

Bitte beachten Sie, dass die englische Version dieses Dokuments maschinell übersetzt und nicht auf Fehler überprüft wurde. Die englische Version dient daher der besseren Zugänglichkeit für Personen mit eingeschränkten Deutschkenntnissen, im Zweifelsfall ist jedoch der Inhalt der deutschen Version verbindlich.

Hinzufügen eines Passkeys / Hauptschlüssels

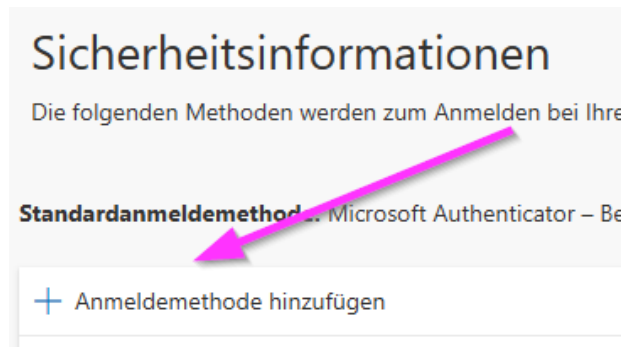
Diese Kurzanleitung beschreibt Schritt für Schritt, wie Sie Ihrem MFA-Profil einen Passkey bzw. Hauptschlüssel hinzufügen können. Die umfangreichere Anleitung für alle Methoden finden Sie unter: https://service.it.tuwien.ac.at/swsupport/docus/windowshello/mfa_handbuch.pdf

Ein **Passkey**, der auch als Hauptschlüssel bezeichnet wird, bietet einen besseren Schutz als beispielsweise SMS und ermöglicht eine sichere, passwortlose Anmeldung. Diese kann mit verschiedenen Endgeräten genutzt werden, etwa mit Smartphone, PC, Hardware-Sicherheitsschlüssel oder Passwortmanagern wie KeepassXC oder 1Password. Je nach Anbieter können Passkeys zudem sicher zwischen mehreren Geräten synchronisiert werden.

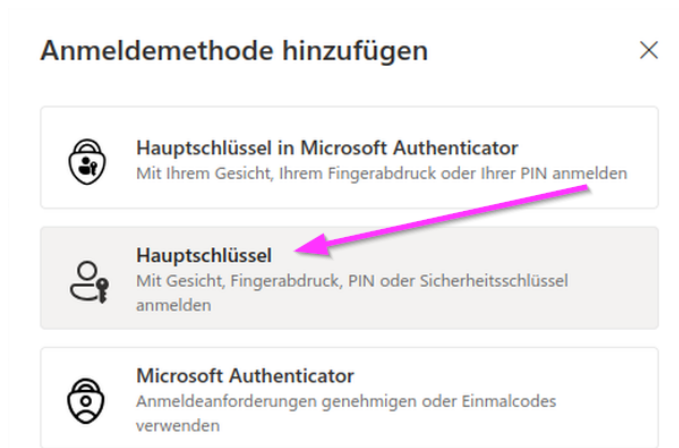
Ein Passkey steht Ihnen unter Windows, Android, Apple und Linux zur Verfügung. Auch eine Nutzung über Browser wie Chrome, Firefox oder Safari ist möglich. Da es sich hierbei jedoch um Produkte von Drittanbietern handelt, kann dafür kein Support angeboten werden.

1 Einrichtung von Passkey in Ihrem Account

- Schritt 1: Öffnen Sie <https://mysignins.microsoft.com/security-info>
- Schritt 2: Melden Sie sich mit Ihrem Benutzernamen und Ihrem Passwort an.
- Schritt 3: Wählen Sie „**Anmeldemethode hinzufügen**“



- Schritt 4: Wählen Sie als Methode „**Hauptschlüssel**“ aus.



- Schritt 5: Bestätigen Sie das Pop-Up mit „**Weiter**“.

Sign in faster with your face, fingerprint, or PIN ×



Erstellen Sie einen Hauptschlüssel, um sich bei Ihrem Konto anzumelden. Es sind keine Apps, Kennwörter oder Codes erforderlich.

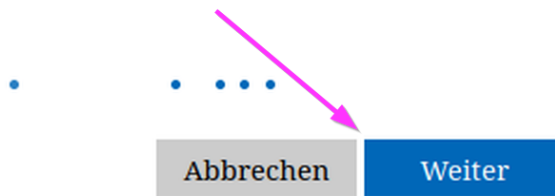
Zurück

Weiter

- Schritt 6: Die Einrichtung wird nun in einem separaten Fenster fortgesetzt. Bitte schließen Sie die Schritte in diesem Fenster ab, sollte der Prozess dann **nicht** automatisiert weiter gehen, bestätigen Sie dies mit „**Weiter**“.

Ihr Hauptschlüssel wird eingerichtet...

Ihr Gerät öffnet ein Sicherheitsfenster. Befolgen Sie die Anweisungen, um die Einrichtung Ihres Hauptschlüssels abzuschließen.



- Schritt 7: Es öffnet sich nun ein Pop-Up, bei dem eine Methode vorgeschlagen wird. Klicken Sie hier nun auf „**Anders speichern**“, um alle Optionen angezeigt zu bekommen.

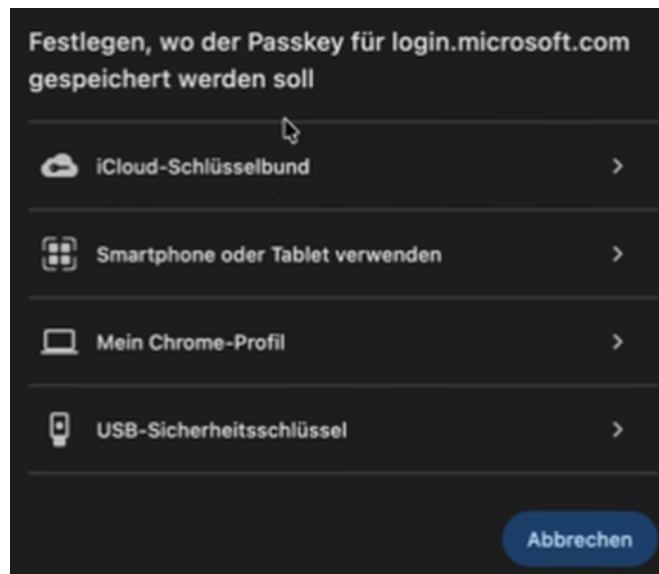
Einen Passkey zur Anmeldung in login.microsoft.com erstellen?

Du kannst diesen Passkey verwenden, um dich auf deinen Geräten schneller anzumelden. Er wird im Google Passwortmanager für gespeichert.



- Schritt 8: Legen Sie nun fest, wo der Passkey gespeichert werden soll. Je nach Gerät stehen hierfür zahlreiche Optionen zur Verfügung (z. B. Windows Hello, KeePass, USB-Sicherheitsschlüssel, Smartphone, Tablet, Google Key Vault, iCloud, Chrome, KeepassXC, 1Password etc.). Die

Abbildung ist an dieser Stelle nur beispielhaft. Bitte bedenken Sie bei der Nutzung der verschiedenen Optionen Datenschutz- und Sicherheitsfragen.



- Schritt 9: Geben Sie abschließend Ihrem Hauptschlüssel noch einen Namen, damit Sie ihn in der Liste leichter finden können, und bestätigen Sie mit „**Weiter**“.

Ihren Hauptschlüssel benennen



Geben Sie Ihrem Hauptschlüssel einen Namen, damit Sie ihn später leichter identifizieren können.

Weiter

- Schritt 10: Der Hauptschlüssel ist nun erstellt und kann zukünftig für alle MFA-Logins verwendet werden.

✓ Hauptschlüssel erstellt

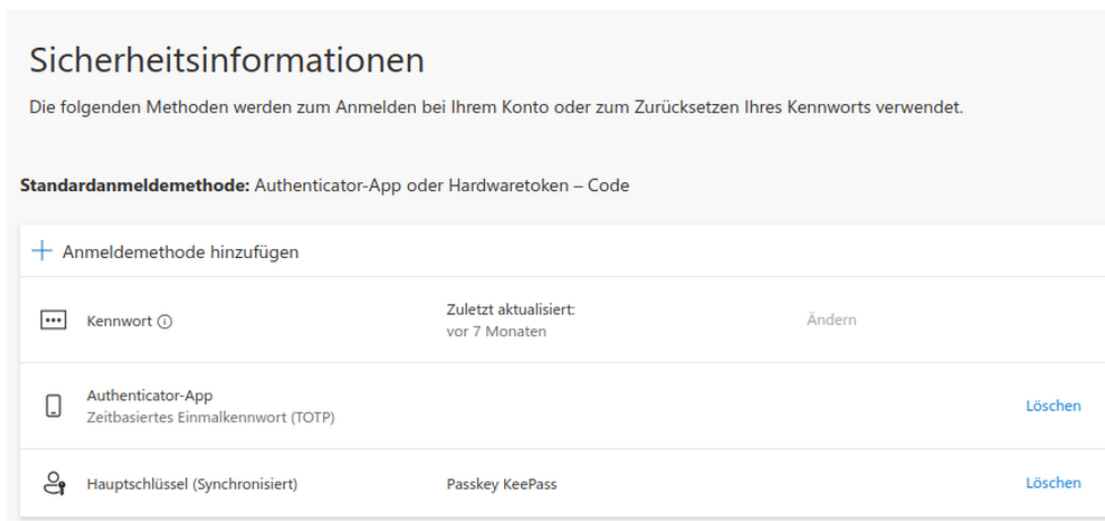


Sie können sich jetzt mit Ihrem Gesicht, Fingerabdruck oder Ihrer PIN bei Ihrem Konto anmelden.

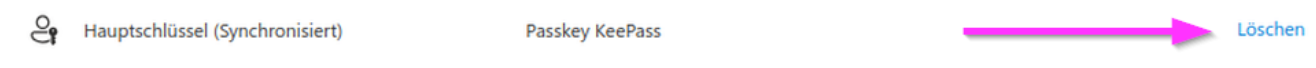
Fertig

2 Übersicht und Löschung:

- Um die bereits bestehenden MFA-Methoden (und Passkeys) zu sehen, gehen Sie auf <https://my-signins.microsoft.com/security-info>



- Um einen bereits angelegten Passkey wieder zu löschen, wählen Sie dafür dann einfach rechts den Button „Delete“ oder „Löschen“.



3 Fehlerbehebung:

3.1 Kein Zugriff auf die hinterlegte MFA-Methode

Wenn Sie keinen Zugriff mehr auf Ihr registriertes Gerät oder Ihre Methode haben:

- Verwenden Sie eine **alternative hinterlegte MFA-Methode** (z. B. Backup-Code oder zweite App).
- Falls keine alternative Methode verfügbar ist, wenden Sie sich an den **IT-Support**, um den Zugriff zurücksetzen zu lassen.

3.2 MFA schlägt aus unbekannten Gründen fehl

Sollten Sie keine klare Fehlermeldung erhalten, die Nutzung von MFA jedoch dennoch vorschlagen, bitten wir Sie, vor Erstellung eines Tickets die folgende URL aufzurufen:

- https://shop.tusoftware.tuwien.ac.at:8888/get_mfa_report

Sie erhalten an dieser Stelle nun eine Anzeige für mögliche Ursachen, die die Nutzung der gewünschten MFA-Methode einschränken könnte.

4 Support und Kontakt

Sollten es bei der Einrichtung oder Nutzung von Passkeys zu Einschränkungen kommen, wenden Sie sich über das Ticketsystem (nur Mitarbeitende) via <https://support.tuwien.ac.at/assystnet/> oder via E-Mail an help@it.tuwien.ac.at an den IT-Support und fügen Sie bitte bei Einschränkungen beim Anlegen des Passkeys einen Screenshot des oben genannten MFA-Reports mit bei. Sie können sich selbstverständlich auch telefonisch an das Service-Center wenden.