IAM Circle #5

Der Mehrwert eines hybriden IAM durch Nutzung von Microsoft Entra ID

Silvano Fari | 13.06.24 | öffentlich

Agenda

14:30 – 14:35	5'	Einleitung / Begrüssung	Sarah
14:35 – 14:50	15'	Einleitung ins Thema	Silvano
14:50 – 15:00	10'	Workshopeinlage 1	Michael, Martin, Marc, Silvano
15:00 – 15:20	20'	Architektur eines hybriden IAM	Michael
15:20 – 15:40	20'	Stärken und Schwächen von Entra ID	Martin
	20'	Pause	
16:00 – 16:15	15'	ID Lifecycle Management im hybriden IAM	Marc
16:15 – 16:30	15'	Authentisierung im hybriden IAM	Silvano
16:30 – 17:00	30'	Workshopeinlage 2	Michael, Martin, Marc, Silvano
Ab 17:00		Apéro	

Abraxas ein Schweizer Unternehmen

In der ganzen Schweiz vor Ort.

Dienstleistungsertrag 2023
In Mio. CHF

206.7

Mitarbeitende
Per 31.12.2023

1'007

Unsere Aktionäre

7 Kantone

134 Gemeinden

ISO-Zertifizierungen

ISO **9001**
Quality Management

ISO **14001**
Bereich Umwelt-management

ISO **27001**
Security Management

ISO **20000**
IT Service Management

Cloud-Zertifizierungen

60+

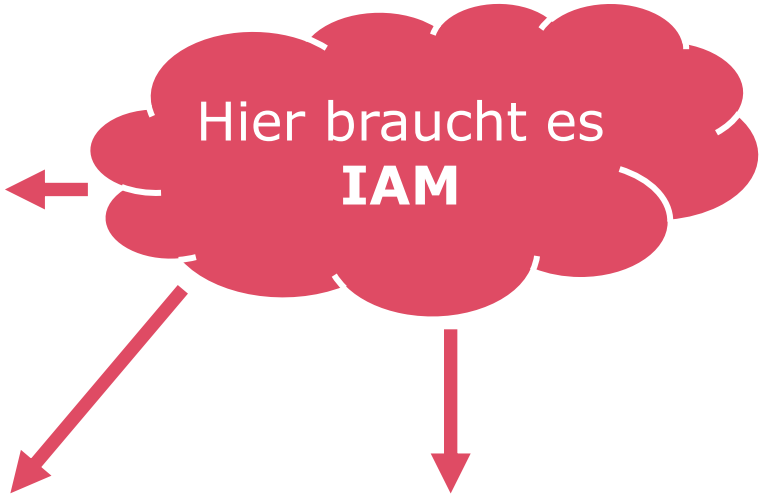
Unsere Kunden im Fokus

- Bund
- Kantone
- Gemeinden
- Bildung
- Polizei & Justiz
- Versicherungen
- Unternehmen

Unsere IT-Lösungen und Dienstleistungen für alle Anforderungen.

Beratung
Von IT-Strategien bis zu komplexen Prozessberatungen.

Fachanwendungen
Von Polizei-Anwendungen bis zu Software für Berufsbildungsämter.

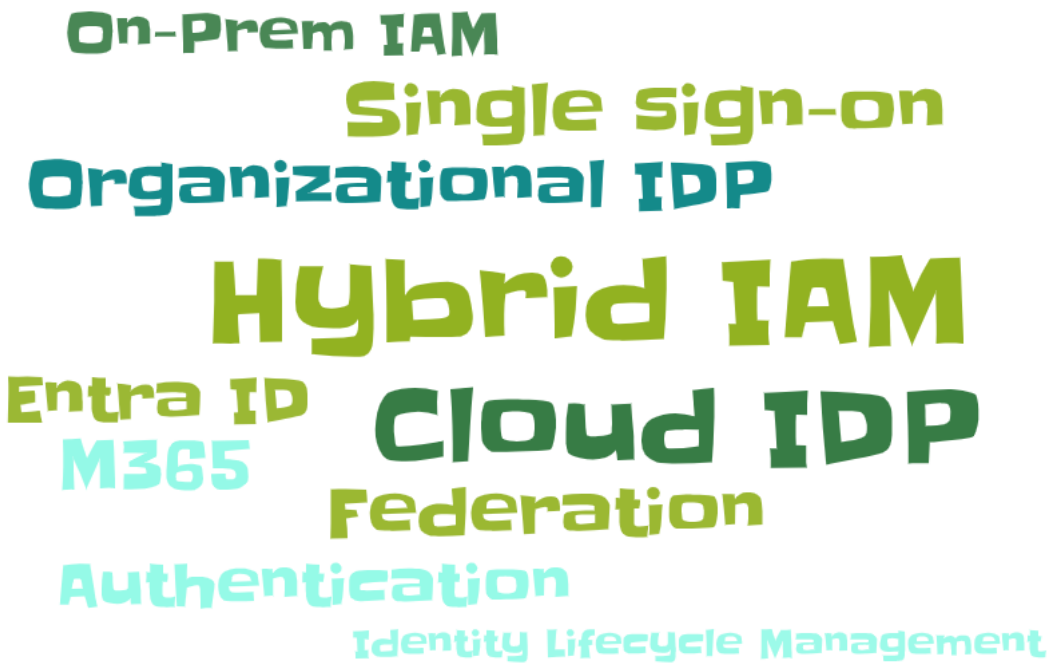


Digital Government
Von Fachanwendungen bis zu voll digitalisierten Verwaltungen.

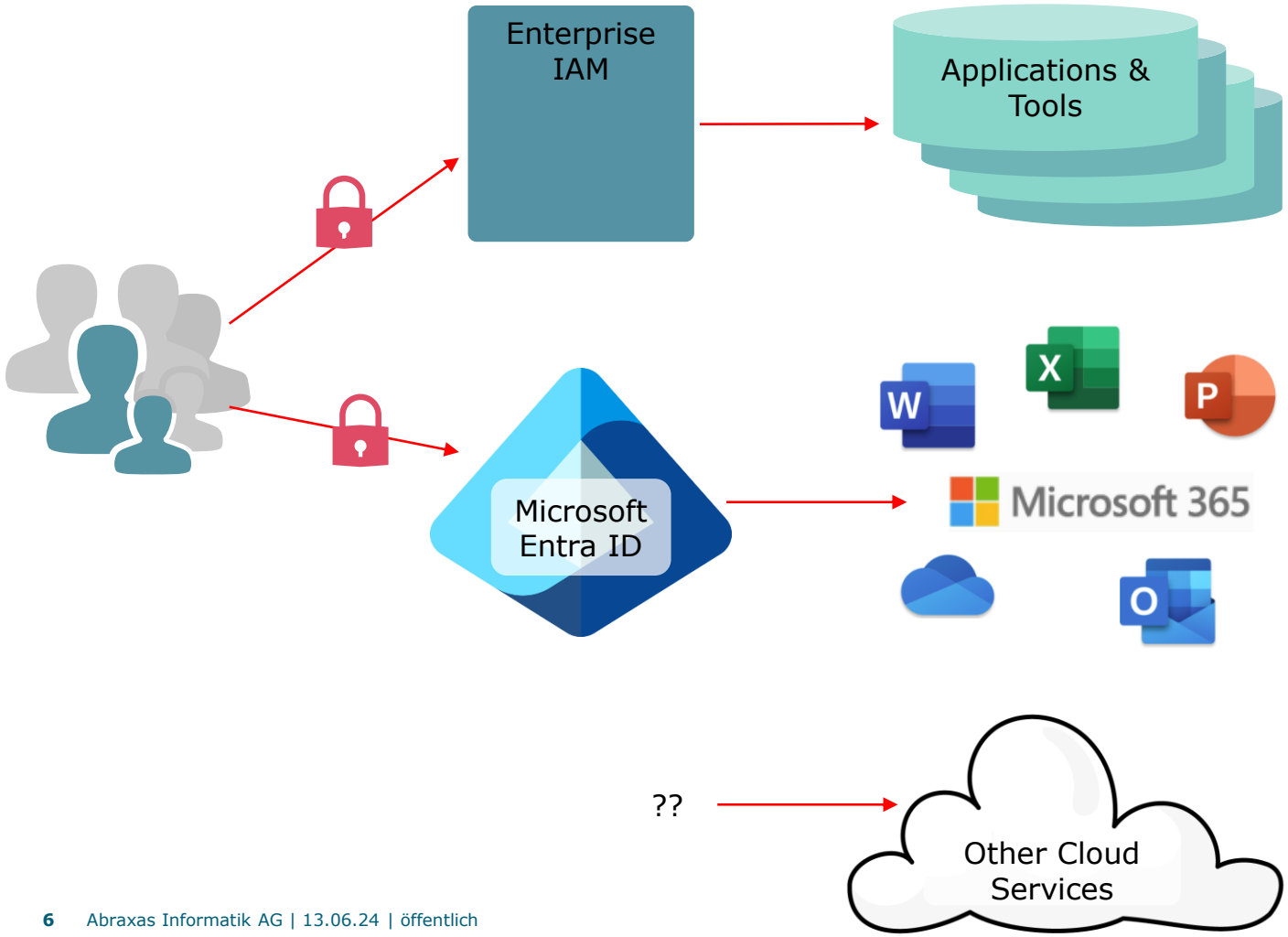
IT Services
Von Workplace bis zu Cloud Services

Der Mehrwert eines hybriden IAM durch Nutzung von Microsoft Entra ID

Silvano Fari

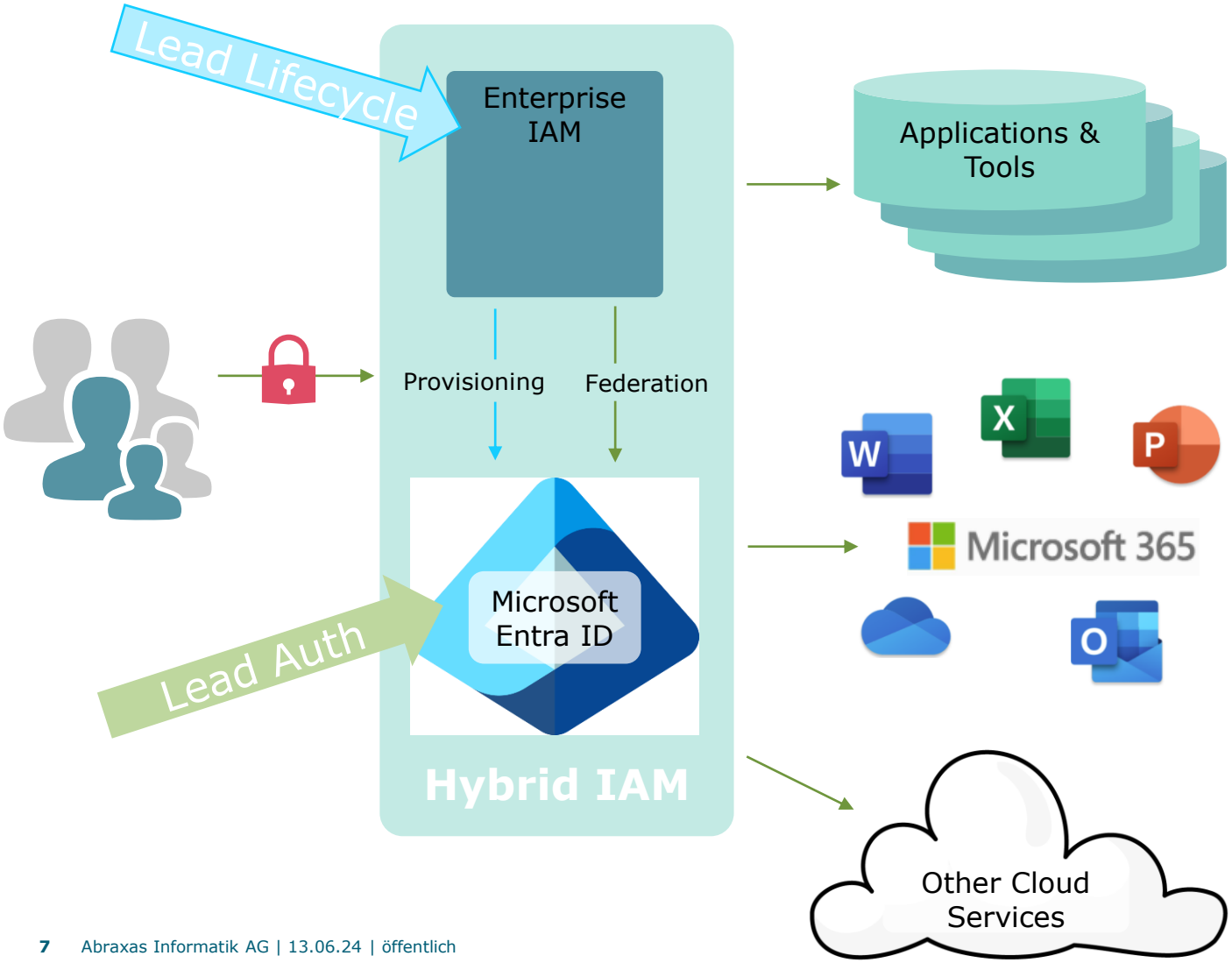


Wie setzt Ihr Euren Cloud IDP ein?



- Applikationen und Werkzeuge der Organisation verwenden das Enterprise IAM als Identity Provider
- Für M365 und Arbeitsplatzlogin wird Entra ID als IDP verwendet
- Verwaltung der Zugriffsdaten wird nicht zentral gemacht > Gefahr von schlechter **Datenqualität**!
- Nutzer:in hat verschiedene Logins > kein **Single sign-on**!

So könntet Ihr Euren Cloud IDP einsetzen!



- Verwaltung der Zugriffsdaten wird zentral über das Enterprise IAM gemacht
- Damit erreichen wir die bestmögliche **Datenqualität**

Perspektive: Lifecycle Management

- Nutzer:in ist mit seinem Windows-Arbeitsplatz bereits eingelogged.
- Damit erreichen wir **Single sign-on** zu allen weiteren Services

Perspektive: Authentication

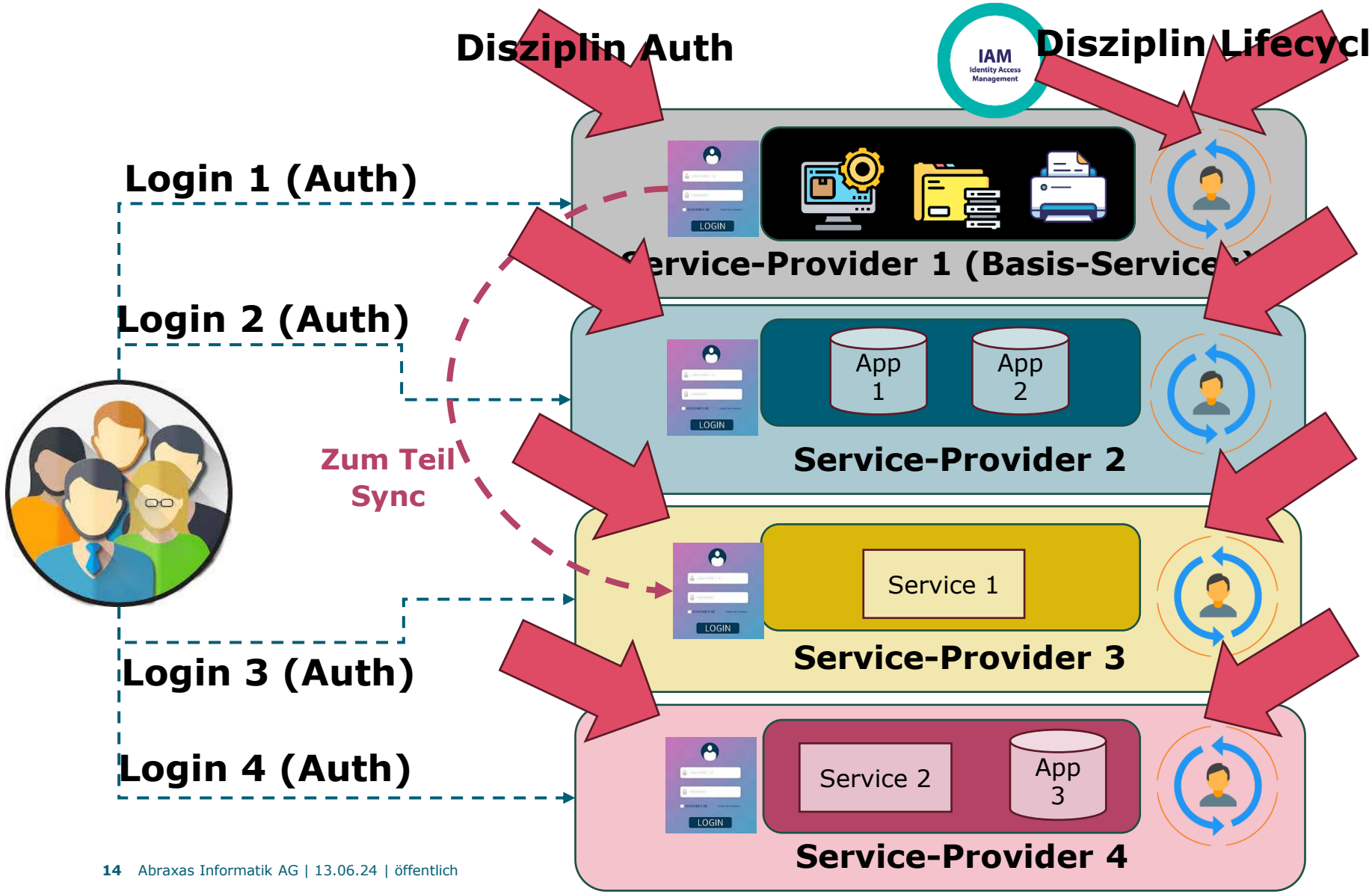
Workshopeinlage 1

- Was sind aus Eurer Sicht die aktuellen Herausforderungen rund um Microsoft Entra ID?
- Welche Fragen habt Ihr zu Hybrid-IAM?
- Aufteilung in die Rubriken:
  - Technik
  - Governance
  - Organisation und Prozesse
  - Vorgehen

Architektur eines hybriden IAM

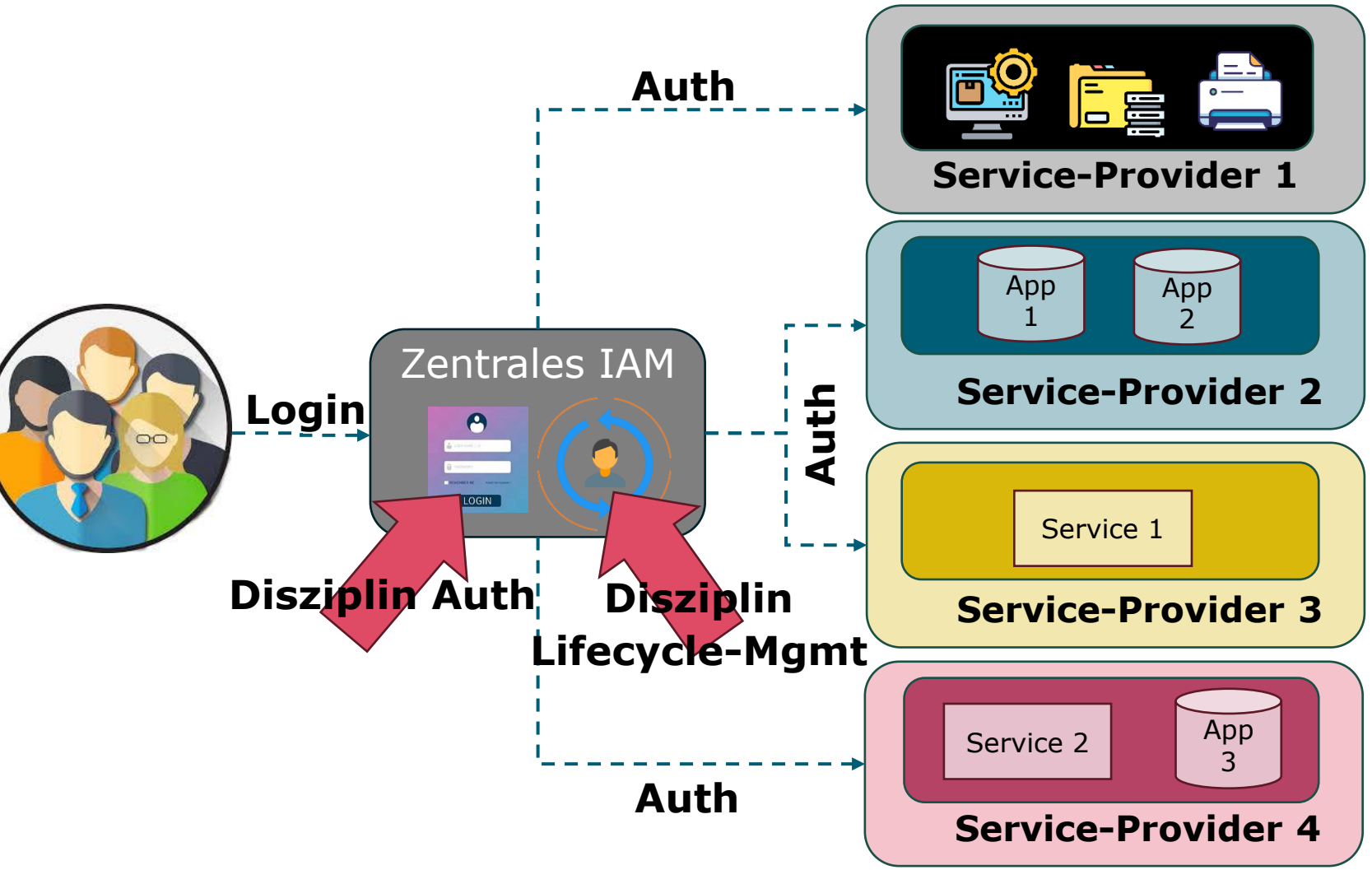
Michael Bommer

Aktueller Zustand von IAM in vielen Organisationen



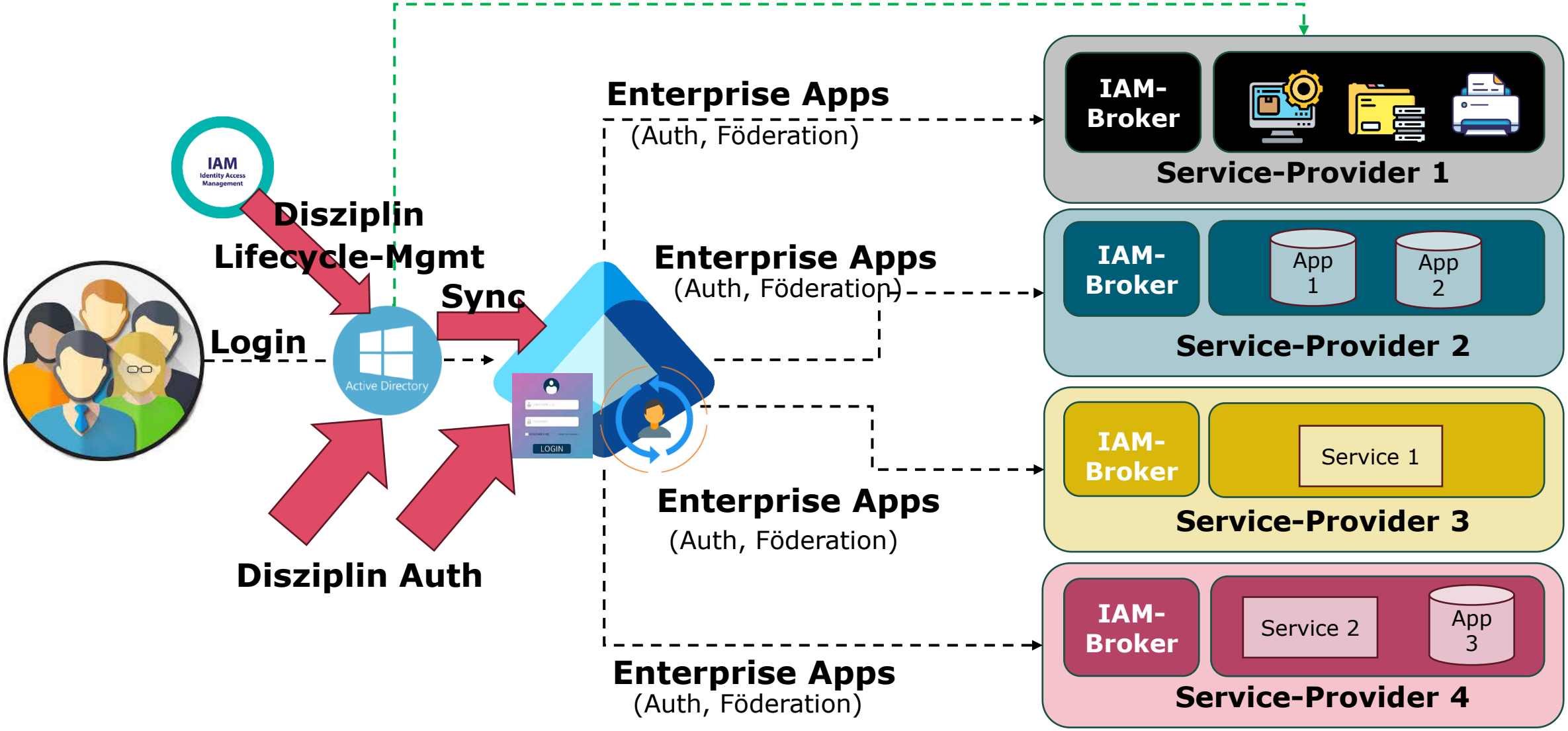
- Pro Benutzer **N** digitale Identitäten/Benutzerkonten
- In diversen, silo-ähnlichen Systemen werden Identitäten/Benutzerkonten gepflegt; versch. Provider im Spiel. Abhängigkeiten von proprietären IAM-Lösungen
- Nur teilweise Kontrolle über von der Organisation genutzte Besucherkonten während des Lebenszyklus
- Geringe Standardisierung
- Kein Single-Sign-On
- Tiefe Benutzerakzeptanz
- Insgesamt hohe Aufwände

Bedürfnisse der Organisationen resp. Kunden

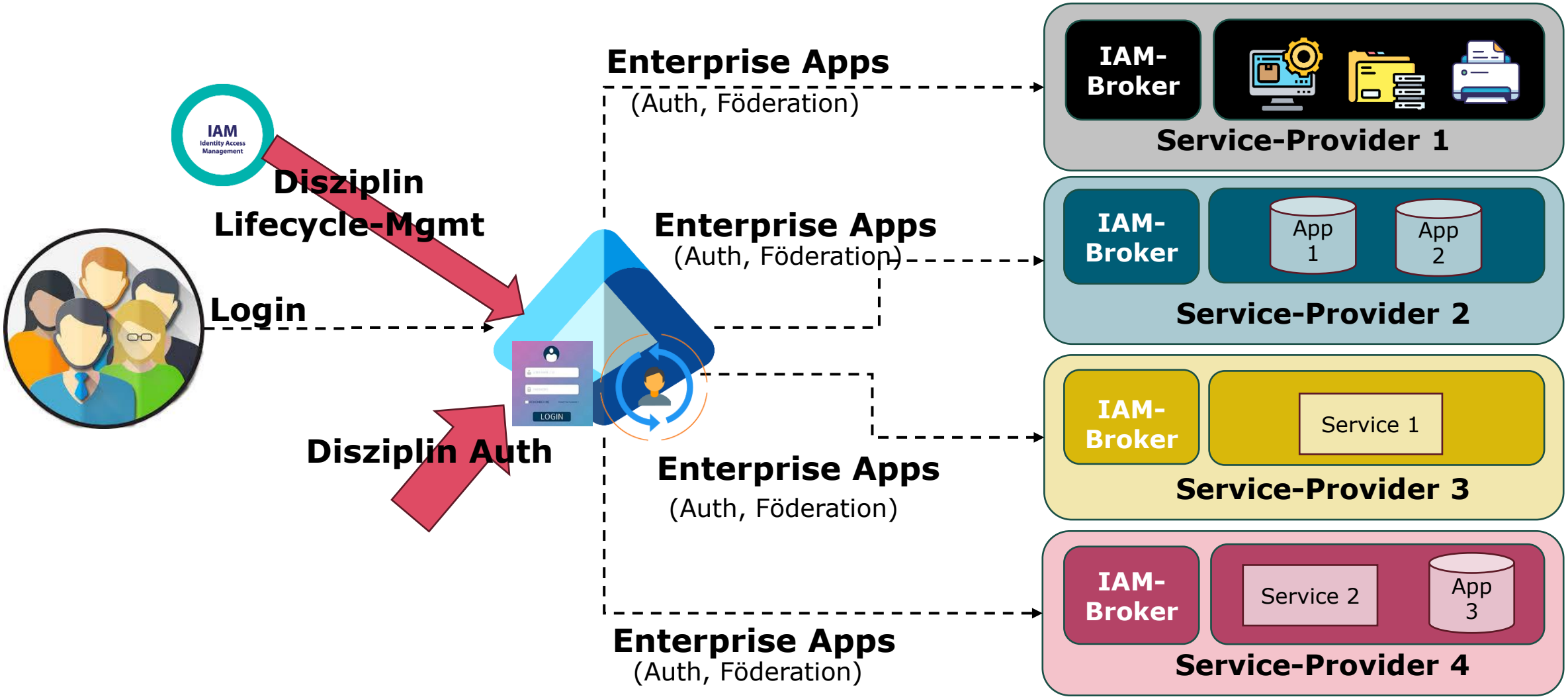


- Pro Benutzer **EINE** digitale Identität/Benutzerkonto
- Vollständige Kontrolle über alle von der eigenen Organisation genutzten Benutzerkonten während des ganzen Lebenszyklus - unabhängig von den verwendeten Applikationen, Services und Providern
- Standardisierte Anbindungen
- Single-Sign-On
- Hohe Benutzerakzeptanz
- Verringerung der Aufwände

Architektur eines hybriden IAM (1)



Architektur eines hybriden IAM (2)



Erreichen wir die gesetzten Ziele?

Ziel	
Pro Benutzer **EINE** digitale Identität/Benutzerkonto	✓
Vollständige Kontrolle über alle von der eigenen Organisation genutzten Benutzerkonten während des ganzen Lebenszyklus - unabhängig von den verwendeten Applikationen, Services und Providern	✓
Standardisierte Anbindungen	✓
Single-Sign-On	✓
Hohe Benutzerakzeptanz	✓
Verringerung der Aufwände	✓

Stärken und Schwächen von Microsoft Entra ID

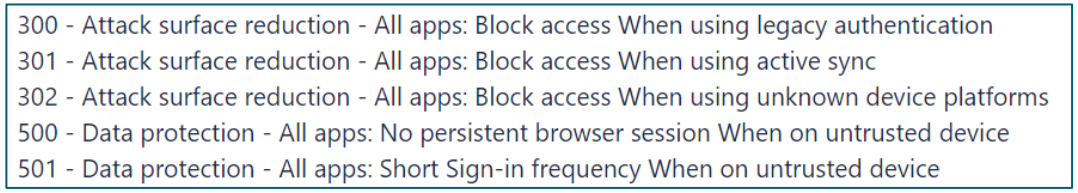
Martin Wüthrich

Entra ID und seine Stärken

- Identity Protection
- Sign-In Protection
- Data Protection
- Föderationen mittels Enterprise Applications
- Gast Identitäten

Identity und Sign-In Protection

- Conditional Access
  - Use-Case basierte Policies verwenden

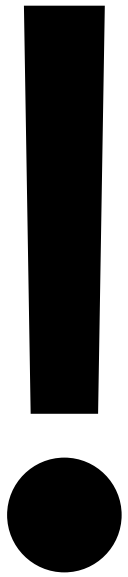


- MFA Registration Campaign einsetzen
- MFA Faktoren von Usern überprüfen
  - Auch durch User selbst!
    - mysignins.microsoft.com/security-info
- Password Leaks erkennen lassen mit PHS
- Passwordless Authentication
  - FIDO2, Microsoft Authenticator, TAP
- Risky Sign-Ins und User Risk via Conditional Access verwalten
  - Entsprechende Alerts auswerten
- Authentication Strength für sensible Bereiche in Betracht ziehen (Quality of Authentication)

Fremdzugriffe und Data Protection

- Gastmanagement
  - Warum ist diese Email Adresse Gast?
  - Muss dieser Gast noch erfasst sein?
  - Wo hat dieser Gast Zugriff?
- Verwaltung von SaaS Applikationen
  - Zugriffe
  - Datenfluss
  - Provisioning
- Service Principals für Automatisierungen
  - App Registration Governance!
- Conditional Access
  - MAM forcieren
  - Limitierter Browserzugriff auf untrusted Devices

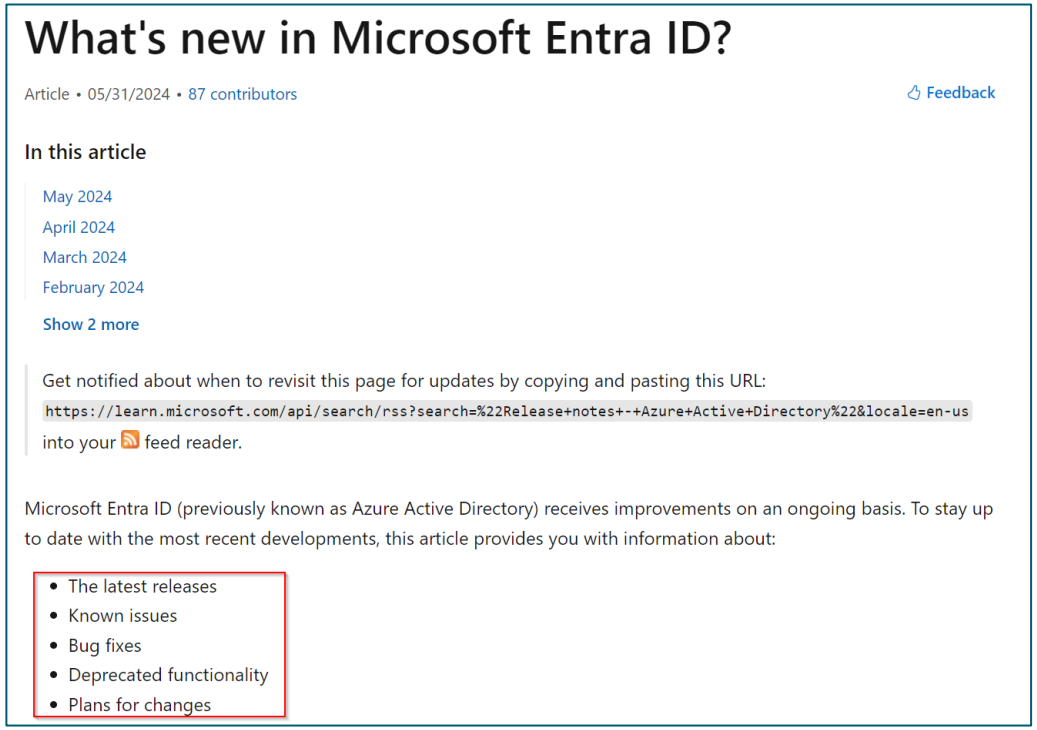
Entra ID und seine Schwächen



- Continuous Integration/Continuous Deployment (CI/CD)
- Externe Zugriffe nur mittels Gast-Objekt zu verwalten
  - Andere Zugriffsmöglichkeiten umgehen das Entra ID (z.B. Sharing Link in SPO)
- Gastmanagement
- Flache Struktur
- Rollenmanagement

Entra ID: CI/CD und ich?

- Was bedeutet das?
- Warum betrifft das mich?
- Wo kann ich mich informieren?
  - ➡ https://learn.microsoft.com/en-us/entra/fundamentals/whats-new
    Public Preview und General Availability



What's new in Microsoft Entra ID?

Article • 05/31/2024 • 87 contributors

Feedback

In this article

May 2024
April 2024
March 2024
February 2024

Show 2 more

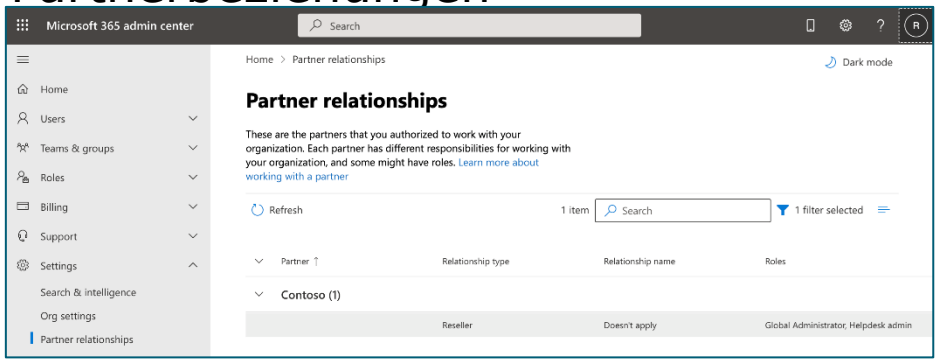
Get notified about when to revisit this page for updates by copying and pasting this URL:
`https://learn.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us`
into your feed reader.

Microsoft Entra ID (previously known as Azure Active Directory) receives improvements on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about:

- The latest releases
- Known issues
- Bug fixes
- Deprecated functionality
- Plans for changes

Externe Zugriffe und Gastmanagement

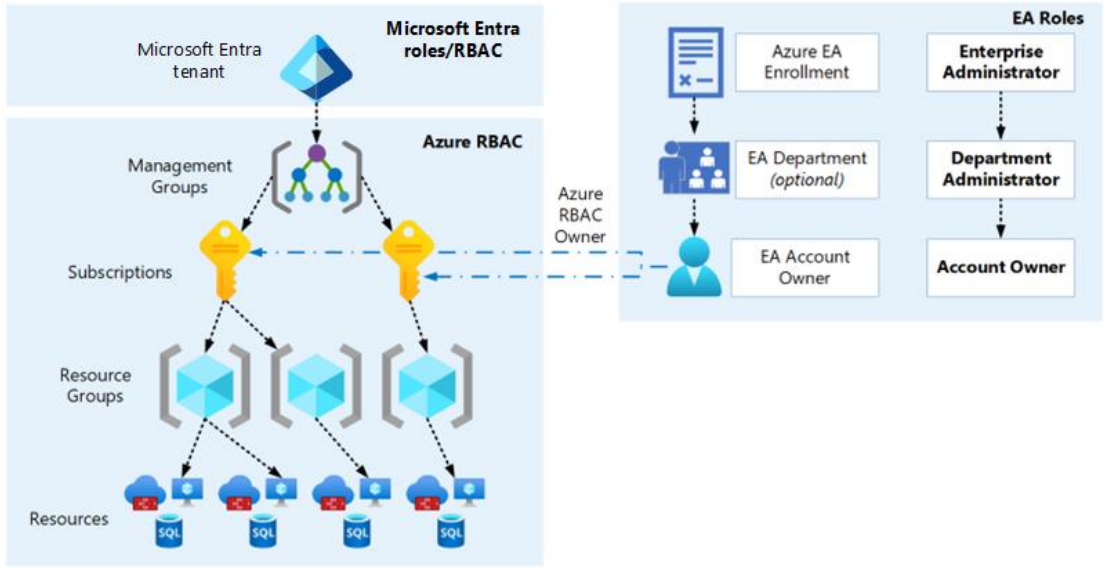
- Externe Zugriffe schwerer zu identifizieren
  - SharePoint Online Links sind allenfalls auch ohne Gastobjekt nutzbar
  - Partner Zugriffe könnten Blindspot darstellen, da ohne Gastobjekt nutzbar
    - Prüfen Sie ihre Partner Zugriffe: "M365 Admin Center" > Einstellungen > Partnerbeziehungen



- Gastmanagement
  - Lösung evaluieren (Power Platform…)
  - Prozesse implementieren

Entra ID Rollen und Hierarchie

- Keine Organizational Units im klassischen Sinn
  - Administrative Units können allenfalls eine Lösung darstellen
- Berechtigungen können mit eigenen Rollen filigran vergeben werden
  - Interessant für App registrations
- Basis für Azure Landing Zone
  - Entra ID steht "über" dem Azure
  - Umbenennung von Azure AD zu Entra ID könnte u.a. aus diesem Grund erfolgt sein



Fragen
&
Anregungen

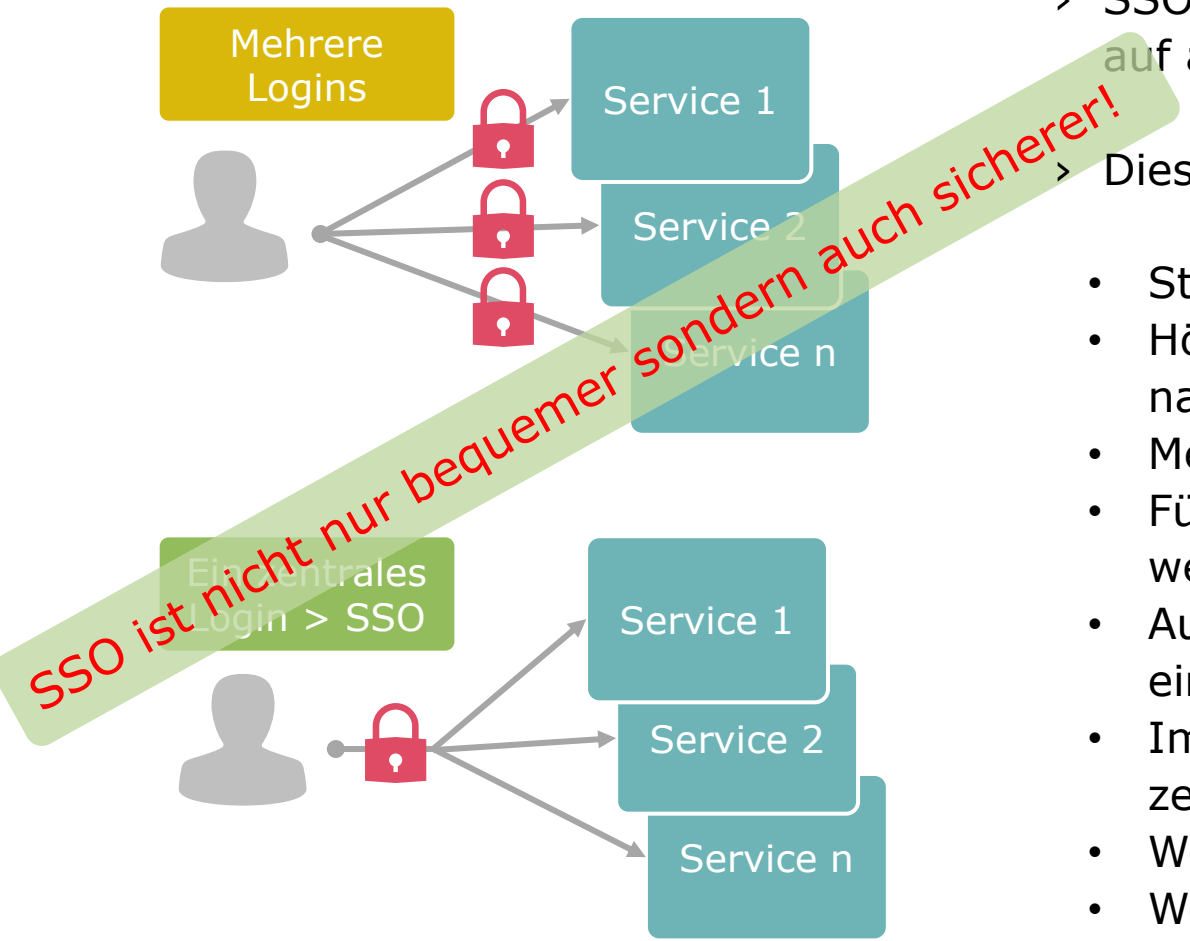
Identity Lifecycle Management im hybriden IAM

Marc Probst

Authentisierung im hybriden IAM

Silvano Fari

Warum ist Single Sign-on wichtig?

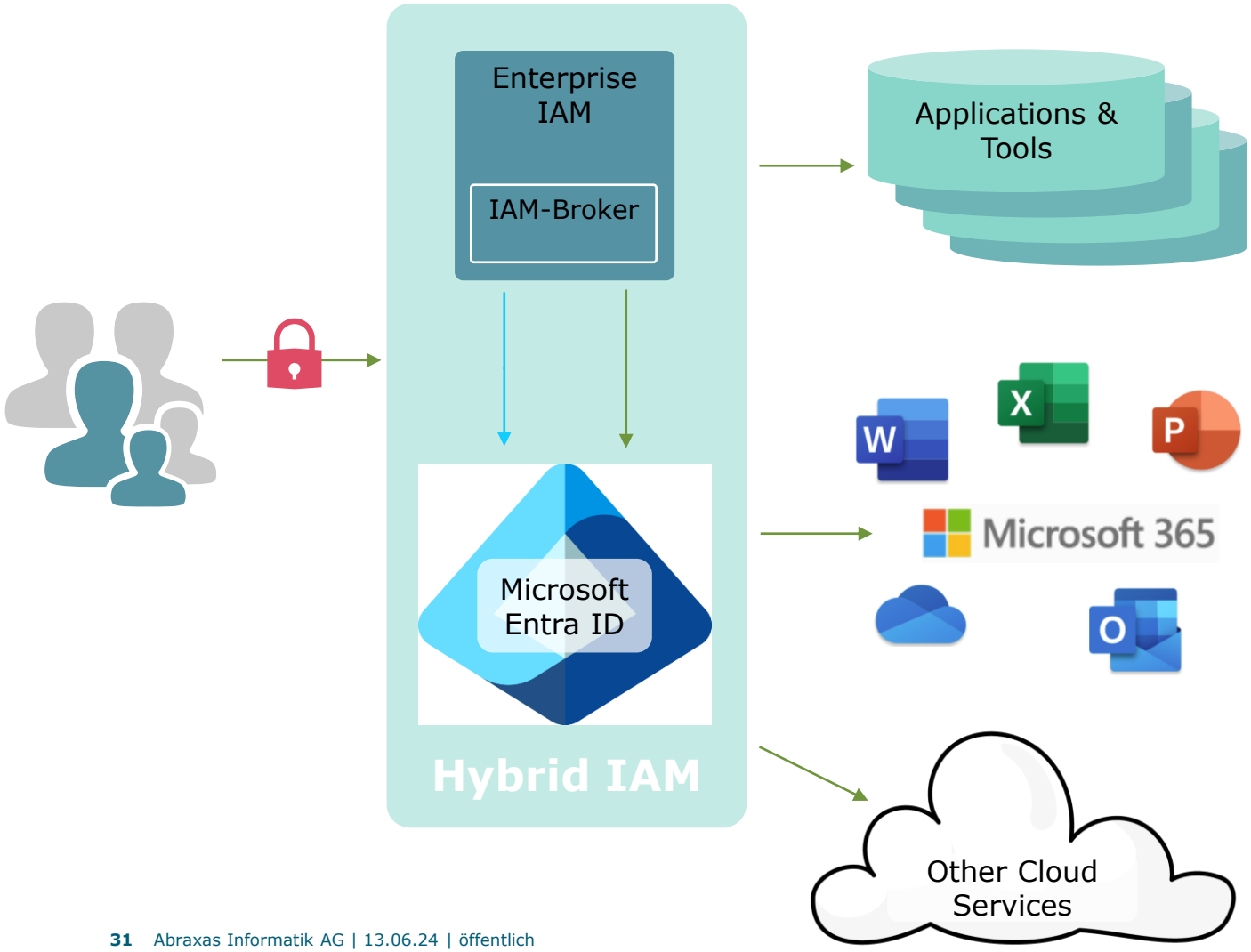


› SSO bedeutet, sich nur einmal anzumelden, um Zugriff auf alle Services zu erhalten.

› Dies bietet folgende Vorteile:

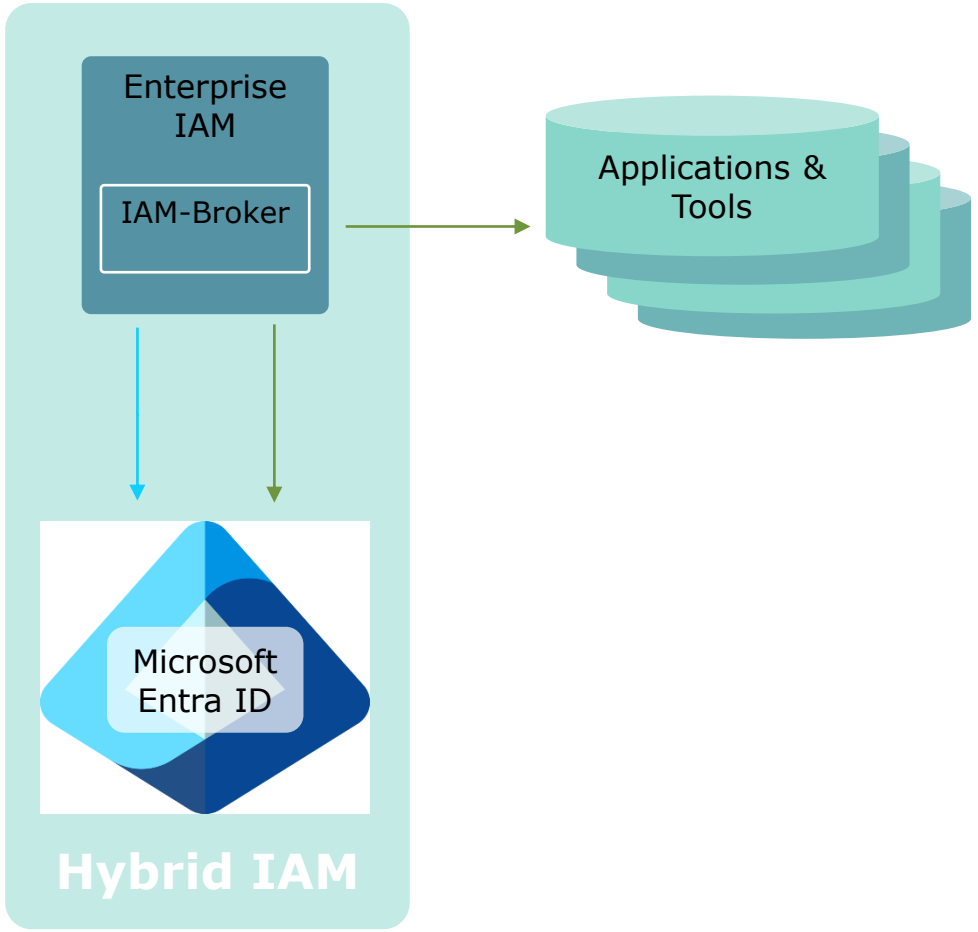
- Steigerung der Produktivität
- Höhere Zufriedenheit der Anwender:innen durch nahtloses Benutzererlebnis
- Mehr Sicherheit da nur ein Login
- Für dieses können stärkere Anmeldedaten gefordert werden
- Auflagen zum Schutz von Daten können einfacher eingehalten werden.
- Im Idealfall wird die Anmeldung am Arbeitsplatz als zentrales Login verwendet.
- Weniger Aufwand beim Helpdesk
- Weniger Aufwand für Verwaltungsprozesse durch zentrale Bereitstellung & Entzug von Zugriffsrechten

SSO mit Hilfe von Entra ID



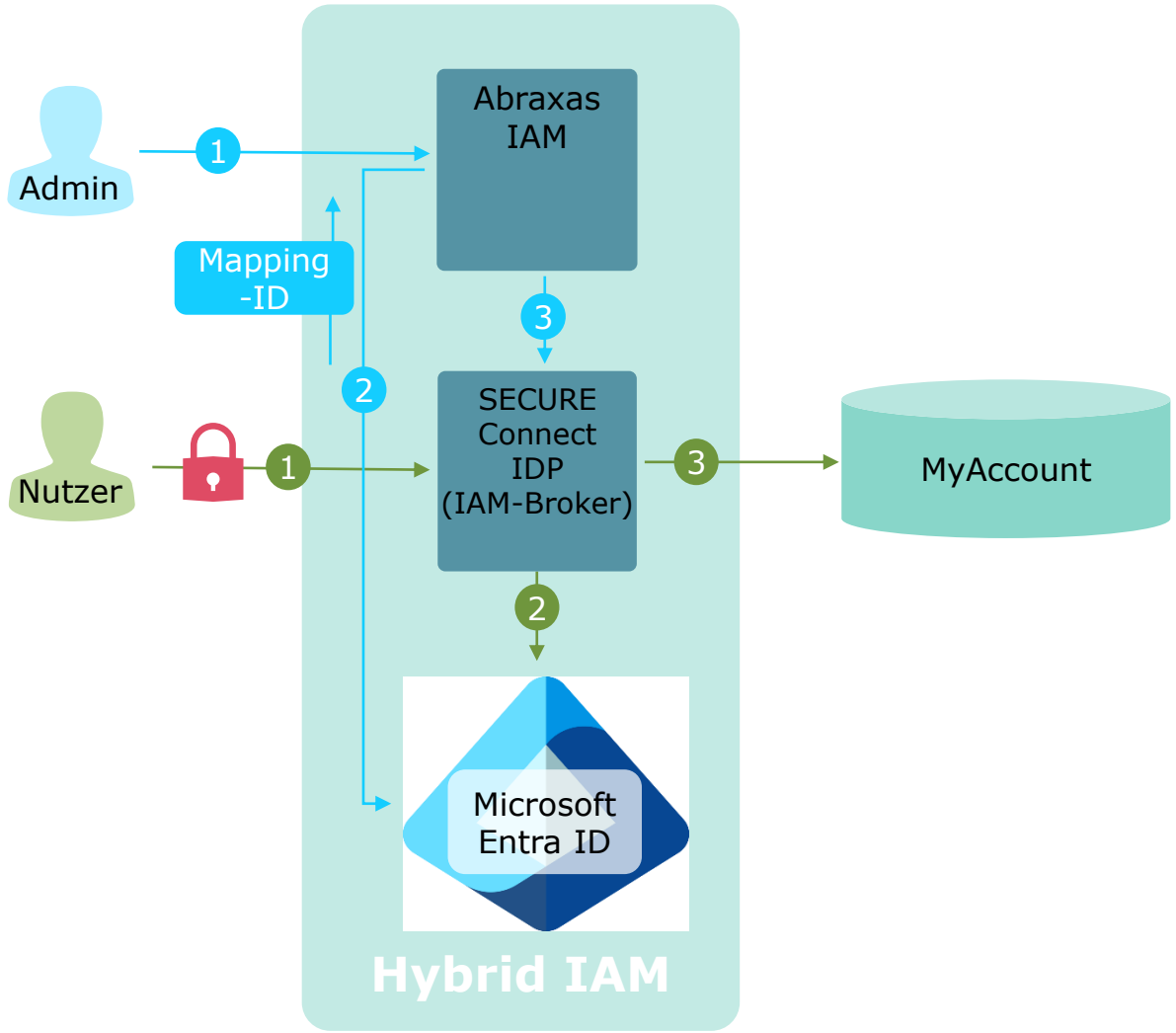
- Benutzer ist mit seinem **Arbeitsplatzlogin** von Entra ID authentifiziert
- Diese Authentifizierung wird für **M365** verwendet
- Diese Authentifizierung wird auch **für andere Cloud-Services** verwendet
- **Organisationseigene Services** authentifizieren die Benutzer über den IAM-Broker vom Enterprise IAM
- Der **IAM-Broker föderiert zum Entra ID** und vertraut dessen Authentifizierung des Benutzers
- Im IAM-Broker gibt es für jeden Benutzer ein **Mapping** zum entsprechenden Benutzer im Entra ID

Brauchen wir einen IAM-Broker?



- **Eigene Services** werden an den zur Organisation gehörenden IAM-Broker angeschlossen
- Entkopplung: **Nur der IAM-Broker föderiert zum Entra ID**
- Föderation vom IAM-Broker zum Entra ID kann für **"Multi-Tenant"** konfiguriert werden
- So können andere Organisationen mit ihren eigenen Entra ID Tenants **kollaborieren**
- Der IAM-Broker kann **Governance** über andere Organisations-Tenants machen
- Risiko des an Microsoft **"ausgeliefert sein"** kann druch Entkopplung mitigiert werden

Demo anhand Abraxas IAM



1. Benutzer wird in IAM erstellt
2. Dieser wird in Entra ID provisioniert
3. Dieser wird in SECURE Connect provisioniert

1. Neu erstellter Benutzer möchte MyAccount verwenden. Er wird auf den IDP von SECURE Connect weitergeleitet
2. Nutzer wählt den Login mit "Microsoft" und wird dadurch zur Anmeldung an Entra ID weitergeleitet
3. Anmeldedaten von Entra ID werden von SECURE Connect übernommen und so wird der Nutzer an MyAccount angemeldet

Fragen & Anregungen

Workshopeinlage 2

- Vier Gruppen diskutieren die in der Workshopeinlage 1 gesammelten Punkte und Fragen
- Jede Gruppe versucht folgende Frage zu beantworten:
  "Welche Vorteile und Chancen entstehen mit dem Einsatz eines hybriden IAM?"
- Eine Person jeder Gruppe macht ein kurzes Wrap-Up