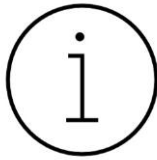


Handbuch

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
Schritt 3: QR-Code in Authenticator App hinzufügen	4
QR-Code Scan nicht möglich? → Manuelle Einrichtung	5
3. Manuelle Einrichtung der Authenticator-App	6
3.1 Microsoft Authenticator	6
3.2 Google Authenticator	6
3.3 Free OTP	7
4. Einrichtung 2FA über einen Generator	8
4.1 Kurzbeschreibung	8
4.2 Vorteile	8
4.3 Verlust des Generators, oder Wechsel der Authentifizierung	8
4.4 Login Prozess mit Einrichtung des Generators	9
5. Smartphone-Wechsel Authenticator	10
5.1 Google Authenticator	10
5.2 Microsoft Authenticator	11
5.3 Free OTP Authenticator	11



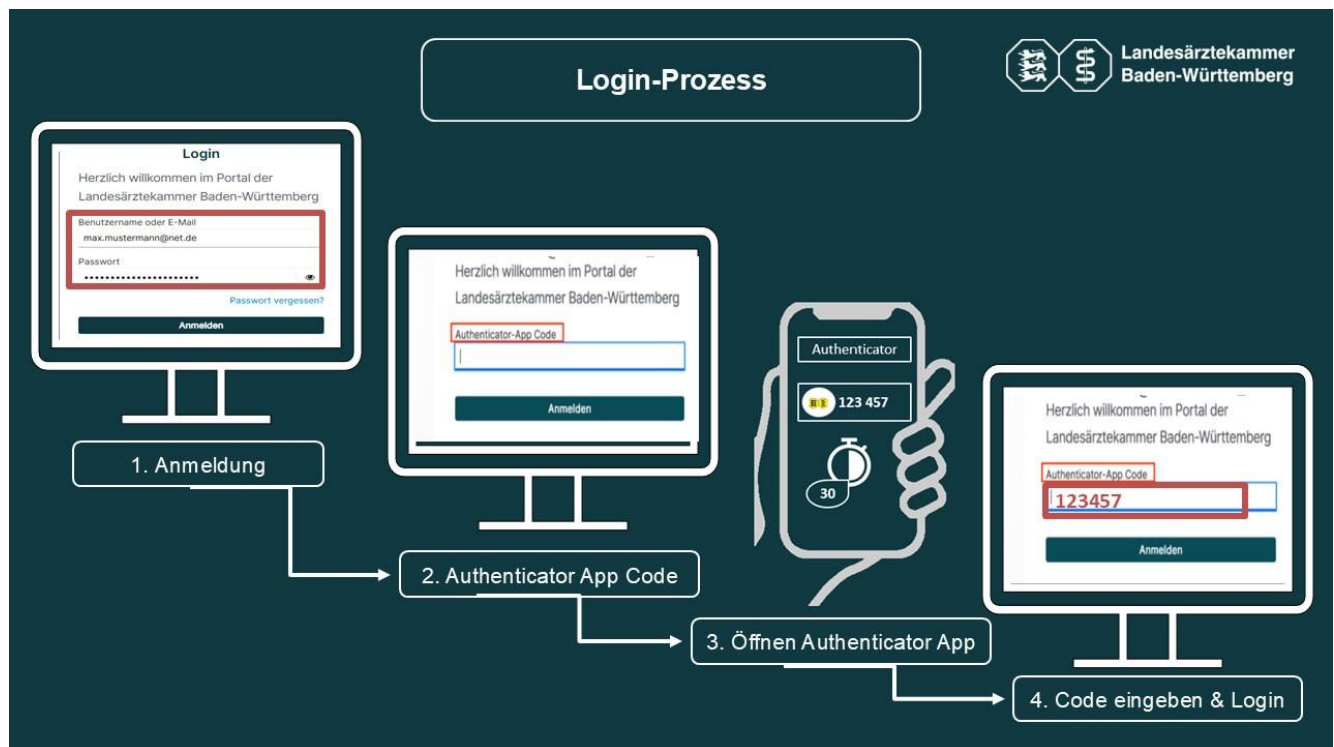
Brauchen Sie Unterstützung?

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.

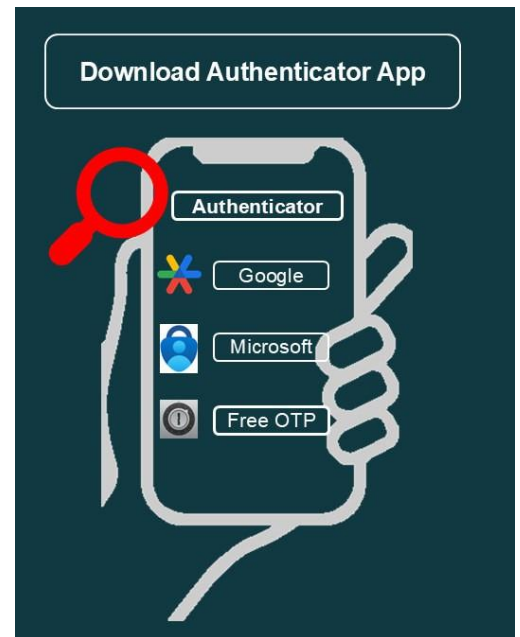
Öffnen Sie den App Store oder Google Play Store auf Ihrem Smartphone und suchen Sie nach „**Authenticator**“.



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.

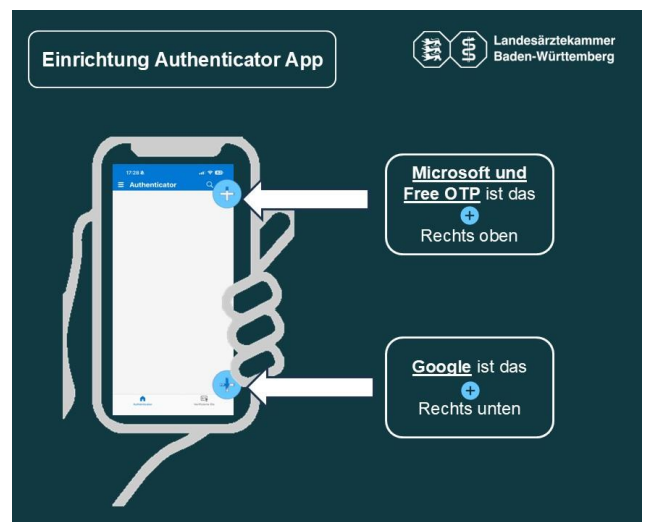


Schritt 2: Einrichtung Authenticator App

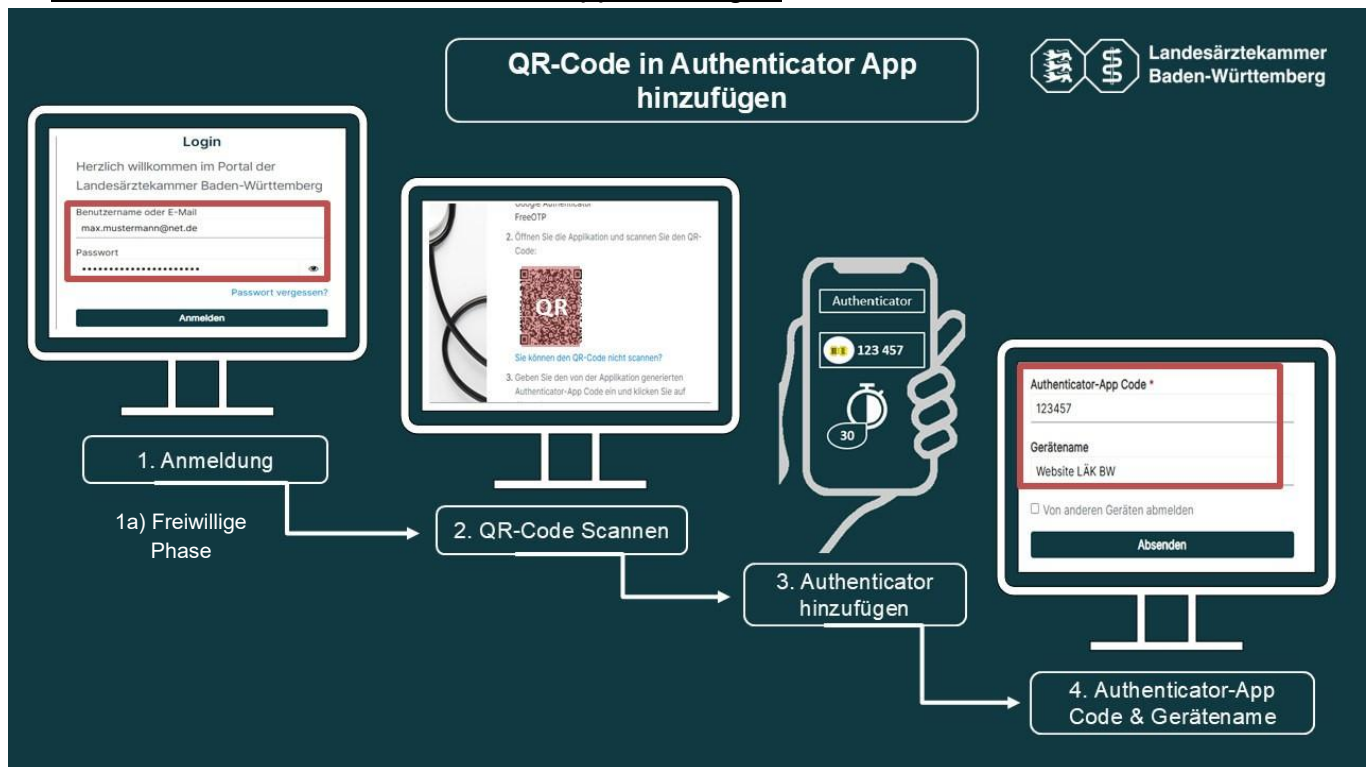
Sobald Sie sich eine Authenticator App auf Ihrem Smartphone heruntergeladen haben, Tippen Sie in der App auf das Plus-Symbol (+)

- **oben rechts** für Microsoft und Free OTP Authenticator, oder
- **unten rechts** für den Google Authenticator.

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



Schritt 3: QR-Code in Authenticator App hinzufügen



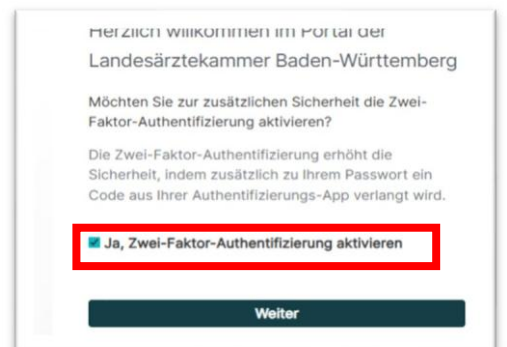
Zum Hinzufügen des QR-Codes in Ihrer Authenticator App befolgen Sie folgende Schritte:

1. Melden Sie sich mit Ihrer E-Mailadresse und Ihrem Passwort auf der Website der Landesärztekammer BW an.

1a) Freiwillige Einrichtung 2FA bis April 2026:

Sie sehen nun folgendes Fenster:

- ➔ Um den 2FA einzurichten, klicken Sie auf den Haken „Ja, Zwei-Faktor-Authentifizierung aktivieren“.



Herzlich willkommen im Portal der
Landesärztekammer Baden-Württemberg

Möchten Sie zur zusätzlichen Sicherheit die Zwei-Faktor-Authentifizierung aktivieren?

Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit, indem zusätzlich zu Ihrem Passwort ein Code aus Ihrer Authentifizierungs-App verlangt wird.

☒ Ja, Zwei-Faktor-Authentifizierung aktivieren

Weiter

2. Scannen Sie den QR-Code mit Ihrer Authenticator App auf dem Smartphone ab, der Ihnen auf der Website angezeigt wird. Dafür tippen 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.



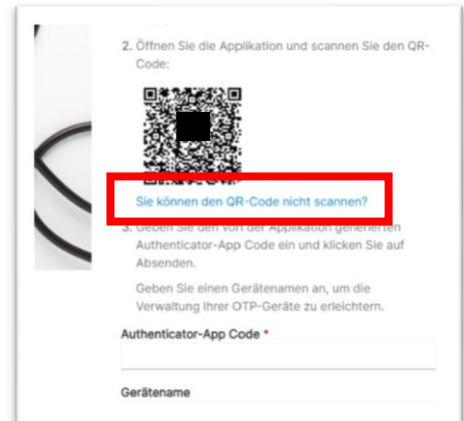
Achtung: Der Authentifizierungs App Code auf Ihrem Smartphone ist nur für 30 Sekunden gültig und aktualisiert sich dann automatisch. Sollte der Code abgelaufen sein, geben Sie einfach den neu erzeugten Code für den Login ein. Ihr zweiter Faktor ist nun eingerichtet. Dieser muss für jeden Login genutzt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

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.



2. Öffnen Sie die Applikation und scannen Sie den QR-Code:

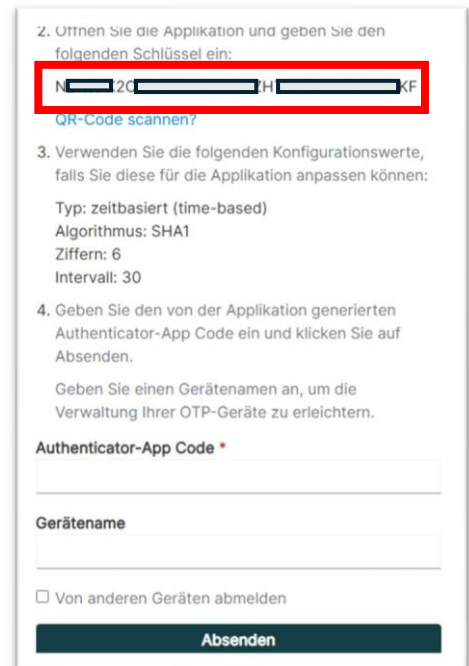
Sie können den QR-Code nicht scannen?

3. Geben Sie den von der Applikation generierten Authenticator-App Code ein und klicken Sie auf Absenden.

Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

Authenticator-App Code *

Gerätename



2. Öffnen Sie die Applikation und geben Sie den folgenden Schlüssel ein:

N 2C H KF

[QR-Code scannen?](#)

3. Verwenden Sie die folgenden Konfigurationswerte, falls Sie diese für die Applikation anpassen können:

Typ: zeitbasiert (time-based)
Algorithmus: SHA1
Ziffern: 6
Intervall: 30

4. Geben Sie den von der Applikation generierten Authenticator-App Code ein und klicken Sie auf Absenden.

Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

Authenticator-App Code *

Gerätename

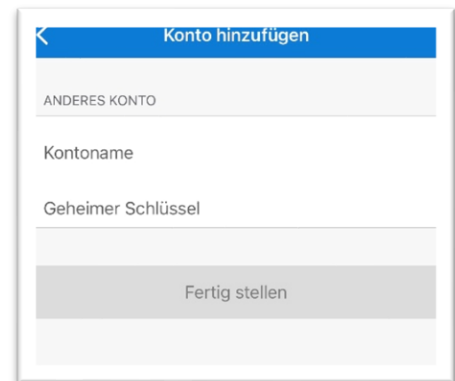
☐ Von anderen Geräten abmelden

Absenden

3. Manuelle Einrichtung der Authenticator-App

3.1 Microsoft Authenticator

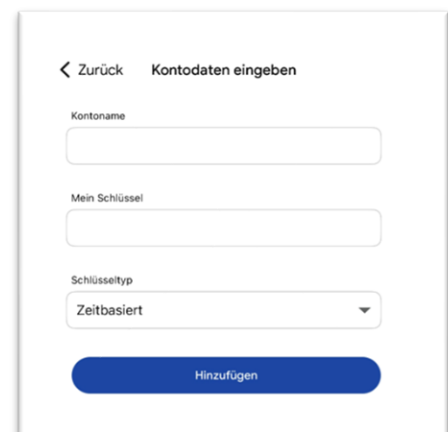
1. Tippen Sie, nachdem sich die Kamera des Authenticators geöffnet hat, auf „Code manuell eingeben“ (Enter code manually).
2. Geben Sie unter „Kontoname“ (Account name) z.B. „Website Landesärztekammer“ ein.
3. Geben Sie unter „Geheimer Schlüssel“ (Secret key) den 32-stelligen Schlüssel von der Website 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. Tippen 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).



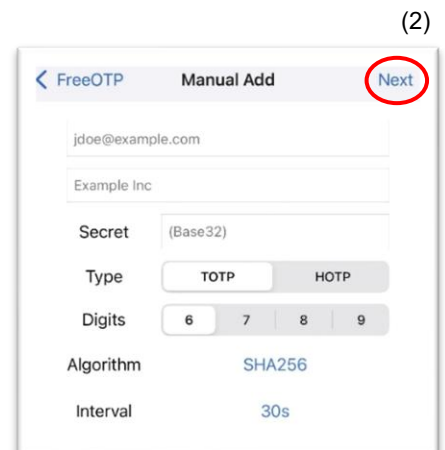
→ Nun erscheint der sechsstellige Code auf dem Handy. Geben Sie diesen ohne Leerzeichen auf der Website ein und klicken auf den Button „Absenden“ und loggen sich ein. Dieser erneuert sich alle 30 Sekunden.

3.3 Free OTP

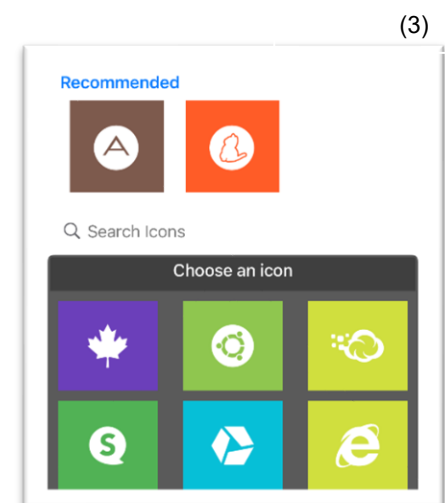
1. Starten Sie die Einrichtung durch Klicken auf das „+“ oben rechts. (1)



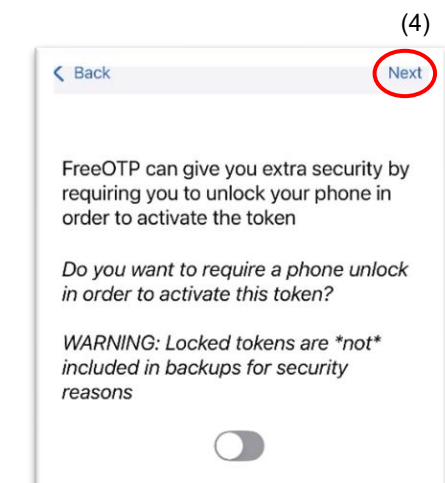
2. Hinterlegen Sie unter „jdoe@example.com“ Ihre Anmelde E-Mail für ihr Landesärztekammer Konto. (2)
3. Tragen Sie im Feld „Example Inc“ „Website Landesärztekammer“ ein. Geben Sie anschließend im Feld „Secret (Base32)“ den 32-stelligen Code ein, welchen Sie auf der Website der Landesärztekammer sehen. (2)



4. Belassen Sie alle weiteren Einstellungen unverändert. (2)
5. Klicken Sie auf „Next“. (2)
6. Wählen Sie ein Icon ihrer Wahl aus (3) und klicken auf „Next“.
7. Wählen Sie im nächsten Schritt (4), ob Sie Ihren 2FA Code durch Gesichtserkennung, Fingerprint, oder ihr Passwort sichern wollen.



8. 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.



Achtung: der Authentifizierungs 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** (STRG + Klicken, um Link zu folgen).

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.

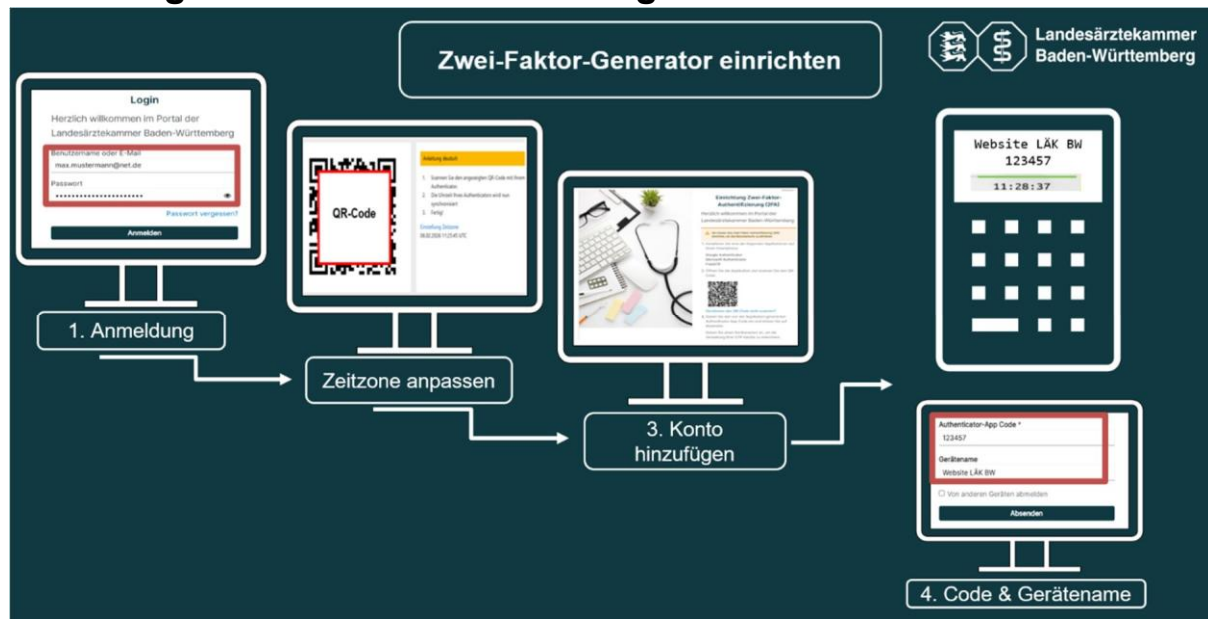
Die Handhabung ist besonders unkompliziert und bei Erfahrung mit Authenticator-Apps ähnlich aufgebaut.

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.

4.4 Login Prozess mit Einrichtung des Generators



1. Melden Sie Sich mit Ihrer E-Mailadresse und Ihrem Passwort auf der Website der Landesärztekammer BW an.
2. Im nächsten Schritt scannen Sie den QR-Code, mithilfe des Generators, um die Zeitzone anzupassen. Diesen Code finden Sie über die Website des Generator-Anbieters. Die Zeitzone wird automatisiert hinzugefügt.
 - ➔ Unsere Empfehlung: Rufen Sie über die Website Ihres Generators die entsprechende Kurzanleitung des Gerätes auf.
 - ➔ In der Regel finden Sie in der Kurzeinleitung den Link, um die Zeitzone einzustellen. Hierbei wird der angezeigte QR-Code (Website GeneratorAnbieter) mit dem Generator gescannt.
3. Nun zeigt Ihnen der Generator an, dass Sie ein Konto hinzufügen müssen. Dies erfolgt durch das Scannen des QR-Codes auf der Website der LÄK-BW.
4. Der Generator wurde erfolgreich eingerichtet, wenn Ihnen ein 6-stelliger Code und GeräteName angezeigt wird.
5. Der Code und der GeräteName werden im letzten Schritt aus dem Generator auf die Portal-Seite übertragen.



Achtung: Der Authentifizierungs-Code im Generator 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.

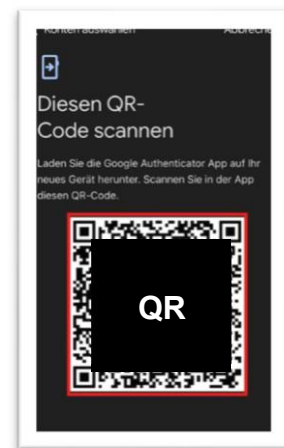
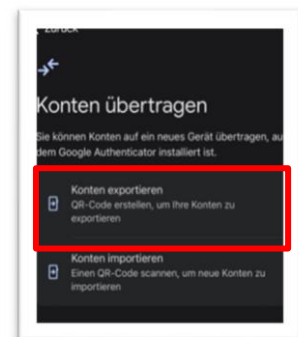
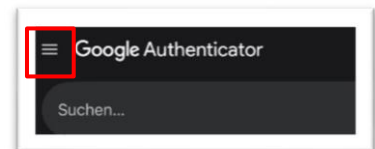
5. Smartphone-Wechsel Authenticator

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 müssen zur Hand sein. Die Google Authenticator App ist auf beiden Geräten installiert:

1. Öffnen Sie den Google Authenticator auf Ihrem **alten Smartphone**.
Tippen 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 Microsoft Authenticator

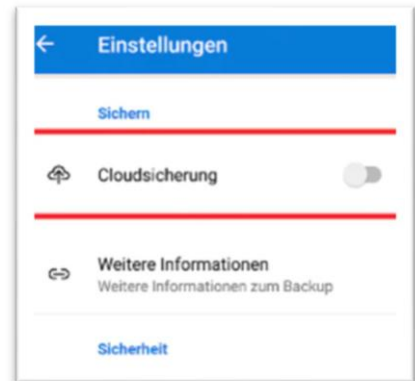
1. Öffnen Sie auf Ihrem **alten** Gerät die Authenticator App.

2. Tippen 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. Wird die App auf einem iPhone genutzt, muss zudem die Sicherung in der iCloud aktiviert sein.



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 Free OTP Authenticator



Achtung:

→FreeOTP bietet keine Cloud-Backups.

Das bedeutet: Beim Gerätewechsel müssen 2FA-Konten **neu eingerichtet** werden.