



SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10.
MAI
2023

Rolle der SAP® Cloud Identity Services im Kontext IAM

Carsten Olt | Xiting GmbH & Alexander Schaffelke | Xiting AG

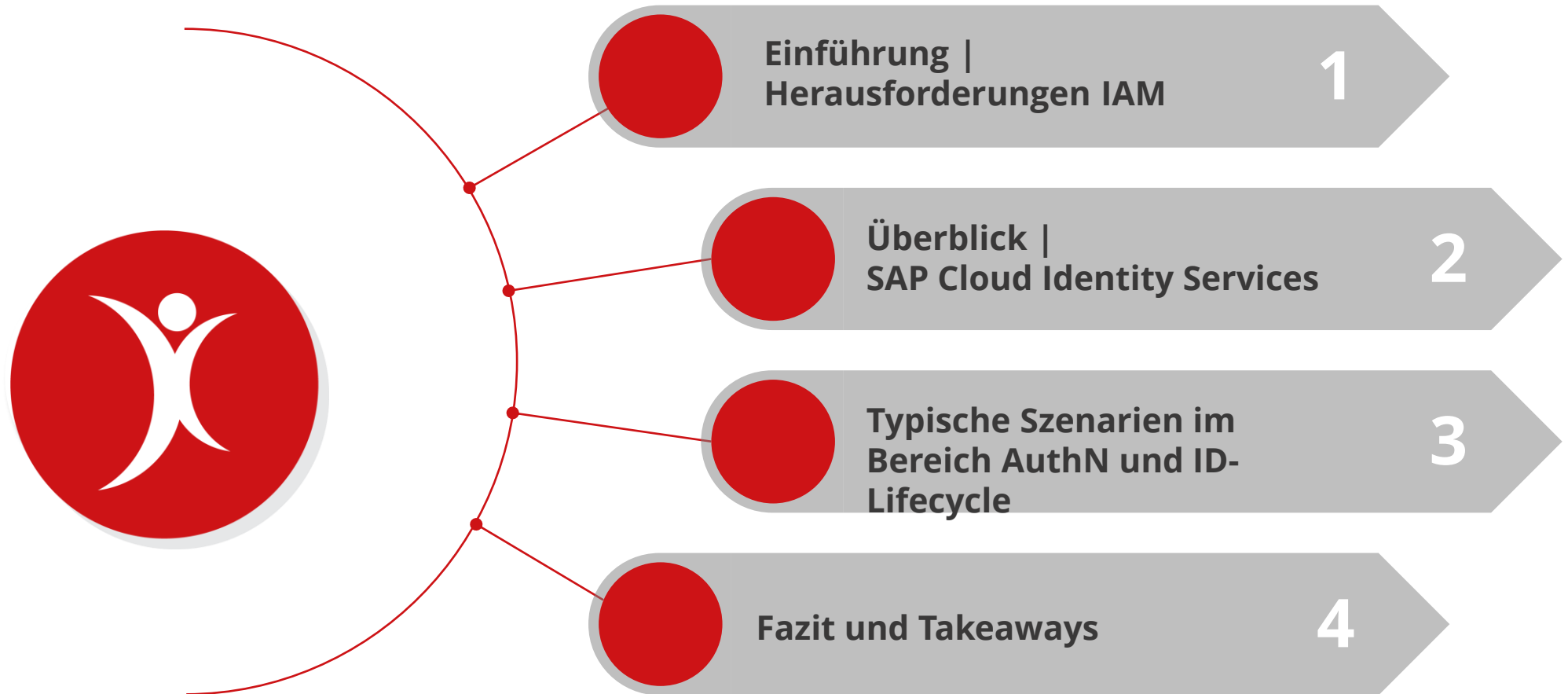
- 1. Einführung | Herausforderungen IAM**
- 2. Überblick | SAP Cloud Identity Services**
- 3. Typische Szenarien im Bereich AuthN und ID-Lifecycle**
- 4. Fazit und Takeaways**



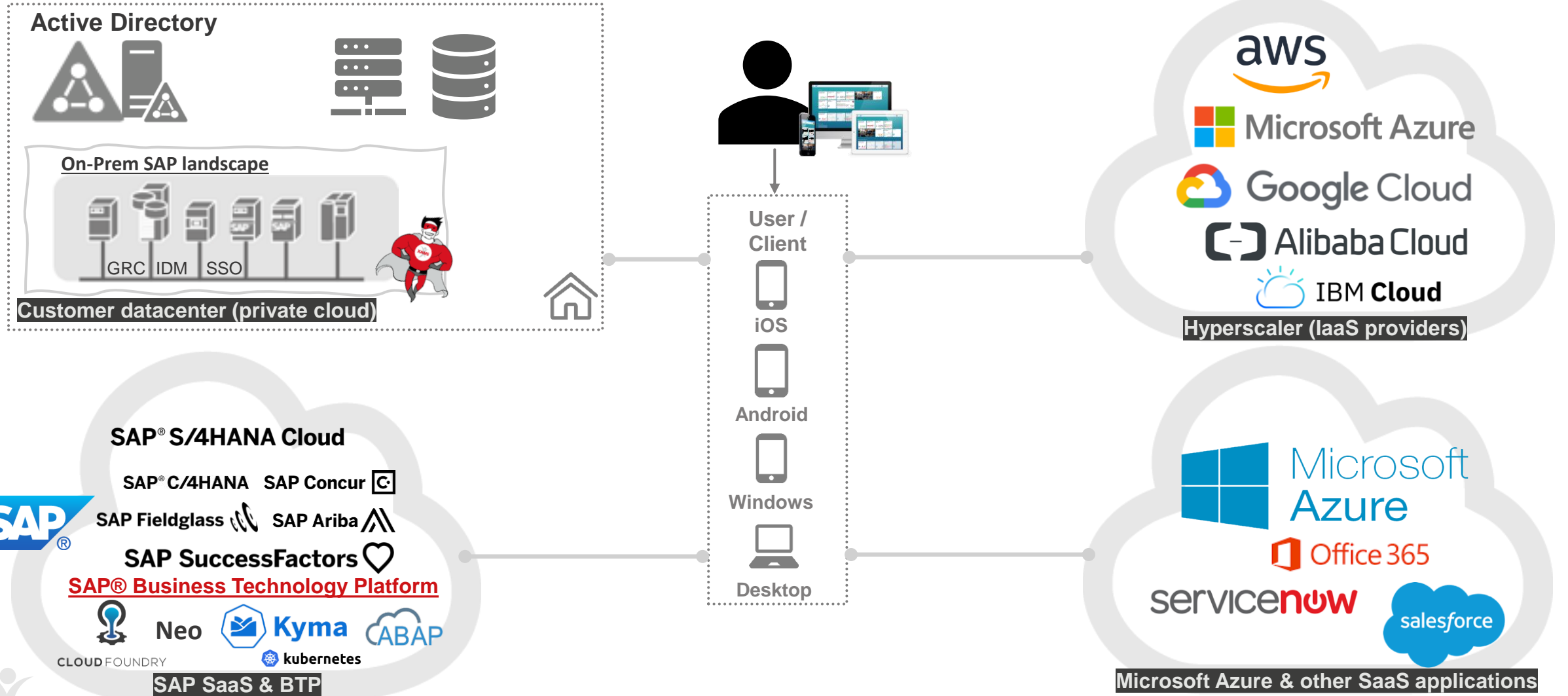
Kapitel 1

Einführung | Herausforderungen IAM

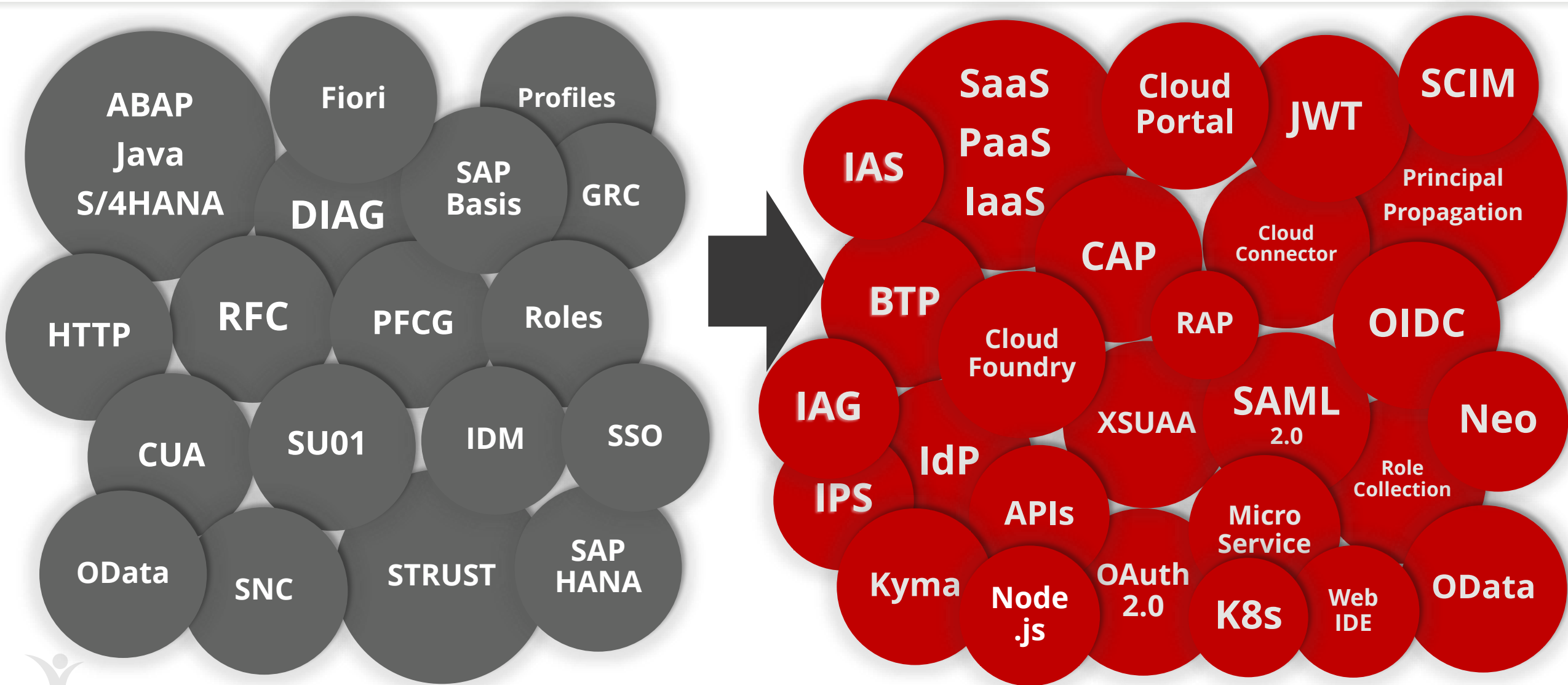
Agenda



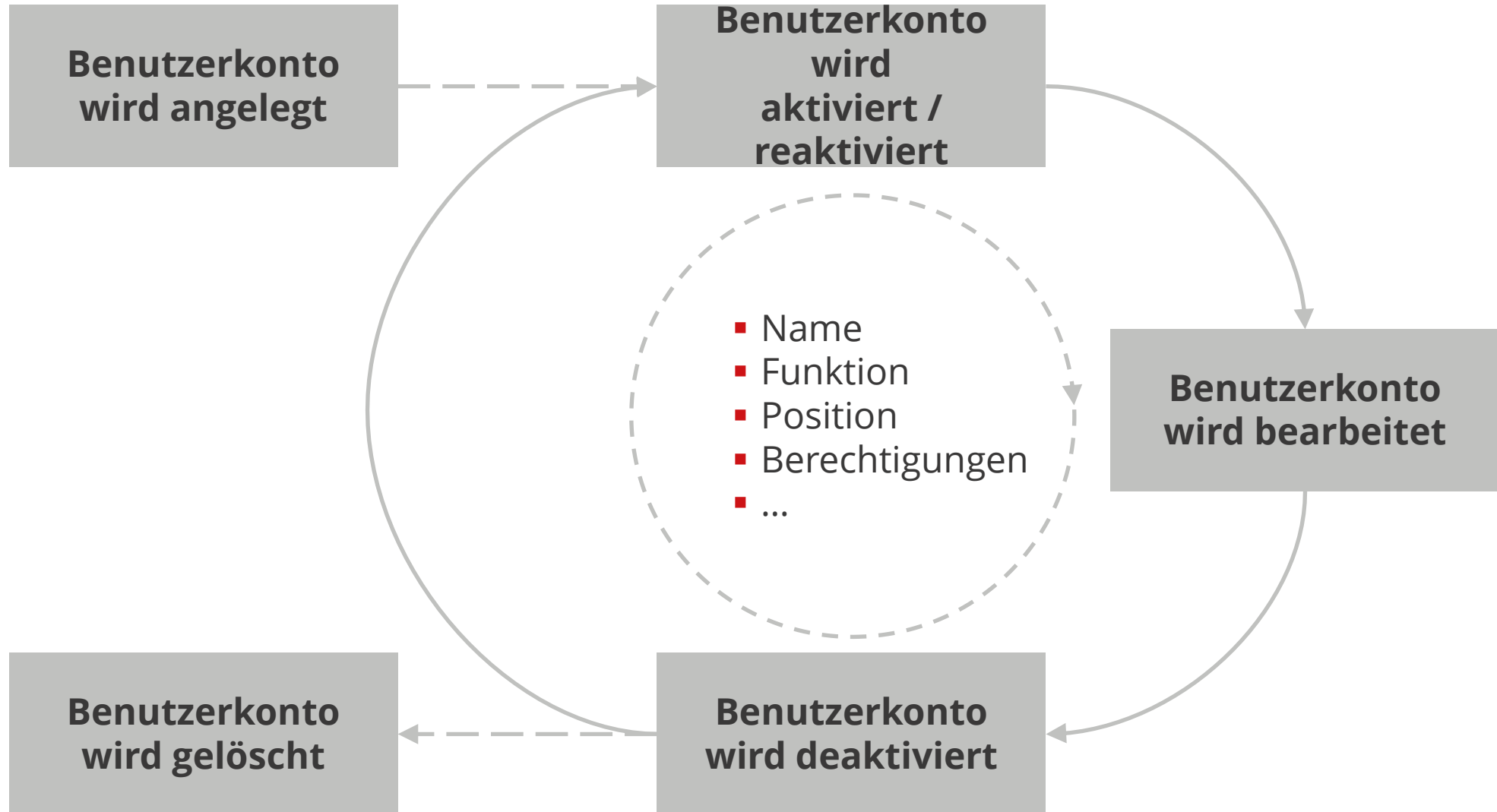
Die SAP Wolke, eine unter vielen



Neue Technologie → Neue Standards und Schnittstellen



Herausforderung: Identity Lifecycle



Wichtige Aspekte in der IAM-Sicherheitsstrategie



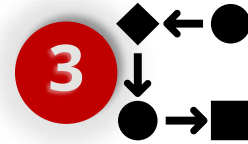
Identifizieren der Personas

- Mitarbeiter
- Partner
- Kunden
- Auftragnehmer



Authentifizierungs-Anforderungen pro Nutzertyp:

- Authentifizierung und SSO
- Risikobasierte Authentifizierung und MFA
- FIDO2 und Biometrie
- Unternehmens-Identitätsanbieter
- Geräteintegrität und Zugriffsrichtlinien



Zugriffssteuerung und Identitätslebenszyklus

- Standard-Schnittstellen
- Aggregierter Endpunkts für die Benutzerbereitstellung
- Automatisierung des ID-Lebenszyklus
- Integration mit IDM-Systemen
- Automatisierung mit Workflows

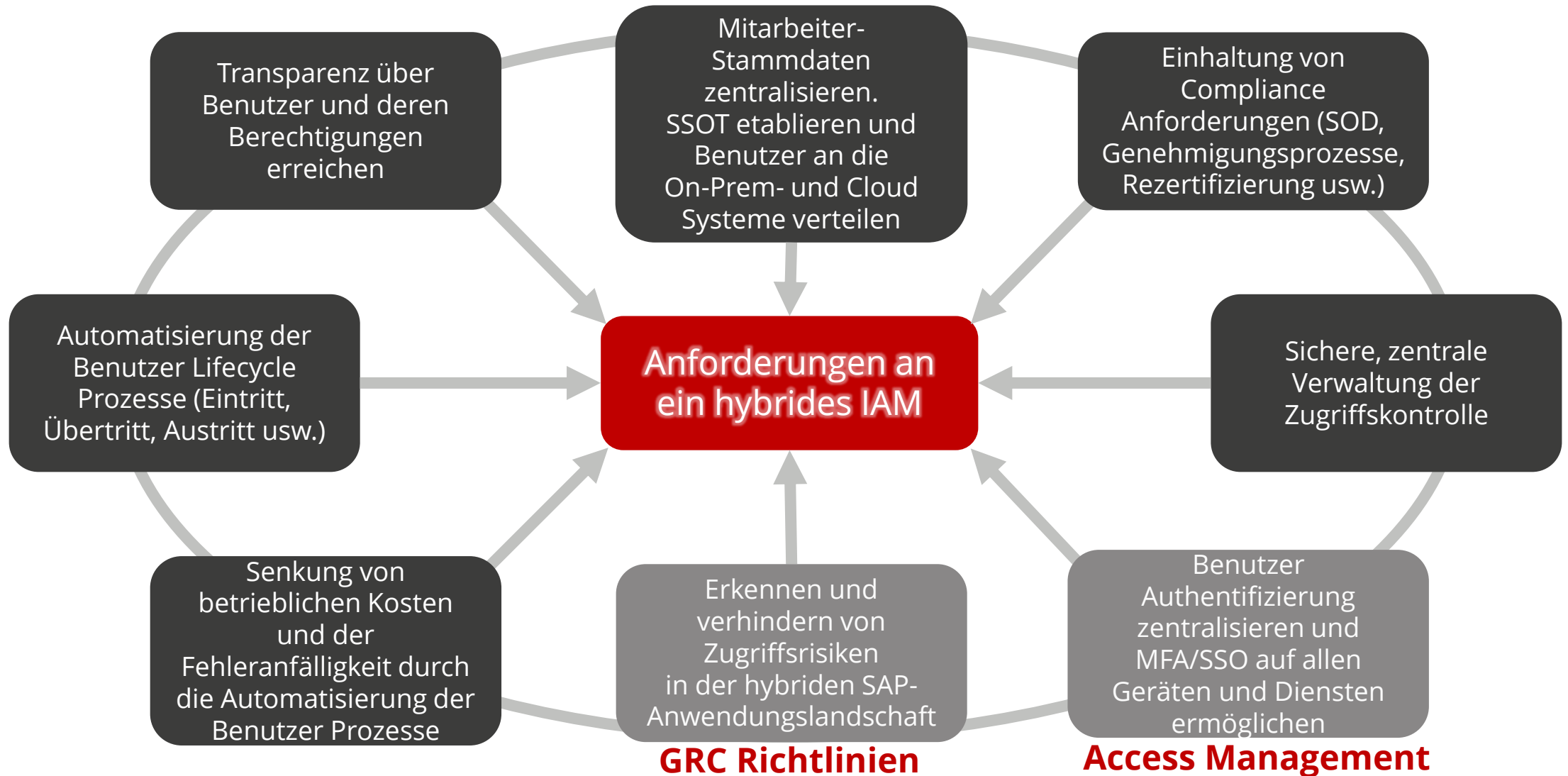


Rollendesign und -Berechtigungen

- RBAC-AuthZ
- Mapping der Rollen für Cloud- und On-Prem Anwendungen
- Zugriffskontrolle
- Governance und Compliance
- SOD-Prüfungen



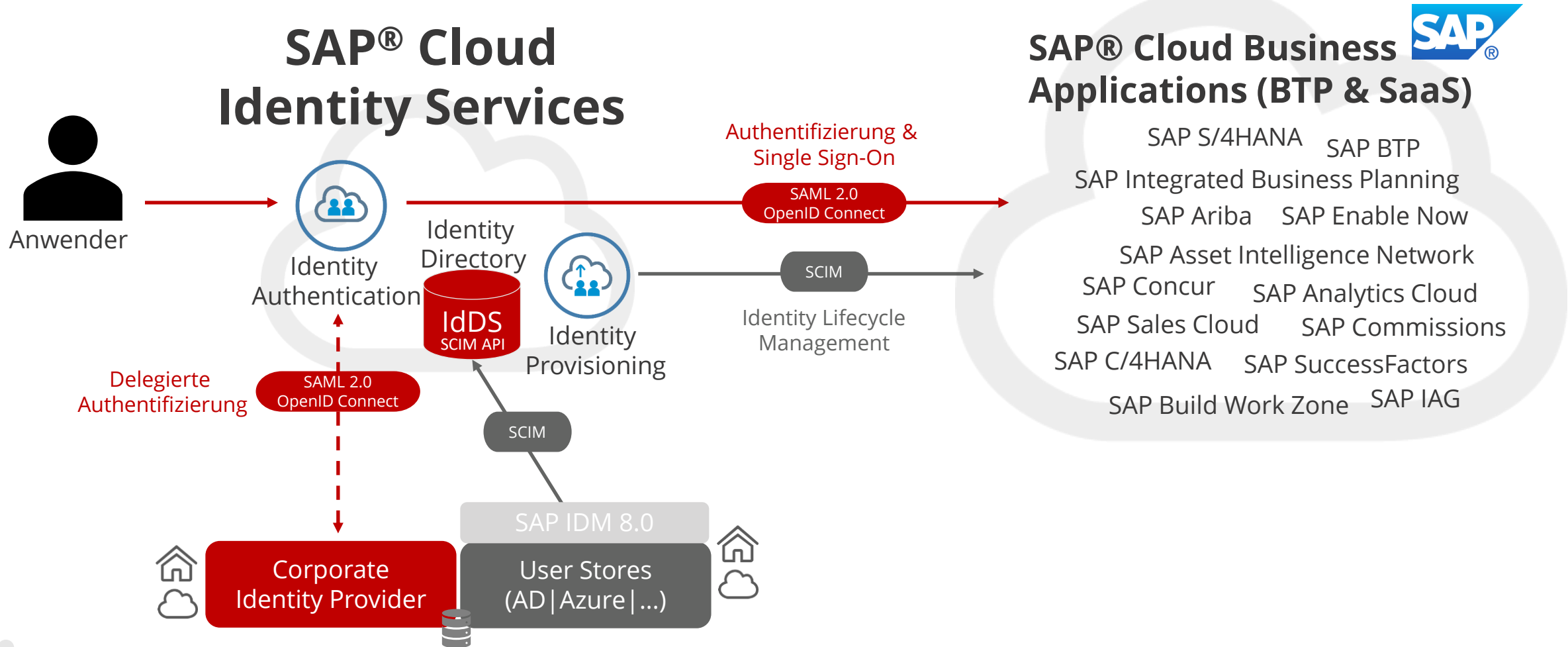
Herausforderung: IAM



Kapitel 2

Überblick | SAP Cloud Identity Services

Überblick | SAP Cloud Identity Services



Aufgabe pro Komponente im Überblick | SAP Cloud Identity Services

Identity Authentication IAS

- Haupt-IDP für alle SAP-Anwendungen
- Automatisiert/Konsolidiert das Vertrauensmanagement
- Standardisiert den Onboarding-Prozess
- Unterstützt SAML 2.0 und OpenID Connect
- Integration an bestehende IDPs als Proxy und Support für ID-Federation

Identity Directory IdDS

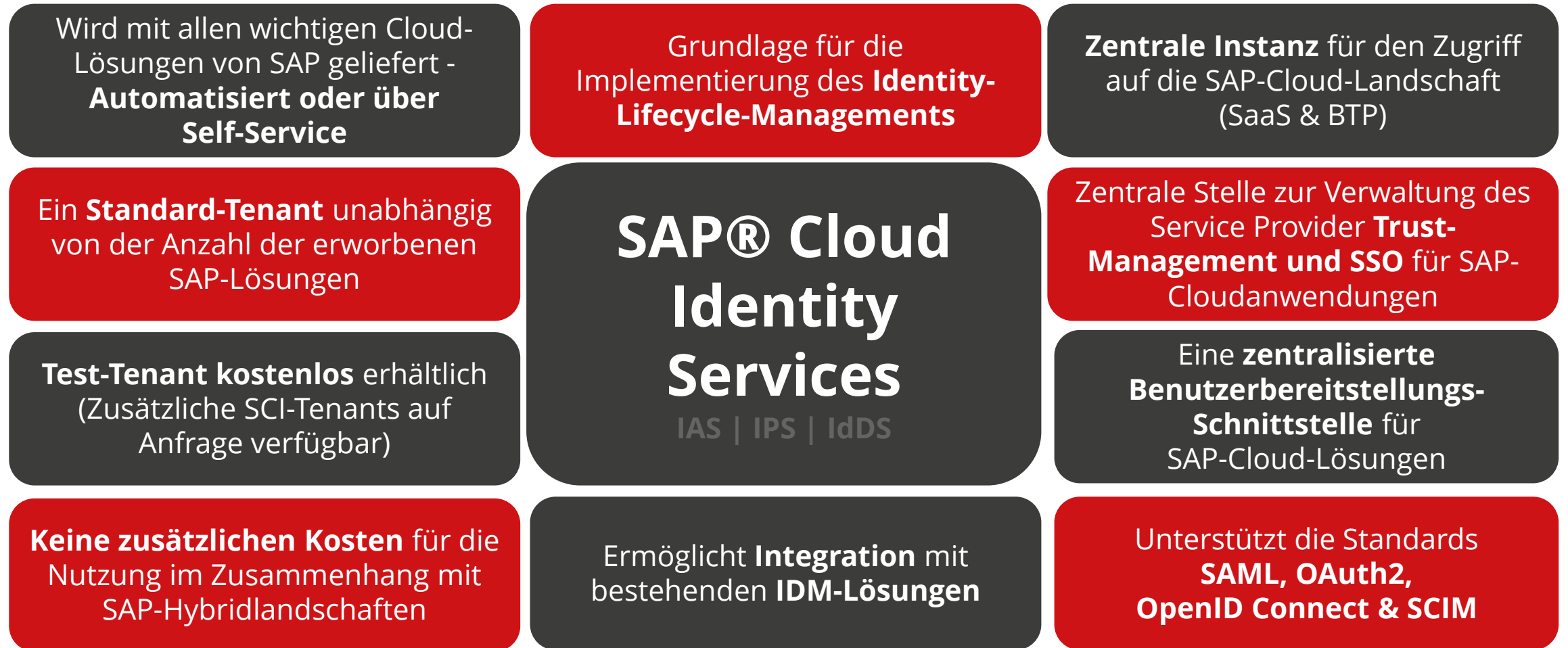
- Zentrale Benutzerdatenbank
- Grundlage zur Automatisierung des Identitätslebenszyklus
- SCIM 2.0 REST-API mit Support von bis zu 400 kundeneigenen Attributen
- Benutzerpersistenz (SAP Global User ID) als Voraussetzung für SAP SuccessFactors und SAP Task Center

Identity Provisioning IPS

- Einfache Möglichkeit zur Automatisierung des Identitätslebenszyklus
- Integration mit IDM-Lösungen
- Unterstützung des SCIM-Protokolls
- Ausgeliefert mit Konnektoren für die wichtigsten Anwendungen
- JSON-Transformations-Framework
- Keine Feature-Parität mit IDM



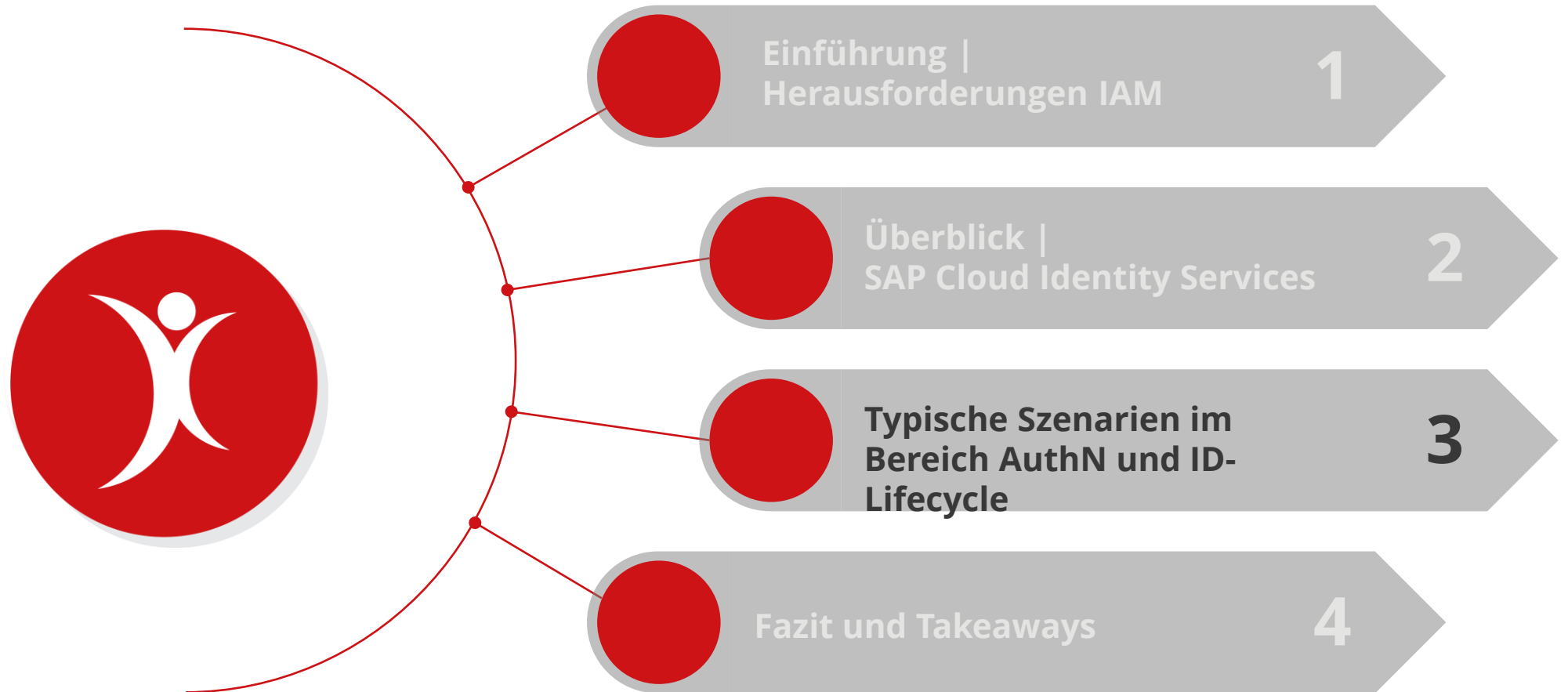
Zusammenfassung | SAP Cloud Identity Services



Kapitel 3

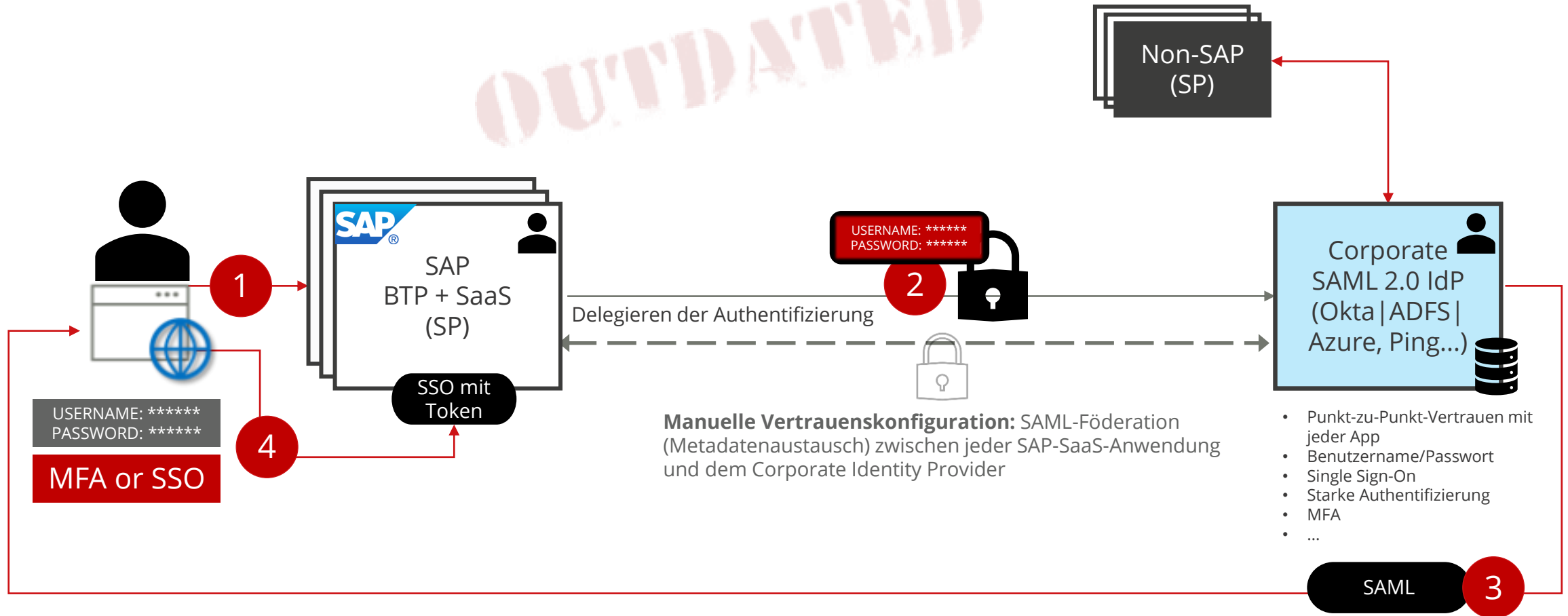
Typische Szenarien im Bereich AuthN und ID-Lifecycle

Agenda



Veralteter Ansatz | SAP SaaS & BTP mit einem vorhandenen IdP

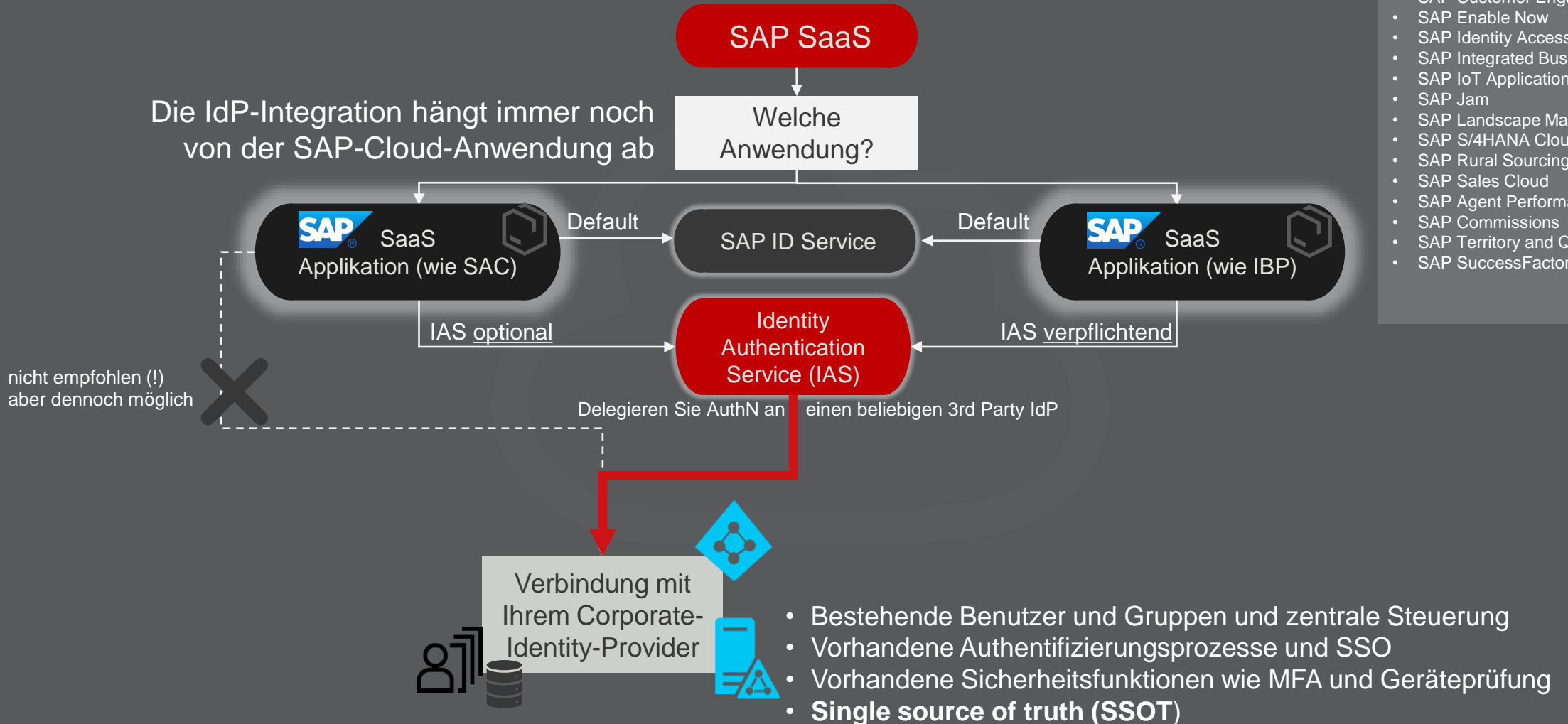
OUTDATED



SAP Cloud Identity Services | AuthN & SSO an SaaS Anwendungen

Mai 2023 - SAP IAS verpflichtend für:

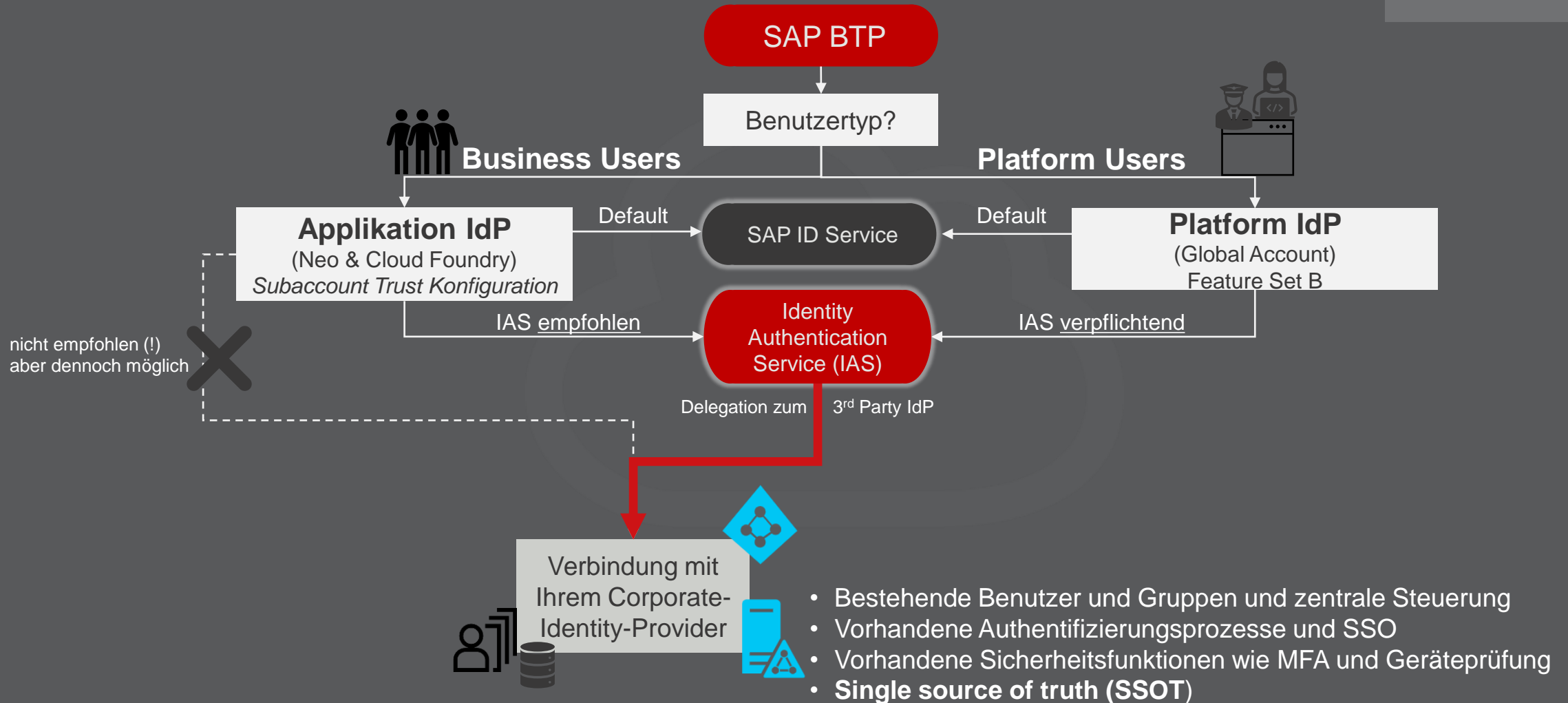
- SAP Asset Intelligence Network
- SAP Build Work Zone
- SAP Customer Engagement Center
- SAP Enable Now
- SAP Identity Access Governance
- SAP Integrated Business Planning
- SAP IoT Application Enablement
- SAP Jam
- SAP Landscape Management Cloud
- SAP S/4HANA Cloud
- SAP Rural Sourcing Management
- SAP Sales Cloud
- SAP Agent Performance Management
- SAP Commissions
- SAP Territory and Quota
- SAP SuccessFactors



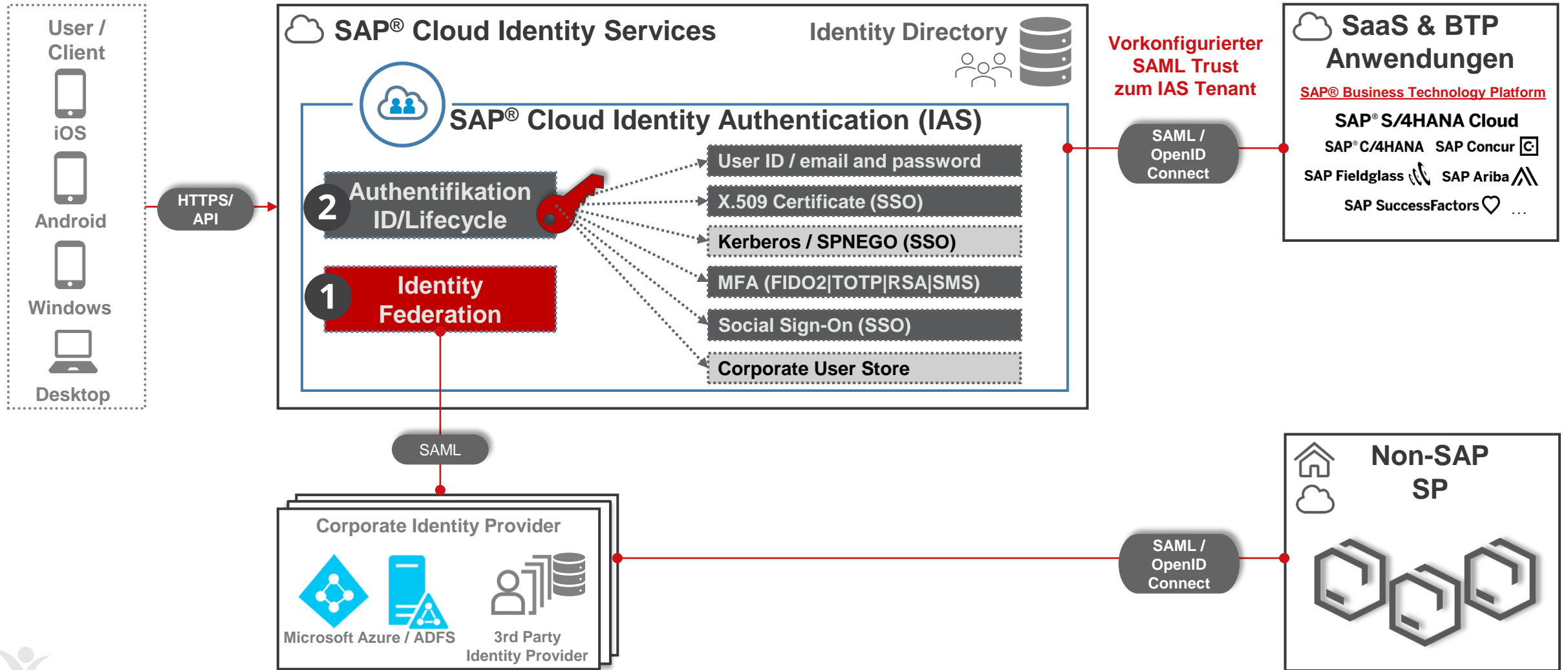
SAP Cloud Identity Services | AuthN & SSO für die BTP

Weitere Infos

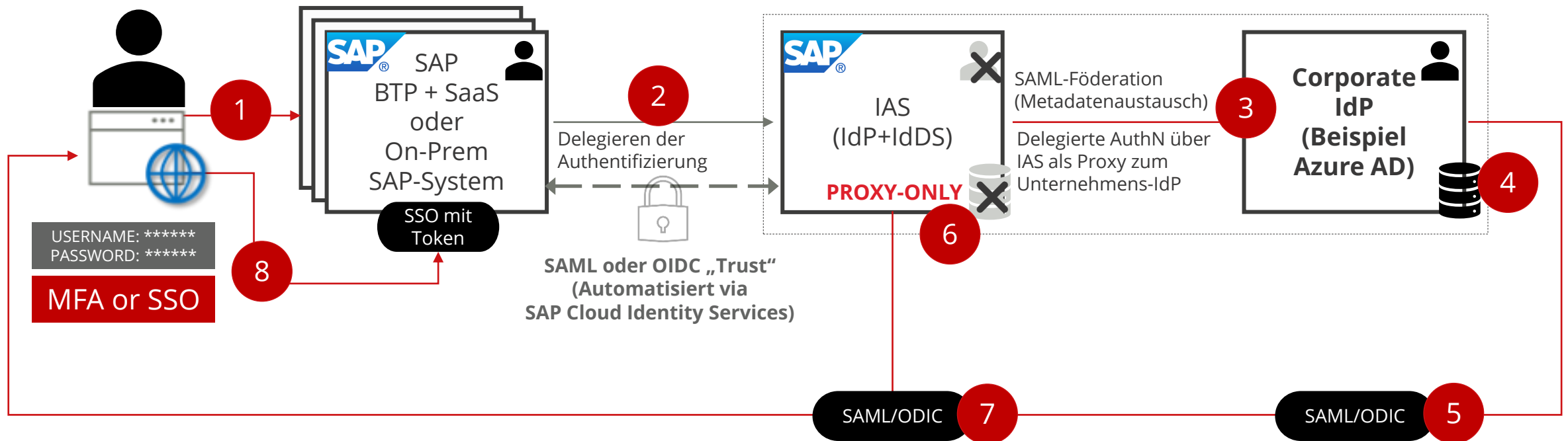
- [Link zum SAP Community Blog](#)
- [Link SAP Documentation](#)



SAP Cloud Identity Authentication Service



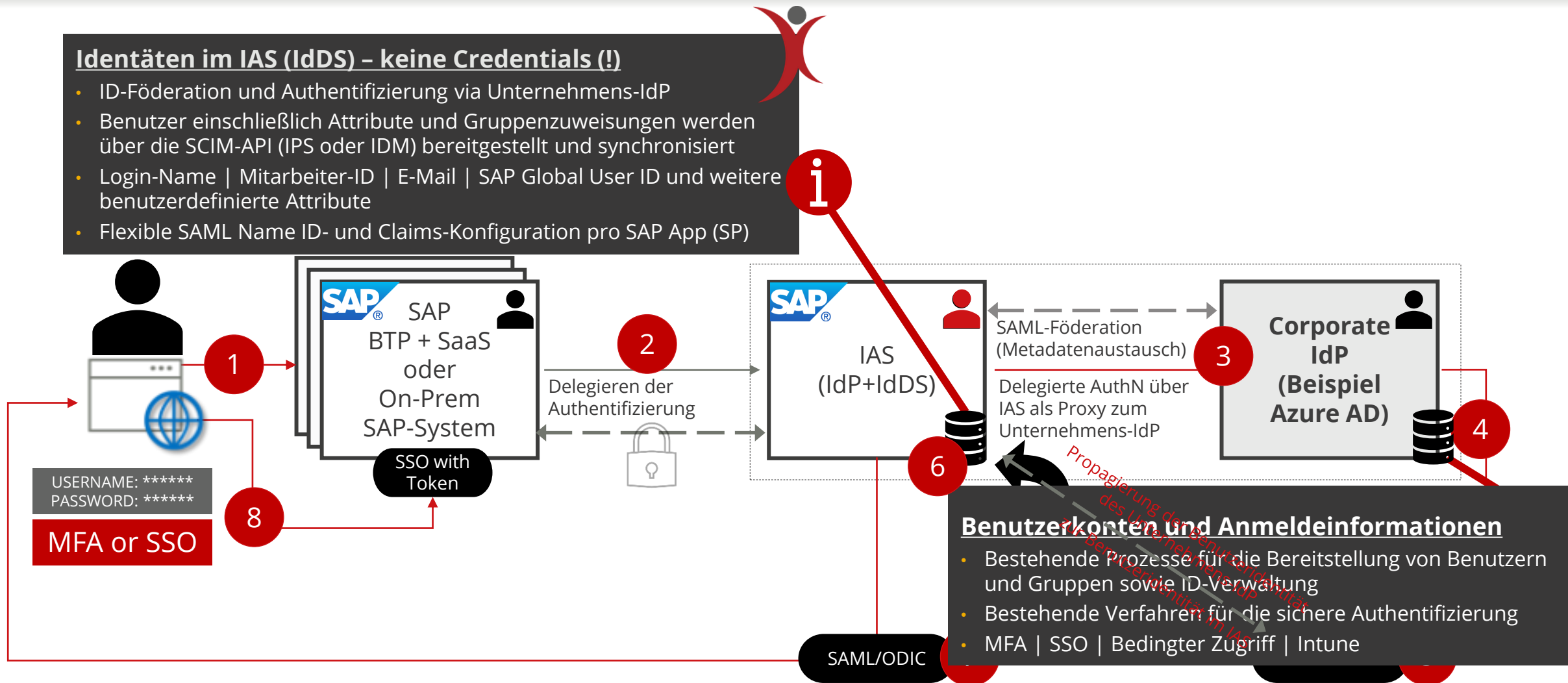
Meist der erste Schritt | SAP IAS und der Unternehmens-IdP (Proxy-Only-Szenario)



Empfohlenes Szenario | Identitätsföderation zwischen IAS & Unternehmens-IdP

Identitäten im IAS (IdDS) – keine Credentials (!)

- ID-Föderation und Authentifizierung via Unternehmens-IdP
- Benutzer einschließlich Attribute und Gruppenzuweisungen werden über die SCIM-API (IPS oder IDM) bereitgestellt und synchronisiert
- Login-Name | Mitarbeiter-ID | E-Mail | SAP Global User ID und weitere benutzerdefinierte Attribute
- Flexible SAML Name ID- und Claims-Konfiguration pro SAP App (SP)

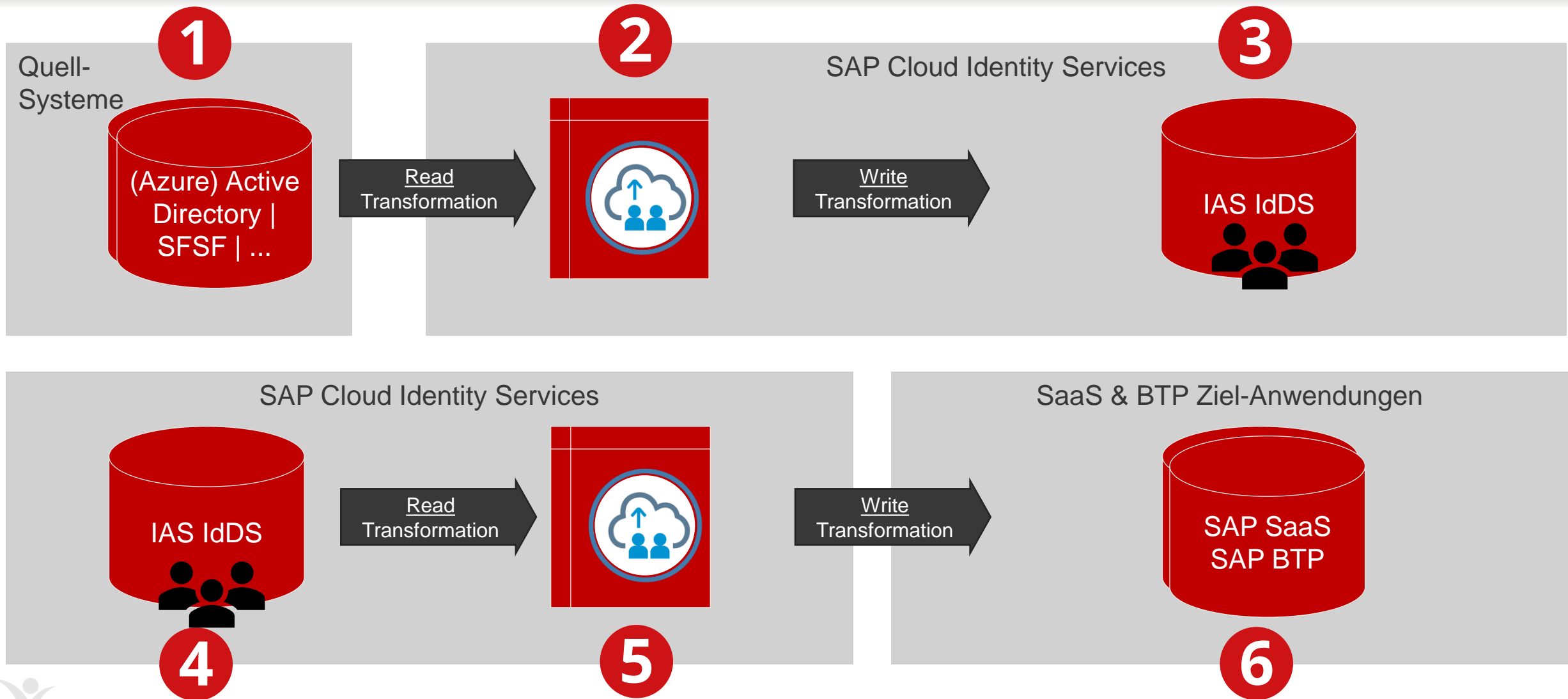


Benutzerkonten und Anmeldeinformationen

- Bestehende Prozesse für die Bereitstellung von Benutzern und Gruppen sowie ID-Verwaltung
- Bestehende Verfahren für die sichere Authentifizierung
- MFA | SSO | Bedingter Zugriff | Intune

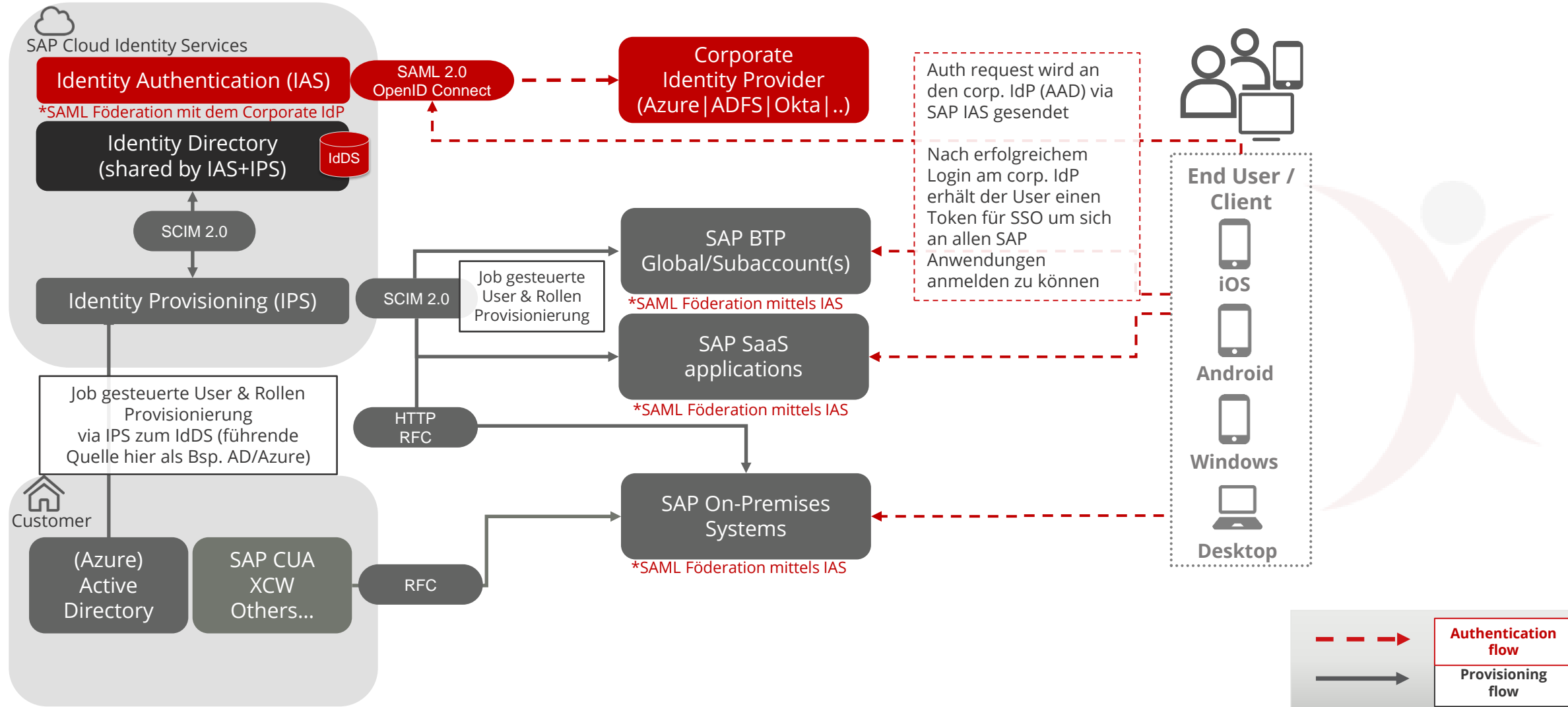


Identitätslebenszyklusmanagement mit SAP IPS | Beispiel-Szenario



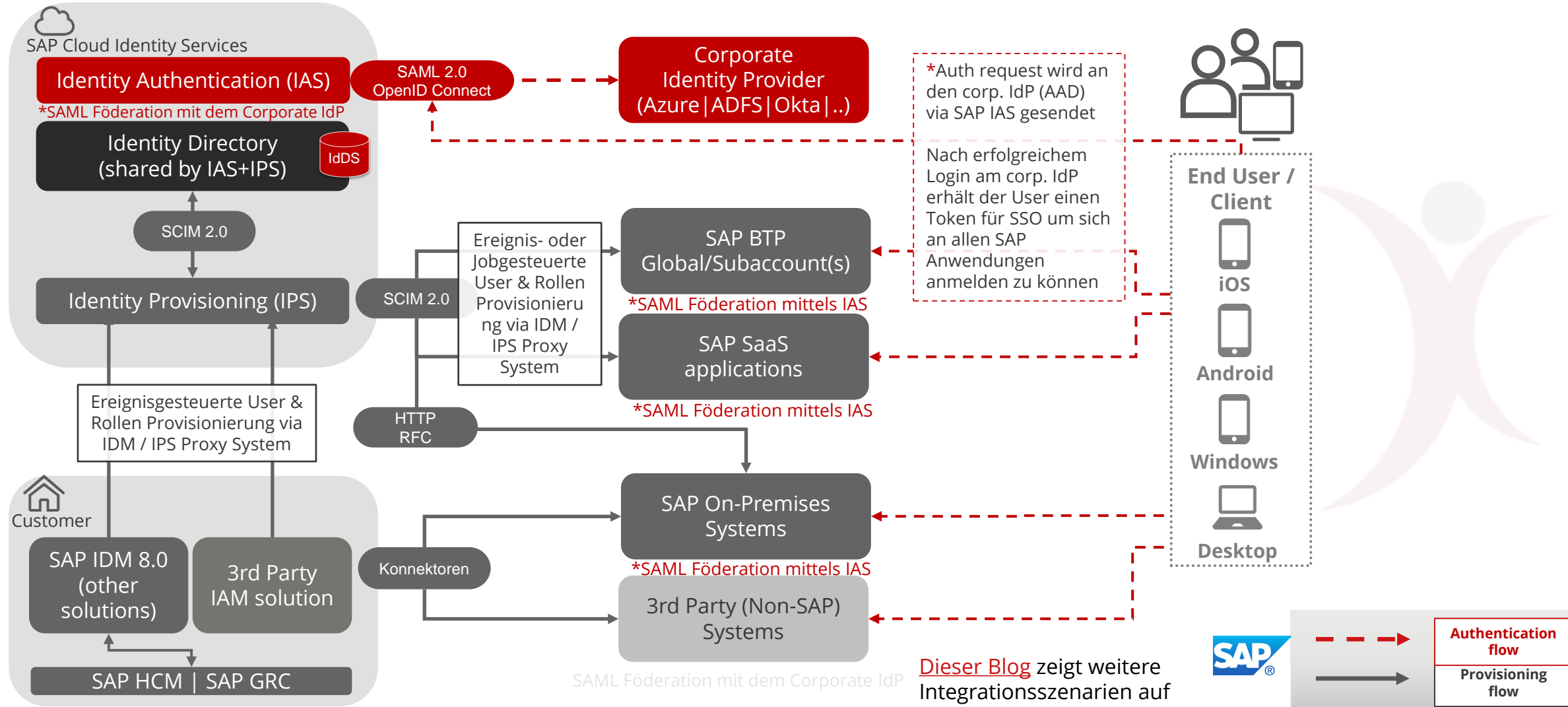
Identity & Access Management und Single Sign-On

Einsatz ohne ein Identity Management System



Hybrides Identity & Access Management und Single Sign-On

Integration mit einer zentralen SAP Identity-Management-Lösung



Kapitel 4

Fazit und Takeaways

Takeaways | SAP Cloud Identity Services – Xiting Best Practices

Authentication & SSO

- SSO & MFA für alle SAP-Anwendungen
- Automatisierung SAML-Trust-Management (Metadaten austausch)
- Flexible SAML Name-ID- und Claim-Konfigurationen pro Anwendung
- Integration mit allen SAP SaaS- und BTP-Anwendungen sowie SAP-Systemen
- Einbindung des eigenen IDP via IAS als IDP-Proxy
- Regelbasierte Risikobasierte Authentifizierung für spezifische Benutzergruppen- und Anwendungen



Identity Lifecycle + IDM Integration

- Aufbau zentraler Identity Services Tenants
- Integrieren führender Quellsysteme
- Persistieren der Identitätsinformationen und wichtiger Benutzerattribute im IdDS
- Zentraler User-Provisioning-Endpunkt
- Automatisieren des ID-Lifecycle für SAP-Cloudanwendungen mit einfachen Jobs
- **Optional:** Integrieren vorhandener IDM-Lösungen via SCIM
- **Optional:** Erkennen und verhindern von Zugriffsrisiken in der hybriden Landschaft durch **Integration mit SAP IAG**

Takeaways | Weitere Informationsquellen

DER SAP SYSTEM INTEGRATION GUIDE ENTHÄLT UMFASSENDE, SZENARIO- SPEZIFISCHE EMPFEHLUNGEN

- https://help.sap.com/docs/SAP_CLOUD_IDENTITY/b95c3d5bab324a3a8409eee5267a5b75/27947dfb325047018603446439050a6b.html

SAP CIO GUIDE: IDENTITY LIFECYCLE IN HYBRIDEN LANDSCHAFTEN

- <https://www.sap.com/documents/2018/05/38ce7d25-067d-0010-87a3-c30de2ffd8ff.html>

WIR EMPFEHLEN DIE REFERENZARCHITEKTUR-BLOGS VON SAP FÜR SSO UND IDENTITY LIFECYCLE MANAGEMENT:

- <https://blogs.sap.com/2022/11/02/sap-cloud-identity-services-why-and-how-to-integrate-them-for-a-consistent-identity-lifecycle/>
- <https://blogs.sap.com/2021/09/24/single-sign-on-sap-reference-architecture-for-identity-access-management/>
- <https://blogs.sap.com/2021/09/27/identity-lifecycle-sap-reference-architecture-for-identity-access-management-part-1/>
- <https://blogs.sap.com/2021/09/28/identity-lifecycle-sap-reference-architecture-for-identity-access-management-part-2/>



Takeaways | Xiting Blogs

XITING BLOGS | SAP CLOUD SECURITY

- <https://xiting.com/en/explained-1-sap-ias-proxy-mode-and-id-federation/>
- <https://xiting.com/en/quickstart-implementation-service-for-sap-cloud-identity-services/>
- <https://blogs.sap.com/2023/02/16/updates-from-sap-teched-concerning-sap-cloud-identity-services/>
- <https://blogs.sap.com/2022/10/06/connecting-sap-ias-as-a-proxy-to-azure-ad-using-openid-connect/>
- <https://xiting.com/en/connecting-sap-identity-authentication-service-to-azure-ad/>
- <https://xiting.com/en/xitings-cloud-security-services-with-focus-on-iam/>



Takeaways | SAP Cloud Identity Services – Xiting Best Practices (E-BOOK)

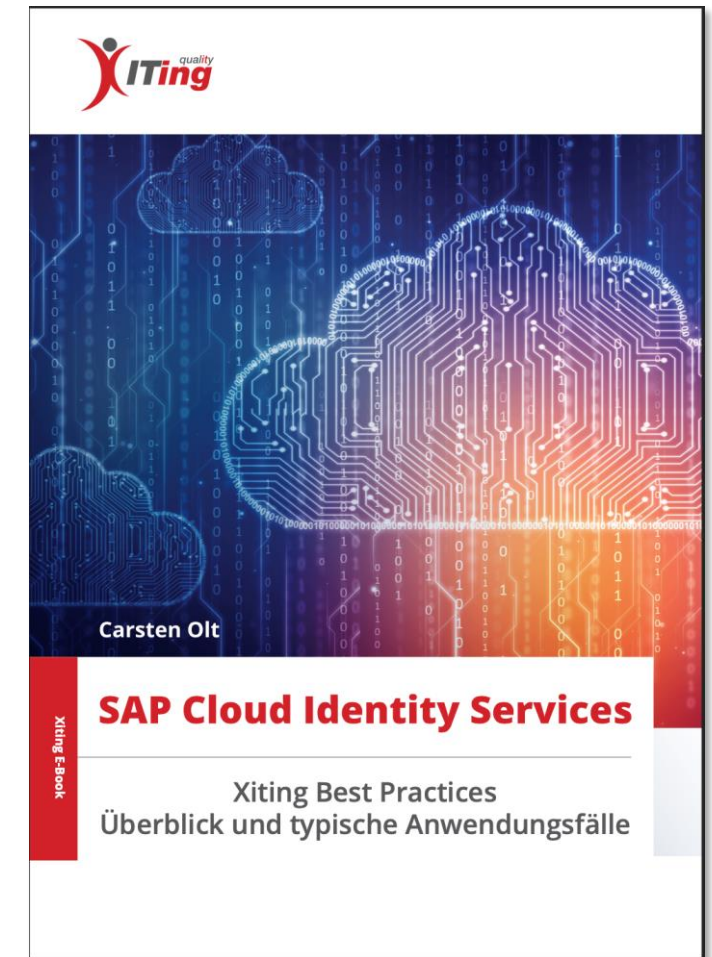
EXKLUSIVES E-BOOK:

SAP CLOUD IDENTITY SERVICES

ÜBERBLICK – BEST PRACTICES – ANWEDUNGSFÄLLE

- In unserem eBook bieten wir einen kompakten Überblick zu den SAP® Cloud Identity Services, einschließlich gängiger Anwendungsfälle und Xiting Best Practices.
- Liefert allen Interessenten im Kontext hybrides SAP IAM einen schnellen und auf das Wesentliche komprimierten Überblick.
- Die Zielgruppe sind Architekten, Projektverantwortliche, SAP-Berater und IDM-Administratoren.
- Unser neues eBook bietet umfassende Informationen zu den SAP Cloud Identity Services, einschließlich verschiedener ID-Lebenszyklus- und Anwendungsfälle und bietet Anleitungen zur Integration von SAP IDM 8.0 als primäres System für den hybriden IDM-Betrieb.

Weitere [Informationen](#)



Takeaways | Xiting QuickStart Implementation Service

BEST PRACTICE KONFIGURATION DER SAP CLOUD IDENTITY SERVICES

Vorteile

- Best Practice Aufbau als zukunftssichere Grundlage zur Verwaltung von Zugriffen und Identitäten in hybriden SAP-Landschaften.

Umfang

- Einrichtung und Integration der Dienste im Rahmen eines Piloten. Konfiguration von 2 SAP-Cloudanwendungen einschließlich SSO und ID-Lifecycle (Quelle: Azure AD).

Zielgruppe

- Kleine und mittlere Unternehmen die kein IDM im Einsatz haben und keine Freigabe-Workflows benötigen.

Weitere [Informationen](#)

DACHHALTIGE VORTEILE

- Das QuickStart-Implementierungspaket macht Sie schnell startklar
- Eine konfigurierte Lösung, die Ihren Geschäftsanforderungen entspricht
- Unsere Experten beantworten individuelle Fragen mit Ihrem umfangreichen Wissen
- Eine klare Strategie und eine etablierte Grundlage für die Integration Ihrer weiteren (SAP-Cloud-) Anwendungen
- Der Service umfasst vorlagenbasierte Ansätze, einschließlich Best Practices, und nutzt die Erfahrungen aus früheren Projekten
- Vorgegebenes Budget und Umfang ermöglichen es Ihnen, entsprechend zu planen
- Ein etablierter zentraler Hub, der für die Benutzeranerkennung und Bereitstellung Ihrer SAP-Cloud-Anwendungslandschaft verantwortlich ist

- Integration mit Ihrem SAML-Identitätsanbieter, um vorhandene Authentifizierungsprozesse und SSO-Funktionen zu nutzen
- Automatisierung Ihrer User-Lifecycle-Prozesse für SAP-Cloud-Anwendungen und Reduzierung von Fehlern sowie manuellem Aufwand
- Einsatz einer auftragsgesteuerten SCIM-basierten Bereitstellung von Benutzern, Gruppen und Berechtigungsrollenzuweisungen
- Ermöglicht die flexible Konfiguration von SAML-NameID-Format und -Ansprüchen für Ihre SAP-Anwendungen (AuthN und AuthZ)
- Abdeckung von Sicherheitsempfehlungen wie bedingte und risikobasierte Authentifizierung einschließlich MFA- und FIDO2-Unterstützung
- Einsatz in Szenarien auch ohne SAP IDM oder Drittanbieter IDM-Lösung

DIE SAP CLOUD IDENTITY SERVICES BESTEHEN AUS ZWEI HAUPTKOMPONENTEN:

SAP Cloud Identity Authentication (IAS)

- Best-Practice-Konfiguration und Ermittlung Ihres IAS-Tenant-Modells
- Integration mit Ihrem bestehenden SAML-Identitätsanbieter (ADFS, Azure, Okta, ...)
- Erstellung von zwei Cloud- oder On-Prem-SAP-Anwendungen in Ihrem IAS (SAML, Trust)

SAP Cloud Identity Provisioning (IPS)

- Best-Practice-Konfiguration und Ermittlung Ihres IPS-Tenant-Modells
- Anbindung Ihres Azure Active Directory Tenant als zentrales Quellsystem zur Benutzerverteilung (weitere Quellen auf Anfrage)
- Einrichtung eines einfachen Benutzergruppenkonzepts zur Verwaltung des ID-Lebenszyklus und der Authentifizierung
- Johngesteuerte Bereitstellung von Benutzern und Gruppen für zwei SAP-Cloud-Anwendungen (SAP BTP & SaaS)

STARTEN SIE IHRE REISE IN DIE SAP-CLOUD-WELT

In einer hybriden SAP-Landschaft ist die Koordination des Zugriffs auf die verschiedenen Anwendungen ein Muss und erfordert ein reibungsloses, effizientes und zentrales Benutzer- und Authentifizierungsmanagement. Erhalten Sie Best Practices und den neuen Implementierungsservice von Xiting zum Festpreis.

Unser Xiting QuickStart-Implementierungspaket ist der schnellste Weg, um Ihr Unternehmen für die SAP Cloud Identity Services einzurichten. Dieser umfasst einen festen Leistungsumfang, der unmittelbare Vorteile und grundlegende Funktionen für die Benutzeranerkennung und -bereitstellung bietet. Dies ist eine Kernanforderung für alle Integrations- und/oder Erweiterungsszenarien, wenn es um SAP BTP- und SaaS-Anwendungen geht.

TYPISCHE HERAUSFORDERUNGEN

- Sie möchten eine zukunftssichere Grundlage schaffen, die den Übergang Ihrer bestehenden User-Lifecycle-Prozesse in das SAP-Cloud-Universum unterstützt
- Sie möchten Ihren User-Lifecycle-Prozess mit Standard-Tools automatisieren und optimieren
- Sie müssen zusätzliche SaaS-Anwendungen wie SAP Analytics Cloud, SAP Integrated Business Planning, SAP Arriba und mehr integrieren
- Sie benötigen mehr Transparenz in der komplexen Hybridarchitektur
- Sie benötigen eine Integration mit Ihrem Active Directory, Azure AD oder externen Identitätsanbieter (Drittanbieter)

Haben Sie spezifischere Anforderungen? Erhalten Sie Ihr individuelles Paket!

- Integrieren Sie Ihr bestehendes Identity Management System zur Unterstützung von Businessrollen und Workflow-basierender Benutzerverwaltung
- Integrieren Sie weitere Quellsysteme, um Ihre Benutzeridentitäten mit zusätzlichen Attributen wie HCM/SFSF anzureichern
- Entwickeln Sie individuelle Berechtigungskonzepte für Ihre SaaS- und BTP-Anwendungen.

5 Tage

Remote

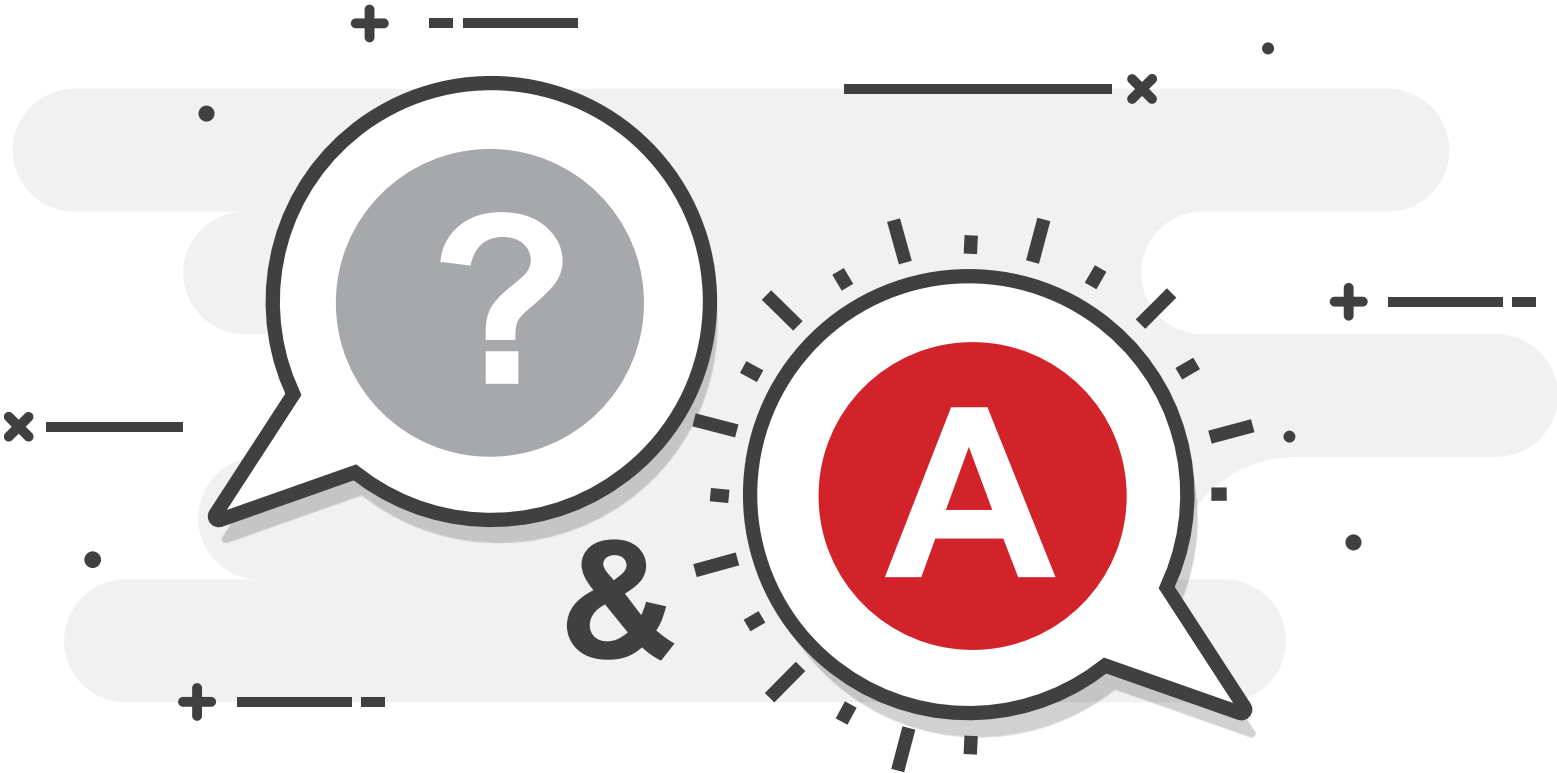
zum Festpreis

Weiterführende Informationen:
cloud-services@xiting.com
www.xiting.com

© 2023 Xiting. All rights reserved.

*Umfang individuell erweiterbar







Carsten Olt

Managing SAP Security Consultant

CISA



Alexander Schaffelke

SAP Security Consultant

Xiting GmbH

Obere Ringstraße 17

79859 Schluchsee

Germany

Vielen Dank
Für Ihre Aufmerksamkeit

Kontaktieren Sie uns unter:
cloud-services@xiting.com

© 2022 Xiting. All rights reserved.

Alle erwähnten Produkt- und Dienstleistungsamen sind Marken der jeweiligen Unternehmen. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung der Xiting AG in irgendeiner Form oder zu irgendeinem Zweck vervielfältigt oder übertragen werden. Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

