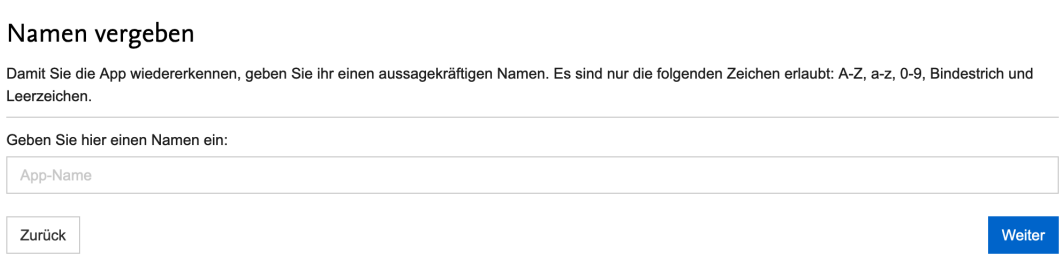
Schritt-für-Schritt-Anleitung für den Google Authenticator:

- Navigieren Sie im ZEDAT-Portal zu *Account* ▸ *Multifaktor-Authentifizierung* ▸ *Authentifizierungs-App* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

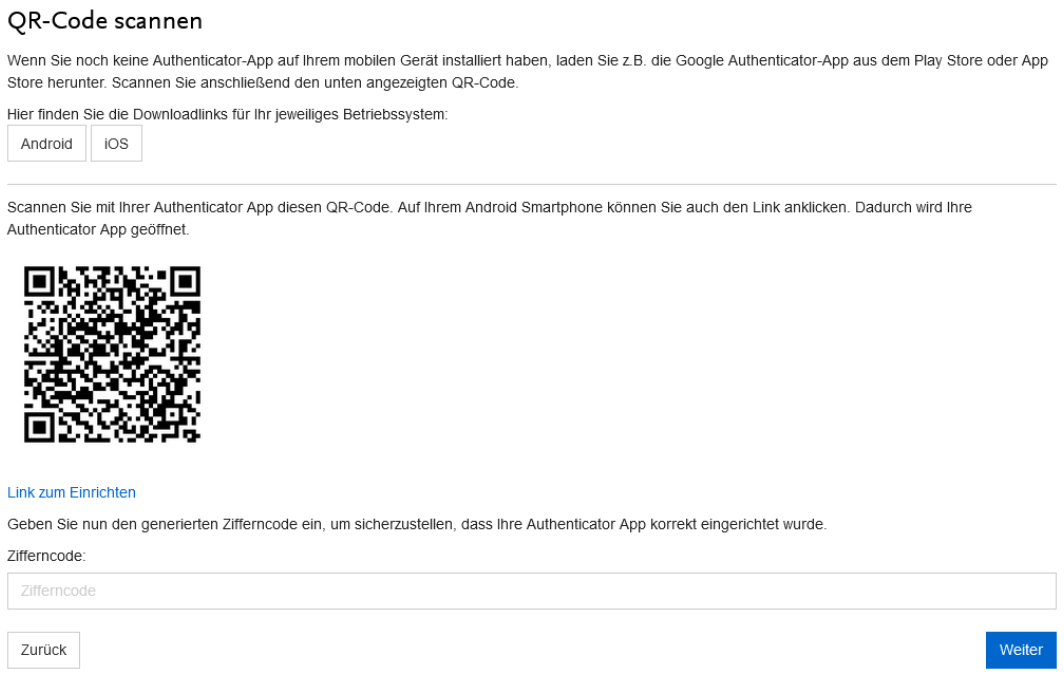


Portal-Seite zur Verwaltung der Authenticator-Apps

- Zuerst vergeben Sie einen Namen für diesen Authenticator. Falls Sie mehrere Authentifizierungs-Apps einrichten, hilft Ihnen dieser Name bei der jeweiligen Identifizierung. Klicken Sie dann auf *Weiter*.

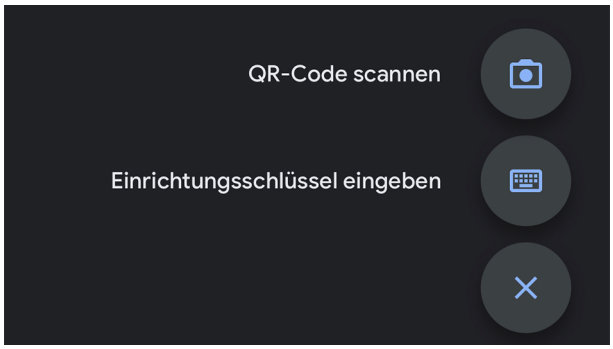


- Zum Einrichten der App wird Ihnen nun im Portal ein individueller QR-Code angezeigt.

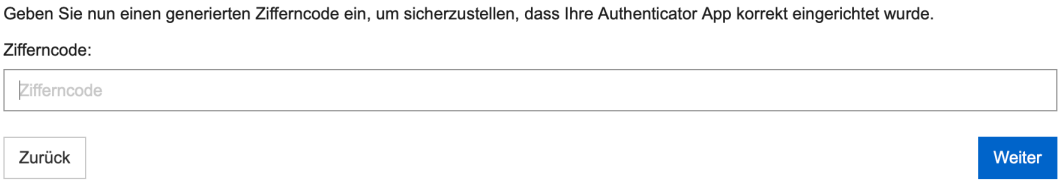


Portal-Seite für die Einrichtung der Authenticator-App

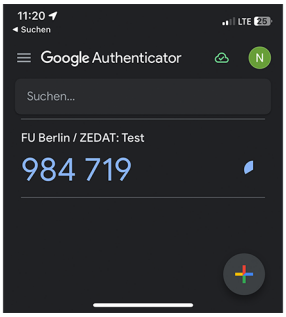
- Installieren Sie zunächst die Google Authenticator App aus dem App Store (iOS) oder Google Play Store (Android).
  • iOS: https://apps.apple.com/de/app/google-authenticator/id388497605
  • Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- Öffnen Sie die Google Authenticator App und tippen Sie auf das Plus-Symbol (+), um Ihren FU-Account hinzuzufügen.
- Wählen Sie *QR-Code scannen* und scannen Sie den QR-Code, der auf dem Bildschirm im ZEDAT-Portal angezeigt wird. Gegebenenfalls müssen Sie der App vorher den Kamerazugriff erlauben.



- Die App generiert nun einen 6-stelligen Code, der alle 30 Sekunden erneuert wird. Geben Sie diesen Code im unten stehenden Eingabefeld im Portal ein.



Den generierten Code in dieses Feld eingeben



Beispiel eines Codes in der Google Authenticator App

- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren wie etwa Ihre Code-Matrix benutzen.
- Bei zukünftigen Anmeldungen können Sie nun den zeitbasierten Zahlencode aus der App als Ihren zweiten Faktor nutzen, wenn Sie dazu aufgefordert werden.

Verfahren 3: Sicherheitsschlüssel / Passkey

Im Verfahren Sicherheitsschlüssel / Passkey können Sie einen physischen Schlüssel (z.B. Yubico Security Key) oder sogenannte Passkeys einrichten. Dies sind digitale Sicherheitsschlüssel, die aus einem öffentlich/privatem Schlüsselpaar bestehen. Passkeys können in Ihrem Gerät gespeichert sein (z.B. mit Windows Hello) oder über eine Cloud zwischen verschiedenen Geräten synchronisiert werden (via Google-Konto, Apple iCloud-Schlüsselbund). Für Passkeys auf Apple Geräten (iPhone, iPad, Mac) muss beispielsweise der iCloud-Schlüsselbund aktiviert sein – der Schlüssel wird hierbei dann auf alle Ihre Apple Geräte sicher per iCloud verteilt. Passkeys können ein sehr schneller und einfacher Weg der sicheren Anmeldung im Alltag sein.

Falls Sie einen Hardware-Sicherheitsschlüssel eingerichtet haben, müssen Sie diesen zur Anmeldung immer bei sich haben. In der Regel genügt es, bei Hardware-Schlüsseln nach Eingabe Ihres Passworts den eingesteckten Schlüssel anzutippen oder an die Rückseite des Smartphones zu halten (NFC) um ihn zu verwenden. Gegebenenfalls müssen Sie USB-Sicherheitsschlüssel mit einer PIN sichern, die vor der Benutzung abgefragt wird.

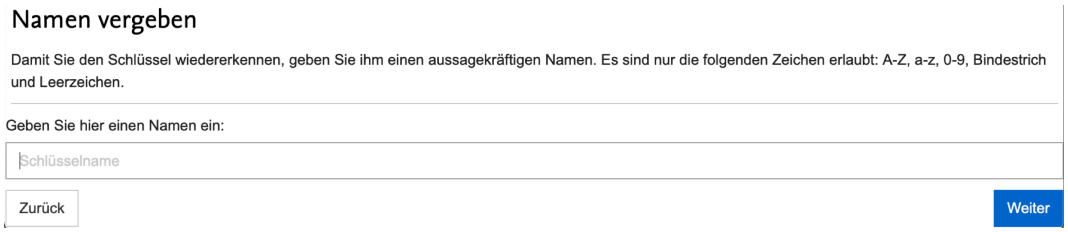
Sie können bis zu **drei** Schlüssel einrichten und alternativ verwenden.

Einrichtung eines Sicherheitsschlüssels / Passkeys:

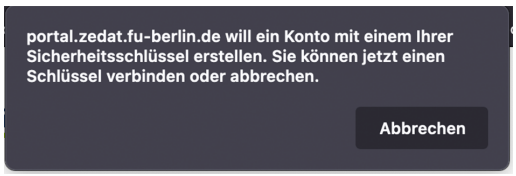
- Navigieren Sie im ZEDAT-Portal zu *Account* ▸ *Multifaktor-Authentifizierung* ▸ *Sicherheitsschlüssel / Passkey* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

Portal-Seite zur Verwaltung der Sicherheitsschlüssel / Passkeys

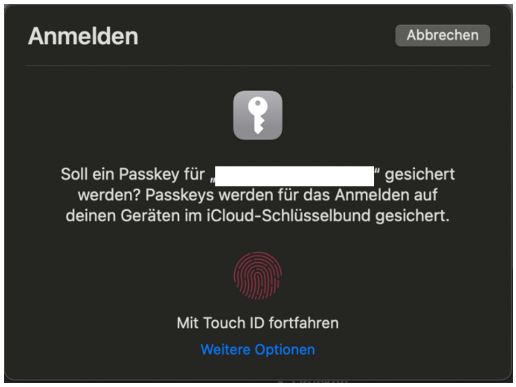
- Zuerst vergeben Sie einen Namen für diesen Schlüssel. Falls Sie mehrere Schlüssel einrichten, hilft Ihnen dieser Name bei der jeweiligen Identifizierung.



- Anschließend werden Sie aufgefordert, Ihren Sicherheitsschlüssel einzurichten, indem Sie diesen z.B. in einen USB-Port stecken und aktivieren. Hierzu öffnet sich in der Regel ein Pop-Up-Fenster im Vordergrund. Wenn Ihr Gerät/Browser Passkeys unterstützt, wird eine Einrichtungsmöglichkeit für diese hier ebenfalls angezeigt. Je nach Typ des Schlüssels und Betriebssystem kann das Vorgehen von dem hier beschriebenen abweichen.
- Ihr Browser oder Betriebssystem führt Sie nun durch die Einrichtung Ihres Sicherheitsschlüssels / Passkeys.



Die Einrichtung ist browserabhängig. Ein solches Fenster kann sich etwa bei Mozilla Firefox öffnen.



Ein solches Fenster kann sich zur Einrichtung eines Passkeys in Safari auf einem Mac oder iOS Gerät öffnen.

- Bitte folgen Sie diesen Anweisungen. Nach erfolgreicher Einrichtung werden Sie automatisch zum nächsten Schritt weitergeleitet.
- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren benutzen.
- Bitte beachten Sie, dass ein physischer Sicherheitsschlüssel bei jedem Login in den Computer eingesteckt und bei der Aufforderung aktiviert werden muss.

Verfahren 4: Telefon-TAN *(Nur für Beschäftigte)*

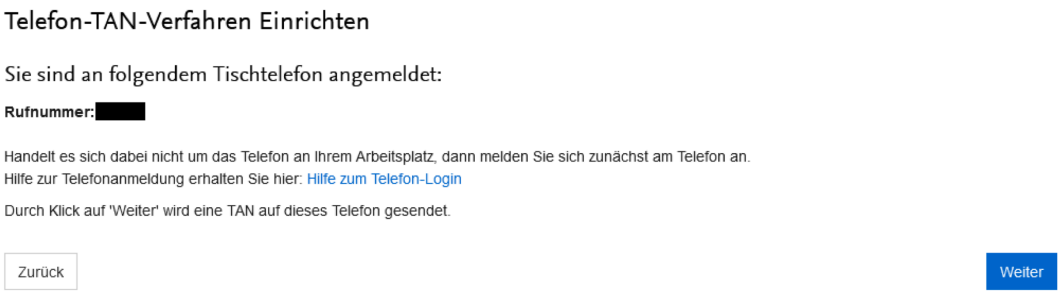
Mit dem Telefon-TAN-Verfahren können Sie Bestätigungscodes als Nachricht auf Ihr Cisco-Tischtelefon erhalten. Dazu ist es notwendig, dass Sie an Ihrem Tischtelefon angemeldet sind. Das ist der Fall, wenn Ihr Name oben links im Telefondisplay steht. Die Codes erhalten Sie **nicht** in der Webex App oder auf dem PC (Softphone).

Einrichtung der Telefon-TAN:

- Stellen Sie sicher, dass Sie bei Ihrem Tischtelefon mit Ihrem FU-Account angemeldet sind. (Benutzername + Telefon-PIN)
- Navigieren Sie im ZEDAT-Portal zu *Account* ▸ *Multifaktor-Authentifizierung* ▸ *Telefon-TAN* und klicken Sie auf *Jetzt einrichten*. Klicken Sie dann auf *Weiter*.

Portal-Seite zur Verwaltung des Telefon-TAN-Verfahrens

- Bestätigen Sie die Angaben zu Ihrem Tischtelefon am Bildschirm und klicken Sie dann auf *Weiter*.



Portal-Seite mit Informationen zum angemeldeten Telefon

- Die Telefon-TAN erscheint nun als Nachricht auf dem Bildschirm Ihres Cisco-Tischtelefons.

Beispiel einer TAN am Cisco-Tischtelefon

- Die angezeigte TAN geben Sie nun in das Eingabefeld im Portal ein.
- Zuletzt bestätigen Sie die Einrichtung, indem Sie ein bereits aktives Verfahren benutzen.
- Bei zukünftigen Anmeldungen erhalten Sie eine Nachricht auf Ihrem angemeldeten Tischtelefon, um den Anmeldevorgang abzuschließen.

Sperren und Deaktivieren von Anmeldeverfahren

Verlust der Code-Matrix

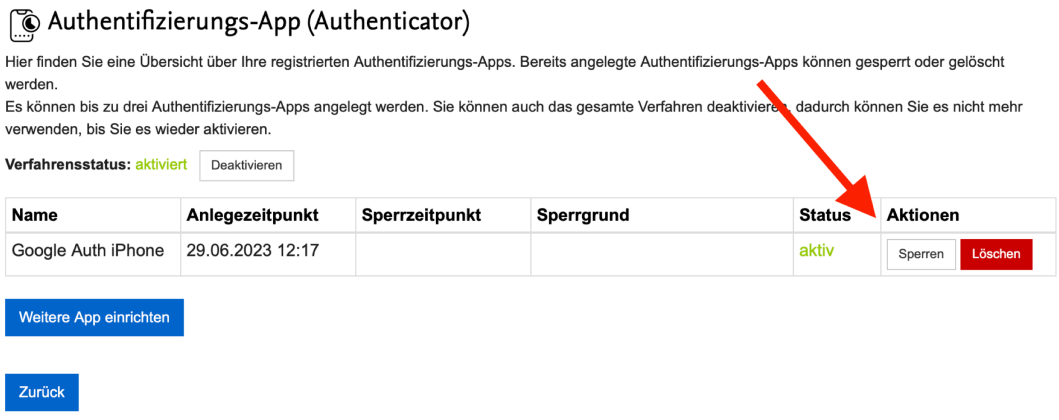
Bei Verlust Ihrer Code-Matrix sollten Sie sich eine *Neue Matrix ausstellen*. Die bisherige Code-Matrix kann dann nicht mehr zur Authentifizierung genutzt werden. Wie bereits in der Erklärung zur Code-Matrix beschrieben, navigieren Sie hierzu im ZEDAT-Portal unter *Account* ▸ *Multifaktor-Authentifizierung* auf die Unterseite zur Code-Matrix und klicken dort auf den entsprechenden Button. Sie benötigen hierfür ein aktiviertes weiteres Anmeldeverfahren. Falls Sie kein weiteres Verfahren aktiviert haben, wenden Sie sich bitte an den Benutzerservice.

Deaktivieren anderer Verfahren

Die Anmeldeverfahren Authenticator-App, Sicherheitsschlüssel und Telefon-TAN können Sie deaktivieren, wenn Sie diese (vorübergehend) nicht zur Authentifizierung verwenden möchten. Navigieren Sie hierzu wieder im ZEDAT-Portal unter *Account* ▸ *Multifaktor-Authentifizierung* auf die entsprechende Unterseite des jeweiligen Verfahrens und klicken Sie dort auf *Deaktivieren*.

Sperren und Löschen einzelner Apps/Schlüssel

Bei den Verfahren Authentifizierungs-App und Sicherheitsschlüssel / Passkey können Sie einzelne Apps/Schlüssel entweder vorübergehend sperren oder endgültig löschen, etwa bei Verlust des Smartphones oder des Hardware-Sicherheitsschlüssels. Navigieren Sie hierzu wieder im ZEDAT-Portal unter *Account* ▸ *Multifaktor-Authentifizierung* auf die entsprechende Unterseite des jeweiligen Verfahrens und klicken Sie dort in der Spalte *Aktionen* auf *Sperren* oder *Löschen*. Falls Sie ein Verfahren sperren, können Sie es nur mit der Bestätigung durch ein anderes aktiviertes Verfahren wieder entsperren.



Sperren und Löschen einer Authentifizierungs-App

Kontakt bei weiteren Fragen

Die Einrichtung der Multifaktor-Authentifizierung ist ein wichtiger Schritt zur Verbesserung der Sicherheit Ihrer Daten und der universitären IT-Systeme. Wir empfehlen Ihnen dringend, diese zusätzlichen Sicherheitsmaßnahmen so schnell wie möglich vollständig einzurichten. Falls Sie noch offene Fragen haben oder weitergehende Hilfe benötigen, wenden Sie sich bitte an den Benutzerservice.

- **+49 (0)30 838 56069**
- benutzerservice@zedat.fu-berlin.de

Hinweis:

Bitte denken Sie daran, dass Sie Ihren zweiten Faktor (Code-Matrix, Authentifizierungs-App, Sicherheitsschlüssel / Passkey oder Telefon-PIN) niemals mit jemandem teilen sollten. Auch unser IT-Personal wird Sie niemals nach Ihrem zweiten Faktor oder Ihrem Passwort fragen.