

Zwei-Faktor-Authentifizierung

Referentin: Angelika Müller

www.bluespice.com



Definition & Hintergrund

Die Zwei-Faktor-Authentifizierung (2FA) ist ein Identifikationsnachweis des Benutzers über zwei unterschiedliche und insbesondere unabhängige Komponenten

Hintergrund: Zugangssicherung

Problem: zu schwache und/oder mehrfach verwendete Passwörter

Gefahr: kompromittierte Passwörter

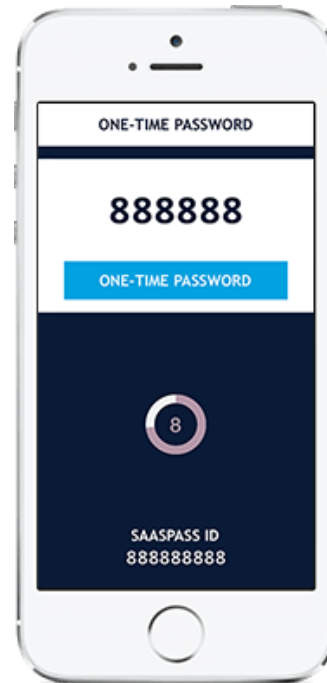
Lösung zweiter Faktor:

- Geheimnishütender Gegenstand: physikalischer Token-Generator (Stick etc.)
- Geheimes Wissen: Einmalpasswort, Transaktionsnummer (TAN), etc.
- Biometrische Charakteristika: Fingerabdruck, Gesichtserkennung, Iris-Scan etc.

Beispiele für unabhängige Komponenten



Geheimnishütender Gegenstand
(Token-Generator)



Geheimes Wissen
(Einmalpasswort)



Biometrisch
(Fingerabdruck)

2FA mit BlueSpice 4

Technische Basis (standardmäßig aktiviert seit BlueSpice 4.1)

- OATHAuth = Authentifizierung mit HMAC-gestützten Einmalpasswörtern
- Webauthn = unterstützt FIDO und Webauthn für z.B. FIDO-Sticks, Windows Hello! (Biometrie)



Achtung! Die 2FA schließt ein Single Sign-on kategorisch aus, da es sich faktisch um zwei konkurrierende Authentifizierungsmechanismen handelt.

Konfiguration

- Benutzereinstellungen
 - Benutzerdaten
 - Zwei-Faktor-Authentifizierung verwalten

Verfügbare Methoden

[Aktivieren](#) TOTP (Einmal-Token)

Der zeitbasierte Einmalpasswortalgorithmus (TOTP) ist eine Erweiterung des HMAC-basierten Einmalpasswortalgorithmus (HOTP), der ein Einmalpasswort generiert, indem die Eindeutigkeit der aktuellen Zeit verwendet wird.

[Aktivieren](#) Web-Authentifizierung (WebAuthn)


WebAuthn (Web Authentication) ist ein vom World Wide Web Consortium (W3C) veröffentlichter Webstandard. WebAuthn ist eine Kernkomponente des FIDO2-Projekts unter Leitung der FIDO Alliance. Ziel des Projekts ist die Standardisierung einer Schnittstelle zur Authentifizierung von Benutzern für webbasierte Anwendungen und Dienste mithilfe von Public-Key-Kryptografie. [Weiterlesen](#)

Beispiel Einmalpasswort

Enable TOTP (one-time token)
--- Special:Manage Two-factor authentication

Step 1: Download a two-factor authentication program
Download a program for two-factor authentication. That can be a mobile application (such as Google Authenticator) or a desktop application.

Step 2: Scan the QR code



Or enter the secret manually:
Account name:
Rail

Two-factor authentication secret key:
JU3C BQ2X X45X BV1Y

Step 3: Write down the scratch codes
The following list is a list of one-time use scratch tokens. These tokens can only be used once, and are for emergency use. Please write these down and keep them in a secure location. If you lose your phone, these tokens are the only way to rescue your account. **These tokens will never be shown again.**

- YPSY SC2K RC7G SOHU
- XQV6 MCLC BVGM S3TE
- X3L2 RTB7 EUKX Q3RK
- V7TE ZSVL AHDP TH56
- IBNM AWS5 BMS2 FBTA
- ABV7 F3GS EM4G NAC2
- SPQK Y2AR QMIO GK3T
- OD5S N2NH 3RH5 TH50
- CVWW M2Q5 MBB5 RB46
- 3H1Q NPAA ZPQ2 GD4R

Step 4: Verification
Enter a code from your authentication device to verify.

Systeme connecten

Log in

Log in

You must have cookies enabled to log in to Labs Test.

Username:

Password:

Your domain:

Token

Remember my login on this browser (for a maximum of 180 days)

[Forgotten your login details?](#)

Anmeldung mit Token