IAM im Rahmen des Open Source Identity Ecosystem

ZKI Verzeichnisdienste,
Augsburg 15.09.2017

Peter Gietz, DAASI International

DAASI International

Inhalt

IAM und Open Source Identity Ecosystem

- DAASI International und Open Source
- IAM und Open Source
- Das Open Source Identity Ecosystem

Beispiele der Interoperabilität

- midpoint
- didmos
- midpoint und LUI v1
- midpoint und LUI v2

Workflow mit midpoint

DAASI International

Über DAASI International

2000: Gründung in Tübingen mit 4 Mitarbeitern als Spin-Off des ZDV der Universität Tübingen aus DFN-Projekten zu X.500/LDAP heraus

2017: 19 Mitarbeiter, ca. 12 FTE,
knapp 1 Million Jahresumsatz

Weiter an Forschungsprojekten beteiligt zu:

- LDAP
- PKI
- Grid-Computing
- Virtuellen Forschungsinfrastrukturen (TextGrid)
- Digital Humanities (DARIAH-DE und DARIAH -EU)
- Föderiertes Identity Management (EU Projekt AARC)

DAASI International

Kernkompetenmzen

Identity & Access Management

- Verzeichnisdienste, Authentifizierungs- und Autorisierungsinfrastrukturen, Zugriffskontrolle, Single Sign-on, Provisionierung
- LDAP, PKI, SAML, SPML, RBAC, OAuth2, OIDC, SCIM,

Open-Source-Software

OpenLDAP, Shibboleth,

didmos, midPoint

Digital Humanities

- AAI, digitale Forschungsinfrastrukturen, Datenbankanwendungen in den Geisteswissenschaften

IAM und Open Source

- Da Identity Management ein großer Markt ist, gibt es einige kommerzielle Lösungen
  - NetIQ, IBM, (SUN), Oracle, etc.
  - hohe Lizenzgebühren (oft pro Eintrag berechnet)
  - trotzdem kein Produkt von der Stange
    - jede IT-Landschaft ist anders
    - es gibt nicht für jedes System fertige Konnektoren
    - es fallen also weitere Kosten für Implementierungsprojekt und Support an
  - Die Hauptprobleme sind organisatorischer Art und werden nicht durch Software gelöst
    - Compliance, Datenschutz, etc.
    - Alle Stake-Holder ins Boot nehmen!

DAASI International

Vorteile von Open Source

- Kosteneinsparung bei Lizenzen (nicht bei Projektkosten und Support)
- Kein Vendor Lock-in,
  - der Kunde hat eine wesentlich stärkere Position und muss nicht um Änderungen an Roadmaps betteln, sondern kann die Roadmap selbst definieren.
  - Wer den Source Code besitzt hat die Macht
- Sehr flexibel erweiter- und anpassbar, auch bei neuen Anforderungen
  - Durch Lieferanten, dem Kunden selbst oder durch einen dritten Dienstleister
- Bedient offene Standards, sodass verschiedene Komponenten zusammenpassen

DAASI International

Open Source Identity Ecosystem

- Ursprüngliche Idee stammt von Radovan Semancik von Evolvum
- Erste Aktivitäten 2015
  - Planung einer festen Organisationsstruktur geht nur langsam voran
  - Aber die Idee wird bereits in einer Vielzahl von Projekten gelebt
- Mitglieder, u.a.:
  - Evolveum (**midpoint, ConnId**)
  - DAASI International (**didmos**, midpoint, OpenLDAP, Shibboleth, ConnId)
  - Symas (**OpenLDAP**, **Apache Fortress,** midpoint)
  - Tirasa (**Apache Syncope, ConnId**)

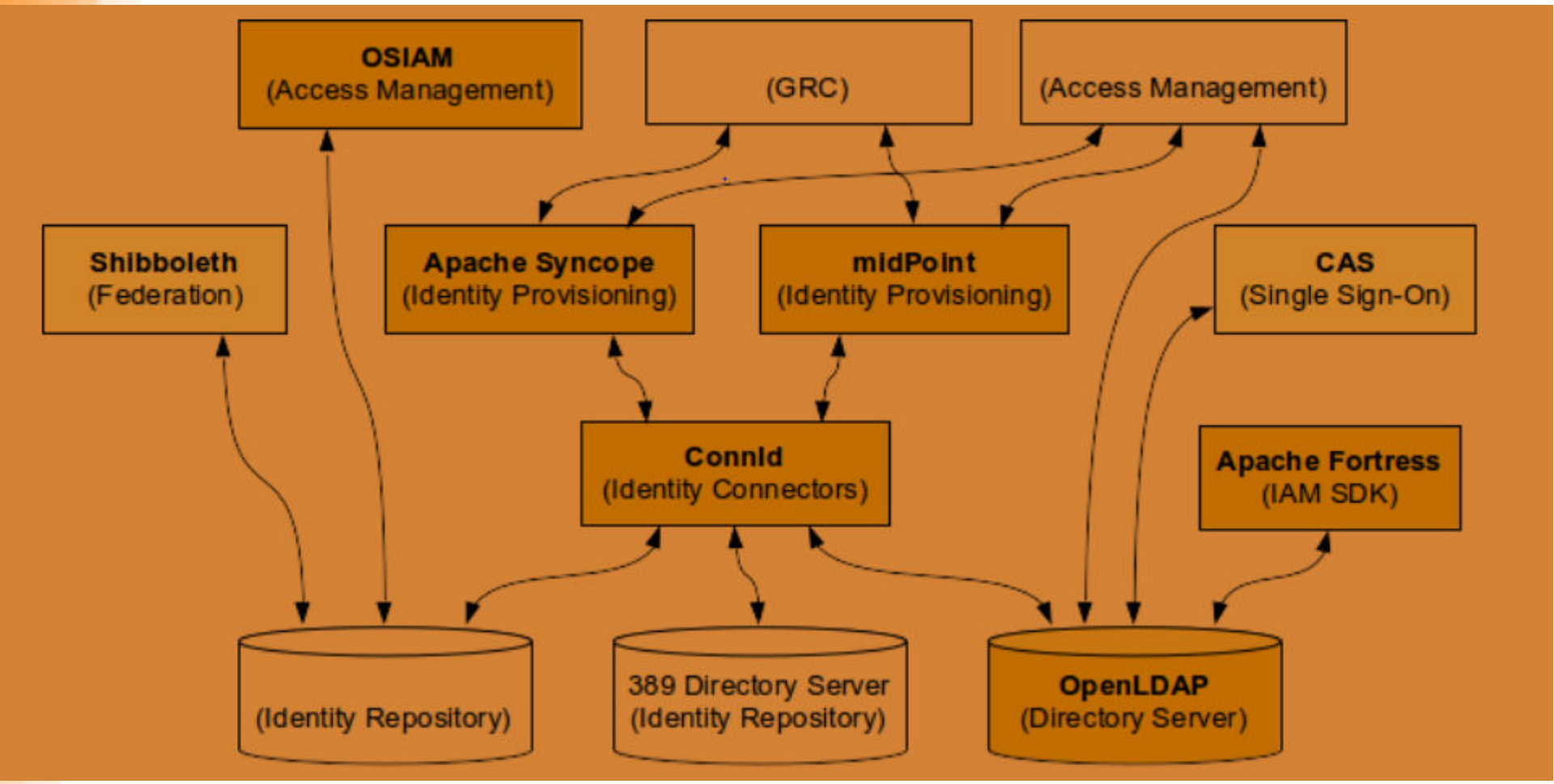
DAASI International

Open Source Identity Ecosystem

- Ziele:
  - Kooperation verschiedener Open Source-Anbieter und Integratoren
  - Interoperabilität der einzelnen Software-Komponenten
  - Vollständige Lösungen
  - Gemeinsames Marketing
- Vorteile für die Kunden:
  - Jeweils einen Ansprechpartner
  - Größere Nachhaltigkeit als die einzelnen kleinen Firmen
  - Besserer Support durch das Kollektiv

DAASI International

Open Source Identity Ecosystem



DAASI International und midPoint

- Wir haben für die Universität Wuppertal eine Studie zu verschiedenen Open-Source IdM-Produkten durchgeführt, bei der midPoint sich als für Hochschulanforderungen sehr geeignetes Produkt herausstellte
- Grundsätzlich empfehlen wir:
  - Bei sehr vielen Spezialanforderungen: didmos, welches sich als Framework sehr flexibel anpassen lässt.
  - Bei eher gängigen IdM-Projekten: midPoint, insbesondere, wenn ein fertiges Produkt gewünscht ist

DAASI International

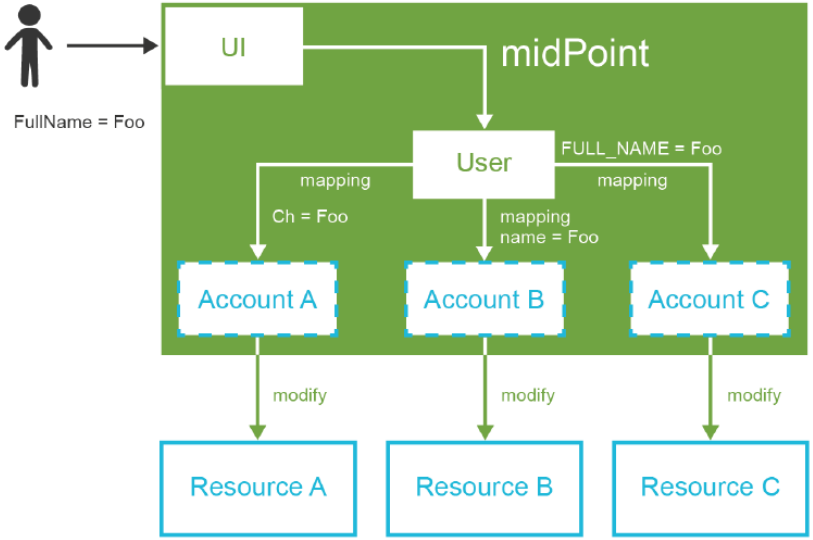
DAASI International und midPoint

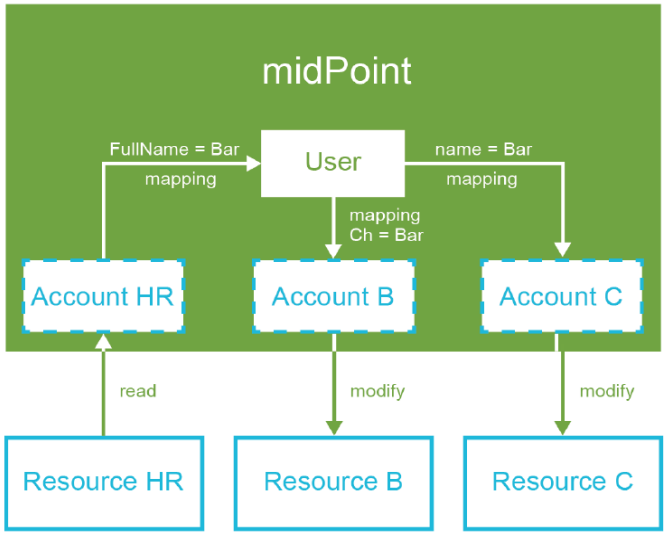
- Seit 2016 sind wir offizielle Vertretung von Evolveum in Deutschland
  - Wir verfügen über sehr gute Kontakte zur Geschäftsführung und zu den Entwicklern
  - Wir haben eine Reihe von PoC-Projekte mit midPoint durchgeführt.
  - Drei große Implementierungsprojekte sind in Vorbereitung
- DAASI Mitarbeiter und midPoint
  - Wir haben bereits drei MA in Bratislava schulen lassen
  - Weitere MA werden intern geschult
- Danach werden wir 3 midPoint Consultants, 1 MidPoint Entwickler und 1 MidPoint Administrator haben

DAASI International

IdM mit MidPoint

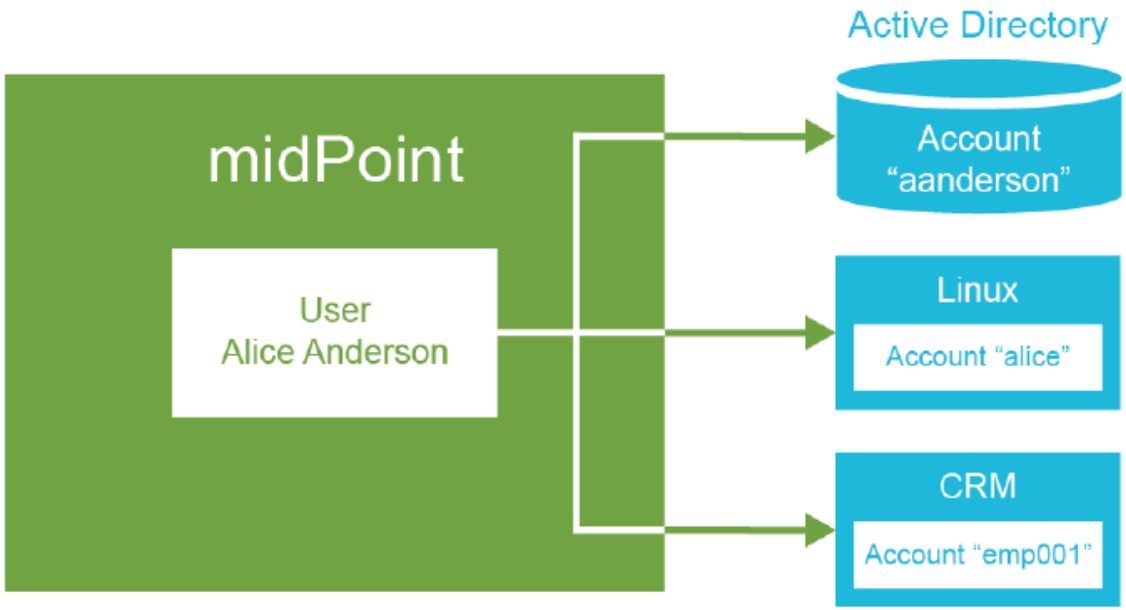
- Unidirektionale Verteilung von Parametern vs. automatische Provisionierung von Änderungen am externen System
- manuelle Eingaben durch attribut-mapping minimieren





IdM mit MidPoint

- Userobjekte mit Zugriff auf externe Accounts
- Zielattribute nicht zwingend homogen



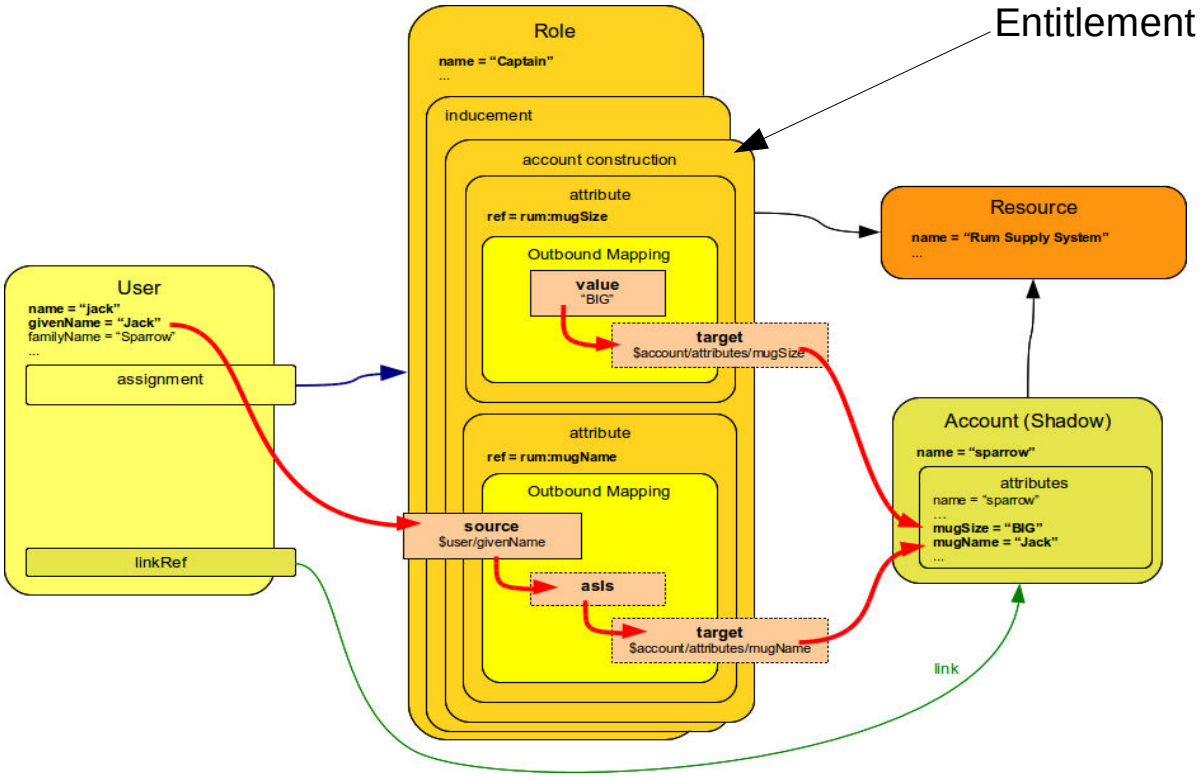
IdM mit MidPoint

- „Assignments“ binden die inhomogenen Attribute einer Ressource (Account) an einen MidPoint-User (→Projections)
- Um eine Policy (→ SOLL) zu erfüllen sind viele manuelle Assignments (→ IST) anzuwenden
- „Rollen“
  - vereinen mehrere Attribute und Assignments
  - bilden Policies ab
  - Können beantragt oder zugewiesen werden
  - werden Nutzern statt Berechtigungen zugewiesen
  - modularer Aufbau für beliebige Kombinationen möglich
  - Durch Skripte individuell erweiterbar
  - Können zeitgesteuert zugewiesen werden

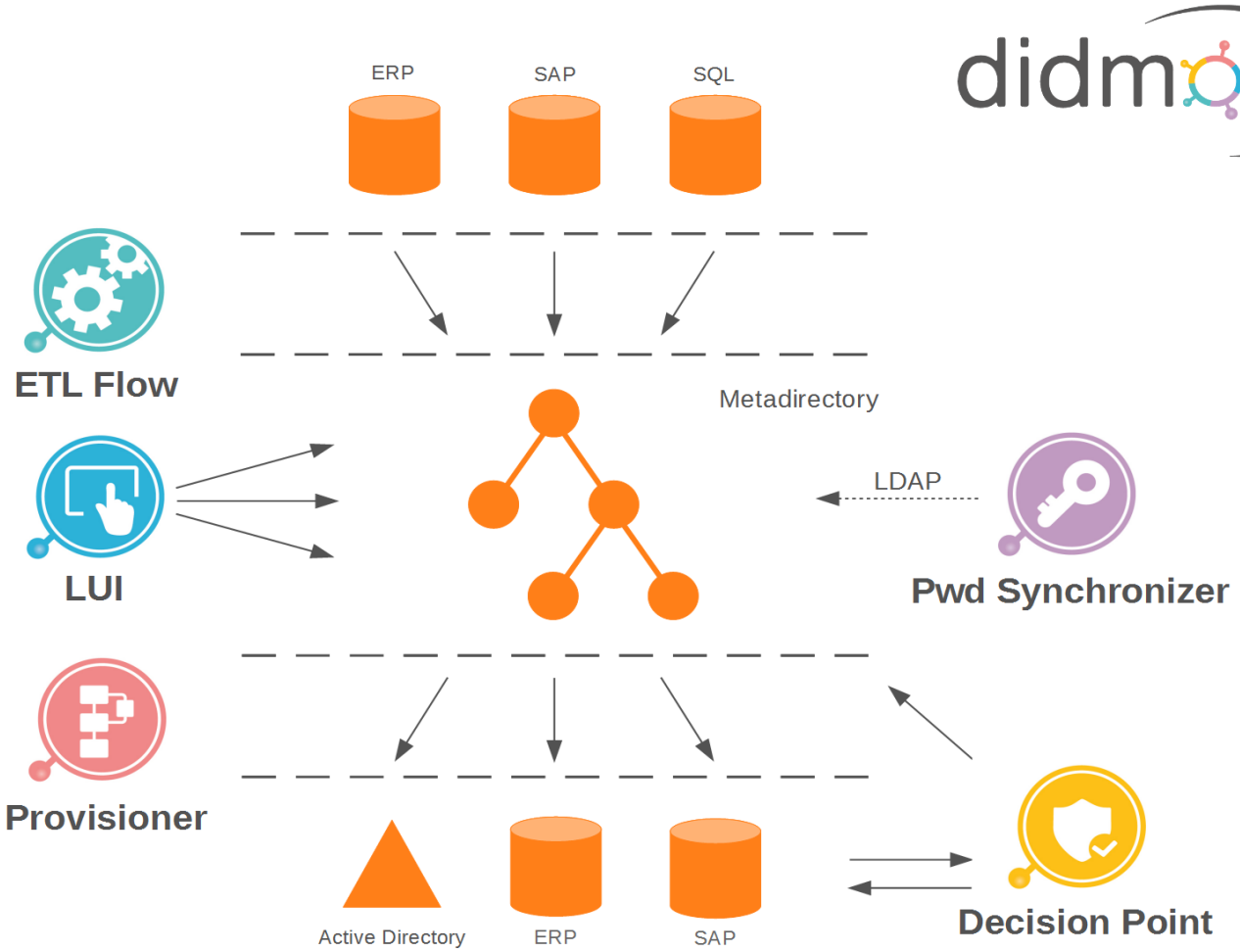
DAASI International

IdM mit MidPoint

- Berechtigungsstrukturen – „Entitlements“ bleiben Ressourcenobjekte (extern)
- Ressource-Shema-Handling und Attribut-Mapping(intern) für die direkte Synchronisation



didmos 1.0


didmos
ERP
SAP
SQL
ETL Flow
Metadirectory
LUI
LDAP
Pwd Synchronizer
Provisioner
Active Directory
ERP
SAP
Decision Point

didmos LUI 1.0

LUI

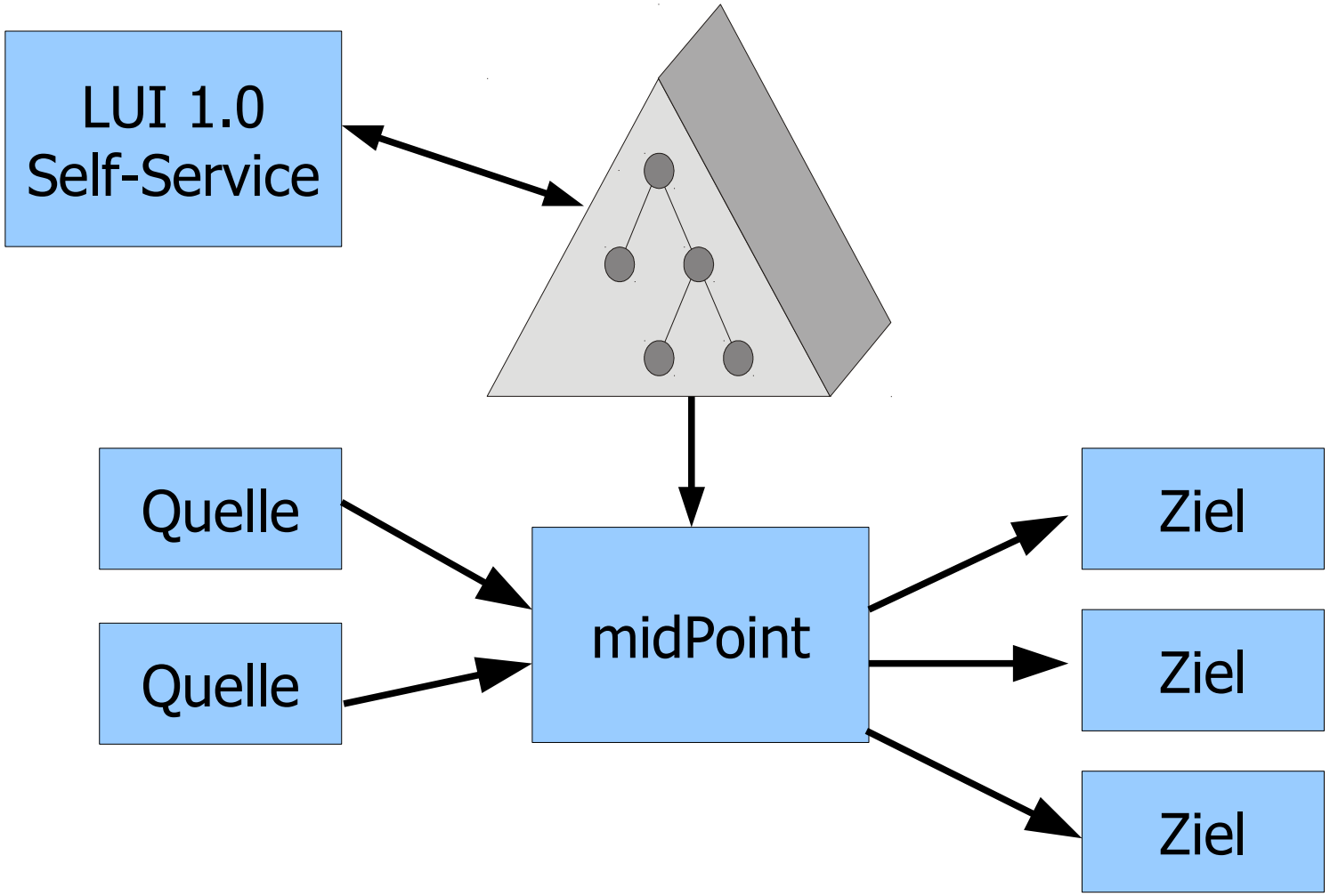
- **L**DAP **U**ser **I**nterface

- Generisches Web-Portal-Framework für
  - Administrative Prozesse
  - Self-Service-Funktionalität

didmos LUI 1.0

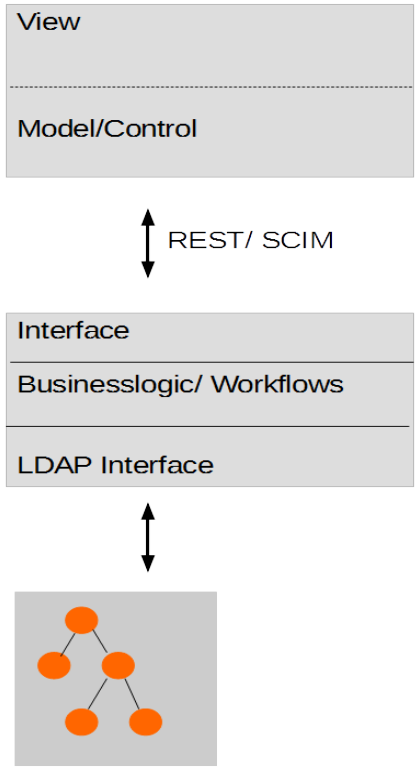
- Anpassbarer Aufbau durch hochgradige Konfigurierbarkeit und Templates
- LDAP-Spezialisierung durch Formulare zur Manipulation von LDAP-Objekten
- Rechtevergabe, rollen- oder gruppenbasiert, für beliebige Funktionalität
- Prüfen von eingegebenen Werten durch konfigurierte reguläre Ausdrücke oder kundenspezifische Funktionen
- Konfiguration von auszuführenden Funktionen über Plugin-Schnittstellen, z.B. beim Speichern oder Laden von Attributwerten, beim Löschen von Einträgen, ...

Integration midPoint mit didmos LUI 1.0

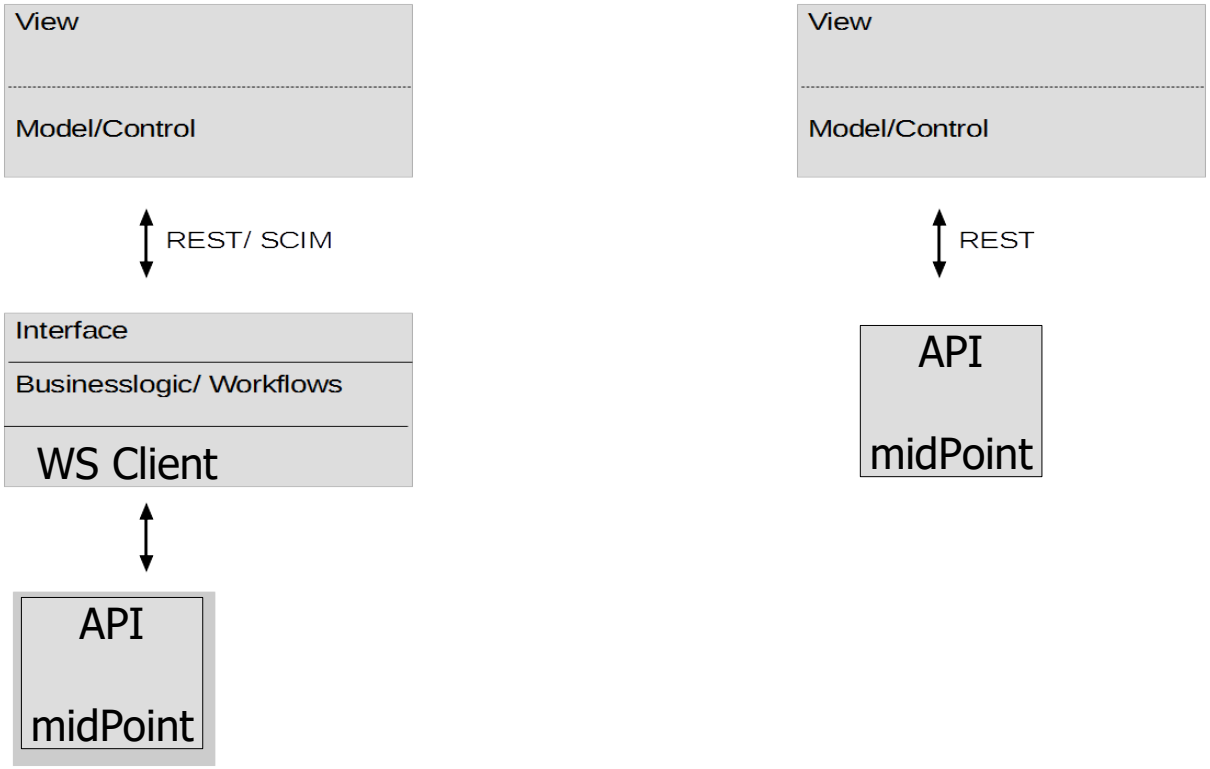


DAASI International

didmos LUI 2.0 Architektur



didmos LUI 2.0 und midPoint



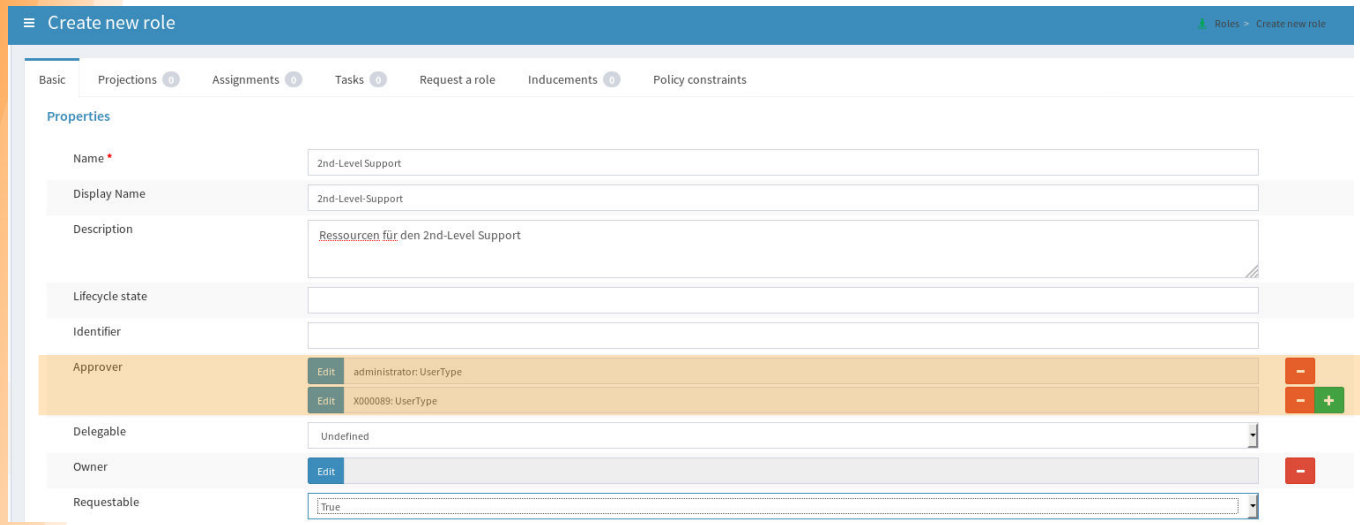
Workflow mit MidPoint

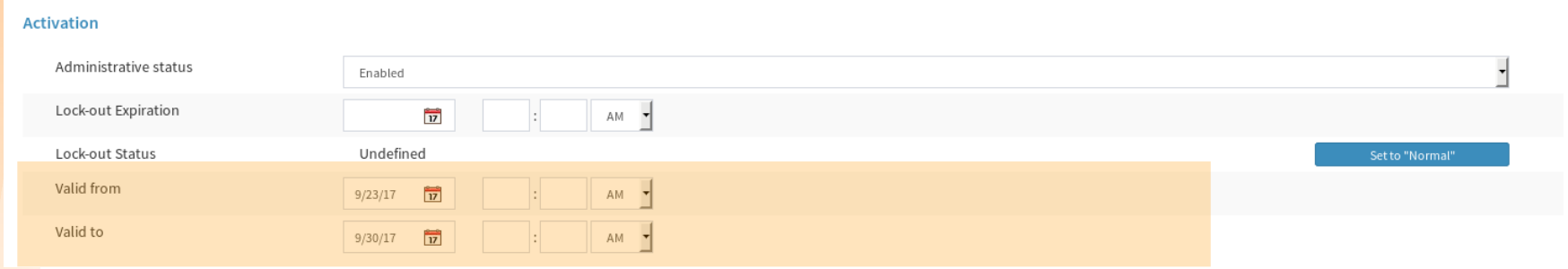
- Die Workflowengine von midPoint verwendet activiti und unterstützt BPMN
- Augenblicklich wird dies noch weiter generalisiert, sodass zukünftig auch andere Workflow-Engines und proprietäte WorkFlows möglich sein könnten
- Intensiv wird an einer Shopping-Cart Oberfläche gearbeitet

DAASI International

Policy-Workflow mit MidPoint

Rolle anlegen



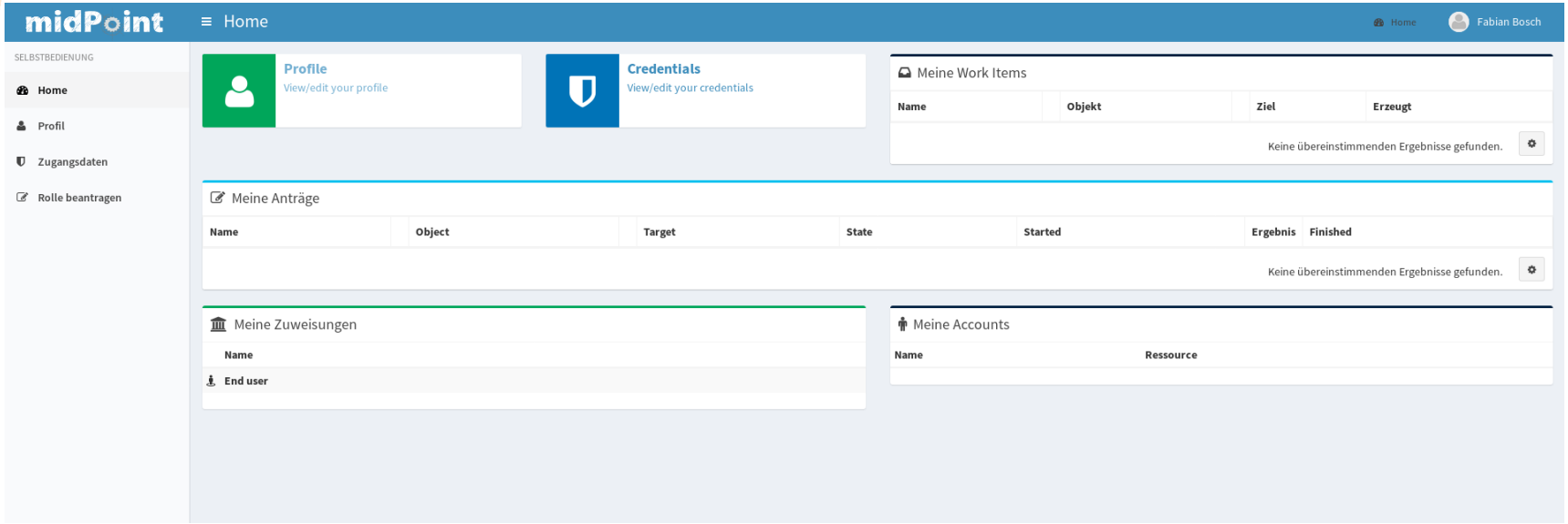


- Angabe von „Approver" und Gültigkeitszeitraum
- beide müssen Rollenbeitritt zustimmen

Policy-Workflow mit MidPoint

EndUser Selfservice

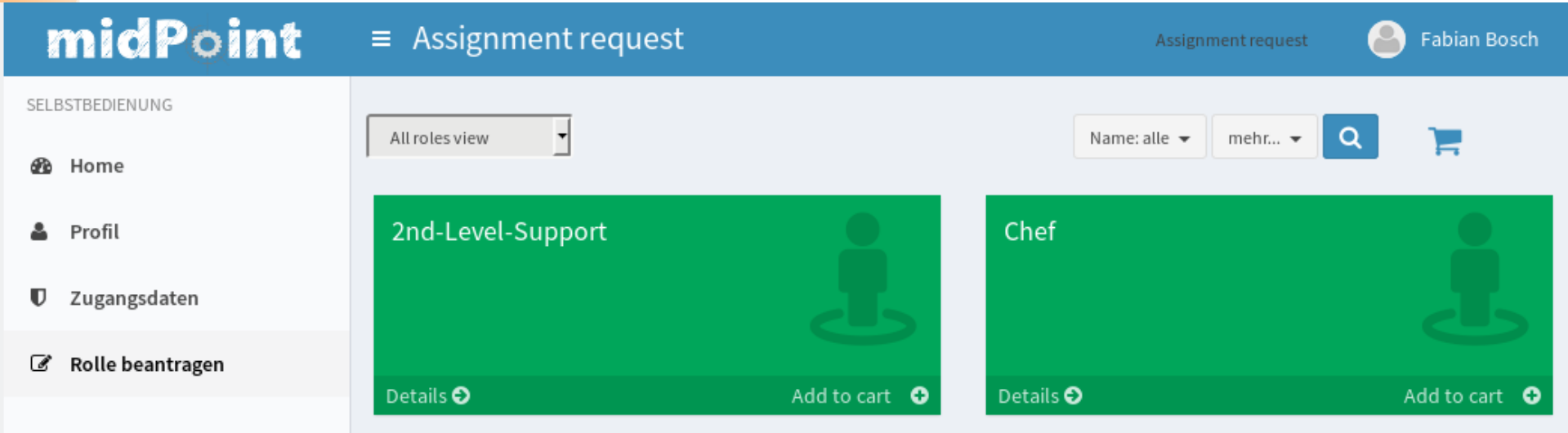
- Persönliche Daten ändern
- Rollen beantragen



Policy-Workflow mit MidPoint

Rollen beantragen - „Shopping Cart“- Modell

- Auswahl der Rollen, die „Requestable“ sind
- Alle Assignments der Rolle werden dem Nutzer übertragen.



Vielen Dank für Ihre Aufmerksamkeit.

DAASI International

www.daasi.de

Telefon: 07071 4071090

E-Mail: info@daasi.de

Schaubilder: Evolveum