

# 2-Faktor-Authentifizierung

**Zum Schutz vor Cyberangriffen: Wir führen 2 Faktor-Authentifizierung (2FA) ein.**

Die jüngsten Vorfälle an den Hochschulen in Karlsruhe, Furtwangen und Villingen-Schwenningen zeigen, dass Cyberkriminalität gegen Hochschulen weiter zunimmt. Der Angriff erfolgt dabei oftmals über Phishing: Mit gefälschten E-Mails verschaffen sich Kriminelle Zugang zu den Systemen einer Hochschule.

Wir wollen den Schutz der Hochschule Offenburg vor Cyberangriffen weiter stärken. Deshalb führen wir in den kommenden Wochen die 2-Faktor-Authentifizierung (2FA) ein. Mit 2FA können sich Mitarbeitende und Studierende wirksam gegen Phishing schützen.

## Wie funktioniert 2FA?

Bei 2FA nutzen Sie zusätzlich zum Benutzerpasswort einen weiteren Faktor, etwa ein Smartphone oder einen Hardwaretoken, um sich einzuloggen. Dies sichert Ihren Benutzeraccount doppelt gegen fremde Übernahme. Viele von Ihnen kennen dieses Verfahren bereits vom Onlinebanking (SMS/TAN).

Die Umstellung unserer Systeme auf 2FA erfolgt am 4. Dezember. Danach wird die Anmeldung bei VPN, Mail (Groupwise/Webmail) sowie Filr nur noch mit 2FA funktionieren. Außerdem werden zusätzliche Dienste nur noch im Hochschulnetz (vor Ort) oder über VPN erreichbar sein.

## Quickstart Guide


Damit ein Gerät als zweiter Faktor verwendet werden kann, muss es registriert werden. Das Gerät wird dadurch ihrem Campus-Benutzerkonto zugeordnet und kann dann zusammen mit Campus-Benutzername und -Passwort für 2FA-Anmeldungen genutzt werden.

Die Einrichtung dauert nur wenige Minuten.

## Registrierung (AA-Portal)

Die Registrierung erfolgt über <https://2fa.cit.hs-offenburg.de/account/>

1. Melden Sie sich zunächst mit ihrem **Campus-Benutzername** und **-Passwort** an



**H** 2-Faktor-Authentifizierung - Hochschule Offenburg

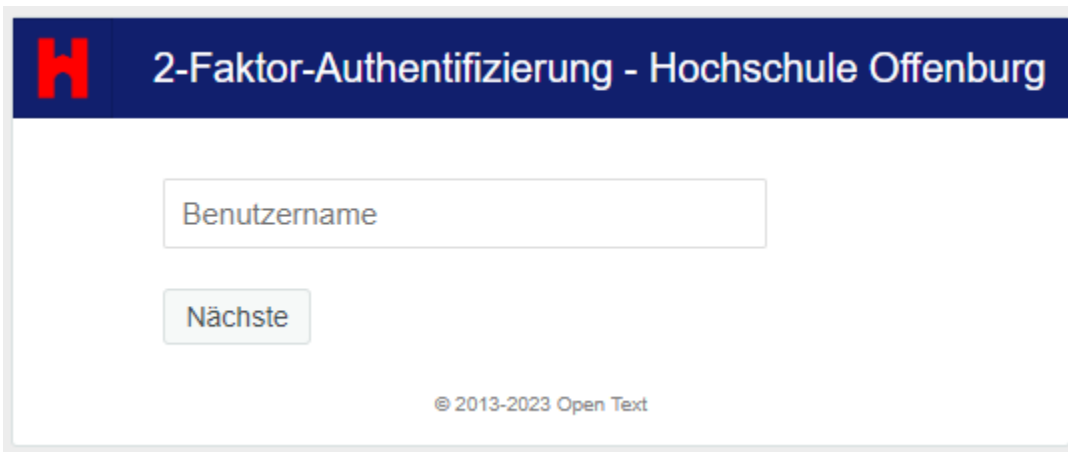
Passwort

Campus-Benutzerpasswort

Anzeigen

Nächste Abbrechen

© 2013-2023 Open Text



2. Nach der Anmeldung sehen Sie eine Seite mit bereits registrierten Faktoren. Zum Hinzufügen eines zweiten Faktors klicken sie auf das Plus. Ihr Benutzerpasswort (LDAP) ist bereit automatisch registriert.

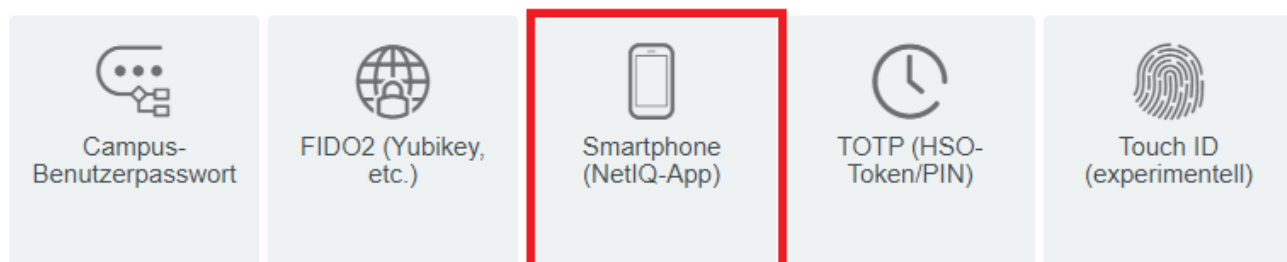


3. Es werden Ihnen mehrere mögliche Methoden vorgeschlagen. Die einfachste und unkomplizierteste Variante ist die **Smartphone** Methode. Klicken Sie auf das Smartphone Symbol.

(Alternativen Methoden ohne Smartphone: siehe unten)

## Verfügbare Methoden für die Registrierung

Wählen Sie eine Authentifizierungsmethode für die Registrierung aus. Nach der Registrierung kann die Methode zur Anmeldung verwendet werden. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.



4. Laden Sie die **NetIQ Advanced Authentication - App** auf ihr Smartphone herunter

Sie finden die App im Google Playstore/Apple Appstore. Die App ist kostenlos.




Android:



Apple:

Für die App müssen Sie einen eigenen Pin bestimmen, In den Einstellungen können Sie später auch alternativ ihren Fingerabdruck (Android) oder FaceID (Apple) hinterlegen.

### 5. Rufen Sie den QR-Code ab

 Smartphone (NetIQ-App)

Die Smartphone-Methode ermöglicht die Authentifizierung mittels Smartphone. Die Smartphone-Methode ist eine Out-of-Band-Authentifizierung. Die NetIQ Advanced Authentication-Anwendung sendet eine Push-Nachricht an das Smartphone, die Sie akzeptieren oder ablehnen können. Zur Verwendung der Methode muss die NetIQ Advanced Authentication-Mobil-App auf dem Smartphone installiert werden.

Anzeigename

Kategorie


Rufen Sie zum Registrieren einen QR-Code ab und scannen Sie ihn mit der Advanced Authentication-Mobil-App:


**QR-Code abrufen**

- Die AdvAuth-Mobil-App stellt einen Einmalpasswort-Code bereit, der als Ersatzmethode verwendet werden kann, wenn auf dem Smartphone keine Internetverbindung verfügbar ist.

### 6. Scannen Sie den QR Code mit ihrer NetIQ-App ab. Dafür müssen Sie auf das blaue Plus in der App klicken.

(bei Apple/iOS ist das Plus oben)

 2-Faktor-Authentifizierung - Hochschule Offenburg

 Smartphone (NetIQ-App)


Die Smartphone-Methode ermöglicht die Authentifizierung mittels Smartphone. Die Smartphone-Methode ist eine Out-of-Band-Authentifizierung. Die NetIQ Advanced Authentication-Anwendung sendet eine Push-Nachricht an das Smartphone, die Sie akzeptieren oder ablehnen können. Zur Verwendung der Methode muss die NetIQ Advanced Authentication-Mobil-App auf dem Smartphone installiert werden.

Anzeigename


Kategorie

Rufen Sie zum Registrieren einen QR-Code ab und scannen Sie ihn mit der Advanced Authentication-Mobil-App:

QR-Code abrufen



- Die AdvAuth-Mobil-App stellt einen Einmalpasswort-Code bereit, der als Ersatzmethode verwendet werden kann, wenn auf dem Smartphone keine Internetverbindung verfügbar ist.



7. Wenn der Code gescannt wurde, klicken Sie auf Speichern

✓ **Registrierung ist abgeschlossen**  
Rufen Sie zum Registrieren einen QR-Code ab und scannen Sie ihn mit der Advanced Authentication-Mobil-App.  
QR-Code abrufen

1.



- Die AdvAuth-Mobil-App stellt einen Einmalpasswort-Code bereit, der als Ersatzmethode verwendet werden kann, wenn auf dem Smartphone keine Internetverbindung verfügbar ist.

Speichern Abbrechen




2.

Ihr zweiter Faktor sollte nun angezeigt werden

## Authentifizierungsmethoden

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung

 <p>Automatisch erstellt Campus-Benutzerpasswort</p>	 <p>Meine Smartphone... Smartphone (NetIQ-App)</p>	 <p>Hinzufügen</p>
---	---	---

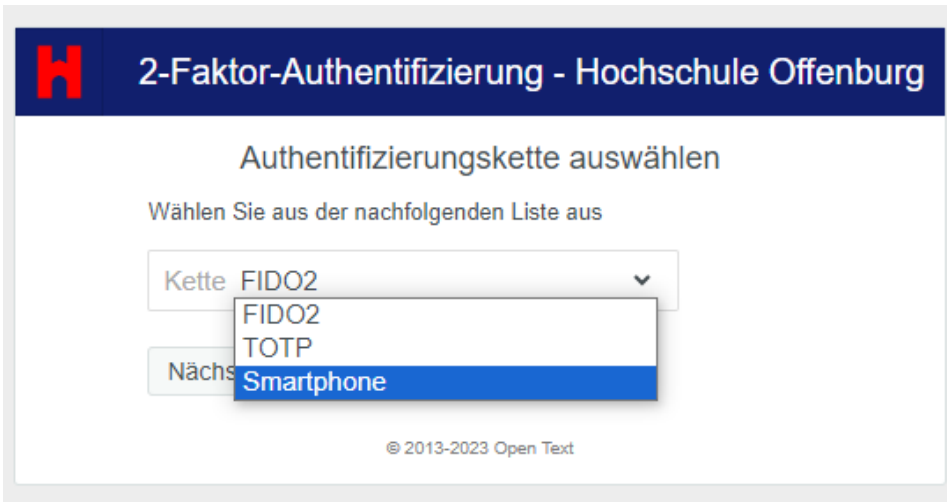
Die Registrierung Ihres zweiten Faktors ist damit abgeschlossen. Wenn Sie keinen weiteren Faktor registrieren wollen, können sich abmelden und die Seite verlassen.

## Anmelden

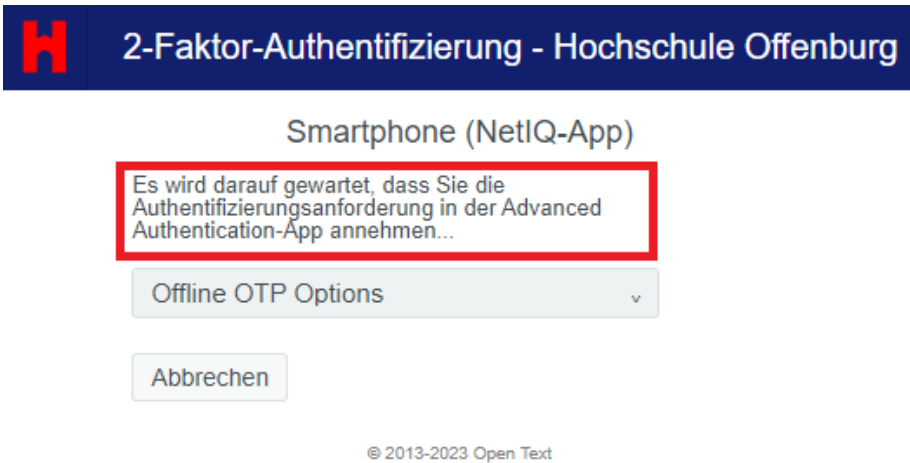
Nachdem Sie ihren zweiten Faktor registriert haben, wird dieser bei zukünftigen Anmeldungen bei Mail (Groupwise/Webmail) verlangt.

Probieren Sie die Anmeldung per Webmail aus: <https://webmail.hs-offenburg.de/>

Nach Eingabe von ihrem Benutzernamen + Passwort wird nun ein weiterer Faktor verlangt. Je nach Anmeldung werden Benutzernamen und Passwort separat abgefragt.

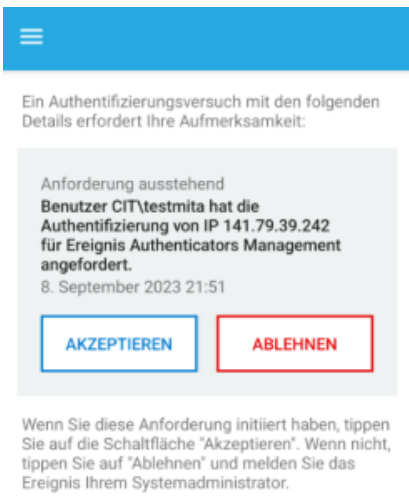


Es erscheint folgendes Fenster.



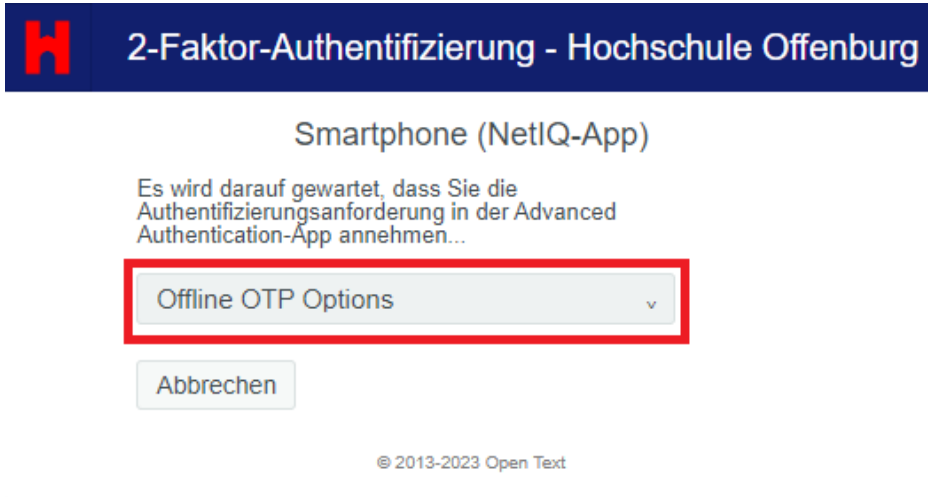
Öffnen Sie auf Ihrem Smartphone die NetIQ-Advanced-Authentication-App und warten Sie einen Moment.

Auf ihrem Smartphone erscheint ein Dialogfeld mit einem "Akzeptieren"-Button

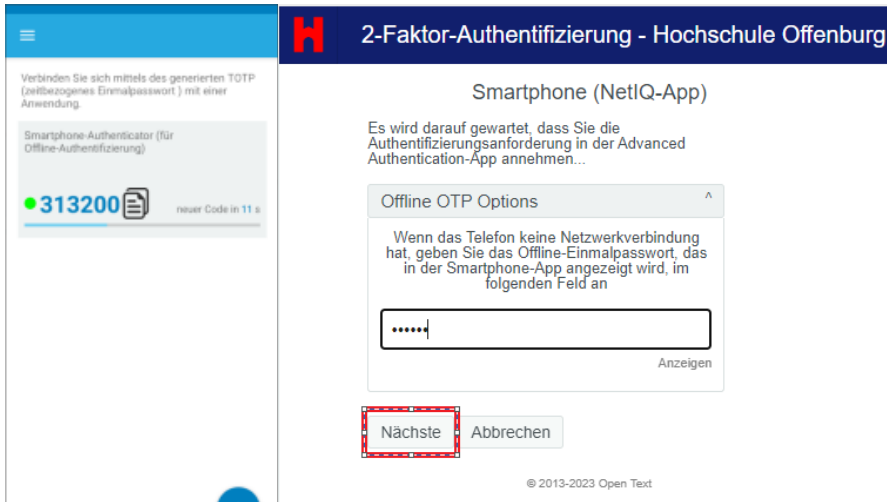


Nach Tippen auf "Akzeptieren" werden sie **automatisch** angemeldet. Warten Sie einen Moment, der Vorgang kann etwas dauern.

Wenn ihr Smartphone offline ist und sie kein Dialogfeld mit "Akzeptieren" bekommen, können sie die Offline OTP Option benutzen:



Geben Sie den Code aus ihrer NetIQ-App ein und klicken Sie auf "Nächste"



## FAQ

### Alternative Methoden

Sie können beliebig weitere Faktoren zusätzlich registrieren über <https://2fa.cit.hs-offenburg.de/account/>

Falls Sie nicht ihr Smartphone benutzen wollen, können Sie einen Token-Generator benutzen wie TOTP oder FIDO2.

## TOTP / HSO-Token / Google-Auth

Einmalpasswort-Token sind kleine Geräte in der Größe von Schlüsselanhänger, die eine Taste und ein Display mit 6 Ziffern haben. Bei der 2FA-Anmeldung mit Einmalpasswort-Token müssen Sie nach der Anmeldung mit Campus-Benutzername und -Passwort die Taste am Gerät drücken und anschließend die angezeigten 6 Ziffern eintippen.

Für diese Methode hat sich auch der Begriff TOTP etabliert. (Time Based One Time Password).

Den HSO-Token (TOTP) können Mitarbeiter bei der Campus-IT erhalten (B205).

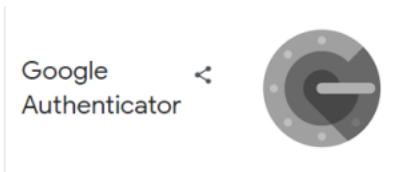
Studenten und Lehrbeauftragte können den HSO-Token in der Hochschulbibliothek in Offenburg oder Gegenbach ausleihen.

Ein Einmalpasswort-Hardware-Token kann nur für ein Benutzerkonto verwendet werden.



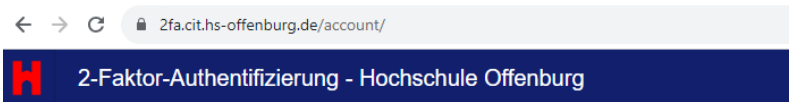
HSO-Token

Alternativ können auch Apps wie Google Authenticator als Einmalpasswort-Generator verwendet werden.



Melden Sie sich auf <https://2fa.cit.hs-offenburg.de/account/> an

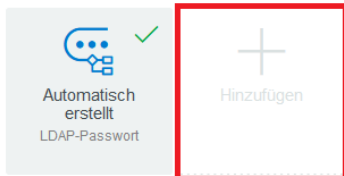
Klicken Sie auf das Plus



### Authentifizierungsmethoden

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung



wählen Sie TOTP aus



**Für den HSO-Token:**

Klicken Sie auf "OATH-Token"

**TOTP (HSO-Token/PIN)**

Die Methode mit zeitbasiertem Einmalpasswort (TOTP) generiert ein Einmalpasswort über ein Einmalpasswort-Hardwaretoken oder die NetIQ Advanced Authentication Mobil-App. Nach der Generierung muss das Einmalpasswort innerhalb eines bestimmten Zeitraums verwendet werden.

Arztname

Kategorie:

Service Name

Account Name

Diese Methode mit einer der folgenden Optionen verwenden:

- Geben Sie im Abschnitt zum OATH-Token die Seriennummer des OATH-Tokens ein, die sich üblicherweise auf der Rückseite des Tokens befindet. Generieren Sie ein Einmalpasswort vom Token und geben Sie es an.
- Klicken Sie auf QR-Code abrufen und scannen Sie dann den QR-Code mit einer Smartphone-App.
- Geben Sie ein manuelles TOTP ein, indem Sie Werte für 'Sekunden' und 'Zeitraum' eingeben.

Die Seriennummer ist auf der Rückseite des Geräts zu finden (unter Barcode)

Das Einmalpasswort (PIN) erhalten Sie, indem Sie auf den roten Knopf drücken.

**OATH-Token**

Seriennummer des OATH-Token

Einmalpasswort (OTP)





Klicken Sie anschließend auf **Speichern**

Ihr Hardware-Token wurde hinzugefügt.

**Für Google Authenticator** (oder ähnliche Apps):

Rufen sie den QR-Code ab und scannen Sie den Code mit ihrer App ab

Diese Methode mit einer der folgenden Optionen verwenden:

- Geben Sie im Abschnitt zum OATH-Token die Seriennummer des OATH-Tokens ein, die sich üblicherweise auf der Rückseite des Tokens befindet. Generieren Sie ein Einmalpasswort vom Token und geben Sie es an.
- Klicken Sie auf QR-Code abrufen und scannen Sie dann den QR-Code mit einer Smartphone-App.
- Geben Sie ein manuelles TOTP ein, indem Sie Werte für 'Geheimnis' und 'Zeitraum' eingeben.

OATH-Token

QR-Code abrufen

Manuelles TOTP

Speichern Abbrechen

Klicken Sie anschließend auf **Speichern**

Die Anmeldung erfolgt wie gewohnt mit Benutzername + Passwort.

Wählen Sie als Anmeldemethode TOTP aus

**H** 2-Faktor-Authentifizierung - Hochschule Offenburg

Authentifizierungskette auswählen

Wählen Sie aus der nachfolgenden Liste aus

Kette PW+FIDO2

PW+FIDO2

**PW+TOTP**

Nächste PW+Smartphone

© 2013-2023 Open Text

Geben Sie den von ihrem HSO-Token oder Google-Authenticator generierten Pin ein



## 2-Faktor-Authentifizierung - Hochschule Offenburg

### TOTP (HSO-Token/PIN)

Einmalpasswort # $\{number\}$  an  $\{masked\_recipient\}$  gesendet

Anzeigen

Nächste

Abbrechen

© 2013-2023 Open Text

Klicken Sie auf Nächste

### FIDO2 (Yubikey, USB-Stick)

Ein Yubikey (auch FIDO2-Stick genannt) ist ein spezieller USB-Stick, der als Schlüsselanhänger mitgeführt werden kann. Bei der 2FA-Anmeldung muss der Yubikey am PC/Notebook eingesteckt sein; nach der Anmeldung mit Campus-Benutzername und -Passwort muss am Yubikey eine Touch-Taste berührt werden - damit ist die Anmeldung abgeschlossen.

Yubikeys haben verschiedene Funktionen - wir unterstützen nur die "FIDO2" genannte Methode; unter diesem Begriff taucht die Methode auch in der Benutzeroberfläche von Programmen auf.



Melden Sie sich auf <https://2fa.cit.hs-offenburg.de/account/> an

Klicken Sie auf das Plus

## Authentifizierungsmethoden

Registrierte Methoden sind Authenticators, die Sie bereits registriert haben und zur Anmeldung verwenden können. Einmalpasswort-Methoden sind Authenticators mit Einmalpasswort.

Ihre registrierten Einfachmethoden für die Anmeldung

Automatisch erstellt  
LDAP-Passwort

Hinzufügen

Campus-Benutzerpasswort

FIDO2 (Yubikey, etc.)

Smartphone (NetIQ-App)

TOTP (HSO-Token/PIN)

Touch ID (experimentell)

Stecken Sie ihren FIDO2-Stick (Yubikey) in einen USB-Port ihres Rechners

### FIDO2 (Yubikey, etc.)

Die FIDO2-Methode ist eine Weiterentwicklung der FIDO-U2F-Methode, die den Standard der Webauthentifizierung verwendet und selbst ohne zugehöriges Passwort ein hohes Maß an Sicherheit bietet. FIDO2 ermöglicht die Authentifizierung unter anderem mit einem Telefon oder einem U2F-Gerät.

Anzeigename

Meine FIDO2 (Yubikey, etc.)

Kategorie

Standard

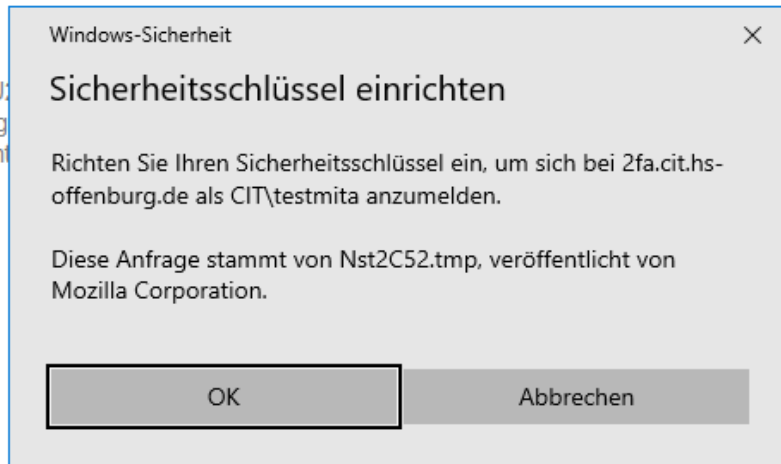
Gerät erkennen

Speichern

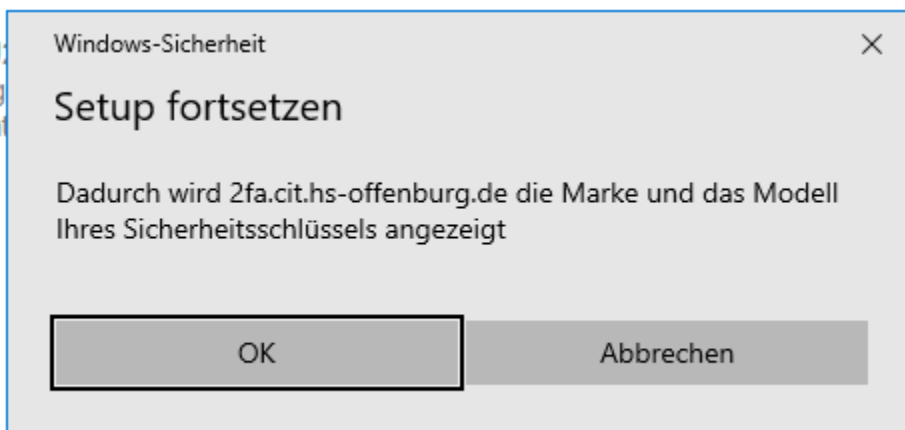
Abbrechen

folgen Sie den Anweisungen und klicken Sie auf ok

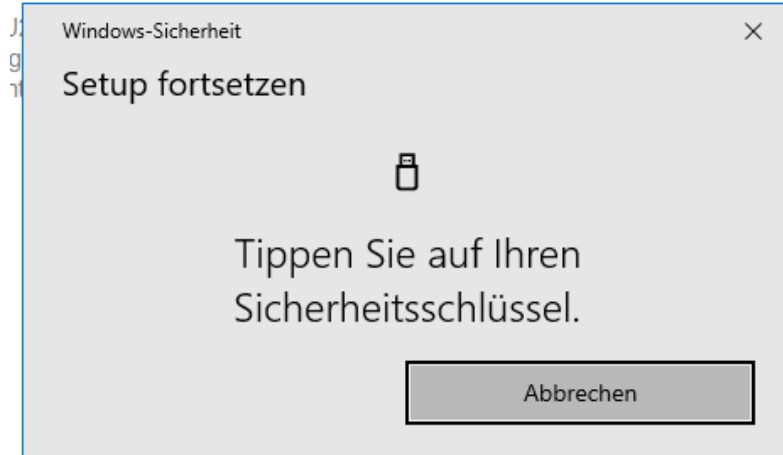
DO-U  
hörig  
rg unt



J  
g  
nt



Tippen Sie auf ihren Yubikey/Fido2-Stick



Klicken Sie auf **Speichern**  
Die Anmeldung erfolgt wie gewohnt mit Benutzername + Passwort.

Wählen Sie als Anmeldemethode FIDO2 aus



## 2-Faktor-Authentifizierung - Hochschule Offenburg

### Authentifizierungskette auswählen

Wählen Sie aus der nachfolgenden Liste aus

Kette PW+FIDO2 ▼  
PW+FIDO2  
PW+TOTP  
PW+Smartphone

© 2013-2023 Open Text

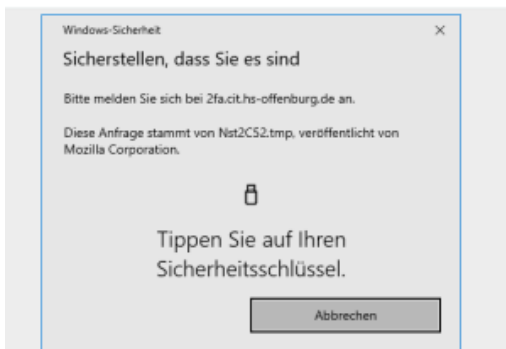
Stecken Sie den FIDO2-Stick/Yubikey in einen USB-Port ihres PCs

#### FIDO-2.0-Authentifizierung (Fast Identity Online Device 2.0)

Tippen Sie auf Ihr FIDO-2.0 (Fast Identity Online-2.0)-Gerät zum Authentifizieren

Abbrechen

© 2013-2023 Open Text



Tippen Sie auf den FIDO2-Stick

### Weitere Alternativen

Die Campus IT unterstützt die oben beschriebenen Methoden (Einmalpasswort/TOTP, Yubikey/FIDO2, Smartphone-Methode).

In einigen Fällen können weitere Methoden angeboten werden, die aber dann von der Campus IT nicht aktiv unterstützt werden. Wenn alles funktioniert, wunderbar - wenn nicht, können wir leider nicht helfen.

Derzeit ist dies vor allem "Touch ID" für Macs. Einige Kollegen berichten, dass die Methode funktioniert, die Handhabung ist ähnlich wie bei Yubikey/FIDO2.

Wir prüfen noch, ob auch "Windows Hello" sinnvoll ist - evtl. verschwindet die Methode auch wieder von der Liste.

### Notfallpasswort / Token vergessen

Falls Sie ihr Smartphone/Token vergessen oder es nicht mehr funktionsfähig ist, können Sie sich bei der Campus IT **vor Ort** (B205) ein eintägiges Notfallpasswort geben lassen oder einen neuen zweiten Faktor eintragen. Das Notfallpasswort gilt für diesen Tag als zweiter Faktor

### IMAP und CalDAV

IMAP und CalDAV sind ein Sonderfall bezüglich 2FA und problematisch, da die Programme wie z.B. Thunderbird, Outlook oder Apple Mail die Technik nicht direkt unterstützen (sie zeigen kein Fenster zur Eingabe des zweiten Faktors an). Deshalb ist von den hier vorgestellten Methoden die Smartphone-Methode die einzig praktikable.

Die allgemeine Vorgehensweise ist wie folgt:

- Registrieren Sie Ihr Smartphone mit der Smartphone-Methode im AA-Portal.
- Sobald 2FA für GroupWise aktiv ist wartet das IMAP- bzw. CalDAV-Programm nach der Anmeldung mit Campus-Benutzernamen und -Kennwort so lange, bis Sie am Smartphone den Zugriff per "Akzeptieren" bestätigt haben.
- Der zweite Faktor hat in diesem Fall eine Gültigkeit von 10 Stunden - d.h. solange ist kein weiteres "Akzeptieren" notwendig, sofern sich nicht die IP-Adresse ändert.
  - Beispielszenario zum IP-Adresswechsel: Sie nutzen ein Notebook und rufen auf diesem per IMAP Ihre Mails ab. Sie haben sich an Ihrem Arbeitsplatz (per Kabel verbunden) erfolgreich per 2FA authentifiziert. Nun wechseln Sie Ihren Standort in ein Besprechungszimmer und möchten dort (per WLAN) Ihre Mails abrufen. Hierfür ist eine erneute Authentifizierung nötig, da Ihr Notebook in einem anderen Netz ist und daher auch eine andere IP Adresse besitzt.

Hinweise:

- Das genaue Verhalten hängt vom jeweiligen Programm ab.
- IMAP- und CalDAV-Programme haben oft im Hintergrund mehrere Verbindungen zum Server offen. Dies kann zu seltsamen Effekten führen - so z.B. dass zwar die Betreffs neuer Mails angezeigt werden, für das Anzeigen kompletter Mails aber erst wieder am Smartphone der zweite Faktor akzeptiert werden muss.
- IMAP und CalDAV sind verschiedene Verbindungen, teilweise müssen diese separat akzeptiert werden.