

# > Multifaktorauthentifizierung (MFA)



### Übersicht I



- 1. <u>Multifaktorauthentifizierung</u> (MFA)
- Was bedeutet MFA?
- Warum ist MFA notwendig?
- 2. <u>Kontakt-Mailadresse</u> als Voraussetzung für MFA
- Wozu dient die Kontakt-Mailadresse?
- Hinterlegung der Kontakt-Mailadresse
- 3. Beispiele: Anmeldung mit einem 2. -Faktor
- Beispiel 1: Profilverwaltung
- <u>Beispiel 2</u>: Tokenverwaltung (MFA-Server)



### Was sind Token?

4. <u>Token</u>

Token-Typen

Übersicht II

- Welche Token stehen an der Universität Koblenz zur Verfügung?
- Wie werden die verschiedenen Token ausgerollt und verwendet?
  - Zeitbasierte Einmalpasswörter (TOTP)
  - TAN-Liste (PPR)
  - <u>WebAuthn</u>
  - Yubico OTP (Yubikey AES Mode)
- 5. Ändern des Uni-Passworts







# Multifaktorauthentifizierung (MFA)

### Multifaktorauthentifizierung (MFA)

#### Was bedeutet MFA?

**Multifaktorauthentifizierung (MFA)** ist ein Sicherheitsverfahren, bei dem mehrere unabhängige Faktoren genutzt werden, um die Identität einer Person zu bestätigen. Es kombiniert mindestens zwei der folgenden Kategorien:

- Wissen Etwas, das nur Sie wissen; z. B. ein Passwort oder eine PIN
- Besitz Etwas, das nur Sie besitzen; z. B. ein Smartphone oder ein Token, das Codes generiert
- Eigenschaft Etwas, das nur Ihnen inhärent ist; z. B. ein Fingerabdruck oder Merkmale Ihres Gesichts für Gesichtserkennung

Durch diese zusätzliche Sicherheitsebene wird der Zugriff auf Systeme auch dann geschützt, wenn ein Faktor kompromittiert wird.





### **Notwendigkeit von MFA**



#### Warum ist MFA notwendig?

- Häufige Passwortsicherheitslücken: Viele Menschen verwenden leicht zu erratende Passwörter oder das gleiche Passwort für mehrere Konten. Wenn eines dieser Passwörter kompromittiert wird, sind andere Konten ebenfalls gefährdet.
- Sicherer Schutz sensibler Daten und Systeme: Durch MFA bleiben vertrauliche Daten und Systeme auch dann geschützt, wenn Ihr Passwort in falsche Hände geraten sollte.
- Schutz vor Phishing und anderen Angriffen: Selbst wenn Angreifende das Passwort über Phishing oder eine Sicherheitslücke erhalten, reicht das allein nicht aus, um auf Ihr Konto zuzugreifen. MFA fügt eine zusätzliche Sicherheitsstufe hinzu, die nur Sie selbst erfüllen können.



### **Notwendigkeit von MFA**

#### **Die Phishing-Falle**

Phishing bezeichnet Cyberangriffe, bei denen täuschend echte E-Mails verwendet werden, um sensible Daten zu stehlen oder Schadsoftware zu verbreiten. Oft geben sich Betrüger\*innen als andere Uni-Accounts, bekannte Kontakte oder Institutionen aus, um das Vertrauen zu gewinnen.

Eine typische Phishing-E-Mail fordert dazu auf, einen Link anzuklicken, einen Anhang zu öffnen und Informationen wie z. B. Passwörter preiszugeben. Auch wenn die Nachricht vertrauenswürdig erscheint, kann ein unvorsichtiger Klick dazu führen, dass persönliche Daten oder Uni-Konten kompromittiert werden. Seien Sie deshalb stets wachsam, besonders bei unerwarteten Nachrichten, und überprüfen Sie immer die Absenderadresse oder wenden Sie sich im Zweifel an die Person, von welcher die E-Mail stammen soll, und verifizieren Sie die Integrität der empfangenen E-Mail.

Wenn Sie zur Sicherheit Ihr Passwort ändern möchten finden Sie hier eine kurze Anleitung.





https://uni-ko.de/phishing-info





### **Kontakt-Mailadresse**



#### Wozu dient die Kontakt-Mailadresse?

In Ihrem Profil muss eine zweite Mailadresse, die sogenannte Kontakt-Mailadresse, hinterlegt werden. Diese Adresse übernimmt mehrere wichtige Funktionen:

- Passwortänderung: Sie erhalten an Ihre Kontakt-Mailadresse den Link zum Ändern Ihres Passworts.
- Alternative Kontakt-Option: Die Kontakt-Mailadresse dient als zusätzliche Möglichkeit, Sie zu erreichen, falls Ihre Uni-Mailadresse nicht verfügbar ist.
- Initial-Faktor für MFA: Die Kontakt-Mailadresse ist Ihr persönlicher, automatisch angelegter Faktor für den Start zur Multifaktorauthentifizierung (MFA).



### Hinterlegung der Kontakt-Mailadresse



#### 1. Schritt: Melden Sie sich bei der Profilverwaltung an

| ← C 🗗 https://pro        | ofile.uni-koblenz.de/login.cgi   |
|--------------------------|--|
| Profilverwaltung: Stammd | aten Heimatverzeichnis Quotierung Passwort Ausdrucke Gruppen Mailinglisten |
|                          | Anmelden mit Ihrer Uni-<br>Mailadresse und Passwort                        |
|                          | Benutzername<br>kaiser-wilhelm@uni-koblenz.de                              |
|                          | Passwort (vergessen?)  |
|                          | Anmelden   |
|                          | Registrieren   |
|                          | [Impressum] [Datenschutzerklärung]   |

Damit Sie sich bei der Profilverwaltung anmelden können, ist es notwendig, dass Sie sich im Universitätsnetz befinden.

Dazu nutzen Sie entweder einen der Rechner auf dem Campusgelände (z. B. im Computerraum A024), verbinden sich mit dem WLAN (z. B. WLAN "eduroam") oder nutzen einen VPN-Tunnel, um in das Universitätsnetz zu gelangen.



### Hinterlegung der Kontakt-Mailadresse



#### 2. Schritt: Geben Sie eine Kontakt-Mailadresse an

| ← C (≜ ht         | ttps:// <b>profile.uni-koblenz.de</b> /user.cgi                                  |
|-------------------|--|
| Profilverwaltung: | Stammdaten Heimatverzeichnis Quotierung Passwort Ausdrucke Gruppen Mailinglisten |
| Ihre Stam         | mdaten   |
| Rechnerkennung    | kaiser-wilhelm   |
| Name              | Kaiser Wilhelm   |
| E-Mail            | kaiser-wilhelm@uni-koblenz.de  |
| Status            | Gast   |
| Kontakt           | Kontakt-Mailadresse Ändern   |
| Gültigkeit        | Bis zum 31.12.2024   |
|                   |  |
|                   |  |
|                   |  |
|                   |  |
|                   |  |
|                   |  |



### Ihr MFA-Token im Profil



#### Ohne angegebene Kontakt-Mailadresse erscheint ein MFA-Token für Sie im Profil

| ← C (                    | rofile.uni-koblenz.de/user.cgi  |
|--------------------------|---|
| Profilverwaltung: Stamme | daten Heimatverzeichnis Quotierung Passwort Ausdrucke Gruppen Mailinglisten |
| Ihre Stammd              | aten  |
| Rechnerkennung           | kaiser-wilhelm  |
| Name                     | Kaiser Wilhelm  |
| E-Mail                   | kaiser-wilhelm@uni-koblenz.de   |
| Status                   | Gast  |
| Kontakt                  | Kontakt-Mailadresse Ändern  |
| Gültigkeit               | Bis zum 31.01.2025  |
| MFA-Code                 | VBytGQhDKNpI5MMS6dbF  |
|                          |   |
|                          |   |
|                          |   |
|                          |   |

Wenn Sie noch keine Kontakt-Mailadresse in Ihrem Profil angegeben haben, wird für Sie ein MFA-Code generiert. Diesen können Sie in Ihrem Profil einsehen.

Um jedoch ohne Kontakt-Mailadresse auf Ihr Profil zugreifen zu können, müssen Sie sich im Universitätsnetz befinden.







#### Voraussetzungen für die Anmeldung in der Profilverwaltung





Wenn Sie sich nicht innerhalb des Universitätsnetzwerks befinden (und keinen VPN-Tunnel benutzen), können Sie sich ohne einen 2. Faktor, wie zum Beispiel eine Kontakt-Mailadresse, nicht anmelden.

<u>Hier</u> gelangen Sie zu der Erklärung, wie Sie eine Kontakt-Mailadresse hinterlegen.





#### 1. Schritt: Eingabe Ihrer Anmeldedaten







### 2. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse







#### 2. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse







#### **Erfolgreiche Anmeldung**

| ← C (⊡ https://pro        | file.uni-koblenz.de/user.cgi                  |                              |
|---------------------------|---|------------------------------|
| Profilverwaltung: Stammda | ten Heimatverzeichnis Quotierung Passwort Aus | drucke Gruppen Mailinglisten |
| Ihre Stammda              | iten  |                              |
| Rechnerkennung            | kaiser-wilhelm                                |                              |
| Name                      | Kaiser Wilhelm                                |                              |
| E-Mail                    | kaiser-wilhelm@uni-koblenz.de                 |                              |
| Status                    | Gast  |                              |
| Kontakt                   | Ihre Kontakt-Mailadresse                      | Ändern                       |
| Gültigkeit                | Bis zum 31.12.2024                            |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |

Auf der ersten Seite Ihres Profils finden Sie alle wichtigen Daten: Z. B. Ihre Rechnerkennung, E-Mailadresse, Ihre Matrikelnummer, falls Sie studieren, sowie Ihre hinterlegte Kontakt-Mailadresse.









### Anmeldung beim <u>MFA-Server</u> der Uni Koblenz

| weiter:denken<br>Anmelden bei MFA Serve                                     | <b>ität<br/>z</b><br>r Uni Koblenz |  |
|---|------------------------------------|--|
| weiter:denken<br>Multifaktor Authentifizierungsserver der Universität Koble | anz                                |  |
| Kennung   |                                    |  |
| kaiser-wilhelm  |                                    |  |
| Passwort  |                                    |  |
|   |                                    |  |
| Anmeldung nicht speichern   | J                                  |  |
| Die gegebene Zustimmung zur Weitergabe Ihrer Info                           | rmationen an diesen Dienst wird    |  |
| Anmeldung   |                                    |  |
| Login with security key / passkeys  |                                    |  |
| Passwort versessen?   |                                    |  |
| <ul><li>Hilfe benötigt?</li></ul>   |                                    |  |
| © Universität Koblenz 2024   Impressum   D                                  | atenschutzerklärung                |  |

Unter <u>mfa.uni-koblenz.de</u> können Sie neue Token ausrollen, mit welchen Sie sich dann bei den meisten Diensten der Universität im Sinne der Multifaktorauthentifizierung anmelden können.

Hier melden Sie sich mit Ihrer Uni-Kennung und dem dazugehörigen Passwort an.





### 1. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse

| Anmelden bei MFA Server Uni Koblenz   | Nachdem Sie Ihre Anmeldedaten<br>bestätigt haben, wird Ihnen   |
|---|--|
| Weiter:denken         Multifaktor Authentifizierungsserver der Universität Koblenz         Bitte das Einmalpasswort für einen der folgenden Token eingeben: | Authentifizierungscode an Ihre<br>hinterlegte Kontakt-Mailadresse<br>gesendet.                               |
| Wienergrüfen  |  |
| Starte Tokenverfahren neu  Passwort vergessen? Hilfe benötigt?  | Wenn Sie den Code in das<br>Eingabefeld eingegeben haben,<br>können Sie mit <i>Überprüfen</i><br>fortfahren. |
| © Universität Koblenz 2024   Impressum   Datenschutzerklärung   |  |





2. Schritt: Nutzungsbedingungen und Informationsweitergabe

Nachdem Sie die Nutzungsbedingungen und Informationsweitergabe gelesen und bestätigt haben, können Sie auf dieser Seite mit Anmelden fortfahren.







#### Erfolgreiche Anmeldung beim MFA-Server

| I Alle Token | Tokenanzahl: 1<br>Seriennummer● ▼      | Тур∙ ▼                          | aktiv• Beschreibung•                                       | <b>T</b> Fehlerzähler•                        | Rollout Status•                 |
|--------------|--|---------------------------------|--|---|---------------------------------|
|              | PIEM004226E5                           | email                           | Kontaktmailadress  | se 0  |                                 |
|              | welche Sie<br>Wenn Sie i<br>haben, wir | für die<br>noch kei<br>d Ihre Ü | All Ihren au<br>MFA nutzen<br>ne weiteren<br>bersicht, wie | können.<br>Token ers<br>e hier im B<br>alten. | Token,<br>tellt<br>eispiel, nur |











#### Was unterscheidet Faktor und Token?

Ein **Token** ist ein *spezifisches Instrument oder Gerät*, das im Rahmen des Faktors *Besitz* verwendet wird.

Ein **Faktor** ist eine *Kategorie der Authentifizierung*, die eine Art von Information beschreibt, die zur Identitätsprüfung verwendet wird.







### Token-Typen I

#### 1. Hardware-Token:

- 1. Physische Geräte wie USB-Sticks, Schlüsselanhänger oder Chipkarten.
- 2. Beispiele: YubiKey, RSA SecurID.
- 3. Funktion: Sie erzeugen Einmalpasswörter (OTP) oder dienen als kryptografischer Schlüssel, der für die Authentifizierung benötigt wird.

#### 2. Software-Token:

- 1. Digitale Tokens, die auf einem Smartphone, Tablet oder Computer per App generiert werden.
- 2. Beispiel-Apps: Google Authenticator, Microsoft Authenticator, den 2FAS (iOS), Aegis (Android) und Andere.
- 3. Funktion: Sie erzeugen zeitbasierte Einmalpasswörter (TOTP) oder bieten Push-Benachrichtigungen zur Authentifizierung.







### Token-Typen II

#### 3. SMS- oder E-Mail-Token:

- 1. Ein einmalig gültiger Code, der per SMS oder E-Mail an die Nutzer\*innen gesendet wird.
- 2. Funktion: Dient als kurzfristig nutzbarer Authentifizierungsfaktor.

#### 4. Biometrische Token:

- 1. Daten wie Fingerabdrücke, Gesichtserkennung oder Sprachmuster.
- 2. Funktion: Stellen sicher, dass der Benutzer persönlich anwesend ist.







## Welche Token stehen an der Universität Koblenz unter mfa.uni-koblenz.de zur Verfügung?





Sie sollten unbedingt **mehr als einen Token** ausrollen, damit Sie immer die Möglichkeit haben, sicher auf Ihr Konto zugreifen zu können!

https://uni-ko.de/mfa-token





#### Zeitbasierte Einmalpasswörter (TOTP)

Bei der Einrichtung wird ein geheimer Startwert z. B. über einen QR-Code auf Ihr Smartphone übertragen. Eine Authentifikations-App (Beispiele siehe <u>Seite</u> <u>26</u>) generiert daraufhin alle 30 Sekunden ein neues Einmalpasswort. Beim Login ist das aktuelle Passwort einzugeben.

#### Vorteil:

 Kann auf jedem Smartphone mit der passenden App genutzt werden – keine zusätzliche Hardware notwendig

#### Nachteil:

 Abhängigkeit vom Smartphone – wenn das Gerät nicht funktionsfähig ist, gibt es keinen Zugriff









### Token

#### TAN-Liste (PPR)

Eine gedruckte Liste mit 100 Einmalpasswörtern zur Authentifizierung. Alle Passwörter sind einmal benutzbar und müssen danach als angewendet markiert werden. Bitte denken Sie rechtzeitig daran, eine neue Liste zu erstellen, bevor die alte aufgebraucht ist.

#### Vorteil:

- Benötigt keine zusätzlichen Geräte oder Software
- Offline anwendbar

#### Nachteil:

- Verlust der Liste verwehrt den Zugriff
- Erfordert manuelle Pflege es müssen immer neue Listen angefertigt/ausgedruckt werden, wenn die alte aufgebraucht ist









### Yubico OTP (Yubikey AES Mode)

Der Yubikey ist ein Sicherheits-Token der Firma Yubico. Er hat einen eingebauten Einmalpasswortgenerator, dessen Startwert in unserem MFA-System hinterlegt werden kann. Bei entsprechender Konfiguration verhält sich der Yubikey wie eine USB-Tastatur und gibt auf Tastendruck ein Einmalpasswort aus. Auch Alternativprodukte zum Yubikey, die den Anforderungen entsprechen, wären für MFA denkbar.

#### Vorteil:

- Einfache Bedienung per Knopfdruck
- Lokal generierte Passwörter Unabhängigkeit vom Netzwerk

Nachteil:

• Abhängigkeit vom Gegenstand – Verlust oder Defekt verwehren den Zugriff









### WebAuthn

Token

Dieses Verfahren nutzt asymmetrische Verschlüsselung: Ein privater Schlüssel bleibt sicher auf Ihrem Gerät, während der öffentliche Schlüssel bei der Gegenstelle hinterlegt wird. Bei Anmeldung wird eine Anfrage gestartet, die nur mit dem privaten Schlüssel beantwortet werden kann. Für die Speicherung kommen unter anderem spezielle USB-Sticks (wie z. B. YubiKey), Sicherheitschips (TPM) oder Smartphones infrage.

#### Vorteil:

 Sehr benutzerfreundlich, da kein Passwort mehr eingegeben werden muss – die Authentifizierung erfolgt per Knopfdruck

#### Nachteil:

- Erfordert spezielle Hardware wie einen YubiKey oder einen Sicherheitschip
- Die Einrichtung ist komplexer im Vergleich zu anderen Token















#### Zeitbasierte Einmalpasswörter (TOTP) ausrollen

|                     | Navan Talam ayan Ilan   |                               |
|---------------------|---|-------------------------------|
|                     |   |                               |
|                     | TOTP: Zeitbasiertes Einmalpasswort.   | ~                             |
|                     | Der TOTP-Token ist ein zeit-basierter Token. Sie können den geheimen Schlüssel hier einfügen oder den Server einer<br>generieren lassen. Diesen können Sie in Ihre Authenticator-App importieren, indem Sie den QR-Code scannen. Beach<br>nicht alle Authenticator-Apps möglicherweise alle Parameter unterstützen. | n Schlüssel<br>hten Sie, dass |
|                     | Tokendaten  |                               |
|                     | 🗹 OTP-Schlüssel auf dem Server erzeugen   |                               |
| Token ausrollen     | Der Server erzeugt den geheimen Schlüssel und es wird ein QR-Code angezeigt, den Sie mit einer Smartphone-App können.   | scannen                       |
|                     | OTP-Länge   |                               |
|                     | 6   | ~                             |
| Hilfe zu Tokentypen | Einige Authenticator-Apps unterstützen lediglich OTPs der Länge 6.  |                               |
|                     | Zeitschritt   |                               |
|                     | 30  | ~                             |
|                     | seconds.  |                               |
|                     | Hash-Algorithmus  |                               |
|                     | sha1  | ~                             |
|                     | Einige Authenticator-Apps unterstützen lediglich den SHA1-Algorithmus.  |                               |
|                     | Beschreibung  |                               |
|                     | App-generierte Zeitbasierte Passwörter  | -                             |
|                     | Token ausrollen   |                               |
|                     |   |                               |

Indem Sie in dem Auswahlmenu *TOTP: Zeitbasiertes Einmalpasswort* auswählen, lässt sich der Token ganz einfach unten über den Button *Token ausrollen* generieren.

In dem Feld *Beschreibung* sollten Sie unbedingt eine Beschreibung für Ihren Token eingeben. So sehen Sie beim Login auf einen Blick, welche Ihrer Token Sie nutzen können.





#### Zeitbasierte Einmalpasswörter (TOTP) ausrollen



Mit einer Authentifikations-App (Beispiele siehe <u>Seite 26</u>) können Sie den QR-Code scannen und somit durchgehend neue Tokens generieren, welche Sie für die Multifaktorauthentifizierung benutzen können.





#### Zeitbasierte Einmalpasswörter (TOTP) ausrollen

|                         | Seriennummer• <b>T</b>               | Type T            | aktive        | Beschreibung• <b>T</b>                    | Fehlerzähler | Rollout Status• T |
|-------------------------|--------------------------------------|-------------------|---------------|---|--------------|-------------------|
| C Token ausrollen       | PIEM004226E5                         | email             | aktiv         | Kontaktmailadresse                        |              |                   |
| <b>3</b> Hilfe zu Token | PPR0004FCC7                          | paper             | aktiv         | Liste von Einmalpasswörtern<br>auf Papier |              |                   |
|                         | TOTP0004A3ED                         | totp              | aktiv         | App-generierte Zeitbasierte<br>Passwörter |              |                   |
| So sie<br>den T         | eht Ihre Übersio<br>Token erfolgreio | cht aus<br>ch aus | s, we<br>gero | nn Sie<br>llt haben.                      |              |                   |



# > TAN-Liste (PPR)

#### Multifaktorauthentifizierung

**Token ausrollen** 

TAN-Liste (PPR) ausrollen

Token

eduMFA

Alle Token

C Token ausrollen

Hilfe zu Tokentypen

|  | PPR: One Time                         |
|--|---------------------------------------|
| Neuen Token ausrollen  | Passworts printed                     |
| PPR: One Time Passwords printed on a sheet of paper.   | on a sheet of pape                    |
| Der Paper-Token ist eine ausgedruckte Liste mit OTP-Werten. Mit diesen OTP-Werten kann sich der Benutzer authentisieren. Er streicht dann die Werte aus der Liste, nachdem er sie benutzt hat. | auswählen, lässt<br>sich der Token    |
| Liste von Einmalpasswörtern auf Papier   | ganz einfach                          |
| Token ausrollen  | unten über den<br>Button <i>Token</i> |

CAktualisieren

kaiser-wilhelm @uni-koblenz.de (user)



Indem Sie in dem

Auswahlmenu

heet of paper ählen, lässt er Token einfach über den n Token ausrollen generieren.

In dem Feld Beschreibung sollten Sie unbedingt eine Beschreibung für Ihren Token eingeben. So sehen Sie beim Login auf einen Blick, welche Ihrer Token Sie nutzen können.







#### TAN-Liste (PPR) ausrollen

| eduMFA       | CAktualisieren kaiser-wilhelm @uni-koblenz.de (user) 🔹   |
|--------------|--|
| I Alle Token | Neuen Token ausrollen   Der Token mit der Seriennummer PPR0004CF3B wurde erfolgreich ausgerollt.   Der OTP-Schlüssel     OTP-Liste drucken     Neuen Token ausrollen |
|              | Über den Button <i>OTP-Liste drucken</i> können<br>Sie Ihre ausgerollte Liste entweder direkt<br>ausdrucken oder als PDF speichern.                                  |





#### TAN-Liste (PPR) ausrollen

| Alle Token        |                                     |                  | aktive        | Beschreibunge                             | Fehlerzähler•     | Rollout Statuse  |
|-------------------|-------------------------------------|------------------|---------------|---|-------------------|------------------|
| C Token ausrollen |                                     |                  |               |   | 1 officization of | - Tonout Statust |
|                   | PIEM004226E5                        | email            | aktiv         | Kontaktmalladresse                        | 0                 |                  |
| 🕄 Hilfe zu Token  | PPR0004FCC7                         | paper            | aktiv         | Liste von Einmalpasswörtern<br>auf Papier |                   |                  |
|                   | TOTP0004A3ED                        | totp             | aktiv         | App-generierte Zeitbasierte<br>Passwörter | 0                 |                  |
| So sie<br>den T   | eht Ihre Übersio<br>oken erfolgreio | cht au<br>ch aus | s, we<br>gero | nn Sie<br>llt haben.                      |                   |                  |







Bitte bewahren Sie die TAN-Liste an einem sicheren Ort auf. Zur Sicherheit sollen Sie immer zwei Token ausrollen, so dass Sie immer eine Alternative haben.



# > WebAuthn (YubiKey)

#### > Multifaktorauthentifizierung

| D Token      | S Aktualisieren kaiser-wilhelm @uni-koblenz.de (user)  |   | Indem Sie in dem              |
|--------------|--|---|-------------------------------|
| ken          | Neuen Token ausrollen  |   | WebAuthn: Einen               |
| ausrollen    | WebAuthn: Einen WebAuthn-Token ausrollen.  | • | ausrollen                     |
| ı Tokentypen | Der WebAuthn-Token ist vom W3C und der Fido Alliance definiert. Sie können diesen Token bei mehreren, verschiedenen<br>Webdiensten registrieren.<br>Beschreibung | ł | auswählen,<br>können Sie ganz |
|              |  |   |                               |

Token ausrollen



eduMFA

Alle Token

C Token ausrol

Hilfe zu Toke

### WebAuthn (mit YubiKey)



WebAuthn: Einen WebAuthn-Token ausrollen auswählen, können Sie ganz einfach unten über den Button Token ausrollen die Erstellung des Tokens starten.

In dem Feld *Beschreibung* sollten Sie unbedingt eine Beschreibung für Ihren Token eingeben. So sehen Sie beim Login auf einen Blick, welche Ihrer Token Sie nutzen können.

Anmeldung mit YubiKey



#### WebAuthn (mit YubiKey)



weiter:denken

Um den YubiKey als WebAuthn zu registrieren, wählen Sie in dem Pop-Up Window unter *Weitere Optionen* die Option *Verwenden eines anderen Geräts* aus.



#### WebAuthn (mit YubiKey)





In dem nächsten Auswahlfenster wählen Sie dann *Sicherheitsschlüssel* aus und bestätigen die Auswahl mit *Weiter*.



# WebAuthn (mit YubiKey)

**Token ausrollen** 







#### WebAuthn (mit YubiKey)







#### WebAuthn (mit YubiKey)





Spätestens jetzt müssen Sie Ihren YubiKey in einen freien USB-Slot einstecken.



#### WebAuthn (mit YubiKey)





Falls Sie noch keinen Sicherheitsschlüssen für Ihren YubiKey festgelegt haben, werden Sie nun aufgefordert einen anzulegen. Ansonsten geben Sie Ihren Sicherheitsschlüssel hier ein.

> Notieren Sie Ihren Sicherheitsschlüssel an einem sicheren Ort oder benutzen Sie einen Passwortmanager.



#### WebAuthn (mit YubiKey)



weiter:denken

An dieser Stelle müssen Sie den Knopf auf Ihrem YubiKey drücken, um das Setup abzuschließen.



#### WebAuthn (mit YubiKey)







#### WebAuthn (mit YubiKey)



|                     | Neuen Token ausro              | ollen                                       | - 11 |
|---------------------|--------------------------------|---|------|
| 🎖 Token ausrollen   | Der Token mit der Seriennummer | r WAN0059A0FB wurde erfolgreich ausgerollt. | - 11 |
|                     | Token ausgerollt               |   | - 11 |
|                     | Anmeldung mit YubiKey          | Der Token wurde ausgerollt.                 | - 11 |
| Hilfe zu Tokentypen |                                | Neuen Token ausrollen                       | - 11 |
|                     |                                |   |      |

Ihr YubiKey ist nun als Token für WebAuthn ausgerollt. Sie können nun einen neuen Token ausrollen oder links über den Reiter *Alle Token* Ihre ausgerollten Token einsehen.





#### TAN-Liste (PPR) ausrollen

|                 |                        | _                            |                   |               |   |               |                 |
|-----------------|------------------------|------------------------------|-------------------|---------------|---|---------------|-----------------|
| Token ausrollen |                        | Seriennummer• Y              | Тур• 🕈            | aktive        | Beschreibung• Y                           | Fehlerzählere | Rollout Status• |
|                 |                        | PIEM004226E5                 | email             | aktiv         | Kontakt-Mailadresse                       | 0             |                 |
| life zu Teken   |                        | PPR0004CF3B                  | paper             | aktiv         | Gedruckte Passwortliste auf<br>Papier     | 0             |                 |
| Hilfe zu Token  |                        | TOTP0004A3ED                 | totp              | aktiv         | App-generierte Zeitbasierte<br>Passwörter | 0             |                 |
|                 |                        | WAN0059A0FB                  | webauthn          | aktiv         | Anmeldung mit YubiKey                     |               |                 |
|                 |                        |                              |                   |               |   |               |                 |
| -               | so sieht l             | hre Ubersic                  | cht aus           | s, we         | nn Sie                                    |               |                 |
| (               | den Toke               | en erfolgreid                | ch aus            | gero          | llt haben.                                |               |                 |
|                 |                        |                              |                   |               |   |               |                 |
| (               | So sieht l<br>len Toke | hre Übersic<br>en erfolgreic | cht aus<br>ch aus | s, we<br>gero | nn Sie<br>llt haben.                      |               |                 |



# > Yubico OTP (Yubikey AES Mode)



### Yubico OTP (Yubikey AES Mode)



Zunächst müssen Sie auf der Webseite von Yubico den YubiKey Manager herunterladen, um Ihren YubiKey zu konfigurieren und als Token nutzen zu können.

Über den QR-Code oder den Link kommen Sie direkt zum Downloadbereich von Yubico:



www.yubico.com/support/d ownload/yubikey-manager





### Yubico OTP (Yubikey AES Mode)



Um Ihren YubiKey als Token ausrollen zu können, müssen Sie zunächst mit dem YubiKey Manager von Yubico eine ID und den Sicherheitsschlüssel generieren.

Um zu beginnen, öffnen Sie die Software von Yubico und stecken Sie Ihren YubiKey in einen freien USB-Slot.





### Yubico OTP (Yubikey AES Mode)







### Yubico OTP (Yubikey AES Mode)



Wenn Ihr YubiKey von dem YubiKey Manager erkannt wurde, klicken sie auf den Reiter *Applications* und wählen darunter die erste Option *OTP* aus.





### Yubico OTP (Yubikey AES Mode)

|                   |  | YubiKey 5 NFC (106637  | '04) 🕐 Help 🛈 About |
|-------------------|--|------------------------|---------------------|
| ubico Home        | Applications Interfaces  |                        | ,                   |
| OTP<br>Home / OTP | Short Touch (Slot 1)<br>This slot is empty<br>Delete Configure | wap This slot is empty |                     |
| < Back            |  |                        |                     |

Auf dieser Seite finden Sie zwei Anwendungsmöglichkeiten: *Short Touch* und *Long Touch*. Ihr YubiKey kann dazu konfiguriert verschiedene Dinge ausgeben, je nach dem wie lange sie den Knopf auf Ihrem YubiKey drücken.

Klicken Sie unter *Short Touch* auf *Configure*, um die Tokenausgabe für eine kurze Berührung des Knopfes einzustellen.





### Yubico OTP (Yubikey AES Mode)

| YubiKey Manager  |                   |                      |                          | - 0  | ×       |
|--|-------------------|----------------------|--------------------------|------|---------|
|  |                   |                      | YubiKey 5 NFC (10663704) | Help | O About |
| ubico Home Applications                                    | Interfaces        |                      |                          |      |         |
| Select Credential Typ<br>Home / OTP / Short Touch (Slot 1) | e                 |                      |                          |      |         |
|  | Yubico OTP        | O Challenge-response |                          |      |         |
|  | O Stat c password | О ОАТН-НОТР          |                          |      |         |
|  |                   |                      |                          |      |         |
|  |                   |                      |                          |      |         |
|  |                   |                      |                          |      |         |
| < Back   |                   |                      |                          | N    | lext ≻  |

Auf dieser Seite lassen Sie Yubico OTP ausgewählt und klicken auf *Next*, um fortzufahren.





### Yubico OTP (Yubikey AES Mode)

| YubiKey Manager                                | - 🗆 X                                   |
|--|---|
|  | YubiKey 5 NFC (10663704) 💿 Help 💿 About |
| Ubico Home Applications Interfaces             |   |
| Yubico OTP                                     |   |
| Home / OTP / Short Touch (Slot 1) / Yubico OTP |   |
|  |   |
| Public ID                                      | Use serial                              |
| Private ID                                     | Generate                                |
| Secret key                                     | Generate                                |
|  |   |
|  |   |
|  |   |
|  |   |
| < Back   | 🗌 Upload 🗸 Finish                       |

Auf dieser Seite wählen Sie zunächst das Feld *Use serial* aus. Damit haben Sie die Taste aktiviert, welche Ihren Code ausgibt. Dann klicken sie jeweils auf *Generate* bei Private ID und beim Secret key.





### Yubico OTP (Yubikey AES Mode)

|   | - 🗆 X                                |
|---|--------------------------------------|
|   | YubiKey 5 NFC (77777) O Help O About |
| ubico Home Applications Interfaces              |                                      |
|   |                                      |
| International Content (Solution 1) / Yubico OTP |                                      |
|   |                                      |
| Public ID                                       | Vse serial                           |
| Private ID                                      | Generate                             |
| jecret key                                      | Generate                             |
|   |                                      |
|   |                                      |
|   |                                      |
|   |                                      |
|   |                                      |
| < Back  |                                      |

Nun haben Sie in jeder Zeile einen einzigartigen Code stehen. Bevor Sie den Vorgang mit *Finish* beenden, sollten Sie sich den Code, welcher neben *Secret key* generiert worden ist, kopieren. Schreiben Sie ihn temporär auf oder speichern Sie ihn kurzfristig, denn Sie brauchen ihn, um Ihren Token auszurollen.





### Yubico OTP (Yubikey AES Mode)

| 👂 YubiKey Manager |   |   | - 0  | ×       |
|-------------------|---|---|------|---------|
| vubico Home       | Applications Interfaces                         | YubiKey 5 NFC (10663704)  | Help | O About |
| OTP<br>Home / OTP | Short Touch (Slot 1)<br>This slot is configured | ← Swap Touch (Slot 2)<br>This slot is empty<br>Delete Configure |      |         |
| < Back            | Configured Y                                    | ubico OTP credential  |      |         |

Nun sollte bei dem Slot, den Sie konfiguriert haben, *This slot is configured* stehen.

Um Ihren YubiKey als Token auszurollen, können Sie jetzt die <u>mfa.uni-koblenz.de</u> Seite aufrufen.





### Yubico OTP (Yubikey AES Mode)

|                      | Neuen Token ausrollen   |  |
|----------------------|---|--|
|                      | Yubikey AES Mode: Einmalpasswort mit dem Yubikey.   |  |
| Alle Token           | Der Yubikey ist ein USB-Gerät, das ein ereignisbasiertes Eir  | nmalpasswort ausgibt. Dazu wird es als Tastatur erkannt. Sie können  |
| ថ្មី Token ausrollen | den Yubikey mit Personalisierungstools von Yubico initialisie<br>Wertes werden hier benötigt. Yubikesy, die mit der Yubiclouz<br>Zeichen UID und 32 Zeichen OTP) aus. Wenn ein Yubikey fi<br>Identity" 6 Bytes sein, was in der UID 12 Zeichen entspricht.<br>wenn Sie einen OTP-Wert in das Testfeld eingeben. | aren. Der geheime Schlüssel in Hex und die gesamte Länge des OTP<br>d kompatibel sind, geben eine Gesamtlänge von 44 Zeichen (12<br>ür den Yubicloud Service programmiert wird, dann muss die "Public<br>. Die gesamte OTP Länge des Yubikeys wird automatisch bestimmt, |
| Hilfe zu Tokentypen  | Tokendaten  |  |
|                      | Yubikey testen  |  |
|                      |   |  |
|                      | OTP-Schlüssel   |  |
|                      | 9638298-778296789-78842878645978  |  |
|                      | OTP-Länge 44  |  |
|                      | Beschreibung  |  |
|                      | Anmeldung mit YubiKey   |  |
|                      | та  | oken ausrollen   |
|                      |   |  |
|                      |   |  |
|                      |   |  |
|                      |   |  |

Wählen Sie hier Yubikey AES Mode: Einmalpasswort mit dem Yubikey.

Klicken Sie hier in das Textfeld und drücken die Taste auf Ihrem YubiKey. Ein Code sollte in dem Feld erscheinen.

Fügen Sie nun den Sicherheitsschlüssel, aus dem YubiKey Manager hier ein.

Im Feld *Beschreibung* sollten Sie unbedingt eine Beschreibung für Ihren Token eingeben. So sehen Sie beim Login auf einen Blick, welche Ihrer Token Sie nutzen können.





#### TAN-Liste (PPR) ausrollen

| Alle Token        | Tokenanzahl: 5         |          |        |   |               |                 |
|-------------------|------------------------|----------|--------|---|---------------|-----------------|
| C Token ausrollen | Seriennummer• <b>T</b> | Тур• 🔻   | aktiv● | Beschreibung•                             | Fehlerzähler• | Rollout Status• |
| -                 | PIEM004226E5           | email    | aktiv  | Kontakt-Mailadresse                       | 0             |                 |
|                   | PPR0004CF3B            | paper    | aktiv  | Gedruckte Passwortliste auf<br>Papier     | 0             |                 |
| • Hille zu Token  | TOTP0004A3ED           | totp     | aktiv  | App-generierte Zeitbasierte<br>Passwörter | 0             |                 |
|                   | UBAM0001A20D           | yubikey  | aktiv  | Anmeldung mit YubiKey                     |               |                 |
|                   | WAN0059A0FB            | webauthn | aktiv  | Anmeldung mit YubiKey                     |               |                 |
|                   |                        |          |        |   |               |                 |
| So sie            | ht Ihre Übersio        | :ht au   | s. we  | nn Sie                                    |               |                 |
| den T             | oken erfolgreid        | h aus    | gero   | llt haben.                                |               |                 |
|                   |                        |          | 0010   |   |               |                 |





### Ändern Ihres Uni-Passworts



### Passwortänderung bei der Profilverwaltung

| ← C 🗅 htt           | ps:// <b>profile.uni-koblenz.de</b> /user.cgi                                   |
|---------------------|---|
| Profilverwaltung: S | tammdaten Heimatverzeichnis Quotierung Passwort Ausdrucke Gruppen Mailinglisten |
| Ihre Stam           | ndaten  |
| Rechnerkennung      | kaiser-wilhelm  |
| Name                | Kaiser Wilhelm  |
| E-Mail              | kaiser-wilhelm@uni-koblenz.de   |
| Status              | Gast  |
| Kontakt             | Kontakt-Mailadresse Ändern  |
| Gültigkeit          | Bis zum 31.12.2024  |
|                     |   |
|                     |   |
|                     |   |
|                     |   |
|                     |   |

Über den Reiter *Passwort* bei der <u>Profilverwaltung</u> gelangen Sie zu der Seite, wo Sie Ihr Passwort ändern oder eine neue Sicherheitsfrage bestimmen können.



### Ändern Ihres Uni-Passworts



#### Passwortänderung bei der Profilverwaltung

| ← C  | enz.de/password.cgi  |   |  |       |
|--|--|---|--|-------|
| Profilverwaltung: Stammdaten Heima<br>Passwort ändern                          | atverzeichnis Quotierung Passwort Ausdrucke Gruppen Mailinglisten Su   |   | Hier können Sie ein<br>Passwort festlegen. | neues |
|  |  |   |  |       |
| Neues Passwort:  | new password   |   |  |       |
| Passwort-Bestätigung:  | repeat password  | - |  |       |
|  | Passwort ändern  |   |  |       |
|  |  |   |  |       |
| Sicherheitsfrage   |  |   |  |       |
| Die folgenden Daten werden benötigt,<br>Beantwortung der Sicherheitsfrage wird | wenn Sie einmal Ihr Passwort vergessen sollten. Nach der korrekten<br>d ein neues Passwort generiert und an die Kontakt-Mailadresse versendet. |   |  |       |
| Sicherheitsfrage:  | security question  |   |  |       |
| Antwort:   | define security answer   |   |  |       |
|  | Sicherheitsfrage ändern  |   |  |       |
|  |  |   |  |       |
|  |  |   |  |       |



### Sicherheitsfrage als 2. Faktor



### Festlegung oder Änderung der Sicherheitsfrage

| ← C (                             |                          |            |           |         |               |    |
|-----------------------------------|--------------------------|------------|-----------|---------|---------------|----|
| Profilverwaltung: Stammdaten Heir | matverzeichnis Quotierur | g Passwort | Ausdrucke | Gruppen | Mailinglisten | Su |
| Passwort ändern                   |                          |            |           |         |               |    |
| Neues Passwort:                   | new password             |            |           |         |               |    |
| Passwort-Bestätigung:             | repeat password          |            |           |         |               |    |
|                                   | Passwort ändern          |            |           |         |               |    |

#### Sicherheitsfrage

Die folgenden Daten werden benötigt, wenn Sie einmal Ihr Passwort vergessen sollten. Nach der korrekten Beantwortung der Sicherheitsfrage wird ein neues Passwort generiert und an die Kontakt-Mailadresse versendet.

Sicherheitsfrage:

Antwort:

Sobald die Multifaktorauthentifizierung flächendeckend zur Anmeldung genutzt werden kann, wird die Sicherheitsfrage als Faktor wegfallen.

Hier können Sie Ihre Sicherheitsfrage, welche Sie als zweiten Faktor für das Login beim Profilmanagement und bei Vergessen Ihres Passworts benutzen können, ändern.





Sollten Sie Fragen zu den hier dargestellten Inhalten haben, können Sie die Mitarbeitenden des ZIMT gerne kontaktieren. Sie erreichen uns unter:



support+mfa@uni-koblenz.de



ZIMT - Webseiten



Zu folgenden Zeiten:



