# Federated Authentication

## Eine Identität für unterschiedlichste Anwendungen

War es bislang für Anwender üblich, sich bei jeder Anwendung und digitalem Dienst individuell zu authentifizieren, ist dies bei der großen Anzahl und Vielfalt heutiger Angebote nicht mehr überschaubar. Entsprechend streben die Anwender nach einem vereinfachten Identitätsmanagement. Gleichzeitig erzwingen gesetzliche Regularien wie die DSGVO von den Anwendungs- und Dienstanbietern den besonderen Schutz der Identitätsinformationen der Anwender. Federated Authentication verspricht hohe Sicherheit und trotzdem einfache Bedienung.

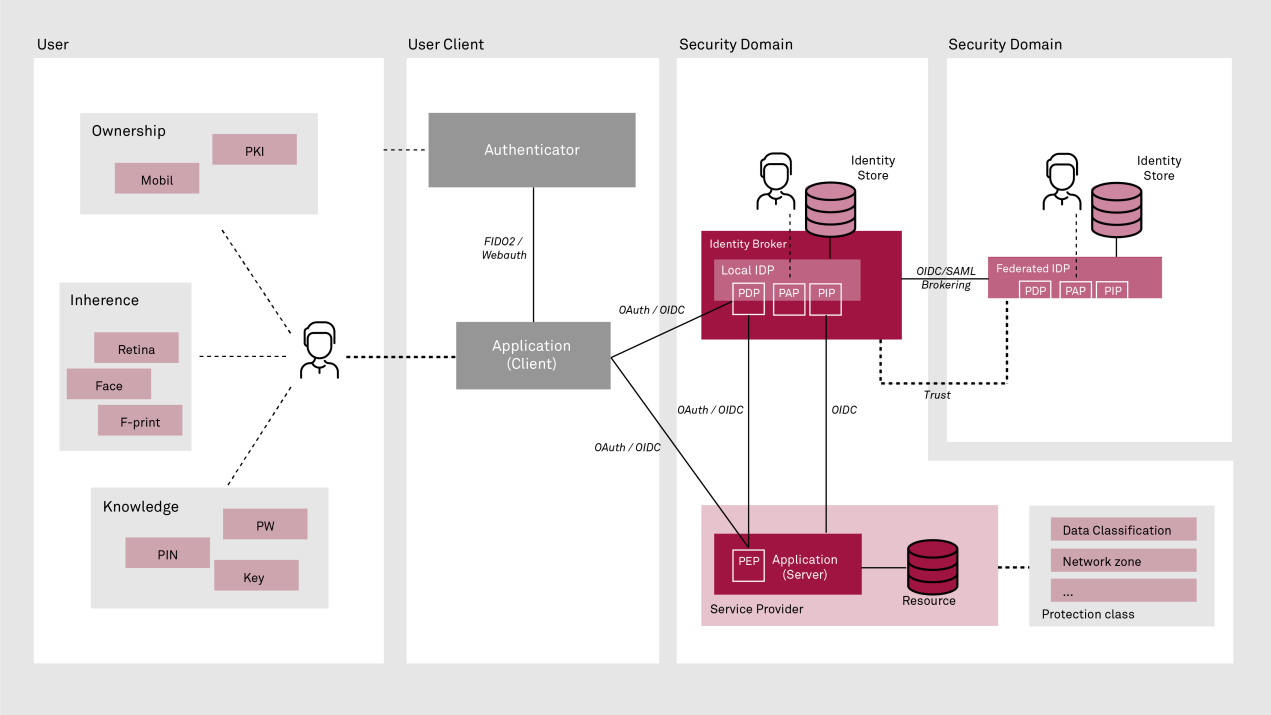
### Definition

Federated Authentication beschreibt die Authentifizierung von Anwendern bei unterschiedlichen Anwendungen und Diensten unter Verwendung zentraler Identitätsverwalter über Sicherheitdomänen hinweg.

Klassischerweise verwaltet jede Anwendung die Identitätsinformationen der Anwender selbstständig und ist damit auch für die Authentifizierung dieser Anwender selbst verantwortlich. Werden mehrere Anwendungen durch dieselbe Person benutzt, müssen die Anwender oder Anbieter diese Identitätsinformationen mehrfach pflegen und synchronisieren. Die Folge: Für jede Anwendung ist eine individuelle Authentifizierung notwendig.

Ein erster Lösungsschritt ist Single-sign-on, kurz #SSO. Innerhalb einer Sicherheitsdomäne, etwa einem Unternehmen, stellt ein Identitätsanbieter einen zentralen Dienst bereit. Dieser Identitätsanbieter verwaltet die Identitätsinformationen der Anwender für alle Anwendungen und ermöglicht gleichzeitig die Authentifizierung der Anwender. Das entbindet die Anwendungen von der Pflicht einer eigenen Identitätsverwaltung, setzt aber auch ein striktes Vertrauensverhältnis zwischen Anwendung und Identitätsanbieter voraus.

Aufgrund der stärkeren Vernetzung von Anwendungen und Diensten sind Anwender nicht mehr nur in einer sondern vielen verschiedenen Sicherheitsdomänen aktiv, etwa unterschiedlichen Unternehmen, sozialen Netzwerken und Medien



oder Cloud- und Plattformlösungen. Jede dieser Sicherheitsdomänen verfügt über eigene Identitätsanbieter, mit eigenen Identitätsinformationen und wiederum eigenen Authentifizierungsdiensten. Damit verlagert sich das Problem der Mehrfachidentitäten und mehrfachen Pflege schlicht auf eine höhere Ebene.

Hier greift Federated Authentication. Es schaltet dem Identitätsanbieter einer Sicherheitsdomäne einen Identitätsmakler vor, der zwischen dem Identitätsanbieter der lokalen Sicherheitsdomäne und den Identitätsanbietern anderer Sicherheitsdomänen vermittelt. Dieses Verfahren ermöglicht es, den Authentifizierungsdienst einer anderen Sicherheitsdomäne zu verwenden, Identitätsinformationen aus dieser zu übernehmen und eine zusammengefasste Identität zu etablieren. Beispiele dafür wären "Sign in with Facebook", "Google Sign-in" oder "Sign in with Apple". Federated Authentication setzt ein Vertrauensverhältnis zwischen dem Identitätsmakler und den Identitätsanbietern der Sicherheitsdomänen voraus.

Mit der Verteilung von Identitätsinformationen steigt das Risiko des Missbrauchs. Der sichere Austausch der Identitätsinformationen ist daher entscheidend. Sicherstellen lässt er sich etwa durch etablierte Standards wie SAML2 und OAuth2, die mit kryptografischen Verfahren wie Verschlüsselung und Signatur arbeiten.

Immer häufiger sind auch Mehrfaktorauthentifizierungen anzutreffen. Neben dem Wissen über ein Geheimnis, etwa ein Kennwort, ziehen sie weitere Faktoren wie Besitz, Eigenschaft, Standort oder Zeit zur Authentifizierung hinzu. Zur Abfrage dieser Eigenschaften kommen beispielsweise Generatoren für Einmalkennwörter oder Fingerabdruckprüfungen zum Einsatz. Für deren standardisierte und sichere Einbindung in einen Authentifizierungsdienst spielen wiederum #FIDO2 und #WebAuthn eine zentrale Rolle.

**Technologien**

- Multi-Faktor-Authentifizierung (MFA)
- biometrische Verfahren
- Verschlüsselung und Signatur
- Federated Identity

**Produkte**

- Identitätsanbieter
- Identitätsvermittler
- Identitätsspeicher
- Authentikatoren

FAU

**Standards**

- OAuth 2.0
- OpenID Connect 1.0
- SAML 2.0
- FIDO2
- WebAuthn

**Herausforderungen**

- verteilte Anwendungen
- soziale Netzwerke
- Gesetzliche Anforderungen (DSGVO)
- Single-sing-on
- Cloud Deployment

## Referenzszenario

Die Mitarbeiter nutzen für ihre tägliche Arbeit eine Vielzahl von Unternehmensanwendungen. Jede dieser Anwendungen verwaltet die Identitätsmerkmale der Mitarbeiter selbst, um sie zu autorisieren. Die Identitätsinformationen der Mitarbeiter sind somit über viele Unternehmensanwendungen verteilt und zudem dupliziert gelagert. Die Mitarbeiter müssen sich deshalb vor der Nutzung bei jeder Anwendung gesondert authentifizieren. Die Pflege und Nachweispflicht im Sinne der DSGVO ist aufwändig. Ein zentraler Identitätsanbieter im Unternehmen löst diese Einschränkung auf. Gleichzeitig stellt das Unternehmen seine Anwendungen auch Anwendern außerhalb der eigenen Sicherheitsdomäne bereit, muss die Identitätsinformationen dieser Anwender aber innerhalb des Unternehmens verwalten, um sie DSGVO-konform behandeln zu können. Hier greifen dann Identitätsmakler.

## Potenzial

Aus Sicht der Anwender führt eine zentralisierte Identitätsverwaltung zu einer stark vereinfachten und verbesserten User Experience. Anwender müssen sich nur noch einmalig für alle verbundenen Anwendungen authentifizieren. Den Anwendern reichen dafür eine Benutzerkennung, ein Kennwort und ein zusätzliches Token. Änderungen an persönlichen Informationen nehmen Anwender und Administratoren einmalig zentral vor.Greifen die Unternehmensanwendungen zudem auf existierende Identitäten sozialer Netzwerke zurück, ermöglichen Sie den Anwendern die Anmeldung denen aus ihrem persönlichen Umfeld gewohnten Zugangsdaten.

Aus Sicht des Unternehmens führt eine zentrale Identitätsverwaltung zu einer massiven Vereinfachung der Administration und ermöglicht sogar eine zentrale Richtlinien- und Rechtesteuerung. Zugleich lassen sich Auflagen der DSGVO einfacher umsetzen. Der Rückgriff auf Logins sozialer Netzwerke entbindet das Unternehmen von der Aufgabe der Identitätsverwaltung für nicht zum Unternehmen gehörende Anwender. Ferner vereinfacht und vereinheitlicht es die Entwicklung neuer Anwedungen, da diese auf etablierte Authentifizierungsdienste

zurückgreifen können.

## Reifegrad

Für Federated Authentication existieren zahlreiche Produkte, die sowohl die Identitäten bereitstellen als auch vermitteln können. Standards wie #OAuth2 zur Abwicklung von Authentifizierungsprozessen sind ausgereift. Den Austausch der Identitätsinformationen übernehmen ebenso ausgereifte Standards wie #SAML2 oder #OpenID Connect. FÜr den Austausch der Identitätsmerkmale haben offene Gremien die Standards #FIDO2 und #WebAuthn nachgelegt. Es gibt eine Vielzahl von Client-Server-Bibliotheken, um auf OAuth2 oder OpenID Connect basierter Identitätslösungen in Anwendnungen einzubinden, oder um FIDO2-basierte Authentikatoren in Clients zu integrieren. Die Nutzung von Logins sozialer Netzwerke ist außerhalb von Unternehmen weitestgehend etabliert. Im Unternehmensumfeld hängt dies im Wesentlichen aber vom Vertrauen in Identitätsanbieter wie Facebook, Google, Apple oder Github ab.

Federated Authentication hat dementsprechend die Hype Phase bereits verlassen und ist auf dem Weg, sich als produktive, zuverlässige, sichere und kostensenkende Lösung zu etablieren.

## Marktübersicht

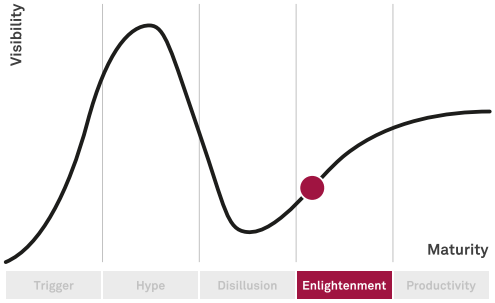
Produkte im Umfeld von Federated Authentication sind klassischerweise der Kategorie Identity & Access Management (IAM) zugeordnet. Hier gibt es zahlreiche kostenpflichte Lösungen auf dem Markt, die regelmäßig von Analysten untersucht werden. Auch Pordukte aus dem Open-Source-Bereich sind verfügbar. Zu den bekanntesten und verbreitetsten Lösungen gehören Redhead Keycloak (Open Source), Microsoft Azure AD, IBM Security Access Manager, Okta SSO, Oracle Access Manager,Ping Identity, Ping Federate und Ping Access sowie Auth0.

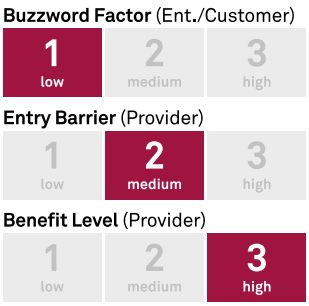
## Alternativen

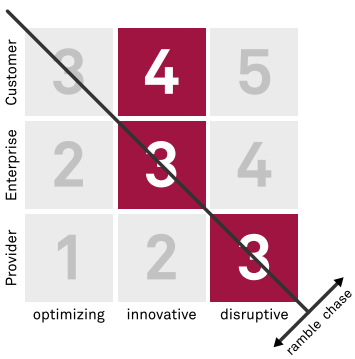
Alternativen zu Federated Authentication reichen von der klassischen lokalen Identitätsverwaltung über zentralisierte Benutzerverwaltungen mit lokaler Anmeldung bis hin zum zentralisierten Authentifizierungsdienst eines Identitätsanbieters. Bei der lokale Benutzerverwaltung und -authentifizierung nutzt die Anwendung einen eigenen Speicher für die Identitäten und übernimmt auch die Authentifizierung selbst. Die in Unternehmen derzeit verbreitete Lösung ist LDAP, bei der die Anwendungen auf einen zentralen Speicher für die Identitäten zurückgreifen, die Authentifizierung aber weiterhin selbst übernehmen. Zentrale Identitätsanbieter verwalten sowohl die Identitätan konsolidiert, übernehmen auch die Authentifizierung stellvertretend für die Anwendungen, sind dazu allerdings nur in der eigenen Sicherheitsdomäne in der Lage.

## Fazit

- \+ Funktionalität lässt sich auslagern
- \+ DSGVO-Aspekte sind zentralisiert abgedeckt
- \+ die User Experience steigt aufgrund von Vereinfachung
- \- Vertrauen ist notwendig
- \- Einhaltung organisatorischer Richtlinien erforderlich
- \- zentrale Infrastruktur notwendig
- \- erhöhtes Risiko bei Identitätsdiebstahl




https://msg.direct/techrefresh

Stand: September 2020

**msg systems ag**

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group