ZKI Verzeichnisdienste
05. März 2013 in Rostock

Andreas Eibisch
Technische Universität Dresden
Projektgruppe DoIT

Anja Soisson
Universität Leipzig
Projekt AlmaWeb

Agenda

1. IDM-Kooperation in Sachsen
   (Anja Soisson)
2. Umsetzungsstand an der Technischen Universität Dresden
   (Andreas Eibisch)
3. Die besondere Dynamik in IDM-Einführungsprojekten
   (Andreas Eibisch)
4. Umsetzungsstand an der Universität Leipzig
   (Anja Soisson)
5. IDM-Einführung im Kontext weiterer Software-Großprojekte
   (Anja Soisson)

1. Die IDM-Kooperation in Sachsen

- Start 2010 nach ZKI – Herbsttagung
- 2011 gemeinsame Ausarbeitung eines Anforderungskatalogs und darauffolgende gemeinsame Ausschreibung
- Kooperationsvertrag zwischen der Technischen Universität Dresden *(TUD)* und Universität Leipzig *(UL)*
- Rahmenvereinbarung für alle Hochschulen Sachsens (145.000 Identitäten)
- Manifestieren der Kooperation auch in den Verträgen mit dem Anbieter
- TUD: Start im November 2011
- UL: Start im April 2012

- Konzepte und Datenmodell der TU Dresden konnten zu großen Teilen in Leipzig wieder verwendet werden
- 2012/13 gab es etliche Abstimmungstermine mit der Hochschule Zittau Görlitz und HTWK
- Treffen im Dezember 2012 in Leipzig gemeinsam mit HS Osnabrück und TU Darmstadt
- Anfang 2013 ist die HTWK Leipzig der Kooperation beigetreten
- Hochschule Zittau/Görlitz in Vorbereitung
- TU Freiberg hat Interesse bekundet, aber noch keinen konkreten Starttermin

Vorteile:

- Unkomplizierte Abstimmung auf dem „kleinen Dienstweg“
- Guter Erfahrungsaustausch „Lessons Learned“: UL lernt von TUD, HTWK von UL u.s.w.
- Hilfreiche Hinweise zum konkreten Umgang mit dem Berater
- TUD und UL setzen Datenlotsenlösung CampusNet und IDM ein -> großer Erfahrungsschatz, aber auch bessere Verhandlungsposition bei konkreten Problemen
- Lose Kooperation mit TU Darmstadt und HS Osnabrück in 2012 hinzugekommen

Grenzen:

- Wiederverwendbarkeit von Konzepten und Entwicklungen begrenzt, da die Unterschiede in den Prozessen bisweilen recht grundlegend
- Noch keine Entwicklungsprojekte entstanden
- Organisatorische Fragestellungen muss jede Hochschule für sich klären
- Beraterverfügbarkeit sinkt mit der Anzahl der parallellaufenden Projekte

2. Umsetzungsstand an der Technischen Universität Dresden

IDM an der TUD – Was bisher geschah

2008 Beginn der Projektgruppe DoIT
- Arbeiten in den Bereichen ERP, SLM und IDM

2009 Start des Projektes IDM
- Ausrichtung zunächst auf Eigenentwicklung

Vortrag auf der Herbsttagung 2009

2010 Änderung der Grundausrichtung (kaufen statt bauen)
Vorbereitung eines Beschaffungsverfahrens

2011 Kooperationsvertrag mit der Universität Leipzig
Durchführung des Beschaffungsverfahrens
Start des IDM-Einführungsprojektes
- Technische Basis der Lösung: Novell Identity Manager
- Unterstützung bei Umsetzung: Maintainet AG

2012 Durchführung des IDM-Einführungsprojektes
Start der TU-weiten Nutzermanagementkonsolidierung

IDM an der TUD – Die Ausgangsposition

DUMAS – **D**resdner **U**ser **M**anagement and **A**ccounting **S**ystem

- Eigenentwicklung des ZIH
  - MySQL
  - PHP
- Betrieb durch das ZIH
  - verwaltet werden Accounts und keine Identitäten
  - vereint Benutzerverwaltung und Projektverwaltung für Hochleistungsrechner

Quellsysteme:

- Identitätsführenden Systeme der Verwaltung
- HIS SOS, HIS SVA, SAP HR

Zielsysteme:

- Basisdienste des ZIH
- Mail, Hochleistungsrechner, PC-Poolverwaltung, …

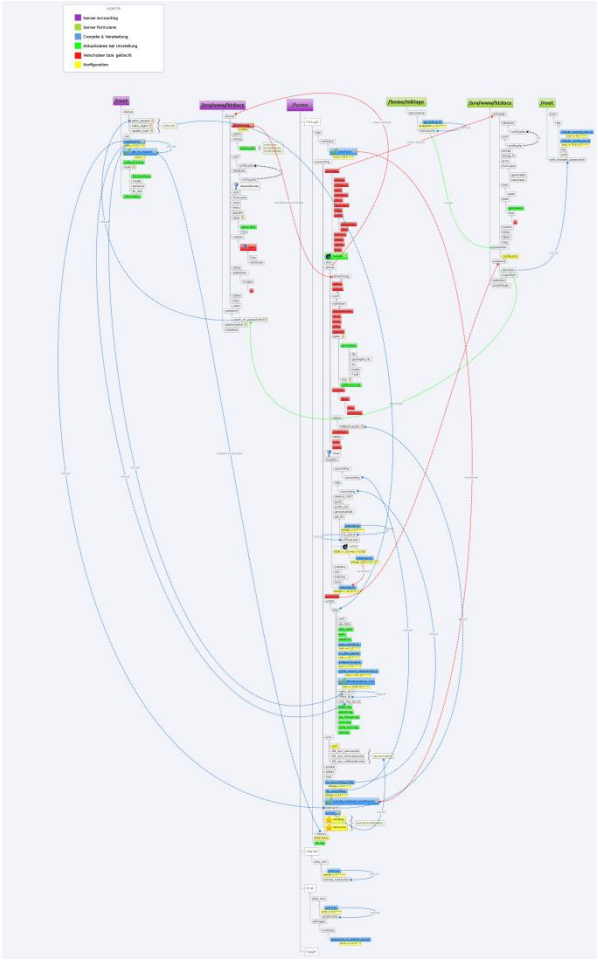
IDM an der TUD – Die Ausgangsposition

Das bestehende System DUMAS ist hochkomplex
- Datenmodell ist auf A3 gerade noch lesbar
- Funktionalität ist auf über 200 Skripte verteilt

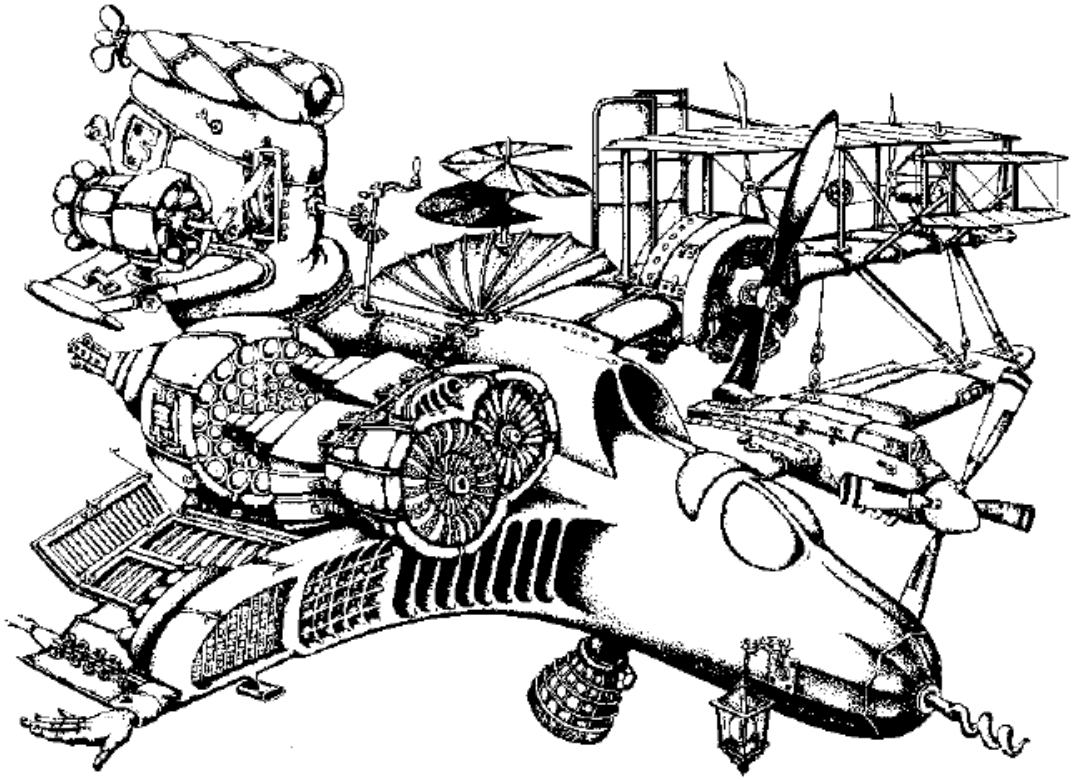
Wartbarkeit ist nicht mehr gewährleistet
- gewachsene Abhängigkeiten ungenügend dokumentiert
- Entwickler mit neuen Projekten ausgelastet

Anforderungen an das System wachsen:
- Umsetzung eines identitätsbasierenden Ansatzes mit einem persönlichen Login pro Benutzer
- Forderung nach einer TU-weiten Konsolidierung
- Trennung von Benutzer- und Projektverwaltung
- Schaffung einer LDAP-Schnittstelle

→ Entscheidung für Ablösung von DUMAS



IDM an der TUD – Das Vorhaben



Ersetzen von wesentlichen Bestandteilen durch
eine zentrale Komponente während des Fluges

IDM an der TUD – Das Einführungsprojekt

Umfang des Einführungsprojekts

- Aufbau der neuen IDM-Lösung
- Bereitstellung des zentralen LDAP-Verzeichnisdienstes
- Migration der aktuellen Benutzerverwaltung DUMAS in die neue IDM-Lösung
- Anbindung der Quell- und Zielsysteme der bestehenden Benutzerverwaltung

Ziel des Einführungsprojektes:

- Ablösung und Abschaltung der bestehenden Benutzerverwaltung DUMAS

Entscheidung für Umsetzung:

- Big Bang statt teilweisem Parallelbetrieb mit gleitendem Übergang

IDM an der TUD – Die Herausforderungen

Umgang mit mehreren Bestandslogins pro Identität

- beide Logins der Identitäten waren potentiell in Benutzung → Löschen nicht möglich
- über 1000 betroffene Identitäten → Einzelfallentscheidungen nicht möglich

- Abweichung von der Zielstellung eines persönlichen Logins pro Identität
  - alle persönlichen Logins bleiben erhalten und werden in das IDM migriert
  - pro Identität wird nur ein persönliches Login in den Ordner „active“ migriert
  - die weiteren Logins werden als Altlasten in den Ordner „active_old“ migriert
  - Zusammenführung der Logins auf Antrag möglich

Migration der Passwörter

- Bei der Migration der Benutzerkonten wird das Passwort einmalig im Klartext benötigt
- Das Passwort liegt in der bestehenden Benutzerverwaltung aber nicht im Klartext vor

- Aktivierung der migrierten Benutzerkonten durch Passwortbestätigung durch Benutzer
  - bei Bestätigung erfolgt Prüfung gegen DUMAS und Eintragung ins IDM
  - neue Zielsysteme können erst nach der Passwortbestätigung genutzt werden

IDM an der TUD – Der aktuelle Stand

- Start des Produktivbetriebs am 10. Dezember 2012
  - nach mehrmaliger Verschiebung
  - mit größerem Umfang als ursprünglich geplant

- Anbindung von 3 Quellsystemen
  - HIS SOS – Studierendenverwaltung der ZUV
  - HIS SVA – Personalverwaltung der ZUV
  - SAP HR – Personalverwaltung des Universitätsklinikums

- Integration der Gästeverwaltung in das IDM

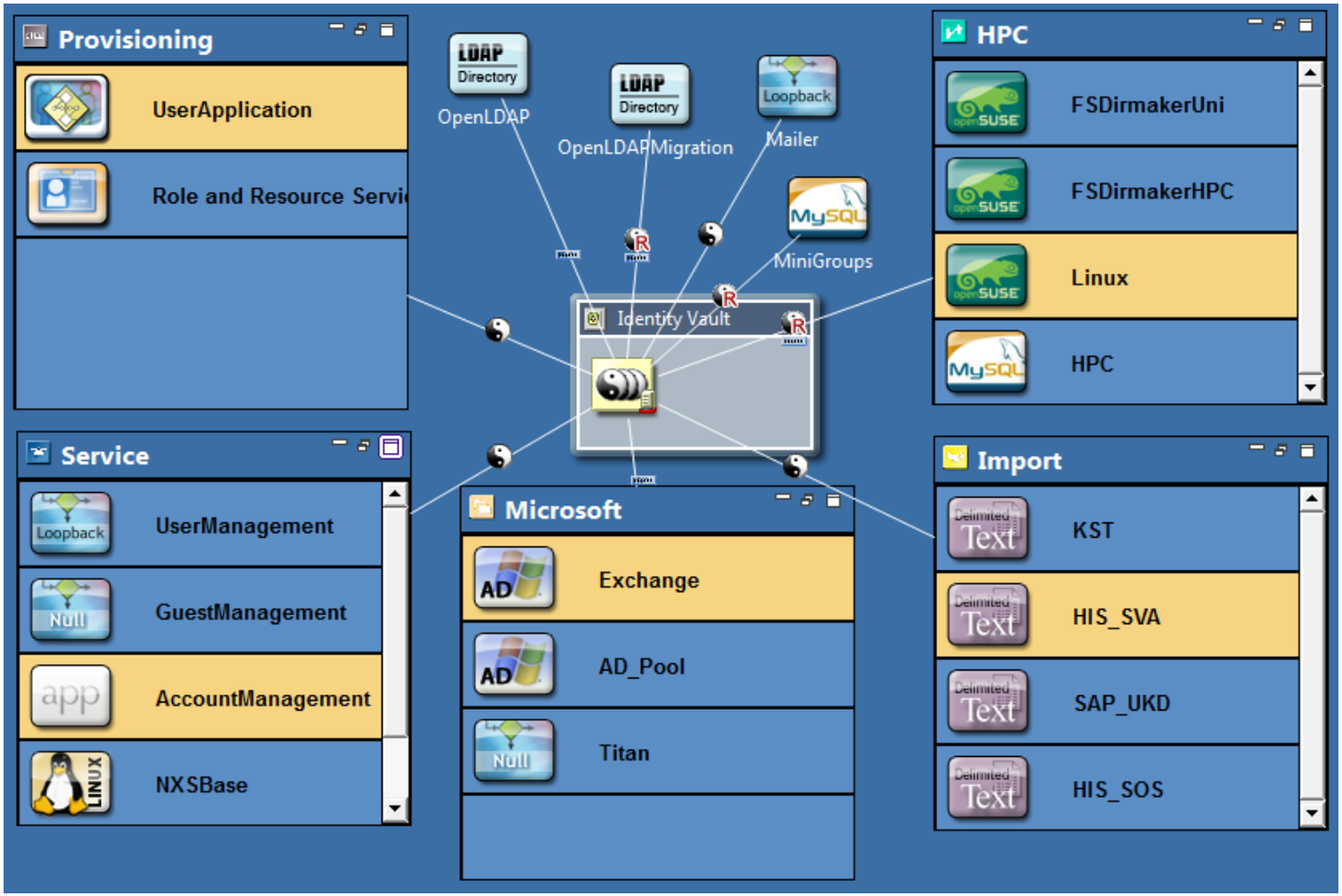
- Anbindung von 47 Servern in 35 Zielsystemen
  - davon 14 Systeme direkt
  - davon 21 Systeme über OpenLDAP

IDM an der TUD – Der aktuelle Stand

- Migrierte Nutzer und Konten
  - Aktive 52.000
  - Aktive Altlasten 1.000
  - Gäste 6.800
  - Inaktive 9.000
  - Blocked 60.000

- bisher haben mehr als 50% der Benutzer ihr Passwort bestätigt

IDM an der TUD – Der aktuelle Stand



IDM an der TUD – Weitere Ergebnis

- Schaffung rechtlicher Grundlagen für den IT-Betrieb
  - Erstellung der Ordnung zum Betrieb des IDM-Systems
    → datenschutzrechtliche Grundlage
  - Neufassung der IuK-Rahmenordnung
    → Festlegung allgemeiner Benutzungsregeln
    → Definition des IT-Sicherheitsmanagements

} Vortrag auf der Herbsttagung 2010

- Dokumentation und Kanalisierung der Datenflüsse
  - Zielsysteme müssen vor Anbindung an das IDM Sicherheitsstandards nachweisen
    → Verfahrensverzeichnis und Sicherheitskonzept vorlegen
    → Ansprechpartner dafür ist die Stabsstelle für Informationssicherheit
  - Durch Ablösung von HIS SOS und HIS SVA versiegen „alternative“ Bezugsquellen
    → Das IDM ist Katalysator für eine TU-weite Dokumentation der IT-Sicherheit
    → Dokumentation erfolgt mit der Anwendung „Verinice“ des Anbieters „Sernet“

IDM an der TUD – Was noch zu tun ist

- Abschluss der Migrationsphase
  - Frist für die Passwortbestätigung läuft am 15. April 2013 ab
  - Anschließend werden alle noch nicht bestätigten Benutzerkonten gesperrt
- Weitere Konsolidierung der Benutzerverwaltungen der TU Dresden
- Anbindung der neuen Systeme für ERP und SLM
  - SAP als Quellsystem für Personaldaten und neues Zielsystem
  - CampusNet als Quellsystem für Studierendendaten und neues Zielsystem
- Implementierung des Rollenmodells
  - Aus den Projekten ERP und SLM entstanden

} Vortrag auf der Frühjahrstagung 2012

3. Die besondere Dynamik von IDM-Einführungsprojekten

Hohe Komplexität

technisch
- sehr breites Spektrum an angeschlossenen Systeme
- sehr hohe Sicherheitsanforderungen insbesondere an Verfügbarkeit und Vertraulichkeit
  →sehr breites und tiefes technisches Know-How erforderlich

organisatorisch
- sehr viele Prozesse sind betroffen
- breites Spektrum an Stakeholdern mit unterschiedlichsten Motiven und Vorbehalten
  → breiter Einflussbereich bringt gewaltige Abstimmungsaufwände mit sich

rechtlich
- datenschutzrechtliche Belange
- Stichwort Compliance
  → rechtliche Rahmenbedingungen erhöhen die Komplexität zusätzlich

Hohe Komplexität

Großer Kommunikationsaufwand
- bindet wichtige Ressourcen
- erfordert große Durchschlagskraft des Projektes

Tendenziell lange Vorbereitungs- und Konzeptionsphase
- verstärkt die klassischen Probleme eines Wasserfallvorgehens
    - ersten Erfolge werden erst recht spät sichtbar
    - einige Konzepte bei Umsetzung bereits veraltet

Vorhandensein unendlich vieler Lösungsmöglichkeiten
- Die Wahl zu haben ist immer besser, aber:
    - klare Strategie notwendig → Konzepte nach ITIL einsetzen!
    - hohe Kompromissbereitschaft notwendig → auch beste Lösung ist Kompromiss!

Hohe Erwartungshaltung

© WhichBox Media

Hohe Erwartungshaltung

Erwartungen → visionär

- Lösung aller organisatorischen Probleme durch Technik
- Automatisierung aller Ausnahmen ☺

Umsetzung → pragmatisch

- nicht alles lässt sich sofort umsetzen
- nicht alles lässt sich überhaupt umsetzen
- ein wissenschaftlicher Ansatz wird zur Kostenfalle

Risiko Projektumfang

Ursachen
- Hohe Komplexität
- Hohe Erwartungshaltung

Folgen
- Vielzahl unterschiedlichster Anforderungen
- Schnell wachsende Zahl von Anforderungen
  - durch während der Projektlaufzeit hinzukommende Systeme
  - durch Zwischenergebnisse geweckte Wünsche

→ Dynamik in den Anforderungen positiv

Risiko
- zu großer Projektumfang des Einführungsprojektes
- während der Projektlaufzeit wachsender Umfang

→ Dynamik in den Projektzielen negativ

Gelernte Lektionen

- Iteratives Vorgehen wählen
  - Zwischenergebnisse erleichtern die Kommunikation enorm
  - Risiko von Fehlentwicklungen wird minimiert
- Initialen Umfang des Einführungsprojektes minimieren
  - Umfang mit jeder Iteration hinterfragen
  - Ziele konsequent priorisieren
- Dokumentation, Kommunikation und Entscheidungsfindung formalisieren
  - kurze Dienstwege funktionieren in diesem Rahmen nicht
  - Querverweis ITIL
- Personalmanagement
  - Ziel Schaffung von Nachhaltigkeit
- Raumsituation
  - Ziel Optimierung der Kommunikation

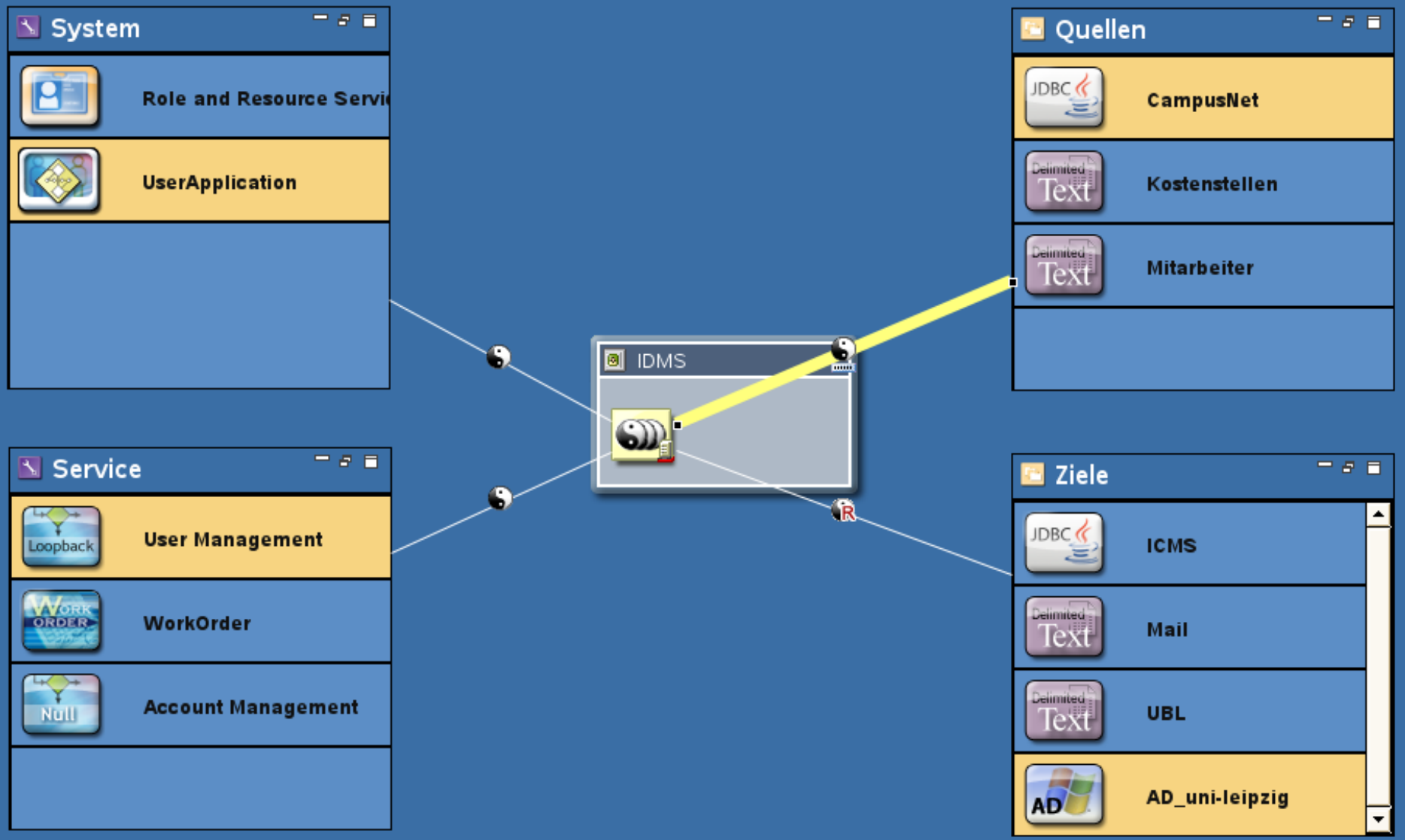
4. Umsetzungsstand an der Universität Leipzig

- Anbindung von 3 Quellen:
  - Studierende aus CampusNet
  - Mitarbeiter aus HIS SVA
  - Kostenstellen ursprünglich aus HIS COP, jedoch manuell nachgearbeitet, damit diese eine Organisationsstruktur ergeben

- Gäste werden über eine Gastverwaltung direkt ins IDM erfasst

- Anbindung von 4 Zielen:
  - zentraler Verzeichnisdienst: Active Directory
  - E-Mail-Server
  - Universitätsbibliothek
  - InterCardManagementSystem für die Erstellung der UniCard

→ alle Treiber sind erstellt, Test der Anwendungsfälle hat begonnen, besonderer Fokus auf Integrationstests


System
Role and Resource Servi
UserApplication
Service
Loopback
User Management
WorkOrder
Account Management
Null
IDMS
R
Quellen
JDBC
CampusNet
Delimited Text
Kostenstellen
Delimited Text
Mitarbeiter
Ziele
JDBC
ICMS
Delimited Text
Mail
Delimited Text
UBL
AD
AD_uni-leipzig

5. IDM-Einführung im Kontext weiterer Software-Großprojekte

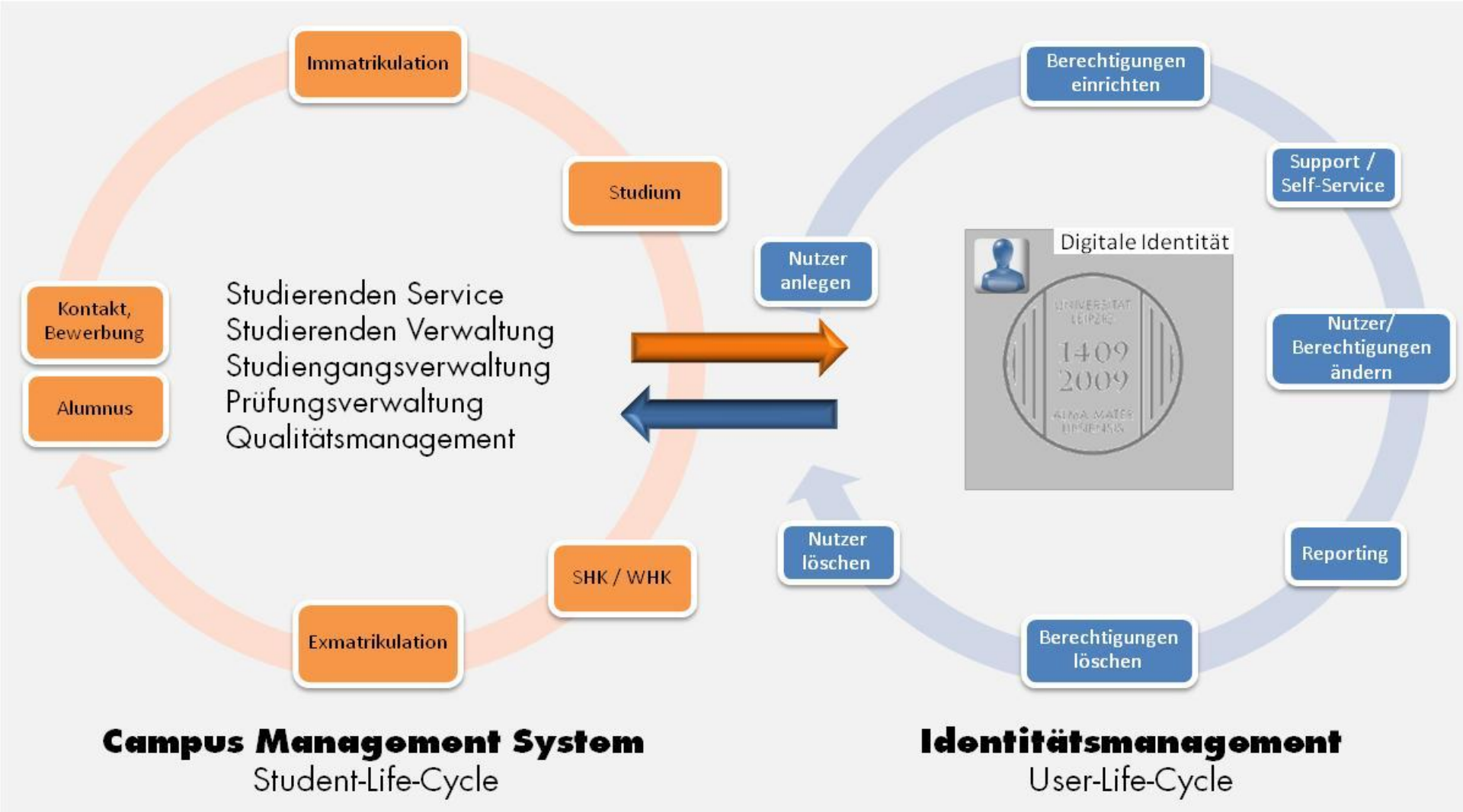
- Projekt EVI: Neue Hochschulsteuerung
  seit Q1/2010
  Fachliche Verantwortung: Dezernat Haushalts- und Wirtschaftsangelegenheiten

- Projekt AlmaWeb: Studierenden-Lifecycle-Management
  seit Q1/2010
  Fachliche Verantwortung: Dezernat Akademische Verwaltung

- Projekt Identitätsmanagement
  seit Q2/2012
  Fachliche Verantwortung: Universitätsrechenzentrum

- Verzahnung AlmaWeb – EVI
  über Reportingschnittstelle

- Verzahnung AlmaWeb – Identitätsmanagement
  über Identitäten – für Accounts
  über Studiendaten – für Shibboleth und UniCard


Immatrikulation
Studium
Kontakt, Bewerbung
Alumnus
Studierenden Service
Studierenden Verwaltung
Studiengangsverwaltung
Prüfungsverwaltung
Qualitätsmanagement
SHK / WHK
Exmatrikulation
Nutzer anlegen
Nutzer löschen
Digitale Identität
Berechtigungen einrichten
Support / Self-Service
Nutzer/ Berechtigungen ändern
Reporting
Berechtigungen löschen
Campus Management System
Student-Life-Cycle
Identitätsmanagement
User-Life-Cycle

Gegenseitige Beeinflussung der Projekte AlmaWeb und IDM

- Konfiguration von CampusNet wirkt sich sowohl auf Attribute als auch auf Prozesse in IDM aus
  - Z.B. Akteurtypen für unterschiedliche Studentenarten wirken unterschiedlich auf Berechtigungen
  - Klärung muss bilateral erfolgen, CampusNet muss die IDM Belange berücksichtigen und IDM die Belange von CampusNet
  - -> Abstimmungen mitunter langwierig und komplex

- Viele wesentliche Änderungen in CampusNet haben Nachwirkungen im IDM (z.B. Eventsteuerung)

- Go-Live-Verschiebung AlmaWeb wirkt sich auf Arbeitspakete IDM aus

- Verschwimmen der Projektgrenzen, IDM wird nicht als eigenständige Aufgabe wahrgenommen

Vorteile:

- Konzeptionen sind umfassender und zukunftsfähig
- tragfähige Architekturen entstehen
- Projektoverhead geringer, da Strukturen gemeinsam genutzt werden können, z.B. Controlling, Kommunikation, Projektleitung
- Erspart aufwändige Zwischenlösungen
- Verkürzt die Gesamtprojektzeit, verlängert allerdings die Einzellaufzeiten geringfügig

Nachteile:

- Höherer Abstimmungsaufwand
- Doppelbelastung der KeyPlayer
- Steigert das Risiko des Scheiterns

Fragen? Jederzeit gern!

Projektgruppe DoIT
Andreas Eibisch
Zellescher Weg 12
01069 Dresden

Telefon: 0351/ 463-42302
Email: andreas.eibisch@tu-dresden.de

www.tu-dresden.de/die_tu_dresden/zentrale_einrichtungen/zih

Projekt AlmaWeb
Anja Soisson
Hainstraße 11
04109 Leipzig

Telefon: 0341/ 97 300 62
Email: anja.soisson@uni-leipzig.de

www.uni-leipzig.de/almaweb