

Wie funktioniert die Multifaktorauthentifizierung via Hardware-Token (FIDO 2) an der UZH?

Ein *Token* ist ein digitales (Software-Token) oder physisches Objekt (Hardware-Token), das regelmäßig wechselnde Codes zur Benutzerauthentifizierung generiert. Im Gegensatz zum Software-Token, muss beim Hardware-Token der Benutzer keine Codes von Hand eingeben. Die Codeüberprüfung findet automatisch statt.

Der Standard um den es sich handelt ist: [FIDO 2 \(Fast Identity Online 2\)](#)

Hardware-Empfehlung der Zentralen Informatik der Universität Zürich:

Die Zentrale Informatik der UZH empfiehlt die Nutzung des Modells: [Token 2 Pin+ Serie \(Link\)](#).

Die ZI behält sich vor, Sicherheitstoken, die nicht den Anforderungen genügen, in Zukunft zu sperren.

Hinweis:

Um Komplikationen zu vermeiden, sollte die initiale Konfiguration des Hardware-Tokens im folgenden Browser vorgenommen werden: [Microsoft Edge](#).

NFC (Near Field Communication):

Die erwähnten Token verfügen über ein NFC-Interface, das auch die Anmeldung über ein NFC-fähiges Mobiltelefon ermöglicht.

Bei der Anmeldung gibt der Benutzer seinen Benutzernamen und sein Passwort ein. Danach wird der vom Hardware-Token generierte Code abgefragt. Bei einigen Hardware-Tokens muss der Benutzer dazu vorgängig einen selbstdefinierten *PIN (Persönliche Identifikationsnummer)* setzen oder eingeben, um das Gerät zu aktivieren, resp. benutzen zu können. Er dient als zusätzliche Schutzschicht. Selbst wenn jemand physischen Zugriff auf den Hardware-Token erlangt, kann er ihn nicht verwenden, ohne den PIN zu kennen.



Abb 1: Hardware-Token in Form von USB-Sticks: Fingerprint-Token (links) und Passwort-Token (rechts).

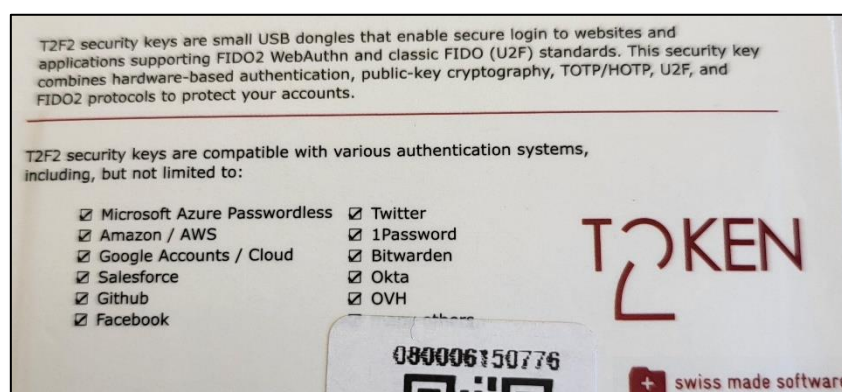
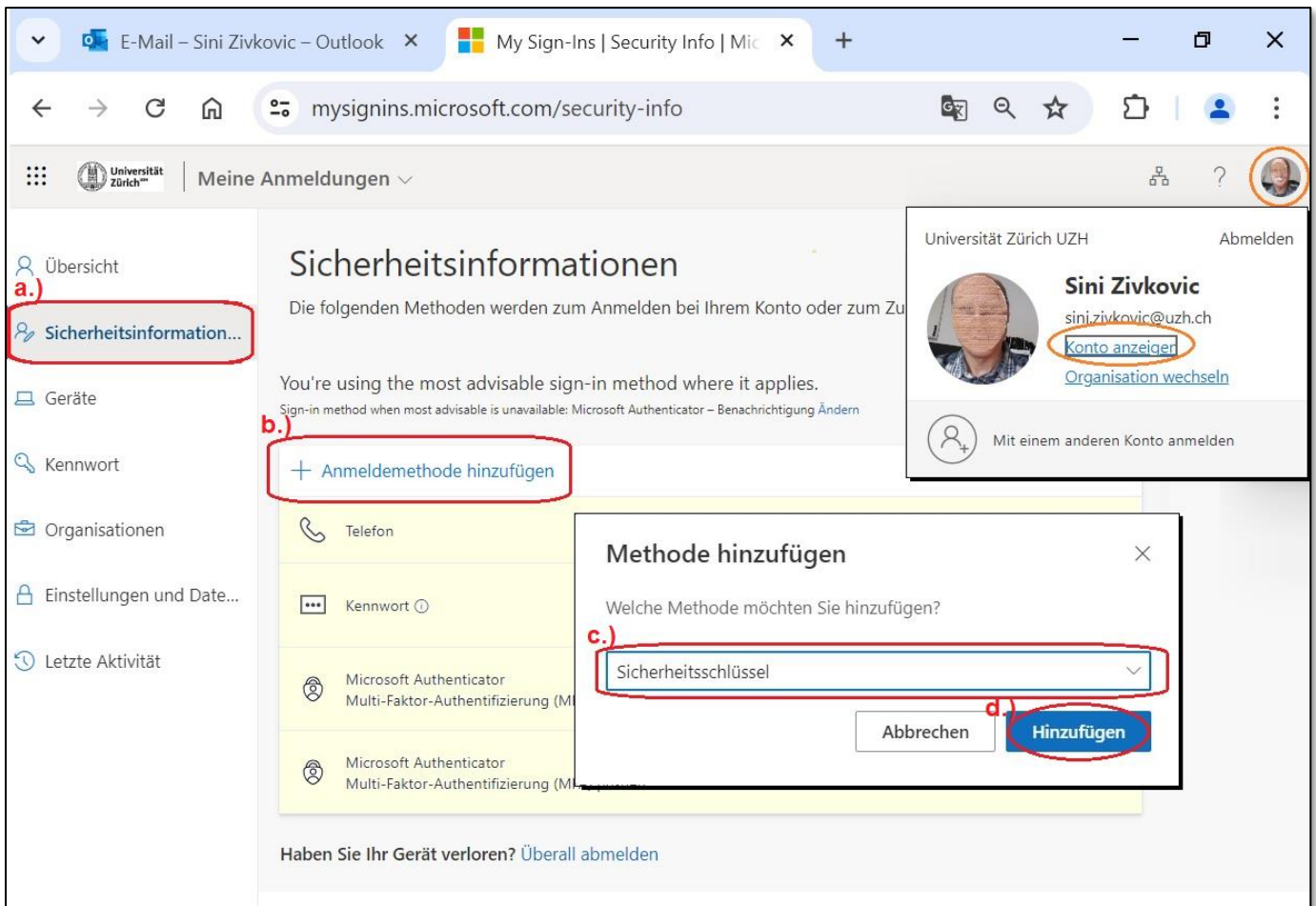


Abb 2: Kompatibilität mit verschiedenen anderen Authentifizierungssystemen.

Setup des Tokens

Loggen Sie sich in Ihr MS365-Profilkonto ein, sei es *direkt* durch Aufruf der URL mysignins.microsoft.com oder *indirekt* via Ihrer Visitenkarte aus Ihrer MS365-Anwendung (Klick auf Ihr *Profilbild* > 'Konto anzeigen').

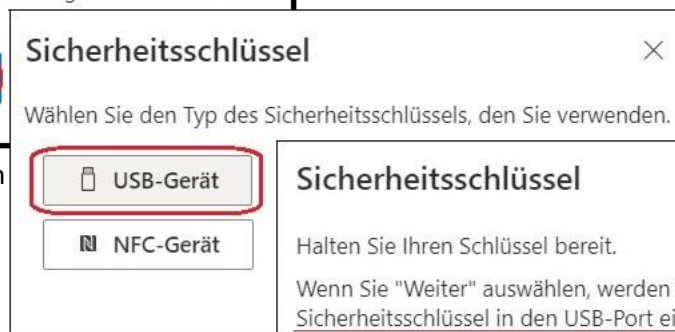


Schritt 1: Führen Sie folgende vier Punkte aus, um in Ihrem Profil die neue Anmeldeverfahren *'Sicherheitsschlüssel'* dem Authentifizierungsprozess hinzuzufügen:

- a.) Zu Register *'Sicherheitsinformationen'* wechseln
- b.) Klick auf Button *'Anmeldeverfahren hinzufügen'*
- c.) Methode *'Sicherheitsschlüssel'* auswählen
- d.) Klick auf Button *'Hinzufügen'*



Schritt 2: Auf *'Weiter'* klicken und *'Anmeldeaufforderung'* mittels Ihrer bisherigen Anmeldeverfahren bestätigen.



Schritt 3: *'USB-Gerät'* auswählen.



Schritt 4: Auf *'Weiter'* klicken.

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



Anders speichern

Schritt 5: Klicken Sie auf *'Anders speichern'*.

Passkey erstellen

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

Smartphone, Tablet oder Sicherheitsschlüssel verwe...

Externen Sicherheitsschlüssel verwenden

Abbrechen

Schritt 6: Wählen Sie *'Externen Sicherheitsschlüssel verwenden'* aus.

Schritte 7 und 8: Klicken Sie auf *'OK'* bei den Info-Dialogboxen *'Sicherheitsschlüssel einrichten'* und *'Setup fortsetzen'* (ohne Abbildung).

Windows-Sicherheit

Setup fortsetzen



Stecken Sie den Sicherheitsschlüssel in den USB-Anschluss.

Schritt 9: **Stecken** Sie das Token in Ihren USB-Anschluss.

Schritt 10: Geben Sie den für dieses Token bei der Erstbenützung (Abb. rechts) vergebenen **PIN** ein und bestätigen mit **'OK'**.

Windows-Sicherheit

Setup fortsetzen

Geben Sie Ihre Sicherheitsschlüssel-PIN ein.



.....

OK

Windows-Sicherheit

Setup fortsetzen

Sie müssen eine PIN für diesen Sicherheitsschlüssel erstellen.



Neue Sicherheitsschlüssel-PIN

Sicherheitsschlüssel-PIN bestätigen

OK

Abbrechen

Windows-Sicherheit

Setup fortsetzen



Tippen Sie auf Ihren Sicherheitsschlüssel.

Abbrechen

PIN Anforderung

Min. 6-Stellig-Komplex

594245

111222

Schritt 11: **Tippen** Sie auf Ihr Token. (Beim Passwort-Token seitlich, beim Fingerprint-Token auf den Fingerprint-Sensor.)

Sicherheitsschlüssel ✕

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

MFAFingerprint

Abbrechen **Weiter**

Schritt 12: Vergeben Sie der Anmeldemethode dieses Tokens einen spezifischen *Namen* und klicken auf *'Weiter'*.

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.

Fertig

Schritt 13: Klicken Sie auf *'Fertig'*.

Universität Zürich | Meine Anmeldungen ▾

Übersicht

Sicherheitsinformation..

Geräte

Kennwort

Organisationen

Einstellungen und Date...

Letzte Aktivität

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

Abb 3: Die neue Anmeldemethode *'Sicherheitsschlüssel'* erscheint neu in der Übersicht der Anmeldemethoden.

Anmeldung via Token



Schritt 1: Rufen Sie im Browser das MS365-Portal (*portal.office.com*) oder Ihre Mailbox (*outlook.office365.com*) auf.



Schritt 2: Auf '*Anmeldeoptionen*' klicken.

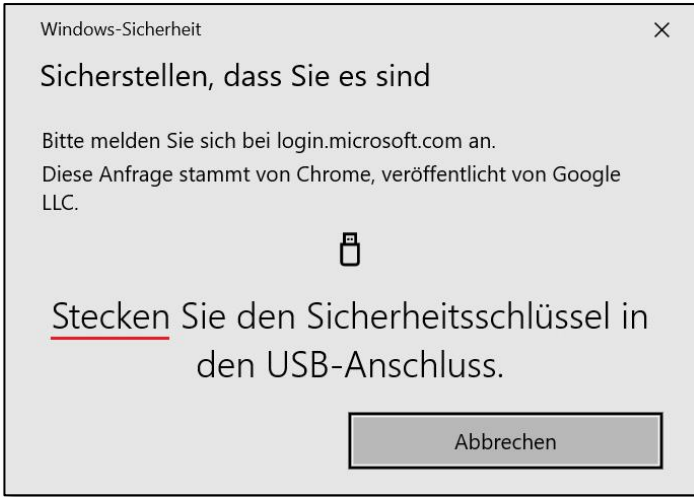


Schritt 3:

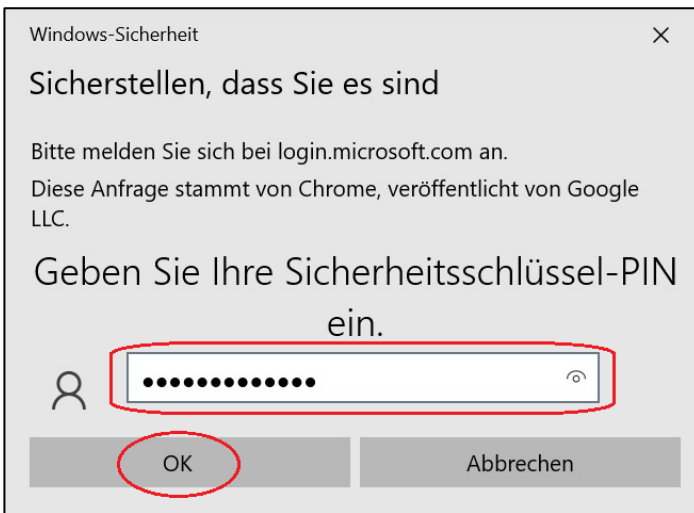
Wählen Sie '*Gesichtserkennung ...*'. (Dieser Schritt entfällt, falls in Schritt 2 eine *E-Mail* eingegeben und auf '*Weiter*' geklickt wurde.)



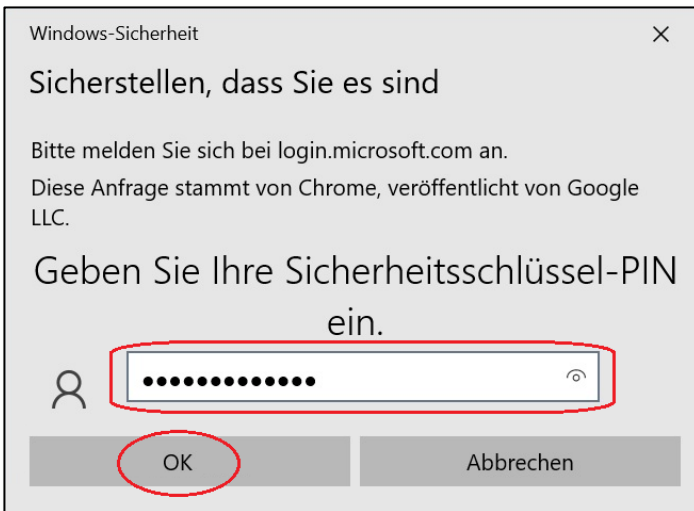
Schritt 4: Wählen Sie '*Win Hello oder externen Sicherheitsschlüssel*' aus.



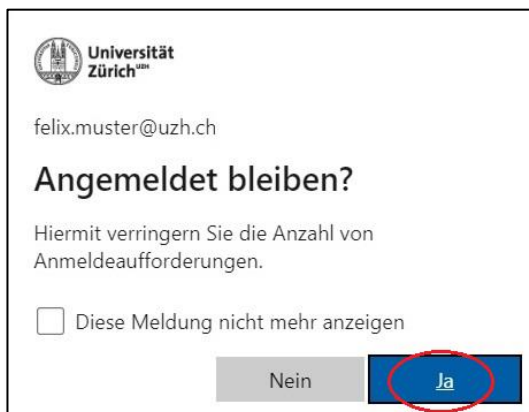
Schritt 5: *Stecken* Sie den USB-Stick in den USB-Anschluss, falls nicht schon geschehen.



Schritt 6: Geben Sie den für diesen Stick definierten *PIN* ein und klicken auf '*OK*'.



Schritt 7: *Tippen* Sie auf den USB-Stick. (Beim Passwort-Stick setilich, beim Fingerprint-Stick oben auf den Fingerabdrucksensor.)



Schritt 8: Klicken Sie auf '*Ja*'.