

Inhalt

1 Einleitung	2
2 Wofür die Zwei-Faktor-Authentifizierung	2
3 Apps für die Token Generierung.....	2
4 Zwei-Faktor-Authentifizierung im EDMS einrichten	2
5 Weitere Informationen.....	6

1 Einleitung

Zur Erhöhung der Sicherheit und dem besseren Schutz Ihrer sensiblen Projektdokumente auf unserem **DBFZ Dokumentenmanagementsystem „EDMS“** führen wir eine Zwei-Faktor Authentifizierung, kurz 2FA, ein.

2 Warum Zwei-Faktor-Authentifizierung

Wie Sie sicher schon aus anderen Bereichen z.B. Online-Banking wissen, wird bei der 2-Faktor-Authentifizierung ein zusätzliches Authentifizierungsmerkmal genutzt. Dieses zusätzliche Merkmal in Form eines Zugangstoken, muss auf Ihrem Smartphone in einer App generiert werden.

Der Token wird nach der Abfrage von Ihrem EDMS Benutzernamen und Kennwort zusätzlich abgefragt. Somit kann verhindert werden, dass ein Hacker nur mit Ihren Zugangsdaten unbefugt auf die Projektdokumente zugreifen kann. Erst mit dem zusätzlichen physischen Zugriff auf Ihr Smartphone könnte ein Unbefugter sich am EDMS anmelden.

3 Apps für die Token Generierung

Es gibt eine Reihe von Apps um ein Token zu generieren. Sie können dafür FreeOTP, Google Authenticator oder eine andere App Ihrer Wahl verwenden. Installieren Sie sich die App über den offiziellen App Store Ihres Smartphones.

4 Zwei-Faktor-Authentifizierung im EDMS einrichten

Sie können schon jetzt die Zwei-Faktor-Authentifizierung nutzen und in Ihrem EDMS Profil aktivieren. Dazu klicken Sie rechts oben auf Ihre Benutzersymbol (1) und klicken auf „Einstellungen“ (2). Danach klicken Sie im linken Menü auf „Zwei-Faktor-Authentifizierung“ (3) oder scrollen nach unten und aktivieren die Zwei-Faktor-Authentifizierung (4).




EDMS

- Profil
- Passwort
- Sprache
- E-Mail-Benachrichtigung
- Zwei-Faktor-Authentifizierung**
- Benutzerkonto löschen

Einstellungen

E-Mail-Benachrichtigung

E-Mail-Benachrichtigung über geänderte Dateien

Die Liste mit den neuen, gelöschten oder veränderten Dateien wird an Ihre E-Mail-Adresse verschickt.

- ☒ Keine E-Mails schicken
- ☐ Stündlich
- ☐ Alle 4 Stunden
- ☐ Täglich
- ☐ Wöchentlich

E-Mail-Benachrichtigungen über die Zusammenarbeit

Wollen Sie Benachrichtigungen über die Zusammenarbeit (z.B. Bibliotheksfreigabe, Gruppenaufnahme) per E-Mail erhalten?

- ☐ Keine E-Mails schicken
- ☒ Stündlich (Wenn Benachrichtigungen nicht innerhalb einer Stunde gelesen werden, dann erhalten Sie eine E-Mail-Benachrichtigung.)

[Absenden](#)

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung wurde für Ihren Account nicht aktiviert. Für einen zusätzlichen Schutz Ihres Accounts aktivieren Sie die Zwei-Faktor-Authentifizierung.

[Zwei-Faktor-Authentifizierung aktivieren](#)

Benutzerkonto löschen

Dieser Vorgang kann nicht rückgängig gemacht werden. Bitte seien Sie sicher, was Sie tun!

[Löschen](#)

Nun müssen Sie den angezeigten QR-Code / Barcode mit der App „Google Authenticator“, „FreeOTP“ oder einer anderen Token-App scannen.

Zwei-Faktor-Authentifizierung aktivieren

Um einen Token-Generator zu verwenden, öffnen Sie bitte die gewünschte App auf einem Smartphone, z.B. Google Authenticator, und scannen Sie den QR-Code hier. Geben Sie anschließend das generierte Token unten ein.



Token:

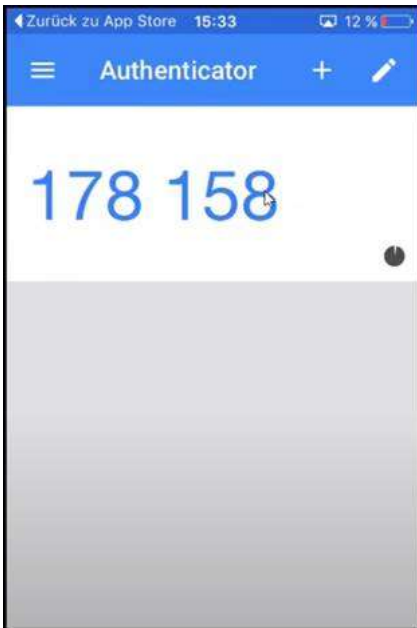
[Abbrechen](#) [Nächste Seite](#)

Öffnen Sie dazu zum Beispiel die App „Google Authenticator“, klicken auf „Einrichtung starten“ und „Barcode (QR-Code) scannen“.



Gehen Sie mit der Kamera auf den QR-Code und es wird automatisch ein neuer Eintrag für das EDMS-DBFZ angelegt und ein 6-stelliger Zahlencode angezeigt. Beachten Sie, dass der Zahlencode alle paar Sekunden neu generiert wird.





Diesen generierten Code geben Sie vor Ablauf der Zeit auf der EDMS Seite ein und klicken auf „Nächste Seite“.

Zwei-Faktor-Authentifizierung aktivieren

Um einen Token-Generator zu verwenden, öffnen Sie bitte die gewünschte App auf einem Smartphone, z.B. Google Authenticator, und scannen Sie den QR-Code hier. Geben Sie anschließend das generierte Token unten ein.



Token:

178158

Speichern Sie sich die Ersatz-Token und klicken auf „Zurück“.

Ersatz-Token

Ersatz-Token können verwendet werden, falls keine Primäre Authentifizierungsmethode verfügbar ist. Die folgenden Token können jeweils einmal für die Anmeldung verwendet werden. Falls alle Ersatz-Token aufgebraucht sind, können hier neue generiert werden. Nur die hier gelisteten Token sind gültig.

zqifykk6
 47jnmj5l
 gjj6rmic
 zozcxuol
 cv7jnzrj
 kmwykbe6
 sfxuq26t
 yfyrb6iu
 ttzcahir
 5k65cnga

Diese Token sollten ausgedruckt und an einem sicheren Ort aufbewahrt werden.

Zurück
Token generieren

Hinweis - Falls Sie Ihr Smartphone mal nicht zur Hand haben

Sie können sich mit Hilfe dieser Ersatz-Token am EDMS anmelden, obwohl Sie gerade das Smartphone nicht zur Hand haben und ein Token generieren können. Speichern Sie diese Liste von Token sicher ab und bei Bedarf nutzen Sie einer dieser Ersatz-Token bei der nächsten Anmeldung.

5 Weitere Informationen

Was ist 2FA:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html (HTML)

Video des Herstellers zur Aktivierung der 2FA:

<https://youtu.be/s5U9R34xMI8?t=76> (Video)