Willkommen im IAM-Circle!

SWISS MADE IAM

abraxas

Delinea
Defining the boundaries of access

ti&m
big ideas. creative technology.

ARCTIC WOLF

COPEBIT

netzmedien

white rabbit
Communications

#7

ITSENSE

Wir sind ITSENSE

FOKUSSIERUNG

Seit 2003 kompromisslosen Fokus auf IAM.

AUS EINER HAND

Als IAM-Hersteller und Integrator sind wir in der Lage auf kundenspezifische Anforderungen einzugehen und in kürzester Zeit zu realisieren.

IAM-EXPERTEN

Langjährige Mitarbeitende Erfahrungen in Consulting, Project Delivery und Software Engineering.

SWISS MADE

Geographische Nähe und das gleiche Qualitätsdenken ermöglichen eine effiziente und partnerschaftliche Zusammenarbeit.

#1

Education

Zugang Wissen &
Experten
Vermittlung Know-how

#2

Maturität

Fachthemen &
Problemlösung

#3

Connecting «Schweiz»

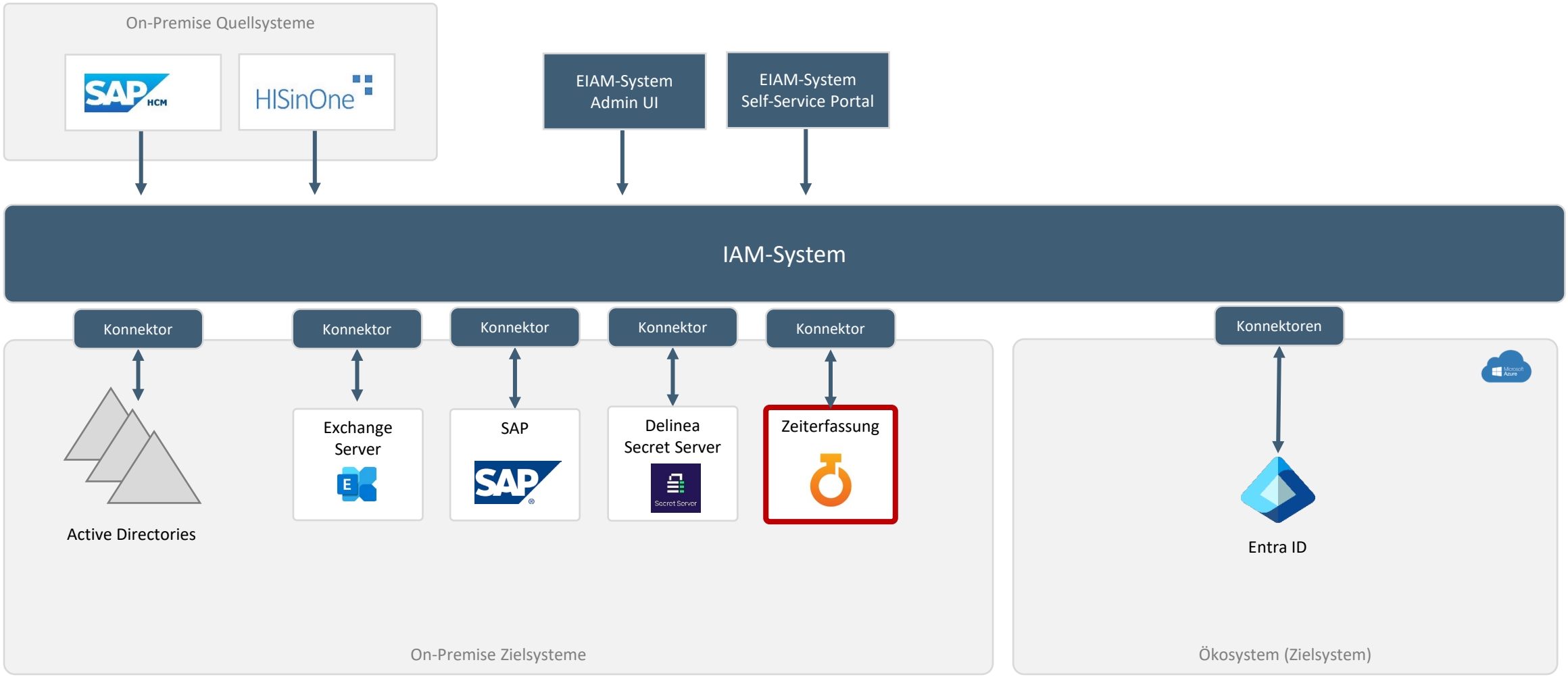
Swissness Intimität
«One-Big-Family»

Vertrauen
ohne Sales-Push

IAM-Circle unterstützt IT-Verantwortliche, IAM-Projekte erfolgreich und kostengünstig in die Machbarkeit zu bringen und umzusetzen.


ITSENSE
Use-Case:
Anbindung einer Fachapplikation an das IAM-System. Wie würdet ihr vorgehen?
Photo by samsommer

Ausgangslage



ITSENSE

Use Case

Die bereits produktive Fachapplikation “Zeiterfassung 1.0” soll an das neue IAM-System angebunden werden.

- **Technische Details**
  - Die Applikationsdaten sind in einer internen Microsoft SQL Datenbank gespeichert
  - Die Applikation besitzt eine gut dokumentierte Schnittstelle (API)
  - Den Benutzer sind bereits 1-8 Berechtigungsrollen zugewiesen
  - Zwischen dem IAM-System und der Fachapplikation sind keine Firewalls vorhanden
- **Mengengerüst**
  - 1‘000 Nutzer (jeder Mitarbeiter)
  - 8 Built-in Berechtigungsrollen innerhalb der Fachapplikation

Use Case

Wie würdet ihr vorgehen?

In Gruppen soll folgendes erarbeitet werden:

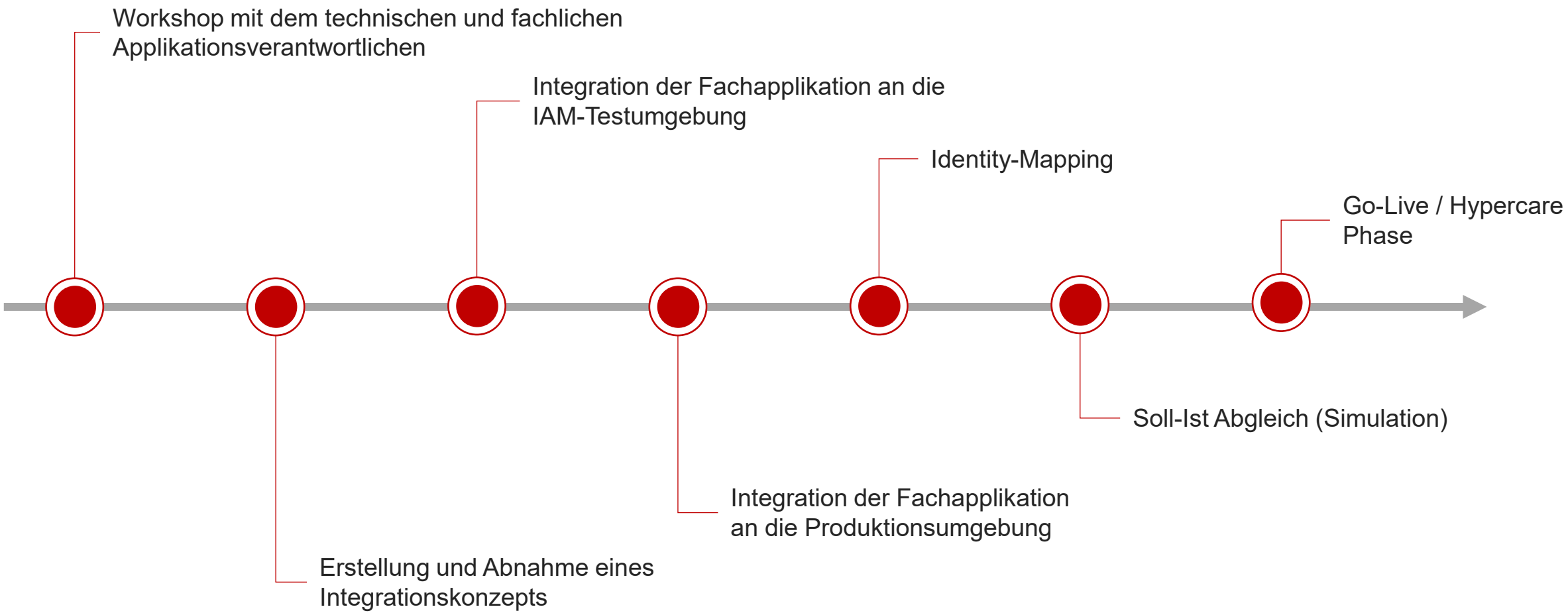
- Welche Informationen werden für die Integration benötigt?
- Wie würdet ihr Vorgehen, so dass die bestehenden Nutzer möglichst nichts mitkriegen?

Zeit: ca. 15 Minuten

Integration von Fachapplikationen im EIAM-Umfeld

Photo by samsommer

Standardisiertes Vorgehensmodell für Fachapplikationen



Informationsbeschaffung

Allgemein

- Hersteller / Release
- Nutzerkreis
- Business Relevanz (Kritikalität)
- Sicherheitsanforderungen (MFA, Verschlüsselung)
- Verfügbarkeitsanforderungen
- Verfügbare Umgebungen der Fachapplikation
- Verfügbare Dokumentationen

Inhaltlich / Logik

- Stammdatenqualität (bestehende Datensätze)
- Logik Benutzermanagement
- Logik und Komplexität Berechtigungsmodell
- Vorhandene Ressourcentypen
- Eindeutiger Identifikator
- Datenfluss / Schnittstellen zu anderen Fachapplikationen

Technisch

- Verfügbare Schnittstellen (API)
- Protokolle und Standards (Bsp. SCIM, SAML, OAuth, OpenID Connect)
- Token Informationen

Verschiedene Arten von «Integration»

Authentifizierung

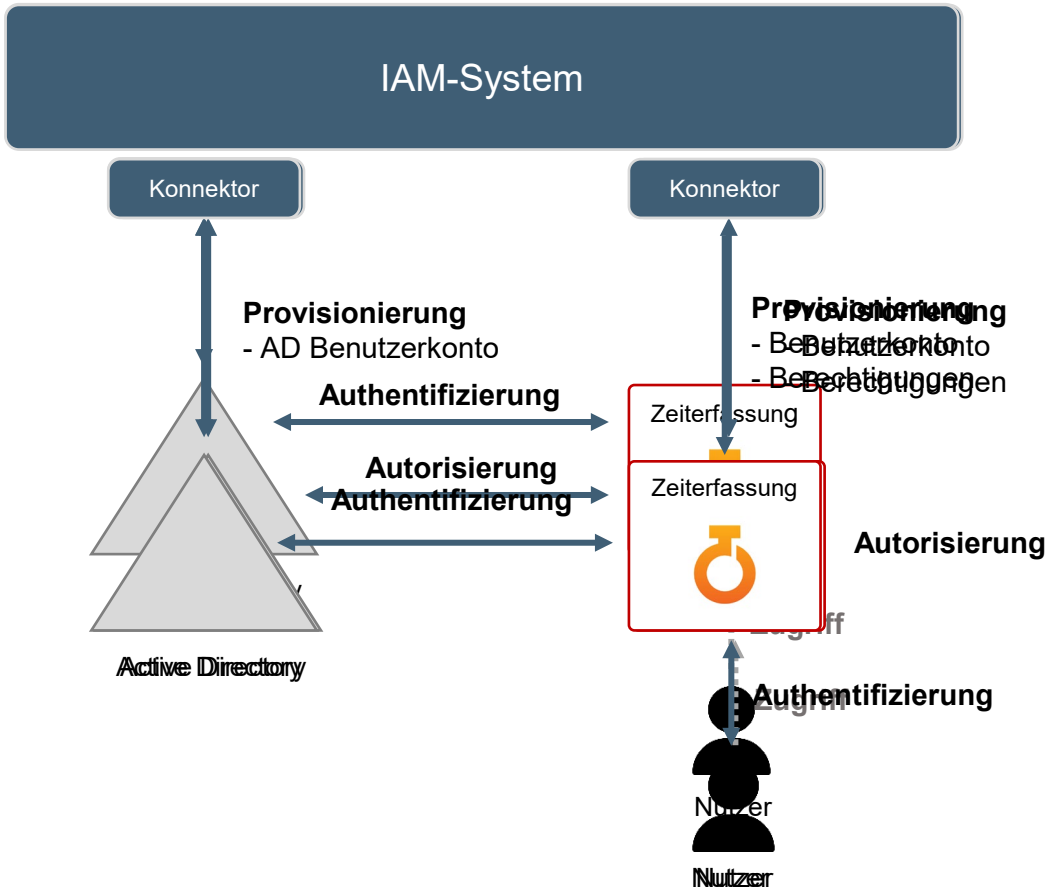
- Erfolgt die Authentifizierung des Nutzers über das Active Directory?

Autorisierung

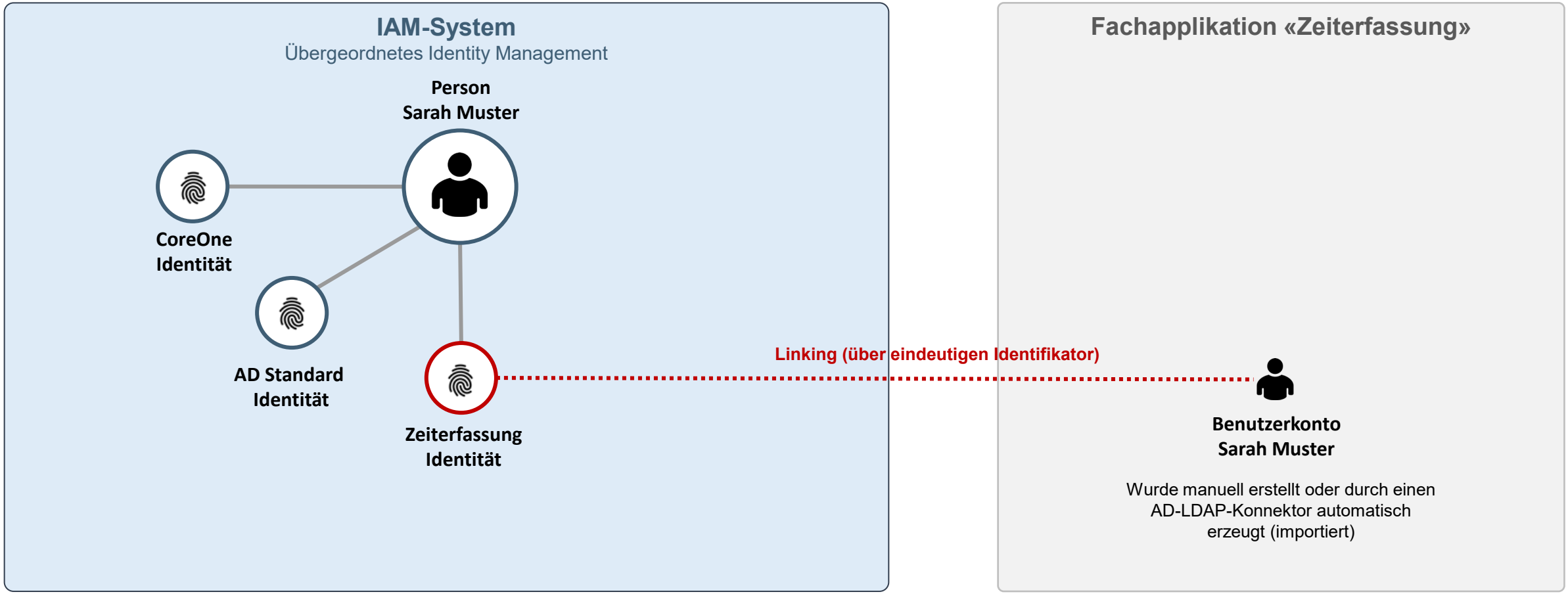
- Erfolgt die Autorisierung des Nutzers über das Active Directory?
- Über welche AD-Gruppen wird die Autorisierung gesteuert?

Provisionierung

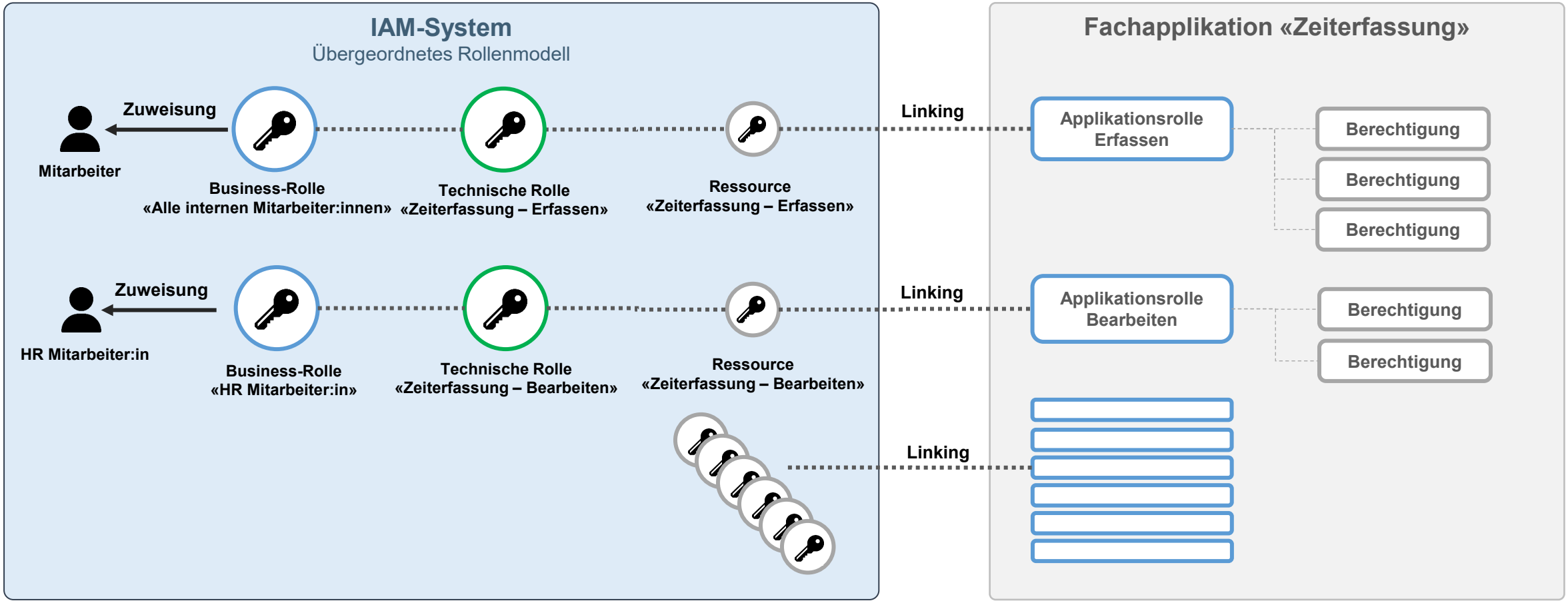
- Was muss das IAM-System in die Fachapplikation provisionieren?
  - Personenobjekte
  - Benutzerkonten
  - Rollenzuweisungen
  - Berechtigungsobjekte



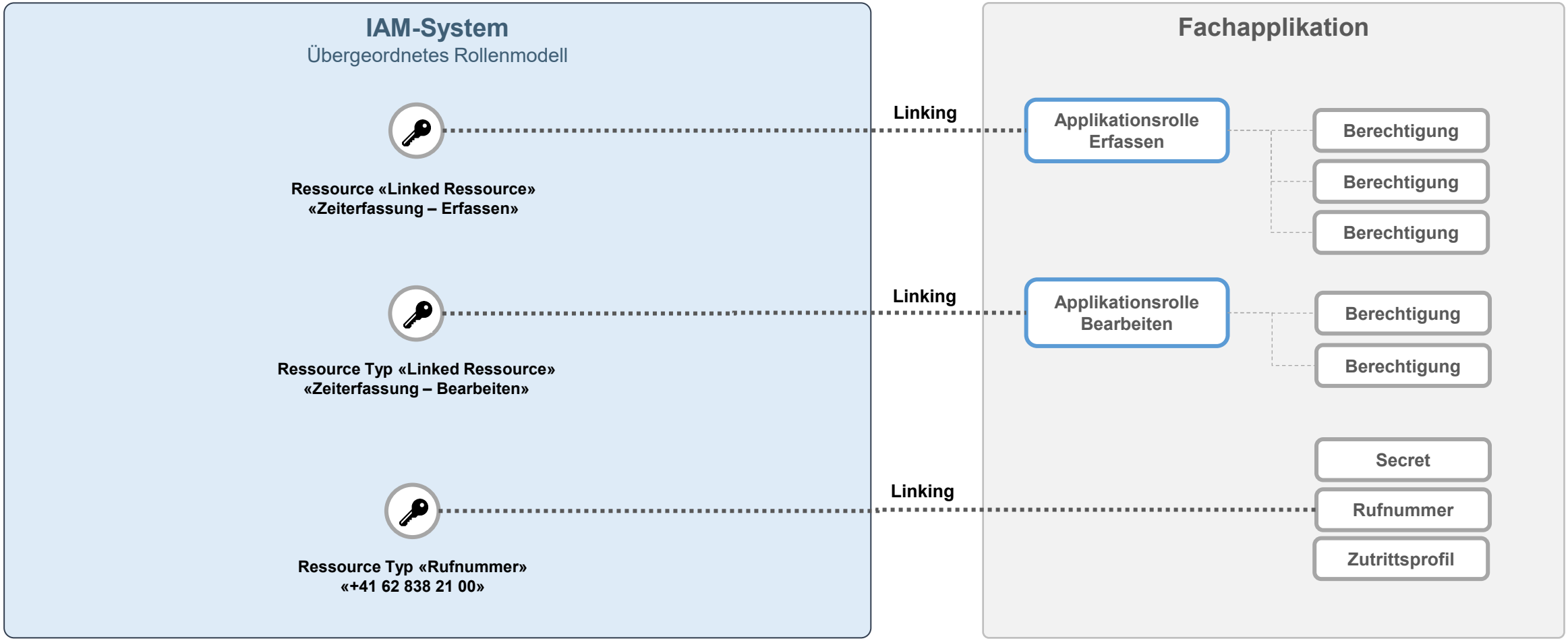
Mapping der Datenmodelle - Benutzerkonten



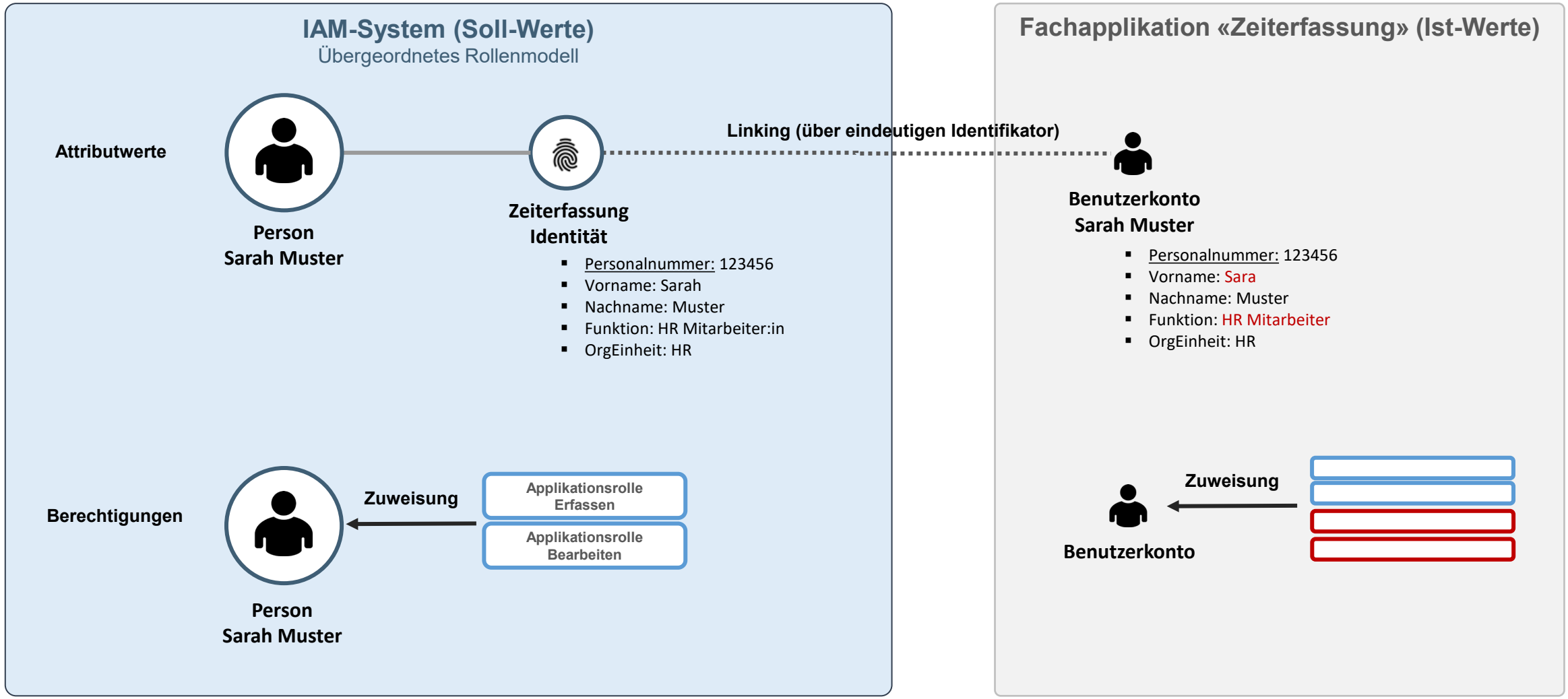
Mapping der Datenmodelle - Berechtigungen



Mapping der Datenmodelle - Ressourcentypen



Soll-Ist-Abgleich



Erfahrungswerte

- Das Mapping von Benutzerkonten nimmt mehr Zeit in Anspruch als gedacht
- Abweichungen in den Soll-Ist-Abgleichen sollten sorgfältig geprüft werden. In der Regel braucht es (je nach Dimensionen) ca. 2 – 6 Iterationen bis der korrekte Soll-Wert bestimmt ist.
- Zeigt Mut zu den «Bereinigungen». Zuviel entzogene Berechtigungen können beispielsweise über ein IAM Self-Service Portal beantragt und damit begründet werden (Nachvollziehbarkeit).
- Alternativ können Berechtigungen vor dem Go-Live manuell entfernt werden, um das Risiko zu minimieren.
- Das klassische Active Directory hat bald ausgedient. Die Zukunft gehört dem Entra ID.
- Eine Schnittstelle (API) ist nicht selbstverständlich. Schon gar nicht eine dokumentierte ☺
- Schnittstellen (APIs) sowie die Logiken für die Benutzer- und Berechtigungsverwaltung innerhalb von Fachapplikationen sind sehr unterschiedlich.
- Die Verwaltungstiefe der Berechtigungen beschränkt sich in der Regel auf Applikationsrollen der Fachapplikation und nicht bis auf Ebene Einzelberechtigung. Manchmal ist weniger mehr!


ITSENSE
Integration von SSO-Applikationen

Der Hersteller hat eine neue Version “Zeiterfassung 2.0” veröffentlich, die SSO unterstützt.

- **Wie gehen wir nun vor?**
  - Was für SSO-Technologien gibt es?
  - Was ändert sich für uns?
  - Müssen wir Daten migrieren?
  - Was müssen wir sonst noch beachten?

Welche Optionen haben wir für SSO?

- **Es gibt unterschiedliche Protokolle**
  Unterschiedliche am Markt etablierte Protokolle stehen zur Auswahl.

WS-Fed

KERBEROS

SAML 2.0

OAUTH 2 OAUTH

OpenID

LDAP

RADIUS

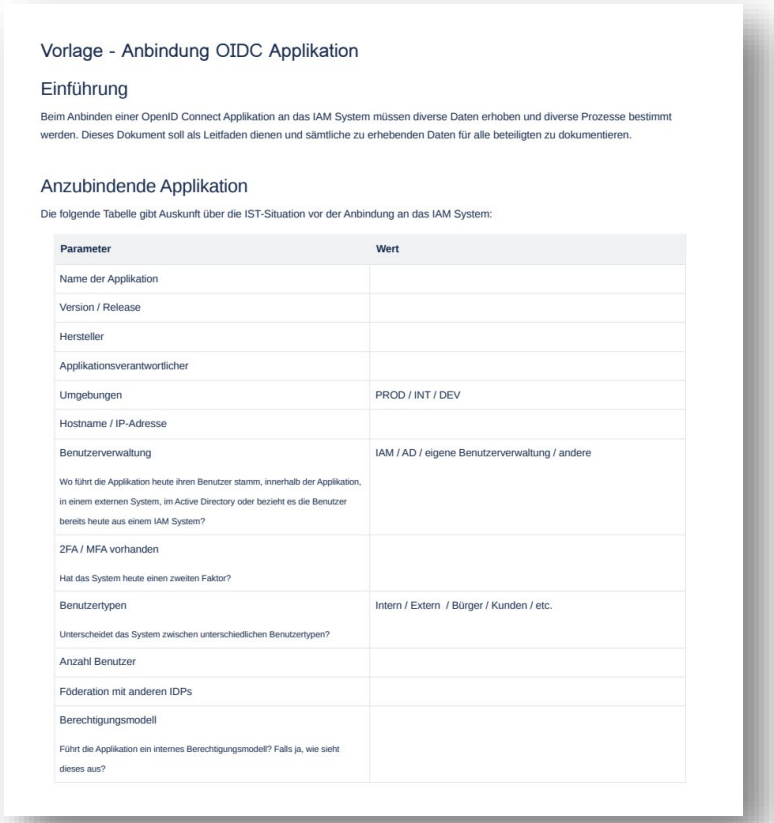
CAS

Stärken und Schwächen

Protokol	Stärken	Schwächen
SAML (Security Assertion Markup Language	▪ Mächtiges Framework für komplexere Anwendungsfälle ▪ Weit verbreitet in Legacy Systemen	▪ Komplex zu implementieren
OAuth 2.0	▪ Flexible und Lightweight ▪ Ideal für webbasierte Applikationen und APIs ▪ Authorization only	▪ Lose Spezifikation (zb. SSL ist kein Muss) ▪ Kein Identity Layer ▪ Muss richtig konfiguriert werden um sicher zu sein
OIDC (OpenID Connect)	▪ Einfach, modern und weit verbreitet ▪ JSON basiert und mobile Freundlich ▪ Identity Layer / Authentication on top of OAuth	▪ Muss richtig konfiguriert werden um sicher zu sein
Kerberos	▪ Sicher und einfach für interne Zwecke	▪ Benötigt synchronisation zwischen Geräten ▪ Limitiert auf Umgebungen wie Active Directory
CAS (Central Authentication Service)	▪ Sicher und einfach für interne Zwecke ▪ Open Source	▪ Limitiere Verbreitung ▪ Nicht so mächtig wie SAML oder OIDC
WS-Federation	▪ Weit verbreitet im Microsoft Ökosystem	▪ Komplex und Outdated
LDAP (Lightweight Directory Access Protocol)	▪ Sicher und einfach für interne Zwecke ▪ Unterstützt hirarchische Beziehungen	▪ Nicht designed für moderne Webapplikationen ▪ Limitiert auf lokale Umgebungen
RADIUS (Remote Authentication Dial-In User Service)	▪ Sicher und einfach für Netzwerkzugriff	▪ Nicht als SSO Protokoll konzipiert
Proprietäre Protokolle	▪ Use-Case spezfisich konzipiert	▪ Schlechte interoperalität

Zeiterfassung 2.0

- **Unterstützt OIDC und SAML 2.0**
  Das sind die beiden Protokolle, die am Markt am meisten verwendet und eingesetzt werden.
- **Wir entscheiden uns für OIDC**
  Leichter zu implementieren und konfigurieren.
- **Wie gehen wir nun vor?**
  Handout → Vorlage – Anbindung OIDC Applikation.



Vorlage - Anbindung OIDC Applikation

Einführung

Beim Anbinden einer OpenID Connect Applikation an das IAM System müssen diverse Daten erhoben und diverse Prozesse bestimmt werden. Dieses Dokument soll als Leitfaden dienen und sämtliche zu erhebenden Daten für alle beteiligten zu dokumentieren.

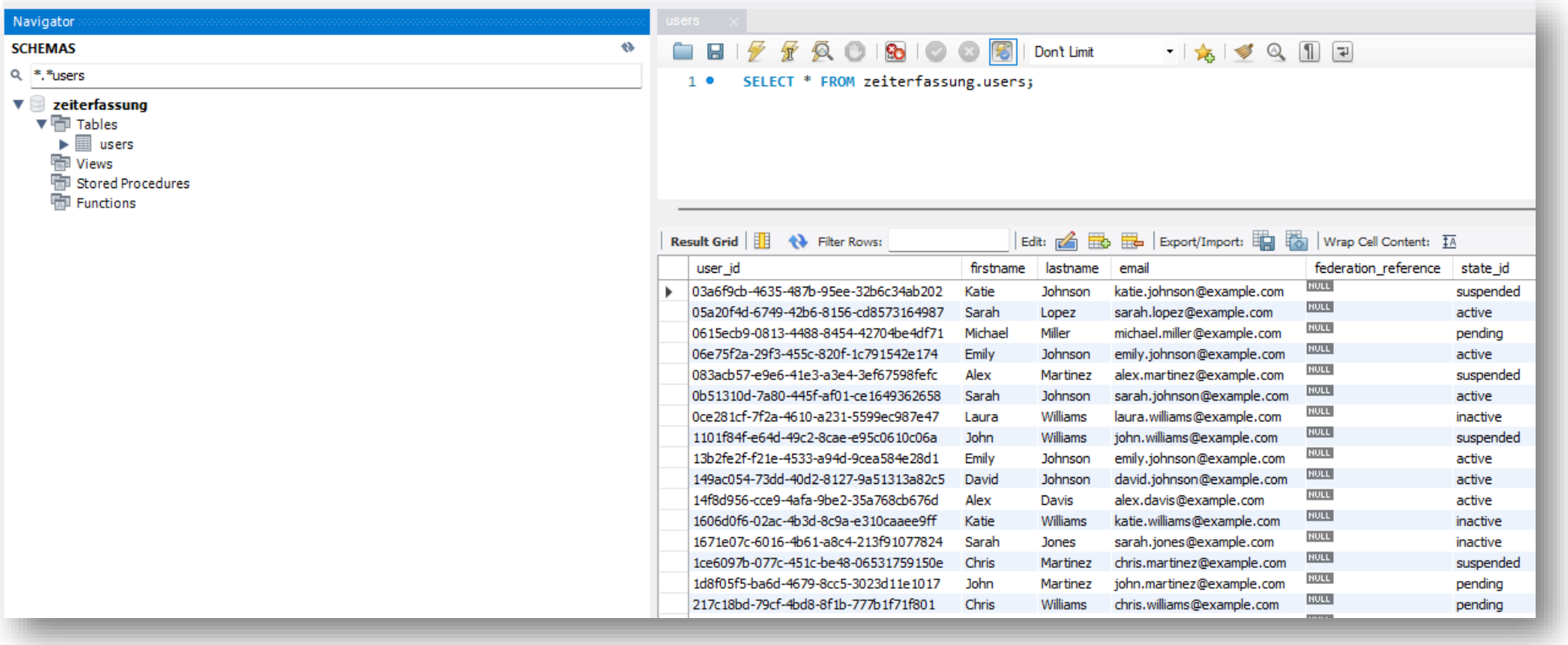
Anzubindende Applikation

Die folgende Tabelle gibt Auskunft über die IST-Situation vor der Anbindung an das IAM System:

Parameter	Wert
Name der Applikation	
Version / Release	
Hersteller	
Applikationsverantwortlicher	
Umgebungen	PROD / INT / DEV
Hostname / IP-Adresse	
Benutzerverwaltung Wo führt die Applikation heute ihren Benutzer stamm, innerhalb der Applikation, in einem externen System, im Active Directory oder bezieht es die Benutzer bereits heute aus einem IAM System?	IAM / AD / eigene Benutzerverwaltung / andere
2FA / MFA vorhanden Hat das System heute einen zweiten Faktor?	
Benutzertypen Unterscheidet das System zwischen unterschiedlichen Benutzertypen?	Intern / Extern / Bürger / Kunden / etc.
Anzahl Benutzer	
Föderation mit anderen IDPs	
Berechtigungsmodell Führt die Applikation ein internes Berechtigungsmodell? Falls ja, wie sieht dieses aus?	

Zeiterfassung 2.0 – IST-Situation

- **Wo führt die Fachapplikation die Benutzer?**
  In der bestehenden Datenbank



Zeiterfassung 2.0 – Onboarding und weiteres

- **Diverse Fragen sind zu klären (siehe Handout)**
  - Wie registrieren sich Benutzer heute an der Fachapplikation und benötigen wir ggf. einen Registrationsprozess?
  - Welche Daten werden erhoben über die Personen?
  - Wie sieht der neue On-Boarding Prozess über das IAM-System aus?
  - Führt die Applikation Organisationen / Unternehmen?
  - Usw.

Zeiterfassung 2.0 – Berechtigungsvergabe

- **Durch den Einsatz eines IdPs verlagern wir die Berechtigung in den Token**
  Berechtigungen liegen nun zentral im IAM-System, dort können sie auditiert, nachvollzogen und zentral verwaltet werden.
- **Fein- vs. Grob-Granularität**
  Wie feingranular wollen wir mit den Berechtigungen werden?
- **Braucht es einen PEN-Test?**
  Macht ein PEN-Test Sinn in diesem Fall?

Zeiterfassung 2.0 – Sicherheitsaspekte

- **Sichere Konfiguration**
  Wahl des richtigen Flows, Secret, Redirect URLs
- **Das System ist nur so sicher, wie das schwächste Glied**
  Die Erfahrung zeigt, die meisten Schwachstellen sind in der Fachanwendung (Signatur Check, Token im Frontend, etc.)


ITSENSE
Panel-Discussion / Q&A

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

#7