SAP SECURITY GROUP

VIENNA EDITION

WHERE SECURITY
SHAPES THE FUTURE

SAP integrieren statt isolieren

IAM als Rückgrat der Unternehmens-IT

Fabian Honervogt
Manager Identity & Access Management · Xiting GmbH

accenture | XITing quality

5. November 2026
Alte Börse | Schottenring 16 | 1010 Wien | Österreich

EINSTIEG

Über das Warum sind wir uns einig. Heute geht es um das Wie.

Dass IAM unternehmensweite Orchestrierung ist, bestreitet niemand mehr. Die offene Frage ist die Umsetzung für das komplexeste Zielsystem im Haus.

Die Leitfrage

Wie bindet man ausgerechnet SAP ein, ohne ein neues Silo zu bauen und ohne die SAP-Kompetenz zu verlieren?

© 2026 Xiting GmbH

KERNBOTSCHAFT

SAP ist ein Zielsystem wie jedes andere, nur mit mehr Regeln. Und die Regeln gehören ins IAM.

AGENDA

In vier Schritten zum Wie

01

Was SAP anders macht

02

Zielbild: IAM als Rückgrat

03

Vier Integrationspunkte

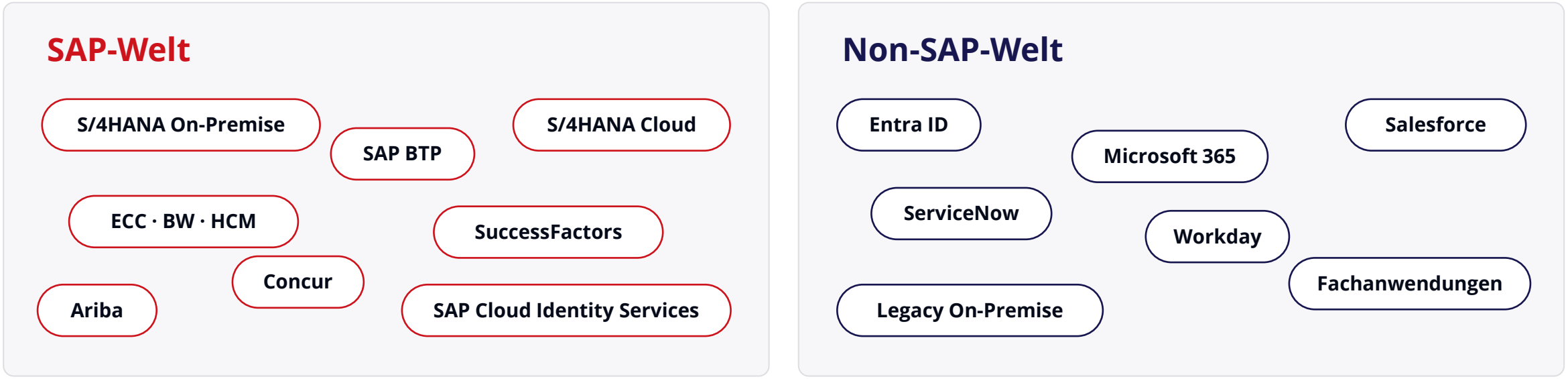
04

Praxis und Empfehlungen



© 2026 Xiting GmbH

SAP selbst ist längst hybrid



Die Grenze verläuft nicht mehr zwischen SAP und dem Rest. Sie verläuft quer durch die SAP-Landschaft.

© 2026 Xiting GmbH

Vier Gründe, warum die Integration schwer ist

Rollenmodell

Rollen, Profile, Objekte, Feldwerte. Eine SAP-Rolle ist kein Attribut, sondern ein Berechtigungsbündel mit eigener Logik.

Risikologik

Konflikte in der Funktionstrennung (SoD) entstehen über Rollen- und Systemgrenzen hinweg und sind von außen nicht sichtbar.

Systemvielfalt

ECC, S/4HANA, BW, HCM, BTP, Mandanten. Jedes System bringt eine eigene Benutzerverwaltung mit.

Lizenzrelevanz

Berechtigungen bestimmen den Lizenztyp und damit Kosten. Kein anderes Zielsystem hat diese Kopplung.

© 2026 Xiting GmbH

Der Zeitdruck ist real

2027

Ende der Mainstream-Wartung SAP Identity Management

2030

Ende der erweiterten Wartung

Wer SAP IDM ablöst, trifft eine Architekturentscheidung, ob er will oder nicht. Besser, man trifft sie bewusst.

© 2026 Xiting GmbH

ZIELBILD

IAM besteht aus vier Funktionen, getrennt gedacht

Wer ist da?

Identity Lifecycle

Eintritt, Wechsel, Austritt. Das HR-System ist die einzige Quelle der Wahrheit.

Wer bist du?

Authentifizierung

Single Sign-On und MFA über alle Systeme: Entra ID, SAP Cloud Identity Services.

Was bekommst du?

Provisionierung

Konten und Rollen in den Zielsystemen anlegen, ändern, entziehen. Automatisiert.

Darfst du das?

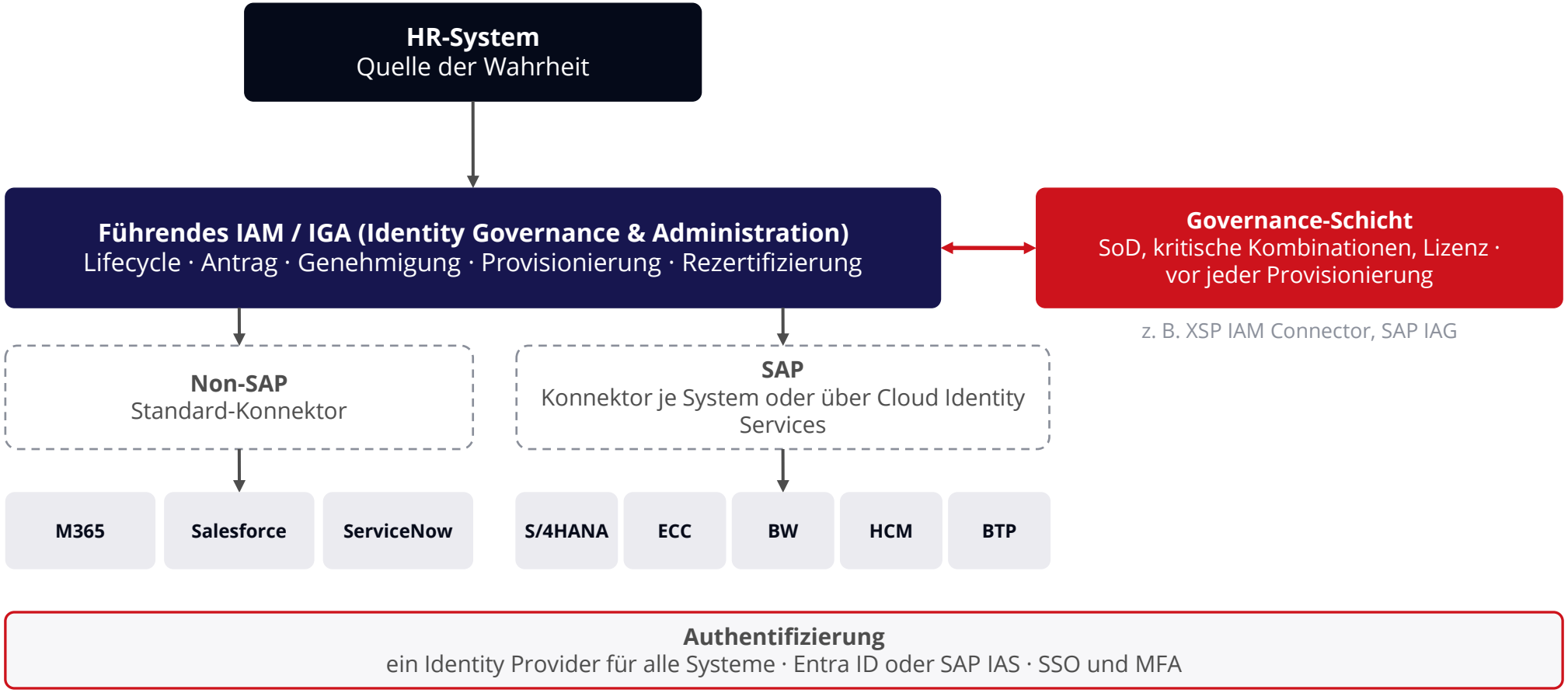
Access Governance

Antrag, Genehmigung, Risikoprüfung, Rezertifizierung. Hier entscheidet sich Compliance.

© 2026 Xiting GmbH

ZIELBILD

Das Rückgrat, und wo SAP darin sitzt



Gezeigt ist der Fall mit Enterprise-IGA. Führt eine SAP-zentrierte IGA, steht sie selbst in der Mitte und bringt die Governance-Schicht mit.

© 2026 Xiting GmbH

VIER INTEGRATIONSPUNKTE

An vier Stellen dockt SAP ans IAM an

01 · Wer ist da?

Identity Lifecycle

Leitfrage: Kommen Eintritt, Wechsel und Austritt automatisch in jedem SAP-System an?

Stolperfalle: Die Lifecycle-Logik steckt heute oft im SAP IDM.

02 · Wer bist du?

Authentifizierung

Leitfrage: Wer ist der Identity Provider für SAP, und gilt er für Fiori, GUI und BTP?

Stolperfalle: Zwei Identity Provider, zwei Passwörter, zwei MFA-Regeln.

03 · Was bekommst du?

Provisionierung

Leitfrage: Auf welchem Weg legt das IGA Konten und Rollen in SAP an?

Stolperfalle: Für den Konnektor ist eine SAP-Rolle nur ein Name.

04 · Darfst du das?

Access Governance

Leitfrage: Wer prüft SoD und Lizenz, bevor vergeben wird?

Stolperfalle: Geprüft wird nachträglich, in einem System, das die Zuweisungen nicht führt.

© 2026 Xiting GmbH

Lifecycle: SAP ist Quelle und Ziel zugleich

Eintritt, Wechsel und Austritt kommen aus einem System. Bei SAP ist das HR-System oft selbst SAP, und die Konten liegen in einem Dutzend weiterer SAP-Systeme.



Wo SAP andockt

SAP liefert die Identität und empfängt sie zurück. HCM oder SuccessFactors speisen das führende IGA, das IGA steuert den Lifecycle in S/4HANA, ECC, BW und BTP, je Mandant.

Was zu klären ist

Ein Datenmodell, klare Regeln für Wechsel und Austritt. Was passiert mit alten Rollen beim Abteilungswechsel? Wird beim Austritt in jedem Mandanten gesperrt und entzogen?

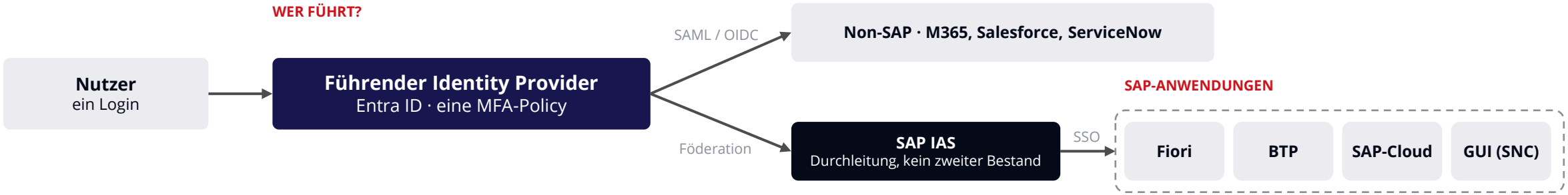
Stolperfalle

Die Lifecycle-Logik steckt im SAP IDM. In Eigenentwicklungen, die niemand mehr ganz kennt. Wer sie nicht erfasst, baut sie blind nach oder verliert sie.

© 2026 Xiting GmbH

Authentifizierung: ein Identity Provider, auch für SAP

SSO und MFA laufen meist über Entra ID. SAP bringt mit den Cloud Identity Services einen eigenen Identity Provider mit. Die Frage ist, wer führt.



Wo SAP andockt

Fiori, BTP und die SAP-Cloud sprechen Standards. SAML oder OpenID Connect, wie jede andere Anwendung. Sonderfall SAP GUI: braucht eine eigene SSO-Anbindung.

Was zu klären ist

Ein führender Identity Provider, SAP IAS nur als Durchleitung. Eine MFA-Policy für alles. Ein vom IGA gesperrtes Konto verliert sofort jeden Zugang, auch in SAP.

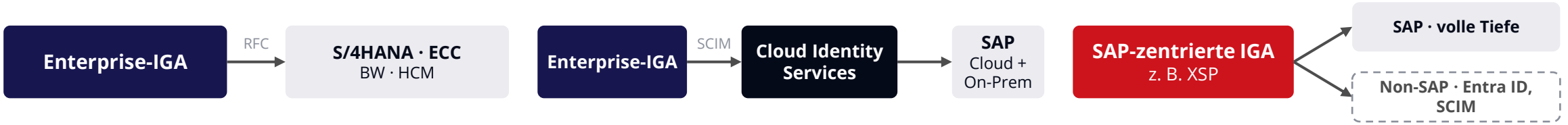
Stolperfalle

Zwei Identity Provider, zwei Benutzerbestände. Der Austritt sperrt Entra ID, das SAP-Passwort funktioniert noch wochenlang.

© 2026 Xiting GmbH

Provisionierung: drei Wege nach SAP, eine Wahrheit

Drei Wege nach SAP, alle funktionieren. Zwei starten beim Enterprise-IGA, einer bei einer SAP-zentrierten IGA. Am Ende führt ein System alle Zuweisungen, SAP und Non-SAP.



Konnektor je System

Direkt, tief, pro System zu pflegen. Das Enterprise-IGA spricht per Standardschnittstelle (RFC, BAPI) mit S/4HANA, ECC, BW und HCM. Der Standardweg der großen Hersteller.

Ein zentraler Endpunkt

Ein Mapping für alle SAP-Ziele. Das Enterprise-IGA spricht SCIM mit den SAP Cloud Identity Services (IAS/IPS), die verteilen weiter. Sinnvoll bei vielen SAP-Cloud-Produkten.

SAP-zentrierte IGA führt

Volle SAP-Tiefe, Non-SAP wird mitbedient. Eine SAP-nahe IGA wie die Xiting Security Platform provisioniert selbst in SAP und über Entra ID oder SCIM in den Rest. Passt, wenn SAP im Zentrum steht.

© 2026 Xiting GmbH

Governance: prüfen, bevor provisioniert wird

01

Antrag im IGA

Fachbereich beantragt in Business-Sprache, Manager genehmigt.

02

Risikoprüfung

Prüfung vor der Vergabe: SoD, kritische Kombinationen, Lizenzwirkung, systemübergreifend.

03

Entscheidung

Ergebnis geht zurück. Risk Owner entscheidet im IGA, Mitigation bleibt in der Governance-Schicht, der Status geht mit.

04

Provisionierung

Das führende IGA provisioniert selbst, direkt oder über die Cloud Identity Services.

05

Eine Wahrheit

Zuweisungen liegen auf Account-Ebene im IGA. Rezertifizierung und Entzug ohne Umweg.

In der Praxis

Für den Konnektor ist eine SAP-Rolle nur ein Name. Schritt 02 braucht deshalb eine Schicht, die SAP-Rollen inhaltlich versteht, etwa SAP IAG oder bei unseren Kunden die XSP mit dem IAM Connector, als Schicht vor dem Enterprise-IGA oder eingebaut in die SAP-zentrierte IGA. Provisioniert wird weiterhin vom führenden IGA.

© 2026 Xiting GmbH

Wer führt die Zuweisungen? Drei Konstellationen

Kriterium	A · Enterprise-IGA führt	B · SAP-zentrierte IGA führt	C · Zwei Systeme führen
Wer führt die Zuweisungen?	Enterprise-IGA, Governance davor	SAP-zentrierte IGA, z. B. XSP	beide, jedes für sich
Wer provisioniert in SAP?	direkt oder über Cloud Identity Services	die SAP-zentrierte IGA	SAP-Schicht, IGA per Abgleich
Sicht auf Account-Ebene	vollständig, im IGA	vollständig, in der SAP-IGA	lückenhaft, zwei Systeme
Rezertifizierung und Entzug	aus einer Hand	aus einer Hand	zweigeteilt
SoD- und Lizenzprüfung	Governance-Schicht davor, nötig	enthalten	enthalten, nur für SAP
Silo-Risiko	gering	gering, Non-SAP flacher	hoch
Passt, wenn	Enterprise-IGA da oder geplant	SAP im Zentrum, kein IGA geplant	nie als Ziel, nur Übergang

Transportweg und Werkzeug sind zweitrangig. Das Silo entsteht erst, wenn zwei Systeme Zuweisungen führen und keines das ganze Bild hat.

© 2026 Xiting GmbH

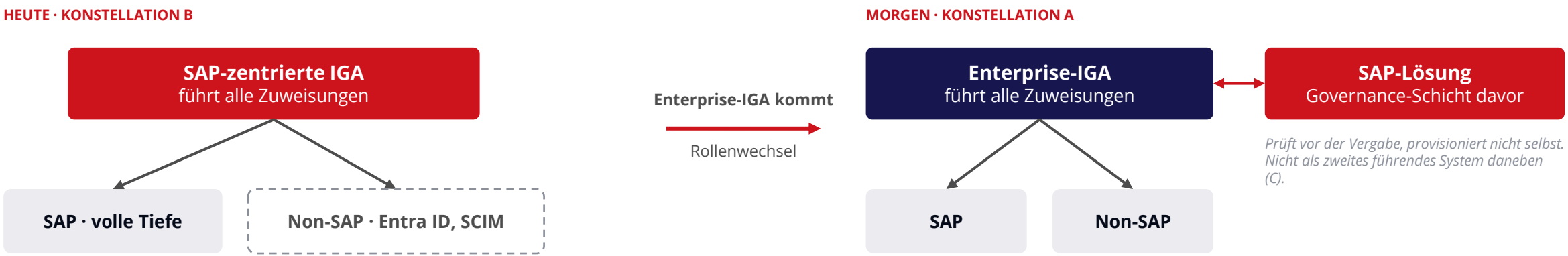
Und wenn es kein Enterprise-IGA gibt?

Die SAP-zentrierte IGA führt

Für SAP-lastige Landschaften das Zielbild, kein Provisorium. Eine SAP-nahe IGA führt Lifecycle, Antrag und Provisionierung für SAP und bedient Non-SAP über Entra ID oder SCIM mit. Eine Wahrheit, schnell umsetzbar.

Die ehrliche Grenze

Bei Non-SAP bleibt die Tiefe hinter einem Enterprise-IGA zurück. Kommt später eines, wechselt die SAP-Lösung die Rolle: Governance-Schicht davor (A), nicht zweites führendes System (C).



© 2026 Xiting GmbH

[Kunde A] · Industriekonzern mit SailPoint-Landschaft

Ausgangslage

- SailPoint als unternehmensweites IGA etabliert
- SAP-Zuweisungen bisher manuell: Freigabe in ServiceNow, Ticket, Berechtigung von Hand gesetzt
- SAP-Risikoanalyse fehlt im Antragsprozess
- SAP-Berechtigungswerkzeuge und Risikoregelwerke vorhanden, aber nicht angebunden

Entscheidung

- SailPoint bleibt führend und provisioniert selbst
- Governance-Schicht prüft vor der Provisionierung Risiken, systemübergreifend und mit bestehenden Regelwerken
- Konstellation C, ein zweites führendes System neben SailPoint, bewusst verworfen

Lessons Learned

- Entscheidung ins IGA, Mitigation in die Governance-Schicht, der Status zurück. Sonst Schatten-Workflow oder doppelte Pflege
- IGA-Implementierungspartner früh einbinden, Schnittstellen gemeinsam definieren

© 2026 Xiting GmbH

[Kunde B] · Energieversorger mit SAP IDM im Lifecycle

Ausgangslage

- SAP IDM steuert seit Jahren Eintritt, Wechsel und Austritt, für SAP und Microsoft
- Viele Eigenentwicklungen, kaum Dokumentation der Prozesse, Schnittstellen und Datenflüsse
- Wartungsende zwingt zur Nachfolgeentscheidung

Entscheidung

- Zuerst Ist-Analyse: Welche Identitätsflüsse laufen heute über das IDM, mit welcher Komplexität?
- Dann festlegen, wo der Lifecycle künftig lebt: in einem System, das SAP und Non-SAP gemeinsam führt (A oder B, nie C)
- Erst danach Zielarchitektur und Ausschreibung

Lessons Learned

- Das IDM-Ende ist eine Integrationsentscheidung, kein Produkttausch
- Wer die Flüsse nicht kennt, baut das Silo im neuen Werkzeug nach
- Was man nicht kennt, kann man nicht ausschreiben und nicht integrieren

© 2026 Xiting GmbH

Fünf Schritte für die nächsten zwölf Monate

1 **Identitätsflüsse rund um SAP erfassen**

Wer legt heute wo Benutzer an, wer vergibt Rollen, wer entzieht sie? Erst das Bild, dann die Architektur.

2 **HR als einzige Quelle der Wahrheit festlegen**

Eintritt, Wechsel, Austritt kommen aus einem System, für SAP und Non-SAP gleichermaßen.

3 **Integrationspunkte bewusst entscheiden**

Je Funktion festlegen, wer führt: Lifecycle, Authentifizierung, Provisionierung, Governance. Nicht dem Konnektor überlassen.

4 **IGA-Team und SAP-Security an einen Tisch**

Governance organisatorisch verankern, mit klaren Zuständigkeiten für beide Schichten.

5 **IDM-Ende als Programm aufsetzen**

Architektur zuerst, Werkzeug danach. Der Termin ist der Hebel für Budget und Aufmerksamkeit.

© 2026 Xiting GmbH

Integrieren heißt: eine Wahrheit über alle Zuweisungen, SAP eingeschlossen. Welches Werkzeug sie führt, ist zweitrangig.

Fragen?

Fabian Honervogt
Manager Identity & Access Management · Xiting GmbH



Fabian Honervogt
Manager | IAM
Product Owner | XCW
Product Manager | XSP

E-Mail: fhonervogt@xiting.com

Vielen Dank für Ihre Aufmerksamkeit!

Wenn Sie weitere Informationen benötigen, können Sie mich gerne kontaktieren.

Hier vernetzen

Xiting GmbH
Obere Ringstraße 17 | DE-79859 Schluchsee
info@xiting.com | www.xiting.com