universität koblenz
weiter:denken

Multifaktorauthentifizierung (MFA)

Übersicht I

universität koblenz
weiter:denken

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

Übersicht II

universität koblenz
weiter:denken

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

Multifaktorauthentifizierung (MFA)

Multifaktorauthentifizierung (MFA)

universität koblenz
weiter:denken

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.

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

Notwendigkeit von MFA

universität koblenz
weiter:denken

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

universität koblenz
weiter:denken

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.

Weitere Informationen erhalten Sie hier:

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

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

Kontakt-Mailadresse als Voraussetzung für MFA

Kontakt-Mailadresse

universität koblenz
weiter:denken

Wozu dient die Kontakt-Mailadresse?

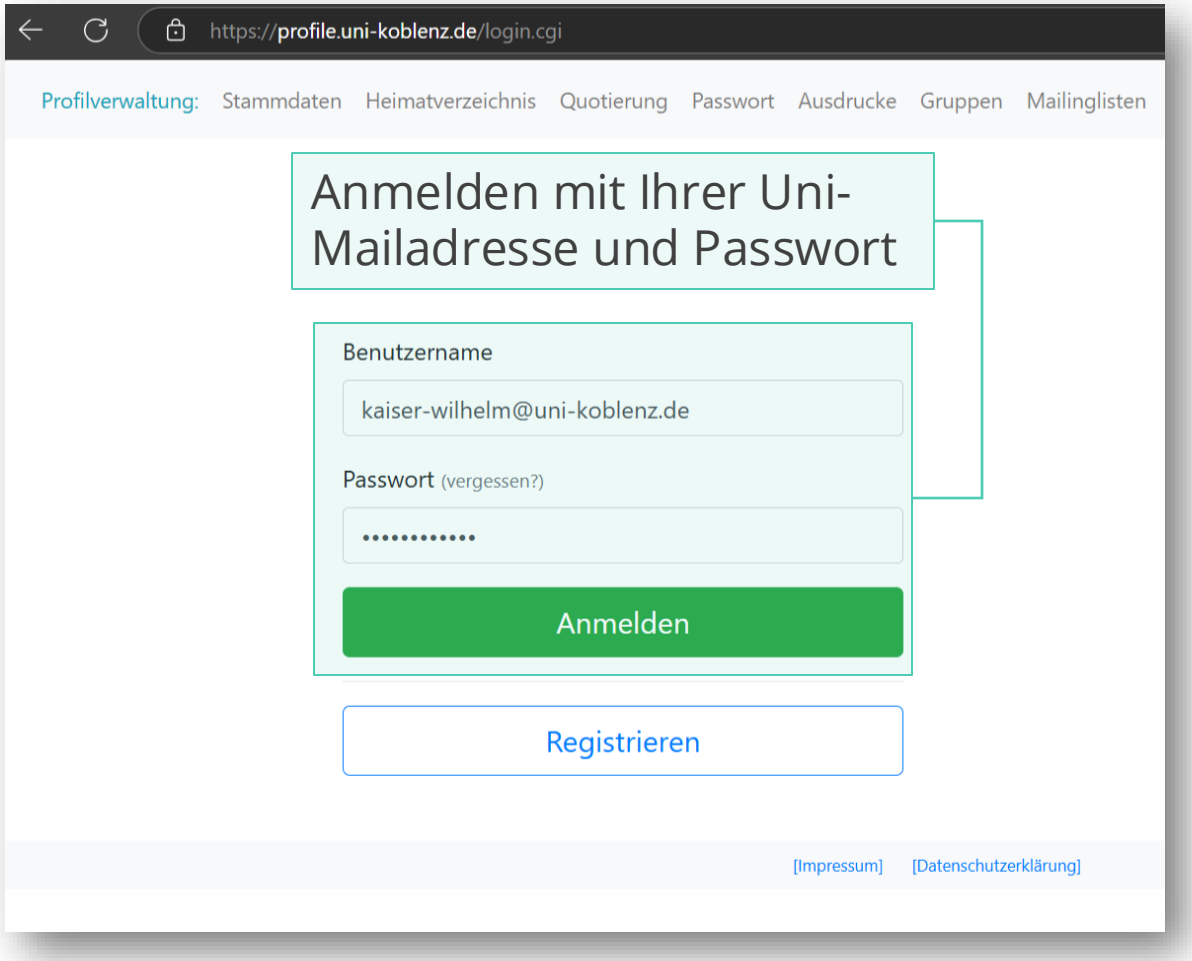
In Ihrem Profil muss eine zweite Mailadresse, die sogenannte Kontakt-Mailadresse, hinterlegt werden. Diese Adresse übernimmt mehrere wichtige Funktionen:

- **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

universität koblenz
weiter:denken

1. Schritt: Melden Sie sich bei der Profilverwaltung an



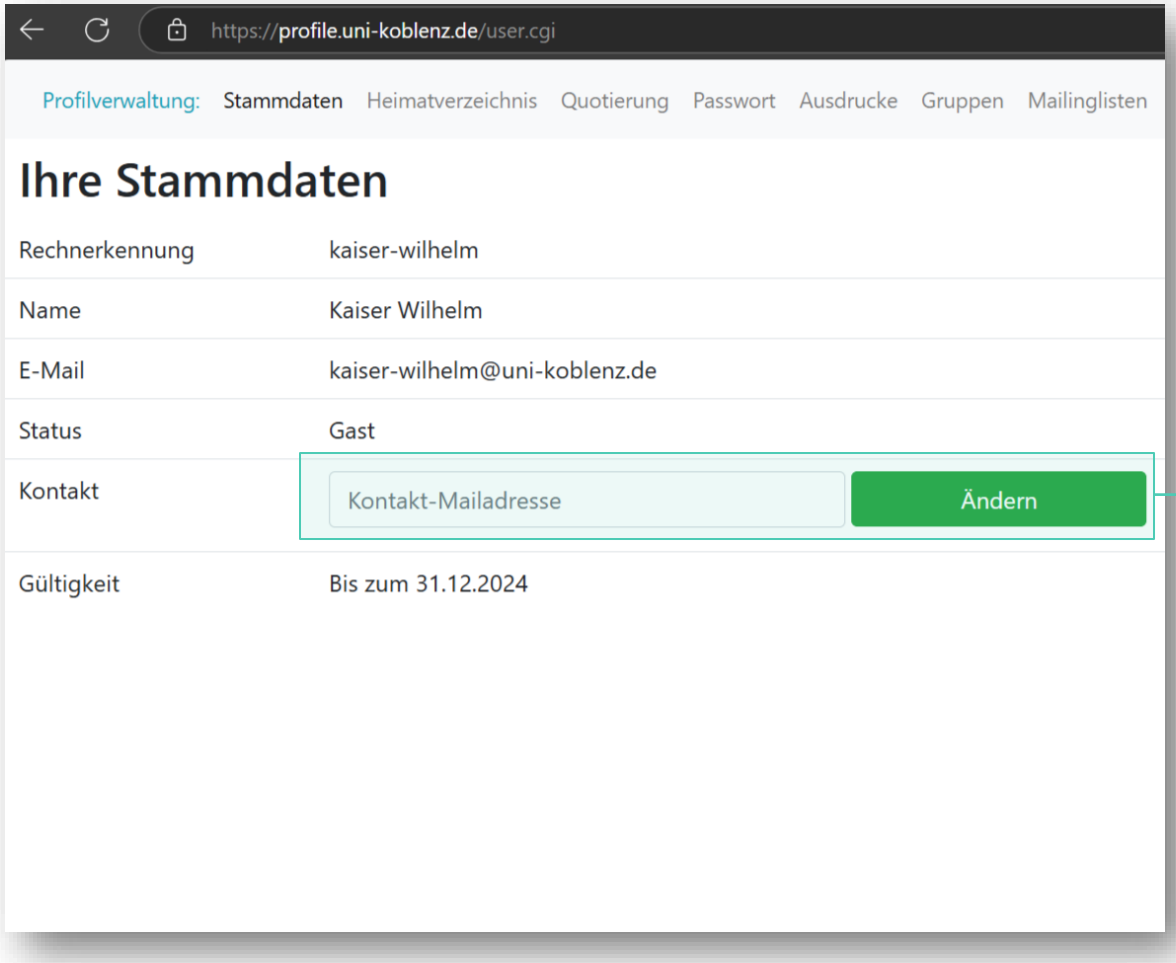
Damit Sie sich bei der Profilverwaltung anmelden können, ist es notwendig, dass Sie sich im Universitätsnetz befinden.

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

universität koblenz
weiter:denken

2. Schritt: Geben Sie eine Kontakt-Mailadresse an

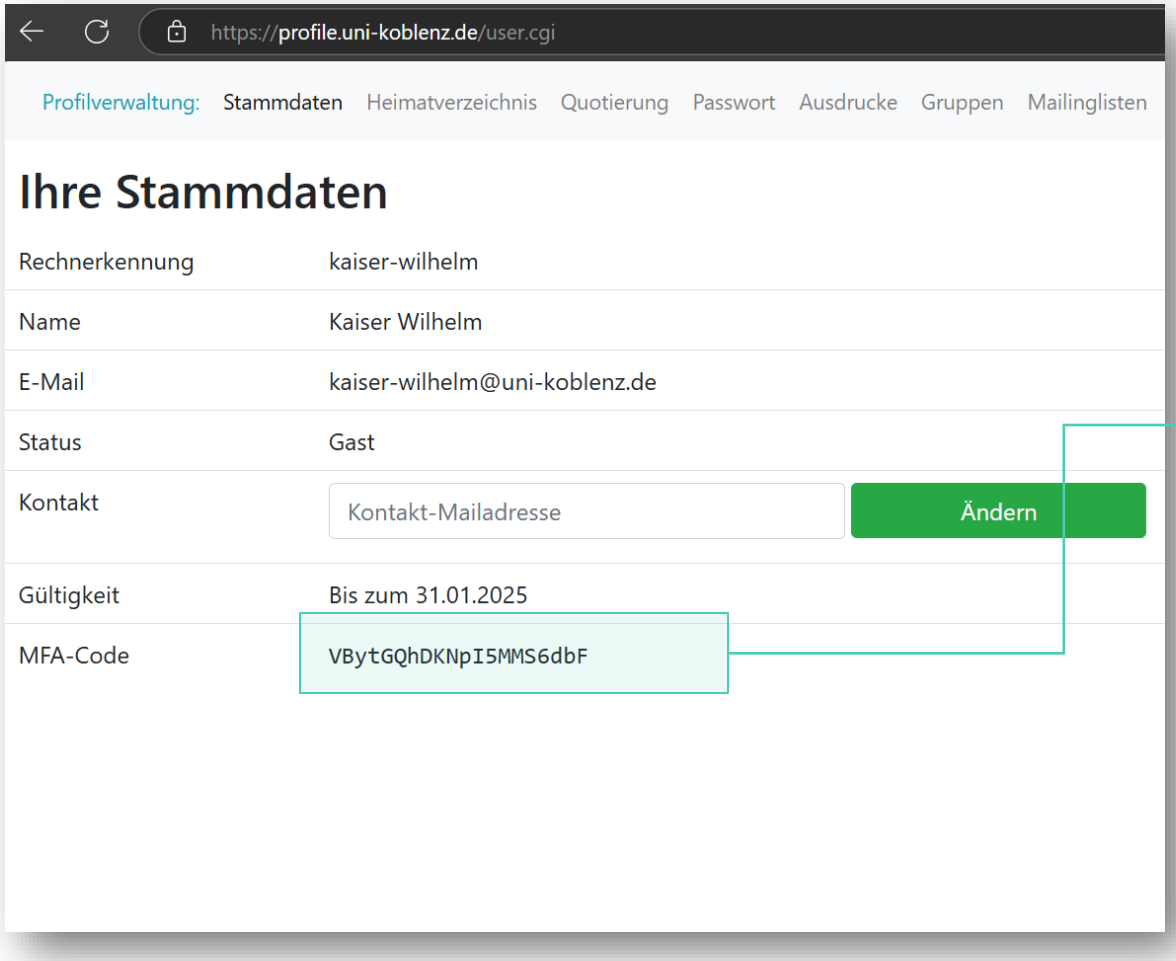


Hier können Sie eine gültige und aktuelle Kontakt-Mailadresse hinterlegen und mit Ändern bestätigen.

Ihr MFA-Token im Profil

universität koblenz
weiter:denken

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



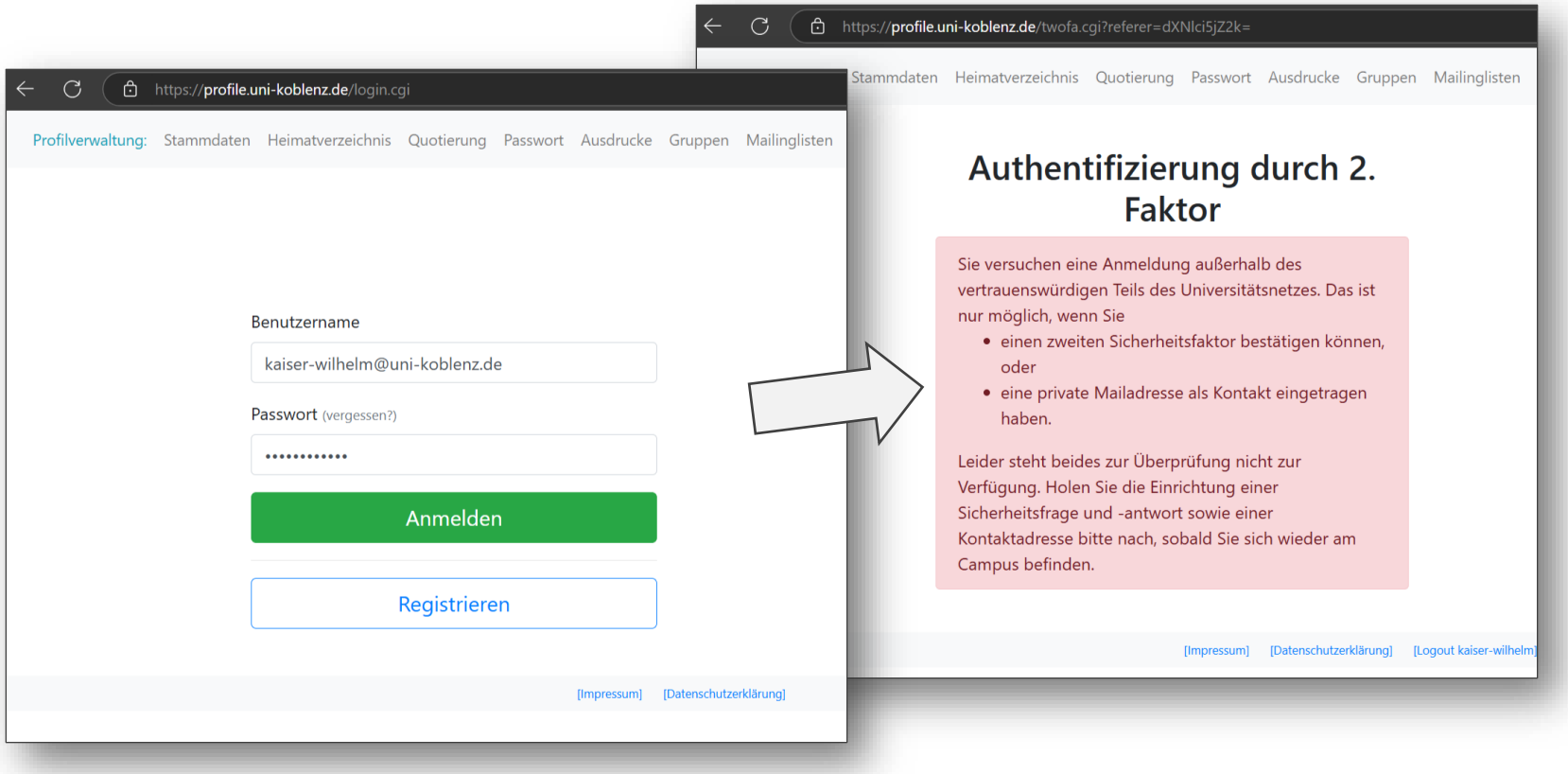
Wenn Sie noch keine Kontakt-Mailadresse in Ihrem Profil angegeben haben, wird für Sie ein MFA-Code generiert. Diesen können Sie in Ihrem Profil einsehen.

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

Beispiel 1: Anmeldung mit 2. Faktor im Profil

Beispiel: Anmeldung mit 2. Faktor

Voraussetzungen für die Anmeldung in der Profilverwaltung

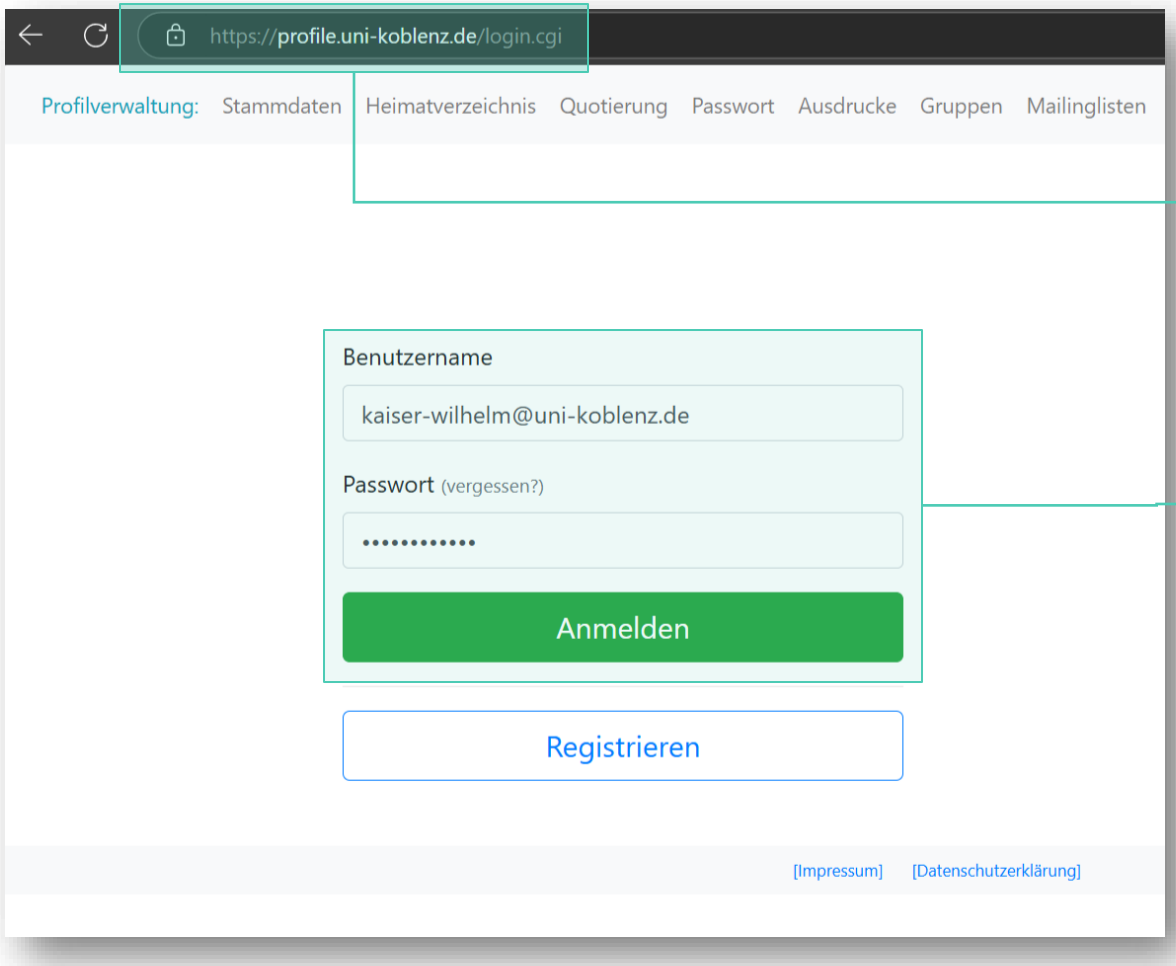


Wenn Sie sich nicht innerhalb des Universitätsnetzwerks befinden (und keinen VPN-Tunnel benutzen), können Sie sich ohne einen 2. Faktor, wie zum Beispiel eine Kontakt-Mailadresse, nicht anmelden.

Hier gelangen Sie zu der Erklärung, wie Sie eine Kontakt-Mailadresse hinterlegen.

Beispiel: Anmeldung mit 2. Faktor

1. Schritt: Eingabe Ihrer Anmeldedaten



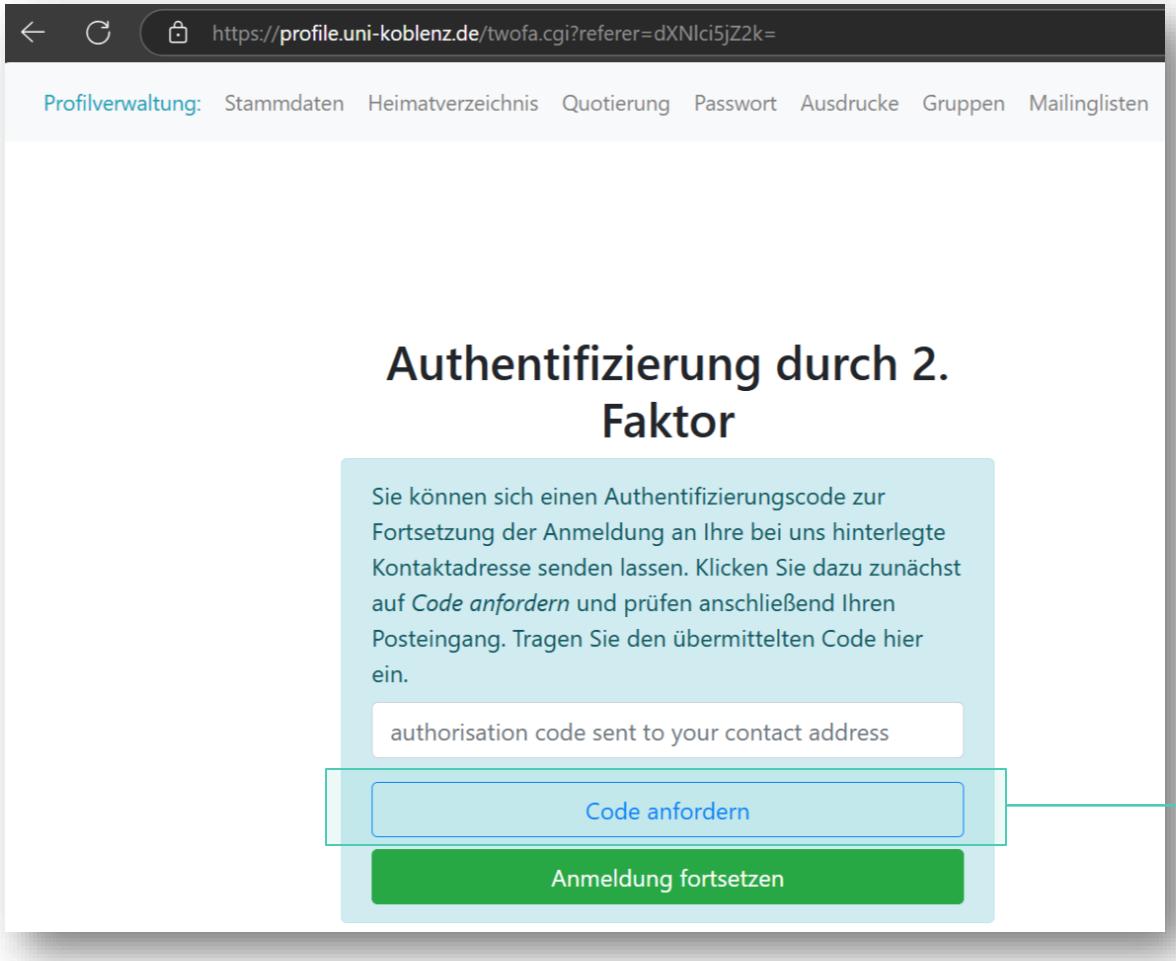
Link zur Profilverwaltung.

Anmelden mit Ihrer Uni-Mailadresse und dem dazugehörigen Passwort.

Beispiel: Anmeldung mit 2. Faktor

universität koblenz
weiter:denken

2. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse

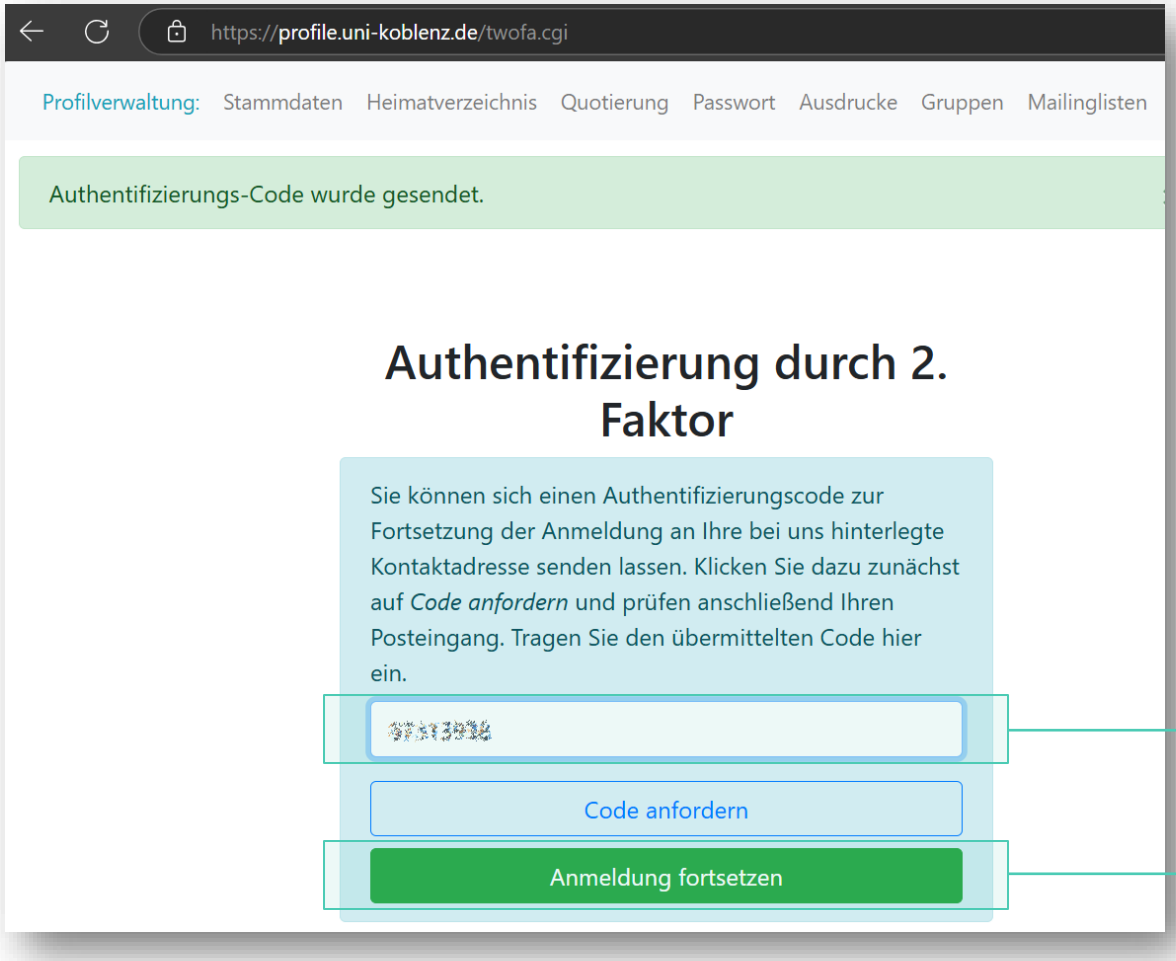


Mit Code anfordern können Sie sich einen Authentifizierungscode, an Ihre hinterlegte Kontakt-Mailadresse senden lassen.

Beispiel: Anmeldung mit 2. Faktor

universität koblenz
weiter:denken

2. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse

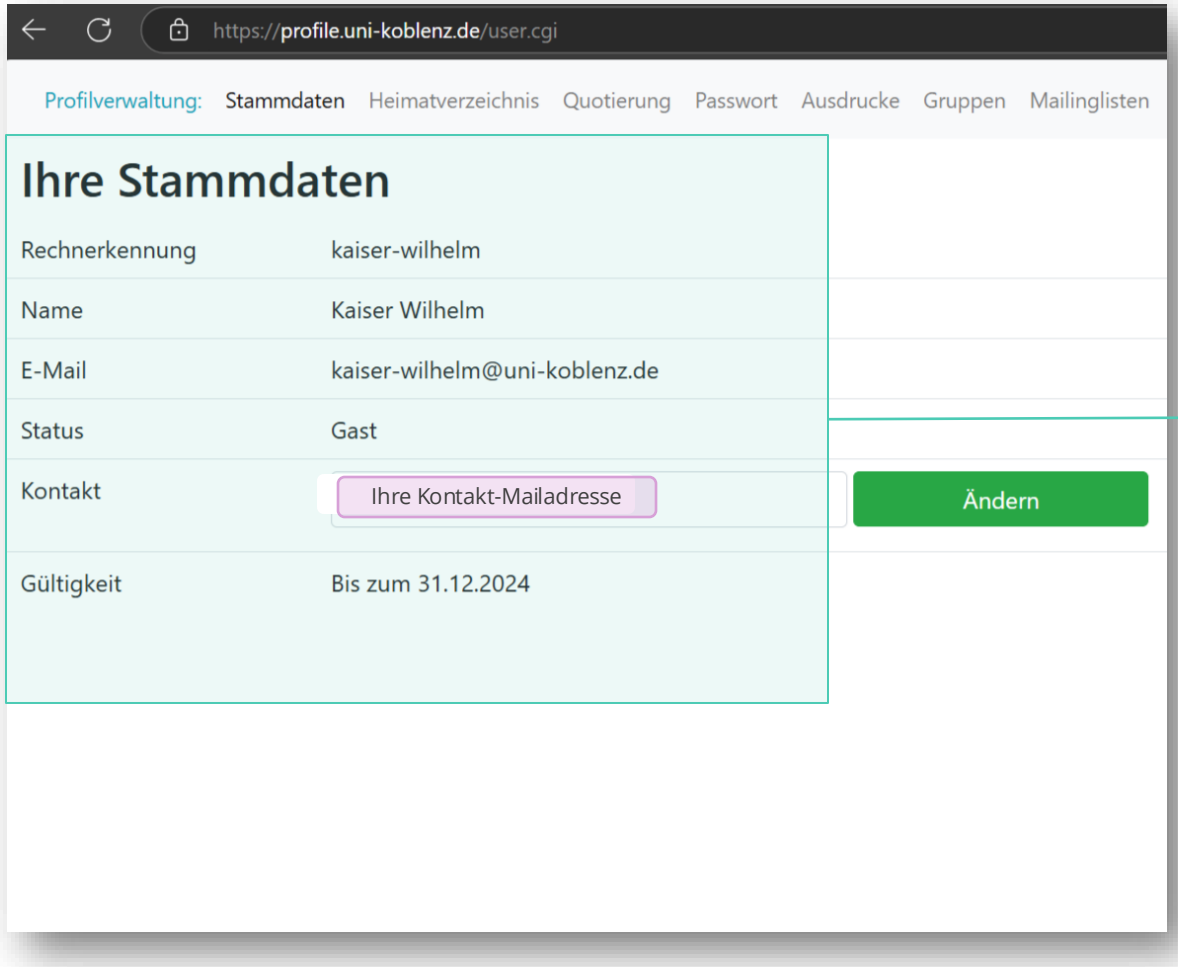


Den Authentifizierungscode, den Sie über Ihre Kontakt-Mailadresse bekommen haben, kopieren Sie in das Eingabefeld.

Klicken Sie hier, um die Anmeldung fortzusetzen.

Beispiel: Anmeldung mit 2. Faktor

Erfolgreiche Anmeldung



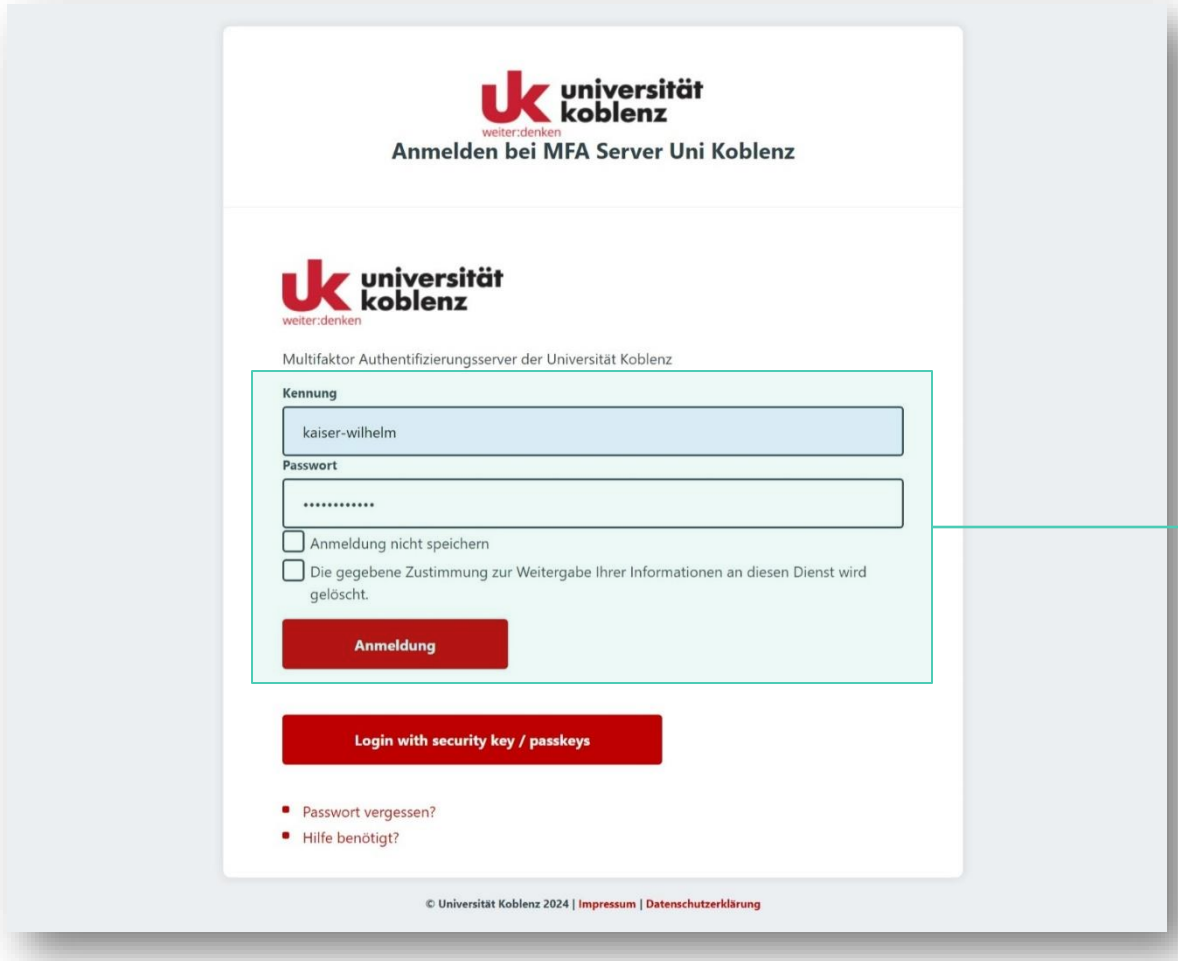
Auf der ersten Seite Ihres Profils finden Sie alle wichtigen Daten: Z. B. Ihre Rechnerkennung, E-Mailadresse, Ihre Matrikelnummer, falls Sie studieren, sowie Ihre hinterlegte Kontakt-Mailadresse.

Beispiel 2: Anmeldung mit 2. Faktor bei der Tokenverwaltung (mfa.uni-koblenz.de)

Beispiel: Anmeldung mit 2. Faktor

universität koblenz
weiter:denken

Anmeldung beim MFA-Server der Uni Koblenz

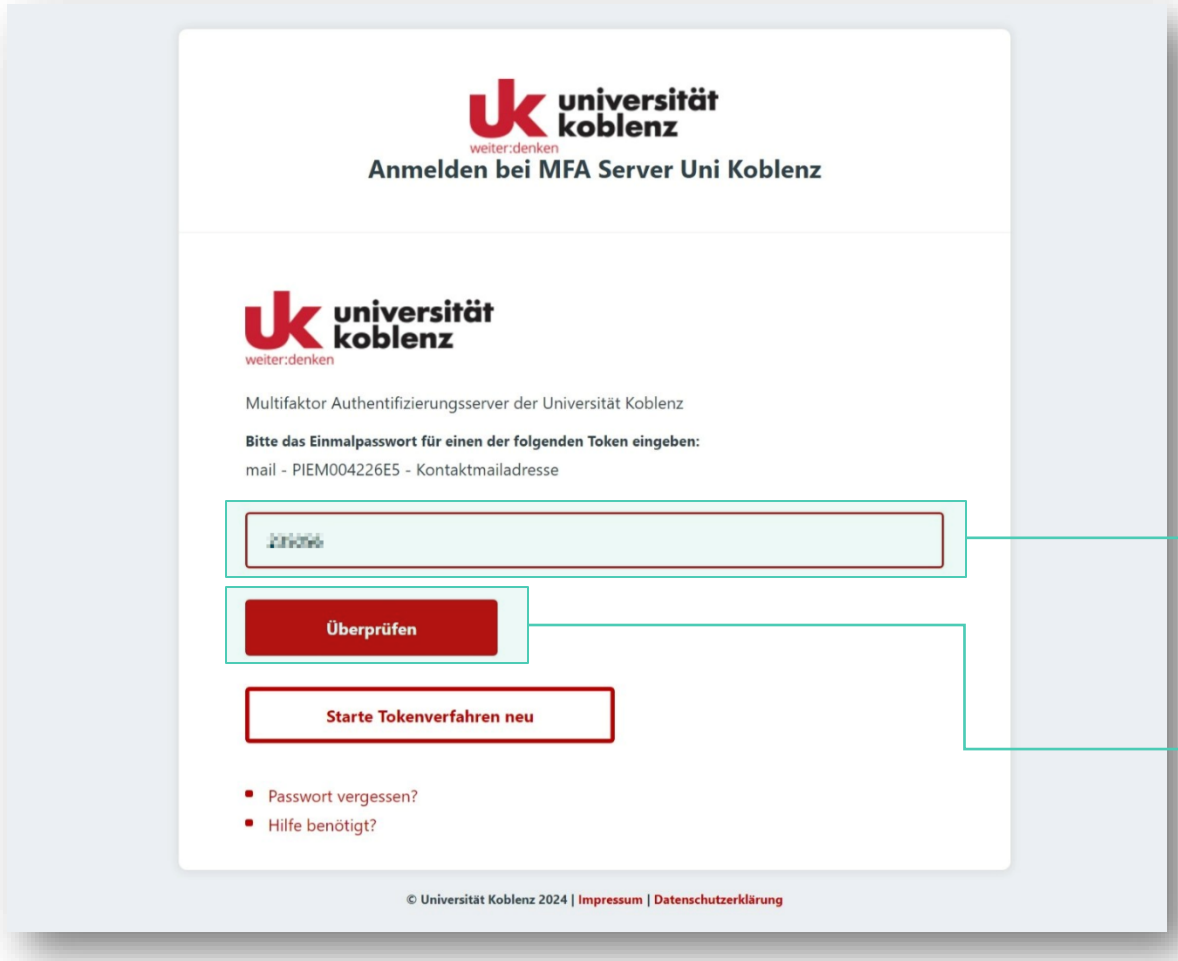


Unter mfa.uni-koblenz.de können Sie neue Token ausrollen, mit welchen Sie sich dann bei den meisten Diensten der Universität im Sinne der Multifaktorauthentifizierung anmelden können.

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

Beispiel: Anmeldung mit 2. Faktor

1. Schritt: Authentifizierung mit Hilfe der Kontakt-Mailadresse



Nachdem Sie Ihre Anmeldedaten bestätigt haben, wird Ihnen automatisch ein Authentifizierungscode an Ihre hinterlegte Kontakt-Mailadresse gesendet.

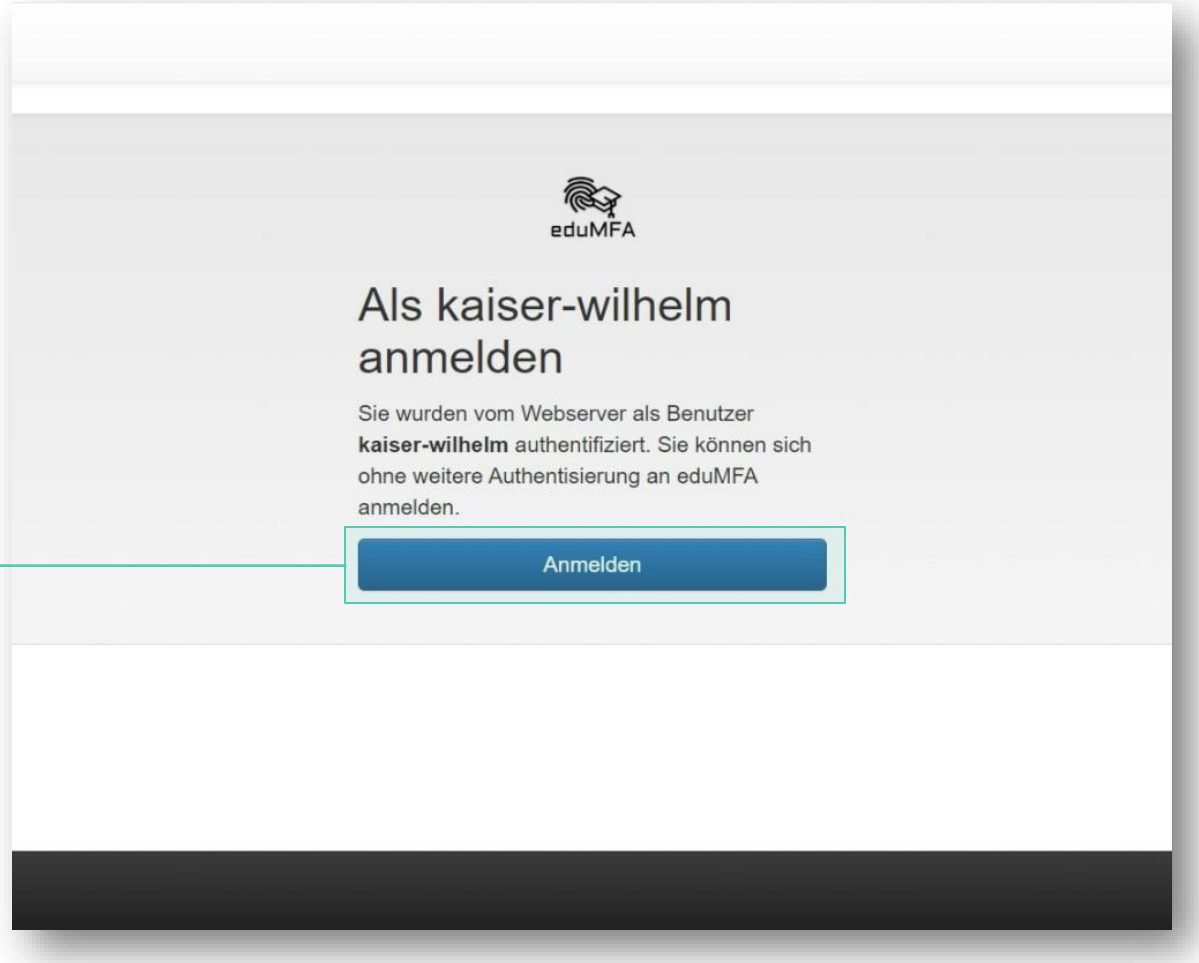
Wenn Sie den Code in das Eingabefeld eingegeben haben, können Sie mit *Überprüfen* fortfahren.

Beispiel: Anmeldung mit 2. Faktor

universität koblenz
weiter:denken

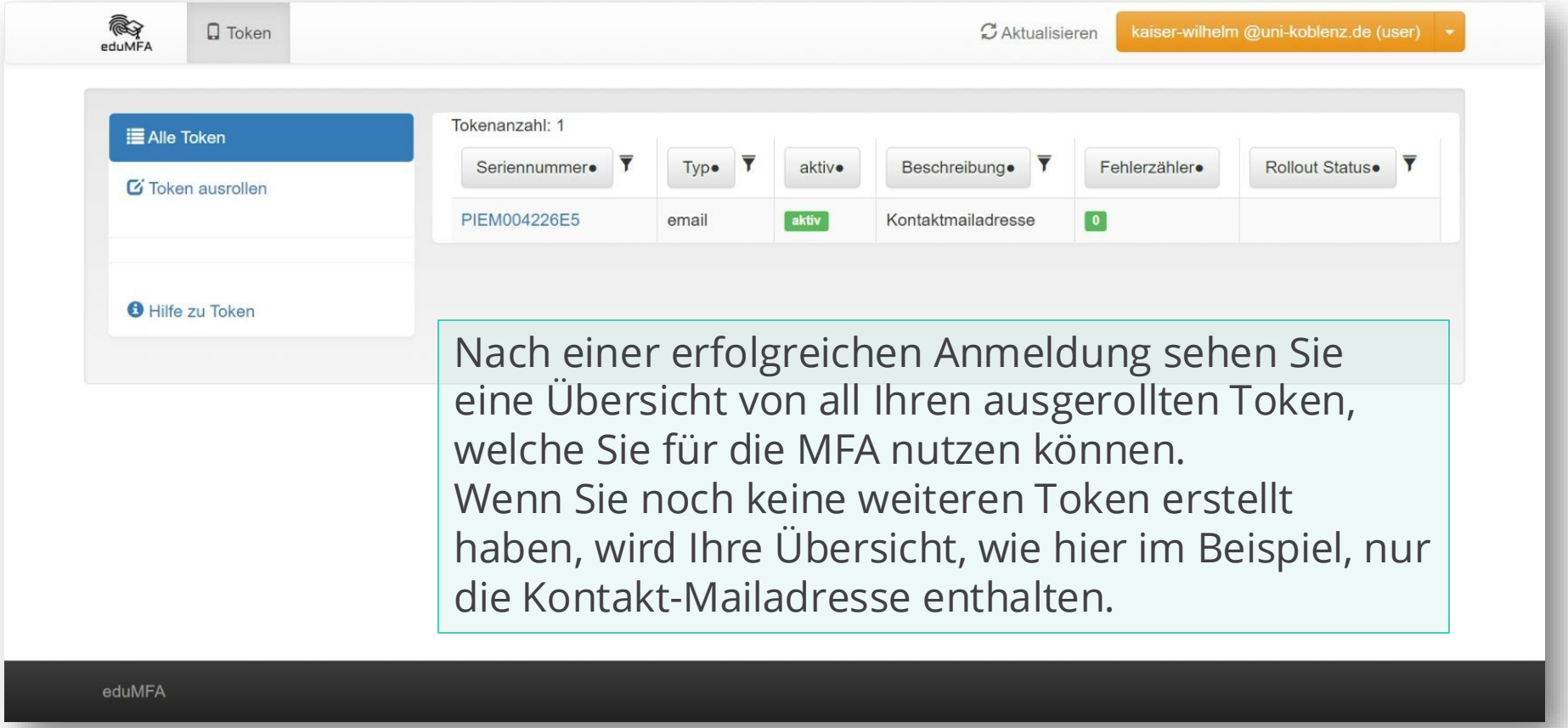
2. Schritt: Nutzungsbedingungen und Informationsweitergabe

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



Beispiel: Anmeldung mit 2. Faktor

Erfolgreiche Anmeldung beim MFA-Server



Nach einer erfolgreichen Anmeldung sehen Sie eine Übersicht von all Ihren ausgerollten Token, welche Sie für die MFA nutzen können.
Wenn Sie noch keine weiteren Token erstellt haben, wird Ihre Übersicht, wie hier im Beispiel, nur die Kontakt-Mailadresse enthalten.

Token

Token

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

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

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.

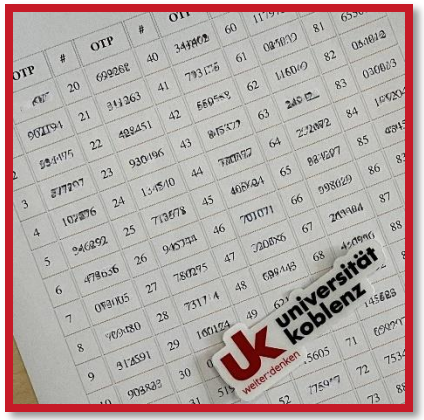
4. Biometrische Token:

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

Token

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

Zeitbasierte Einmalpasswörter (TOTP)



TAN-Liste (PPR)

Yubico OTP (Yubikey AES Mode)

WebAuthn

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

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 Seite 26) 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

Hier kommen Sie zu der Anleitung, wie Sie diesen Token ausrollen.

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

Hier kommen Sie zu der Anleitung, wie Sie diesen Token ausrollen.

Token

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

Hier kommen Sie zu der Anleitung, wie Sie diesen Token ausrollen.

Token

WebAuthn

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

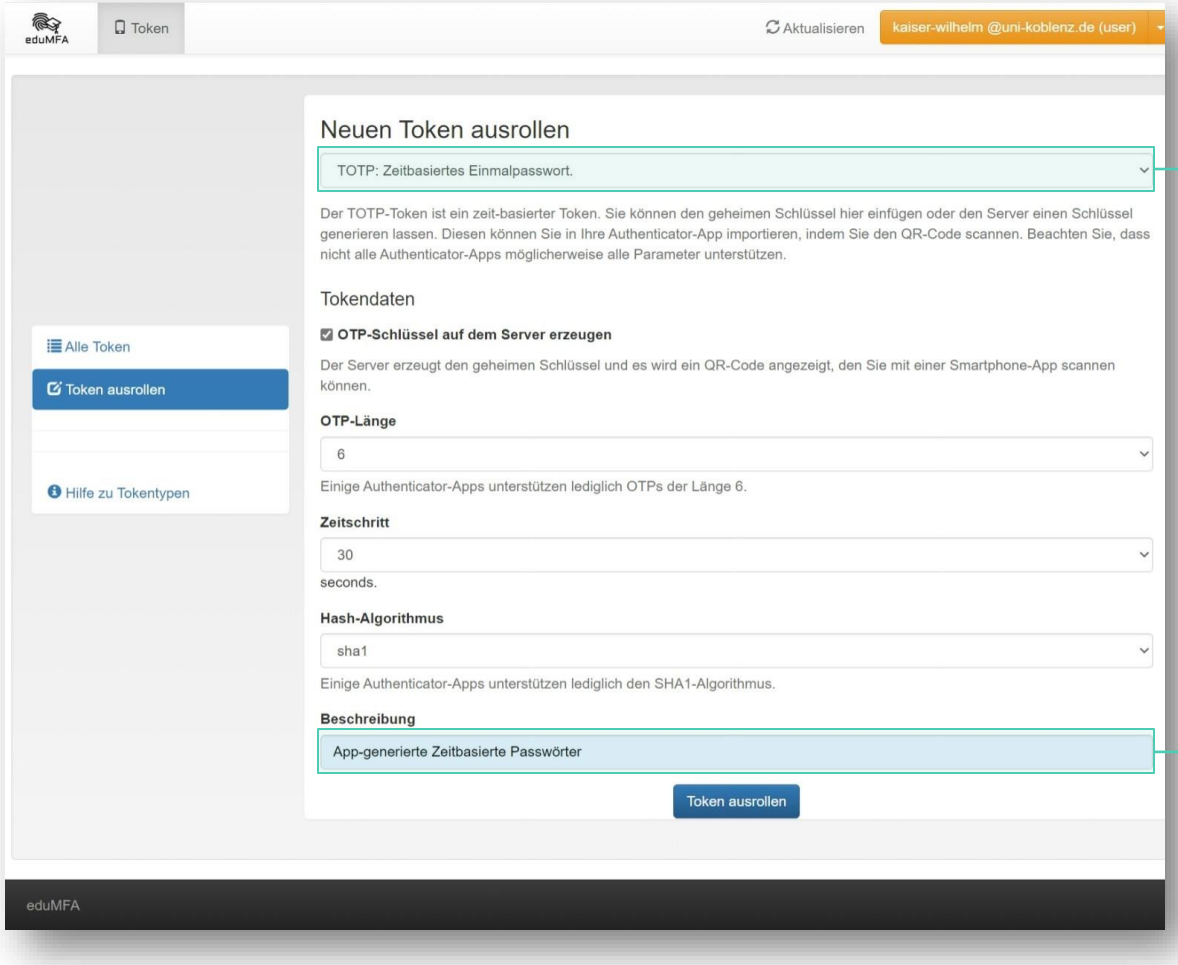
Hier kommen Sie zu der Anleitung, wie Sie diesen Token ausrollen.

Wie werden die verschiedenen Token ausgerollt und verwendet?

Zeitbasierte Einmalpasswörter (TOTP)

Token ausrollen

Zeitbasierte Einmalpasswörter (TOTP) ausrollen

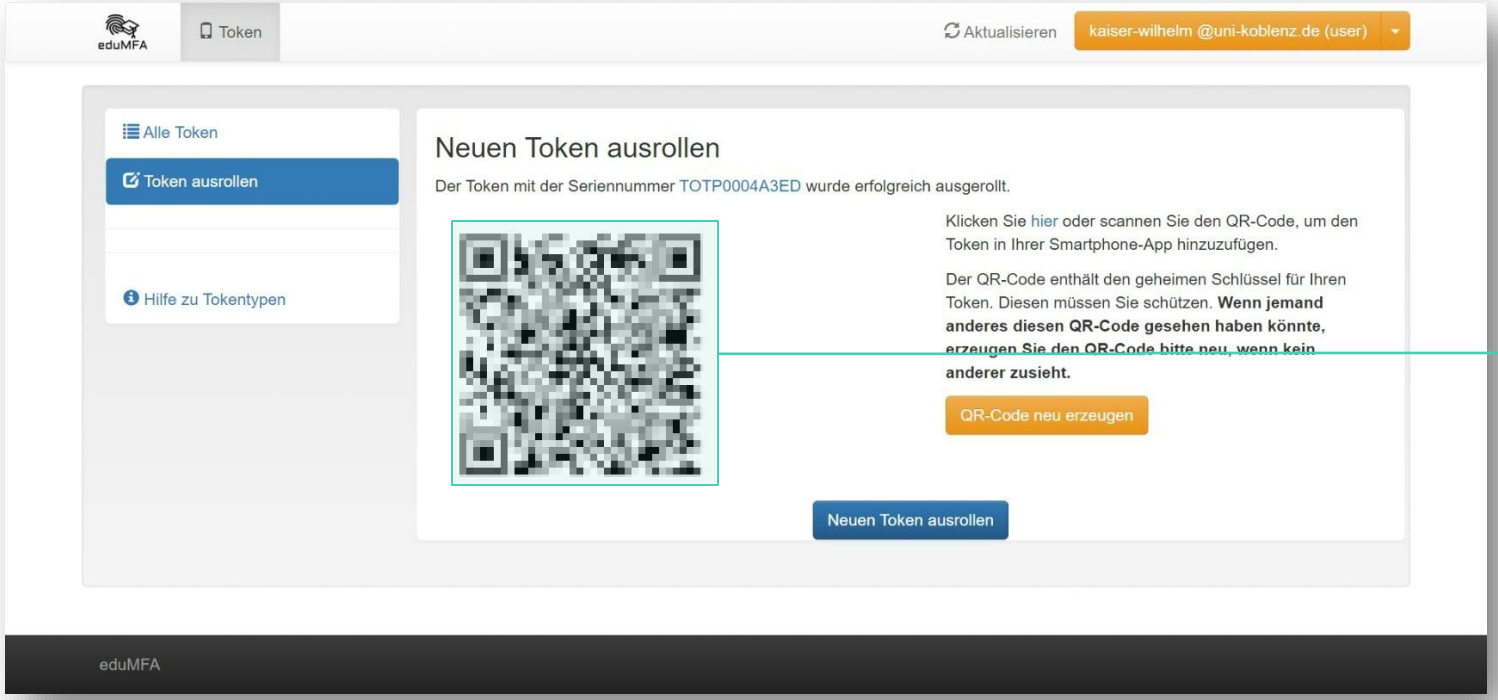


Indem Sie in dem Auswahlmenu *TOTP: Zeitbasiertes Einmalpasswort* auswählen, lässt sich der Token ganz einfach unten über den Button *Token ausrollen* generieren.

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.

Token ausrollen

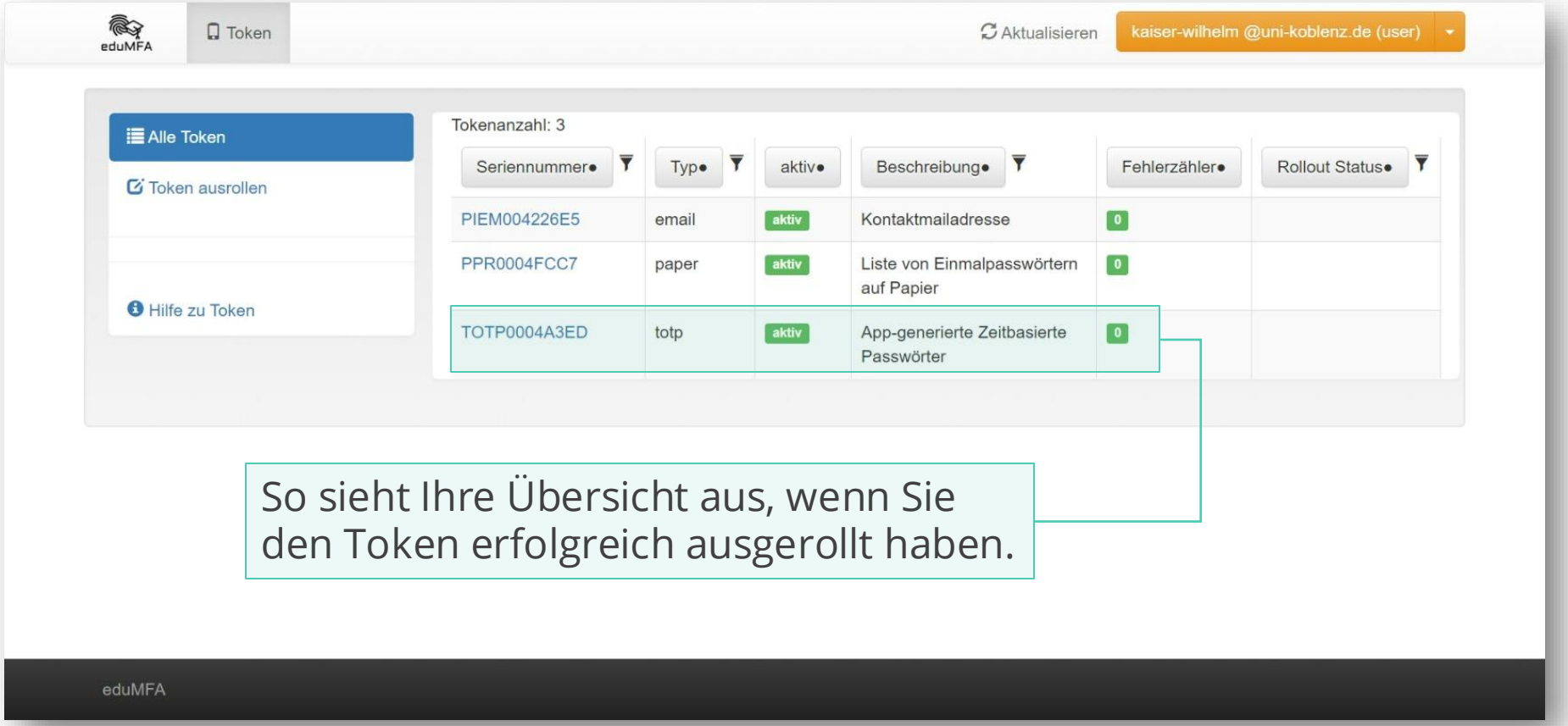
Zeitbasierte Einmalpasswörter (TOTP) ausrollen



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

Token ausrollen

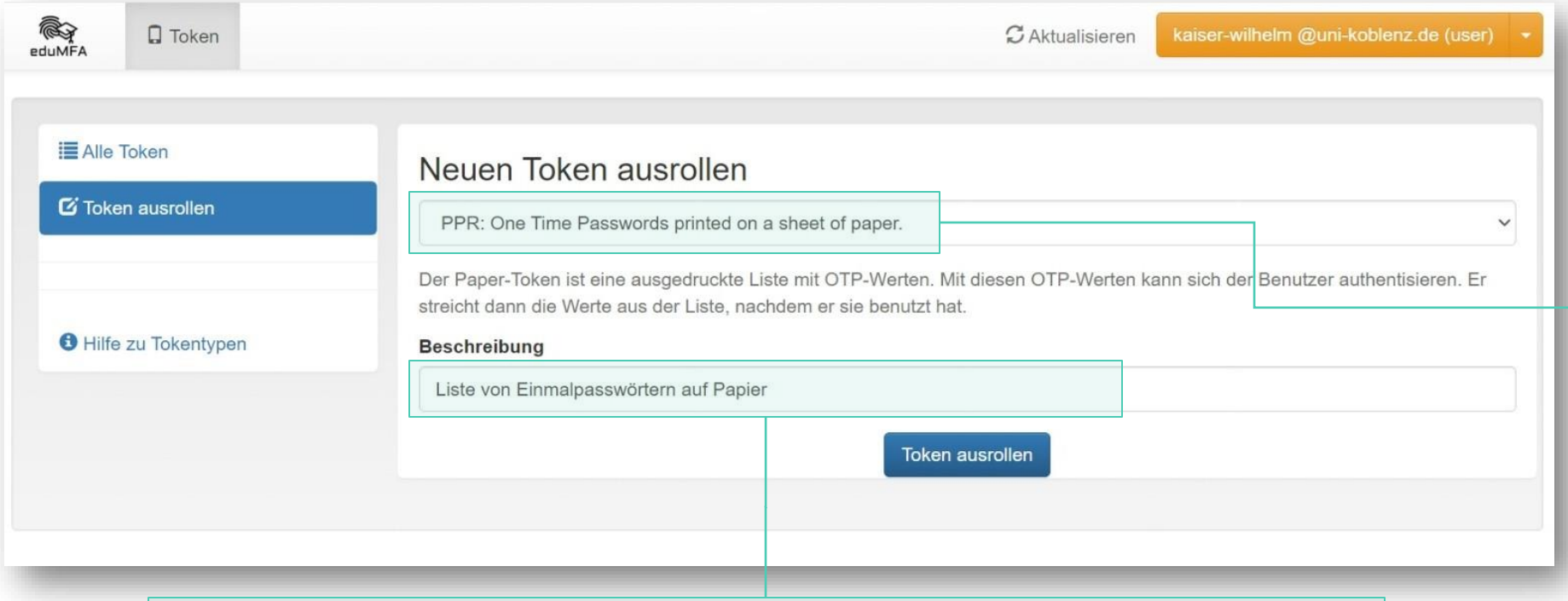
Zeitbasierte Einmalpasswörter (TOTP) ausrollen



TAN-Liste (PPR)

Token ausrollen

TAN-Liste (PPR) ausrollen

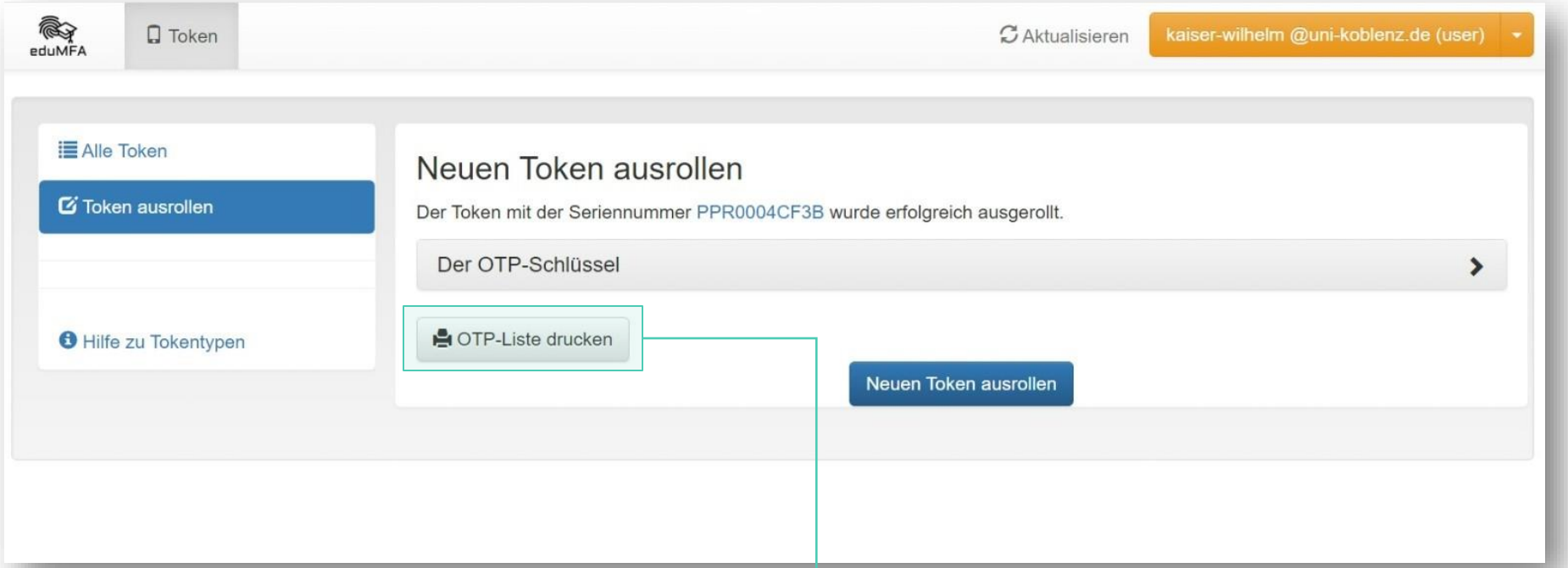


Indem Sie in dem Auswahlmenu *PPR: One Time Passworts printed on a sheet of paper* auswählen, lässt sich der Token ganz einfach unten über den Button *Token ausrollen* generieren.

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.

Token ausrollen

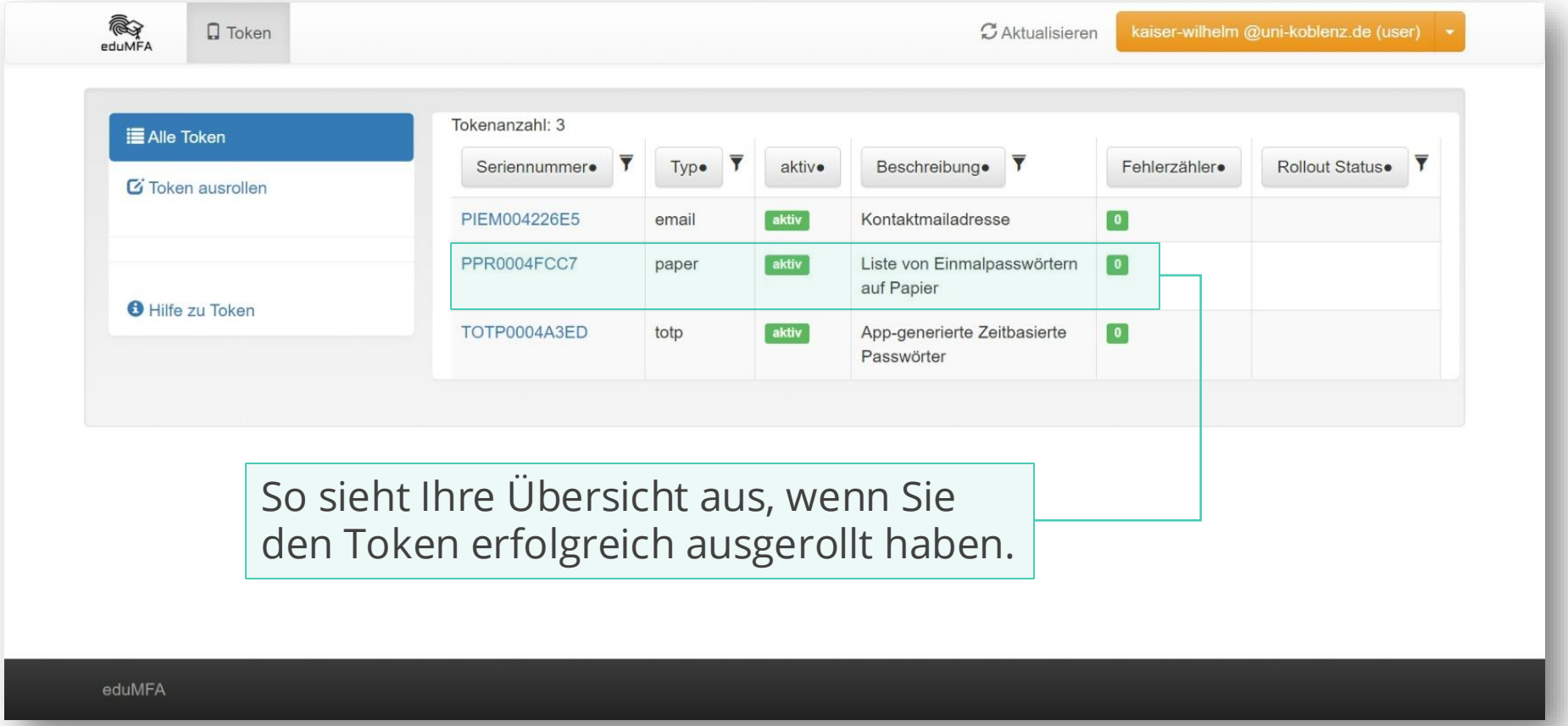
TAN-Liste (PPR) ausrollen



Über den Button *OTP-Liste drucken* können Sie Ihre ausgerollte Liste entweder direkt ausdrucken oder als PDF speichern.

Token ausrollen

TAN-Liste (PPR) ausrollen



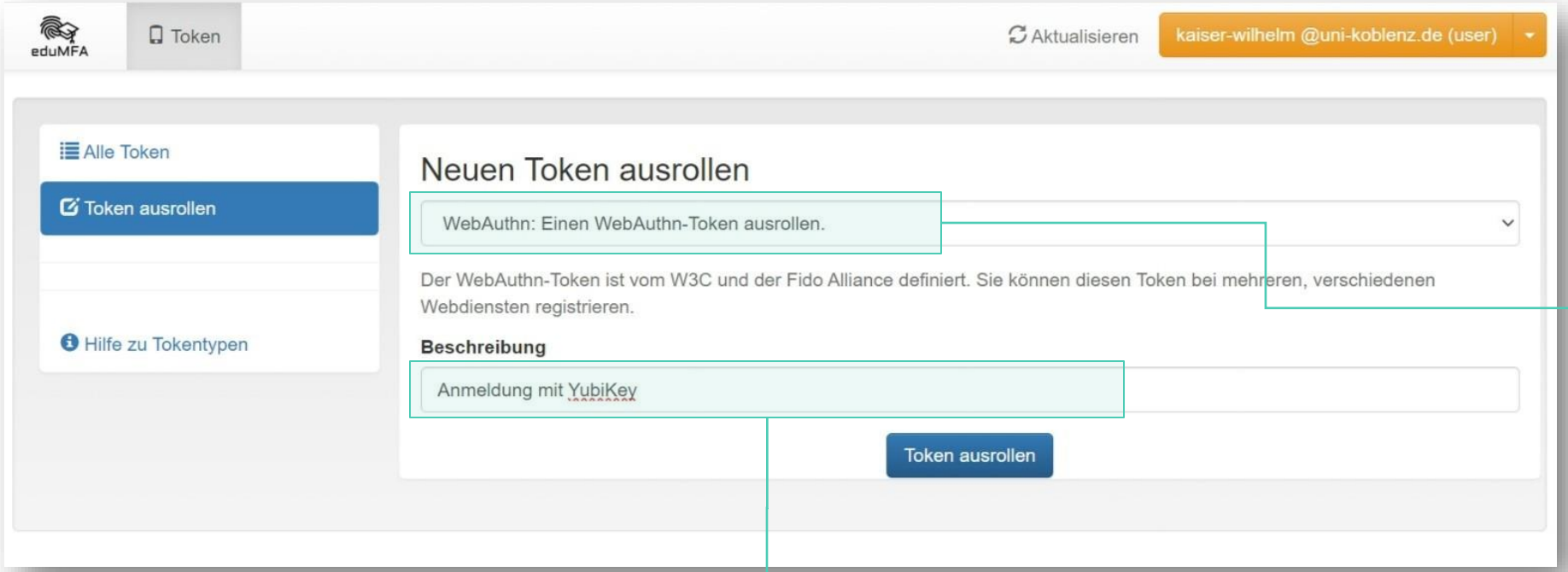
Hinweis

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)

Token ausrollen

WebAuthn (mit YubiKey)

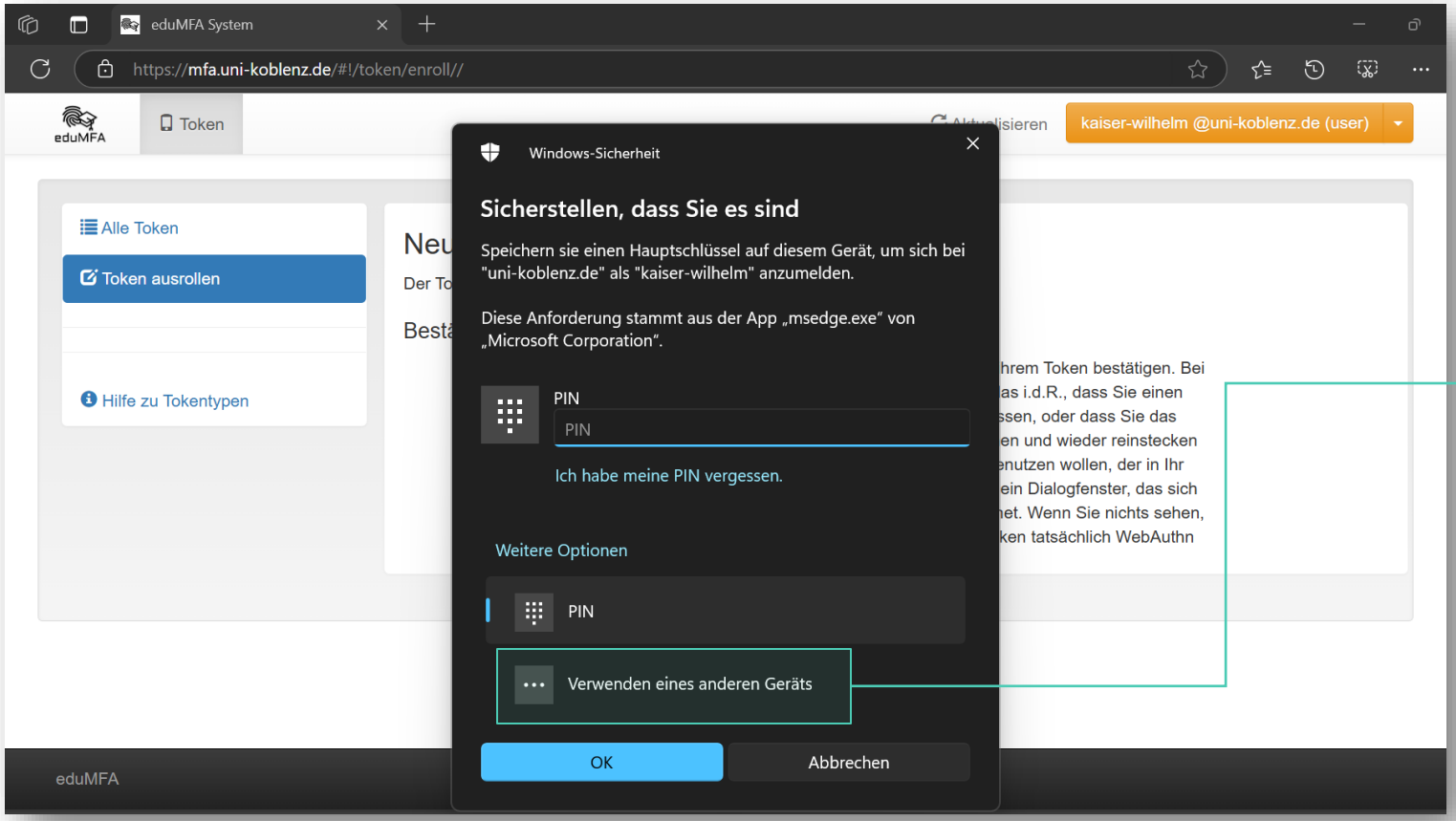


Indem Sie in dem Auswahlmenu *WebAuthn: Einen WebAuthn-Token ausrollen* auswählen, können Sie ganz einfach unten über den Button *Token ausrollen* die Erstellung des Tokens starten.

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.

Token ausrollen

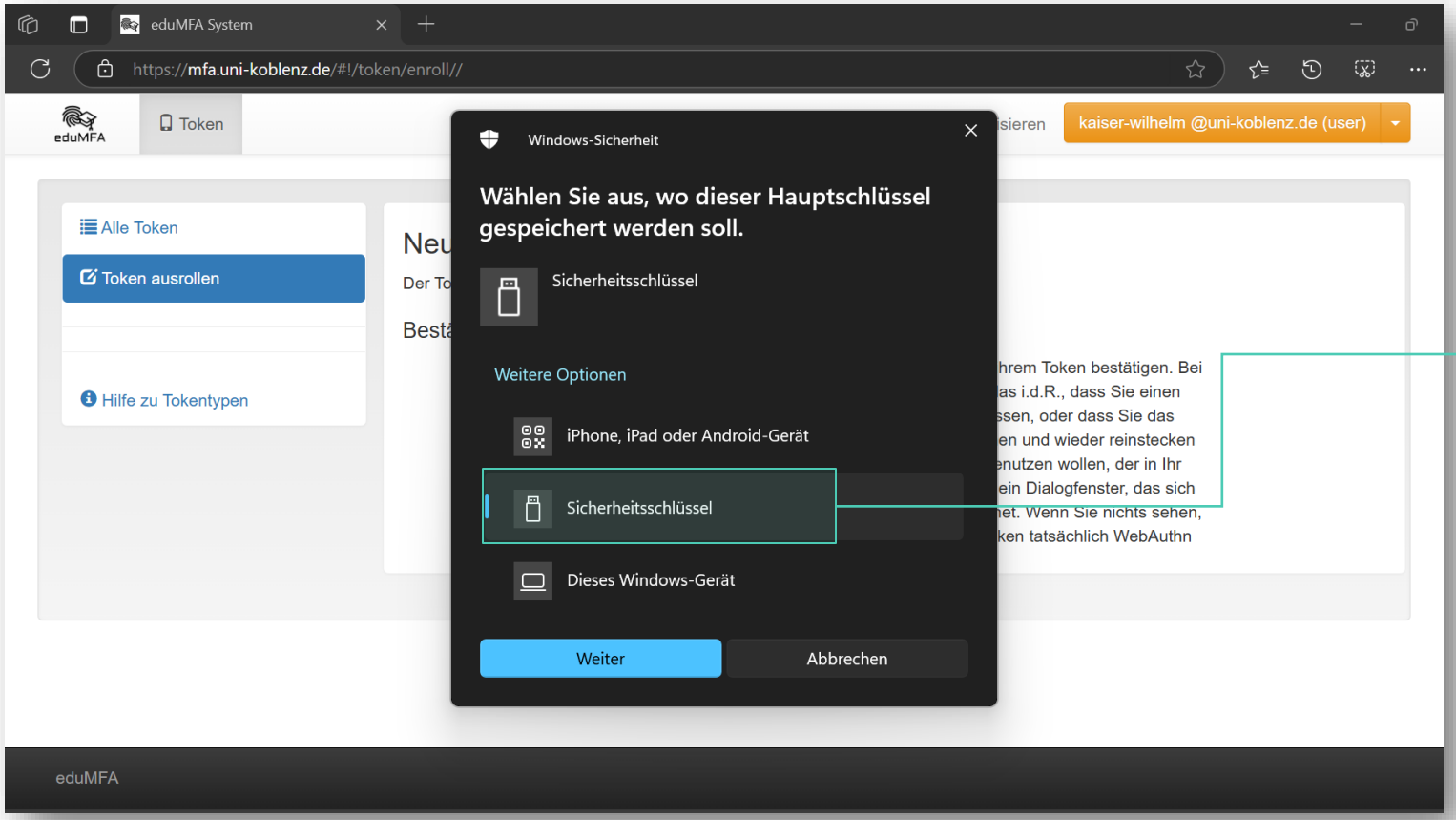
WebAuthn (mit YubiKey)



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

Token ausrollen

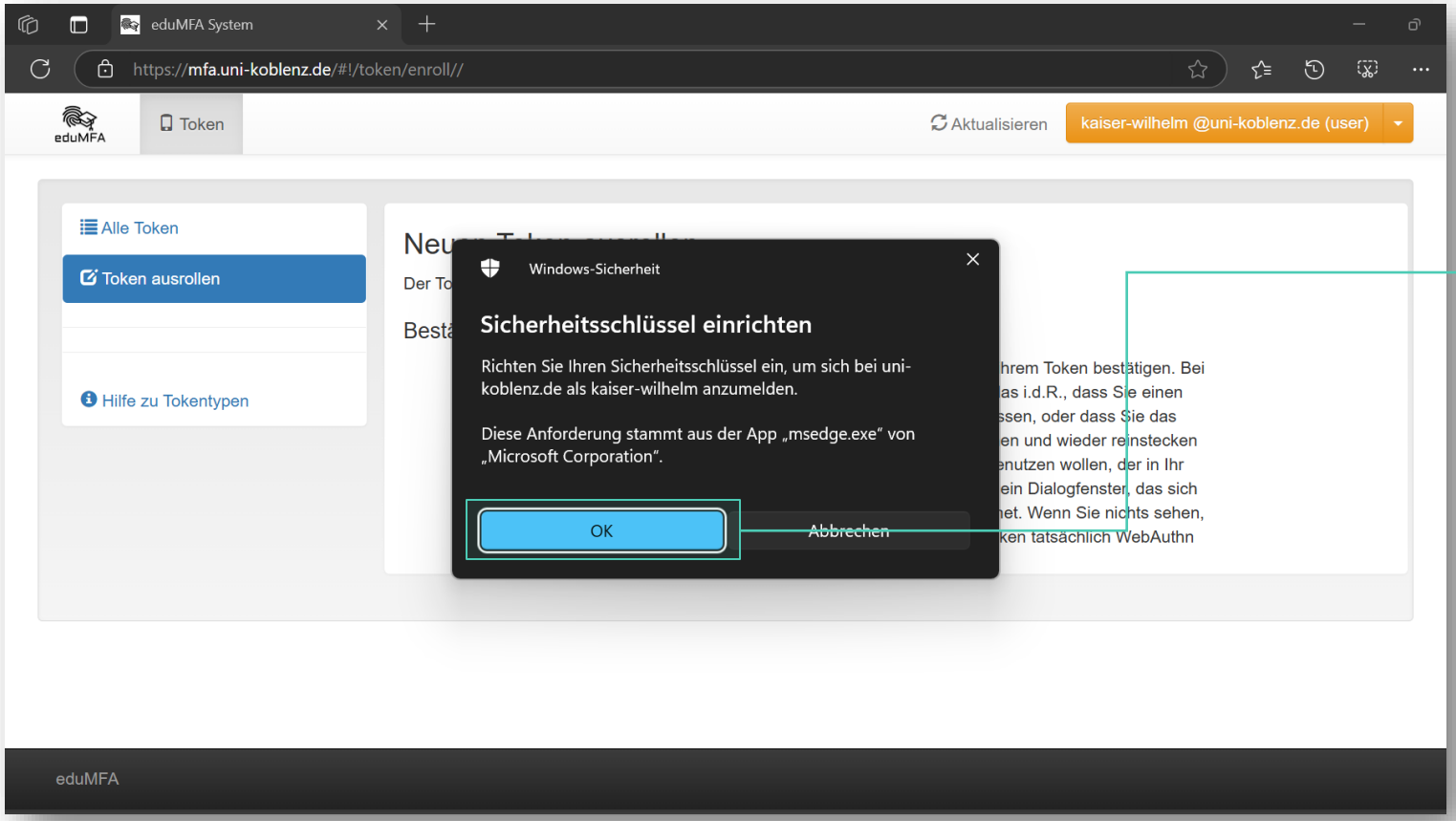
WebAuthn (mit YubiKey)



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

Token ausrollen

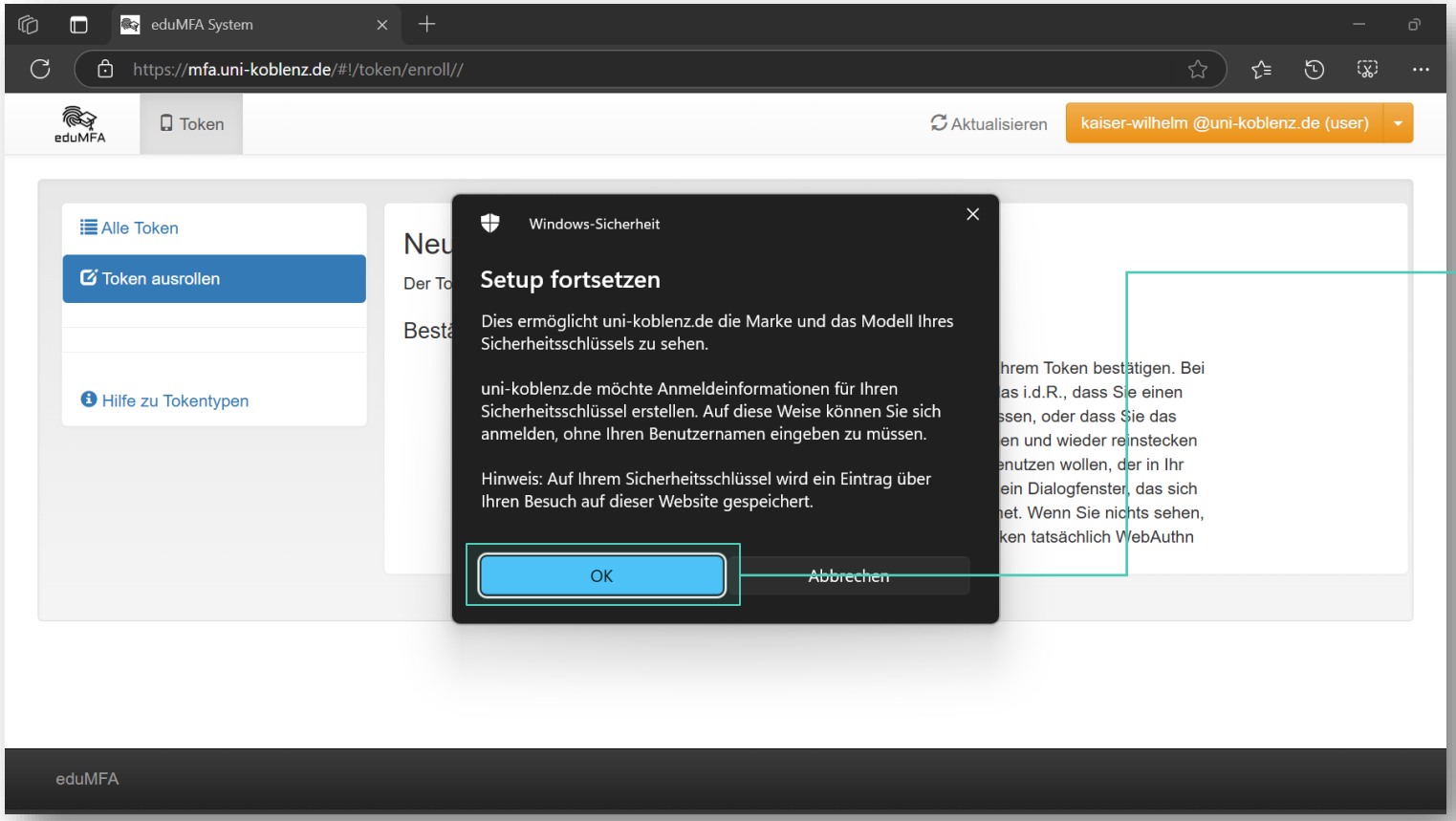
WebAuthn (mit YubiKey)



Hinweis lesen und mit *OK* bestätigen.

Token ausrollen

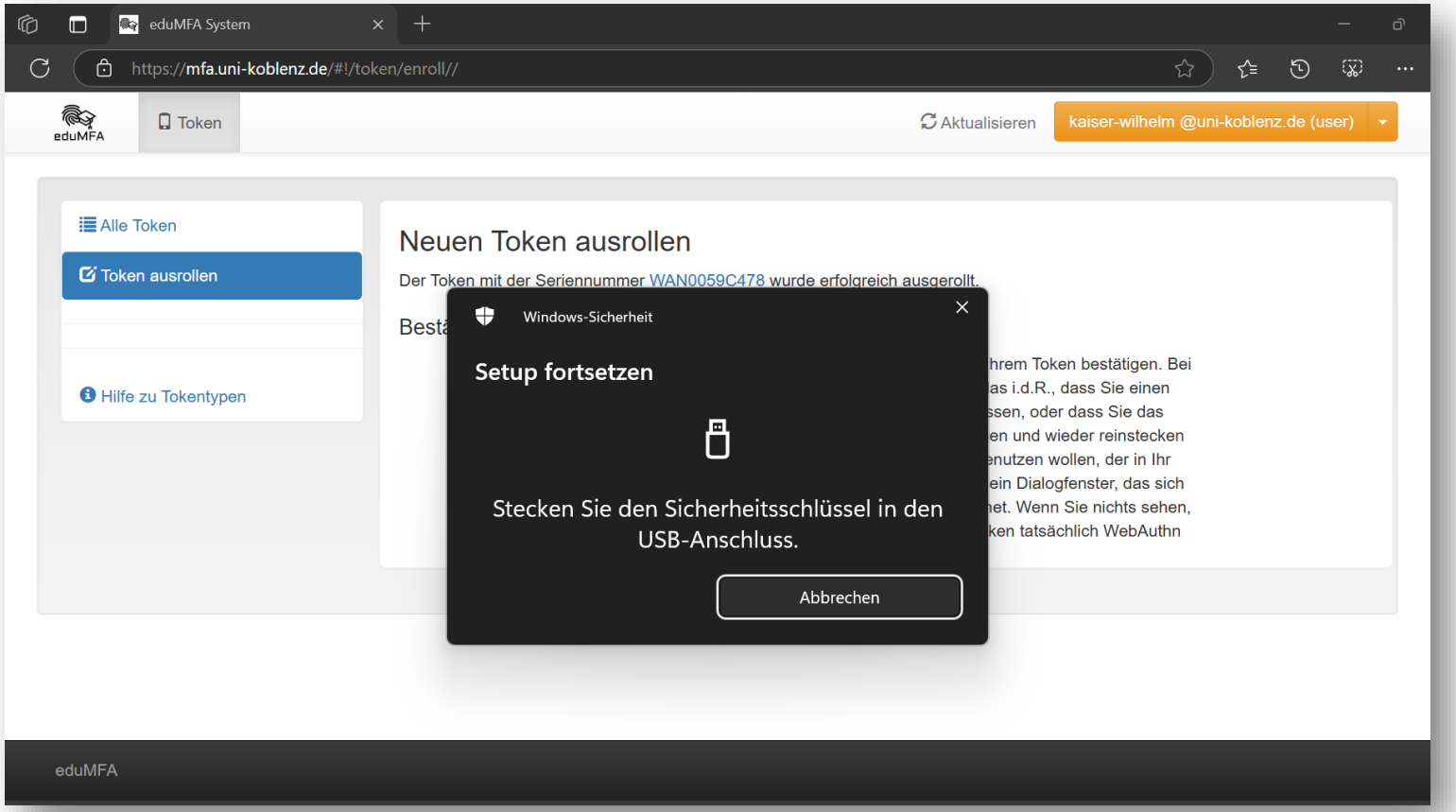
WebAuthn (mit YubiKey)



Hinweis lesen und mit *OK* bestätigen.

Token ausrollen

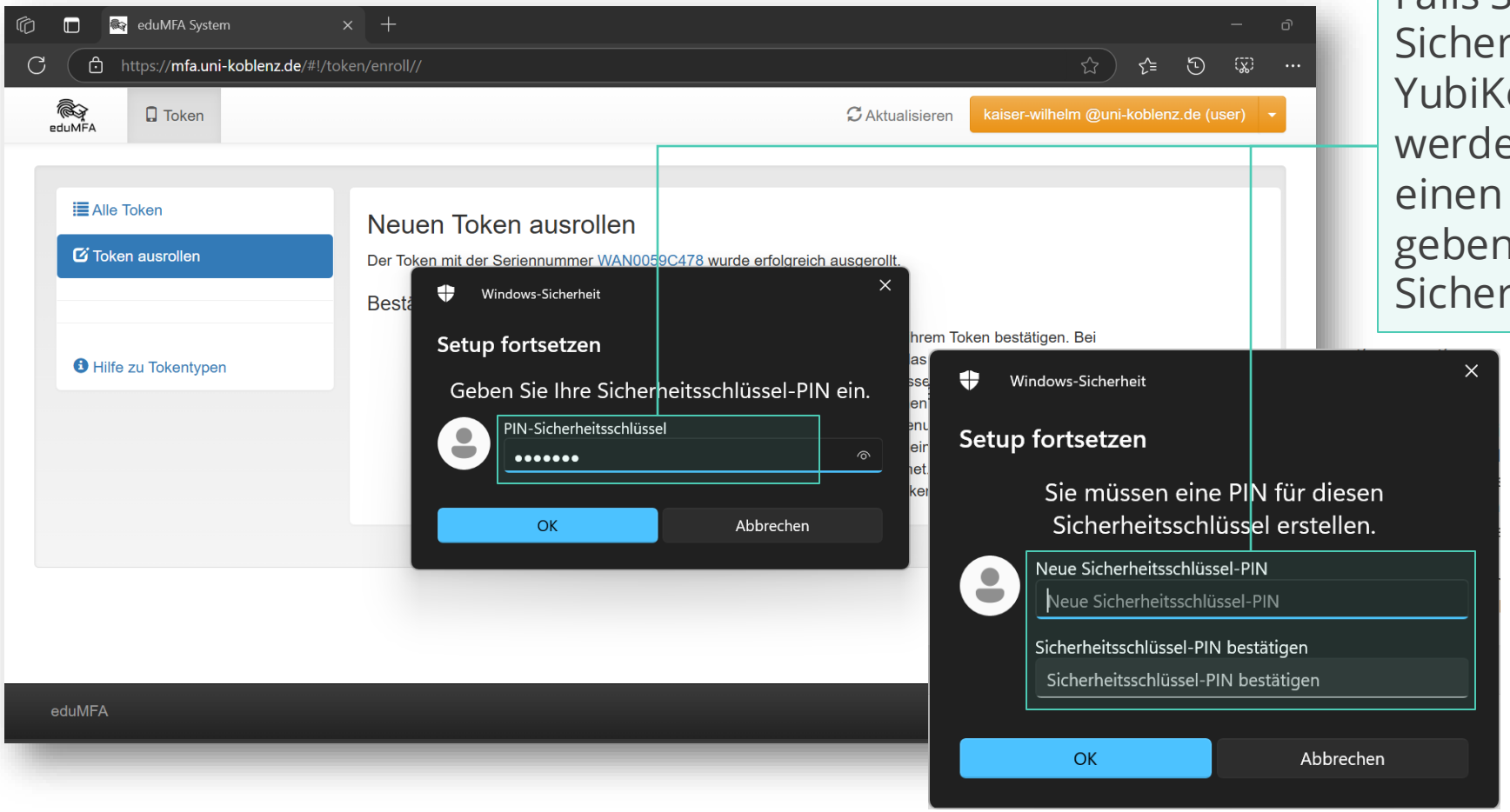
WebAuthn (mit YubiKey)



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

Token ausrollen

WebAuthn (mit YubiKey)

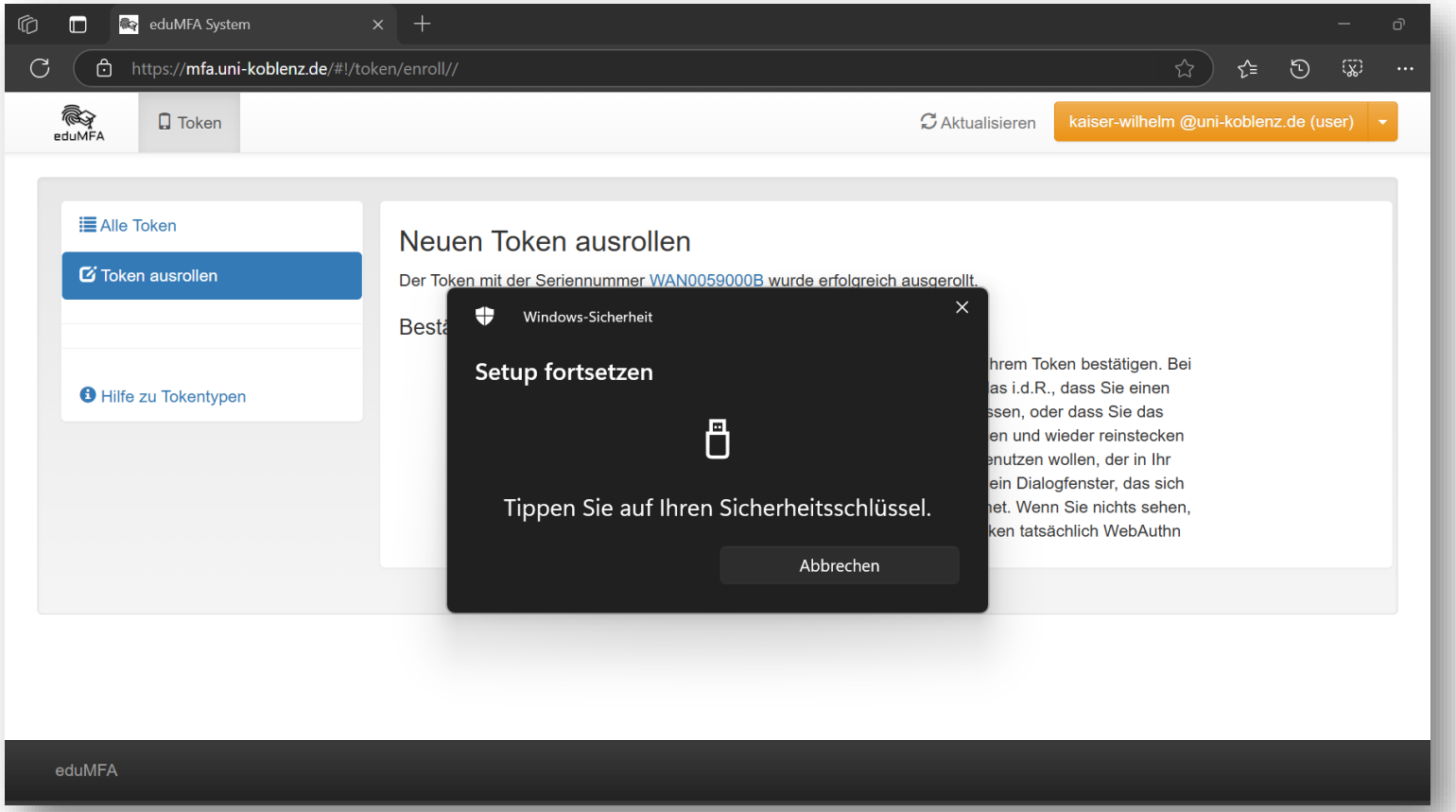


Falls Sie noch keinen Sicherheitsschlüssen für Ihren YubiKey festgelegt haben, werden Sie nun aufgefordert einen anzulegen. Ansonsten geben Sie Ihren Sicherheitsschlüssel hier ein.

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

Token ausrollen

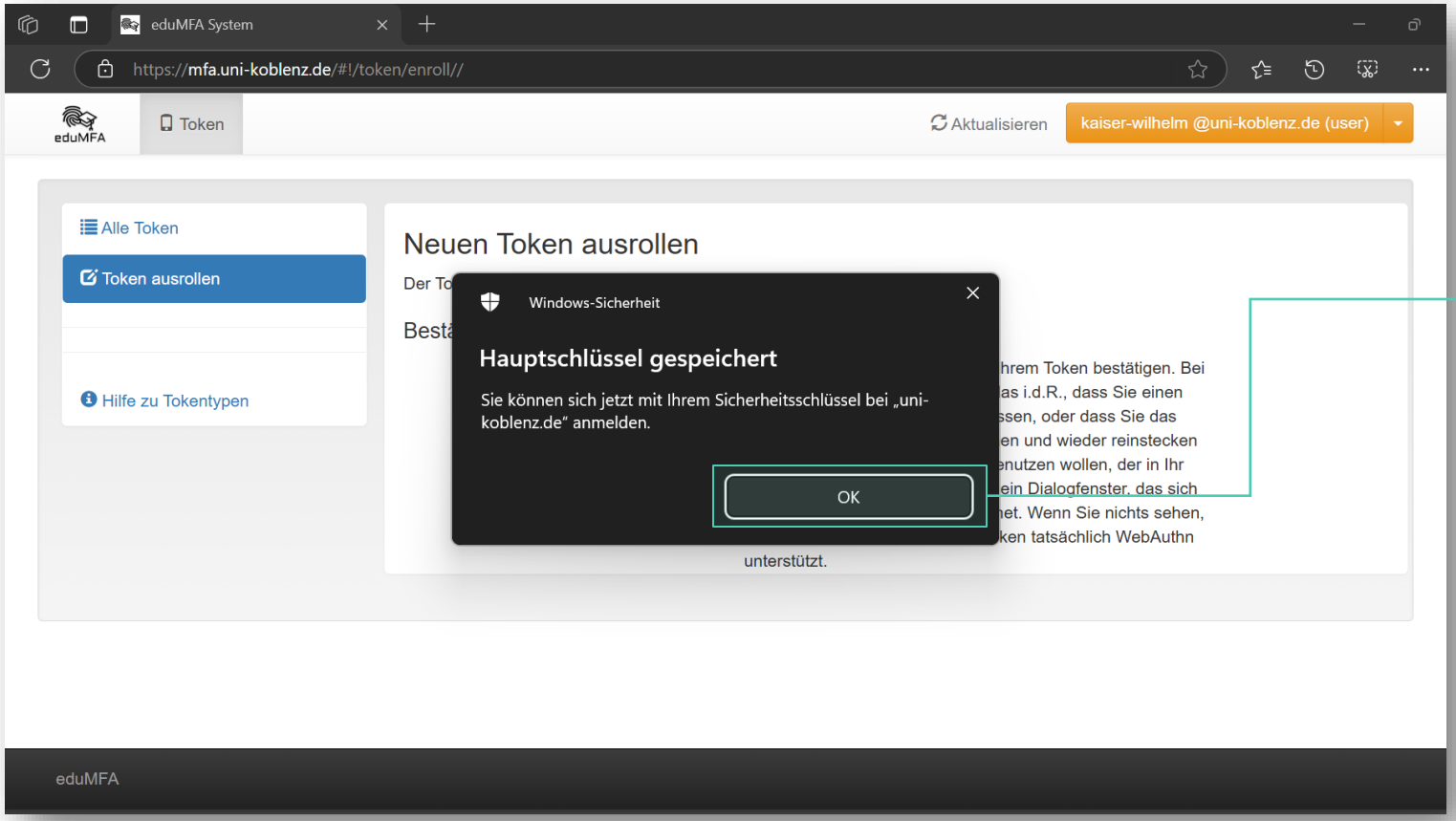
WebAuthn (mit YubiKey)



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

Token ausrollen

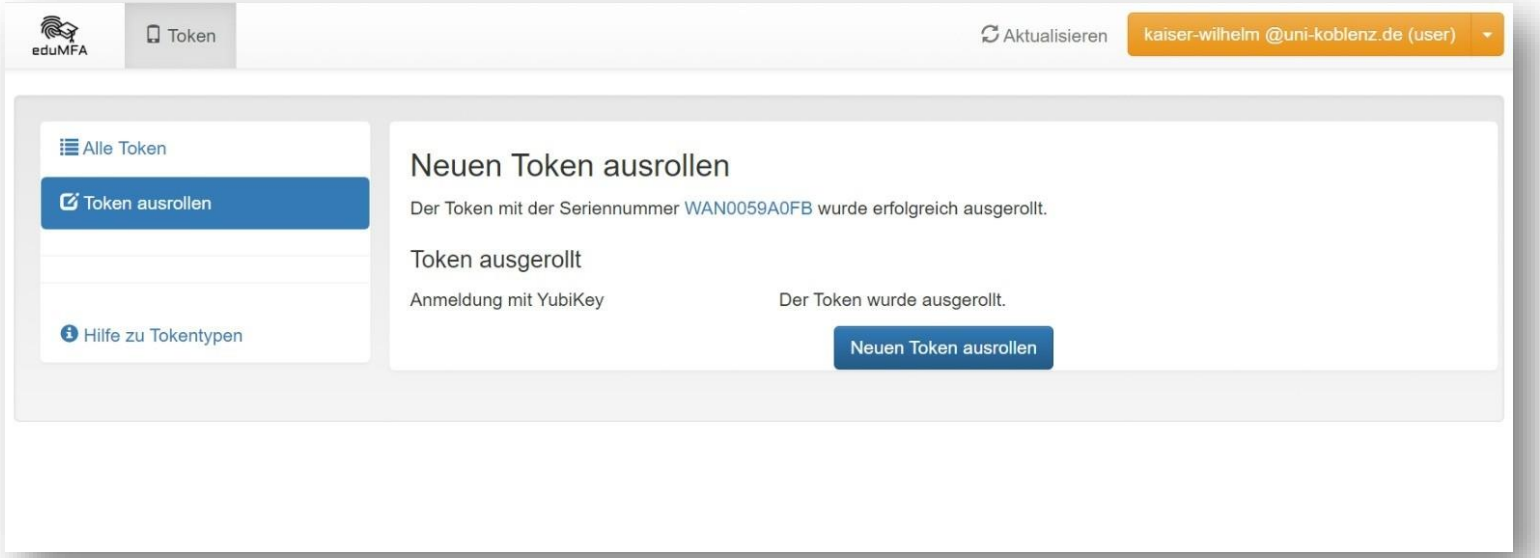
WebAuthn (mit YubiKey)



Ihr Setup ist nun abgeschlossen. Mit *OK* beenden Sie das Setup.

Token ausrollen

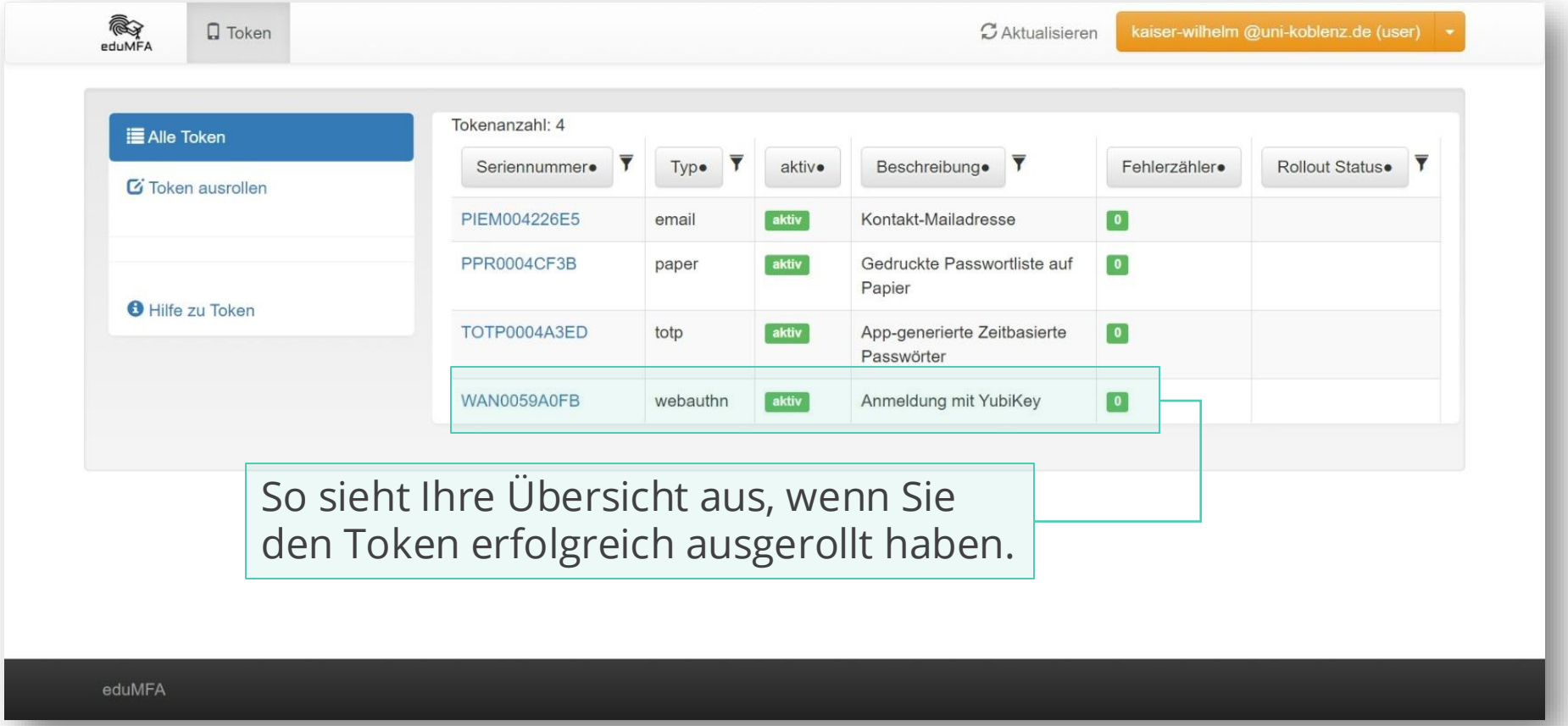
WebAuthn (mit YubiKey)



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.

Token ausrollen

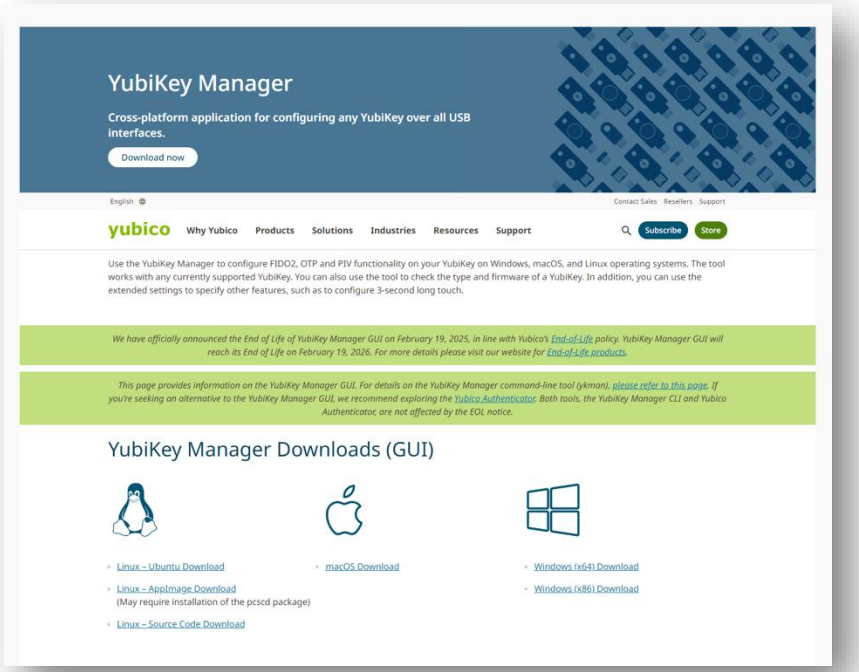
TAN-Liste (PPR) ausrollen



Yubico OTP (Yubikey AES Mode)

Token ausrollen

Yubico OTP (Yubikey AES Mode)



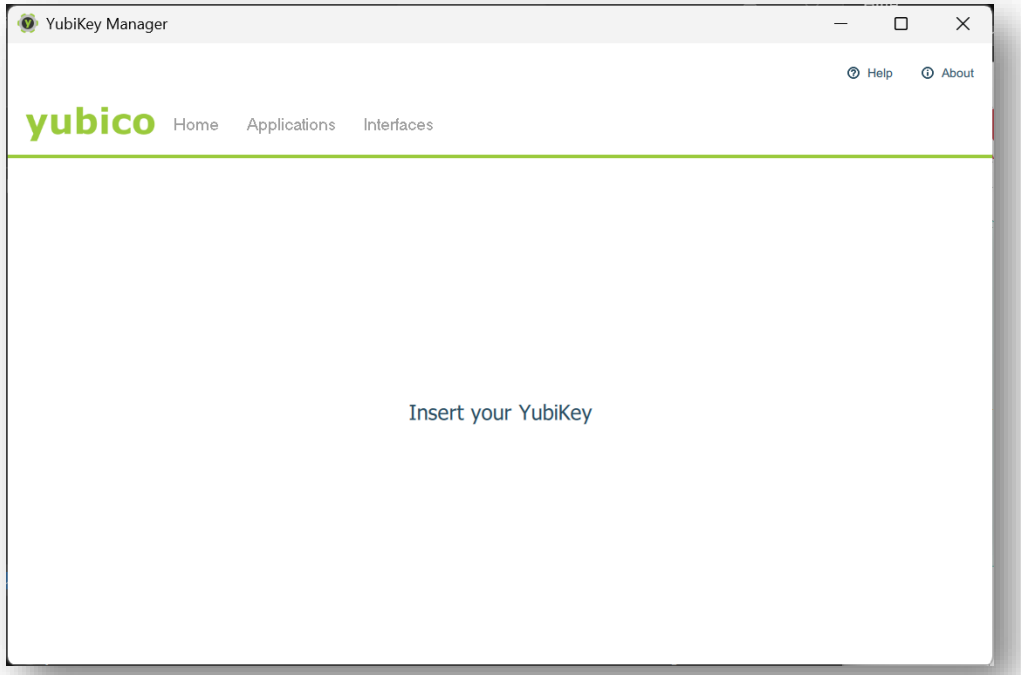
Zunächst müssen Sie auf der Webseite von Yubico den YubiKey Manager herunterladen, um Ihren YubiKey zu konfigurieren und als Token nutzen zu können.

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

www.yubico.com/support/download/yubikey-manager

Token ausrollen

Yubico OTP (Yubikey AES Mode)

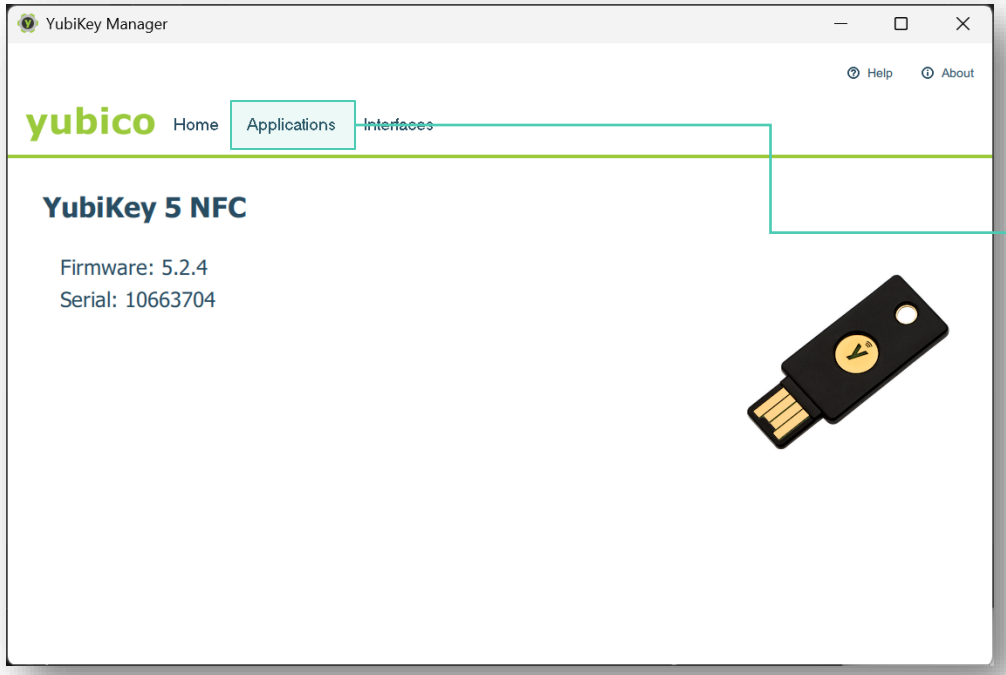


Um Ihren YubiKey als Token ausrollen zu können, müssen Sie zunächst mit dem YubiKey Manager von Yubico eine ID und den Sicherheitsschlüssel generieren.

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

Token ausrollen

Yubico OTP (Yubikey AES Mode)

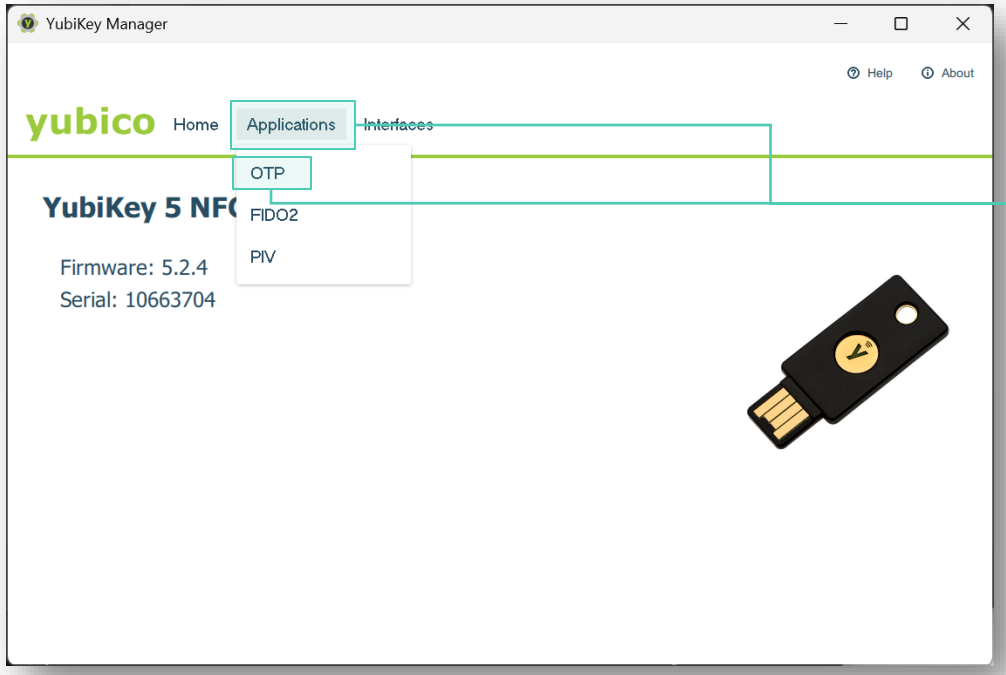


So sieht das Interface aus, wenn Ihr YubiKey von der Software erkannt wurde.

Drücken Sie als nächstes auf den Reiter *Applications*.

Token ausrollen

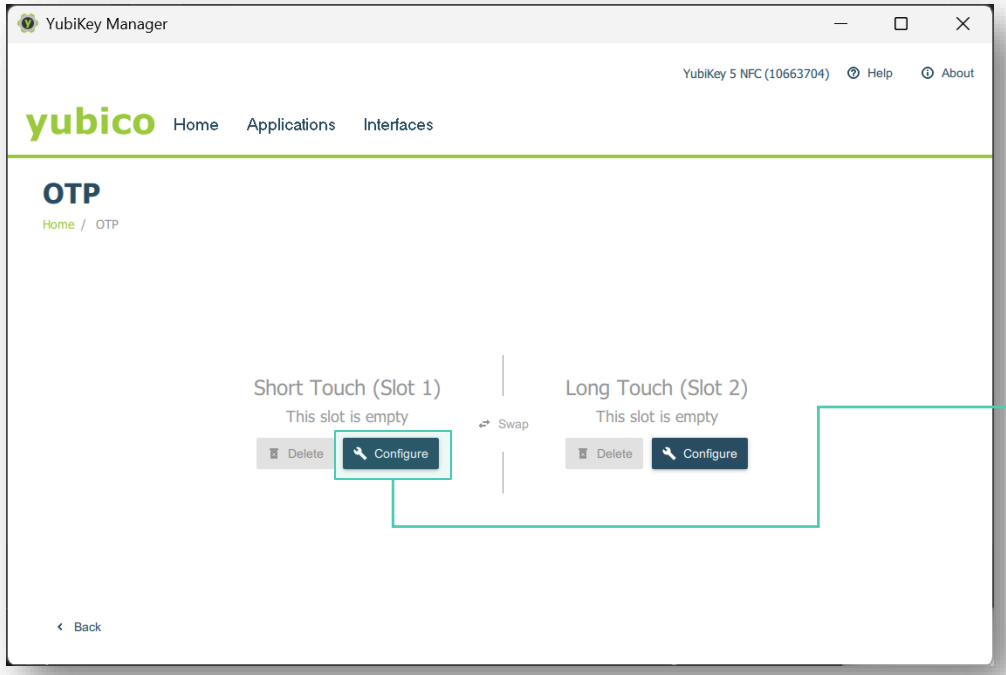
Yubico OTP (Yubikey AES Mode)



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

Token ausrollen

Yubico OTP (Yubikey AES Mode)

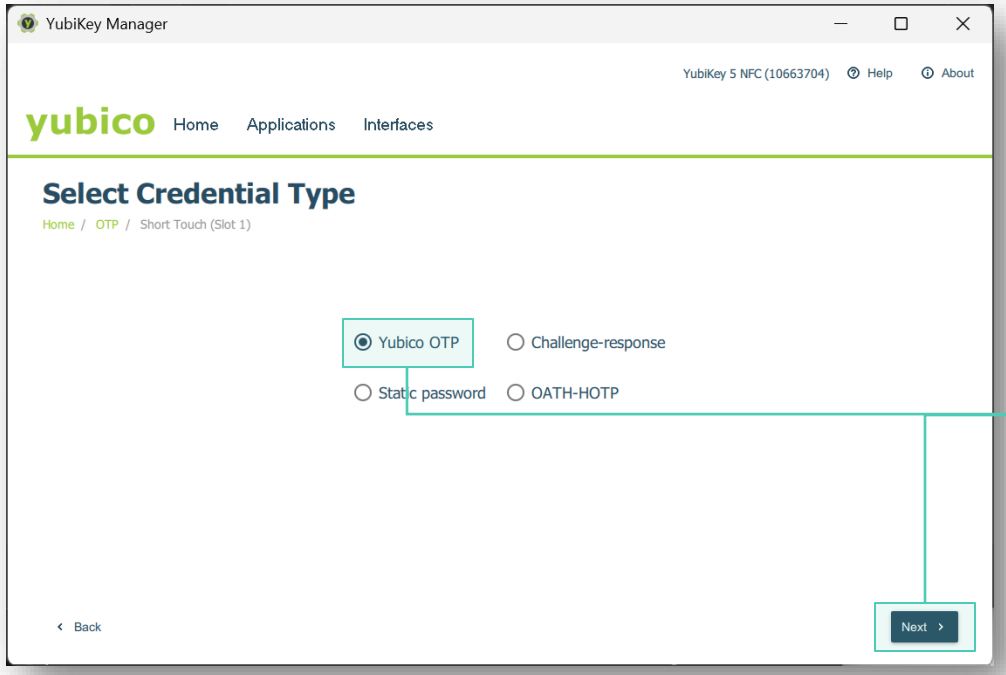


Auf dieser Seite finden Sie zwei Anwendungsmöglichkeiten: *Short Touch* und *Long Touch*. Ihr YubiKey kann dazu konfiguriert verschiedene Dinge ausgeben, je nach dem wie lange sie den Knopf auf Ihrem YubiKey drücken.

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

Token ausrollen

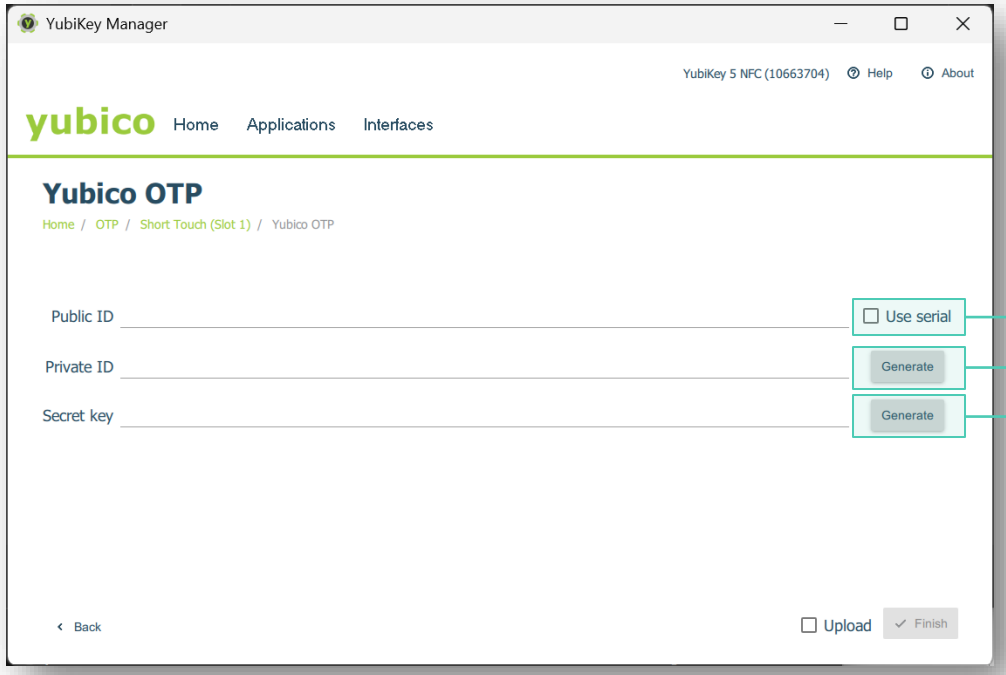
Yubico OTP (Yubikey AES Mode)



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

Token ausrollen

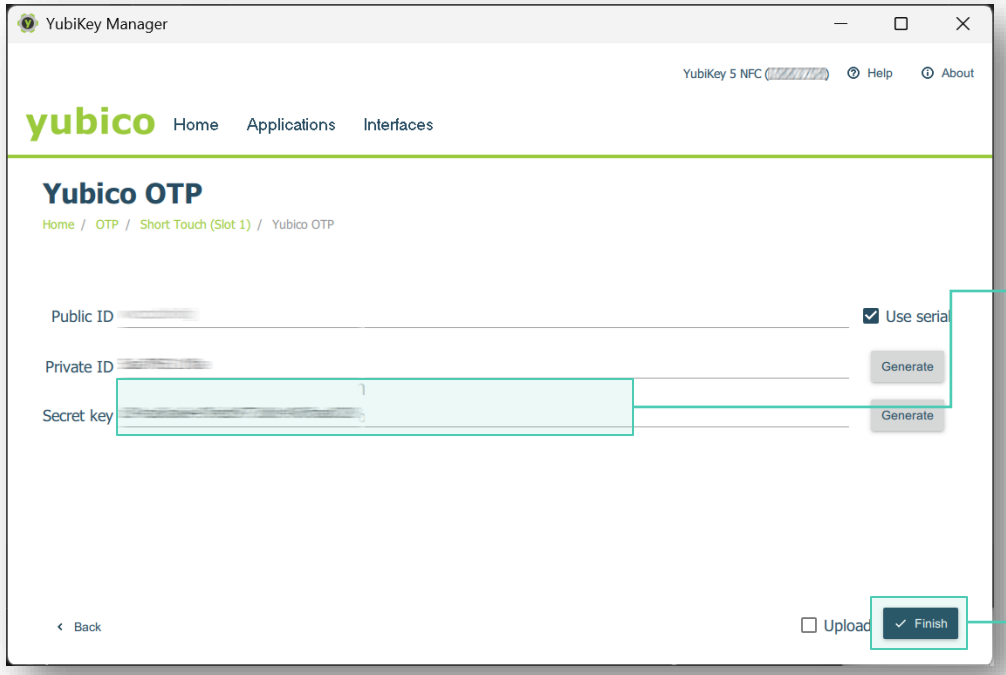
Yubico OTP (Yubikey AES Mode)



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.

Token ausrollen

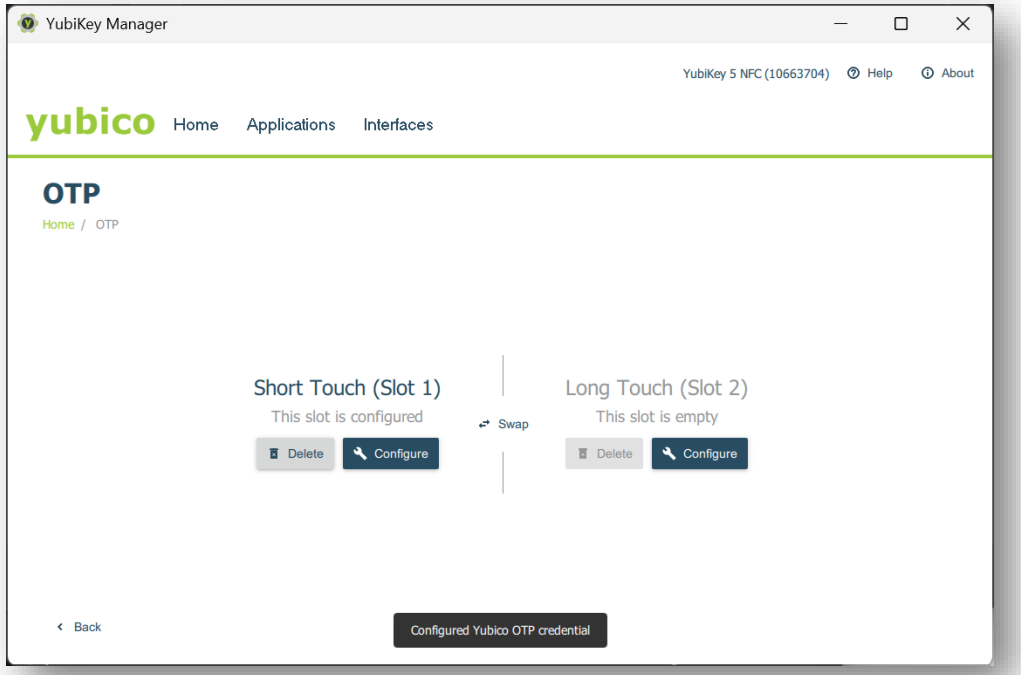
Yubico OTP (Yubikey AES Mode)



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.

Token ausrollen

Yubico OTP (Yubikey AES Mode)

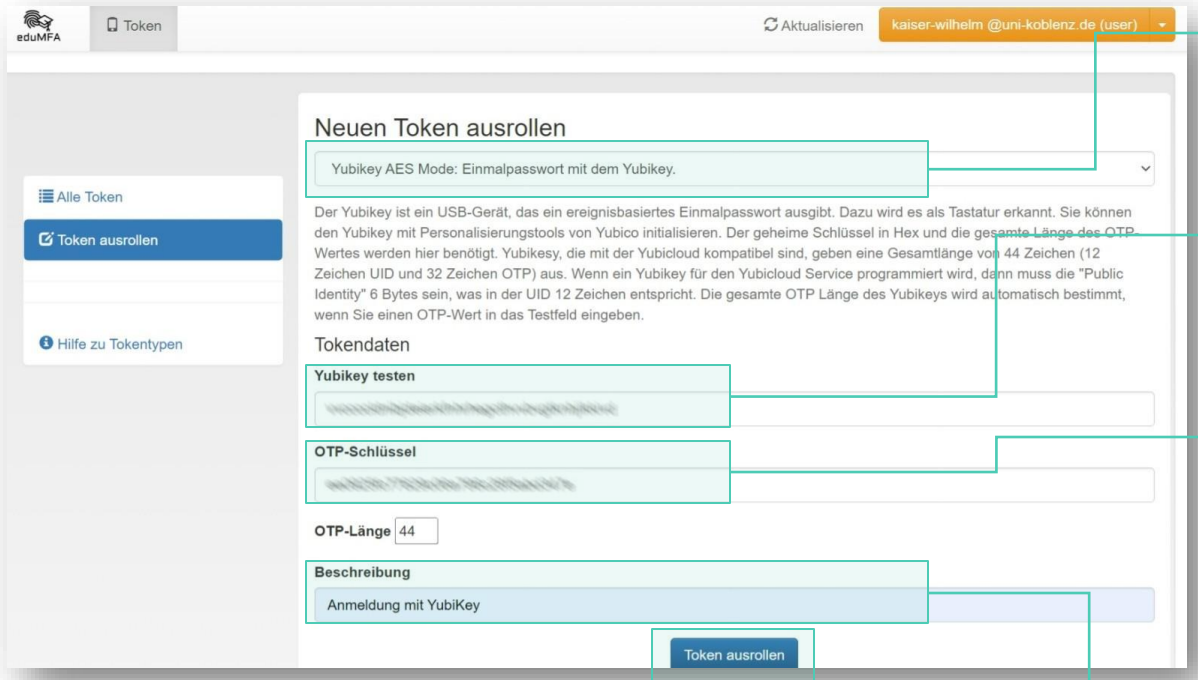


Nun sollte bei dem Slot, den Sie konfiguriert haben, *This slot is configured* stehen.

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

Token ausrollen

Yubico OTP (Yubikey AES Mode)



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.

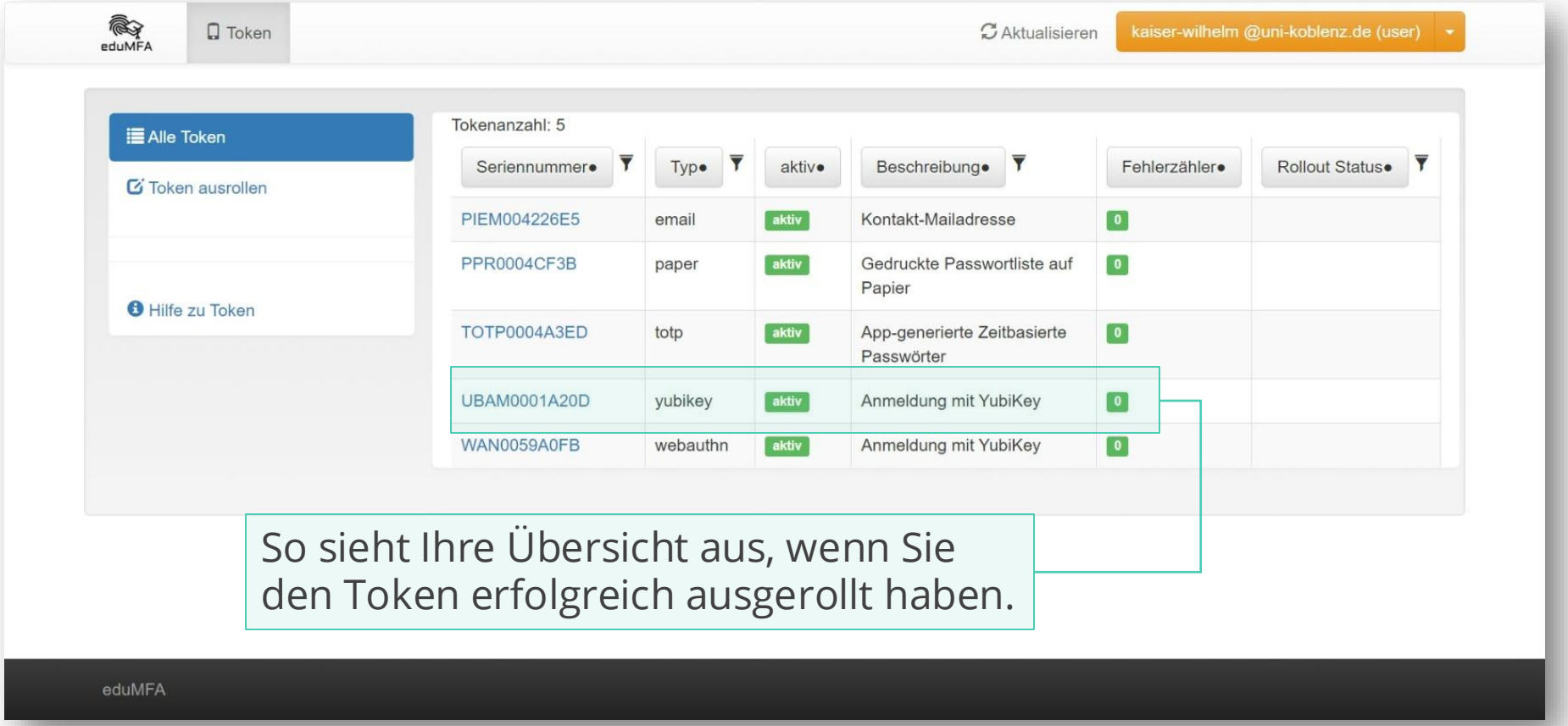
Fügen Sie nun den Sicherheitsschlüssel, aus dem YubiKey Manager hier ein.

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.

Mit dem Button *Token ausrollen* ist Ihr Token fertig ausgerollt.

Token ausrollen

TAN-Liste (PPR) ausrollen

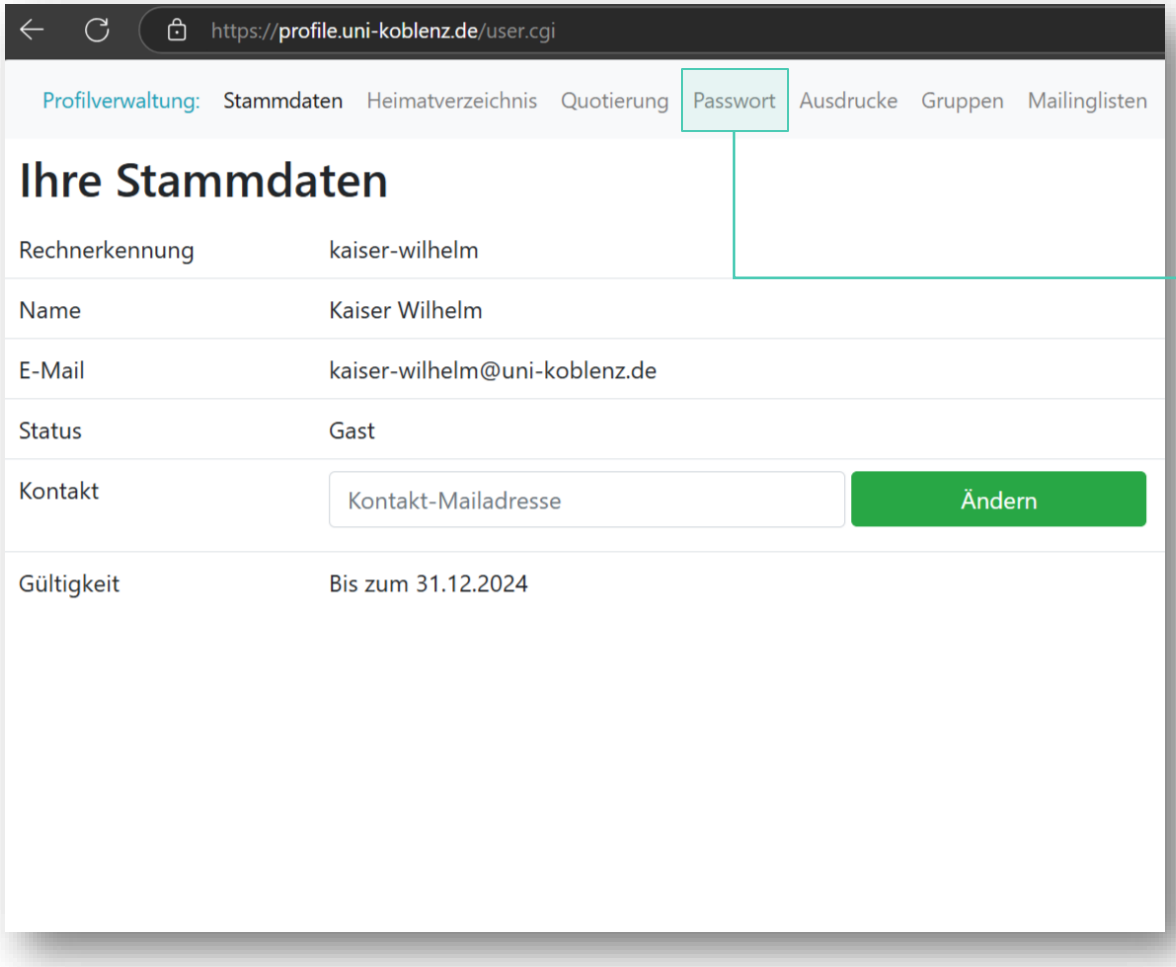


Ändern Ihres Uni-Passworts

Ändern Ihres Uni-Passworts

universität koblenz
weiter:denken

Passwortänderung bei der Profilverwaltung

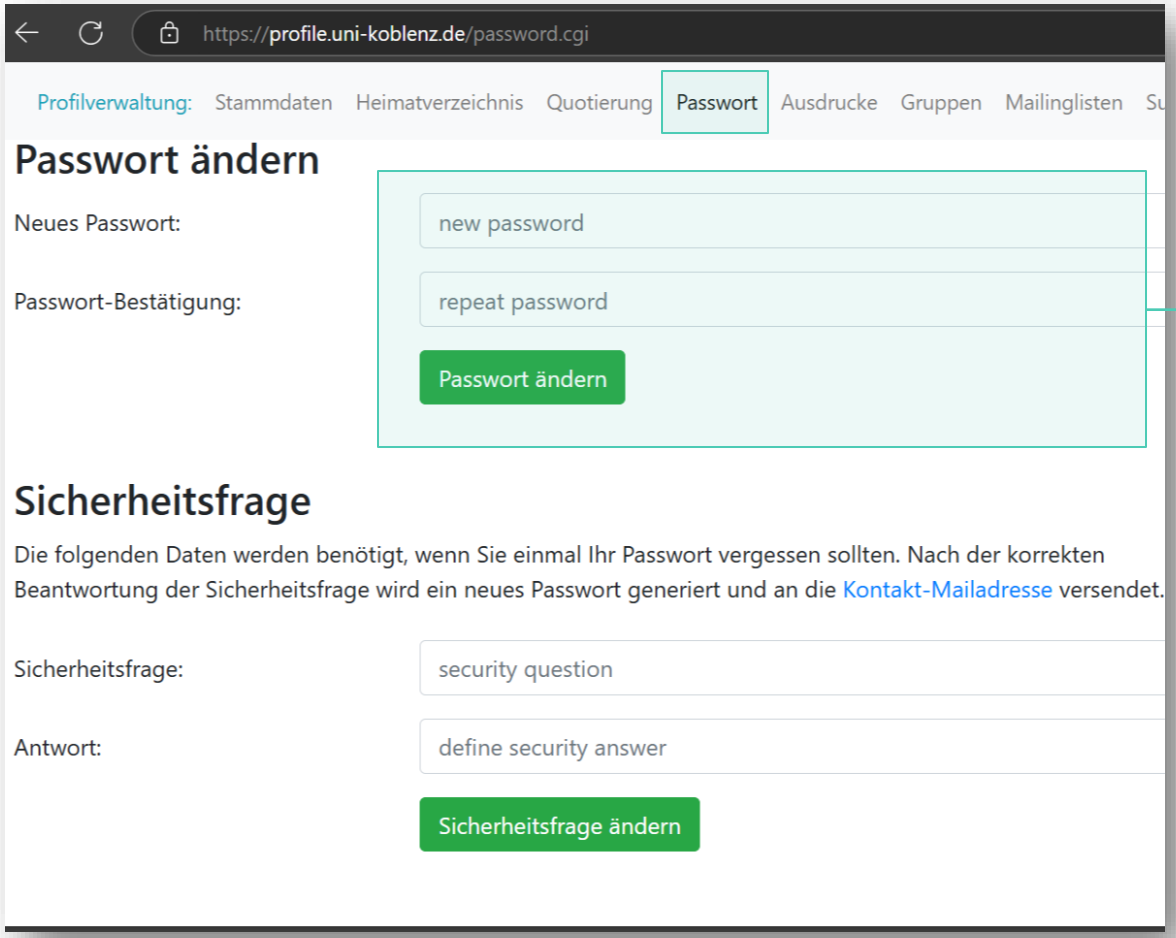


Über den Reiter *Passwort* bei der Profilverwaltung gelangen Sie zu der Seite, wo Sie Ihr Passwort ändern oder eine neue Sicherheitsfrage bestimmen können.

Ändern Ihres Uni-Passworts

universität koblenz
weiter:denken

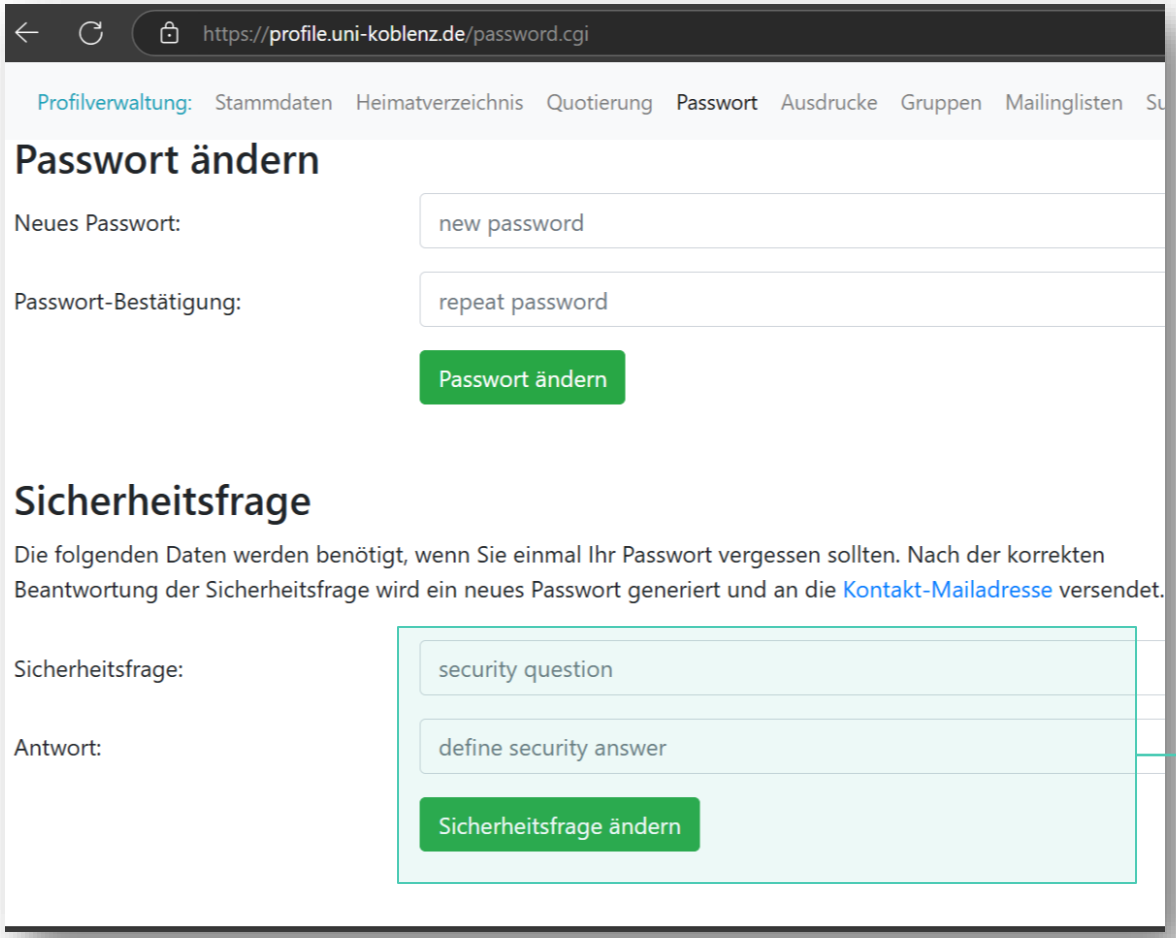
Passwortänderung bei der Profilverwaltung



Hier können Sie ein neues Passwort festlegen.

Sicherheitsfrage als 2. Faktor

Festlegung oder Änderung der Sicherheitsfrage



Sobald die Multifaktor-authentifizierung 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.

Hilfe

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

+49 261 287 1301

Zu folgenden Zeiten:

Mo.– Di. 9:30 - 11:30 & 12:30 - 14:30 Uhr

Fr. 12:30 - 14:30 Uhr

https://www.uni-koblenz.de/de/zimt