IDM-Projekt Universität Konstanz
Identity Management mit OpenIDM

Andreas Schnell
Michael Längle
Universität Konstanz

Identity Management
Agenda

Universität Konstanz

I Ausgangssituation

II Vorgehensweise

III Projekt

IV Warum OpenIDM?

V Fragen

Identity Management
Ausgangsituation - Universität Konstanz

Universität Konstanz

- Campus-Universität
- 3 Sektionen
  - Mathematisch-Naturwissenschaftliche Sektion
  - Geisteswissenschaftliche Sektion
  - Sektion Politik – Recht – Wirtschaft
- 2 Graduiertenschulen
- 1 Excellence-Cluster

- ca. 3.000 Mitarbeiterinnen und Mitarbeiter
  davon ca. 1.000 bei zentralen Einrichtungen, Rest wissenschaftlich
- ca.10.500 Studierende

Identity Management
Ausgangsituation - Datenquellen

Universität Konstanz

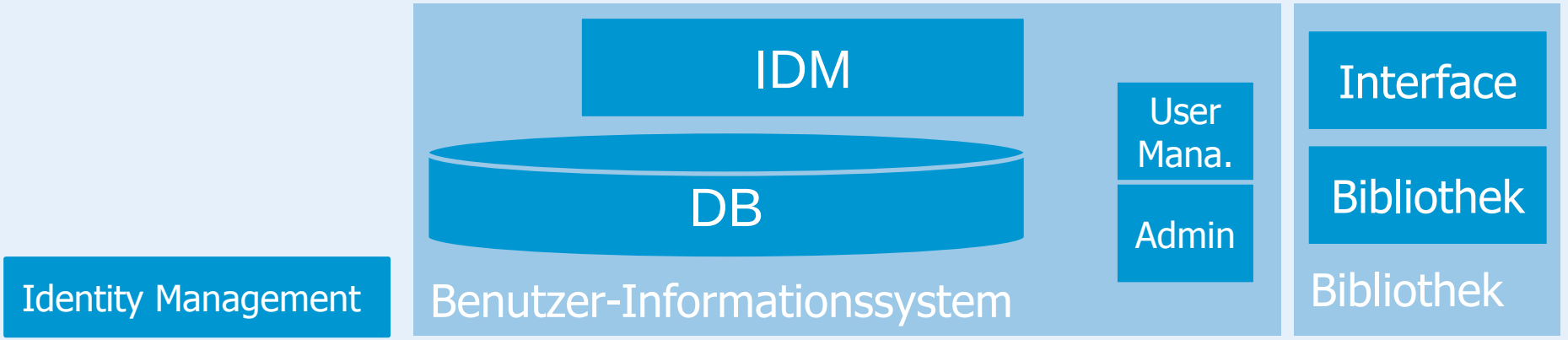
Datenquellen

- Mehrere unterschiedliche führende Datenquellen
  - Mitarbeiter, Studierende, Externe, Gäste, Bibliotheksbenutzern usw.
- Teilzeitmitarbeiter mit mehreren Verträgen in unterschiedlichen Organisationseinheiten und unterschiedlichen Laufzeiten
- Studierende als wissenschaftliche Hilfskräfte
- Mitarbeiter ohne „Vertrag“
- Unzureichende Datenqualität und fehlende Attribute
- DFN-AAI-Konformität erfordert persönliches Erscheinen
- Nutzung von Accounts über das Vertragsende hinaus

- Gesamt ca. 13.000 Accounts, ca. 40.000 externe Bibliotheksbenutzer
- ca. 4.000-5.000 wechselnde Accounts pro Jahr

Identity Management
Ausgangsituation - Benutzer-Informationssystem

Universität Konstanz



- Support einer zentrale Komponente abgekündigt
- neue Anforderungen technisch nur schwer umsetzbar
- Graphische Oberflächen als separate Anwendungen
- Anbindung Bibliothek ist zu ändern

- Teilweise Verwaltung von mehreren Accounts pro Identität

Identity Management
Ausgangsituation - Verzeichnisdienste

Universität Konstanz

Verzeichnisdienste

LDAP Zentral | LDAP Mail | AD | LDAP Bib.

- Mehrere LDAPs
- Unterschiedliche Datenstrukturen und –Inhalte auf den einzelnen Systemen
- AD aufgrund Struktur nur für einen Teil der Mitarbeiter nutzbar
- AD auf Basis von Windows 2003

Identity Management
Ausgangsituation - Anwendungen

Universität Konstanz

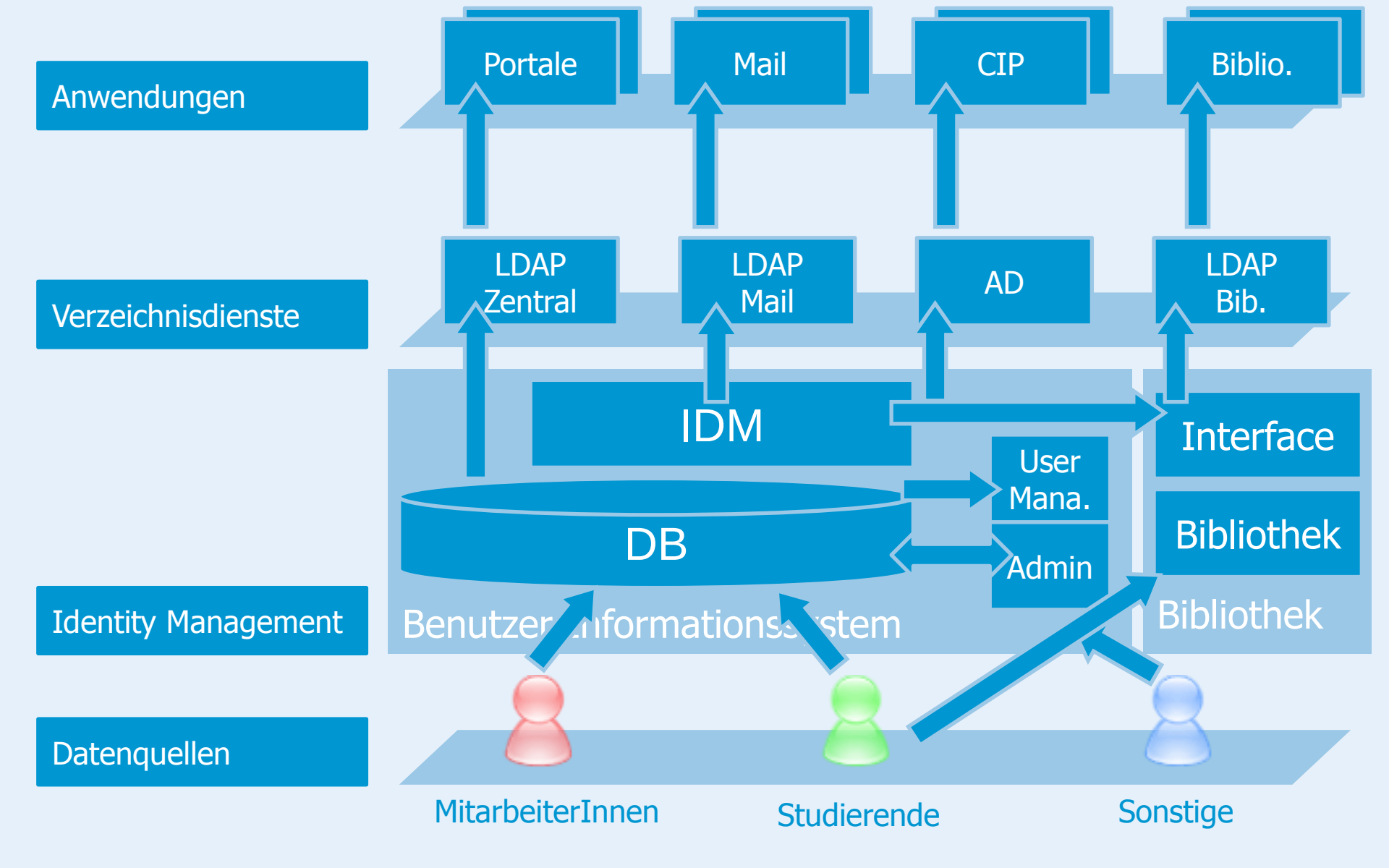
Anwendungen

Portale | Mail | CIP | Biblio.

- Integration von Portalen aufgrund unterschiedlicher Dateninhalte schwierig
- Fehlende Attribute für Anwendungen
- Teilweise eigene Datenverwaltung in den Anwendungen
- keine einheitliche Struktur

Identity Management
Ausgangsituation - Architektur

Universität Konstanz



Identity Management
Vorgehensweise - Ziele

- Automatisierte zentrale Bereitstellung von AuthN-Informationen
- Automatisierte zentrale Bereitstellung von AuthZ-Informationen
- Identitäten statt Accounts

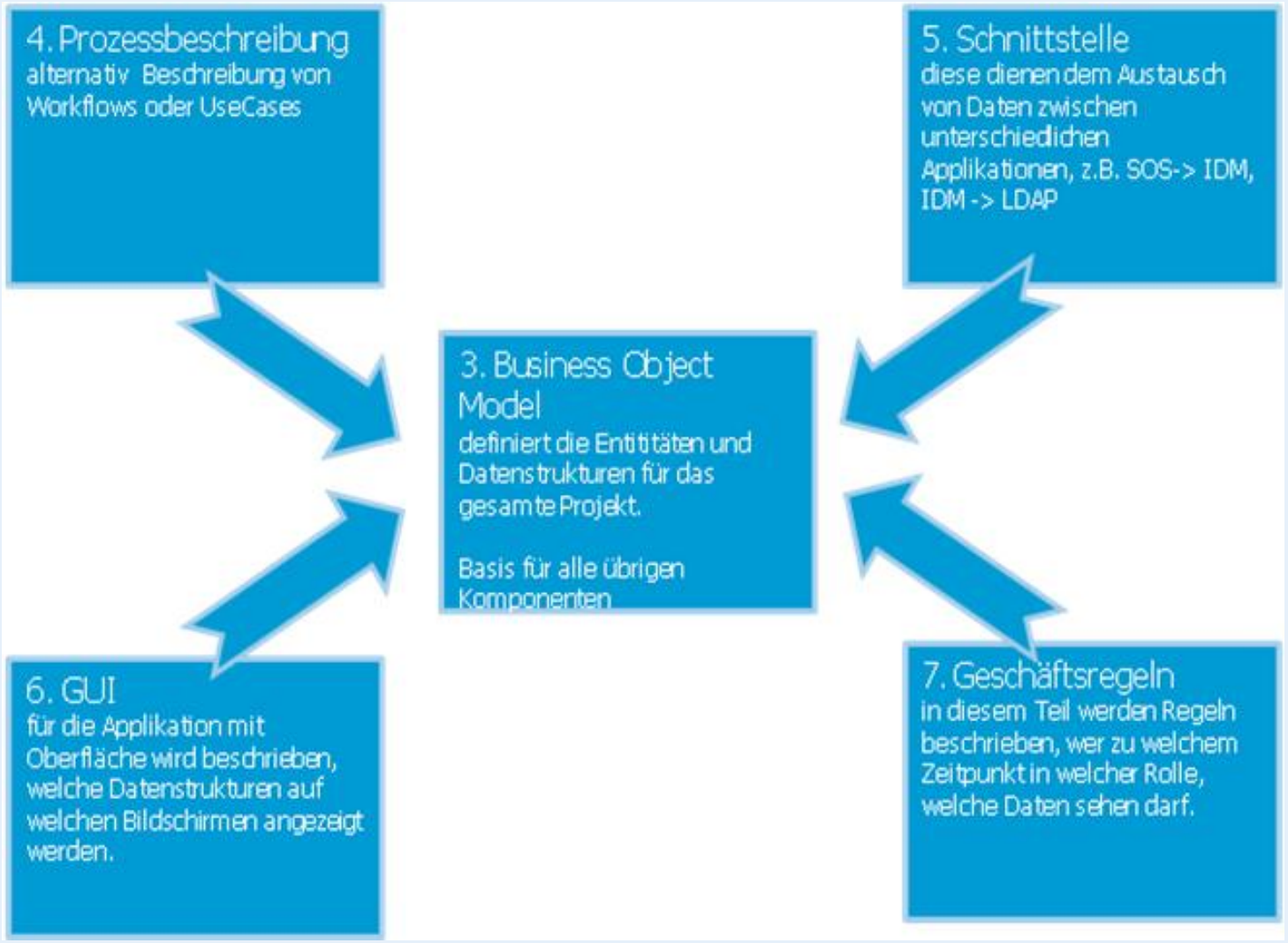
Identity Management
Vorgehensweise - Unterteilungen

Universität Konstanz

- **Juristische Unterteilung**
  - Mitglieder nach Landeshochschulgesetz
  - Angehörige nach Grundordnung der Universität
  - Sondergruppen
- **Betriebliche Unterteilung**
  - Bedienstete (Professoren, hauptberuflich tätig, Gastprofessoren, usw.)
  - Nicht-bedienstete Mitglieder (Emeriti, Privatdozenten, Ehrensenatoren, usw.)
  - Studierende (Eingeschriebener Studierender bzw. Doktorand, Schülerstudent, beurlaubt …)
  - Alumni/VEUK (ehemalige Mitglieder)
- **Wissenschaftliche Unterteilung**
  - Wissenschaftlich tätig, Verwaltung
- **Organisatorische Unterteilung**
  - Fachbereiche, Lehrstühle, Arbeitsgruppe, Projekte, Sonderforschungsbereich
  - gemäß Organigramm
- **Kollaborative Unterteilung**
  - Freie Gruppeneinteilung (Senat, Asta, fachübergreifende Arbeitsgruppen, usw.)

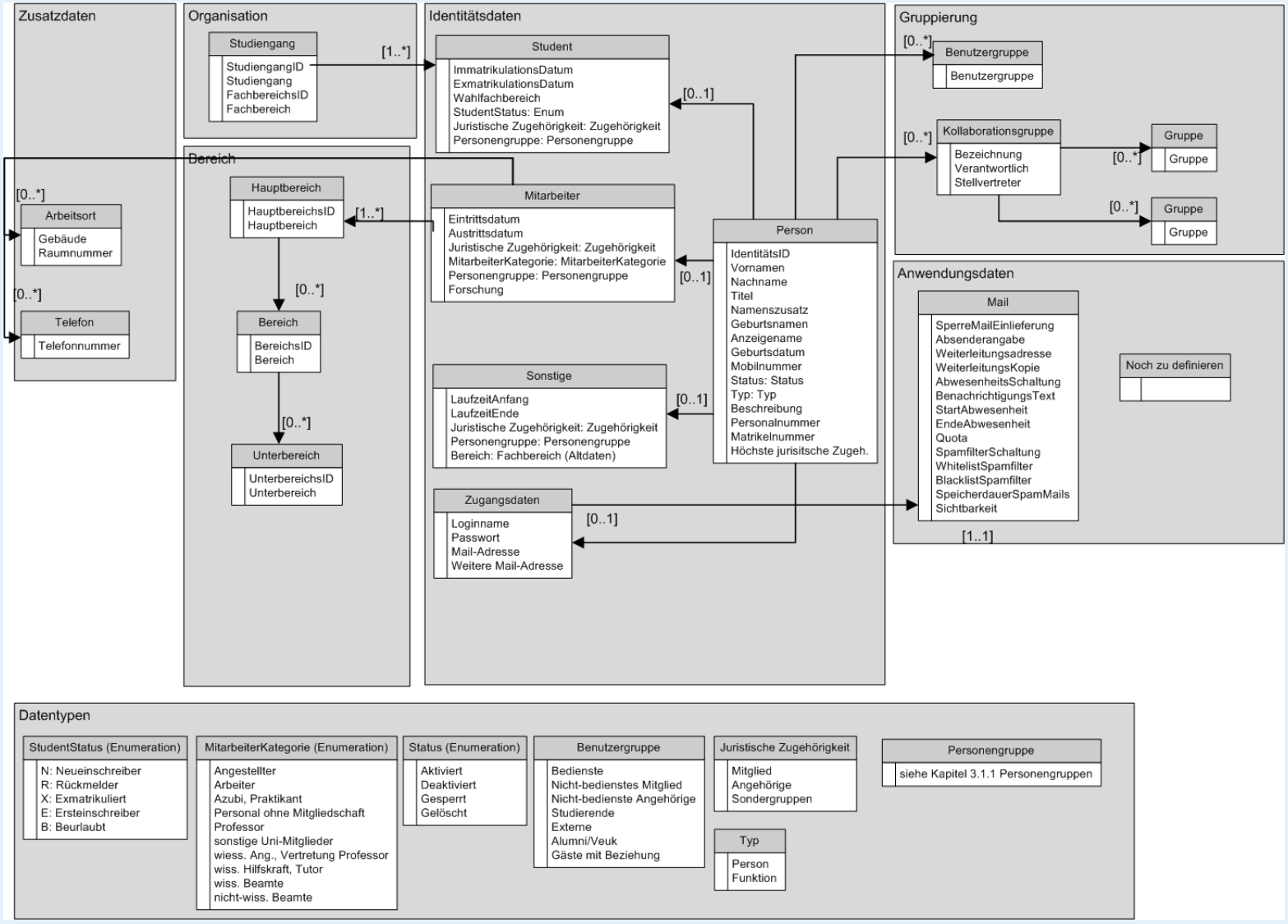
Identity Management
Projekt - Projektdokumentation

Universität Konstanz



Identity Management
Projekt - Business Object Model(1)

Universität Konstanz



Identity Management
Projekt - Business Object Model(2)

Universität Konstanz

Attribut	Datentyp	Beschreibung	Identifizierendes Attribut ?	Führendes System
IdentitätsID (PopID)	String (10)	Eindeutige Kennung einer Person. Jede berechtigte Person hat nur eine einzige PopID. Die PopID hat den Prefix pop, gefolgt von 4-6 Ziffern, z.B. pop245789	Nein	IDM
Vornamen	String (30)	Alle Vornamen, ohne Kennzeichnung des Rufnamens in der Formatierung der Verwaltung	Ja	SOS, SVA, IDM
Nachname	String (35)	Nachname ohne Namenszusatz und ohne Titel	Ja	SOS, SVA, IDM
Titel	String (255)	Akademischer Titel, z.B. Dr.	Nein	SOS, SVA, IDM
Namenszusatz	String (30)	Namensbestandteil z.B. "von"	Nein	SOS, SVA, IDM

Identity Management Projekt - Prozesse(1)

Universität Konstanz

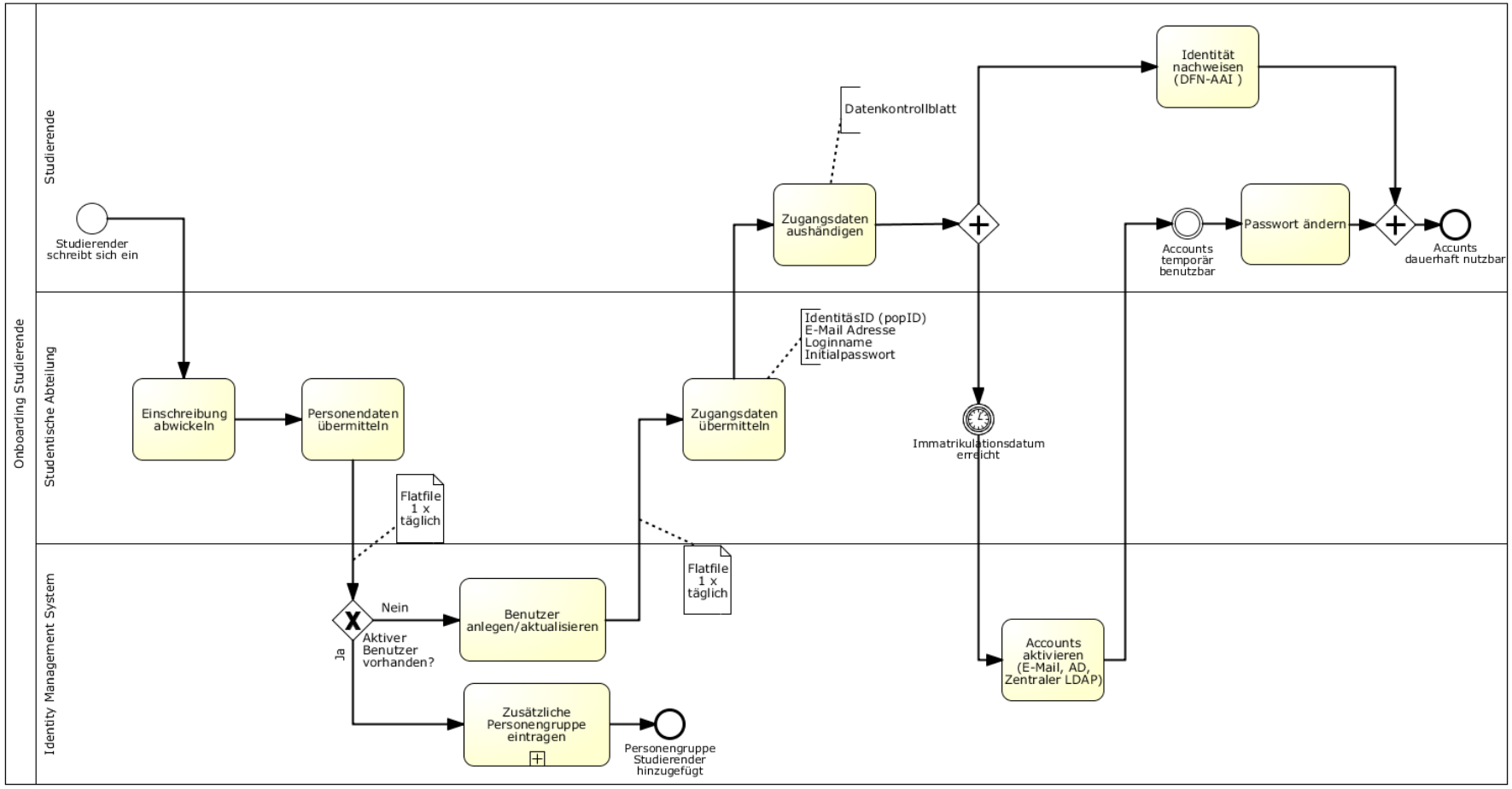
- Onboarding von Mitarbeitern, Studierenden und sonstigen Personen
- Account-Aktivierungs-Prozess
- Passwort Wiederherstellung
- Änderung der E-Mail-Adresse
- Offboarding von Mitarbeitern, Studierenden und sonstigen Personen
- ...

➢ Aufgrund unterschiedlicher Datenquellen sollen ähnliche Prozesse möglichst den gleichen Ablauf haben

Identity Management
Projekt - Prozesse(2)

Universität Konstanz

Onboarding Studierende



Identity Management Projekt - Schnittstellen(1)

Universität Konstanz

Vorwärts

- HIS-SOS → IDM
- HIS-SVA → IDM
- IDM → Active Directory
- IDM → E-Mail LDAP
- IDM → Zentraler LDAP

- (Libero → IDM)

Rückwärts

- IDM → HIS-SVA
- IDM → HIS-SOS

- (IDM → Libero)

Identity Management
Projekt - Schnittstellen(2)

Universität Konstanz

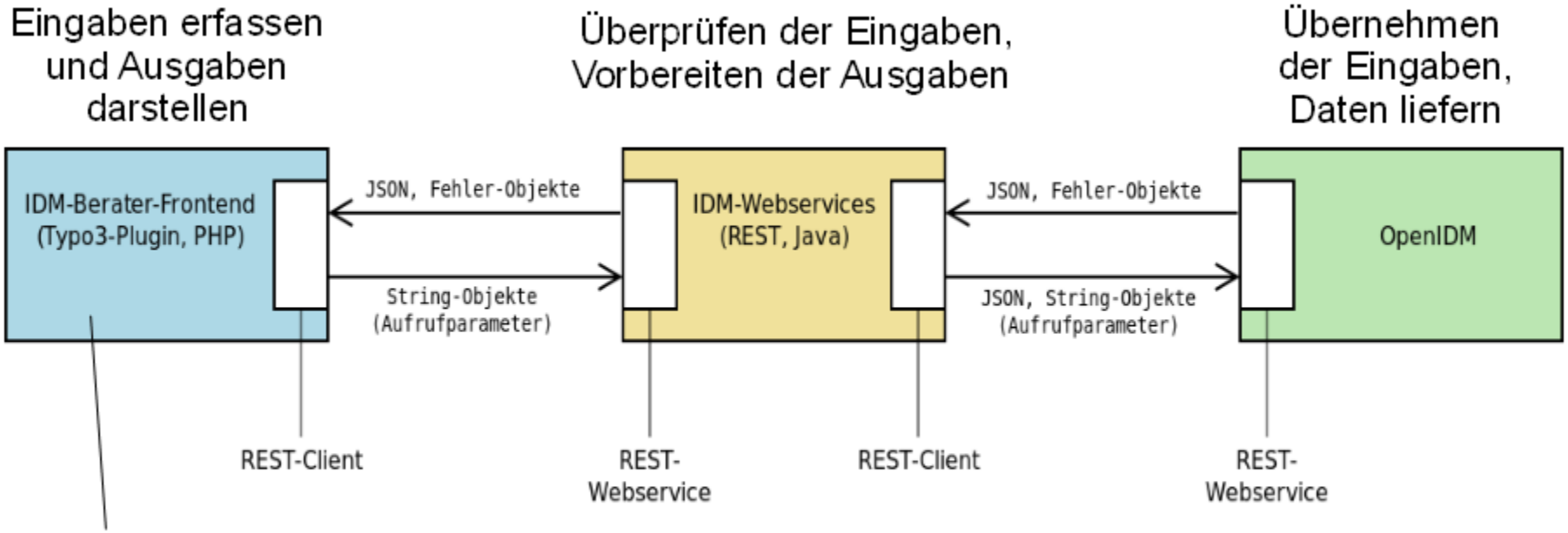
PERSONALNUMMER	BOM.Mitarbeiter.Personalnummer
VORNAMEN	BOM.Person.Vornamen
NACHNAME	BOM.Person.Nachname
TITEL	BOM.Person.Titel
GEBURTSNAMEN	BOM.Person.Geburtsnamen
GEBURTSDATUM	BOM.Person.Geburtsdatum
EINTRITTSDATUM	BOM.Mitarbeiter.Eintrittsdatum
AUSTRITTSDATUM	BOM.Mitarbeiter.Austrittsdatum
MITARBEITERKATEGORIE	BOM.Mitarbeiter.MitarbeiterKategorie
JURISTISCHEZUGEHOERIGKEIT	BOM.Mitarbeiter.Juristische Zugehörigkeit
PERSONENGRUPPE	BOM.Mitarbeiter.Personengruppe
BENUTZERGRUPPE	BOM.Mitarbeiter.Benutzergruppe

Universität Konstanz

BR0202_PasswortPolicy	Prüfen der Passwort-Policy • Mindestlänge: 8 Zeichen • Maximallänge: 15 Zeichen • Zulässige Zeichen: [A-Z], [a-z], [0-9] und zulässige Sonderzeichen • Zulässige Sonderzeichen: ! " # $ & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { } ~ • Nicht zulässige Sonderzeichen: | % und das Leerzeichen Grund: Probleme bei der Authentifizierung bei angeschlossenen Anwendungen z.B. ESEM, Fernleihe Zwei der vier nachfolgenden Regeln müssen erfüllt sein • Mindestens ein Grossbuchstabe ist enthalten • Mindestens eine Ziffer ist enthalten • Mindestens ein zulässiges Sonderzeichen ist enthalten • Es muss mindestens ein Kleinbuchstabe enthalten sei

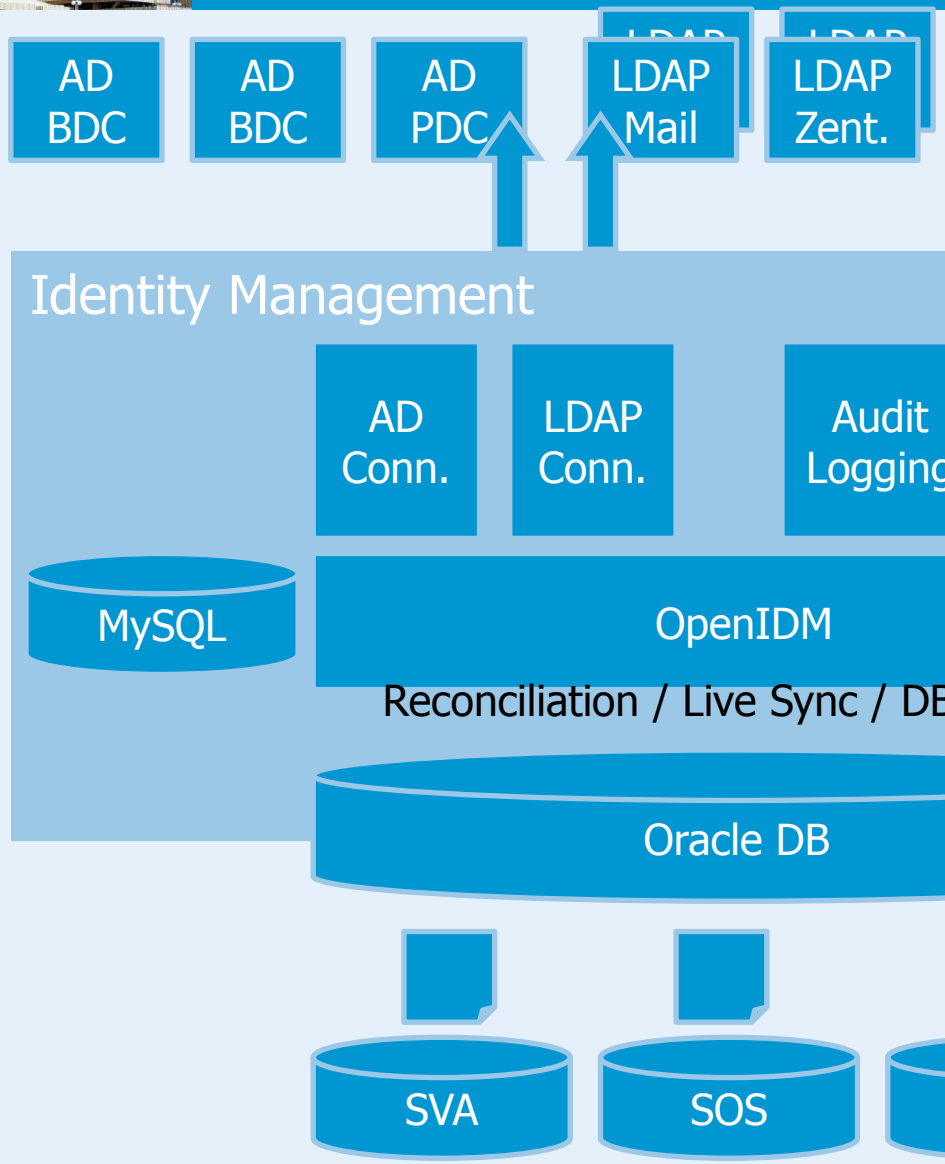
Identity Management
Projekt - Architektur - FrontEnd

Universität Konstanz



Identity Management
Projekt - Architektur - Gesamt

Universität Konstanz



Identity Management
Warum OpenIDM?

- OpenSource traditionell in universitären Umgebungen
- Offene Plattform
  - eigene Erweiterungsmöglichkeiten
  - Integration in bestehende Umgebung
- „Roter Faden“ in der Architektur erkennbar
- Know-How der Mitarbeiter vorhanden
- Kosten überschaubar
- Direkte Beratung durch Hersteller oder Partnerfirmen gegeben
- Austauschplattform mit Einfluss auf Entwicklung
- Erweiterungsmöglichkeiten
- …

Identity Management
Nächste Schritte

Universität Konstanz

- Ablösung des bestehenden Systems in 2013
- Auditierung
- Compliance, Verfahrensverzeichnis

- Integration von Workflows mit Acitiviti

- Föderatives Identity Management in Baden-Württemberg (bwIDM)

Vielen Dank

Universität Konstanz

Michael Längle

Leiter Informationsdienste
Universität Konstanz
☎+49 7531 88-3677
✉ Michael.Laengle@uni-konstanz.de

Andreas Schnell

Koordinator Serviceverbund KIM
Universität Konstanz
☎+49 7531 88-2804
✉ Andreas.Schnell@uni-konstanz.de