BlueSpice MediaWiki | Summit

11. & 12. Mai 2022

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

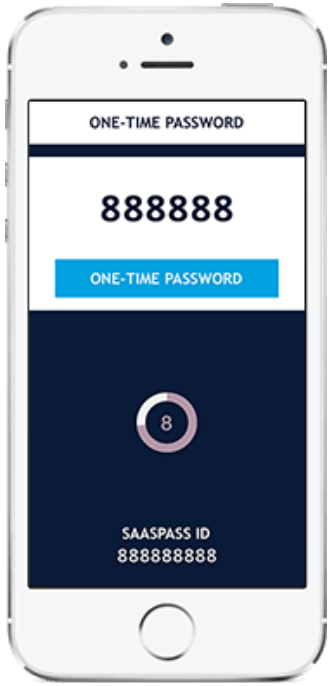
Gefahr: kompromittierte Passwörter

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

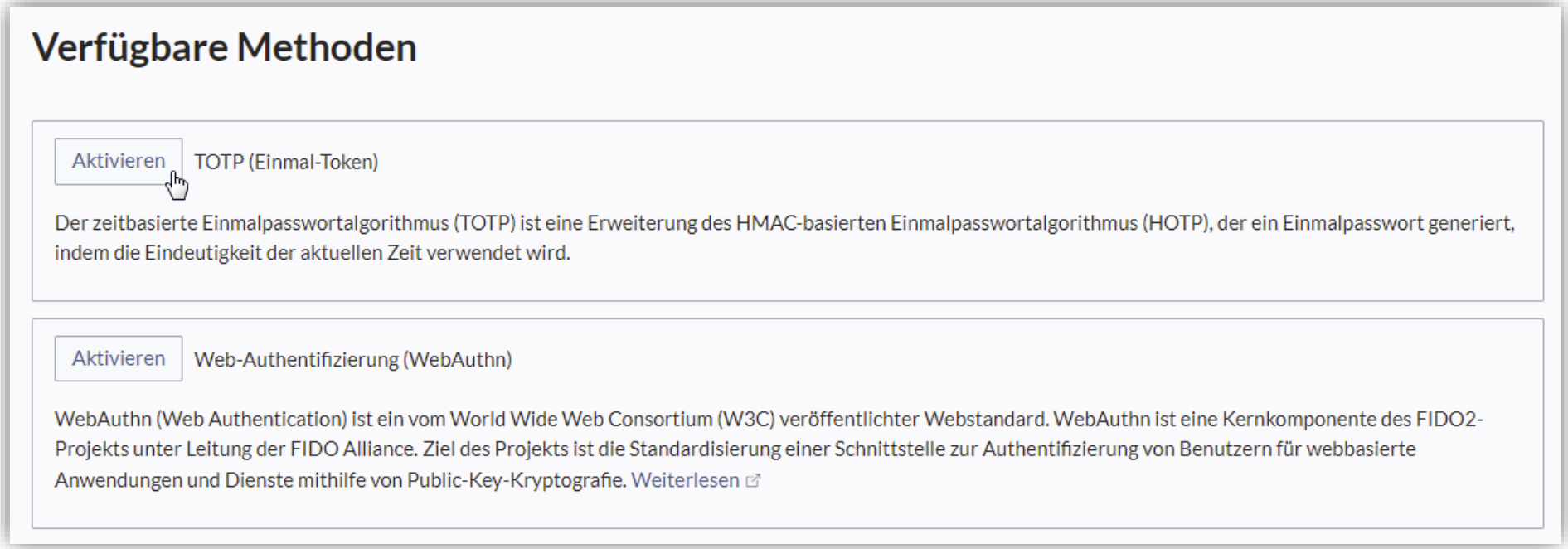
Technische Basis (standardmäßig aktiviert seit BlueSpice 4.1)

- 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.

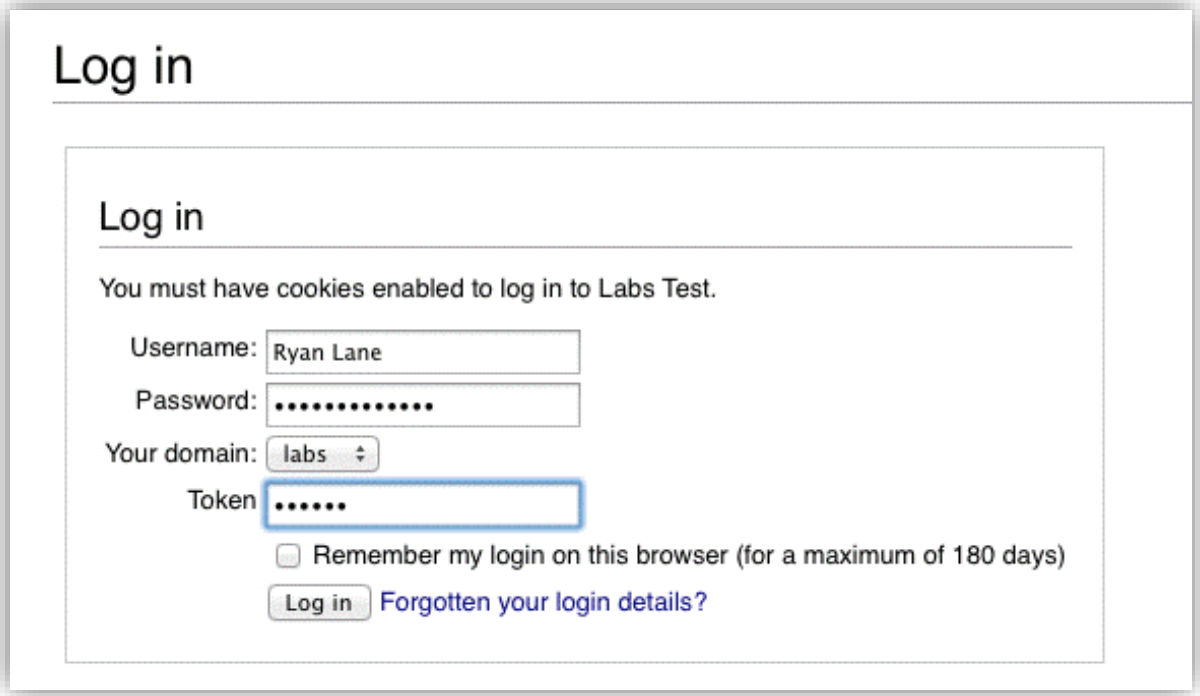
Konfiguration

- Benutzereinstellungen
  - Benutzerdaten
    - Zwei-Faktor-Authentifizierung verwalten



Beispiel Einmalpasswort

Systeme connecten



Anmeldung mit Token