Hinweise zur Einführung der Zwei-Faktor-Authentifizierung (2FA) bei der Anmeldung an die GDI-DE Testsuite

Aus Sicherheitsgründen wird mit der Bereitstellung des aktuellen Releases für die Anmeldung an der GDI-DE Testsuite eine Zwei-Faktor-Authentisierung (2FA) eingeführt.

Eine Zwei-Faktor-Authentisierung bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

Im Zuge der Authentisierung wird ein wechselnder Schlüsselcode, ein sogenannter Token, generiert und ist als zusätzliche Eingabe zu den Login-Daten (Benutzername / Passwort)erforderlich.

Die Generierung des Tokens kann mit Browser-Plug-Ins oder mit Smartphone-Apps erfolgen.

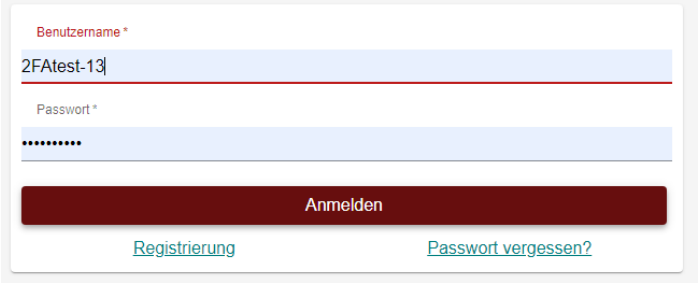
Ein empfehlenswertes browserbasiertes Plug-In für eine Zwei-Faktor-Authentisierung ist eine Browser-Erweiterung namens 'Authenticator' (unterstützt von Chromium & Mozilla Firefox)

Empfehlenswerte Smartphone-APPs sind Google Authenticator, Microsoft Authenticator oder Authy

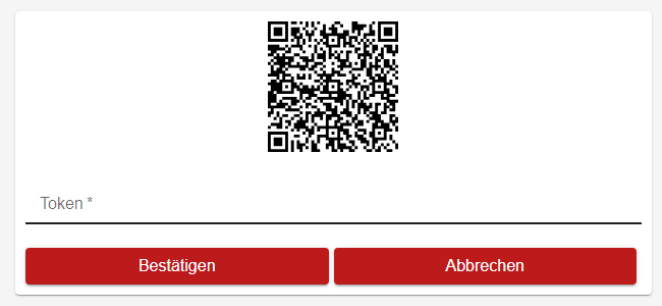
Jeder Anmeldevorgang benötigt einen eigenen Token, d. h. für jede Sitzung muss per Browser-Plug-In oder Smartphone-App ein neuer Token erstellt werden. Ein Token ist in seiner Gültigkeit auf eine bestimmte Zeit begrenzt und muss daher zeitnah in das Anmeldeformular eingetragen werden.

Vorgehensweise bei der Erstanmeldung mit einem vorhandenen Benutzeraccount nach erfolgter Aktivierung 2FA in der GDI-DE Testsuite.

Trägt der Nutzer seine bisherigen Login-Daten erstmalig in das Anmeldeformular ein, erkennt das System automatisch den 2FA-Status



und zeigt nach dem betätigen des „Anmelden“-Buttons das nachfolgende Fenster mit einem QR-Code und einem Eingabefeld für den Token an:

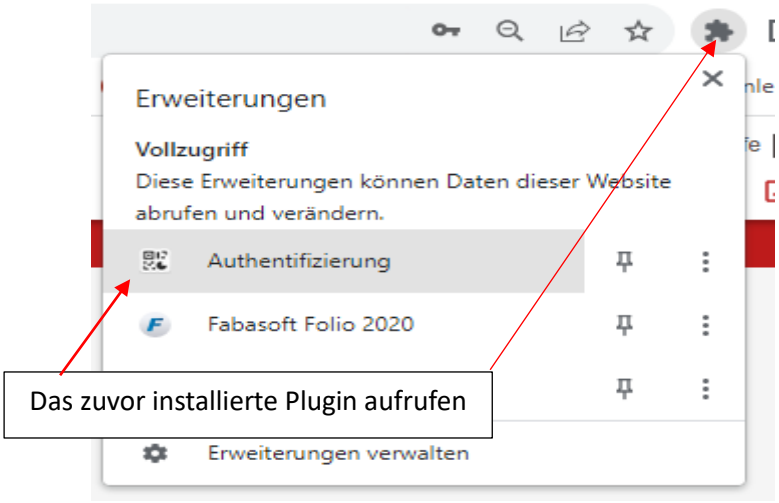


Dieser QR-Code wird nur bei der ersten Anmeldung angezeigt. Mithilfe des Plug-Ins oder der Handy-App wird der QR-Code gescannt und ein neues Konto für die GDI-DE Testsuite erstellt. Damit wird ein zeitbasierter Token erstellt, der ab sofort bei jeder Anmeldung neu abgerufen und eingegeben werden kann.

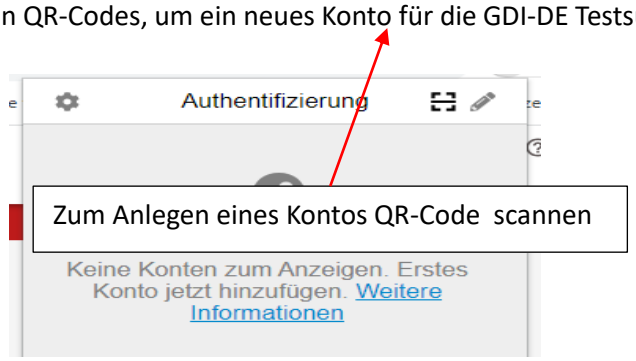
Die einzelnen Schritte am Beispiel des Chrome-Browser-Plugins

(analoges Vorgehen bei anderen Plugins oder Smartphone.Apps)

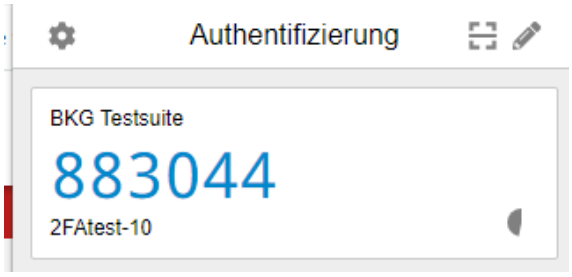
1. Aufruf des Plugins



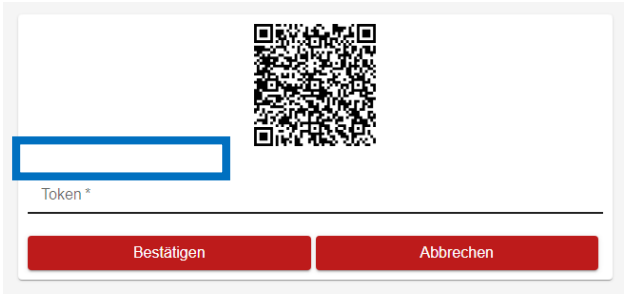
2. Scannen des angezeigten QR-Codes, um ein neues Konto für die GDI-DE Testsuite zu erstellen:



3. Nach erfolgreichem Scan wird das aktuelle Token für die GDI-Testsuite im Plugin angezeigt



4. Anmeldung mit der Eingabe des aktuellen Tokens abschließen



Nach Eingabe des Tokens schließt der Nutzer den Anmeldevorgang mit Klick auf 'Bestätigen' ab. Ist das Token korrekt, wird für das Benutzerkonto die 2FA initialisiert und der Nutzer automatisch zur Übersichtstabelle der Test weitergeleitet.

5. Bei jeder erneuten Anmeldung wird nach dem Passwort nur noch die Eingabe eines aktuellen Tokens erwartet:

Das Fenster zur Tokeneingabe erscheint nur, wenn ein **korrektes Passwort** eingegeben wurde.