Nutzerdokumentation

- Single-Sign-On

Single-Sign-On

Authentik (sso.fsrvi.de) dient als zentrale Login-Möglichkeit für Dienste des FSR VI. Um einen Account zu erhalten benötigst du eine Einladung, wende dich dazu an die IT.

Multi-Faktor-Authentisierung (MFA)

Alle Nutzer*innen müssen Multi-Faktor-Authentisierung (MFA), auch bekannt als Zwei-Faktor-Authentisierung (2fa), einrichten.

MFA schützt den Account auch bei Abhandenkommen des Passworts vor Missbrauch, in dem ein weiterer Faktor („Besitz“) als Ergänzung zum Faktor „Wissen“ (dem Passwort) hinzukommt.

Du kannst mehrere Methoden oder Geräte als Faktor hinterlegen, bei der Anmeldung benötigst du nur eins. Du wirst bei der Registrierung/Login automatisch aufgefordert ein Gerät einzurichten. In deinem Konto kannst du Geräte hinzufügen oder löschen.

Für eine MFA stehen in Authentik zwei Möglichkeiten zur Verfügung:

Authenticator-App (TOTP)

Bei dieser Authentisierungsmethode wird eine App verwendet, die anhand eines Geheimnisses und der Uhrzeit alle 30 Sekunden einen neuen Zahlencode erzeugt. Beim Login muss der aktuelle Code angegeben werden.

Als Verfahren wird TOTP (Time-based one-time password) verwendet. TOTP ist ein Standard, der von verschiedenen Apps (und sogar Hardware-Geräten) implementiert wird.

Genutzt werden kann jede beliebige App, die TOTP unterstützt. Empfehlenswerte Apps sind bspw. 2fas, FreeOTP oder Aegis (alle Open Source). Aber auch Apps wie der Google Authenticator, Microsoft Authenticator o.Ä. können benutzt werden. Auch viele Passwortmanager unterstützen TOTP, allerdings erhöht das Verwenden des Passwortmanagers das Risiko, dass beide Faktoren zusammen abhanden kommen.

Das Hinzufügen des Authentik-Accounts zur Authenticator-App erfolgt durch scannen des angezeigten QR-Codes mit der App, oder manuell durch Übetragung des angezeigten Geheimnisses. Zu Bestätigung muss ein aktueller Code eingegeben werden.

WebAuthn/FIDO2/Passkeys

WebAuthn ist ein Webstandard für eine sichere und bequeme Anmeldung im Web. In Zukunft wird es in vielen Bereichen Passwörter komplett ersetzen. Passkeys sind eine Implementierung von WebAuthn, FIDO2 der zugrunde liegende Standard.

WebAuthn arbeitet mit Public-Key-Kryptografie und verwendet entweder einen FIDO2-kompatiblen Hardware-Dongle (bspw. Yubikey, Nitrokey, Token2, …) oder Funktionen des Betriebssystems/Browsers (Apple Keychain, Google Chrome/Android Passwortmanager, Windows Hello) zur Authentifizierung.

Der*die Nutzer*in authentisiert sich gegenüber dem Gerät (bspw. mit Fingerabdruck oder PIN) und dieses bestätigt der Webseite kryptografisch die erfolgreiche Authentisierung. Dabei kann Phishing technisch nahezu ausgeschlossen werden.

Ob dein Gerät Unterstützung für WebAuthn bietet probierst du am besten durch Hinzufügen eines WebAuthn-Gerätes aus.

Mehr Infos zu Passkeys findest du beim BSI oder heise.