SAP Security Group Deutschland

Xiting Kunden-Event
mit Partnern

9./10. MAI 2023

Rolle der SAP® Cloud Identity Services im Kontext IAM

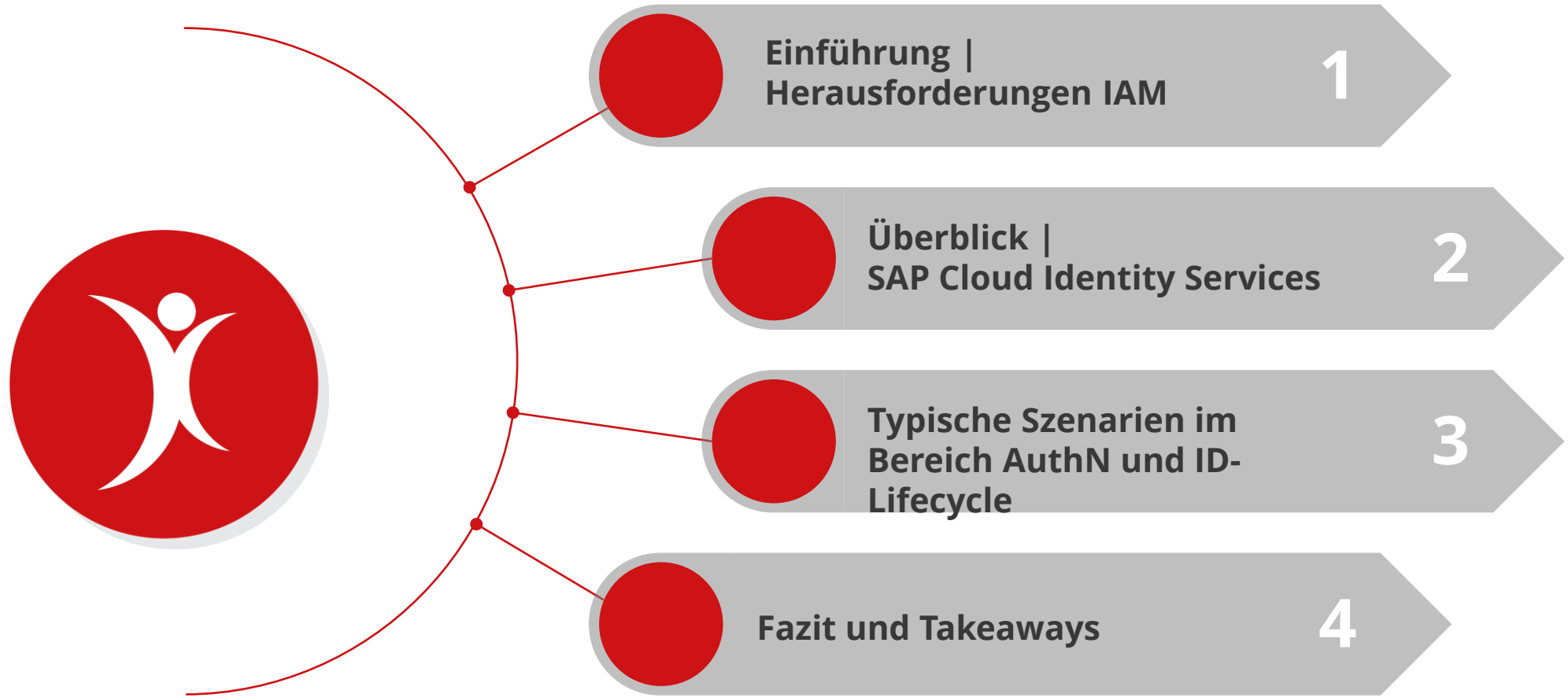
Carsten Olt | Xiting GmbH & Alexander Schaffelke | Xiting AG

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

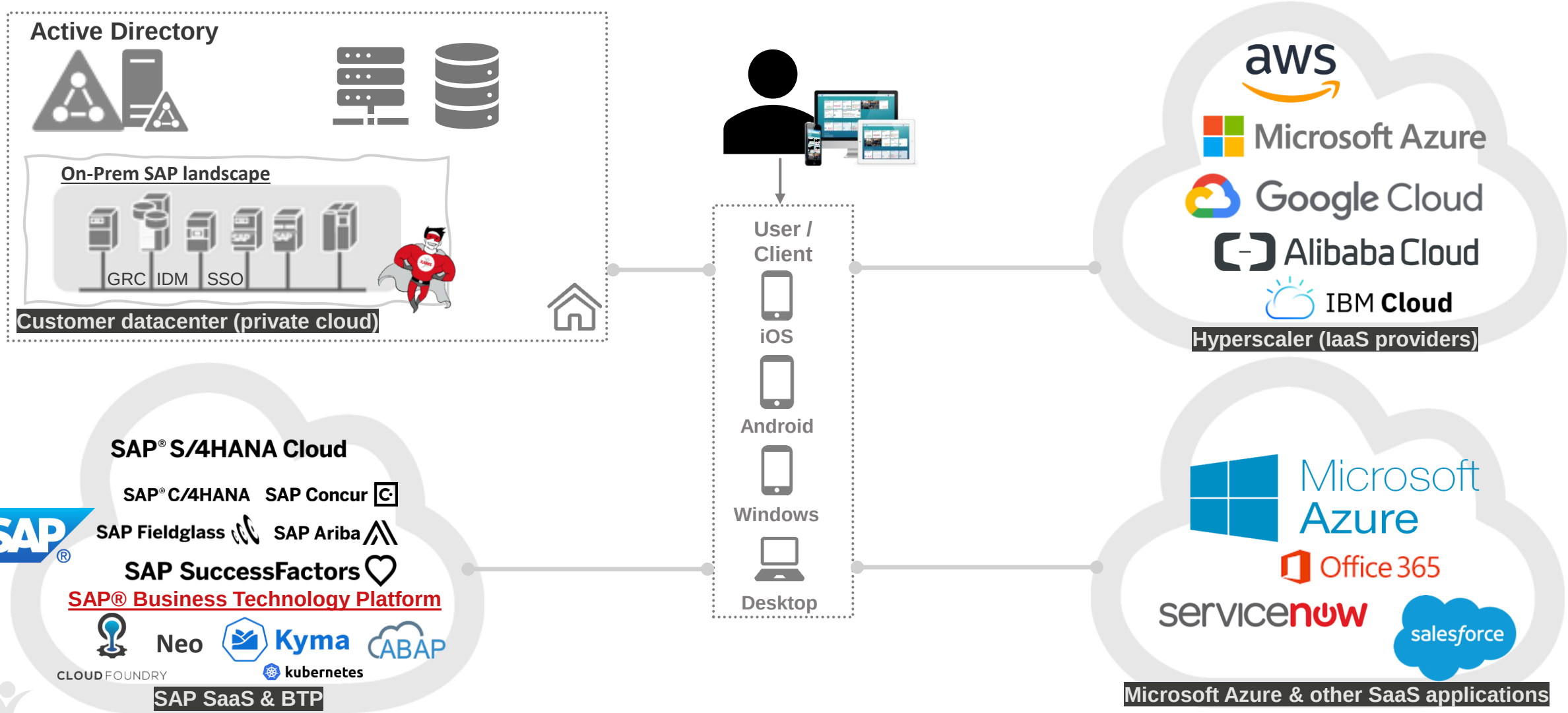
Kapitel 1

Einführung | Herausforderungen IAM

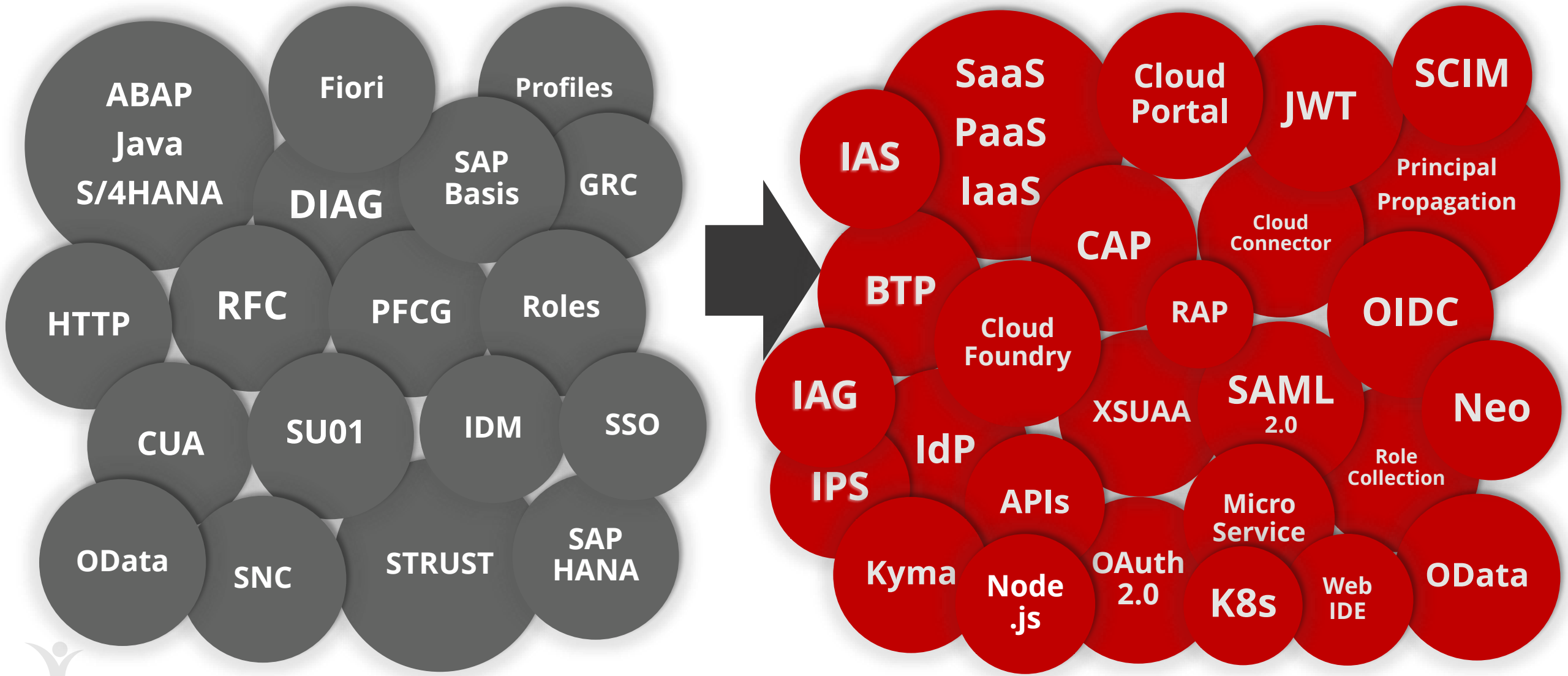
Agenda


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

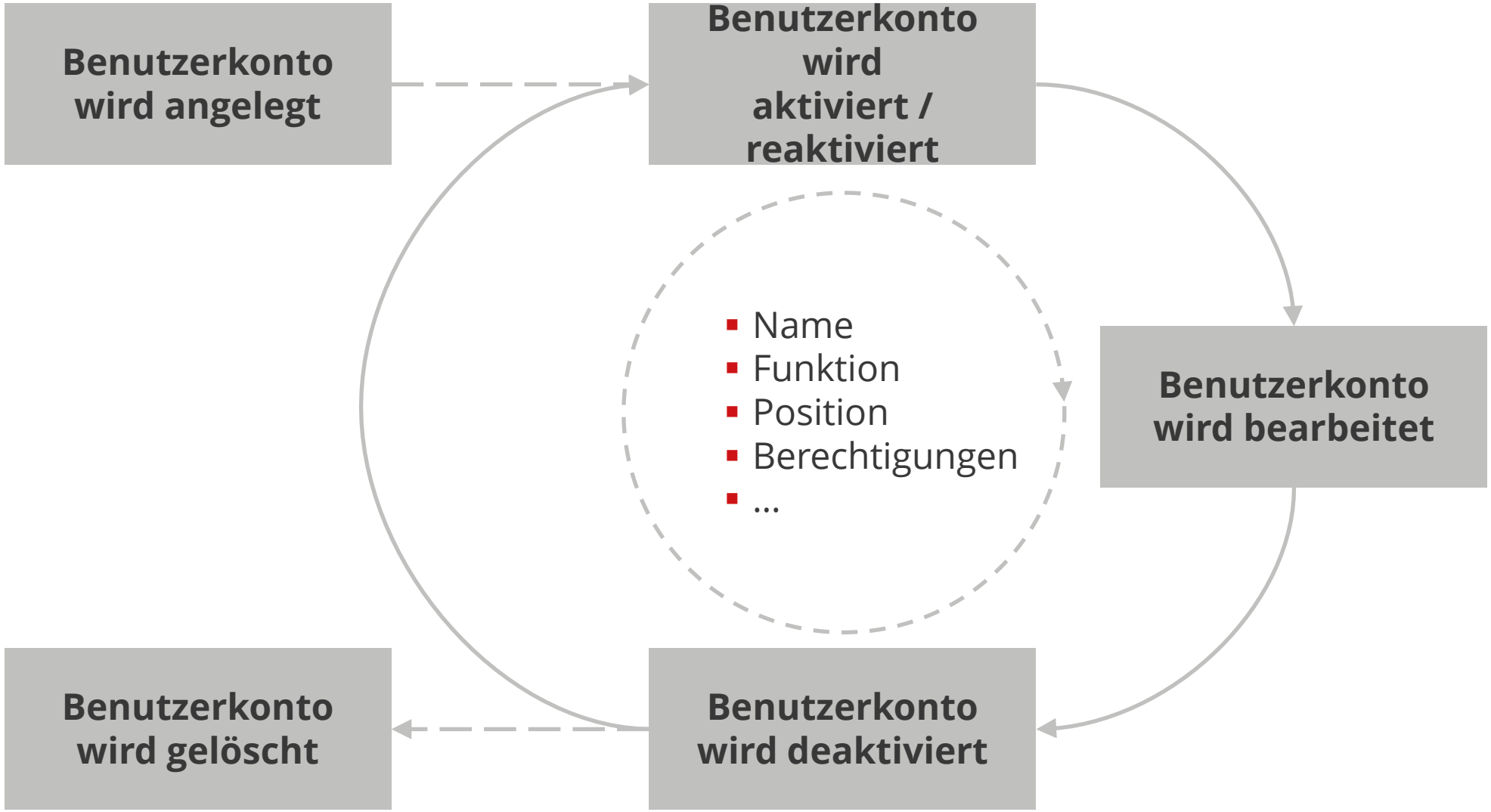
Die SAP Wolke, eine unter vielen



Neue Technologie → Neue Standards und Schnittstellen



Herausforderung: Identity Lifecycle



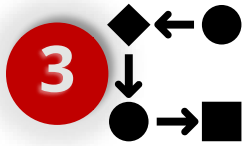
Wichtige Aspekte in der IAM-Sicherheitsstrategie

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

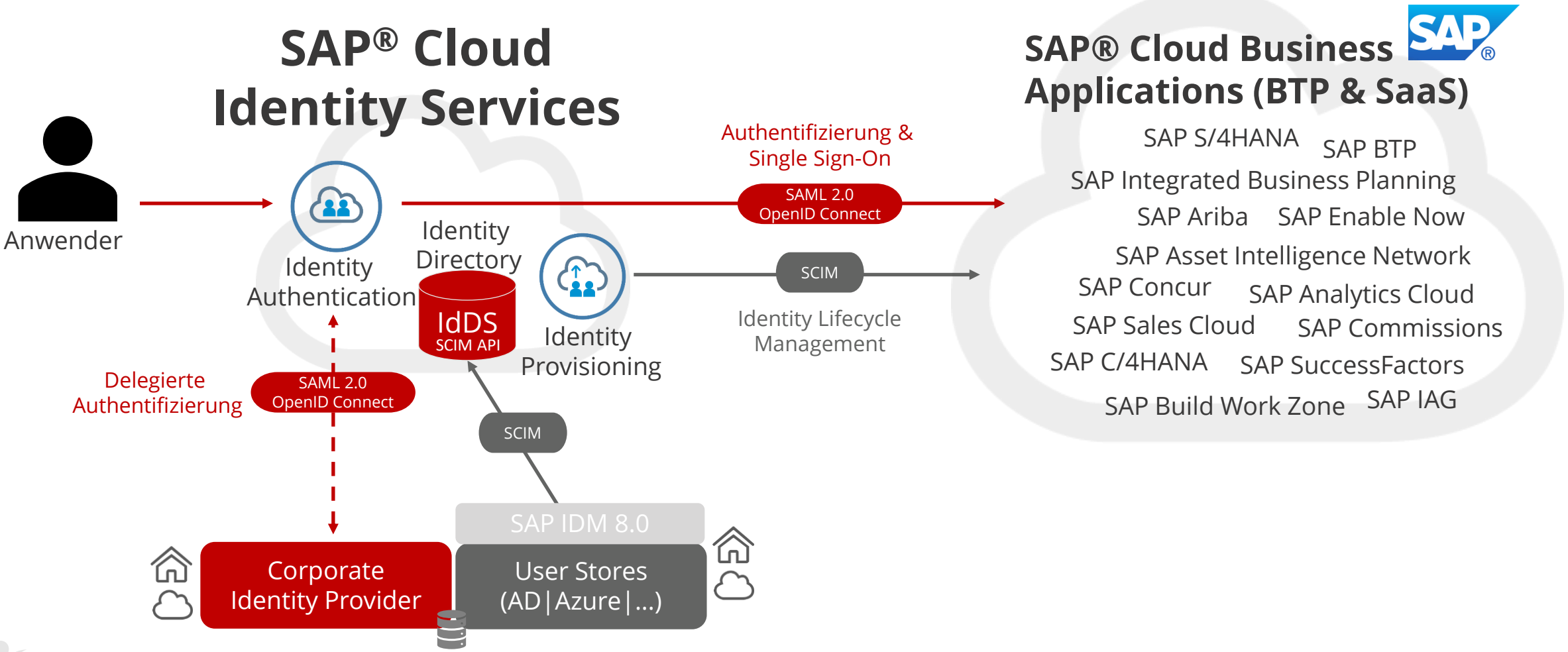
- RBAC-AuthZ
- Mapping der Rollen für Cloud- und On-Prem Anwendungen
- Zugriffskontrolle
- Governance und Compliance
- SOD-Prüfungen

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

Wird mit allen wichtigen Cloud-Lösungen von SAP geliefert - **Automatisiert oder über Self-Service**

Grundlage für die Implementierung des **Identity-Lifecycle-Managements**

Zentrale Instanz für den Zugriff auf die SAP-Cloud-Landschaft (SaaS & BTP)

Ein **Standard-Tenant** unabhängig von der Anzahl der erworbenen SAP-Lösungen

SAP® Cloud Identity Services

IAS | IPS | IdDS

Zentrale Stelle zur Verwaltung des Service Provider **Trust-Management und SSO** für SAP-Cloudanwendungen

Test-Tenant kostenlos erhältlich (Zusätzliche SCI-Tenants auf Anfrage verfügbar)

Eine **zentralisierte Benutzerbereitstellungs-Schnittstelle** für SAP-Cloud-Lösungen

Keine zusätzlichen Kosten für die Nutzung im Zusammenhang mit SAP-Hybridlandschaften

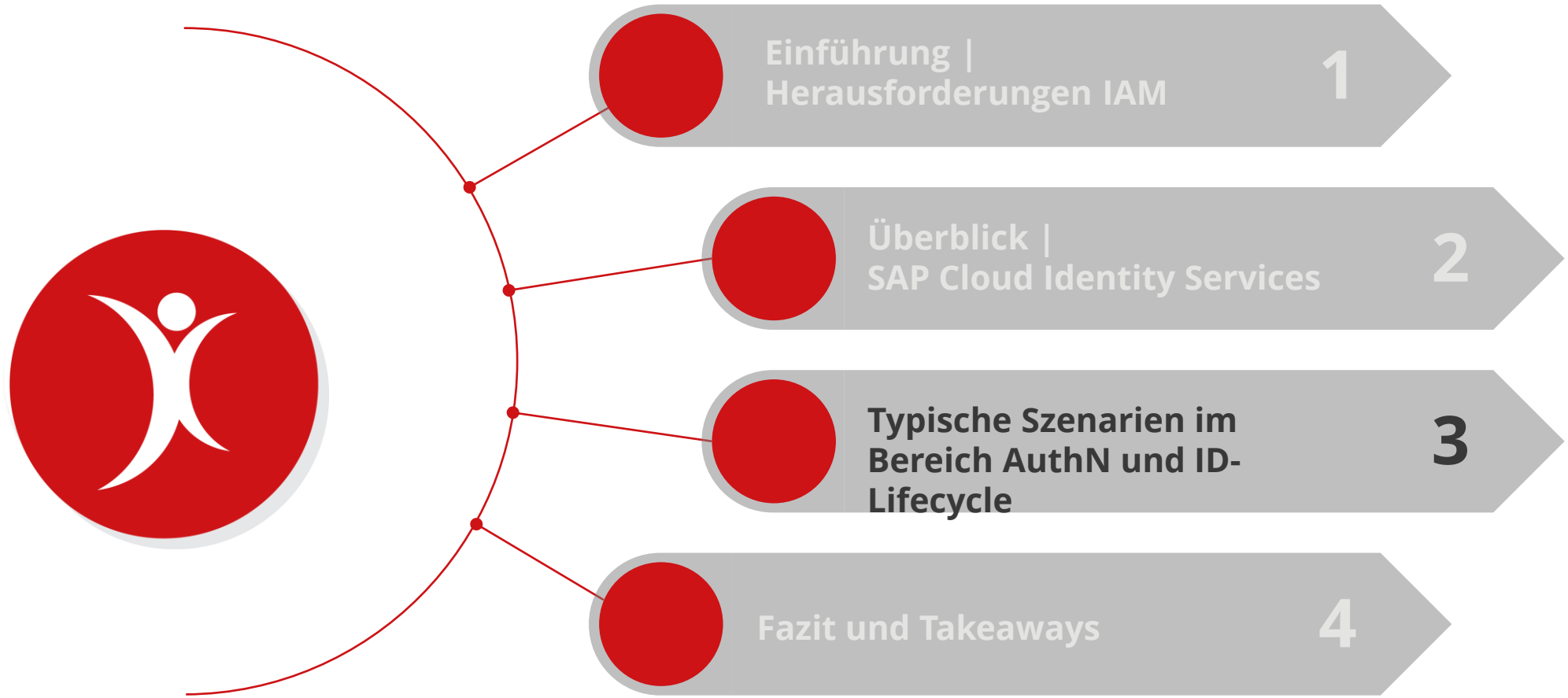
Ermöglicht **Integration** mit bestehenden **IDM-Lösungen**

Unterstützt die Standards **SAML, OAuth2, OpenID Connect & SCIM**

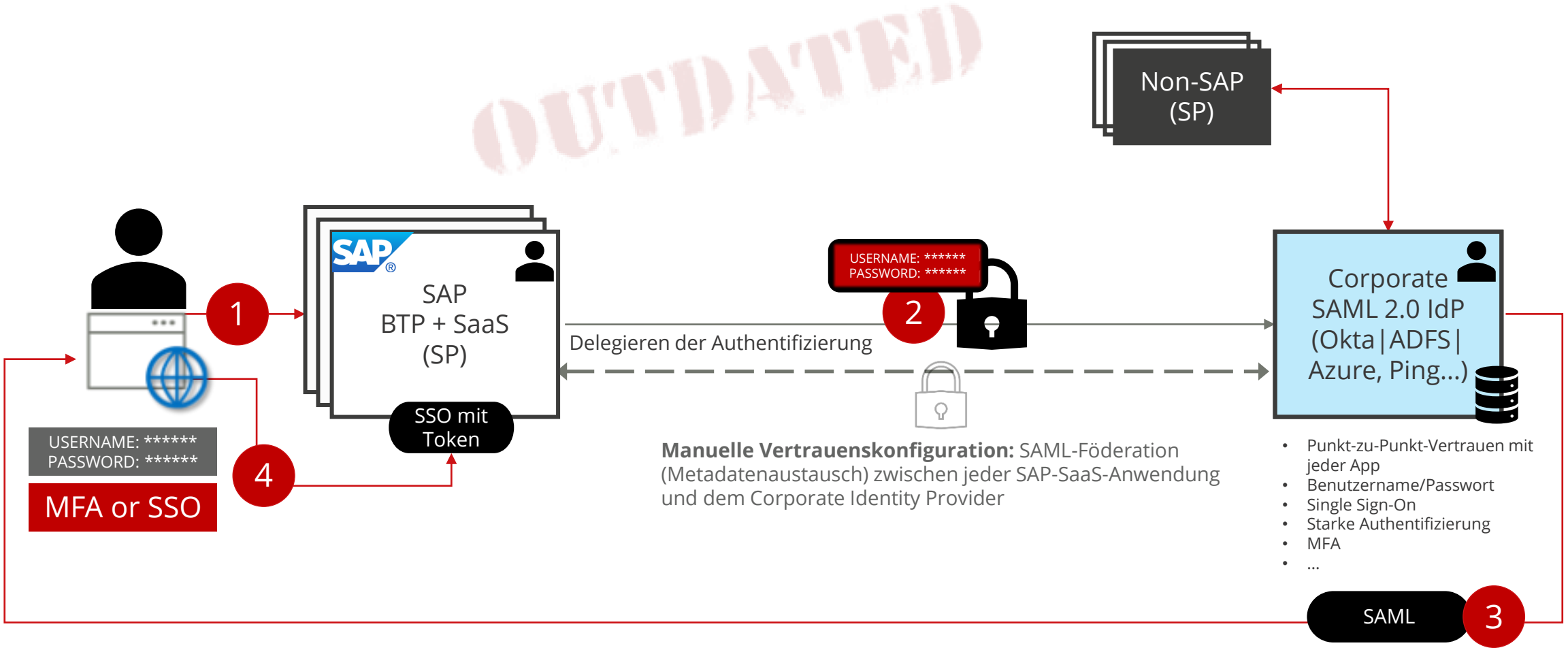
Kapitel 3

Typische Szenarien im Bereich AuthN und ID-Lifecycle

Agenda


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

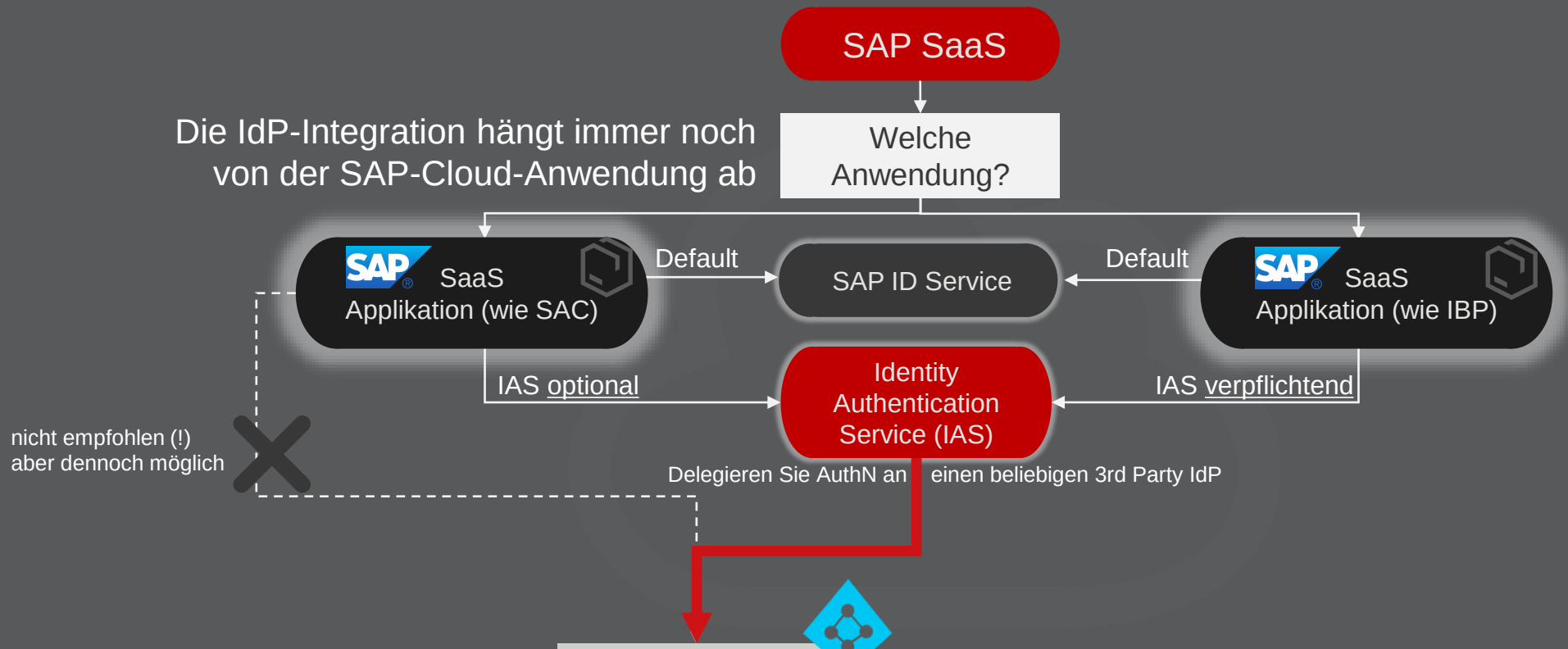
Veralteter Ansatz | SAP SaaS & BTP mit einem vorhandenen IdP



SAP Cloud Identity Services | AuthN & SSO an SaaS Anwendungen

Mai 2023 - SAP IAS verpflichtend für:

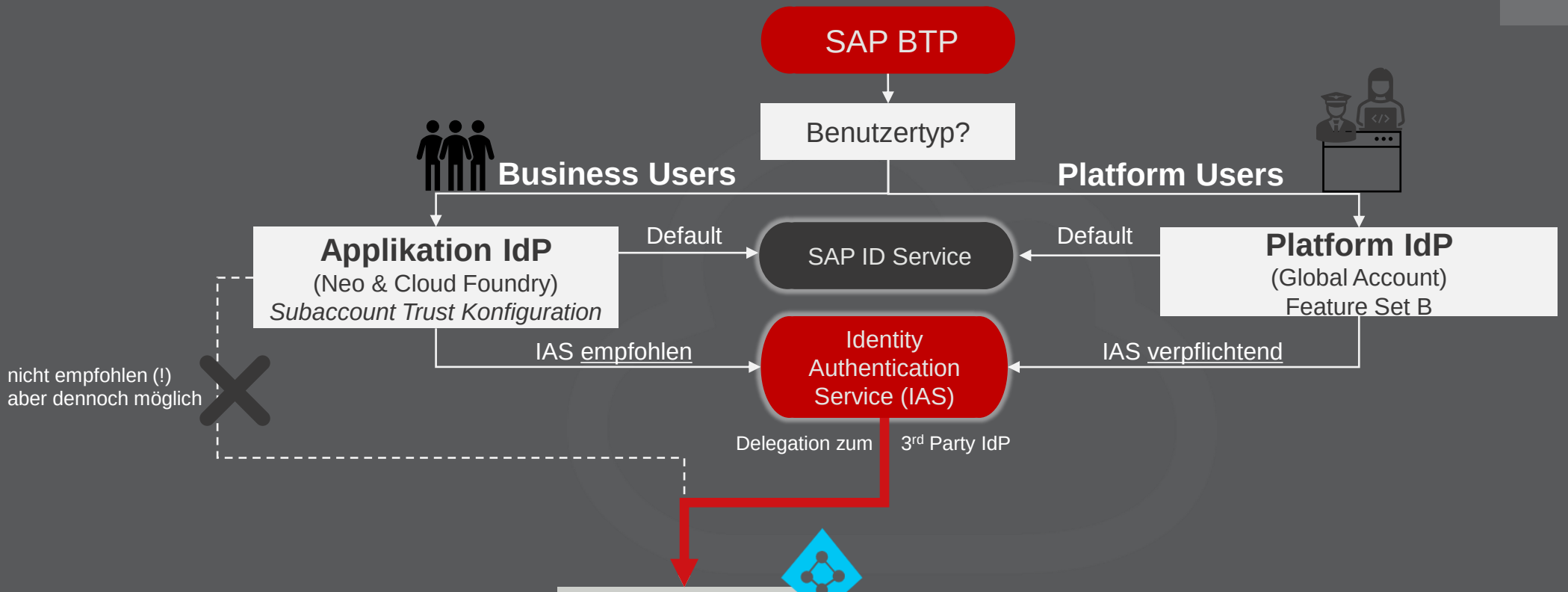
- SAP Asset Intelligence Network
- SAP Build Work Zone
- SAP Customer Engagement Center
- SAP Enable Now
- SAP Identity Access Governance
- SAP Integrated Business Planning
- SAP IoT Application Enablement
- SAP Jam
- SAP Landscape Management Cloud
- SAP S/4HANA Cloud
- SAP Rural Sourcing Management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



- Bestehende Benutzer und Gruppen und zentrale Steuerung
- Vorhandene Authentifizierungsprozesse und SSO
- Vorhandene Sicherheitsfunktionen wie MFA und Geräteprüfung
- **Single source of truth (SSOT)**

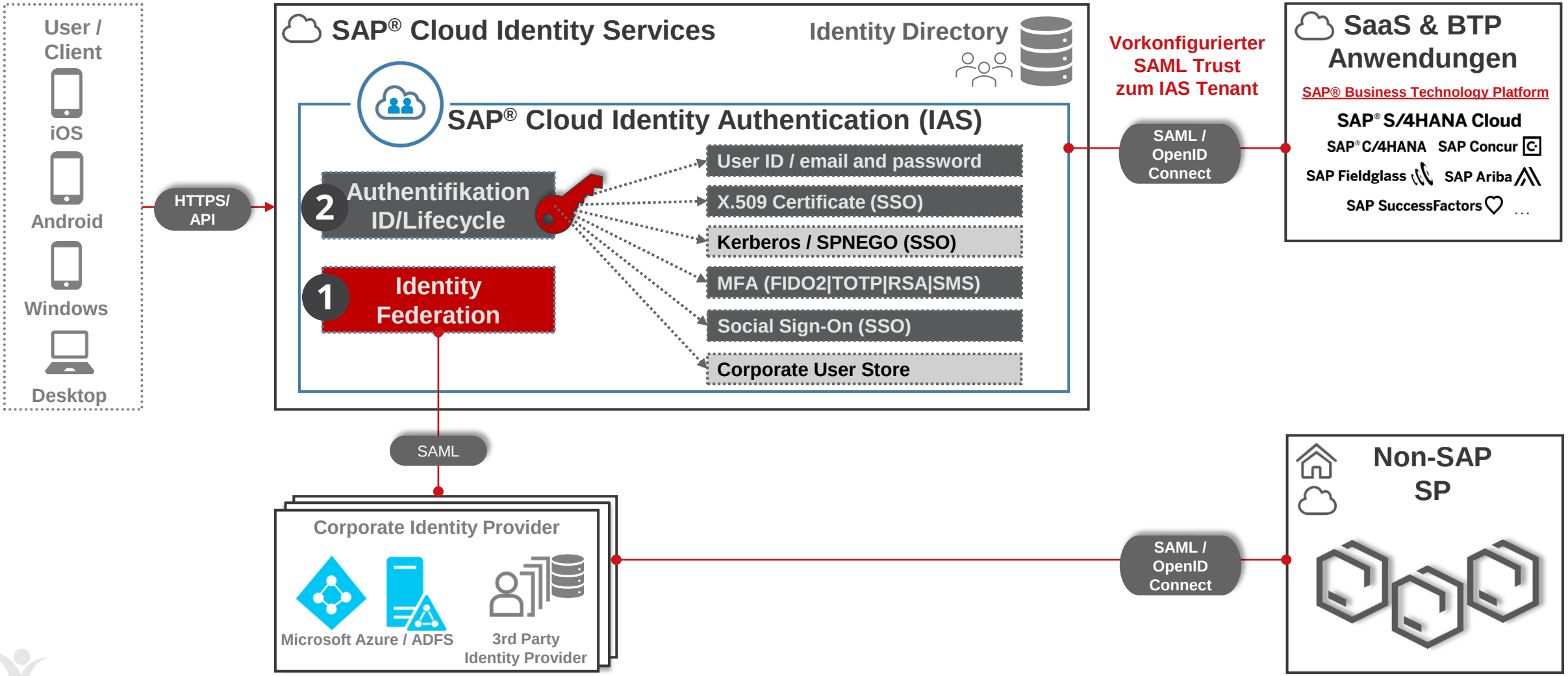
SAP Cloud Identity Services | AuthN & SSO für die BTP

Weitere Infos
- Link zum SAP Community Blog
- Link SAP Documentation

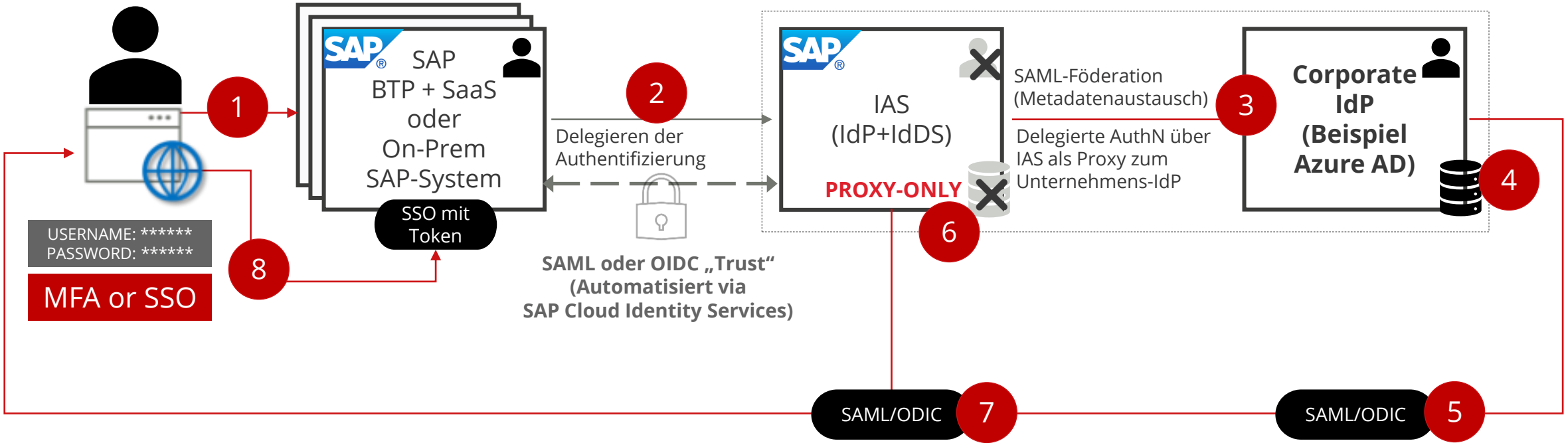


- Bestehende Benutzer und Gruppen und zentrale Steuerung
- Vorhandene Authentifizierungsprozesse und SSO
- Vorhandene Sicherheitsfunktionen wie MFA und Geräteprüfung
- **Single source of truth (SSOT)**

SAP Cloud Identity Authentication Service



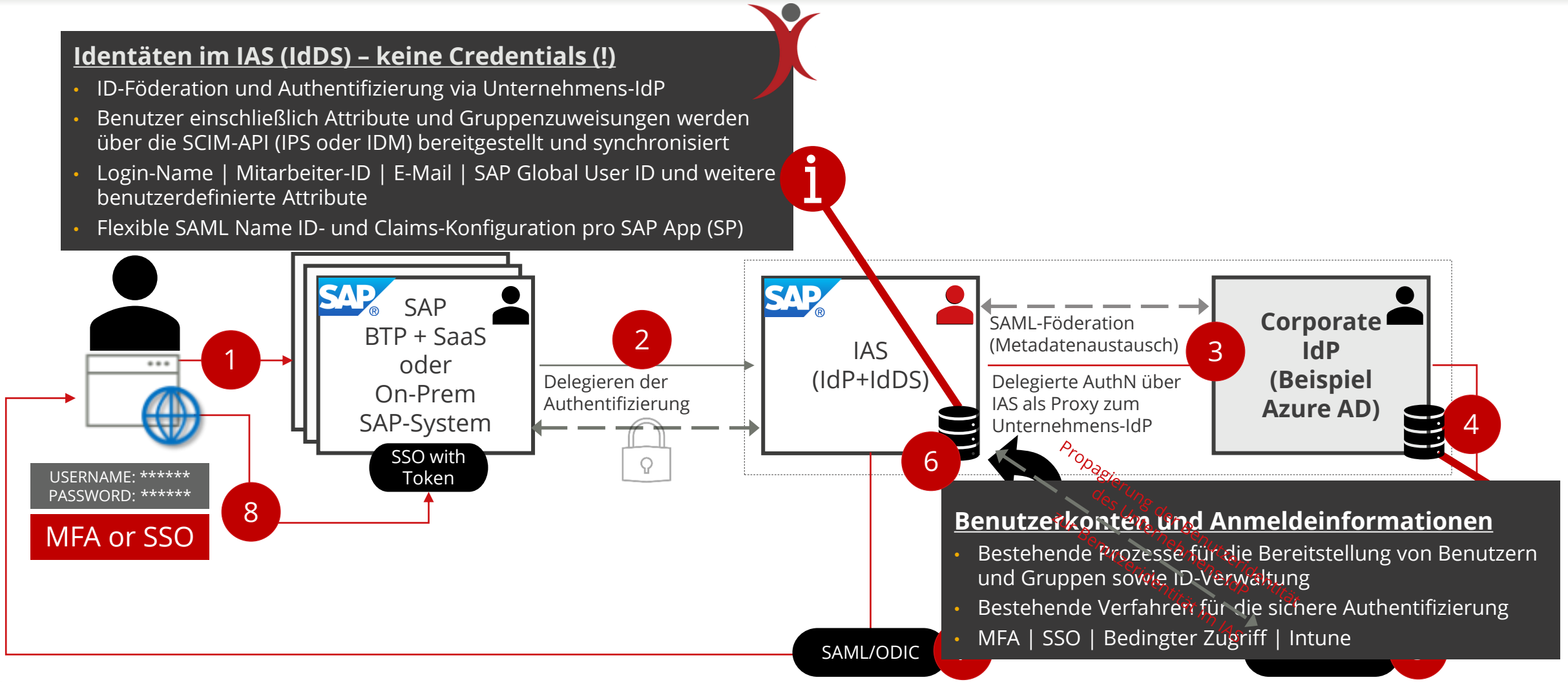
Meist der erste Schritt | SAP IAS und der Unternehmens-IdP (Proxy-Only-Szenario)



Empfohlenes Szenario | Identitätsföderation zwischen IAS & Unternehmens-IdP

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

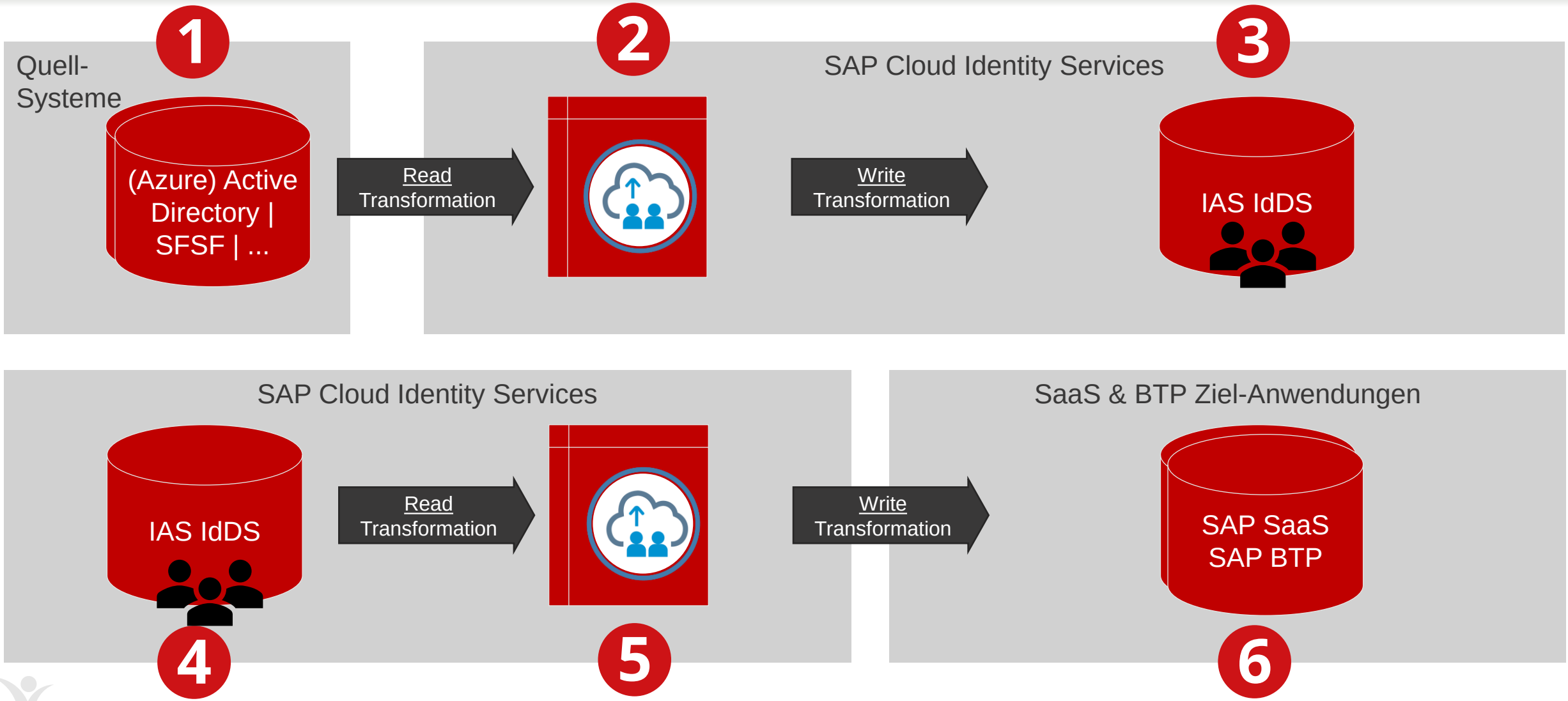
- ID-Föderation und Authentifizierung via Unternehmens-IdP
- Benutzer einschließlich Attribute und Gruppenzuweisungen werden über die SCIM-API (IPS oder IDM) bereitgestellt und synchronisiert
- Login-Name | Mitarbeiter-ID | E-Mail | SAP Global User ID und weitere benutzerdefinierte Attribute
- Flexible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



Benutzerkonten und Anmeldeinformationen

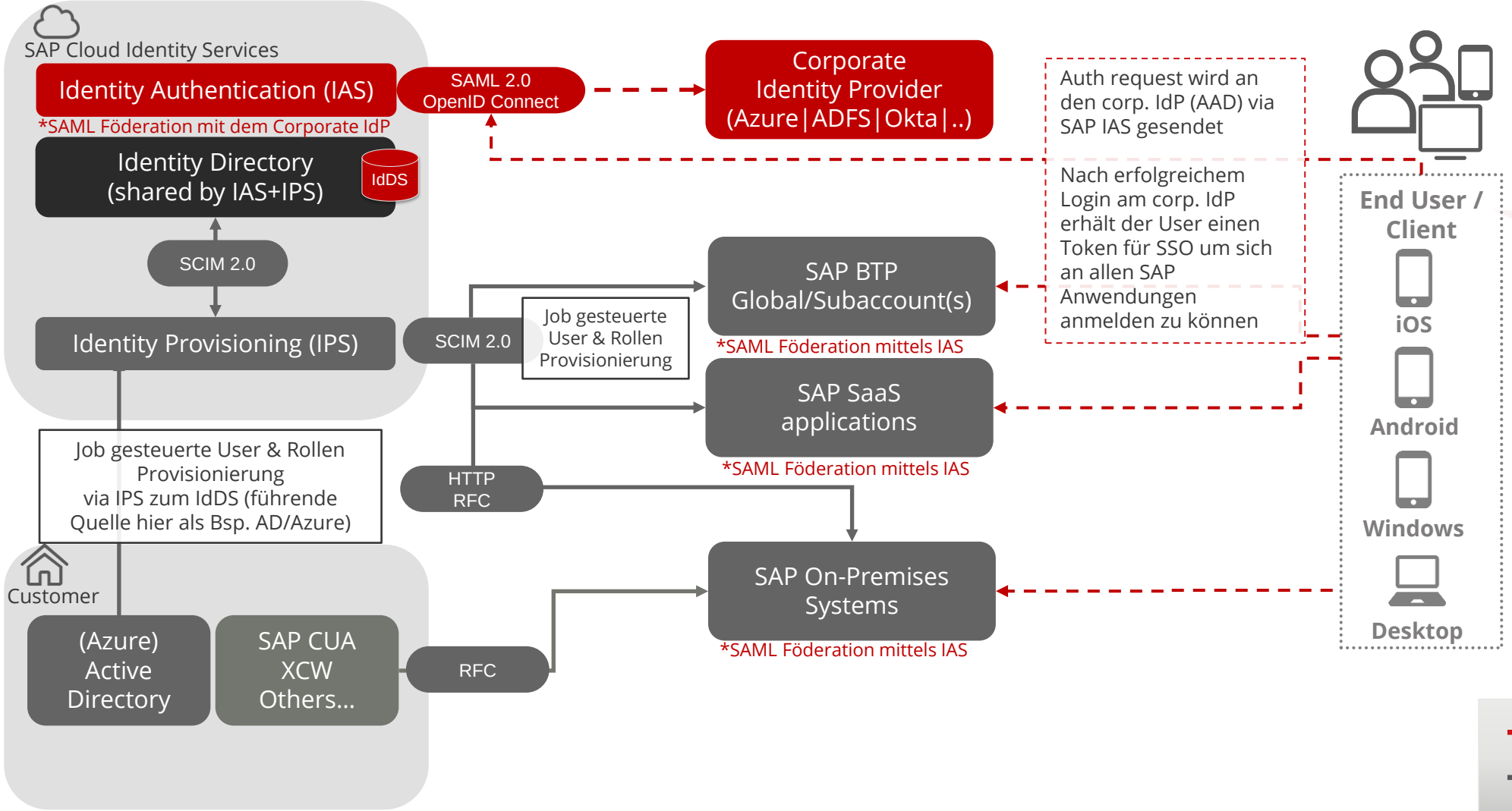
- Bestehende Prozesse für die Bereitstellung von Benutzern und Gruppen sowie ID-Verwaltung
- Bestehende Verfahren für die sichere Authentifizierung
- MFA | SSO | Bedingter Zugriff | Intune

Identitätslebenszyklusmanagement mit SAP IPS | Beispiel-Szenario



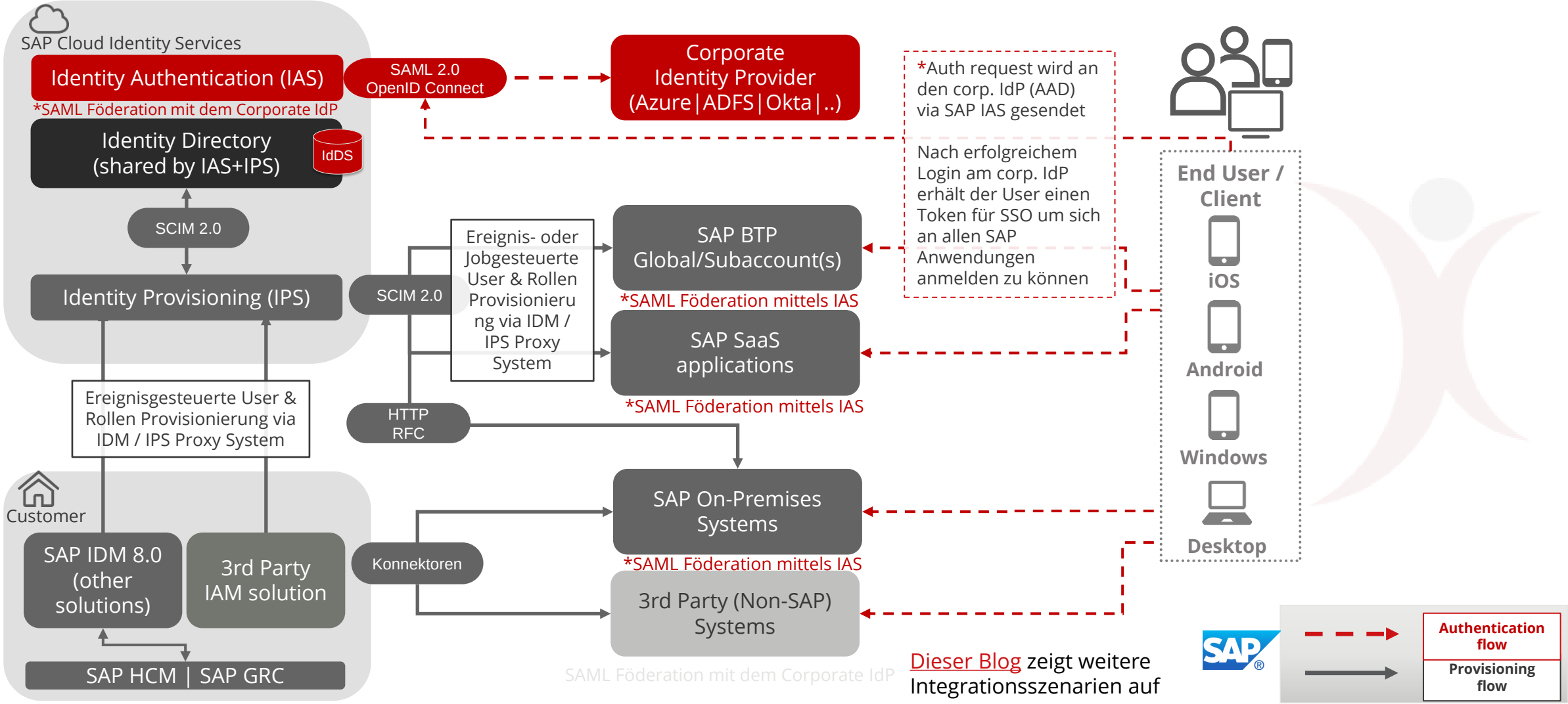
Identity & Access Management und Single Sign-On

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 (Metadatenaustausch)
- 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)

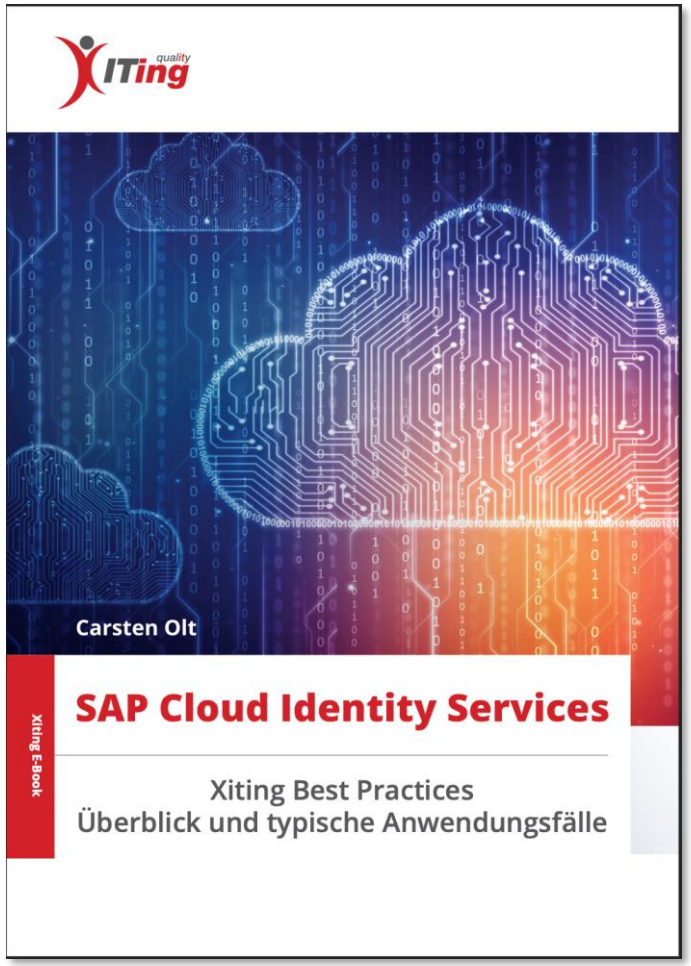
EXKLUSIVES E-BOOK:

SAP CLOUD IDENTITY SERIVCES

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).

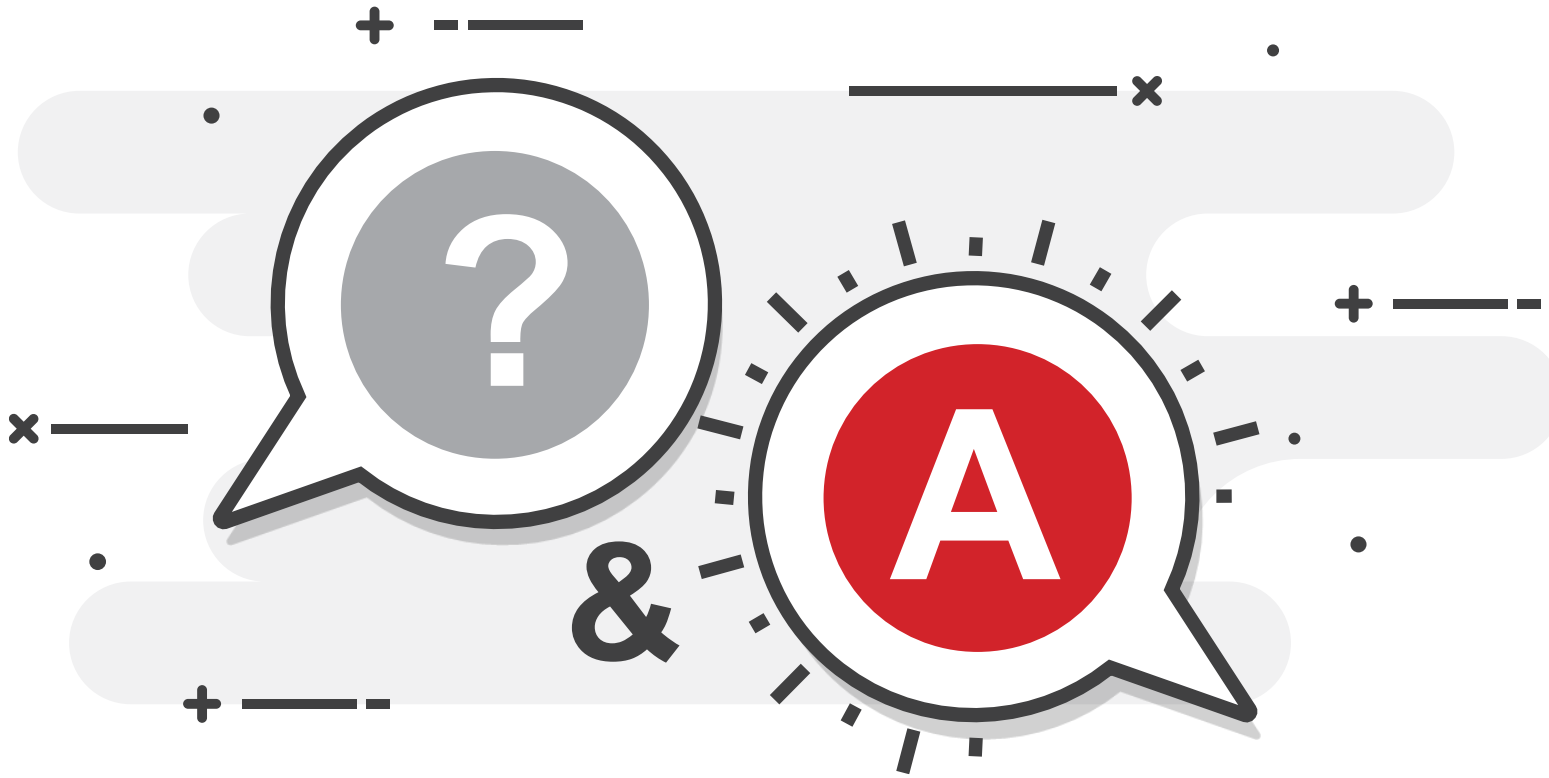
Zielgruppe

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

Weitere Informationen

*Umfang individuell erweiterbar

FRAGEN UND DISKUSSIONEN



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