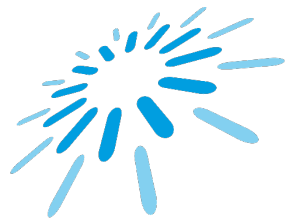


Schulungen IT-Sicherheit

# Multi-Faktor-Authentisierung (MFA) an der TH Aschaffenburg mit eduMFA

Bernd Hans Ottow

Januar 2025



TH Aschaffenburg  
university of applied sciences

# Erweiterung der Web-basierten Anmeldung mit Shibboleth

The screenshot shows the login page for Moodle at TH Aschaffenburg. At the top right, there is a language dropdown set to 'Deutsch (de)' and a 'Login' button. The main header features the TH Aschaffenburg logo and the text 'Anmelden bei Moodle der Technischen Hochschule Aschaffenburg'. The login form includes fields for 'Benutzername' and 'Passwort', a checkbox for 'Anmeldung nicht speichern', and a checkbox for 'Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.'. Below the form are two buttons: 'Anmelden' and 'Mit Passkey Anmelden'. A large grey arrow points from the left towards the 'Mit Passkey Anmelden' button. At the bottom left, there are links for 'Passwort vergessen?' and 'Hilfe benötigt?'. The page is framed by a blue border with the university logo and 'Lernpla' on the left, and a photo of a student reading on the right.

Deutsch (de) Login

TH Aschaffenburg  
university of applied sciences

Lernpla

TH Aschaffenburg  
university of applied sciences

Anmelden bei Moodle der Technischen Hochschule  
Aschaffenburg

Benutzername

Passwort

Anmeldung nicht speichern

Die zu übermittelnden Informationen anzeigen, damit ich die Weitergabe gegebenenfalls ablehnen kann.

Anmelden


Mit Passkey Anmelden

Passwort vergessen?  
Hilfe benötigt?

eduMFA erweitert die Authentisierung mit mehreren Faktoren

**Aus Sicherheitsaspekten** (*siehe Schulung zu Passwörtern, MFA, Passkeys*) müssen Sie sich u. a. bei den folgenden webbasierten Diensten mit Shibboleth zukünftig primär passwortlos mit Hilfe eines Passkey anmelden:

- Moodle
- Zoom
- FAUBox
- HISinOne – CampusPortal
- Opencast
- UCware Telefon-Softclient
- Helpdesk Ticketsystem
- BayernCollab
- ...



Konkrete Vorgehensweise:  
**Passwortlose Anmeldung mit  
Passkeys**  
**2 Varianten**

# Option 1: HW-Token - Sicherheitsschlüssel



# 1- Empfehlung für höchste Sicherheit: FIDO2 Key, HW Token

- **Nutzung eines physischen Sicherheitsschlüssels**

- FIDO2-Keys, Hardware Tokens (u.a. Yubikey)
- Verbindung typisch über USB teilweise auch NFC
- **Diese Variante stellt die aktuell sicherste Form der Authentisierung dar.**



- Jeder Token ist ein Unikat und kann nicht kopiert werden!
- **Daher wird eine Backup-Lösung benötigt:**
  - Ein zweiter Key oder eine alternative Authentisierung z. B. via Smartphone bei Verlust/Defekt des Tokens

# 1- Empfehlung für höchste Sicherheit: FIDO2 Key, HW Token

- **Vorgehen:**

- **Ersteinrichtung:**

- PIN (empfohlen mind. 8 Zeichen) für den Token vergeben
- Passkey auf dem Token speichern

- **Zur Authentisierung im (beliebigen) Webbrowser mit Passkey**

- „*Externer Sicherheitsschlüssel*“ auswählen
- Nach Aufforderung den Token per USB mit dem Gerät verbinden.
- Eingabe der PIN
- Physisches Antippen des Token → *angemeldet!*



# Option 2: Smartphone bzw. Smart Device





## 2 - Empfehlung für hohe Sicherheit & Komfort: Smartphone

- **Nutzung eines vorhandenen Smartphones:**
  - Ihr Smartphone hat bereits alle nötigen Funktionen zur Mehrfaktor-Authentisierung mit biometrischen Verfahren
  - Der private Hauptschlüssel („Passkey“) kann in den bereits integrierten Passwort Managern gespeichert werden:
    - **Android:** Google Passwort Manager (oder optional andere Hersteller-abhängige Dienste – z. B. Samsung Pass)
    - **Apple:** iCloud Schlüsselbund
  - **Durch die Cloud-Synchronisierung entfällt hier die zwingende Backup-Lösung!** Passkey-Nutzung z. B. auch vom Tablet



## 2 - Empfehlung für hohe Sicherheit & Komfort: Smartphone

- **Vorgehen:**

- **Ersteinrichtung:**

- Biometrische Verfahren aktivieren
    - QR Code scannen zur Kopplung und Einrichtung
    - Passkey im Passwort Manager des Telefons speichern

- **Unterstützte Browser am Anmelde-PC (Win 10 oder 11):**

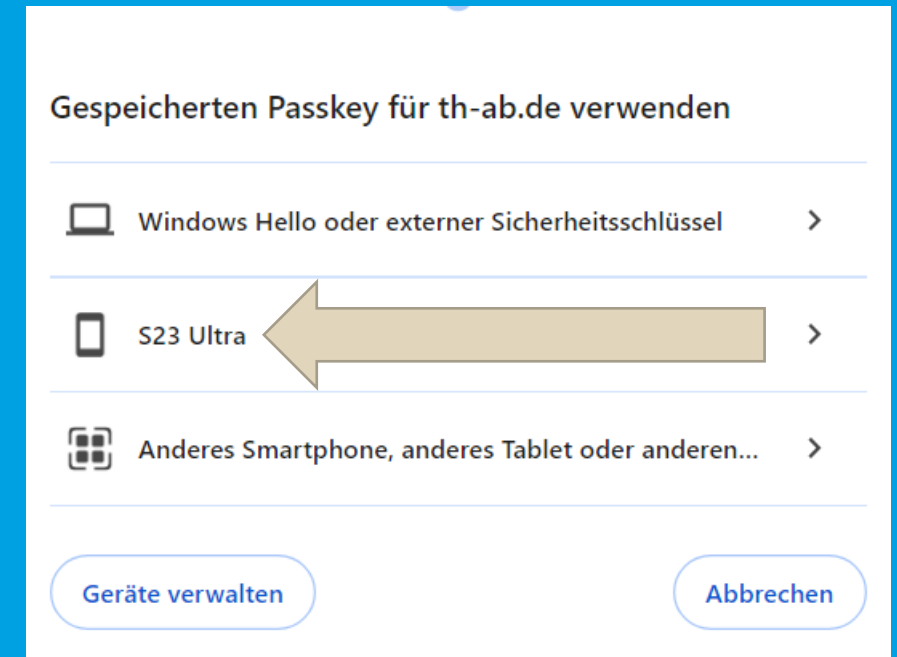
- Microsoft Edge (vorinstalliert auf TH Systemen)
    - Google Chrome

- **ACHTUNG: Keine Unterstützung in Mozilla Firefox – erst mit aktuellstem Win 11!**




## 2 - Empfehlung für hohe Sicherheit & Komfort: Smartphone

- **Vorgehen:**
  - Zur Authentisierung mit Passkey im Webbrowser des Anmelde-PC:
    - *Eingerichtetes Smartphone* auswählen
    - Am Smartphone mit biometrischem Verfahren bestätigen  
→ *angemeldet!*

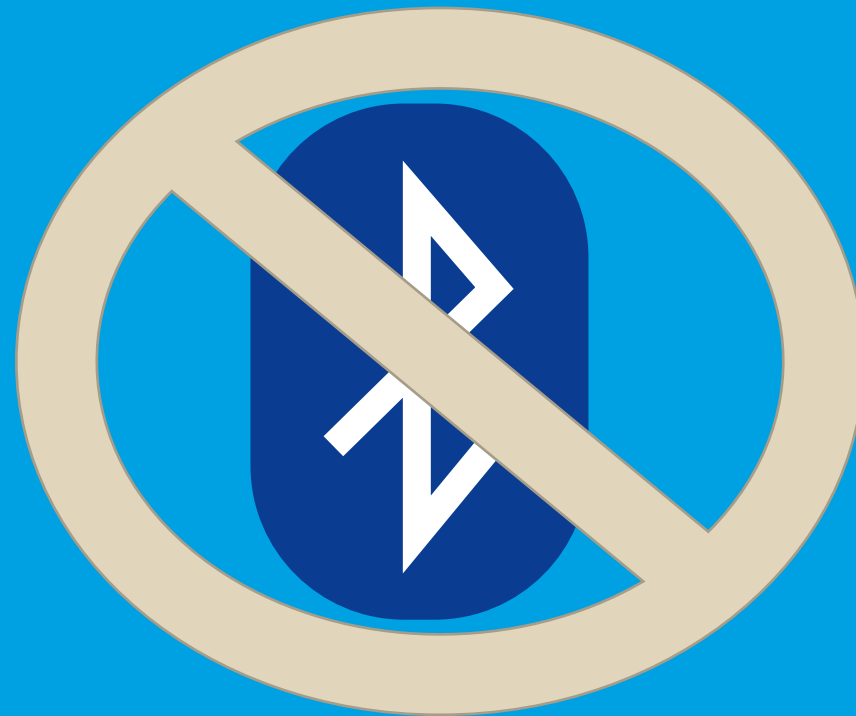


- **ACHTUNG: Bluetooth-Verbindung zu dem Anmelde-PC nötig!**



Konkrete Vorgehensweise:  
**Sonderfälle, die eine Anmeldung  
mit Passwort + Einmalkennwort  
erfordern  
1 Variante**

# Option 3: Kein USB – Kein Bluetooth



### 3 - Empfehlung NUR für Sonderfälle: kein BT / kein USB

- Falls ein von Ihnen genutztes Gerät kein Bluetooth unterstützt (v. a. Rechnerräume), Sie kein USB-Hardware Token besitzen, bzw. kein USB-Port nutzbar ist (z. B. spezielle Laborechner oder virtuelle Systeme):
  - Nur für diese Ausnahmefälle dürfen Sie eine Anmeldung mit Nutzernamen und Passwort und zusätzlichem Time-Based One Time Password (TOTP) nutzen
  - Auch dieses Verfahren muss wie ein Passkey vorher eingerichtet werden.



### 3 - Empfehlung NUR für Sonderfälle: kein BT / kein USB


- **Vorgehen:**

- **Ersteinrichtung:**

- Sie benötigen eine „Authenticator App“ auf ihrem Smartphone, der die zeitbasierten Einmalcodes generiert
- QR-Code scannen zur Generierung der korrekten Einmalcodes
- Verifizierung durch korrekte Eingabe eines aktuellen Codes

- **Zur Authentisierung im Webbrowser mit Benutzer, Passwort und Einmalkennwort**

- Wie bisher Nutzernamen und Passwort eingeben und auf „Anmelden“ klicken
- Danach Einmalpasswort eingeben → *angemeldet!*



Umsetzung der 3 Optionen je nach  
**Benutzergruppe**  
&  
**Zugriffsberechtigungen**





Gruppe A:  
**Angestellte Mitarbeitende  
Professorinnen und Professoren**

## Angestellte Mitarbeitende, Professorinnen & Professoren

- **Option 1: Primäre Nutzung eines Sicherheitsschlüssels (Yubikey) mit eingerichteten TH-Passkey zur Authentisierung**
  - Der Yubikey wird von der Hochschule zum dienstlichen Gebrauch leihweise zur Verfügung gestellt (wie Dienst-PC)
- **Option 2: Einrichtung eines TH-Passkey am privaten Smartphone mindestens als Backup, falls der Yubikey vergessen wird oder abhanden kommt**
  - Hinweis: *In notwendigen Fällen kann ein zweiter Yubikey als Backup-Lösung zur Verfügung gestellt werden*
- **Option 3: Falls Sie mit Systemen (u. a. Hörsäle, Labore, etc.) ohne BT/USB arbeiten: Einrichtung von TOTP**





Gruppe B:  
**Studierende**  
**Externe Lehrbeauftragte**

## Studierende, externe Lehrbeauftragte

- **Option 2: Einrichtung eines TH-Passkey am privaten Smartphone zur primären Authentisierung**
- **Option 3: Einrichtung von TOTP, da die Geräte in Hörsälen, Labors, etc. unter Umständen kein Bluetooth bereitstellen und Sie auch hier Möglichkeiten zur Anmeldung benötigen.**
- **OPTIONAL:**
  - Option 1: Private Beschaffung und Nutzung eines Sicherheitsschlüssels (z. B. Yubikey) und Einrichtung von Passkeys (auch private) zur Authentisierung mit höchster Sicherheit





Einrichtung und Aktivierung  
**eduMFA und Passkeys auf**  
**<https://mfa.th-ab.de>**

## Anleitungen zur Einrichtung

- **Hands-on Videos zu den 3 Optionen im Moodle-Kurs zur IT-Sicherheit – Einrichtung Yubikey, Passkeys, TOTP am Smartphone:**
- ***„Aktivierung MFA an der TH für webbasierte Dienste“***
  - ID 6159: „IT-Sicherheit – Schulungen für Beschäftigte“
  - ID 7280: „IT-Sicherheit – Schulungen für Studierende“
- **Anleitungen in der Knowledge Base des Helpdesks:**
  - <https://helpdesk.th-ab.de/help/de-de/10/161>



**WICHTIG:**

**„Einmal MFA – immer MFA!“**

Eine risikobehaftete Authentisierung nur mit Nutzernamen + Kennwort wie bisher ist nach Aktivierung nicht mehr möglich und aus Sicherheitsaspekten auch nicht vorgesehen!



**WICHTIG:**


**„Einmal MFA – immer MFA!“**

Richten Sie daher zeitgleich zur Yubikey Aktivierung (Opt. 1) ihre Backup-Lösung mit Smartphone (Opt. 2) bzw. zweitem Yubikey ein, bzw. die zeitbasierten Einmalkennwörter TOTP (Opt. 3)!





**Bitte aktivieren Sie die Multifaktor  
Authentisierung (MFA) mit Passkeys  
schnellstmöglich!**



**Probleme? Fragen? Anregungen?**  
**Ihre Mail an [helpdesk@th-ab.de](mailto:helpdesk@th-ab.de)**

**Dankeschön!**