Einleitung

Was sind Passkeys? Passkeys sind eine moderne, sichere Alternative zu herkömmlichen Passwörtern. Sie verwenden kryptografische Schlüssel, um Benutzer zu authentifizieren, ohne dass ein Benutzername oder ein Kennwort erforderlich ist. Passkeys bieten eine stärkere Verifizierung, da sie sicher auf Ihrem Gerät gespeichert werden und eine biometrische Authentifizierung (z. B. Fingerabdruck oder Gesichtserkennung) oder eine Geräte-PIN erfordern, was sie sicherer macht als herkömmliche Benutzernamen und Passwörter.

Befolgen Sie diese Anweisungen, um Ihren Hauptschlüssel in Microsoft Authenticator als kennwortlose Anmeldemethode einzurichten, sich mit einem Hauptschlüssel anzumelden oder einen Hauptschlüssel zu löschen.

Zum Abschnitt springen (Strg + Klick verwenden):

Vergewissern Sie sich, dass Ihr Mobilgerät für Passkeys bereit ist

Um einen Hauptschlüssel auf Ihrem Mobilgerät zu registrieren, muss Ihr Mobilgerät über Folgendes verfügen:

- iOS Version 17 oder Android Version 14 oder höher
- Microsoft Authenticator-App für Passkeys installiert und aktiviert

1. Überprüfen Sie Ihre iOS- oder Android-Version

   - **Für IOS-Geräte:** Öffnen Sie auf Ihrem Gerät die **App "Einstellungen**", tippen Sie auf **"Allgemein**" und dann auf **"Info"**

   - **Für Android-Geräte:** Öffnen Sie auf Ihrem Gerät die **App "Einstellungen**", tippen Sie auf **"Über das Smartphone"**

2. Überprüfen, ob Microsoft Authenticator installiert ist

   FÜR LILLY iOS-GERÄTE: Microsoft Authenticator sollte auf Ihrem Lilly iOS-Gerät installiert sein. Wenn nicht, stellen Sie sicher, dass Sie die Anleitung Mobility@Lilly: Einrichten und Registrieren Ihres Lilly iPhone/iPad, einschließlich des Microsoft iOS-Registrierungsverfahrens, abgeschlossen haben.

   FÜR PRIVATE MOBILGERÄTE: Laden Sie die Microsoft Authenticator-Anwendung aus dem Apple App Store (iPhone/iPad) oder Google Play Store (Android) herunter. Stellen Sie sicher, dass die Microsoft Authenticator-App auf Ihrem Mobilgerät über den entsprechenden App Store auf dem

neuesten Stand ist.

3. Aktivieren Sie Authenticator als Passkey-Anbieter in den **Einstellungen** Ihres Mobilgeräts:

Für iOS-Geräte:

- Öffnen Sie auf Ihrem iOS-Gerät **die Einstellungen**.
- Öffnen Sie **Allgemein** und wählen Sie **Automatisches Ausfüllen & Passwörter**
- Aktivieren Sie unter **Automatisches Ausfüllen von Authenticator**

Für Android-Geräte:

Hinweis: Der genaue Wortlaut der Einstellungen und des Bildschirmlayouts kann je nach Betriebssystemversion und Anpassungen des Geräts variieren.

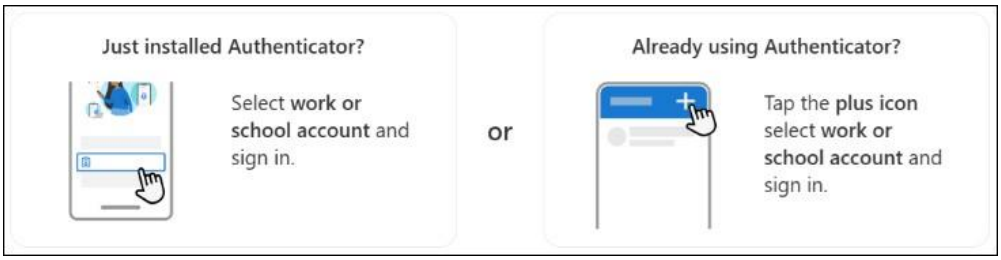
- Öffnen Sie auf Ihrem Android-Gerät **die Einstellungen**.
- Öffnen Sie **Passwörter & Konten**.

- Unter **Zusätzliche Anbieter** aktivieren **Authenticator**.

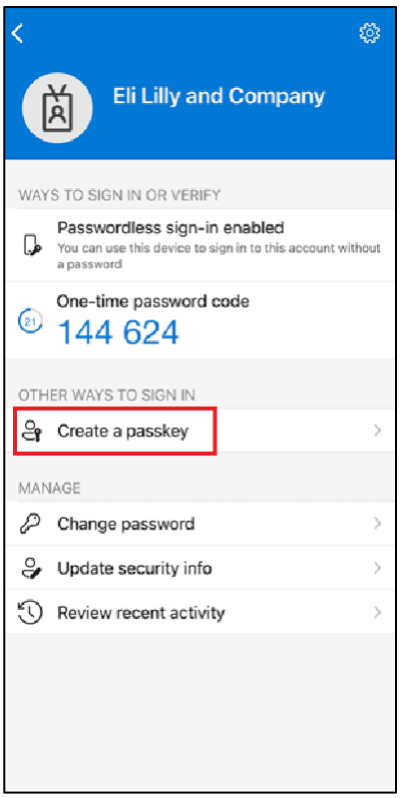
Registrieren Sie den Passkey auf einem Lilly Mobilgerät

Befolgen Sie diese Anweisungen, um einen Hauptschlüssel in Microsoft Authenticator auf einem von Lilly bereitgestellten Mobilgerät einzurichten. Wenn Sie ein Gerät verwenden, das nicht von Lilly stammt, verwenden Sie die Funktion "Passkey registrieren" auf einem Mobilgerät, das nicht von Lilly stammt , um Ihre Registrierung abzuschließen.

1. Öffnen Sie Microsoft Authenticator auf Ihrem Mobilgerät
2. Wählen Sie in Microsoft Authenticator **Ihr Lilly-Konto aus**. Wenn Sie Ihr Lilly-Konto nicht sehen, führen Sie die folgenden Schritte aus.



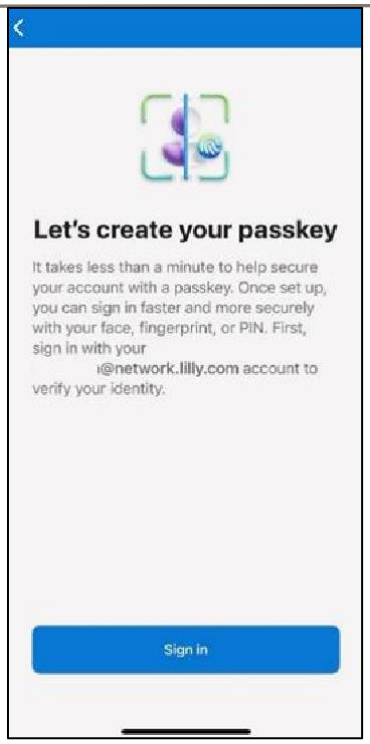
3. Klopfen **Erstellen eines Hauptschlüssels** oder tippen Sie auf Einstellungen ⚙ und wählen Sie **Erstellen eines Hauptschlüssels**

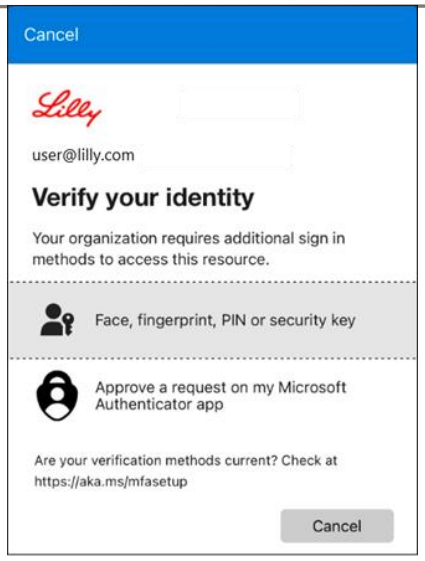


4. Wählen Sie auf dem **Bildschirm Erstellen Sie Ihren** Hauptschlüssel die Option Anmelden aus, um die mehrstufige Authentifizierung (MFA) abzuschließen.

   Wählen Sie auf dem **Bildschirm "Identität bestätigen**" eine der verfügbaren Authentifizierungsmethoden aus.

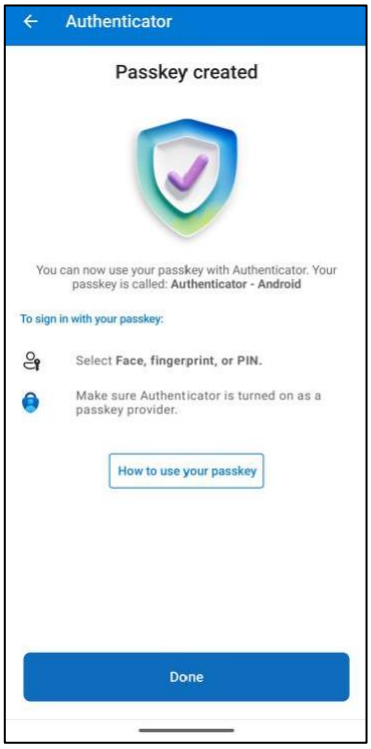
   Wenn der Bildschirm **"Etwas ist schief gelaufen**" angezeigt wird, wählen Sie **Andere Anmeldemöglichkeiten** und dann eine Ihrer verfügbaren Authentifizierungsmethoden aus.



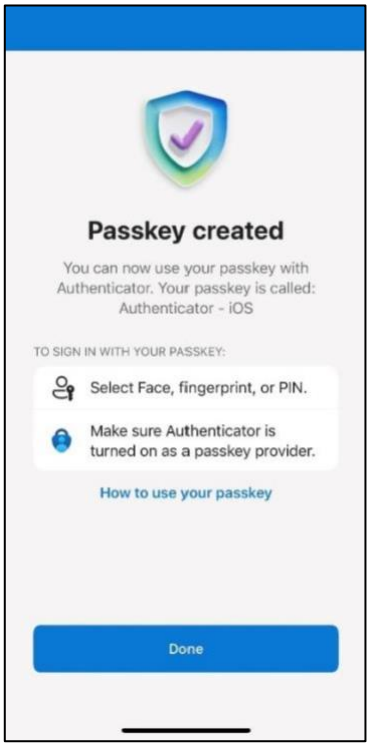


5. Ihr Hauptschlüssel wurde erfolgreich als Anmeldemethode für Ihr Konto hinzugefügt. Wählen Sie **Fertig** aus.

Für Android-Mobilgeräte:



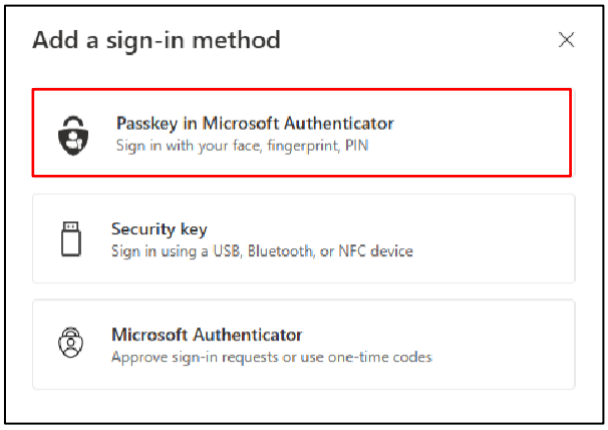
Für iOS-Mobilgeräte:



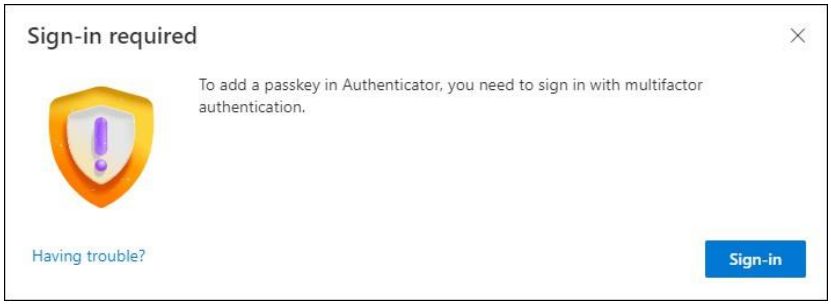
Passkey auf einem Mobilgerät registrieren, das nicht von Lilly stammt

Wenn Sie ein mobiles Gerät verwenden, das nicht von Lilly stammt, befolgen Sie diese Anweisungen, um einen Hauptschlüssel über den Browser Ihres Mobilgeräts oder über einen separaten Computer einzurichten. Diese Registrierung setzt voraus, dass Bluetooth aktiviert ist und eine Internetverbindung für beide Geräte besteht.

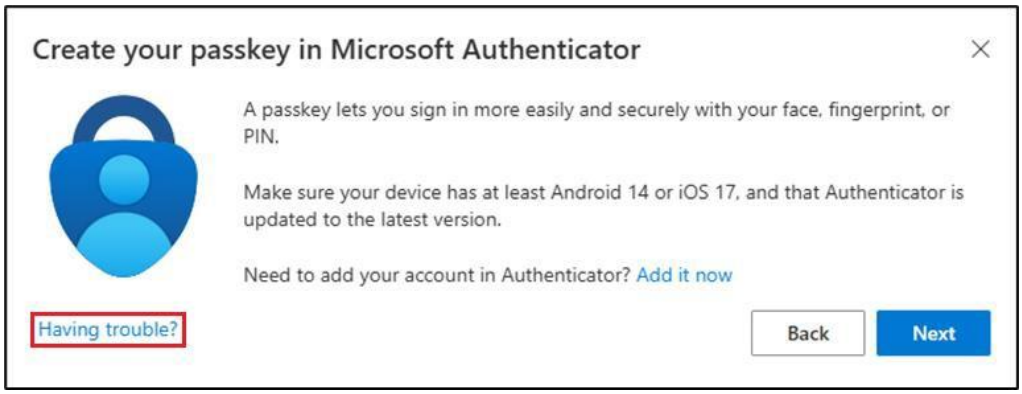
1) Öffnen Sie Microsoft Edge, und greifen Sie auf Meine Anmeldungen zu.
2) Klicken Sie in der oberen rechten Ecke auf Ihr Bild, und stellen Sie sicher, dass Sie mit dem Konto angemeldet sind, das Sie mit Ihrem Hauptschlüssel verwenden möchten (z. B. Standardkonto, -CA oder -DS).
3) Wählen Sie **+ Anmeldemethode hinzufügen aus.**
4) Wählen Sie den **Hauptschlüssel in der Microsoft Authenticator-Methode** aus, und wählen Sie **Hinzufügen** aus.



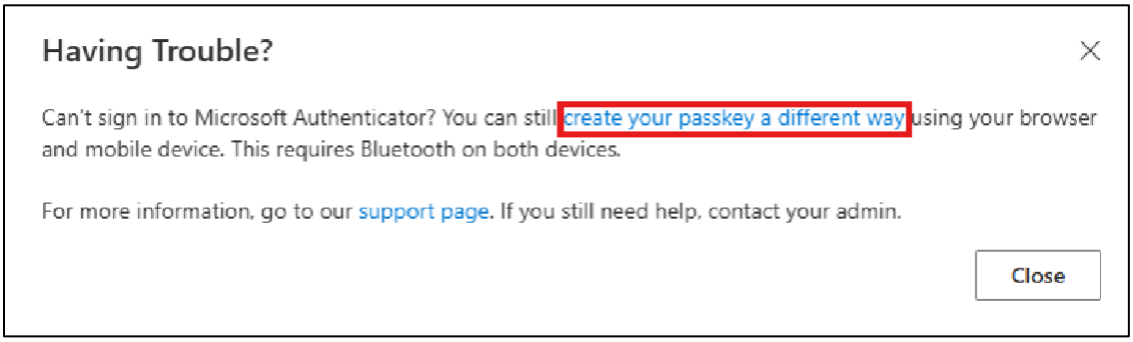
5) Wählen Sie **Anmelden aus**, um Ihre Identität zu bestätigen, indem Sie sich mit Ihrer bevorzugten Authentifizierungsmethode (Windows Hello for Business, Mobiltelefonbenachrichtigung oder Sicherheitsschlüssel) authentifizieren.



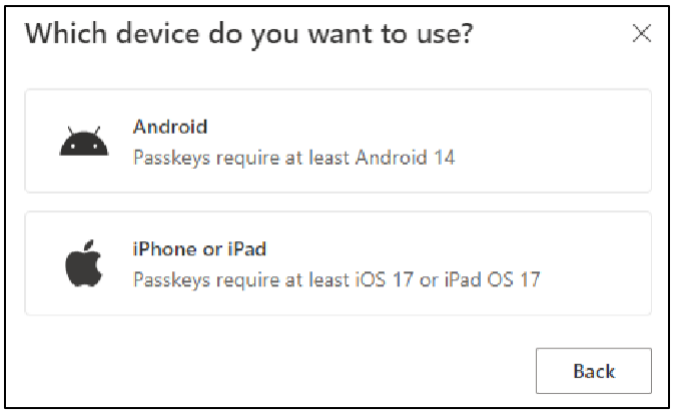
6) Wählen Sie auf dem **Bildschirm Erstellen Sie Ihren Hauptschlüssel in Microsoft Authenticator** die Option "**Haben Sie Probleme?**"-Verknüpfung.



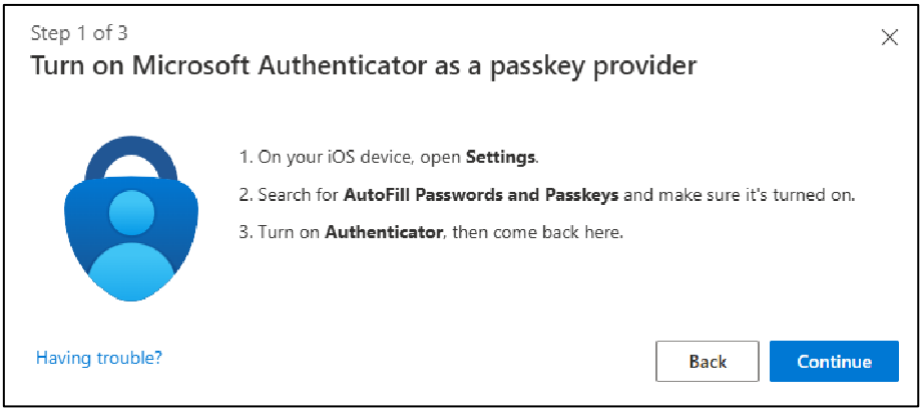
7) Hast **du Probleme?** wählen Sie den Link "Erstellen Sie Ihren Passkey auf eine andere Weise" aus, um einen Passkey für PPA zu registrieren.



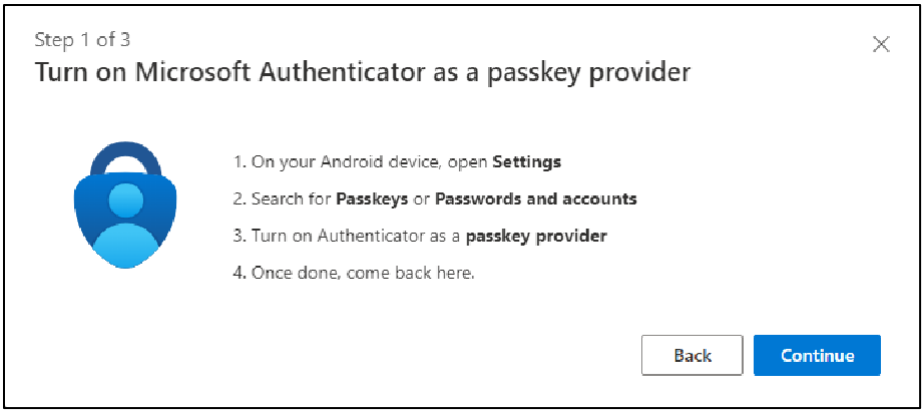
8) Wählen Sie Ihren Gerätetyp aus:



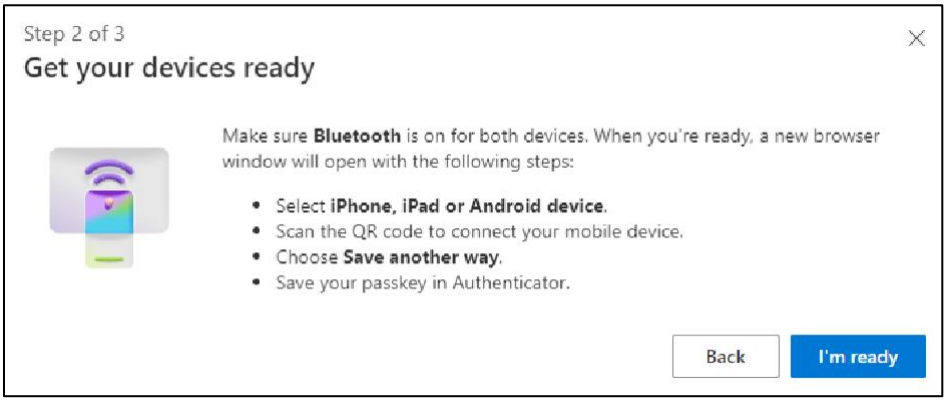
9) Wählen Sie auf dem **Bildschirm Microsoft Authenticator als Hauptschlüsselanbieter aktivieren** die Option **Weiter aus**. **Für iOS-Geräte:**



Für Android-Geräte:

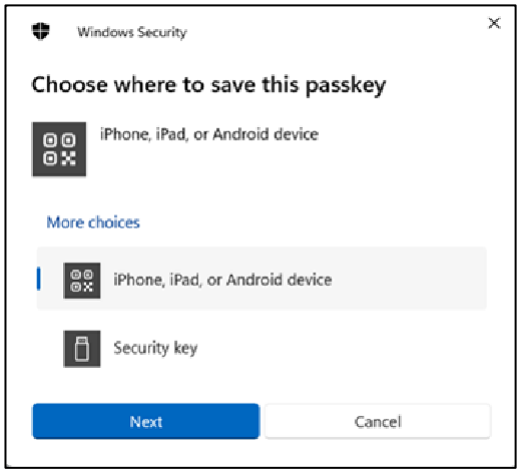


10) Vergewissern Sie sich, dass Bluetooth für beide Geräte aktiviert ist, und wählen Sie **Ich bin bereit** aus.

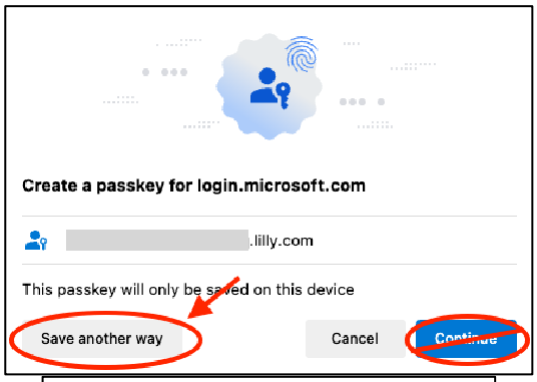


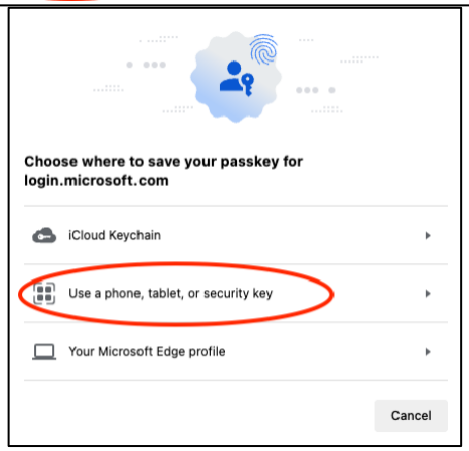
11) Wählen Sie aus, wo Sie Ihren Hauptschlüssel speichern möchten.

Für Windows-Geräte:
Wählen Sie im Sicherheitsdialogfeld, das in Ihrem Browser geöffnet wird**, iPhone, iPad oder Android-Gerät aus** und tippen Sie auf **Weiter**.



Für Mac-Geräte:
Wählen Sie im Sicherheitsdialogfeld, das in Ihrem Browser geöffnet wird, die Option **Auf andere Weise speichern** aus, und wählen Sie im nächsten Dialogfeld **Telefon, Tablet oder Sicherheitsschlüssel verwenden aus.**

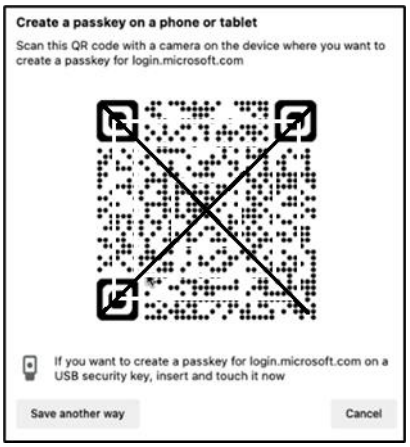




12) Scannen Sie mit der Kamera Ihres Mobilgeräts den QR-Code auf Ihrem Bildschirm und tippen Sie dann auf **Speichern eines Hauptschlüssels**.

Für Windows-Geräte:

Für Mac-Geräte:



13) Ihr Gerät sollte jetzt über Bluetooth eine Verbindung zu dem Gerät herstellen, mit dem Sie die Registrierung begonnen haben.

Für Windows-Geräte:

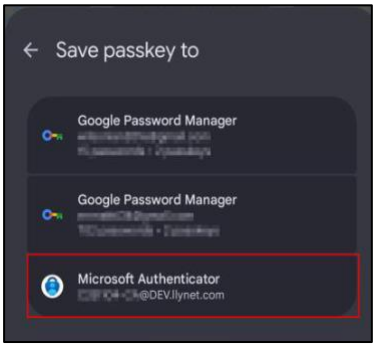
Für Mac-Geräte:

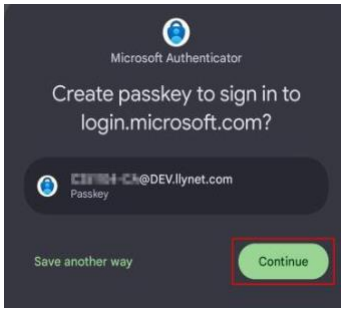
Hinweis: Für diesen Schritt sind Bluetooth und eine Internetverbindung erforderlich, die auf Ihrem Mobil- und Computergerät aktiviert sein müssen.

14) Ihr Gerät fordert Sie auf, einen Hauptschlüssel zu speichern oder zu erstellen. Wählen Sie **Weiter** aus, um den Hauptschlüssel in Authenticator zu speichern.

Für Android-Mobilgeräte:

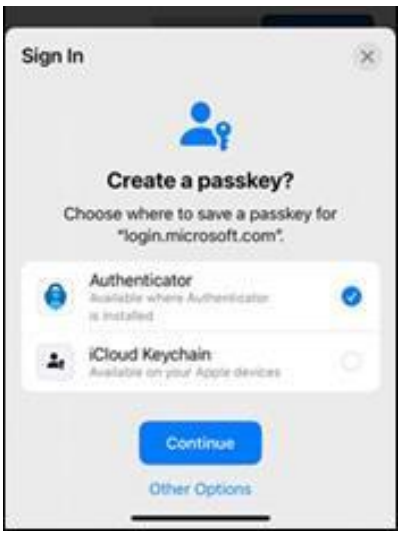
Wählen Sie **Microsoft Authenticator** als Speicherort für den Hauptschlüssel aus. Drücken Sie dann **auf Weiter.**



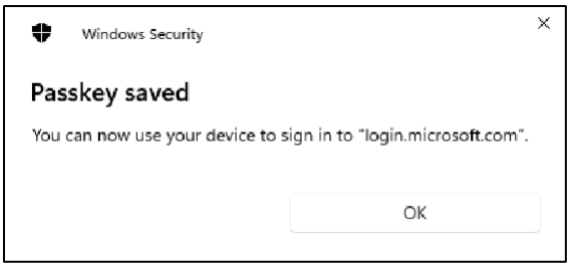


Für iOS-Mobilgeräte:

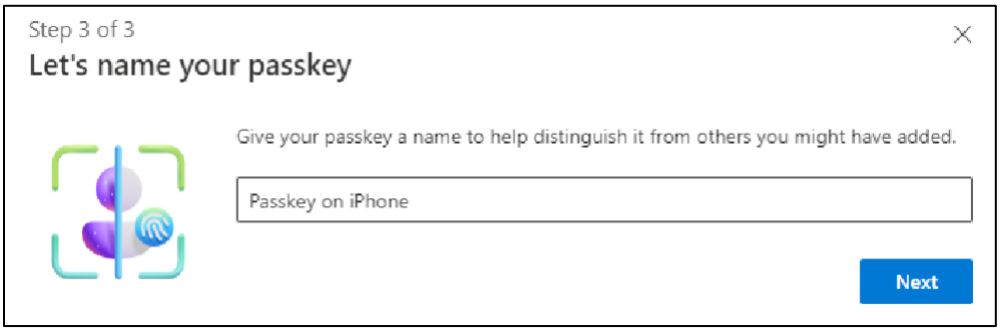
Stellen Sie sicher, dass das Kontrollkästchen für **Authenticator** und drücken **Sie Weiter.**



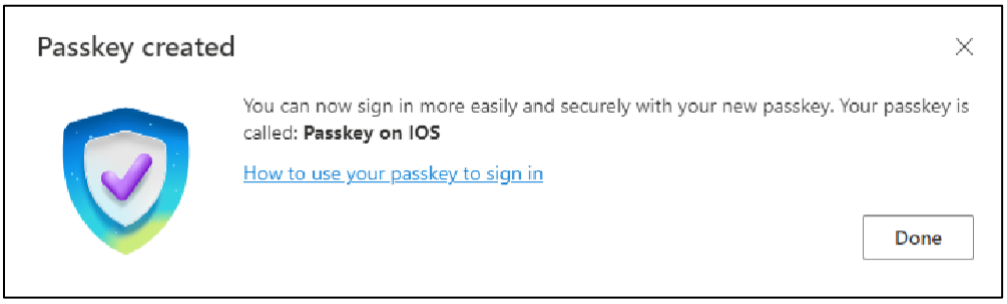
15) Nachdem der Hauptschlüssel erfolgreich auf Ihrem Gerät erstellt wurde, werden Sie zurück zu "Meine Sicherheit"-Informationen weitergeleitet. Wenn Sie dazu aufgefordert werden, wählen Sie **OK** aus.



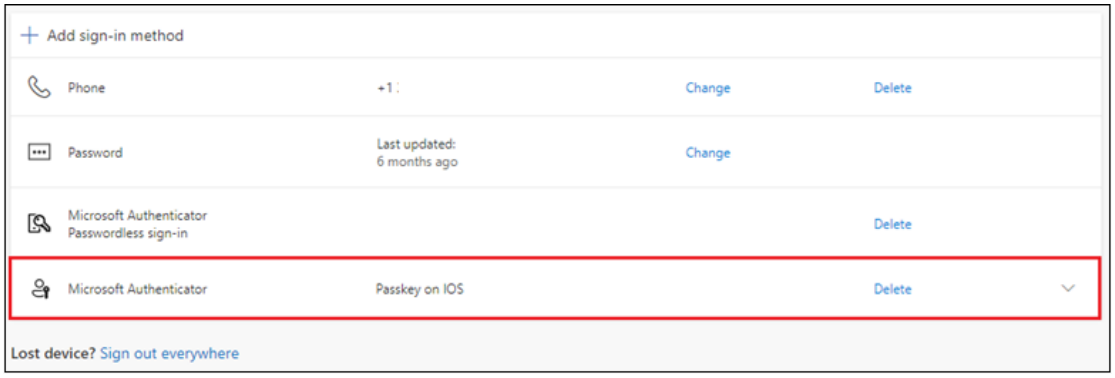
16) Geben Sie einen Hauptschlüsselnamen ein, um ihn von anderen Schlüsseln zu unterscheiden, und wählen Sie **Weiter** aus.



17) Ihr Hauptschlüssel wurde erfolgreich erstellt. Wählen Sie Fertig aus **.**



18) In den Sicherheitsinformationen sehen Sie, dass der neue Hauptschlüssel hinzugefügt wurde.

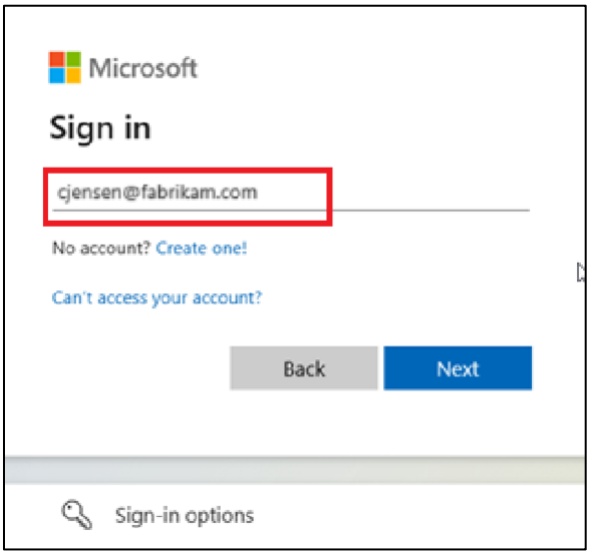


Melden Sie sich mit Passkeys in Authenticator für Android- und iOS-Geräte an

Hinweis: Um sich mit einem Hauptschlüssel in Microsoft Authenticator anzumelden, muss auf Ihrem Mobilgerät iOS Version 17 oder Android Version 14 oder höher ausgeführt werden.

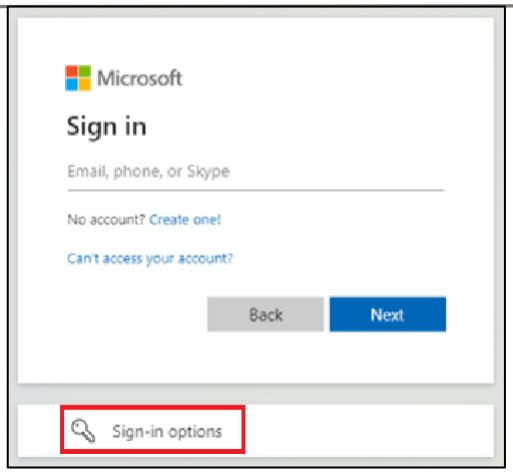
Führen Sie die folgenden Schritte aus, um sich mit einem Hauptschlüssel in Authenticator auf Ihrem iOS-Gerät bei Microsoft Entra ID anzumelden. Navigieren Sie im Computerbrowser zu der Web-URL, auf die Sie zugreifen möchten, z. B. Meine Anmeldungen.

1. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeadresse ein:



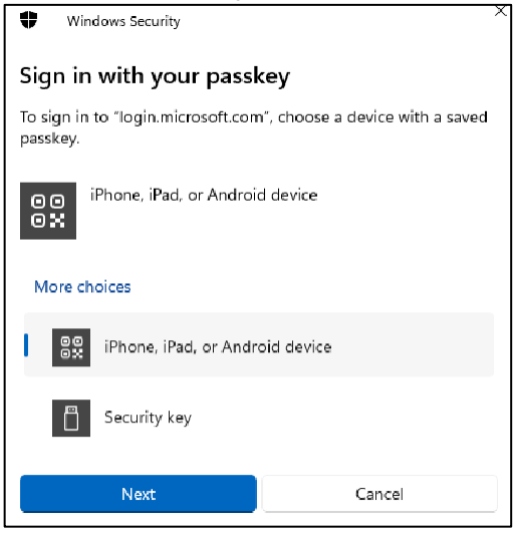
Wenn Sie zuletzt einen Hauptschlüssel für die Authentifizierung verwendet haben, werden Sie automatisch aufgefordert, sich mit einem Hauptschlüssel zu authentifizieren. Andernfalls können Sie auf **andere Anmeldemöglichkeiten** klicken und dann **Gesicht, Fingerabdruck, PIN oder Sicherheitsschlüssel** auswählen.

Alternativ können Sie auf **Anmeldeoptionen klicken**, um sich bequemer anzumelden, ohne einen Benutzernamen eingeben zu müssen.



Wenn Sie **Anmeldeoptionen ausgewählt haben**, wählen Sie **Gesicht, Fingerabdruck, PIN oder Sicherheitsschlüssel aus**. Andernfalls fahren Sie mit dem nächsten Schritt fort.

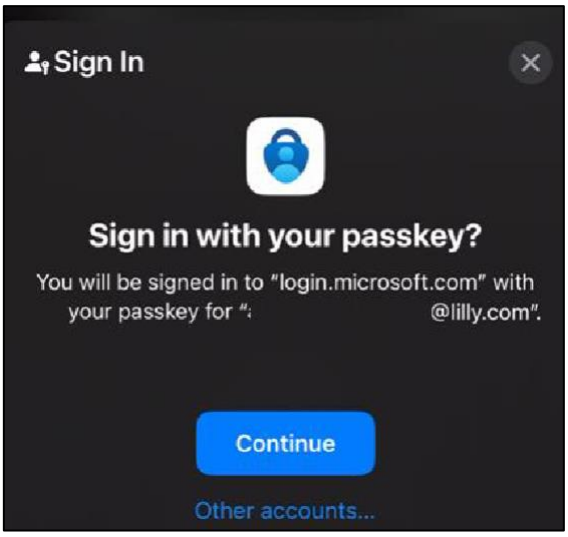
2. Wählen Sie **iPhone, iPad oder Android-Gerät aus**.



3. Auf dem Bildschirm sollte ein QR-Code erscheinen. **Öffnen Sie auf Ihrem Mobilgerät die Kamera-App** und **scannen Sie den QR-Code**.

Hinweis: Für diesen Schritt sind Bluetooth und eine Internetverbindung erforderlich, die beide auf Ihrem Mobil- und Computergerät aktiviert sein müssen.

4. Um Ihren Hauptschlüssel auszuwählen, führen Sie die Schritte im Dialogfeld "Android-Betriebssystem" aus. Vergewissern Sie sich, dass Sie es sind, indem Sie Ihr Gesicht oder Ihren Fingerabdruck scannen oder die PIN Ihres Geräts oder eine Entsperrgeste eingeben.



5. Sie sind jetzt in Ihrem Computerbrowser bei "Meine Anmeldungen" angemeldet.

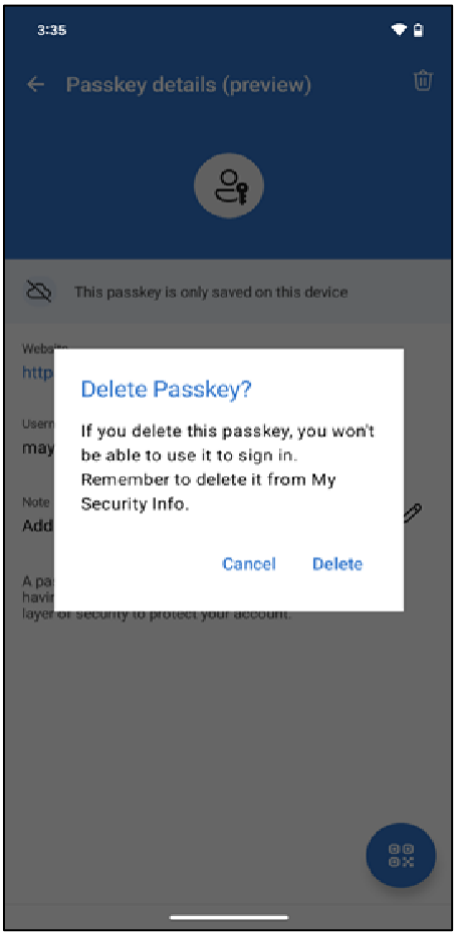
Löschen Sie Ihren Passkey in Authenticator für Android oder iOS

Hinweis: Um die Passkey-Methode vollständig zu entfernen, müssen Sie den Passkey sowohl aus der **Microsoft Authenticator-App auf Ihrem Gerät als** auch aus der Infoseite "Meine Sicherheit " in Ihrem Computerbrowser löschen.

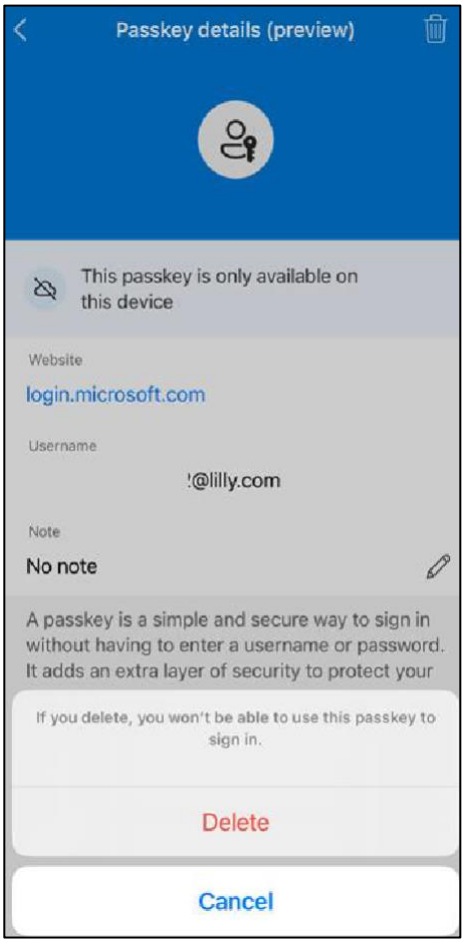
Führen Sie die folgenden Schritte aus, um den Hauptschlüssel aus der Microsoft Authenticator-App auf Ihrem Gerät zu löschen.

1. **Öffnen Sie die Authenticator-App** auf Ihrem Gerät und wählen Sie das Konto aus, von dem Sie den Passkey entfernen möchten.
2. Wählen Sie Passkey unter Ihrem Konto aus, klicken Sie auf das Papierkorbsymbol in der oberen rechten Ecke des Bildschirms und tippen Sie dann zur Bestätigung auf **Löschen** .
3. Sie haben den Hauptschlüssel erfolgreich aus der Microsoft Authenticator-App gelöscht**.** Führen Sie die nächsten Schritte aus, um den Hauptschlüssel von der Infoseite "Meine Sicherheit" auf Ihrem Computer zu entfernen.

Für Android-Mobilgeräte:



Für iOS-Mobilgeräte:

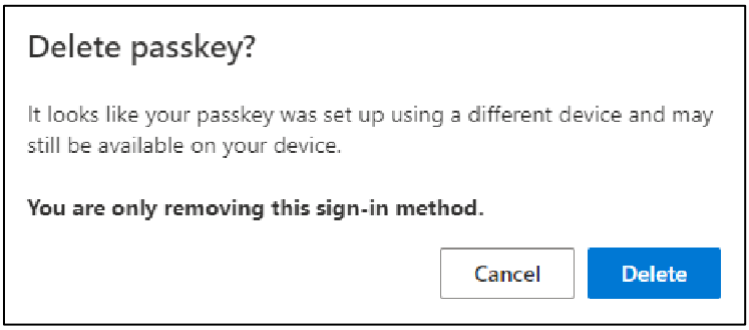


4. Öffnen Sie den Browser auf Ihrem Computer und greifen Sie auf Meine Anmeldungen zu. Klicken Sie in der oberen rechten Ecke auf Ihr Bild, und stellen Sie sicher, dass Sie mit dem Konto angemeldet sind, von dem Sie Ihren Hauptschlüssel entfernen möchten (z. B.

-CA).

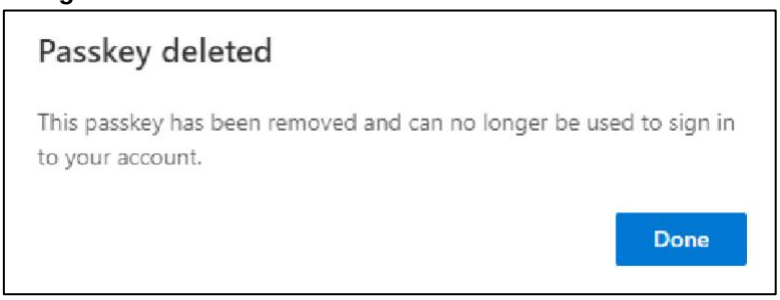
5. Wählen Sie **Entfernen aus**, um den Hauptschlüssel aus den Anmeldemethoden auf der Infoseite "Meine Sicherheit" zu löschen.

6. Wenn Sie dazu aufgefordert werden, wählen Sie **Löschen** aus, um das Entfernen des Hauptschlüssels zu



bestätigen.

7. Sie haben den Hauptschlüssel erfolgreich aus den "Meine Sicherheit"-Informationen gelöscht. Wählen Sie **Fertig** aus.



Zusätzliche Hilfe

Bitte lesen Sie diese häufig gestellten Fragen , um Unterstützung zu erhalten. Wenn Ihre Frage nicht beantwortet wird, empfehlen wir Ihnen, sie in der Community für die Einführung von Identitätsdiensten zu posten.

Für technische Hilfe, die nicht in den FAQs oder Arbeitshilfen behandelt wird, verwenden Sie ChatNow in Teams oder die ChatNow-App auf Ihrem Lilly-Mobilgerät (iPhone, iPad). Erstellen Sie einen Incident und weisen Sie ihn der MFA-SUPP-GLB-Queue zu.