loginfactor

Identity & Access Management

Ein Login.
Zentrale Kontrolle.



Die Grundlage für sichere
und vernetzte digitale Services.

KI-generiert

Identitäten zentral verwalten

Identity & Access Management (IAM) schafft eine gemeinsame Basis für Benutzer und Zugriffe. Alle angebundenen Services nutzen dieselben verlässlichen Identitäten.

Benutzerdaten

Ein Profil über alle Services hinweg. Das IAM verbindet vorhandene Verzeichnisse und führende Systeme oder verwaltet Konten selbst. Zuständigkeiten für die Daten bleiben klar.

Anmeldemittel

Passwörter, Passkeys und weitere Anmeldeverfahren folgen gemeinsamen Regeln. Eigene Identity Provider können die Anmeldung übernehmen.

Rollen und Rechte

Das IAM stellt Rollen und Freigaben bereit. Anwendungen prüfen diese beim Zugriff und ergänzen ihre fachlichen Regeln.

EINE IDENTITÄTSINFRASTRUKTUR FÜR ALLE SERVICES



Vorhandene Verzeichnisse bleiben integrierbar.

Einmal anmelden.
Services nahtlos nutzen.

Single Sign-On (SSO) verbindet Ihre Anwendungen. Nutzer melden sich einmal an und wechseln anschließend zwischen freigegebenen Services.

SSO mit klaren Zugriffsgrenzen

Ein Login vereinfacht die Nutzung. Welche Daten und Funktionen erreichbar sind, bestimmen weiterhin die jeweiligen Rechte.

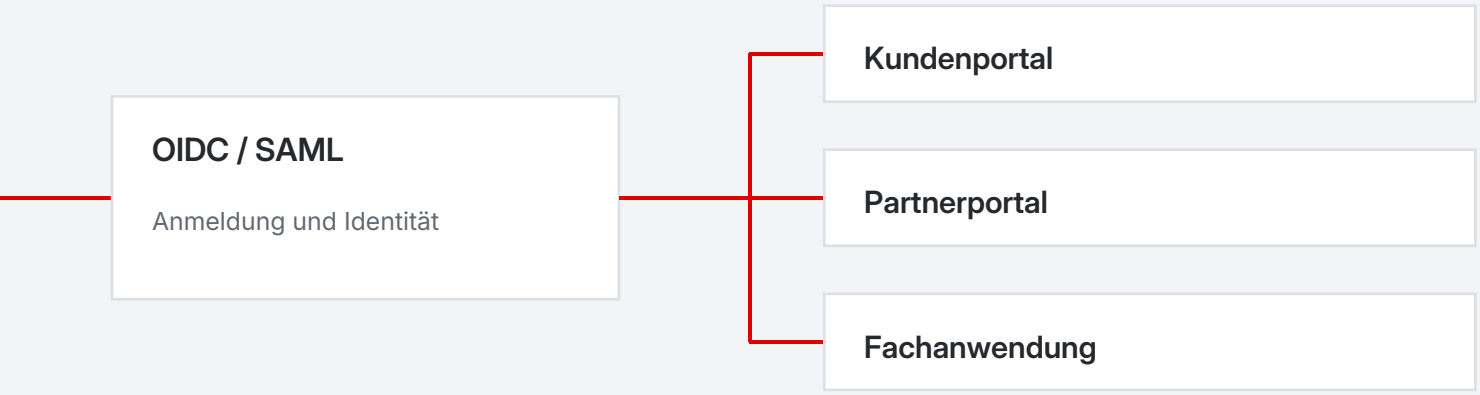
MFA für zusätzlichen Schutz

Multi-Faktor-Authentifizierung (MFA) verbindet verschiedene Faktoren. Passkeys, Hardware-Token oder Einmalcodes lassen sich passend zum Schutzbedarf einsetzen.

Offene Standards verbinden Systeme

OIDC	OpenID Connect für moderne Anwendungen und Logins.
SAML	Bewährter Standard für Unternehmens-SSO.
SCIM	Benutzer und Gruppen systemübergreifend bereitstellen.

ANMELDUNG UND DATEN ÜBER KLARE SCHNITTSTELLEN



SCIM ergänzt die Verwaltung von Benutzer- und Gruppendaten.

Identity is the new perimeter

Cloud, Multi-Cloud und mobile Arbeit lösen feste Netzwerkgrenzen auf. Die Identität wird zu einer zentralen Sicherheitsgrenze: Wer greift worauf zu?

Ein kompromittiertes Konto kann weit reichen

Mit einer gestohlenen Identität können Angreifer mehrere freigegebene Services erreichen. Je weiter die Rechte reichen, desto größer ist der mögliche Schaden.

Sichere Identitäten sind die Basis für Zero Trust

Jeder Zugriff braucht eine geprüfte Identität und passende Rechte. Der Standort im Netzwerk allein begründet kein Vertrauen.

Schutz braucht mehrere Ebenen

IAM verbindet starke Anmeldung und begrenzte Rechte. Geräteprüfung, Überwachung und die Absicherung der Anwendungen ergänzen den Schutz.

SSO erhöht den Komfort. MFA und begrenzte Rechte schützen den Zugang.

Eine zentrale Sicherheitsfunktion verdient besonderen Schutz:
hochverfügbarer Betrieb, Updates und geschützte Administration.

Zugriffe auch zwischen Systemen absichern

APIs, Hintergrunddienste und automatisierte Prozesse brauchen eigene Identitäten. IAM steuert auch diese Machine-to-Machine-Zugriffe.

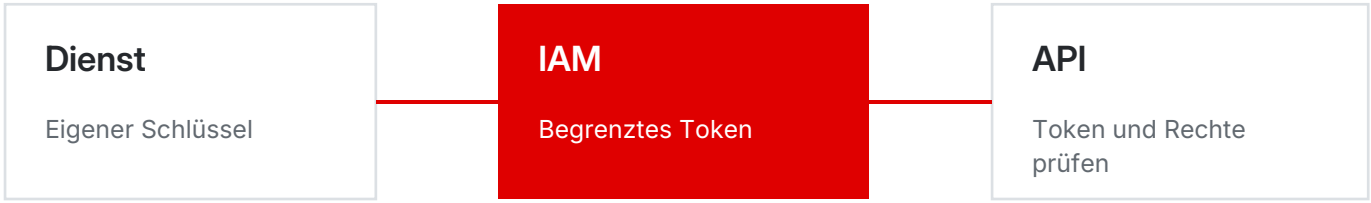
Eigene Identität für jeden Dienst

Ein Service meldet sich mit einem geschützten Schlüssel oder anderen technischen Anmeldemitteln an. Sein Token erlaubt nur die benötigten Zugriffe, zum Beispiel über OAuth 2.0.

Technische Zugänge gezielt begrenzen

Rechte gelten für definierte APIs und Zwecke. Schlüssel lassen sich wechseln, Zugriffe protokollieren und kompromittierte Dienste zentral sperren.

DAS PRINZIP DES MASCHINENZUGRIFFS



Konten zentral sperren. Sessions beenden.

Bei einem Vorfall kann das IAM neue Anmeldungen stoppen und seine laufenden Sessions beenden. Angebundene Anwendungen müssen Sperren und Abmeldungen übernehmen.

Kurze Token-Laufzeiten und geeignete Prüfungen begrenzen die verbleibende Gültigkeit bereits ausgestellter Zugriffe.

Für Projekt- / Service- / Anwendungsverantwortliche

Kürzere Time-to-Market

Sie verantworten einen digitalen Service? Eine gemeinsame Identitätsverwaltung bringt Ihre Anwendung schneller zu den richtigen Nutzern.

01 **Einfacheres Onboarding**

Klare Schnittstellen erleichtern die Anbindung neuer Anwendungen. Joiner-, Mover- und Leaver-Prozesse regeln den Eintritt, Rollenwechsel und Austritt. Ihr Service übernimmt die passenden Identitäten und Freigaben aus diesen Abläufen.

02 **Vorhandene Nutzer sofort erreichen**

Der Benutzerstamm anderer angebundener Services steht Ihrer Anwendung direkt zur Verfügung. Sobald die erforderlichen Freigaben vorliegen, können Kunden, Partner und Mitarbeitende starten. Weniger Registrierungs- und Integrationsaufwand verkürzt die Time-to-Market.

KLARE PROZESSE FÜR DEN GESAMTEN IDENTITÄTSLEBENSZYKLUS

01 **Joiner / Eintritt**

Konto anlegen und passende Zugriffe bereitstellen.

Für Projekt- / Service- / Anwendungsverantwortliche

Mehr Zeit für Ihren Service

Gemeinsame IAM-Funktionen entlasten Ihr Team. So können Sie sich auf den Nutzen und die Fachlogik Ihrer Anwendung konzentrieren.

03 Weniger Aufwand für IAM-Compliance

Login, Passwortregeln und MFA folgen zentralen Vorgaben. Ihr Team muss diese Kontrollen nicht für jede Anwendung neu entwickeln und pflegen. Fachliche Berechtigungsprüfungen und anwendungsspezifische Compliance bleiben Bestandteil Ihres Services.

04 Bewährte Funktionen wiederverwenden

Kontoverwaltung, Self-Service und standardisierte Anmeldeprozesse stehen gemeinsam bereit. Das verringert doppelte Entwicklung und Wartung. Neue Anwendungen starten auf einer erprobten Basis und profitieren von Verbesserungen am zentralen IAM.

RECHTE PASSEN SICH AN DIE AUFGABE AN

02 Mover / Wechsel

Rechte ändern.
Alte Freigaben entziehen.

03 Leaver / Austritt

Zugang sperren.
Sessions beenden.

Für CISOs

Sicherheit unter Ihrer Kontrolle

Sie tragen Verantwortung für Informationssicherheit? IAM bündelt identitätsbezogene Kontrollen und macht ihre Umsetzung über Services hinweg nachvollziehbar.

01 Compliance zentral kontrollieren

Passwort- und MFA-Regeln sowie zentrale Rollenvergaben lassen sich an einer Stelle prüfen. Sie müssen diese IAM-Kontrollen nicht in jeder Anwendung einzeln nachvollziehen. Gemeinsame Protokolle erleichtern Audits. Fachliche Kontrollen ergänzen die Prüfung.

02 Neue Sicherheitsrichtlinien schneller umsetzen

Neue Anforderungen an Kryptografie, Passwörter und MFA lassen sich zentral steuern. Ein gemeinsamer Rahmen beschleunigt die Umsetzung in angebundenen Services. Änderungen an Verfahren und Schlüsseln stimmen Sie mit den Integrationen ab.

03 Unzulässige Rechtekombinationen verhindern

Segregation of Duty schließt Rollen- und Gruppenkombinationen aus, die sich nicht in einer Person treffen dürfen. Zentrale Regeln unterstützen das Vier-Augen-Prinzip und die Trennung kritischer Aufgaben über Anwendungen hinweg.

ZERO TRUST BEGINNT MIT EINER VERLÄSSLICHEN IDENTITÄT

Starke Anmeldung und begrenzte Rechte

IAM schafft eine Grundlage für Zero Trust. Geräteprüfung, Überwachung und geschützte Anwendungen ergänzen sie.

Für CISOs

Klare Zuständigkeiten. Schnelle Reaktion.

Ein gemeinsames IAM schafft einen festen Ansprechpartner für Identitätsschutz und einen zentralen Hebel für die Reaktion auf Vorfälle.

04 Sicherheit bleibt beim Fachteam

Ein spezialisiertes Team verantwortet Anmeldung, Identitätslebenszyklus und zentrale Sicherheitsregeln. Anwendungsteams entwickeln ihre Fachlogik und setzen die jeweiligen Zugriffsprüfungen um. Diese Aufgabenteilung hält die Sicherheitsstrategie unter Ihrer Kontrolle.

05 Ein IAM-Kompetenzteam aufbauen

Bündeln Sie Know-how zu Standards, sicheren Anmeldeverfahren und Integrationen. Das Team begleitet neue Projekte, pflegt gemeinsame Vorgaben und entwickelt die Identitätsinfrastruktur weiter. Wissen bleibt im Unternehmen und steht allen Service-Teams zur Verfügung.

06 Bei kompromittierten Konten sofort handeln

Wenn Kundenidentitäten kompromittiert sind, können Sie zentral neue Anmeldungen sperren und IAM-Sessions beenden. Angebundene Services übernehmen die Abmeldung. So lässt sich der Zugriff für betroffene Identitäten koordiniert unterbrechen.

EIN VORFALL. EINE KOORDINIERTE REAKTION.

01	02	03
Konten sperren	**Sessions beenden**	**Services abmelden**

Die Wirkung in den Services hängt von Abmeldeintegration und Token-Laufzeiten ab.

Für Marketing

One digital face to the customer

Sie gestalten das digitale Kundenerlebnis? Ein gemeinsamer Zugang macht Ihre Marke über alle Services hinweg sichtbar und vertraut.

01 Ein einheitlicher Markenauftritt

Login, Kontoverwaltung und Self-Service folgen Ihrem Look & Feel. Kunden finden dieselbe Gestaltung und vertraute Abläufe in allen Services. Das schafft Wiedererkennung, vermittelt Professionalität und stärkt das Vertrauen in Ihre digitale Marke.

02 SSO verbindet Ihre Services

Kunden melden sich einmal an und wechseln anschließend zwischen freigegebenen Anwendungen. Trotz unterschiedlicher Services entsteht der Eindruck eines zusammenhängenden Systems. Das reduziert Unterbrechungen und macht die Customer Journey flüssiger.

EIN VERTRAUTER ZUGANG FÜR IHRE DIGITALE MARKE

Ein Login. Eine durchgängige Customer Journey.

Einmal anmelden und nahtlos zwischen Services wechseln.

Für Marketing

Weniger Reibung.
Stärkere Kundenbindung.

Eine gemeinsame Identität begleitet Kunden durch Ihr digitales Angebot. Jeder weitere Service kann an eine vertraute Beziehung anknüpfen.

03 Eine Identität stärkt die Kundenbeziehung

Kunden nutzen für alle Services dasselbe Konto. Neue Angebote schließen an den bestehenden Zugang an. Eine konsistente Identität erleichtert die Nutzung weiterer Services und unterstützt langfristige Kundenbindung. Ihr digitales Angebot wirkt professionell und aus einem Guss.

04 Zufriedenere Kunden und Partner

Ein Benutzerkonto und ein Satz Anmeldemittel reduzieren die Komplexität. Nutzer müssen sich weniger Konten und Passwörter merken und pflegen ihre freigegebenen Daten an einer Stelle. Der einfachere Zugang spart Zeit und macht die Nutzung angenehmer.

DIESELBE IDENTITÄT BEGLEITET DEN GESAMTEN WEG

Kundenportal	Weiterer Service	Self-Service
Vertrauter Einstieg	Direkt weitermachen	Konto selbst pflegen

Für die Geschäftsführung

Weniger Kosten.
Mehr Handlungsspielraum.

Sie verantworten Wachstum und Wirtschaftlichkeit? Zentrale Identitätsverwaltung senkt wiederkehrenden Aufwand und schafft klare Zuständigkeiten.

01 Self-Service entlastet den Support

Kunden und Mitarbeitende setzen ihr Passwort selbst zurück und ändern freigegebene Stammdaten, etwa ihre Adresse. Wiederkehrende Anliegen erreichen seltener den Support. Das spart manuelle Arbeit und hält Ihr Team für anspruchsvollere Aufgaben frei.

02 Administration an Kunden und Partner delegieren

Kunden- und Partneradministratoren onboarden ihre Kollegen und verwalten ausgewählte Rechte selbst. Sie übertragen klar begrenzte Aufgaben an die Organisation, die ihre Nutzer am besten kennt. So wächst der Verwaltungsaufwand langsamer als die Zahl der angebundenen Unternehmen.

03 Rechtliche Anforderungen leichter erfüllen

Zentral gesteuerte Daten und Rechte schaffen klare Zuständigkeiten. Dokumentierte Freigaben und ein geregelter Entzug von Zugängen erleichtern Nachweise. Das unterstützt die rechtssichere Gestaltung Ihrer Prozesse und macht den Umgang mit Identitäten besser kontrollierbar.

WIEDERKEHRENDE ARBEIT LÄSST SICH GEZIELT VERLAGERN

Nutzer pflegen ihre Daten selbst

Kunden- und Partneradministratoren verwalten ihre Kollegen.

Für die Geschäftsführung

Vertrauen schützen. Digitalisierung ermöglichen.

IAM verbindet den wirtschaftlichen Nutzen im Alltag mit einer belastbaren Grundlage für neue digitale Angebote.

04 Reputation stärken und Risiken begrenzen

Starke Anmeldung und zentral gesteuerte Rechte machen Ihr Sicherheitsversprechen nachvollziehbar. Klare Zuständigkeiten und schnelle Reaktionen auf kompromittierte Konten helfen, Schäden zu begrenzen. Ein professioneller Zugang stärkt zugleich das Vertrauen Ihrer Kunden und Partner.

05 IAM als Enabler der Digitalisierung

Neue Portale, zusätzliche Services und automatisierte Prozesse nutzen vorhandene Identitäten und gemeinsame Sicherheitsregeln. Auch Machine-to-Machine-Zugriffe passen in diesen Rahmen. Eine wiederverwendbare Basis erleichtert neue Geschäftsmodelle und die Erweiterung Ihrer digitalen Angebote.

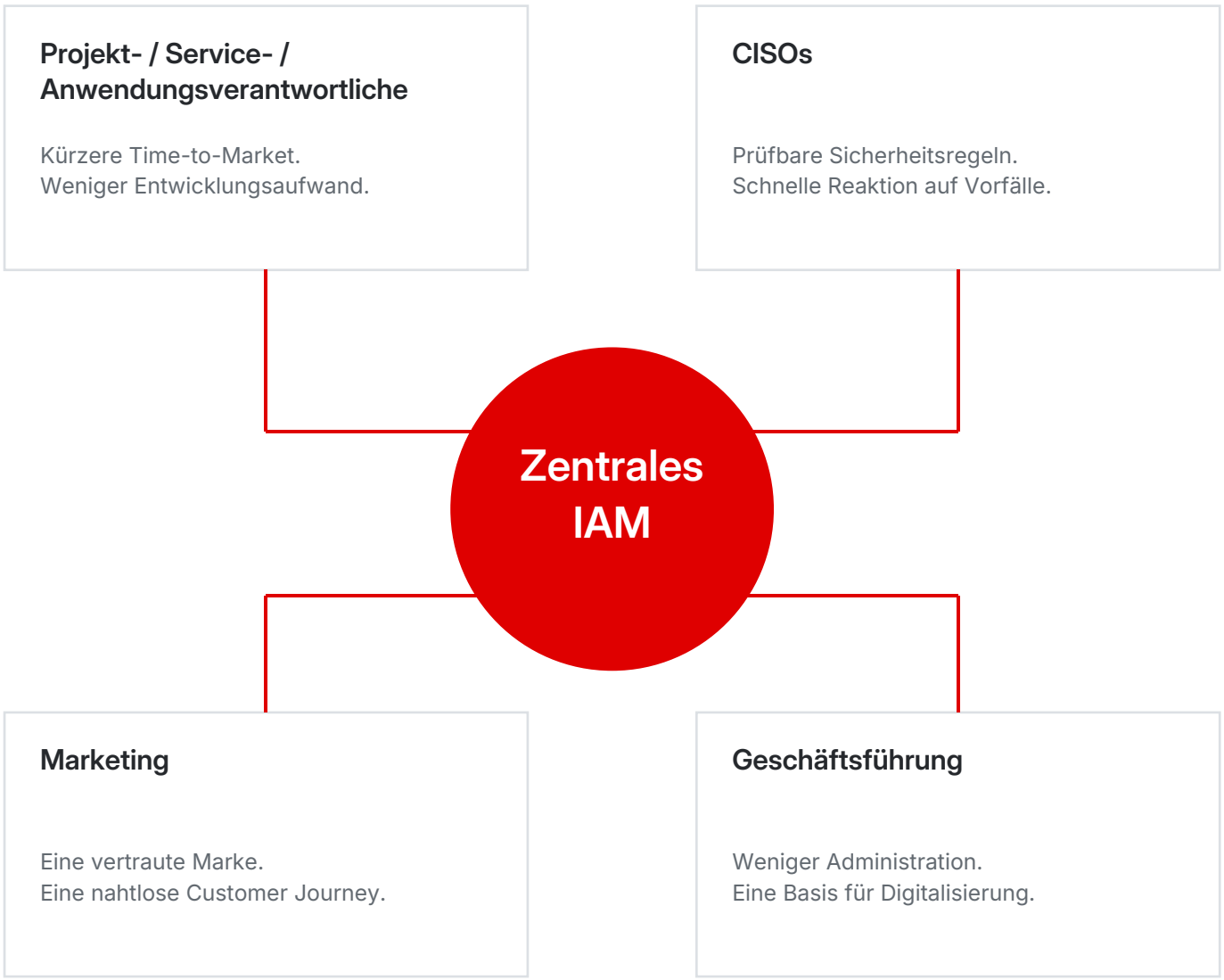
MEHR SPIELRAUM FÜR IHR GESCHÄFT

Weniger Administration. Mehr Kapazität für Neues.

Gemeinsame Identitäten verbinden Ihre digitalen Angebote.

Vier Perspektiven.
Ein gemeinsamer Gewinn.

Zentrale Identitätsverwaltung verbindet die Ziele Ihrer Teams. Ein gemeinsam betriebenes IAM zahlt auf das gesamte digitale Angebot ein.



Eine Win-Win-(Win-Win-)Situation

Gemeinsame Infrastruktur. Nutzen für jedes Team.

Offene Technologie. Persönliche Expertise.

loginfactor verbindet Keycloak als Open-Source-Basis mit Beratung, Umsetzung und verlässlichem Betrieb.

Passend zu Ihrer Systemlandschaft

Wir klären Benutzerquellen, Rollen und Zuständigkeiten. Ein erster Service zeigt, wie Login, MFA und Lebenszyklus im Alltag zusammenspielen.

Offene Standards und gezielte Erweiterungen

OIDC und SAML verbinden Anwendungen. Erweiterungen ergänzen unter anderem SCIM, delegierte Administration und den Ausschluss unzulässiger Rechtekombinationen.

Betrieb mit klaren Verantwortlichen

Cloud in deutschen Rechenzentren oder Ihre eigene Infrastruktur. Monitoring, Backups und proaktive Sicherheitsupdates stützen den vereinbarten Betrieb.

DIE GEMEINSAME BASIS BRAUCHT EINEN GUTEN BETRIEB

Verfügbarkeit und Integration von Anfang an mitplanen

Gemeinsam planen wir Ausfallsicherheit, geschützte Administration und die Umsetzung von Sperren bis in die Anwendungen.

loginfactor

Ihr nächster Schritt

Eine Identität.
Viele Möglichkeiten.

Planen Sie Ihr zentrales IAM mit uns.

Wir verbinden Ihre Services mit einer gemeinsamen Identitätsverwaltung und begleiten Sie von der Architektur bis zum laufenden Betrieb.

Beratung, Umsetzung und Betrieb
Auf Basis von Keycloak

KONTAKT

info@loginfactor.com
+49 5251 5449490
www.loginfactor.com

Mehr erfahren

loginfactor ist eine Marke der ActiDoo GmbH.
Technologiepark 20 · 33100 Paderborn · Deutschland