Zwei-Faktor-Authentisierung

Bei der Zwei-Faktor-Authentisierung wird der Account nicht nur durch den Benutzernamen und dem zugehörige Kennwort gesichert, sondern durch eine zweite Abfrage. Die zweite Abfrage fordert in der Regel zur Eingabe eines Passwortes auf, das nur einmal verwendet werden kann und nur über einen kurzen Zeitraum gültig ist.

Hardware-Token - OTP(one-time password)-Generator

Für die Erzeugung des Einmalpasswortes erhalten die Angehörigen der Zentralen Universitätsverwaltung ein Hardware-Token, genauer einen OTP(one-time password)-Generator.

Beschaffung von Hardware-Tokens

- Sekretariate können die Hardware-Tokens für ihre Einrichtung per E-Mail an **ciso@uni-ulm.de** anfordern.
- Der Bedarf sollte möglichst frühzeitig an **ciso@uni-ulm.de** gemeldet werden, damit eine rechtzeitige Beschaffung veranlasst werden kann.

Ausgabe der Hardware-Tokens

Angehörigen der Zentralen Universitätsverwaltung erhalten die Hardware-Tokens von ihren Sekretariaten.

Aufbewahrung von Hardware-Tokens

Da Hardware-Tokens eine vergleichbare Funktion wie Schlüssel erfüllen, müssen sie genau so sorgfältig aufbewahrt und behandelt werden.

Verlust oder Defekt von Hardware-Tokens

Sollte ein Hardware-Token als verloren oder defekt gelten, kann das zuständige Sekretariat ein Neues ausgeben. Ein verlorenes Hardware-Token sollte umgehend deaktiviert werden. Dazu muss das IDM-Passwort neu gesetzt werden.

Beenden der Tätigkeit in der ZUV

Beim Beenden der Tätigkeit in der ZUV sind sämtliche erhaltene Hardware-Tokens an das zuständige Sekretariat zurückzugeben.

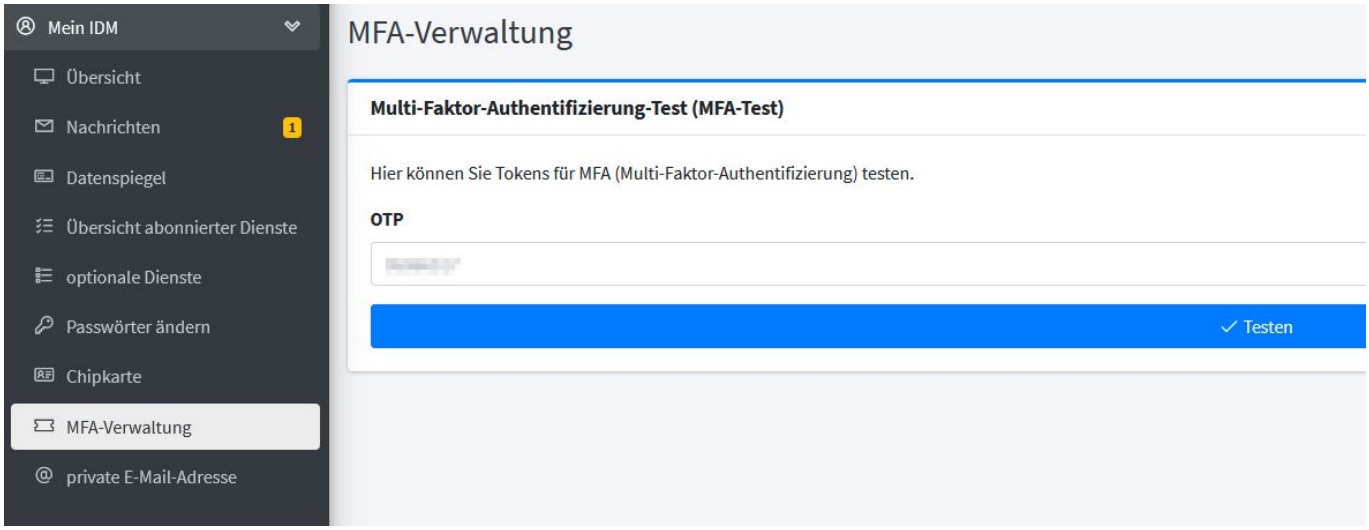
Bedienung und Anzeigeelemente des Hardwaretokens

- Nach der Betätigung des **Einschaltknopfes** erscheint das **Einmalpasswort** im Display.
- Der **Timer** zeigt die Gültigkeitsdauer des Passwortes an. Die maximale Gültigkeitsdauer beträgt 30 Sekunden. Die Gültigkeitsdauer beginnt am Anfang (hh:mm:00) einer Minute und dann wieder nach 30 Sekunden (hh:mm:30). Es stehen also nicht immer die vollen 30 Sekunden zur Eingabe des Einmalpasswortes zur Verfügung.
- Die Batterie sollte mindestens fünf Jahre halten. Befindet sich die **Batteriestatusanzeige** im letzten drittel, sollte das Hardware-Token ersetzt werden.

Aktivierung der Zwei-Faktor-Authentisierung

Nach Erhalt des Hardware-Tokens müssen Sie sich diesen über das **IDM-Self-Service Portal** des kiz zuweisen. Hierfür sind folgende Schritte notwendig:

- Melden Sie sich am IDM-Self-Service-Portal des kiz an.
- Wählen Sie im Bereich **Mein IDM** die Funktion **MFA-Verwaltung** aus.
- Nun können Sie per Tastendruck auf Ihrem Hardware-Token ein sechsstelliges Einmalpasswort erzeugen. Geben Sie dieses in das Feld **OTP** ein. Mit einem Klick auf **Testen** wird Ihnen dieses Hardware-Token zugewiesen. Wobei das System automatisch prüft und erkennt, welcher Hardware-Token zu diesem Zeitpunkt das eingegebenen Einmalpasswort erzeugt hat. Bitte beachten Sie, dass die erzeugten Passwörter alle 30-Sekunden neu generiert werden.



- Ihr Hardware-Token ist ab diesem Zeitpunkt als zweiter Faktor einsatzfähig und für die Verbindung zum ZUV-VPN-Server zwingend erforderlich.
- Bitte nutzen Sie nach erfolgreicher Zuweisung eines Hardware-Tokens die oben beschriebene Funktion erneut, um die Zuweisung einmal zu testen. Sollte es zu Problemen kommen, wenden Sie sich bitte an den Helpdesk des kiz (helpdesk@uni-ulm.de).
- Sie können die Funktion des Tokens jederzeit überprüfen, indem Sie durch Tastendruck auf das Token ein neues Einmalpasswort erzeugen und in das Feld „OTP“ eingeben und auf **Zuweisen/Überprüfen** klicken.
- Erscheint die Fehlermeldung **Hardware-Token kann nicht zugewiesen werden**, bitte ein neues Einmalpasswort erzeugen und nochmal probieren.

Ein neues Hardware-Token aktivieren

- Bei Verlust oder Defekt eines Hardware-Tokens muss dieses zuerst durch das Neusetzen des IDM-Passwortes deaktiviert werden. Dazu gibt es zwei Möglichkeiten:
  - Neusetzen des IDM-Passwortes über das SB-Terminal: Gehen Sie mit Ihrer Chipkarte und der zugehörigen PIN-Nummer zu einem der SB-Terminals und lassen Sie sich ein neues IDM-Initialpasswort generieren.
  - Zurücksetzen des IDM-Passwortes über den Helpdesk: Ist es Ihnen nicht möglich das IDM-Passwort am SB-Terminal zurückzusetzen, nehmen Sie mit dem kiz-Helpdesk Kontakt auf.

Ein Hardware-Token deaktivieren

Generell gilt, das ändern des IDM-Passwortes deaktiviert das Hardware-Token. Ein Hardware-Token wird dann zur Anmeldung nicht mehr benötigt.

Die Technik hinter Zwei-Faktor-Authentisierung

In diesem Artikel ist das technische Prinzip beschrieben, auf dem die **Zwei-Faktor-Authentisierung** basiert Zwei-Faktor-Authentisierung.