Handbuch
Zwei-Faktor-Authentifizierung (2FA)

Inhalt

1. Überblick Login-Prozess 2
2. Einrichtung 2FA auf dem Smartphone 3
Schritt 1: Download Authenticator App 3
Schritt 2: Einrichtung Authenticator App 3
QR Code Scan nicht möglich? Manuelle Einrichtung 5
3. Manuelle Einrichtung der Authenticator-App 5
3.1 Microsoft Authenticator 5
3.2 Google Authenticator 6
3.3 Free OTP 7
3.3.1 Free OTP via iOS 7
3.3.2 Free OTP via Android 8
4. Einrichtung 2FA über einen Generator 9
4.1 Kurzbeschreibung 9
4.2 Vorteile 9
4.3 Verlust des Generators, oder Wechsel der Authentifizierung 9
5. Authenticator übertragen bei Smartphonewechsel 10
5.1 Google Authenticator 10
5.2 Free OTP Authenticator 11
5.3 Microsoft Authenticator 11
5.3.1 Microsoft Authenticator via iOS 11
5.3.2 Microsoft Authenticator via Android 12

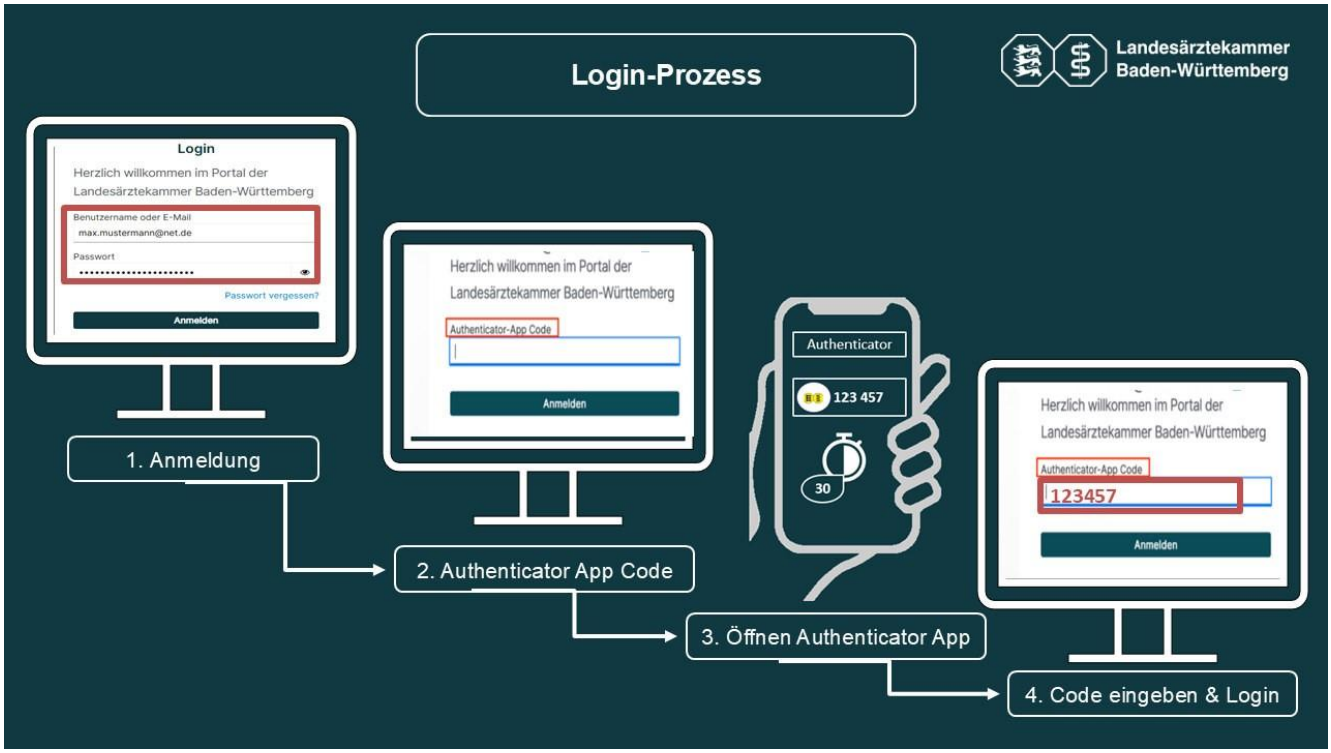
Brauchen Sie Unterstützung?

Kontakt zum Support:

E-Mail: portal-support@laek-bw.de

Tel: 0711 76989-2698

1. Überblick Login-Prozess



1. Geben Sie Ihre E-Mailadresse und Ihr Passwort auf der Website ein und klicken anschließend auf den Button „Anmelden“.
2. Sie werden zur Eingabe des „Authenticator-App Codes“ aufgefordert.
3. Öffnen Sie dazu Ihre Authenticator App auf Ihrem Smartphone. Dort wird Ihnen der 6-stellige Authentifizierung-Code angezeigt.
4. Diesen Code geben Sie nun in das Feld „Authenticator-App Code“ auf der Website ein. Geben Sie den Code ohne Leerzeichen ein. Klicken Sie anschließend auf den Button „Anmelden“.

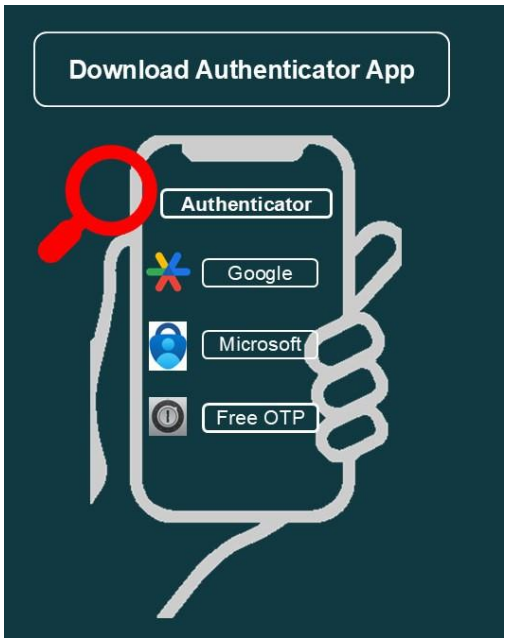
Achtung: der Authentifizierung-App Code auf Ihrem Smartphone ist nur für 30 Sekunden gültig und aktualisiert sich dann automatisch. Sollte der Code abgelaufen sein, geben Sie einfach den neu erzeugten Code für den Login ein.

2. Einrichtung 2FA auf dem Smartphone

Schritt 1: Download Authenticator App

Um die Zwei-Faktor-Authentifizierung nutzen zu können, benötigen Sie eine Authenticator-App auf Ihrem Smartphone.

Öffnen Sie den App Store oder Google Play Store auf Ihrem Smartphone und suchen Sie nach „**Authenticator**“.



Wählen Sie eine App aus, wir empfehlen: Google, Microsoft oder Free OTP Authenticator. **Diese Apps sind kostenfrei**.

Laden Sie die gewählte Authenticator App aus dem App Store oder Google Play Store herunter.

Im nächsten Schritt werden Sie dazu aufgefordert, die Zwei-Faktor-Authentifizierung einzurichten.

Schritt 2: Einrichtung Authenticator App

Sobald Sie sich eine Authenticator App auf Ihrem Smartphone heruntergeladen haben, klicken Sie in der App auf das Plus-Symbol (+)

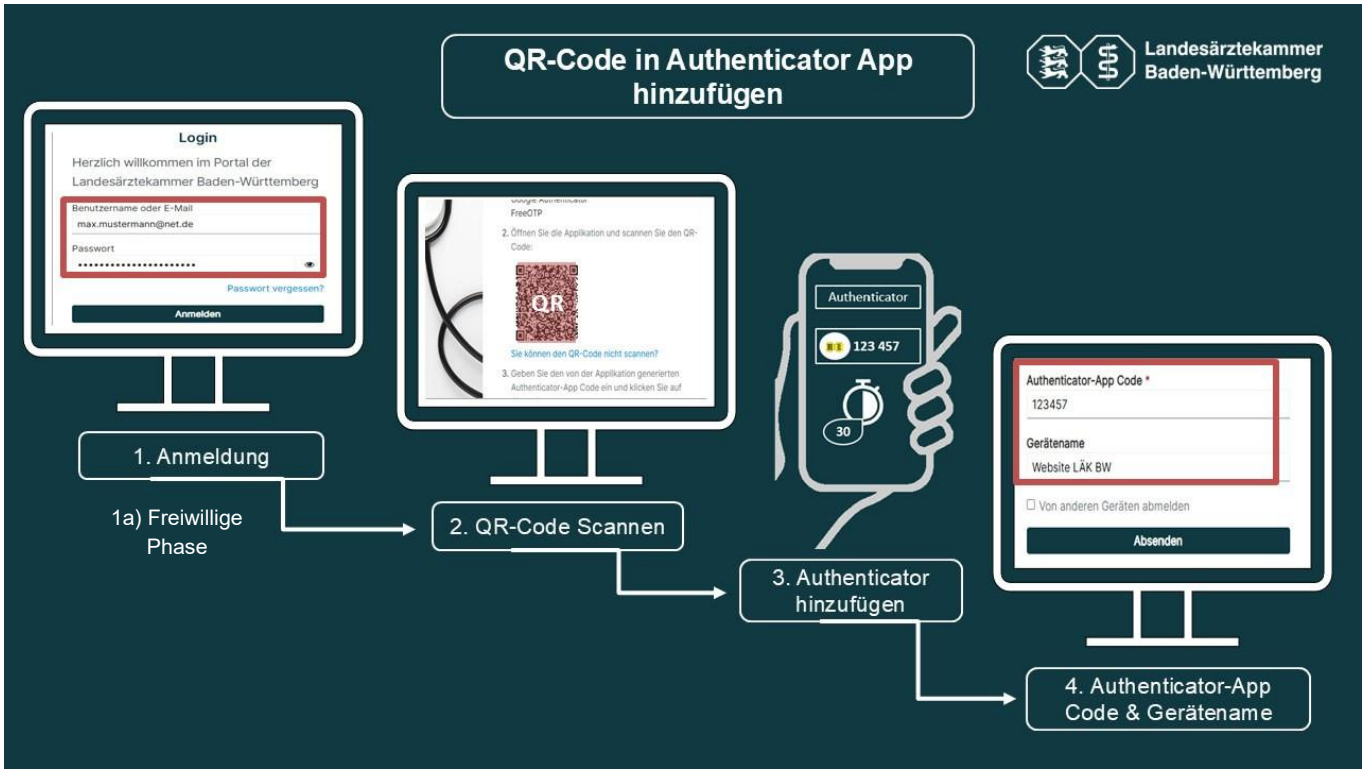
- **oben rechts** für Microsoft und Free OTP Authenticator *iOS*, oder
- **unten rechts** für Google Authenticator, Free OTP Authenticator *Android*

Im nächsten Schritt kann der Authenticator per QR Code hinzugefügt werden.



Beim **Free OTP Authenticator** via **iOS** muss für die Einrichtung per QR Code auf das QR Code Symbol oben rechts geklickt werden, nicht auf das Plus.

Schritt 3: QR Code in Authenticator App hinzufügen



Zum Hinzufügen des QR Codes in Ihrer Authenticator App befolgen Sie folgende Schritte:

1. Melden Sie sich mit Ihrer E-Mailadresse und Ihrem Passwort auf der Website der Landesärztekammer BW an.
2. Scannen Sie den QR Code mit Ihrer Authenticator App auf dem Smartphone ab, der Ihnen auf der Website angezeigt wird. Dafür klicken Sie in Ihrer Authentifizierungs-App auf "QR Code scannen“. Erlauben Sie der App den Zugriff auf Ihre Kamera. Das Konto wird automatisch in Ihrer Authentifizierungs-App hinzugefügt.
3. Nun zeigt Ihre Authentifizierung App einen 6-stelligen Code auf Ihrem Smartphone an.
4. Geben Sie im Feld „Authenticator App Code“ den 6-stelligen Code aus Ihrer Authentifizierungsapp ohne Leerzeichen ein und klicken auf den Button „Absenden“ und loggen sich ein.

Achtung: Der Authentifizierung App Code auf Ihrem Smartphone ist nur für 30 Sekunden gültig und aktualisiert sich dann automatisch. Sollte der Code abgelaufen sein, geben Sie einfach den neu erzeugten Code für den Login ein. Ihr zweiter Faktor ist nun eingerichtet. Dieser muss für jeden Login genutzt werden. Werfen Sie gerne einen Blick auf Kapitel 1: Überblick Login-Prozess.

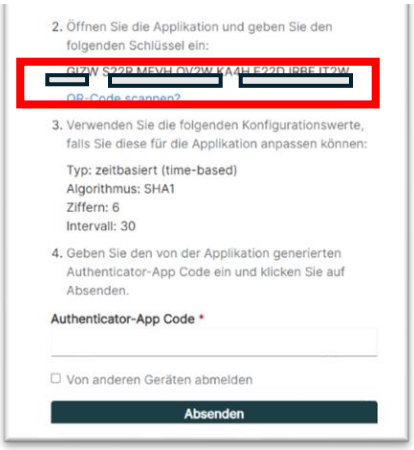
QR Code Scan nicht möglich? Manuelle Einrichtung

Falls der Scan des QR Codes nicht möglich ist, bietet sich die Möglichkeit an, den Code manuell in der Authenticator App auf Ihrem Smartphone einzugeben.

Klicken Sie im Login Fenster unterhalb des QR Codes auf den Button „Sie können den QR Code nicht scannen?“



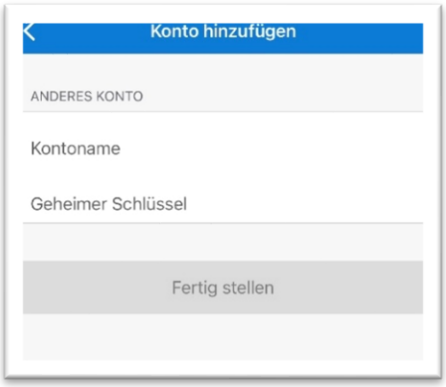
Es öffnet sich nun ein 32-stelliger Code auf der Website der LÄK BW. Diesen können Sie manuell in Ihrer Authenticator App hinzufügen.



3. Manuelle Einrichtung der Authenticator-App

3.1 Microsoft Authenticator

1. Klicken Sie, nachdem sich die Kamera des Authenticators geöffnet hat, auf „Code manuell eingeben“ (Enter code manually).



2. Geben Sie unter „Kontoname“ (Account name) z.B. „Website Landesärztekammer“ ein.

3. Geben Sie unter „Geheimer Schlüssel“ (Secret key) den 32-stelligen Schlüssel von der Website ein.

4. Beenden Sie die Einrichtung durch Klicken auf „Fertig stellen“ (Finish).

→ Nun erscheint der sechsstellige Code auf dem Handy. Geben Sie diesen ohne Leerzeichen auf der Website ein und klicken auf den Button „Absenden“ und loggen sich ein. Dieser erneuert sich alle 30 Sekunden.

3.2 Google Authenticator



1. Klicken Sie auf „Einrichtungsschlüssel eingeben“ (Enter setup key).

2. Geben Sie unter “Kontoname“ (Account name) „Website Landesärztekammer“ ein.

3. Geben Sie unter „Mein Schlüssel“ (Your key) ihren 32-stelligen Schlüssel ein.

4. Belassen Sie das Feld „Zeitbasiert“ (Time based) unverändert.

5. Beenden Sie die Einrichtung durch Klicken auf „Hinzufügen“ (Add).

→ Nun erscheint der sechsstellige Code auf dem Handy. Geben Sie diesen ohne Leerzeichen auf der Website ein und klicken auf den Button „Absenden“ und loggen sich ein. Dieser erneuert sich alle 30 Sekunden.

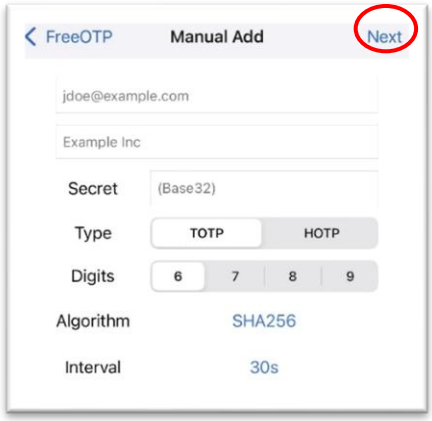
3.3 Free OTP

Free OTP richtet sich abhängig vom Betriebssystem unterschiedlich ein.

Unter **3.3.1** wird die Einrichtung via iOS geschildert und unter **3.3.2** die Einrichtung für Android.

3.3.1 Free OTP via iOS

(1)



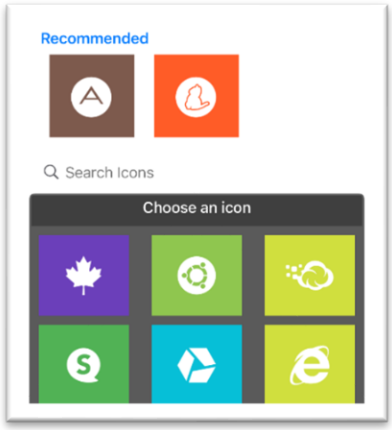
1. Hinterlegen Sie im Feld jdoe@ Ihre Anmelde-Mail für ihr Landesärztekammer Konto. (1)

2. Tragen Sie im Feld „Example Inc“ „Website Landesärztekammer“ ein (1). Geben Sie anschließend im Feld „Secret (Base32)“ den 32-stelligen Code ein, welchen Sie auf der Website der Landesärztekammer sehen.

3. Belassen Sie alle weiteren Einstellungen unverändert. (1)

4. Klicken Sie auf „Next“. (1)

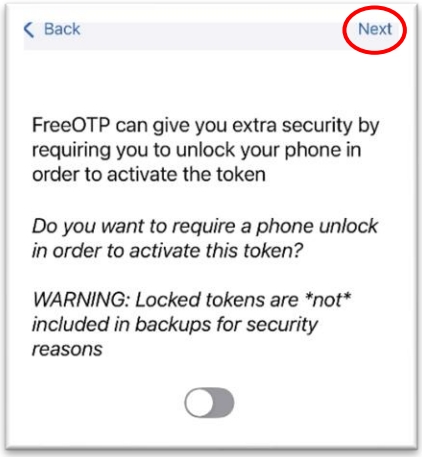
(2)



5. Wählen Sie ein Icon ihrer Wahl aus (2) und klicken auf „Next“.

6. Wählen Sie im nächsten Schritt (3), ob Sie Ihren 2FA Code durch Gesichtserkennung, Fingerprint, oder ihr Passwort sichern wollen.

(3)

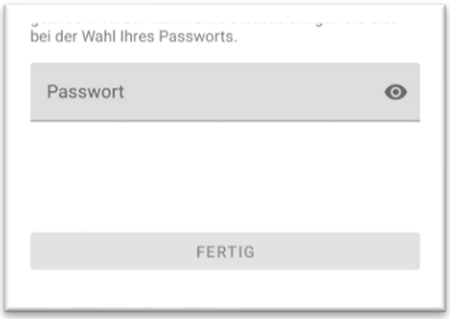


7. Beenden Sie die Einrichtung durch Klicken auf Next“.

→ Nun erscheint der sechsstellige Code auf dem Handy. Geben Sie diesen ohne Leerzeichen auf der Website ein und klicken auf den Button „Absenden“ und loggen sich ein. Dieser erneuert sich alle 30 Sekunden.

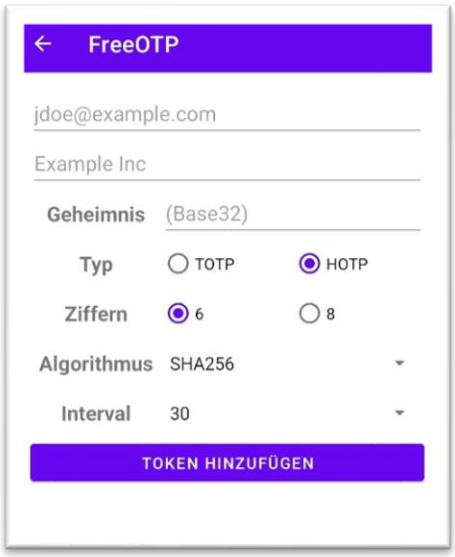
3.3.2 Free OTP via Android

(1)



1. Bei der erstmaligen Einrichtung muss ein Masterkennwort vergeben werden. Dieses Kennwort wird zur Entsperrung der Wiederherstellungsdatei benötigt und kann bei Verlust oder Vergessen nicht wiederhergestellt werden. Bitte bewahren Sie das Masterkennwort daher sicher auf. (1)

(2)



2. Starten Sie die Einrichtung durch Klicken auf das „+“ unten rechts und wählen Sie das Stiftsymbol aus.

3. Hinterlegen Sie unter jdoe@ Ihre Anmelde E-Mail für ihr Landesärztekammer Konto. (2)

4. Tragen Sie im Feld „Example Inc“ „Website Landesärztekammer“ ein. Geben Sie anschließend im Feld „Geheimnis (Base32)“ den 32-stelligen Code ein, welchen Sie auf der Website der Landesärztekammer sehen. (2)

5. Stellen Sie „Typ“ auf „TOTP“ um und belassen Sie alle weiteren Einstellungen unverändert. (2)

6. Klicken Sie auf „Token Hinzufügen“. (2)

→ Nun erscheint der sechsstellige Code auf dem Handy. Geben Sie diesen ohne Leerzeichen auf der Website ein und klicken auf den Button „Absenden“ und loggen sich ein. Dieser erneuert sich alle 30 Sekunden.

4. Einrichtung 2FA über einen Generator

4.1 Kurzbeschreibung

Ersatzweise zum Smartphone kann ein Zwei-Faktor-Generator (Hardware-Token) zur Verifizierung eingesetzt werden.

Dieser Generator wird nicht von der LÄK BW zur Verfügung gestellt und kann privat über den Onlinemarkt erworben werden.

Ähnlich wie bei den Authenticator-Apps, die auf dem Smartphone installiert werden, muss der Generator mithilfe eines QR Codes gekoppelt werden, damit ein 6-stelliger Code generiert werden kann.

4.2 Vorteile

Diese weitere Komponente schützt Ihr Benutzerkonto vor Missbrauch und Identitätsdiebstahl, selbst wenn Ihre Logindaten ausfindig gemacht wurden.
Das Gerät funktioniert unabhängig von Ihrem Smartphone und Netzempfang.
Die Handhabung ist besonders unkompliziert und bei Erfahrung mit Authenticator-Apps ähnlich aufgebaut.

4.3 Verlust des Generators, oder Wechsel der Authentifizierung

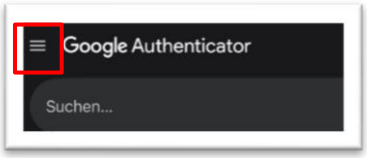
Möchten Sie Ihren hinterlegten zweiten Faktor ändern, oder ist der Generator abhandengekommen, wenden Sie Sich bitte an den Support.

Ihre Authentifizierung wird zurückgesetzt und kann neu eingerichtet werden.

5. Authenticator übertragen bei Smartphonewechsel

Wenn Sie ein neues Smartphone einrichten möchten und Sie bereits auf Ihrem alten Gerät den 2FA nutzen, kann dies auf Ihr neues Smartphone übertragen werden. Für die sicherer Übertragung benötigen Sie dafür Zugriff Ihr **altes Smartphone**.

5.1 Google Authenticator



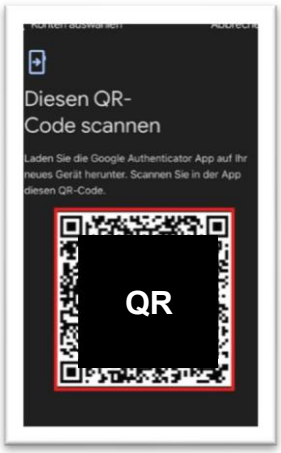
Das neue und alte Smartphone sollten zur Hand sein. Die Google Authenticator App ist auf beiden Geräten installiert:



1. Öffnen Sie den Google Authenticator auf Ihrem **alten Smartphone**.
   Klicken Sie oben auf das **Menü** (drei Striche).

2. Klicken Sie, nach dem sich das Menü geöffnet hat, auf **„Konten übertragen“**.

3. Wählen Sie **„Konten exportieren“**.



4. **Authentifizieren** Sie Sich durch Fingerabdruck/PIN/Face-ID, etc.

5. Wählen Sie die Konten aus, die übertragen werden sollen.

6. Sie sehen einen **QR Code**. Diesen QR Code müssen Sie mit Ihrem **neuen Gerät** vom alten Smartphone abscannen.

7. Um den Scan auf Ihrem neuen Gerät zu starten, befolgen Sie Schritt 1 und 2. Anschließend wählen Sie **„Konten importieren“** und Ihre Kamera öffnet sich zum Scan automatisiert.

   Wenn alles funktioniert hat, sehen Sie nun einen 6-stelligen Code auf der Authenticator App des neuen Smartphones.

Achtung:
Löschen Sie den Google Authenticator auf dem alten Gerät erst, wenn Sie sicher sind, dass alles funktioniert.

5.2 Free OTP Authenticator

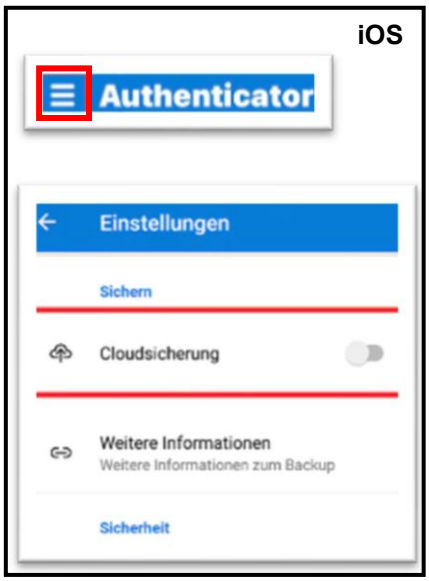
Achtung:
FreeOTP bietet keine Cloud-Backups.
Die Übertragung der Schlüssel ist auf Android über exportieren der Einrichtungsschlüssel Datei möglich. Auf iOS muss der zweite Faktor erneut eingerichtet werden, da hier keine Übertragung möglich ist. In diesem Fall wenden Sie sich bitte an den Technischen Support (Seite 2).

5.3 Microsoft Authenticator

Beim Microsoft Authenticator lässt sich, abhängig vom Betriebssystem das Backup auf unterschiedlich Weise erstellen.

Unter **5.3.1** wird die Einrichtung eines Backups über iOS geschildert und unter **5.3.2** die Einrichtung eines Backups über Android.

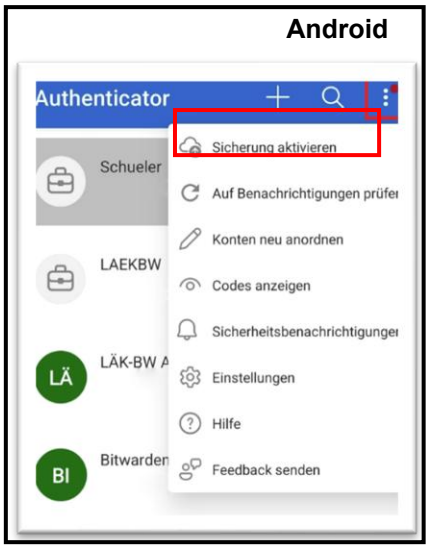
5.3.1 Microsoft Authenticator via iOS



1. Öffnen Sie auf Ihrem **alten** Smartphone die Authenticator App.
2. Klicken Sie oben rechts auf die **drei Punkte (⋮)** oder auf **Ihr Konto-Symbol**.
3. Verbinden Sie Ihren Microsoft Account bzw. erstellen Sie einen neuen Microsoft Account.
4. Aktivieren Sie die Sicherung in die iCloud.
5. Öffnen Sie die Einstellungen in der Authenticator App und stellen Sie sich, dass im Bereich Backup das „Cloud Backup“ bzw. das „iCloud Backup“ aktiviert ist.
6. Wenn Sie die Cloudsicherung eingeschaltet haben und ein Microsoft-Konto besitzen, können Sie die Authenticator App auf Ihrem neuen Gerät herunterladen und sich an Ihrem neuen Gerät mit Ihren Microsoftzugangsdaten anmelden. Die Daten werden nun aus der Cloud auf Ihr neues Smartphone übertragen und Sie sehen Ihren 6-stelligen Code.

Achtung:
Ohne aktiviertes Backup kann keine Wiederherstellung erfolgen!

5.3.2 Microsoft Authenticator via Android



1. Öffnen Sie auf Ihrem **alten** Smartphone die Authenticator App.

2. Klicken Sie oben rechts auf die **drei Punkte (⋮)** oder auf **Ihr Konto-Symbol**.

3. Klicken Sie auf „Sicherung aktivieren“.
   Je nach Version der App müssen Sie zuerst „Einstellungen“ anwählen und anschließend die Option „Cloudsicherung“ aktivieren.

4. Verbinden Sie Ihren Microsoft Account bzw. erstellen Sie einen neuen Microsoft Account.

5. Prüfen Sie zur Sicherheit in den Einstellungen, ob das Cloud Backup weiterhin aktiv ist. (siehe Schritt 3).

6. Wenn Sie die Cloudsicherung eingeschaltet haben und ein Microsoft-Konto besitzen, können Sie die Authenticator App auf Ihrem neuen Gerät herunterladen und sich an Ihrem neuen Gerät mit Ihren Microsoftzugangsdaten anmelden. Die
   Daten werden nun aus der Cloud auf Ihr neues Smartphone übertragen und Sie sehen Ihren 6-stelligen Code.

Achtung:
Ohne aktiviertes Backup kann keine Wiederherstellung erfolgen!