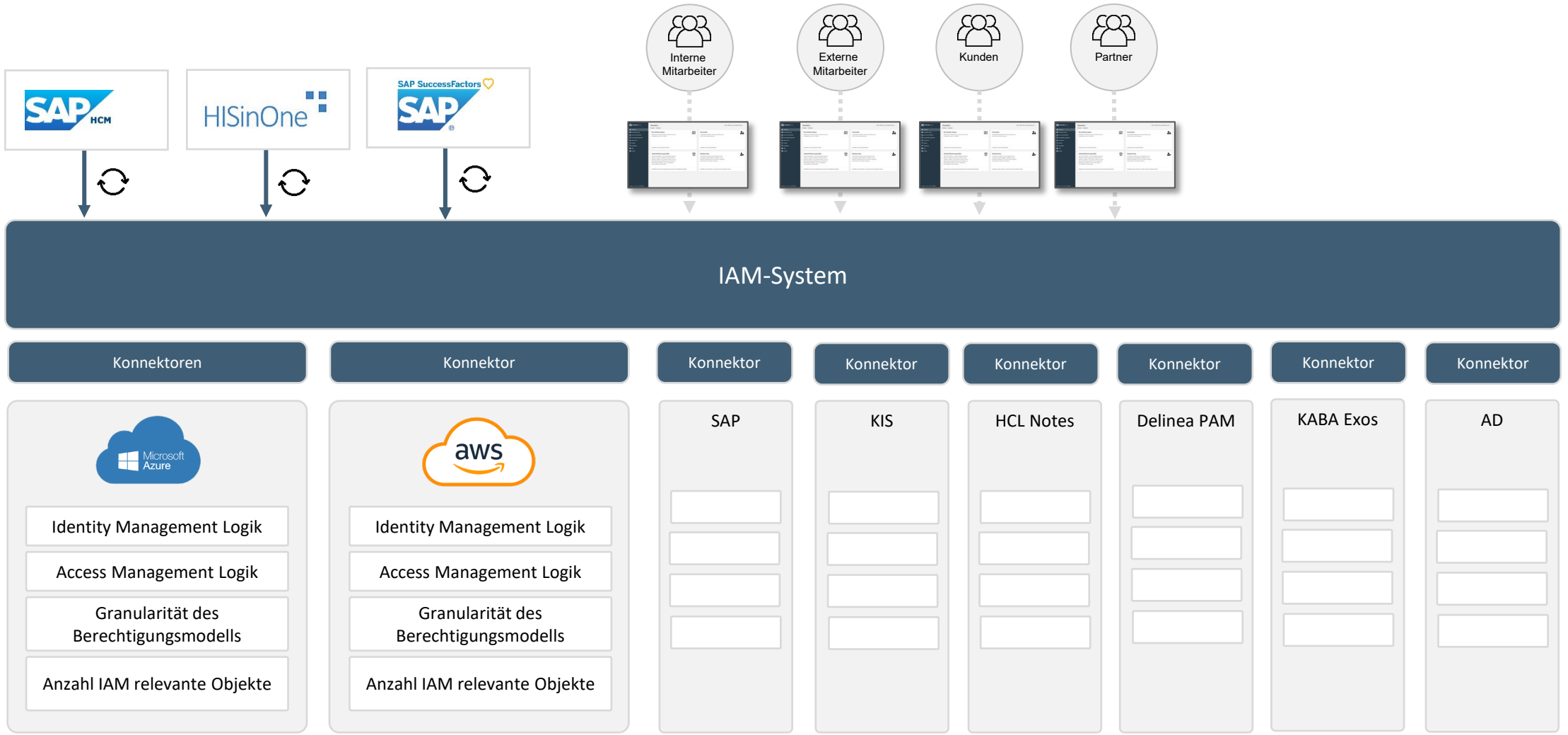

ITSENSE

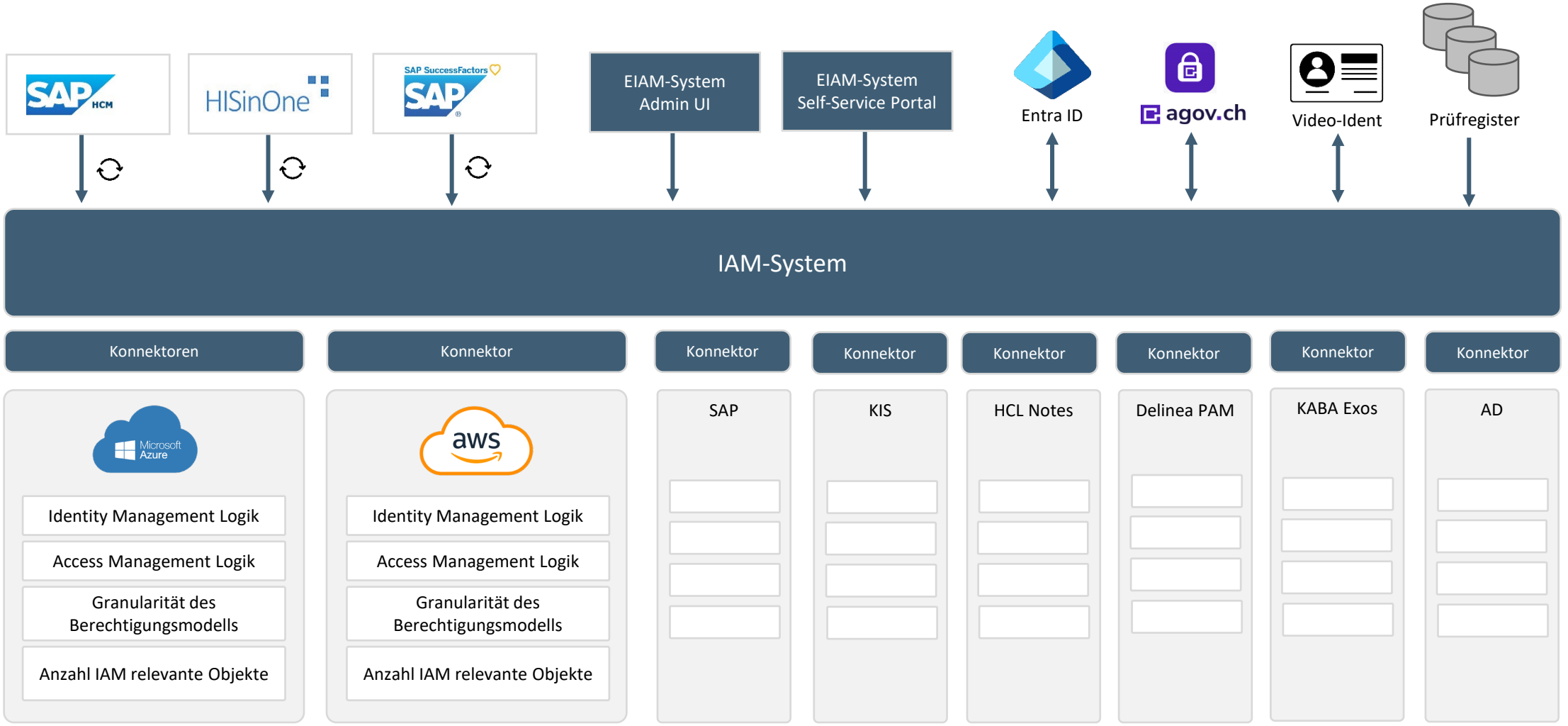
Hybride und heterogene IAM Umgebungen und ihre Herausforderungen



ITSENSE

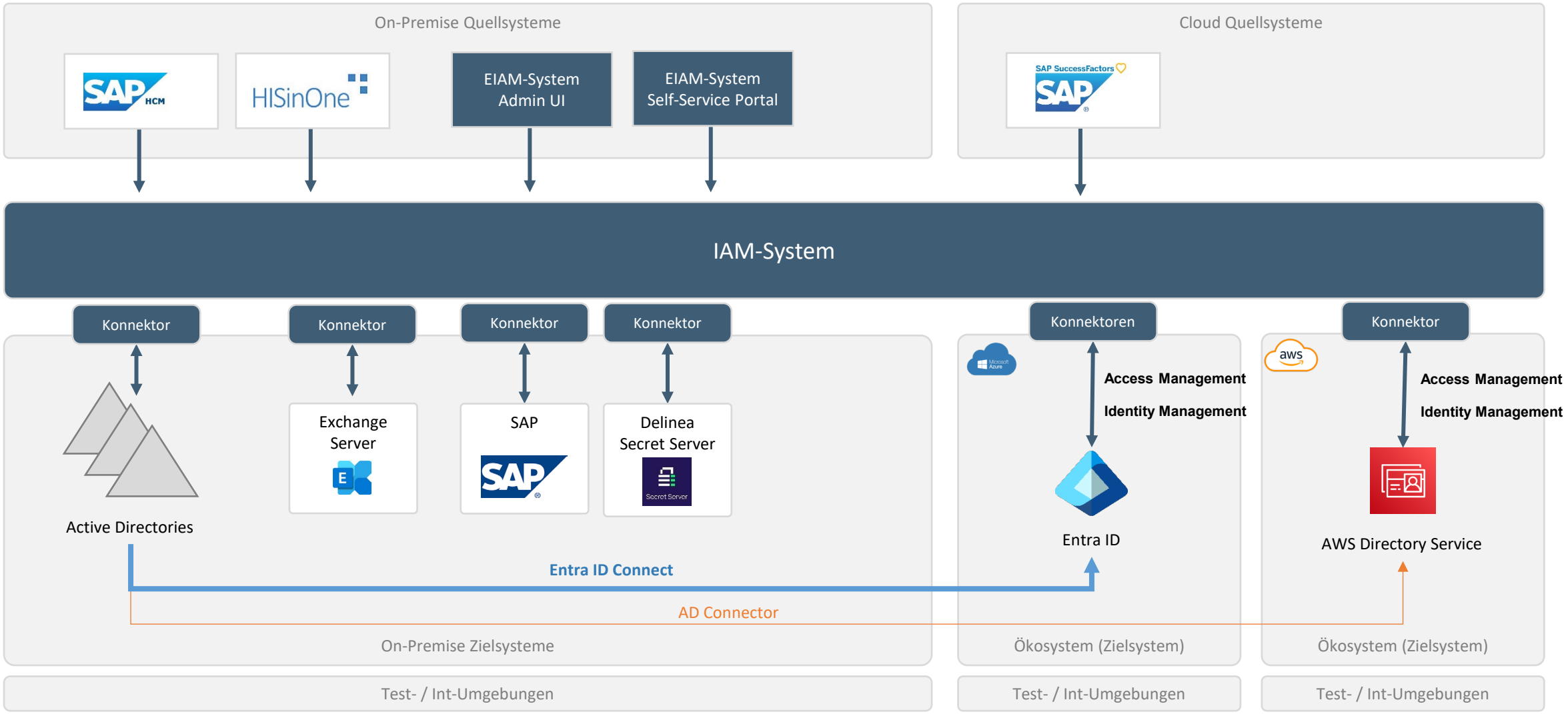

ITSENSE
Integration von heterogenen
Quell- / Zielsystemen,
insbesondere Azure Cloud
Photo by samsommer

Hybride und heterogene IAM Umgebungen und ihre Herausforderungen



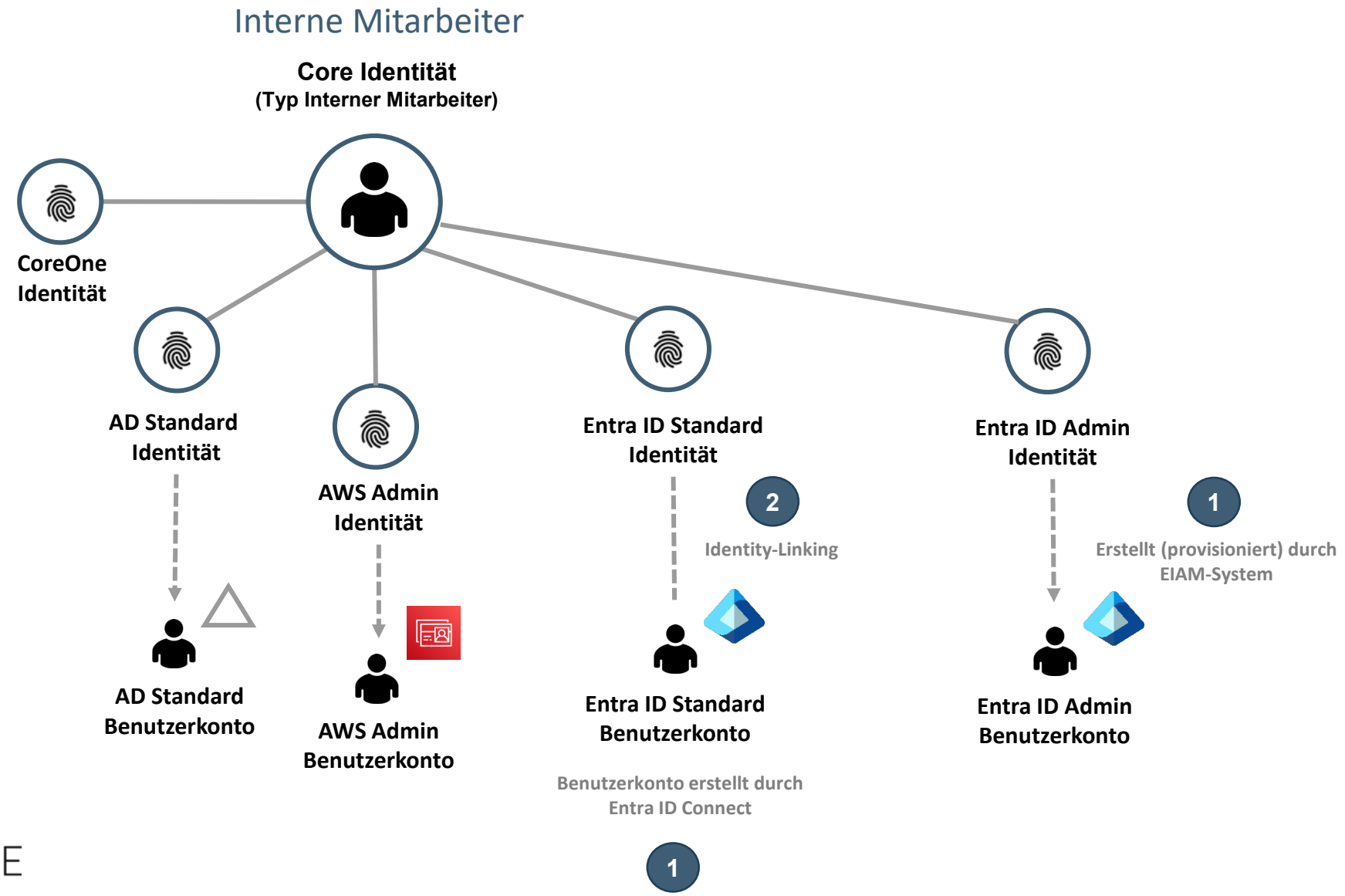
ITSENSE

Integration von Entra ID



ITSENSE

Übergreifendes Identity Management



ITSENSE

IAM relevante Objekte im Azure Cloud Ökosystem

IAM-System

Konnektoren

Entra ID

Benutzerobjekte

- Entra ID Accounts (Standard)
- Entra ID Accounts (Admin)
- Guests Accounts
- Service Principals
- Managed Identities
- Federated Identities
- B2C Identitäten

Gruppenobjekte

- Azure Security Groups
- M365 Groups
- Verteilergruppen
- Mail-enabled Security Groups

Berechtigungen

- Rollen
- Richtlinien

Access Governance

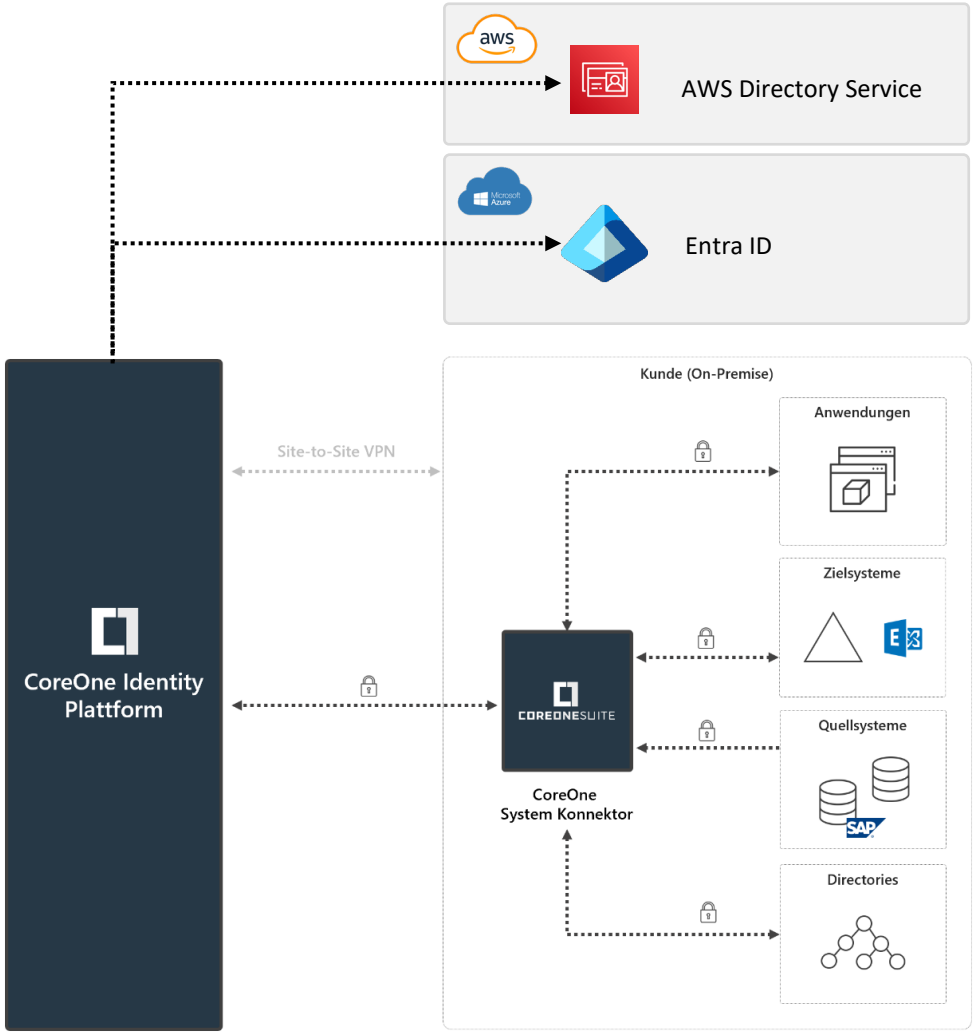
- Access Reviews

Single Sign-On (SSO)

- Applications
- Externe IDPs

ITSENSE

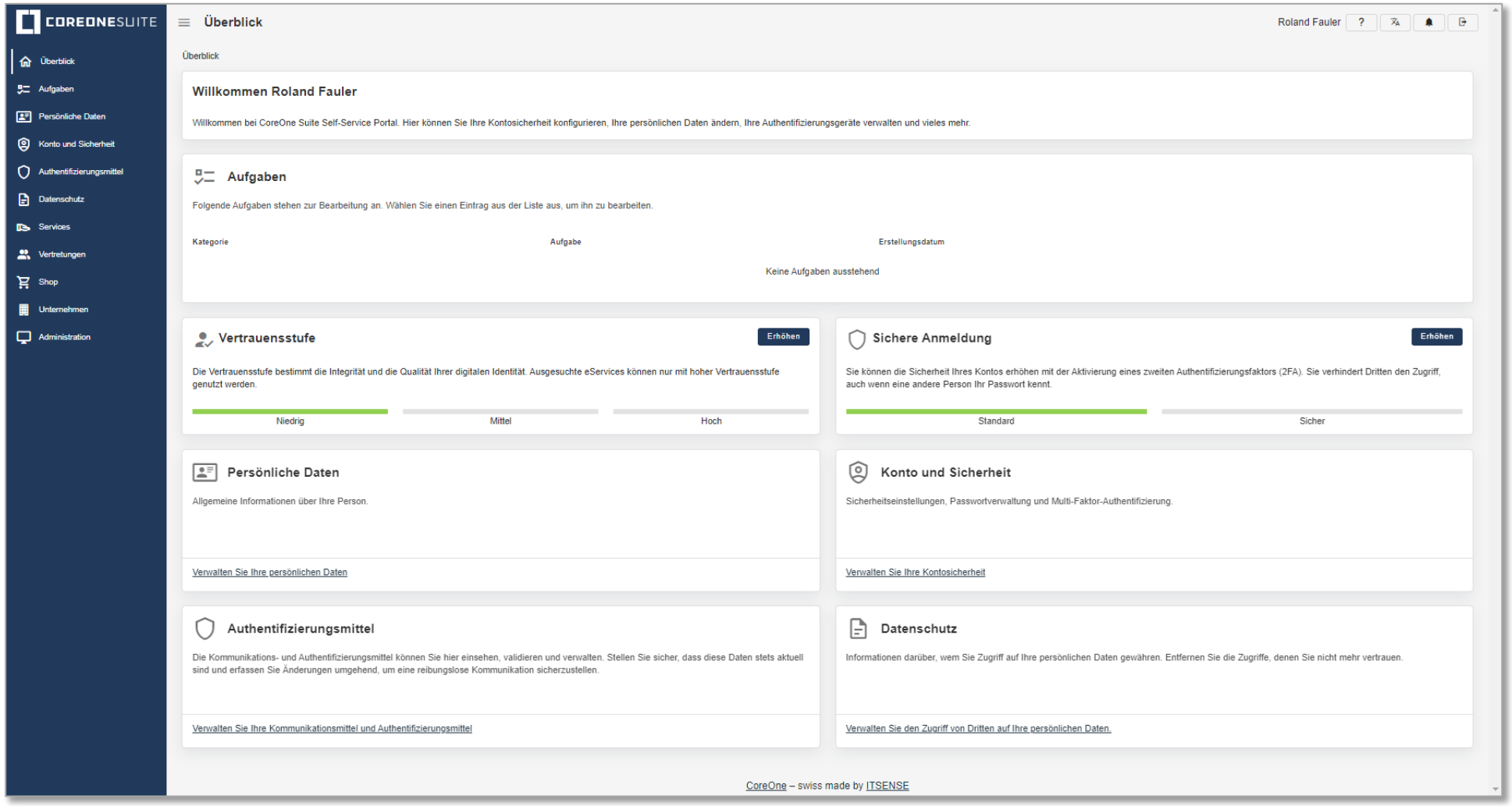
Plattform übergreifende Provisionierung

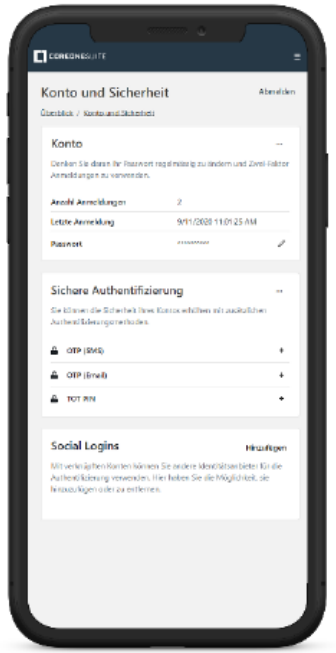


ITSENSE


ITSENSE
Heterogene Nutzerkreise
und ihre Bedürfnisse
Photo by samsommer

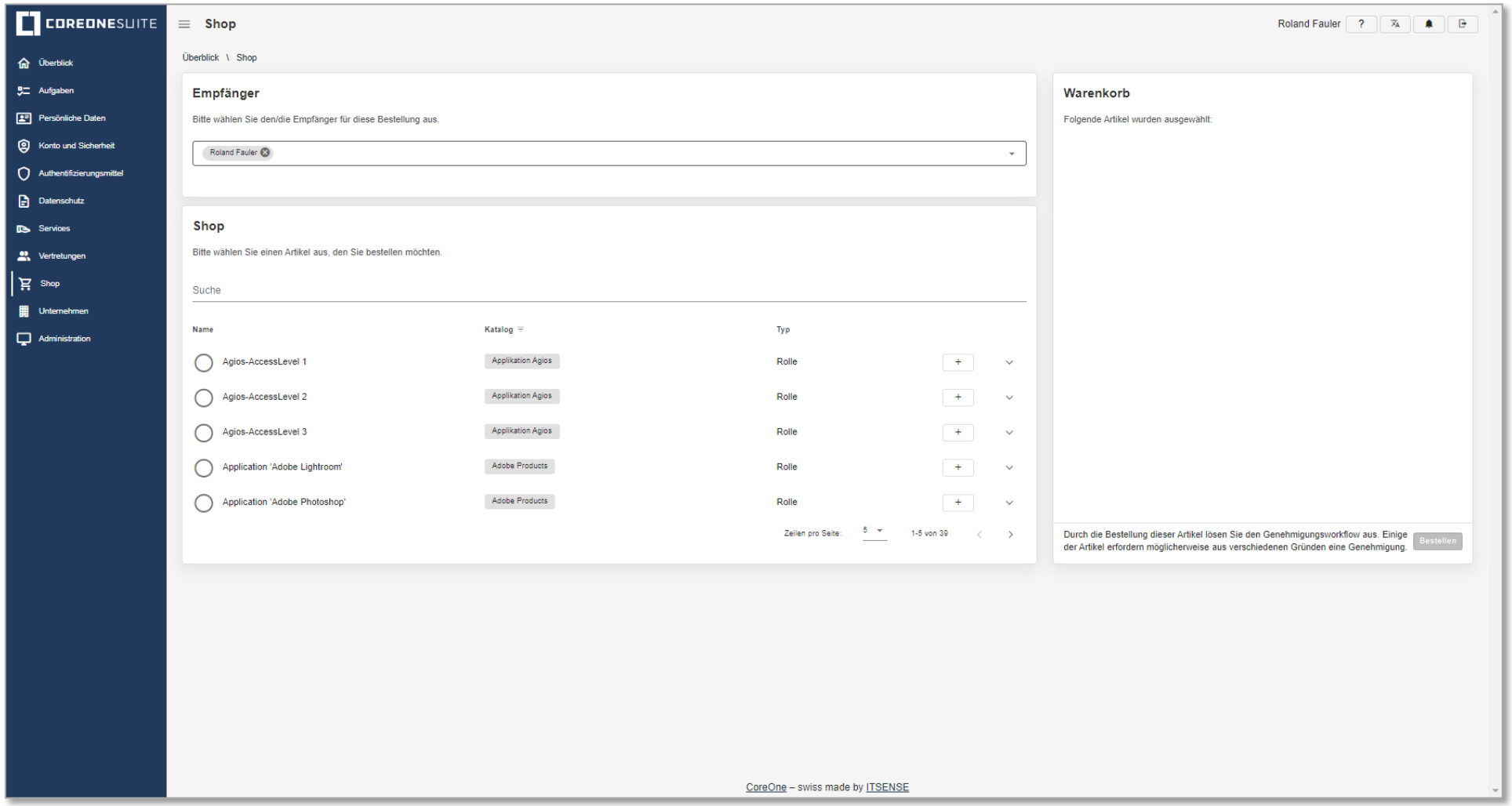
Intuitive, einfache und barrierefreie Benutzeroberflächen





ITSENSE

Shop Erlebnis



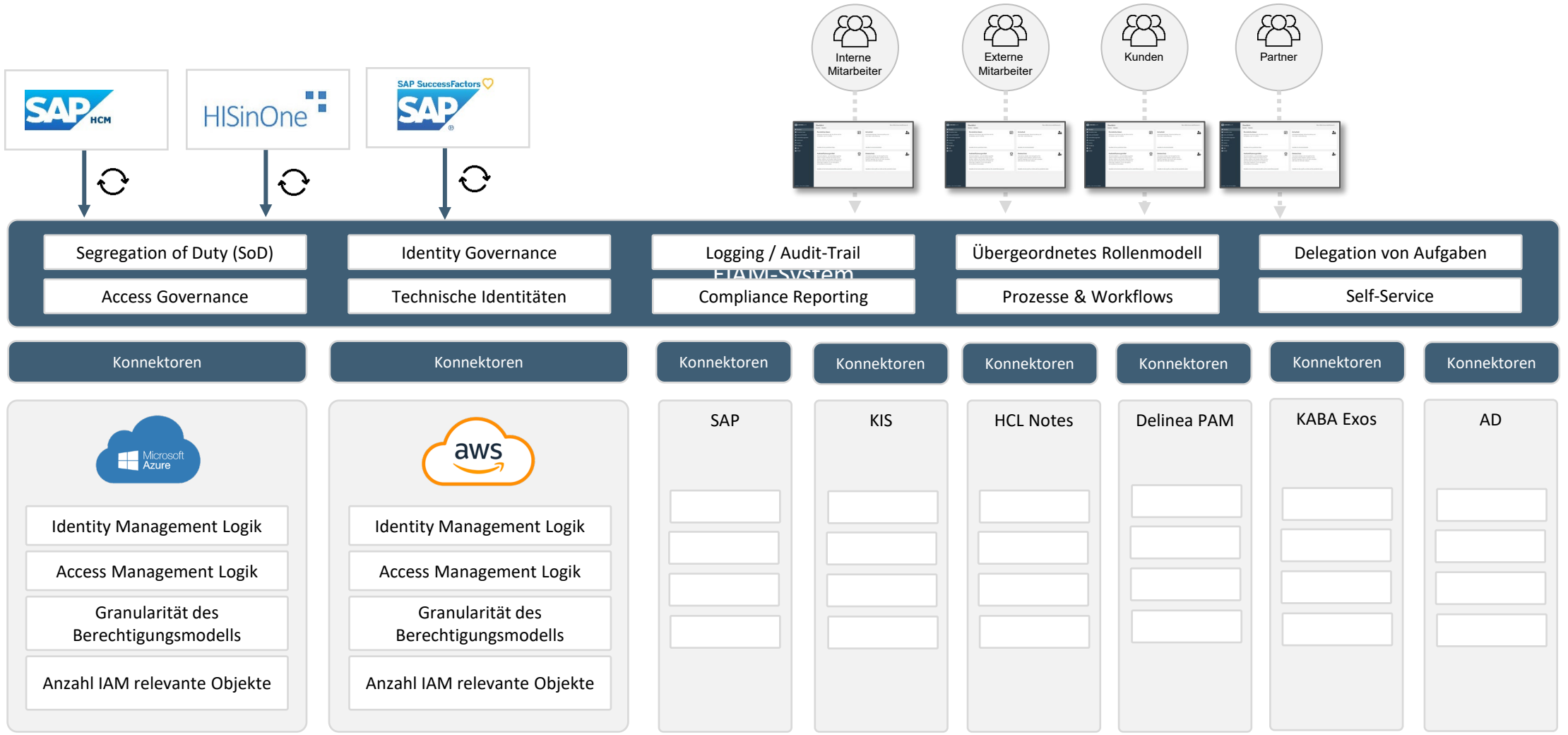
ITSENSE


ITSENSE
Übergreifende Fähigkeiten
für ein ganzheitliches IAM
Photo by samsommer

EIAM + Entra ID = Mehrwert ^{2}

ITSENSE

Übergreifende Fähigkeiten für ein ganzheitliches IAM



ITSENSE

Vorteile eines übergeordneten EIAM-Systems

- **Zentrale Verwaltung von Identitäten**: Ermöglicht die konsolidierte, zentrale Verwaltung der Identity-Lifecycles von verschiedenen Personenkreisen (interne Mitarbeiter, externe Mitarbeiter, Kunden, Partner, etc.) über alle Plattformen hinweg (On-Premise, Azure, AWS, Google Cloud).
- **Zentrale Verwaltung von Berechtigungen**: Ermöglicht die konsolidierte, zentrale sowie **feingranulare und hierarchische** Verwaltung sämtlicher Zugriffs- und Zutrittsverwaltung über alle Plattformen hinweg.
- **Zentrales Meta Directory:** Ermöglich die konsolidierte, zentrale Datenhaltung in einem übergeordneten Meta Directory.
- **Manuelle Verwaltung:** Ermöglich die zentrale und/oder delegierte Verwaltung von Identitäten und Zugriffsberechtigungen für nicht in Quellsystem geführten Stammdaten (Bsp. externe Mitarbeiter).
- **Kontrolle über Azure Guest Accounts:** Ermöglich die zentrale Verwaltung von Azure Guest Accounts. Insbesondere die Bestellung / Genehmigung und die Rezertifizierung durch die Fachbereiche.
- **Kohärente Sicherheitsrichtlinien**: Zentrale und einheitliche Definition von Richtlinien (u.A. Segregation of Duty) und Sicherheitsstandards über alle Plattformen hinweg.
- **Erweiterte Access Governance**: Risk-based Access Control, Rezertifizierungs-Kampagnen
- **Skalierbarkeit**: Unterstützt die flexible Integration neuer Systeme und Applikationen.
- **Verbesserte Auditing- und Compliance-Funktionalitäten**: Nachvollziehbarkeit und Audittierbarkeit von sämtlichen Vorgängen über alle Plattformen hinweg.
- **Optimale User-Experience**: Übergeordnete und abgestimmte Prozessführung und Interaktionen über alle Plattformen hinweg
- **Provisioning von Entra ID als leistungsfähiger Identity Provider (IdP) für Single Sign-On (SSO)** über verschiedene Plattformen hinweg

Stärken und Schwächen

Aspekt	Enterprise IAM (traditionell)	Microsoft Entra ID (Azure AD)
Cloud-Integration	**Schwäche**: Meist auf On-Premise fokussiert, Cloud-Support erfordert oft Zusatzmodule oder Anpassungen.	**Stärke**: Native Cloud- und SaaS-Integration, besonders mit Microsoft 365 und Azure.
On-Premise-Integration	**Stärke**: Tiefe Unterstützung für komplexe On-Premise-Systeme, Legacy-Anwendungen und ältere IT-Infrastrukturen.	**Schwäche**: Eingeschränkte Funktionalität für komplexe On-Premise-Umgebungen, zusätzliche Tools erforderlich (z.B. Azure AD Connect).
Hybride Umgebungen	**Stärke**: Entwickelt für hybride Infrastrukturen, einfache Integration von On-Premise- und Cloud-Ressourcen.	**Schwäche**: Komplexere Konfiguration in hybriden Umgebungen, Synchronisation zwischen lokal und Cloud erforderlich.
Flexibilität und Anpassbarkeit	**Stärke**: Hochgradig anpassbar, geeignet für spezielle Geschäftsanforderungen und branchenspezifische Use-Cases.	**Schwäche**: Weniger anpassbar, standardisierte Lösung ohne tiefere Anpassungsmöglichkeiten.
Sicherheit	**Stärke**: Bietet erweiterte Sicherheitsoptionen, oft in Verbindung mit Drittsystemen konfigurierbar.	Stärke: Integrierte Sicherheitsfunktionen wie MFA, bedingter Zugriff, Zero-Trust-Modelle nativ verfügbar.
Kostenstruktur	**Stärke**: Oft modular, mit einmaligen Lizenzkosten oder niedrigeren On-Premise-Kosten.	**Schwäche**: Abonnementmodell kann mit steigender Benutzeranzahl und Nutzung von Premium-Funktionen kostspielig werden.
Granularität der Zugriffssteuerung	**Stärke**: Sehr granulare Zugriffssteuerung, komplexe Berechtigungsmodelle und detaillierte Rollenverwaltung möglich.	**Schwäche**: Weniger granular als Enterprise IAM-Systeme, eingeschränkte Rollen- und Berechtigungsverwaltung.
Single Sign-On (SSO)	**Schwäche**: SSO für Cloud-Dienste erfordert oft zusätzliche Module oder Integrationen.	**Stärke**: Nahtlose SSO für Cloud- und On-Premise-Anwendungen, besonders im Microsoft-Ökosystem.
Automatisierung (Provisionierung/Deprovisionierung)	**Stärke**: Hohe Automatisierbarkeit, jedoch meist auf On-Premise beschränkt.	**Stärke**: Native automatisierte Provisionierung/Deprovisionierung für Cloud-basierte Anwendungen.
Integration in heterogene Umgebungen	**Stärke**: Entwickelt für heterogene IT-Landschaften, unterstützt viele verschiedene Plattformen und Technologien.	**Schwäche**: Am besten für Microsoft-zentrierte Umgebungen geeignet, schwieriger in Nicht-Microsoft-Umgebungen zu integrieren.
Self-Service-Funktionen	**Schwäche**: Häufig eingeschränkte Benutzerfreundlichkeit oder zusätzliche Module erforderlich.	**Stärke**: Benutzerfreundliche Self-Service-Funktionen (z.B. Passwortzurücksetzung) nativ vorhanden.
Abhängigkeit von der Cloud	**Stärke**: Funktioniert auch ohne Cloud, ideal für Unternehmen mit eingeschränktem Internetzugang oder sehr hohen Verfügbarkeitsanforderungen	**Schwäche**: Starke Abhängigkeit von Cloud-Diensten und Internetverfügbarkeit.
Compliance und Audit	**Stärke**: Umfangreiche, anpassbare Audit- und Compliance-Funktionen, oft für spezifische Anforderungen konfigurierbar.	**Schwäche**: Eingeschränkte Berichts- und Auditmöglichkeiten im Vergleich zu spezialisierten IAM-Lösungen.
Skalierbarkeit	**Schwäche**: Kann bei grossen, globalen Umgebungen komplex und schwer skalierbar werden.	**Stärke**: Cloud-native Lösung, die einfach für grosse, globale Unternehmen skaliert werden kann.

Stay tuned, stay secure!

SWISS MADE IAM

abraxas

Delinea
Defining the boundaries of access

ti&m
big ideas. creative technology.

ARCTIC WOLF

COPEBIT

netzmedien

white rabbit
Communications

#6


ITSENSE
Anhang

Stärken und Schwächen

Aspekt	Enterprise IAM (traditionell)	Microsoft Entra ID (Azure AD)
Cloud-Integration	**Schwäche**: Meist auf On-Premise fokussiert, Cloud-Support erfordert oft Zusatzmodule oder Anpassungen.	**Stärke**: Native Cloud- und SaaS-Integration, besonders mit Microsoft 365 und Azure.
On-Premise-Integration	**Stärke**: Tiefe Unterstützung für komplexe On-Premise-Systeme, Legacy-Anwendungen und ältere IT-Infrastrukturen.	**Schwäche**: Eingeschränkte Funktionalität für komplexe On-Premise-Umgebungen, zusätzliche Tools erforderlich (z.B. Azure AD Connect).
Hybride Umgebungen	**Stärke**: Entwickelt für hybride Infrastrukturen, einfache Integration von On-Premise- und Cloud-Ressourcen.	**Schwäche**: Komplexere Konfiguration in hybriden Umgebungen, Synchronisation zwischen lokal und Cloud erforderlich.
Flexibilität und Anpassbarkeit	**Stärke**: Hochgradig anpassbar, geeignet für spezielle Geschäftsanforderungen und branchenspezifische Use-Cases.	**Schwäche**: Weniger anpassbar, standardisierte Lösung ohne tiefere Anpassungsmöglichkeiten.
Sicherheit	**Stärke**: Bietet erweiterte Sicherheitsoptionen, oft in Verbindung mit Drittsystemen konfigurierbar.	Stärke: Integrierte Sicherheitsfunktionen wie MFA, bedingter Zugriff, Zero-Trust-Modelle nativ verfügbar.
Kostenstruktur	**Stärke**: Oft modular, mit einmaligen Lizenzkosten oder niedrigeren On-Premise-Kosten.	**Schwäche**: Abonnementmodell kann mit steigender Benutzeranzahl und Nutzung von Premium-Funktionen kostspielig werden.
Granularität der Zugriffssteuerung	**Stärke**: Sehr granulare Zugriffssteuerung, komplexe Berechtigungsmodelle und detaillierte Rollenverwaltung möglich.	**Schwäche**: Weniger granular als Enterprise IAM-Systeme, eingeschränkte Rollen- und Berechtigungsverwaltung.
Single Sign-On (SSO)	**Schwäche**: SSO für Cloud-Dienste erfordert oft zusätzliche Module oder Integrationen.	**Stärke**: Nahtlose SSO für Cloud- und On-Premise-Anwendungen, besonders im Microsoft-Ökosystem.
Automatisierung (Provisionierung/Deprovisionierung)	**Stärke**: Hohe Automatisierbarkeit, jedoch meist auf On-Premise beschränkt.	**Stärke**: Native automatisierte Provisionierung/Deprovisionierung für Cloud-basierte Anwendungen.
Integration in heterogene Umgebungen	**Stärke**: Entwickelt für heterogene IT-Landschaften, unterstützt viele verschiedene Plattformen und Technologien.	**Schwäche**: Am besten für Microsoft-zentrierte Umgebungen geeignet, schwieriger in Nicht-Microsoft-Umgebungen zu integrieren.
Self-Service-Funktionen	**Schwäche**: Häufig eingeschränkte Benutzerfreundlichkeit oder zusätzliche Module erforderlich.	**Stärke**: Benutzerfreundliche Self-Service-Funktionen (z.B. Passwortzurücksetzung) nativ vorhanden.
Abhängigkeit von der Cloud	**Stärke**: Funktioniert auch ohne Cloud, ideal für Unternehmen mit eingeschränktem Internetzugang oder sehr hohen Verfügbarkeitsanforderungen	**Schwäche**: Starke Abhängigkeit von Cloud-Diensten und Internetverfügbarkeit.
Compliance und Audit	**Stärke**: Umfangreiche, anpassbare Audit- und Compliance-Funktionen, oft für spezifische Anforderungen konfigurierbar.	**Schwäche**: Eingeschränkte Berichts- und Auditmöglichkeiten im Vergleich zu spezialisierten IAM-Lösungen.
Skalierbarkeit	**Schwäche**: Kann bei grossen, globalen Umgebungen komplex und schwer skalierbar werden.	**Stärke**: Cloud-native Lösung, die einfach für grosse, globale Unternehmen skaliert werden kann.

Access Governance Funktionen, die über Entra ID und AWS hinausgehen

Funktion	Enterprise IAM (EIAM)	Microsoft Entra ID (Azure AD)
Rollenbasierte Zugriffskontrolle (RBAC)	Sehr feingranulare Rollenmodellierung, anpassbare Hierarchien und mehrstufige Genehmigungen	Verfügbar, aber oft weniger granular
Risikobasierte Zugriffskontrolle (Risk-Based Access Control)	Vollständig integrierte risikobasierte Modelle, dynamische Berechtigungsvergabe auf Basis von Echtzeitdaten	Eingeschränkt verfügbar, aber nicht tief integriert
Provisioning/De-Provisioning	Erweiterte Automatisierung über diverse Quellsysteme und mehrere Cloud-Plattformen	Automatisierung über Azure AD Connect und SCIM
Multi-Faktor-Authentifizierung (MFA)	Breite Unterstützung für verschiedene MFA-Anbieter, inklusive Integration von physischen Token und Smartcards	Native MFA-Unterstützung (Microsoft Authenticator, FIDO, SMS, etc.)
Single Sign-On (SSO)	Plattformübergreifendes SSO für alle Cloud- und On-Premise-Systeme sowie Legacy-Anwendungen	Unterstützt SSO für Azure- und Microsoft-Services sowie SaaS-Anwendungen
Access Certification & Review	Erweiterte Access-Certification-Prozesse mit benutzerdefinierten Workflows und Auditing-Funktionalitäten	Eingeschränkte Möglichkeiten für regelmässige Überprüfungen von Zugriffsrechten
Audit und Reporting	Erweiterte Berichts- und Auditfunktionen über alle Systeme hinweg, inkl. Compliance-Anforderungen (DSGVO, SOX, etc.)	Standard-Reporting für Microsoft-Dienste, beschränkt auf Azure-Umgebung
Compliance und Governance	Detaillierte Compliance-Management-Tools, anpassbar an branchenspezifische Anforderungen (z.B. E-Government, Finanzwesen)	Grundlegende Compliance-Berichte, z.B. DSGVO-konforme Identitätsverwaltung
Feingranulare Berechtigungssteuerung	Tiefgreifende Berechtigungsmodelle, benutzerdefinierte Zugriffsrichtlinien für spezifische Szenarien und Rollen	Begrenzte granulare Kontrolle, basierend auf Azure-Struktur
Rollen- und Zugriffsmodellierung	Unterstützt komplexe und dynamische Rollen- und Attributmodelle für fein abgestimmte Steuerung	Unterstützt Standard-RBAC und ABAC (Attribute-based Access Control)
Integration in heterogene Umgebungen	Tiefe Integration in Legacy-Systeme, multiple Clouds (Azure, AWS, Google), On-Premise und hybride Umgebungen	Starke Integration in Microsoft-Ökosystem, beschränkte Integration ausserhalb
Self-Service für Benutzer	Umfassende Self-Service-Portale für Benutzer, um Zugriffsanforderungen, Genehmigungen und Rollenänderungen anzustossen	Verfügbar für grundlegende Aufgaben (Passwortrücksetzung, Rollenanforderung)
Dynamische Rollen	Umfassende dynamische Rollen basierend auf Echtzeit-Attributen und Geschäftslogiken	Grundlegende Unterstützung für dynamische Zuweisungen
Cloud-Hybrid-Unterstützung	Erweiterte Unterstützung für hybride Umgebungen, die mehrere Cloud-Anbieter und On-Premise-Systeme umfassen	Native Unterstützung für hybride Azure-Umgebungen