Welche MFA-Methoden unterstützt Bare.ID?

Tolleiv Nietsch - 2026-11-05 - Fragen zum Produkt

> **Hinweis**: Dieses Feature muss erst für Dein Konto freigeschaltet werden und ist ggf. nicht Teil Deiner Buchung. Bitte wende Dich bei Fragen an den Kundensupport.

In den Authentifizierungs-Flows legst Du für jede Authentifizierungsstärke fest, welche Anmeldearten akzeptiert werden. Jede Anmeldeart besteht aus einer **Primären Methode**, die den Login startet und den Nutzer identifiziert, und optional aus **Erforderlichen zweiten Faktoren**, die den Login anschließend bestätigen.

Dieser Artikel listet alle Methoden auf, die Du dort auswählen kannst, und ordnet ein, ob eine Methode im Sinne der Mehr-Faktor-Authentifizierung (MFA) als ein oder als zwei Faktoren zählt.

Was zählt als Faktor?

Bei der MFA wird die Identität eines Nutzers durch mehrere unabhängige Faktoren überprüft. Ein Faktor gehört zu einer dieser Kategorien:

- **Wissen:** etwas, das nur der Nutzer weiß, z. B. ein Passwort oder eine PIN.
- **Besitz:** etwas, das nur der Nutzer hat, z. B. ein Smartphone, ein Sicherheitsschlüssel oder der Zugang zu einem E-Mail-Postfach.
- **Eigenschaft:** ein biometrisches Merkmal des Nutzers, z. B. ein Fingerabdruck oder das Gesicht.

Eine Anmeldung ist erst dann eine MFA, wenn mindestens zwei Faktoren aus **unterschiedlichen** Kategorien geprüft werden. Bare.ID zählt dabei keine Faktoren für Dich: Ob eine Stärke MFA erfordert, ergibt sich allein aus den Anmeldearten, die Du für sie festlegst. Die folgende Einordnung hilft Dir, diese Anmeldearten passend zusammenzustellen.

Übersicht

Methode	Verwendung	Zählt als	Phishing-resistent
Passkey	Primär	2 Faktoren[1]	ja
Passwort	Primär	1 Faktor	nein
E-Mail Magic Link	Primär	1 Faktor	nein
Kerberos	Primär	1 Faktor	nein
Zertifikat	Primär	1 Faktor	ja
Identity Provider	Primär	1 Faktor[2]	nein
Authenticator-App	Zweiter Faktor	1 Faktor	nein
E-Mail-Code	Zweiter Faktor	1 Faktor	nein
SMS-Code	Zweiter Faktor	1 Faktor	nein
Sicherheitsschlüssel	Zweiter Faktor	1 Faktor	ja
Wiederherstellungscode	Zweiter Faktor	1 Faktor	nein

[1] Nur wenn im Reiter “Authentifizierungsmethoden” für den Passkey die “Nutzerverifizierung” auf “Erforderlich” steht. Andernfalls zählt der Passkey als 1 Faktor.

[2] Eine MFA, die der Nutzer beim Identity Provider selbst durchläuft, wird in Bare.ID nicht als weiterer Faktor angerechnet.

Phishing-resistente Methoden sind kryptografisch an die Anmeldeseite gebunden. Die Anmeldedaten können

weder abgefangen noch auf einer gefälschten Anmeldeseite wiederverwendet werden.

Primäre Methoden

Primäre Methoden starten einen Login und identifizieren den Nutzer. Jede Anmeldeart beginnt mit genau einer Primären Methode.

Passkey

Zählt als: 2 Faktoren (Besitz und Wissen oder Eigenschaft)

Der Nutzer meldet sich ohne Passwort mit einem Passkey (WebAuthn) an, der auf seinem Gerät oder einem Sicherheitsschlüssel gespeichert ist. Der Besitz des Passkeys ist der erste Faktor. Gibt der Nutzer den Passkey zusätzlich per Geräte-PIN oder Biometrie frei, ist das der zweite Faktor.

Diese Freigabe ist nur garantiert, wenn die “Nutzerverifizierung” des Passkeys im Reiter “Authentifizierungsmethoden” auf “Erforderlich” steht. Bei “Bevorzugt” oder “Nicht empfohlen” kann der Login auch ohne Freigabe gelingen, dann zählt der Passkey nur als 1 Faktor.

Mehr zur passwortlosen Anmeldung findest Du im Artikel Was ist passwortlose Authentifizierung?.

Passwort

Zählt als: 1 Faktor (Wissen)

Die klassische Anmeldung mit einem geheimen Passwort. Optional prüft “haveIBeenPwned (HIBP)”, ob das Passwort in bekannten Datenlecks aufgetaucht ist, und eine Passwortrichtlinie erzwingt Mindestanforderungen an das Passwort. Für eine MFA kombinierst Du das Passwort mit einem zweiten Faktor, z. B. der Authenticator-App.

E-Mail Magic Link

Zählt als: 1 Faktor (Besitz)

Der Nutzer erhält einen einmaligen Anmeldelink an seine E-Mail-Adresse und bestätigt die Anmeldung mit einem Klick darauf. Damit weist er den Zugang zu seinem E-Mail-Postfach nach. Der Link ist nur für eine begrenzte Zeit gültig.

Kerberos

Zählt als: 1 Faktor (Besitz)

Der Nutzer wird automatisch über seine bestehende Windows-/Kerberos-Sitzung angemeldet, noch bevor das Benutzernamen-Formular erscheint. Damit weist er nach, dass er an einem Gerät seiner Organisation angemeldet ist. Wie die Anmeldung an Windows selbst abgesichert wurde, kann Bare.ID nicht erkennen. Kerberos zählt daher als 1 Faktor.

Zertifikat

Zählt als: 1 Faktor (Besitz)

Der Nutzer meldet sich mit einem Client-TLS-Zertifikat an, das ihn identifiziert. Im Reiter “Authentifizierungsmethoden” heißt diese Methode “TLS-Zertifikat”. Das Zertifikat belegt den Besitz des Geräts oder der Smartcard, auf dem es gespeichert ist.

Identity Provider

Zählt als: 1 Faktor

Der Nutzer meldet sich über einen verbundenen Login Provider an. Im Reiter “Authentifizierungsmethoden” heißt diese Methode “Login Provider”. Auch wenn der Nutzer beim Login Provider selbst mehrere Faktoren nutzt, zählt die Anmeldung in Bare.ID als 1 Faktor. Wenn Du für Anmeldungen über einen Login Provider eine MFA verlangen willst, kombiniere die Methode mit einem zweiten Faktor.

Zweite Faktoren

Zweite Faktoren bestätigen einen Login nach der Primären Methode. Einen Login allein starten können zweite Faktoren nicht.

Authenticator-App

Zählt als: 1 Faktor (Besitz)

Eine Authenticator-App (z. B. Google Authenticator oder 1Password) erzeugt auf dem Smartphone des Nutzers regelmäßig einen neuen Einmalcode (TOTP). Zur Anmeldung gibt der Nutzer den aktuell angezeigten Code ein. Mehr dazu findest Du unter Einmalpasswort (OTP) per Authenticator-App.

E-Mail-Code

Zählt als: 1 Faktor (Besitz)

Ein Einmalcode wird an die E-Mail-Adresse des Nutzers gesendet, den dieser zur Bestätigung eingibt. Mehr dazu findest Du unter Einmalpasswort (OTP) per E-Mail.

> **Hinweis**: Der E-Mail-Code hängt von der erfolgreichen Zustellung der E-Mail ab. Wenn die Zustellung für manche Nutzer verzögert oder unzuverlässig ist, konfiguriere weitere Methoden wie die Authenticator-App, Passkeys oder Wiederherstellungscodes.

SMS-Code

Zählt als: 1 Faktor (Besitz)

Ein Einmalcode wird per SMS an die hinterlegte Mobilfunknummer des Nutzers gesendet, den dieser zur Bestätigung eingibt. Mehr dazu findest Du unter Einmalpasswort (OTP) per SMS.

Sicherheitsschlüssel

Zählt als: 1 Faktor (Besitz)

Der Nutzer bestätigt die Anmeldung mit einem Sicherheitsschlüssel (WebAuthn), z. B. einem FIDO-Token. Anders als der Passkey dient der Sicherheitsschlüssel nur als zweiter Faktor und ersetzt kein Passwort. Mehr dazu findest Du im Kapitel Mehr-Faktor-Authentifizierung.

Wiederherstellungscode

Zählt als: 1 Faktor

Eine Liste vorab erzeugter Einmalcodes, die der Nutzer sicher aufbewahrt. Er nutzt einen Code, wenn ein anderer zweiter Faktor (z. B. das Smartphone) nicht verfügbar ist. Jeder Code lässt sich nur einmal verwenden. Mehr dazu findest Du unter Einrichten von Recovery-Codes erlauben.

Hinweise zur Zusammenstellung

- Zwei Methoden aus derselben Kategorie ergeben keine MFA. Kombinierst Du z. B. “E-Mail Magic Link” mit “E-Mail-Code”, hängen beide vom selben E-Mail-Postfach ab. Wer Zugriff auf das Postfach hat, erfüllt beide.

- Ein Passkey mit der “Nutzerverifizierung” “Erforderlich” erfüllt eine MFA bereits allein. Eine Anmeldeart, die nur aus einem Passkey besteht, ist damit eine vollwertige Alternative zu Passwort und zweitem Faktor.

- Die Methoden “Zertifikat”, “Kerberos” und “SMS-Code” müssen ggf. erst für Dein Konto freigeschaltet werden und sind ggf. nicht Teil Deiner Buchung. Ist eine Methode nicht gebucht, steht sie in den Authentifizierungs-Flows nicht zur Auswahl.

> ***Wie Du Stärken, Richtlinien und die Standardregel einrichtest, beschreiben die Kapitel Authentifizierungs-Flows und Step-up-Authentifizierung des Bare.ID-Handbuchs.***