loginfactor

Identity & Access Management

One login.
Central control.



The foundation for secure
and connected digital services.

AI-generated

Manage identities centrally

Identity & Access Management (IAM) creates a shared foundation for users and access. All connected services use the same trusted identities.

User data

One profile across all services. IAM connects existing directories and systems of record, or manages accounts itself. Responsibility for the data remains clear.

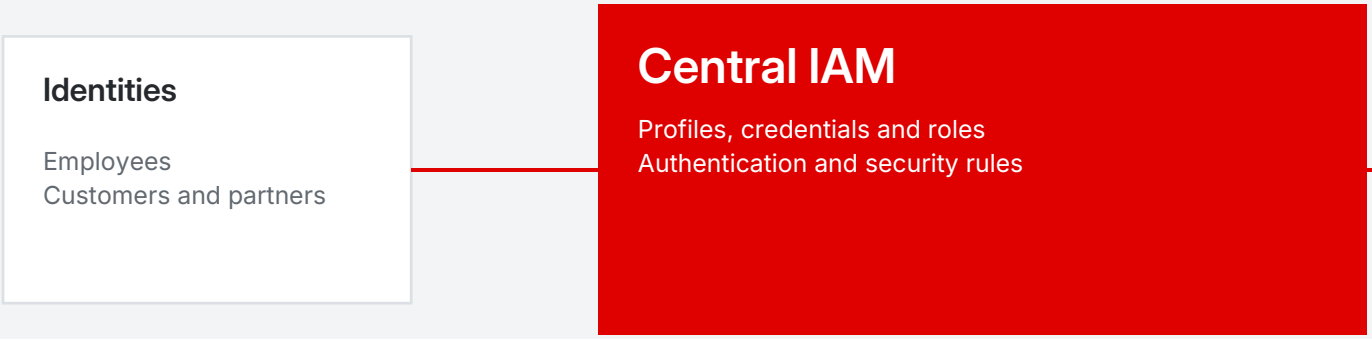
Credentials

Passwords, passkeys and other sign-in methods follow shared rules. Your own identity providers can handle authentication.

Roles and permissions

IAM provides roles and access grants. Applications check them when users access a service and apply their own business rules.

ONE IDENTITY INFRASTRUCTURE FOR ALL SERVICES



Existing directories can still be integrated.

Sign in once.
Use services seamlessly.

Single Sign-On (SSO) connects your applications. Users sign in once and then move between the services they are authorised to use.

SSO with clear access boundaries

One login makes services easier to use. The relevant permissions still determine which data and functions each user can access.

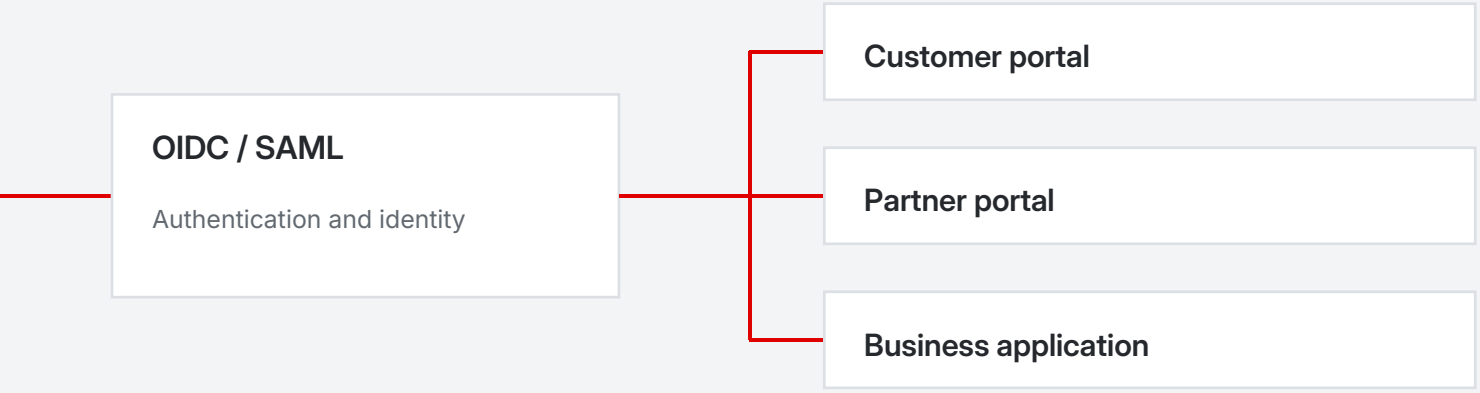
MFA for additional protection

Multi-factor authentication (MFA) combines different factors. Passkeys, hardware tokens or one-time codes can be selected to match your security needs.

Open standards connect systems

OIDC	OpenID Connect for modern applications and sign-ins.
SAML	An established standard for enterprise SSO.
SCIM	Provision users and groups across systems.

AUTHENTICATION AND DATA THROUGH CLEAR INTERFACES



SCIM adds provisioning for user and group data.

Identity is the new perimeter

Cloud, multi-cloud and mobile working dissolve fixed network boundaries. Identity becomes a key security boundary: who can access what?

A compromised account can have a wide impact

With a stolen identity, attackers can reach several authorised services. The broader its permissions, the greater the potential damage.

Secure identities are the basis for Zero Trust

Every access needs a verified identity and appropriate permissions. A location within the network alone does not establish trust.

Protection needs several layers

IAM combines strong authentication with limited permissions. Device checks, monitoring and application security add further protection.

SSO makes access convenient. MFA and limited permissions keep it secure.

A central security function deserves special protection:
high availability, updates and secure administration.

Secure access between systems too

APIs, background services and automated processes need their own identities. IAM also controls this machine-to-machine access.

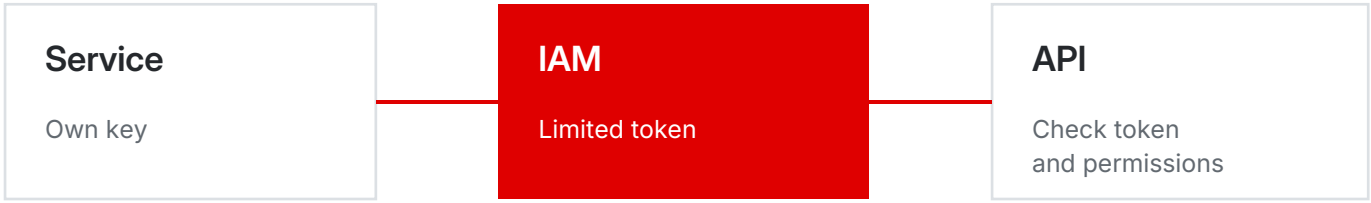
A separate identity for every service

A service authenticates with a protected key or other technical credentials. Its token permits only the access it needs, for example through OAuth 2.0.

Limit technical access precisely

Permissions apply to defined APIs and purposes. Keys can be rotated, access logged and compromised services blocked centrally.

HOW MACHINE ACCESS WORKS



Block accounts centrally. End sessions.

During an incident, IAM can stop new sign-ins and end its active sessions. Connected applications must enforce account blocks and sign-outs.

Short token lifetimes and suitable checks limit the remaining validity of access already granted.

For project / service / application owners

Shorter time-to-market

Responsible for a digital service? Shared identity management brings your application to the right users faster.

01 Easier onboarding

Clear interfaces make new applications easier to connect. Joiner, mover and leaver processes govern entry, role changes and departure. Your service receives the right identities and access grants from these processes.

02 Reach existing users immediately

The user base of other connected services is directly available to your application. Once the required access is approved, customers, partners and employees can get started. Less registration and integration work shortens time-to-market.

CLEAR PROCESSES THROUGHOUT THE IDENTITY LIFECYCLE

01 Joiner / Joining

Create an account and provide the right access.

For project / service / application owners

More time for your service

Shared IAM functions reduce the load on your team. You can focus on your application's value and business logic.

03 Less work on IAM compliance

Sign-in, password policies and MFA follow central requirements. Your team does not need to develop and maintain these controls for every application. Business authorisation checks and application-specific compliance remain part of your service.

04 Reuse proven functions

Account management, self-service and standard sign-in processes are shared across services. This reduces duplicate development and maintenance. New applications start on a proven foundation and benefit from improvements to the central IAM.

PERMISSIONS ADAPT TO THE TASK

02 Mover / Role change

Change permissions.
Revoke old access.

03 Leaver / Leaving

Block access.
End sessions.

For CISOs

Security under your control

Responsible for information security? IAM brings identity controls together and makes their implementation traceable across services.

01 Monitor compliance centrally

Password and MFA policies, as well as central role assignments, can be reviewed in one place. You do not need to check these IAM controls separately in every application. Shared logs make audits easier. Business controls complement the review.

02 Implement new security policies faster

New requirements for cryptography, passwords and MFA can be managed centrally. A shared framework speeds up implementation in connected services. Changes to methods and keys are coordinated with the integrations.

03 Prevent conflicting permissions

Segregation of Duties excludes role and group combinations that no single person should hold. Central rules support dual control and the separation of critical duties across applications.

ZERO TRUST STARTS WITH A TRUSTED IDENTITY

Strong authentication and limited permissions

IAM provides a foundation for Zero Trust. Device checks, monitoring and secure applications complement it.

For CISOs

Clear responsibilities. Fast response.

A shared IAM provides a clear point of contact for identity protection and a central means of responding to incidents.

04 Security stays with the specialists

A specialist team owns authentication, the identity lifecycle and central security rules. Application teams develop their business logic and implement the relevant access checks. This division of responsibilities keeps the security strategy under your control.

05 Build an IAM centre of expertise

Bring together expertise in standards, secure sign-in methods and integrations. The team supports new projects, maintains shared policies and develops the identity infrastructure. Knowledge stays within the company and is available to every service team.

06 Act immediately on compromised accounts

If customer identities are compromised, you can centrally block new sign-ins and end IAM sessions. Connected services enforce the sign-out. This allows you to interrupt access for affected identities in a coordinated way.

ONE INCIDENT. ONE COORDINATED RESPONSE.

01	02	03
Block accounts	**End sessions**	**Sign out of services**

The effect in each service depends on sign-out integration and token lifetimes.

For marketing

One digital face to the customer

Shaping the digital customer experience? A shared login makes your brand visible and familiar across all services.

01 A consistent brand experience

Sign-in, account management and self-service follow your look and feel. Customers encounter the same design and familiar processes in every service. This creates recognition, conveys professionalism and builds trust in your digital brand.

02 SSO connects your services

Customers sign in once and then move between authorised applications. Different services feel like parts of one connected system. This reduces interruptions and makes the customer journey smoother.

A FAMILIAR LOGIN FOR YOUR DIGITAL BRAND

One login. One seamless customer journey.

Sign in once and move seamlessly between services.

For marketing

Less friction.
Stronger customer loyalty.

A shared identity accompanies customers across your digital offering. Each additional service can build on an established relationship.

03 One identity strengthens customer relationships

Customers use the same account for every service. New offerings connect to their existing access. A consistent identity makes further services easier to use and supports lasting customer loyalty. Your digital offering feels professional and cohesive.

04 Happier customers and partners

One user account and one set of credentials reduce complexity. Users have fewer accounts and passwords to remember, and manage the data they are allowed to change in one place. Easier access saves time and makes services more pleasant to use.

THE SAME IDENTITY THROUGHOUT THE JOURNEY

Customer portal

A familiar starting point

Another service

Continue straight away

Self-Service

Manage your own account

For executive management

Lower costs.
More room to act.

Responsible for growth and profitability? Central identity management reduces recurring work and establishes clear responsibilities.

01 Self-service reduces support work

Customers and employees reset their own passwords and update permitted profile data, such as their address. Fewer routine requests reach support. This saves manual work and frees your team for more demanding tasks.

02 Delegate administration to customers and partners

Customer and partner administrators onboard colleagues and manage selected permissions themselves. You delegate clearly defined tasks to the organisation that knows its users best. Administration effort then grows more slowly than the number of connected companies.

03 Meet legal requirements more easily

Centrally managed data and permissions establish clear responsibilities. Documented access approvals and a controlled revocation process make it easier to provide evidence. This supports legally compliant processes and gives you greater control over identity management.

SHIFT RECURRING WORK TO THE RIGHT PEOPLE

Users manage their own data

Customer and partner administrators manage their colleagues.

For executive management

Protect trust.
Enable digital transformation.

IAM combines everyday business benefits with a sound foundation for new digital offerings.

04 Strengthen your reputation and limit risks

Strong authentication and centrally managed permissions make your security commitment tangible. Clear responsibilities and a fast response to compromised accounts help limit damage. A professional login experience also strengthens the trust of your customers and partners.

05 IAM enables digital transformation

New portals, additional services and automated processes use existing identities and shared security rules. Machine-to-machine access fits within this framework too. A reusable foundation makes new business models and the expansion of your digital offering easier.

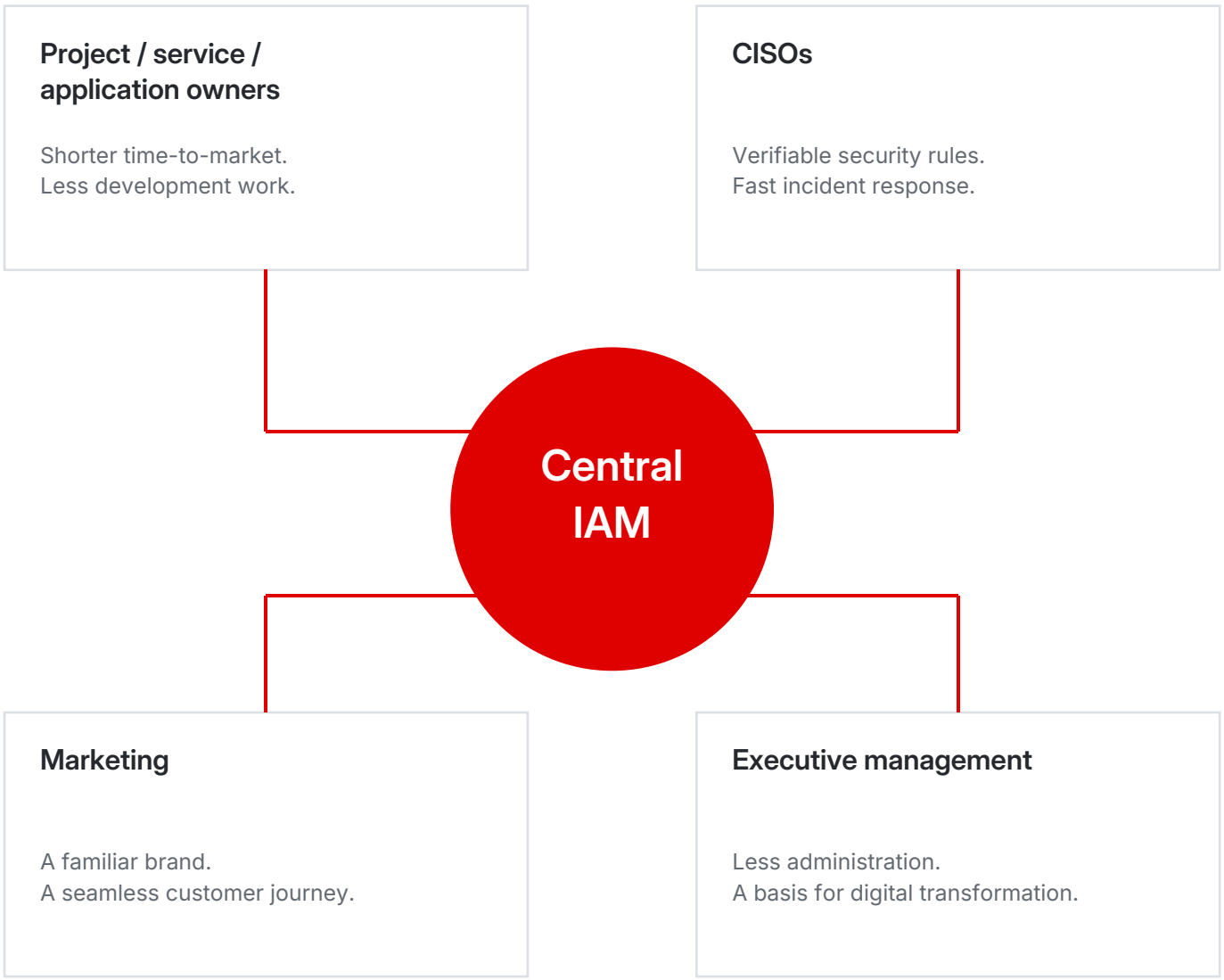
MORE ROOM FOR YOUR BUSINESS

Less administration. More capacity for new ideas.

Shared identities connect your digital offerings.

Four perspectives. One shared win.

Central identity management brings your teams' goals together. A jointly operated IAM benefits your entire digital offering.



A win-win-(win-win-)situation

Shared infrastructure. Benefits for every team.

Open technology. Personal expertise.

loginfactor combines Keycloak as an open-source foundation with consulting, implementation and reliable operations.

A fit for your system landscape

We clarify user sources, roles and responsibilities. An initial service shows how sign-in, MFA and the identity lifecycle work together in practice.

Open standards and targeted extensions

OIDC and SAML connect applications. Extensions add capabilities such as SCIM, delegated administration and the prevention of conflicting permissions.

Operations with clear responsibilities

Cloud in German data centres or your own infrastructure. Monitoring, backups and proactive security updates support the agreed operating model.

A SHARED FOUNDATION NEEDS RELIABLE OPERATIONS

Plan for availability and integration from the start

Together, we plan resilience, secure administration and the enforcement of account blocks in your applications.

loginfactor

Your next step

One identity.
Many possibilities.

Plan your central IAM with us.

We connect your services through shared identity management and support you from architecture to ongoing operations.

Consulting, implementation and operations

Built on Keycloak

CONTACT

info@loginfactor.com

+49 5251 5449490

www.loginfactor.com

Learn more

loginfactor is a brand of ActiDoo GmbH.
Technologiepark 20 · 33100 Paderborn · Germany