How Does Multi-Factor Authentication via Hardware Token (FIDO 2) Work at UZH?

A *token* is a digital (software token) or physical object (hardware token) that generates regularly changing codes for user authentication. Unlike software tokens, hardware tokens do not require the user to enter any codes manually. The code check takes place automatically. The standard in question is: FIDO 2 (Fast Identity Online 2).

Hardware recommendation of the Central IT of the University of Zurich:

The Central IT of the UZH recommends the use of the model: Token 2 Pin+ series (link).
UZH reserves the right to block security tokens that do not meet the requirements in the future.

Note:

To avoid complications, the initial configuration of the hardware token should should be carried out in the following browser: Microsoft Edge.

NFC (Near Field Communication):

The tokens mentioned have an NFC interface, which also enables login via an NFC-enabled mobile phone.

When logging in, the user enters their user name and password. The code generated by the hardware token is then requested. With some hardware tokens, the user must first set or enter a self-defined *PIN (personal identification number)* in order to activate or use the device. It serves as an additional layer of protection. Even if someone gains physical access to the hardware token, they cannot use it without knowing the PIN.

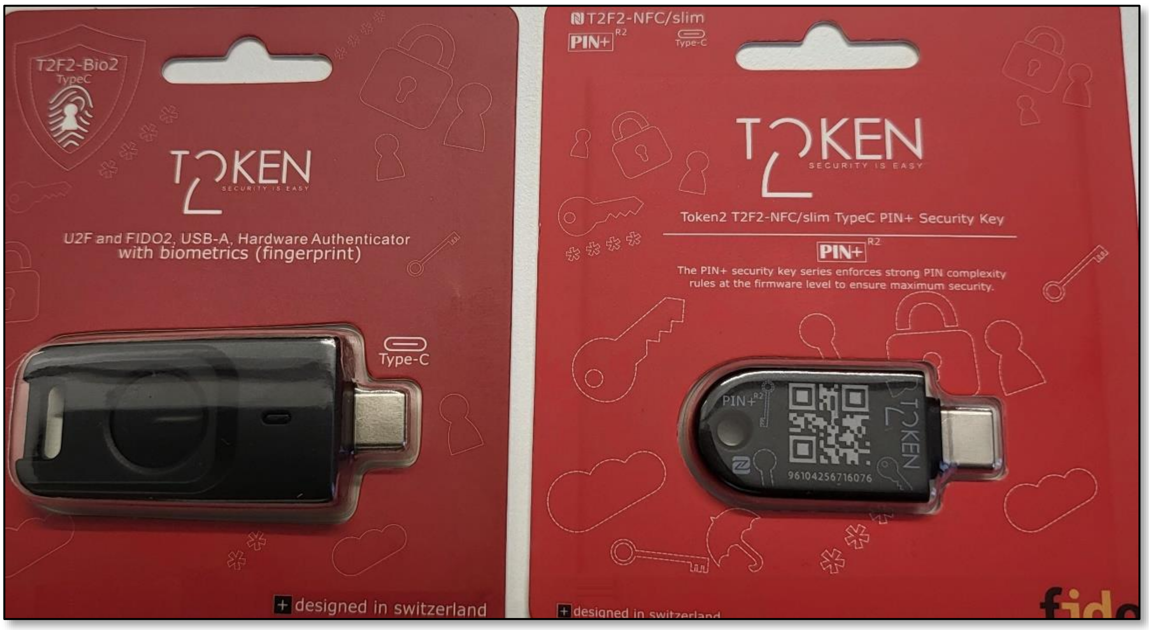
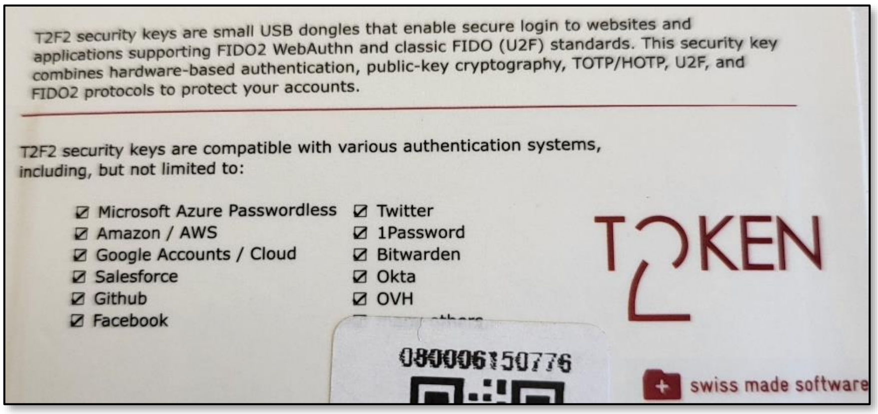

T2F2-Bio2
TypeC
TOKEN
SECURITY IS EASY
U2F and FIDO2, USB-A, Hardware Authenticator
with biometrics (fingerprint)
Type-C
designed in switzerland
T2F2-NFC/slim
PIN+ R2
Type-C
TOKEN
SECURITY IS EASY
Token2 T2F2-NFC/slim TypeC PIN+ Security Key
PIN+ R2
The PIN+ security key series enforces strong PIN complexity rules at the firmware level to ensure maximum security.
PIN+
TOKEN
96104256716076
designed in switzerland
fido

Fig 1: Hardware token in the form of USB sticks: fingerprint token (left) and password token (right).



T2F2 security keys are small USB dongles that enable secure login to websites and applications supporting FIDO2 WebAuthn and classic FIDO (U2F) standards. This security key combines hardware-based authentication, public-key cryptography, TOTP/HOTP, U2F, and FIDO2 protocols to protect your accounts.

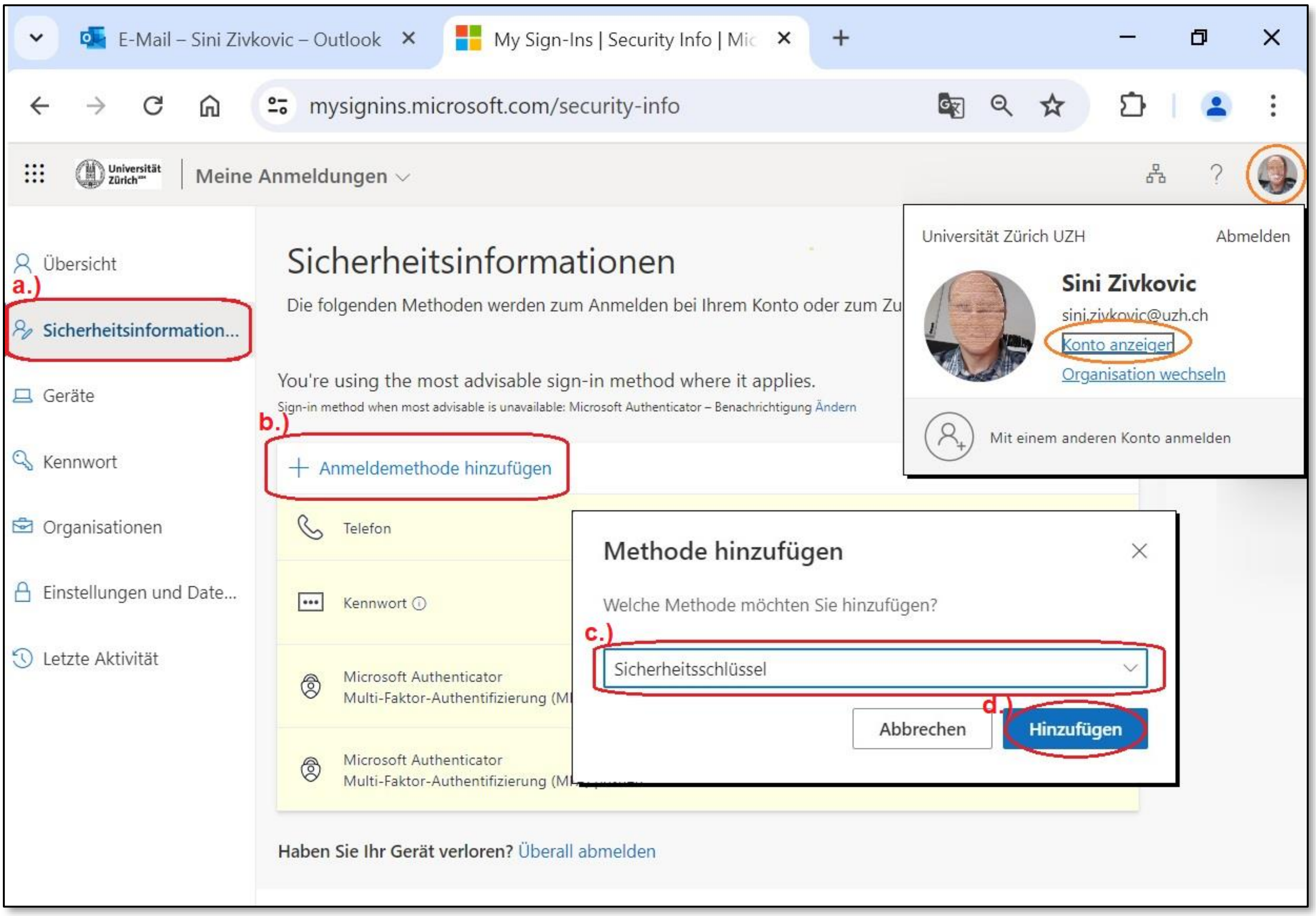
T2F2 security keys are compatible with various authentication systems, including, but not limited to:

- ☑ Microsoft Azure Passwordless
- ☑ Amazon / AWS
- ☑ Google Accounts / Cloud
- ☑ Salesforce
- ☑ Github
- ☑ Facebook
- ☑ Twitter
- ☑ 1Password
- ☑ Bitwarden
- ☑ Okta
- ☑ OVH
- others

Fig 2: Compatibility with various other authentication systems.

Setting up the token

Log in to your MS365 profile account, either *directly* by calling up the URL *mysignins.microsoft.com* or *indirectly* via your business card from your MS365 application (click on your *profile picture* > *'Show account'*).



E-Mail – Sini Zivkovic – Outlook

My Sign-Ins | Security Info | Mic

mysignins.microsoft.com/security-info

Universität Zürich

Meine Anmeldungen

Übersicht

a.)

Sicherheitsinformation...

Geräte

Kennwort

Organisationen

Einstellungen und Date...

Letzte Aktivität

Sicherheitsinformationen

Die folgenden Methoden werden zum Anmelden bei Ihrem Konto oder zum Zu

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator – Benachrichtigung Ändern

b.)

+ Anmeldemethode hinzufügen

Telefon

Kennwort

Microsoft Authenticator
Multi-Faktor-Authentifizierung (M

Microsoft Authenticator
Multi-Faktor-Authentifizierung (M

Haben Sie Ihr Gerät verloren? Überall abmelden

Universität Zürich UZH — Abmelden

Sini Zivkovic
sini.zivkovic@uzh.ch
Konto anzeigen
Organisation wechseln

Mit einem anderen Konto anmelden

Methode hinzufügen

Welche Methode möchten Sie hinzufügen?

c.)

Sicherheitsschlüssel

d.)

Abbrechen — Hinzufügen

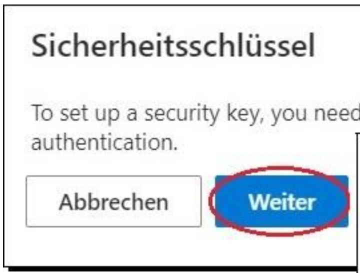
Step 1: Complete the following four steps to add the new *'Security key'* login method to your profile to the authentication process in your profile:

a.) Switch to *'Security information'* tab

b.) Click on *'Add login method'* button

c.) Select the *'Security key'* method

d.) Click on the *'Add'* button

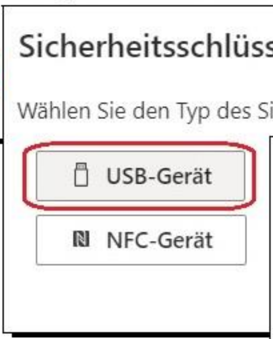


Sicherheitsschlüssel

To set up a security key, you need to sign in with two-factor authentication.

Abbrechen — Weiter

Step 2: Click on *'Next'* and confirm *'Login request'* using your previous login method.



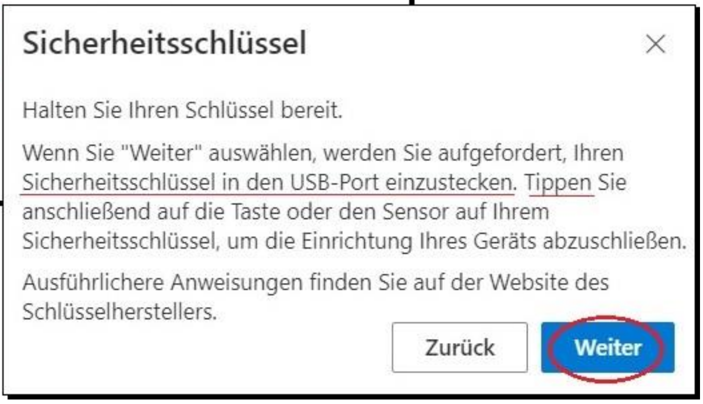
Sicherheitsschlüssel

Wählen Sie den Typ des Sicherheitsschlüssels, den Sie verwenden.

USB-Gerät

NFC-Gerät

Step 3: Select *'USB device'*.



Sicherheitsschlüssel

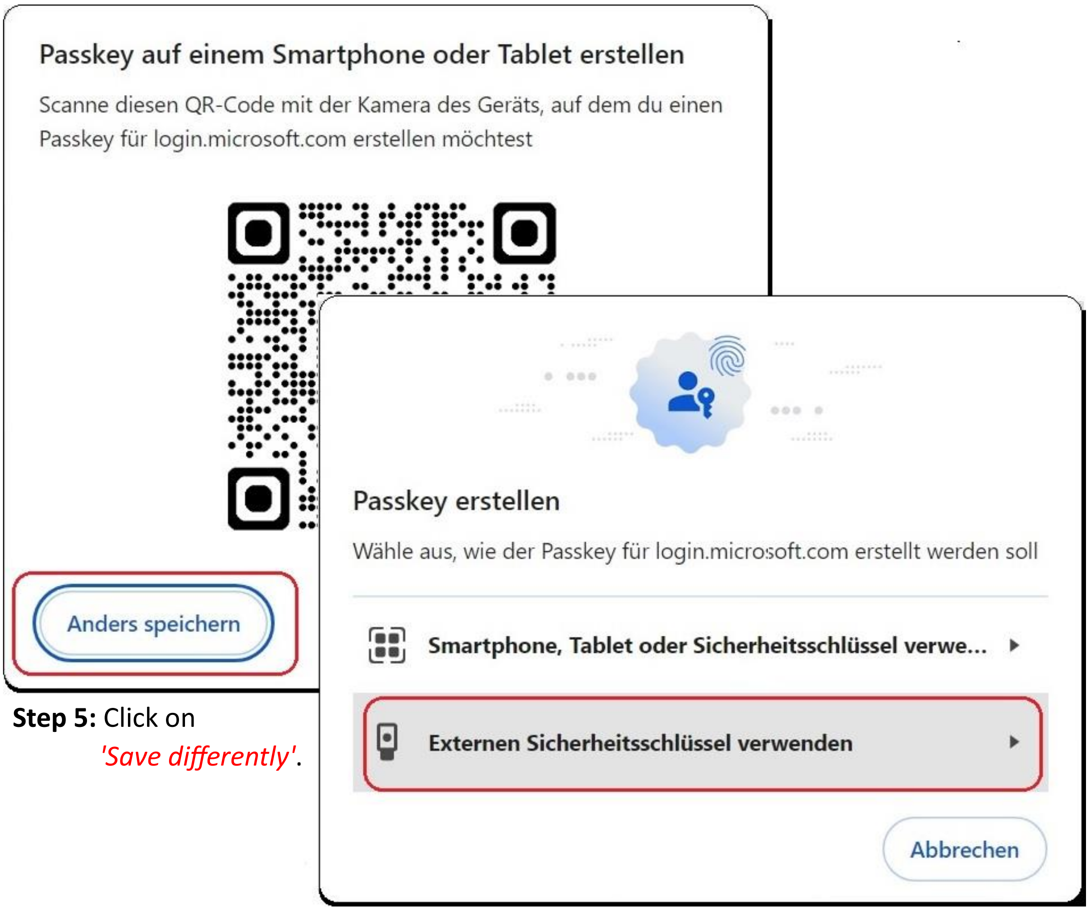
Halten Sie Ihren Schlüssel bereit.

Wenn Sie "Weiter" auswählen, werden Sie aufgefordert, Ihren Sicherheitsschlüssel in den USB-Port einzustecken. Tippen Sie anschließend auf die Taste oder den Sensor auf Ihrem Sicherheitsschlüssel, um die Einrichtung Ihres Geräts abzuschließen.

Ausführlichere Anweisungen finden Sie auf der Website des Schlüsselherstellers.

Zurück — Weiter

Step 4: Click on *'Next'*.



Passkey auf einem Smartphone oder Tablet erstellen

Scanne diesen QR-Code mit der Kamera des Geräts, auf dem du einen Passkey für login.microsoft.com erstellen möchtest

Passkey erstellen

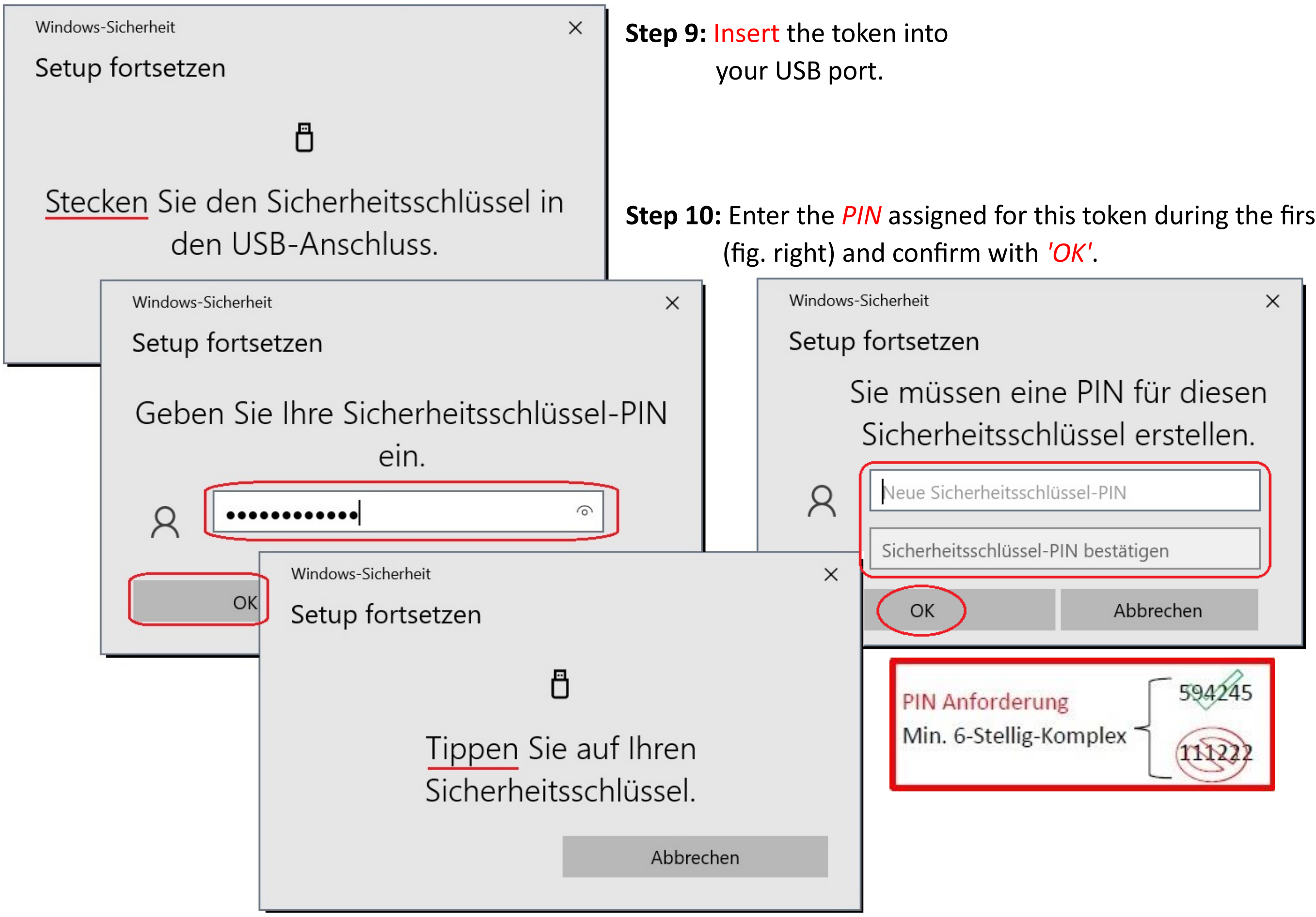
Wähle aus, wie der Passkey für login.microsoft.com erstellt werden soll

Smartphone, Tablet oder Sicherheitsschlüssel verwe...
Externen Sicherheitsschlüssel verwenden
Abbrechen

Step 5: Click on *'Save differently'*.

Step 6: Select *'Use external security key'*.

Steps 7 and 8: Click on *'OK'* in the *'Set up security key'* and *'Continue setup'* info dialog boxes (without illustration).



Windows-Sicherheit

Setup fortsetzen

Stecken Sie den Sicherheitsschlüssel in den USB-Anschluss.

Windows-Sicherheit

Setup fortsetzen

Geben Sie Ihre Sicherheitsschlüssel-PIN ein.

••••••••••••

Windows-Sicherheit

Setup fortsetzen

Tippen Sie auf Ihren Sicherheitsschlüssel.

Windows-Sicherheit

Setup fortsetzen

Sie müssen eine PIN für diesen Sicherheitsschlüssel erstellen.

Neue Sicherheitsschlüssel-PIN

Sicherheitsschlüssel-PIN bestätigen

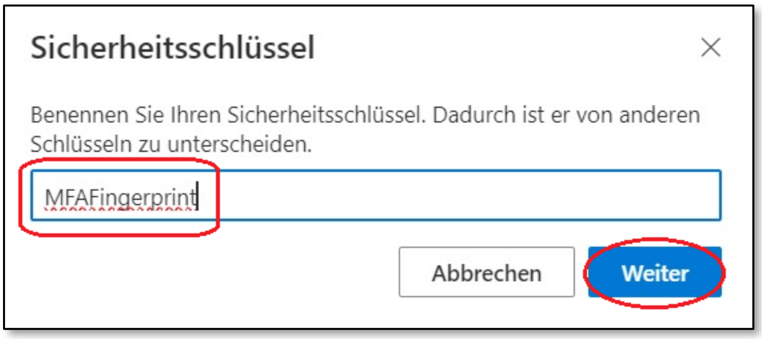
PIN Anforderung
Min. 6-Stellig-Komplex

594245 ✓
111222

Step 9: Insert the token into your USB port.

Step 10: Enter the *PIN* assigned for this token during the first use (fig. right) and confirm with *'OK'*.

Step 11: Tap on your token. (On the side of the password token, on the fingerprint sensor for the fingerprint token).

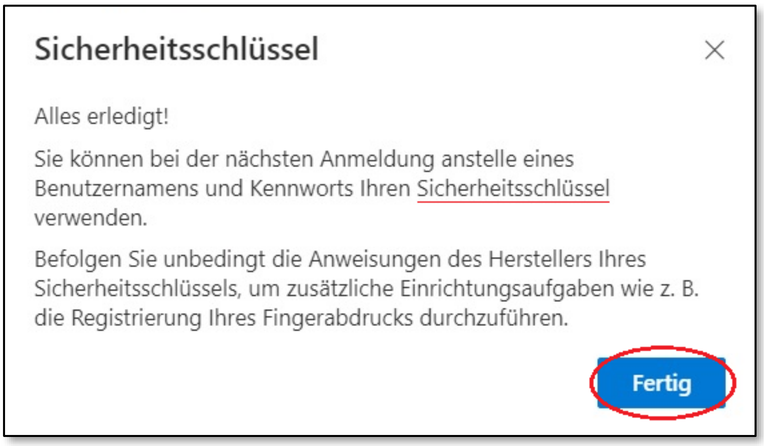


Sicherheitsschlüssel

Benennen Sie Ihren Sicherheitsschlüssel. Dadurch ist er von anderen Schlüsseln zu unterscheiden.

MFAFingerprint

Step 12: Assign a specific *name* to the login method of this token and click on *'Next'*.



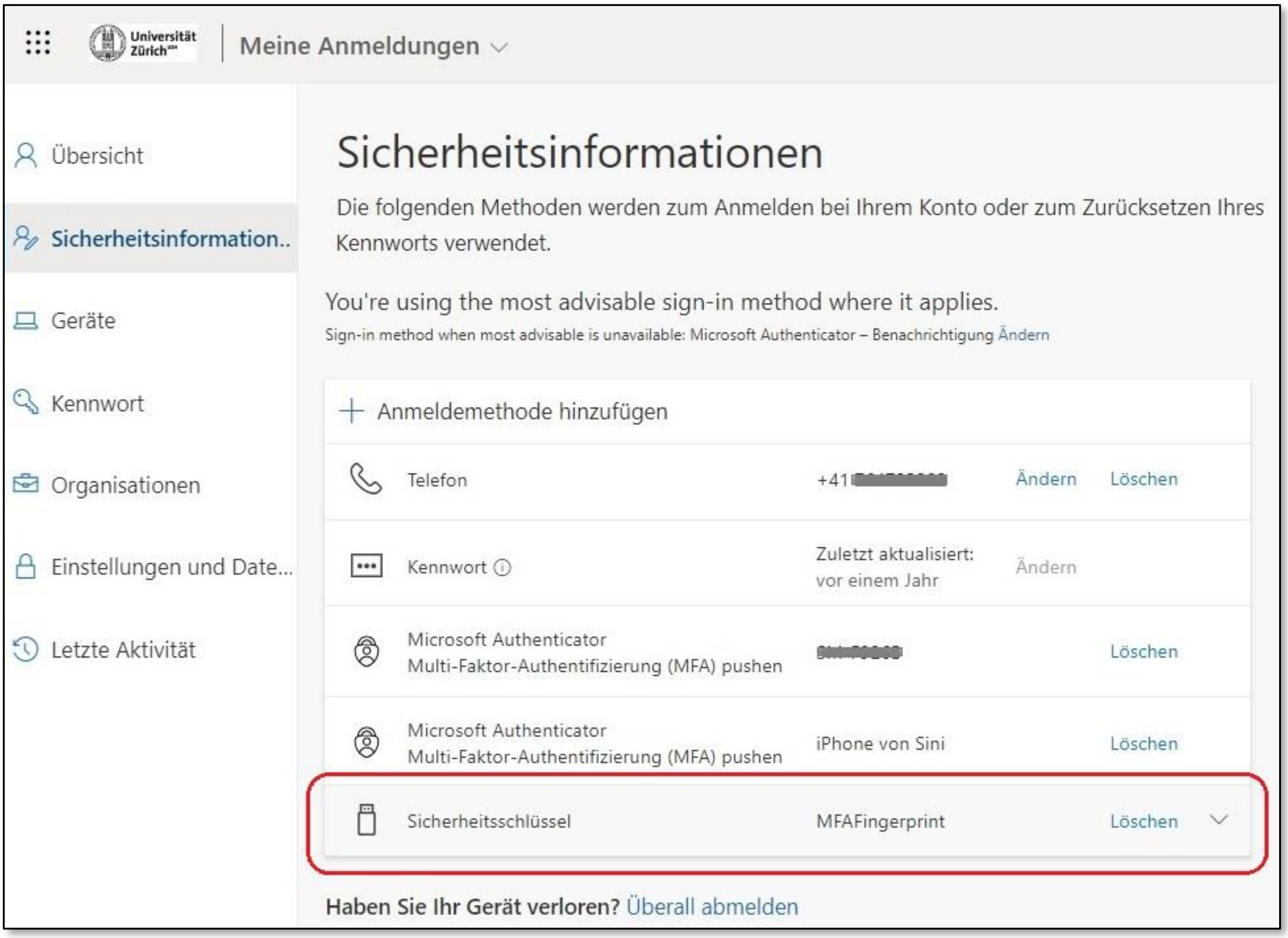
Sicherheitsschlüssel

Alles erledigt!

Sie können bei der nächsten Anmeldung anstelle eines Benutzernamens und Kennworts Ihren Sicherheitsschlüssel verwenden.

Befolgen Sie unbedingt die Anweisungen des Herstellers Ihres Sicherheitsschlüssels, um zusätzliche Einrichtungsaufgaben wie z. B. die Registrierung Ihres Fingerabdrucks durchzuführen.

Step 13: Click on *'Done'*



Sicherheitsinformationen

Die folgenden Methoden werden zum Anmelden bei Ihrem Konto oder zum Zurücksetzen Ihres Kennworts verwendet.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator – Benachrichtigung Ändern

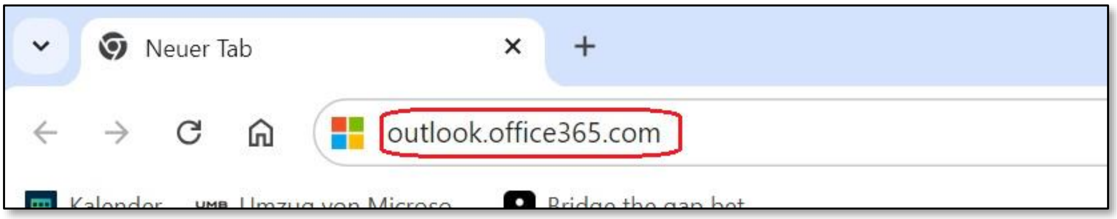
+ Anmeldemethode hinzufügen

Telefon	+41[redacted]	Ändern	Löschen
Kennwort ⓘ	Zuletzt aktualisiert: vor einem Jahr	Ändern	
Microsoft Authenticator Multi-Faktor-Authentifizierung (MFA) pushen	[redacted]		Löschen
Microsoft Authenticator Multi-Faktor-Authentifizierung (MFA) pushen	iPhone von Sini		Löschen
Sicherheitsschlüssel	MFAFingerprint		Löschen

Haben Sie Ihr Gerät verloren? Überall abmelden

Fig 3: The new login method *'Security key'* now appears in the overview of login methods.

Login via Token

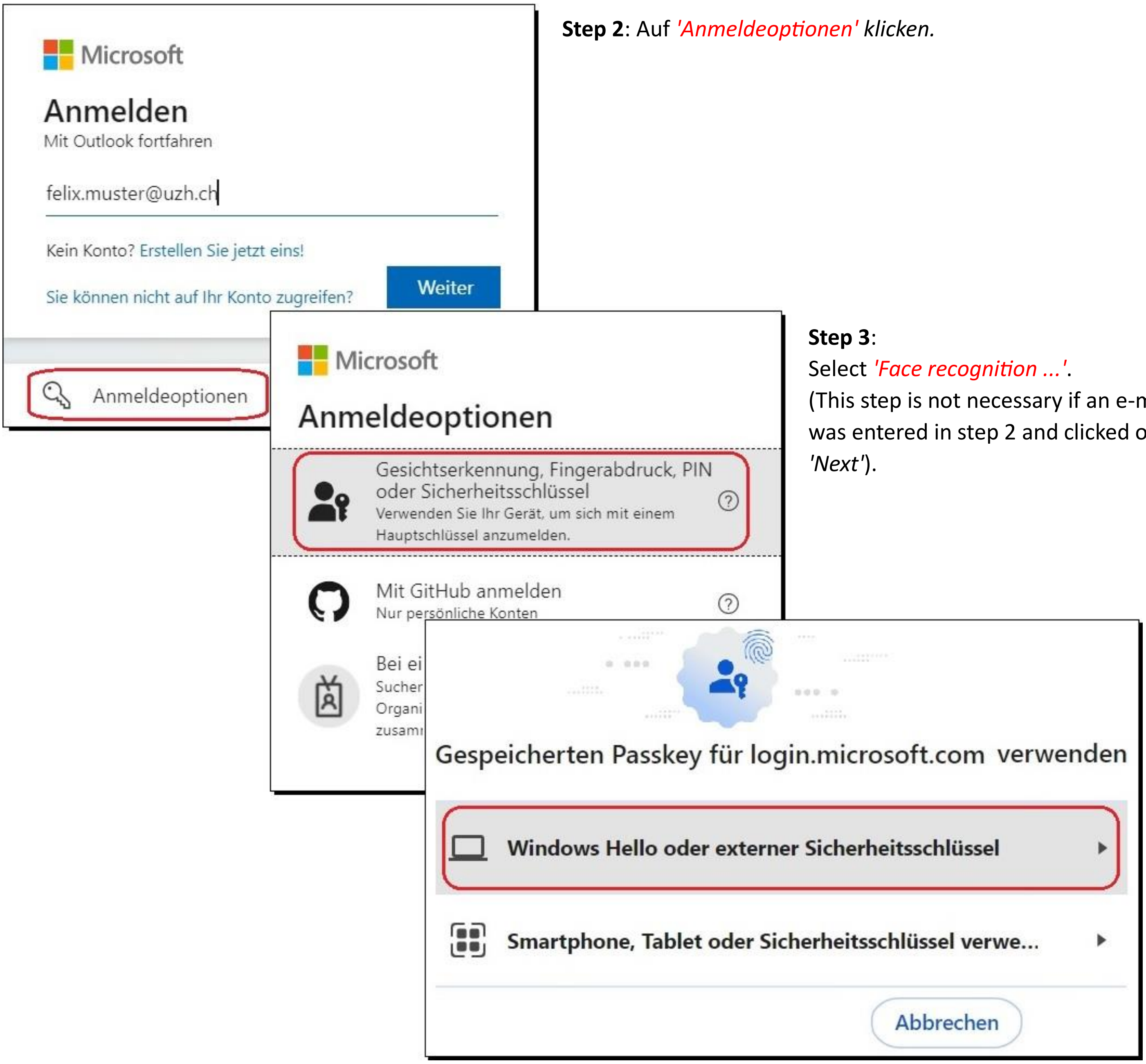


Neuer Tab

outlook.office365.com

Kalender Umzug von Microso Bridge the gap bot

Step 1: Open the MS365 portal *(portal.office.com)* or your mailbox *(outlook.office365.com)* in the browser.



Microsoft

Anmelden

Mit Outlook fortfahren

felix.muster@uzh.ch

Kein Konto? Erstellen Sie jetzt eins!

Sie können nicht auf Ihr Konto zugreifen?

Weiter

Anmeldeoptionen

Microsoft

Anmeldeoptionen

Gesichtserkennung, Fingerabdruck, PIN oder Sicherheitsschlüssel
Verwenden Sie Ihr Gerät, um sich mit einem Hauptschlüssel anzumelden.

Mit GitHub anmelden
Nur persönliche Konten

Bei ei
Sucher
Organi
zusami

Gespeicherten Passkey für login.microsoft.com verwenden

Windows Hello oder externer Sicherheitsschlüssel

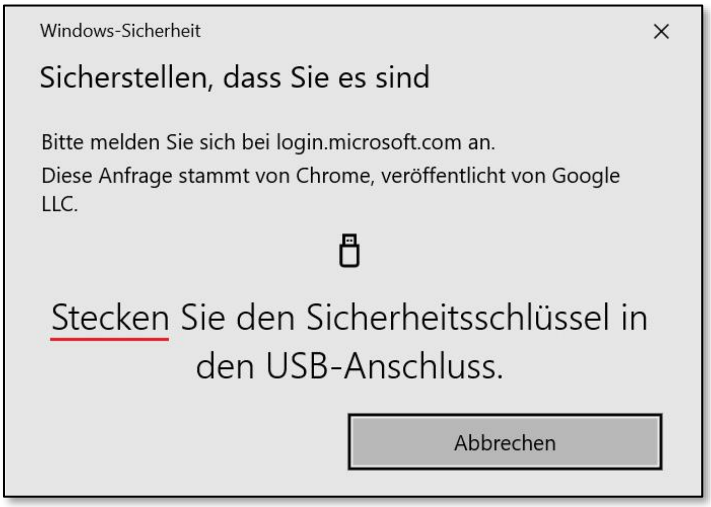
Smartphone, Tablet oder Sicherheitsschlüssel verwe...

Abbrechen

Step 2: Auf *'Anmeldeoptionen' klicken.*

Step 3:
Select *'Face recognition ...'*.
(This step is not necessary if an e-mail was entered in step 2 and clicked on *'Next'*).

Step 4: Select *'Win Hello or external security key'*.



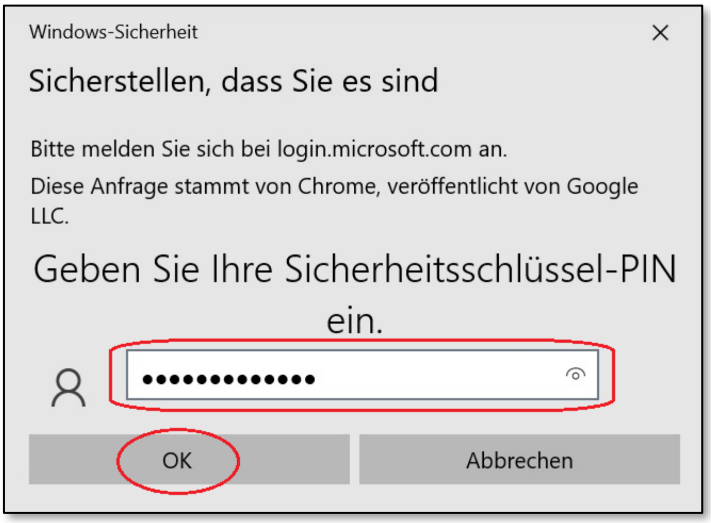
Windows-Sicherheit

Sicherstellen, dass Sie es sind

Bitte melden Sie sich bei login.microsoft.com an.
Diese Anfrage stammt von Chrome, veröffentlicht von Google LLC.

Stecken Sie den Sicherheitsschlüssel in den USB-Anschluss.

Step 5: *Insert* the USB stick into the USB port, if not already done.



Windows-Sicherheit

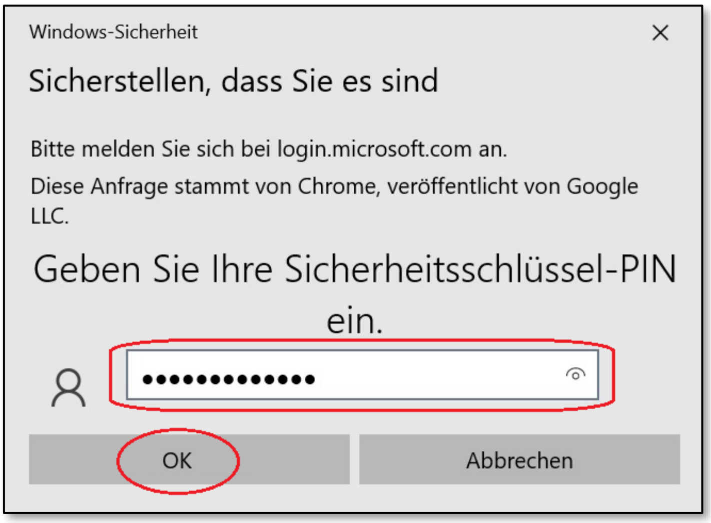
Sicherstellen, dass Sie es sind

Bitte melden Sie sich bei login.microsoft.com an.
Diese Anfrage stammt von Chrome, veröffentlicht von Google LLC.

Geben Sie Ihre Sicherheitsschlüssel-PIN ein.

•••••••••••••

Step 6: Enter the *PIN* defined for this stick and click on *'OK'*.



Windows-Sicherheit

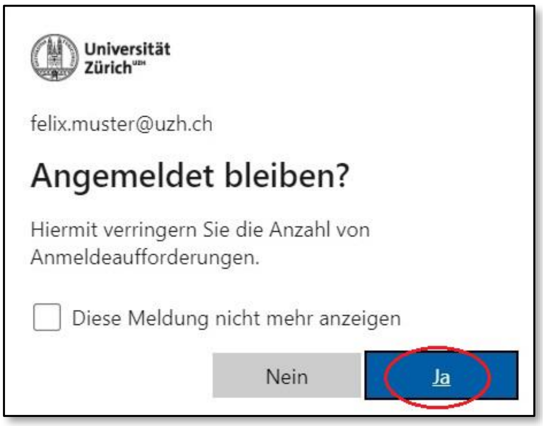
Sicherstellen, dass Sie es sind

Bitte melden Sie sich bei login.microsoft.com an.
Diese Anfrage stammt von Chrome, veröffentlicht von Google LLC.

Geben Sie Ihre Sicherheitsschlüssel-PIN ein.

••••••••••••••

Step 7: *Tap* on the USB stick.
For the password stick on the side,
for the fingerprint stick on top of the sensor.



felix.muster@uzh.ch

Angemeldet bleiben?

Hiermit verringern Sie die Anzahl von Anmeldeaufforderungen.

☐ Diese Meldung nicht mehr anzeigen

Step 8: Click on *'Yes'*.