Der kleine ALOIS und der aktive Verzeichnisdienst

oder

Identity-Management an der Universität Augsburg

Maria Schmaus, Rechenzentrum

5. Oktober 2010

Universität Augsburg University

Es war einmal …

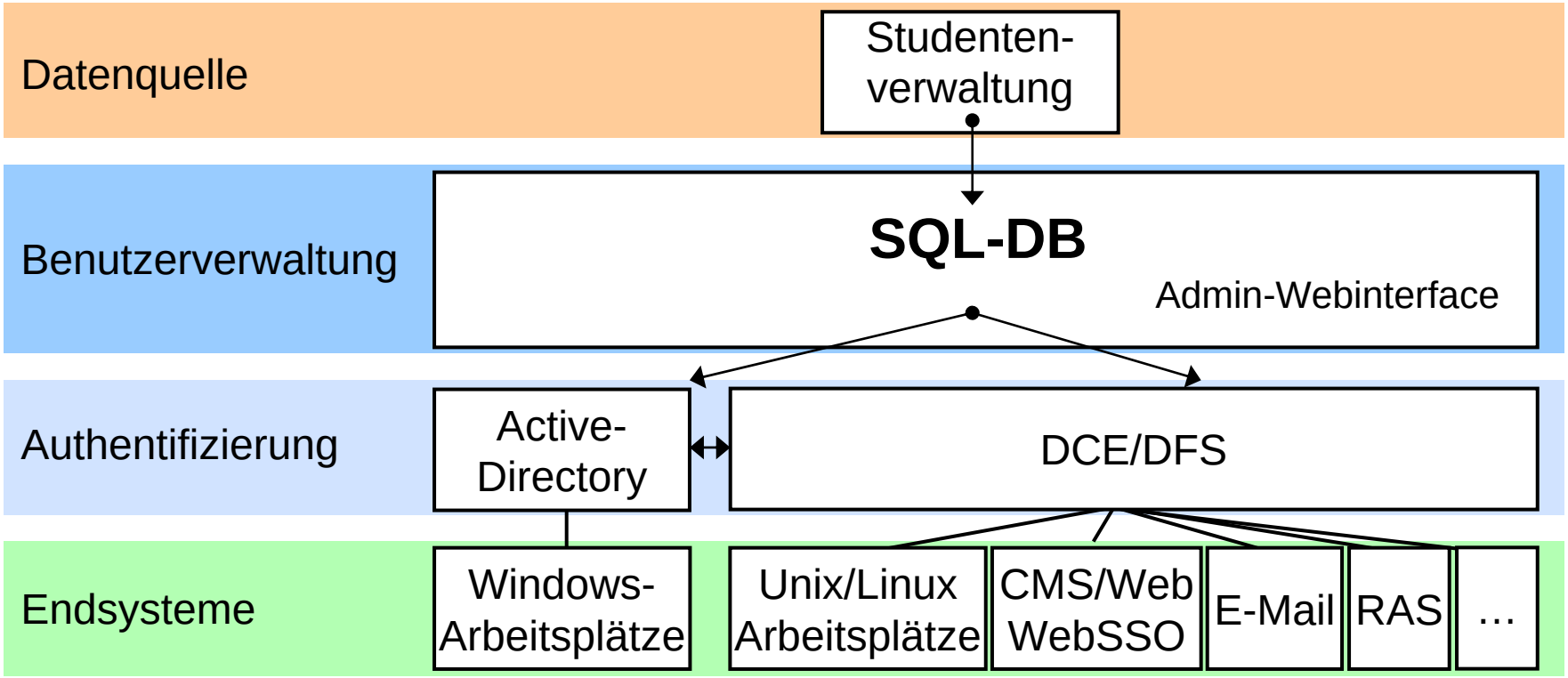
Überblick

- IT-Landschaft der Universität Augsburg
- Identity-Management an der Uni Augsburg
  - Benutzerverwaltung gestern und heute
  - Motivation für Identity-Management morgen
  - Identity-Managment Grundsätze
  - ALOIS-Architektur
- ALOIS liefert Struktur für Verzeichnisdienste
  - Mehrwert nutzen
  - am Beispiel vom Active Directory
- Fazit

Die IT-Landschaft der Universität Augsburg

- Die Dienstleistungen des Rechenzentrums nutzen
  - über 20.000 Anwender an
  - gut 3.500 Computer-Arbeitsplätzen
- Keine homogene Betriebssystemstruktur
  - Windows 2000, XP, Vista, Windows 7
  - AIX, Solaris, IRIX, Debian, Ubuntu, SuSE, …
  - MacOS und andere
- Vielzahl personalisierter IT-Dienste
  - CMS, Digicampus, Studentenportal und weitere personalisierte Webanwendungen
  - E-Mail, RAS, Drucken, Datenbanken, Lizenzserver, …

Unsere Benutzerverwaltung – gestern und heute



Unser derzeitiges Datenmodell

- Vorname, Nachname
- Status (Mitarbeiter, Student, Gast, externer Student)
- Zusatzinformationen
  - Für Studierende: Fakultät, Matrikelnummer
  - Sonst: Kontaktdaten (z.B. Tel.Nr., Ansprechpartner)
- Login
  - Name
  - Gültigkeitsdatum
  - Status (vorbereitet, eingerichtet, gelöscht)
- E-Mail-Adressen der Studierenden

Derzeitige Schwachstellen

- Manuelle Verwaltung von Mitarbeitern und Gästen
- Keine Start- und Endedaten von Mitarbeitern
- Keine Organisationszugehörigkeiten
- Alle sind gleich: keine Gruppierung von Benutzern / Benutzerkennungen
- Divergente Gruppierung in AD und DCE/DFS
- Starres SQL-Datenmodell, Workflows nicht flexibel

Auf zum Identity-Management!

- Anbindung aller Datenquellen
  - Automatisierte Anbindung der Personalverwaltung
  - Etablierung einer zusätzlichen Gästeverwaltung
- Gruppierung von Benutzerkennungen
  - automatisch anhand der Quell-Informationen
  - manuell entsprechend der Kooperationsbedürfnisse
- Übergang auf einen Verzeichnisdienst
  - Strukturierung der verwalteten Informationen
  - automatisierte Delegation administrativer Aufgaben
  - elegante Anbindung von Quell- und Zielsystemen

Projekt: Aufbau eines IT-Servicezentrums

Universität Augsburg University

- IuK-Führungskompetenz schaffen
- Übergreifende IuK-Strategie und -Planung
- Vorhandene Ressourcen optimal einsetzen
  - Bereichsübergreifend handeln
  - Kompetenzen bündeln
  - Betrieb optimieren
- Serviceorientierte, personalisierte IT-Dienste
- Abbildung des Student-Life-Cycle
- Gefördert durch die DFG

⇨ Identity-Management als Teilprojekt

IdM Grundsätze (1)

- Einschränkung auf „identitätsstiftende“ Daten, das sind
  - Vor-/Nachname(n), Titel, Geburtsdatum, Matrikelnummer, Personalnummer, Gastnummer (Identifizierung)
  - Studienfächer/Beschäftigungsstellen/Mitarbeitertyp (automatische Gruppierung)
  - Start- und Endedaten (Befristung)
- Also: Klarer Fokus bleibt „Zugang zu unseren IT-Systemen“

⇨ Ein kleines, modulares IdM-System,

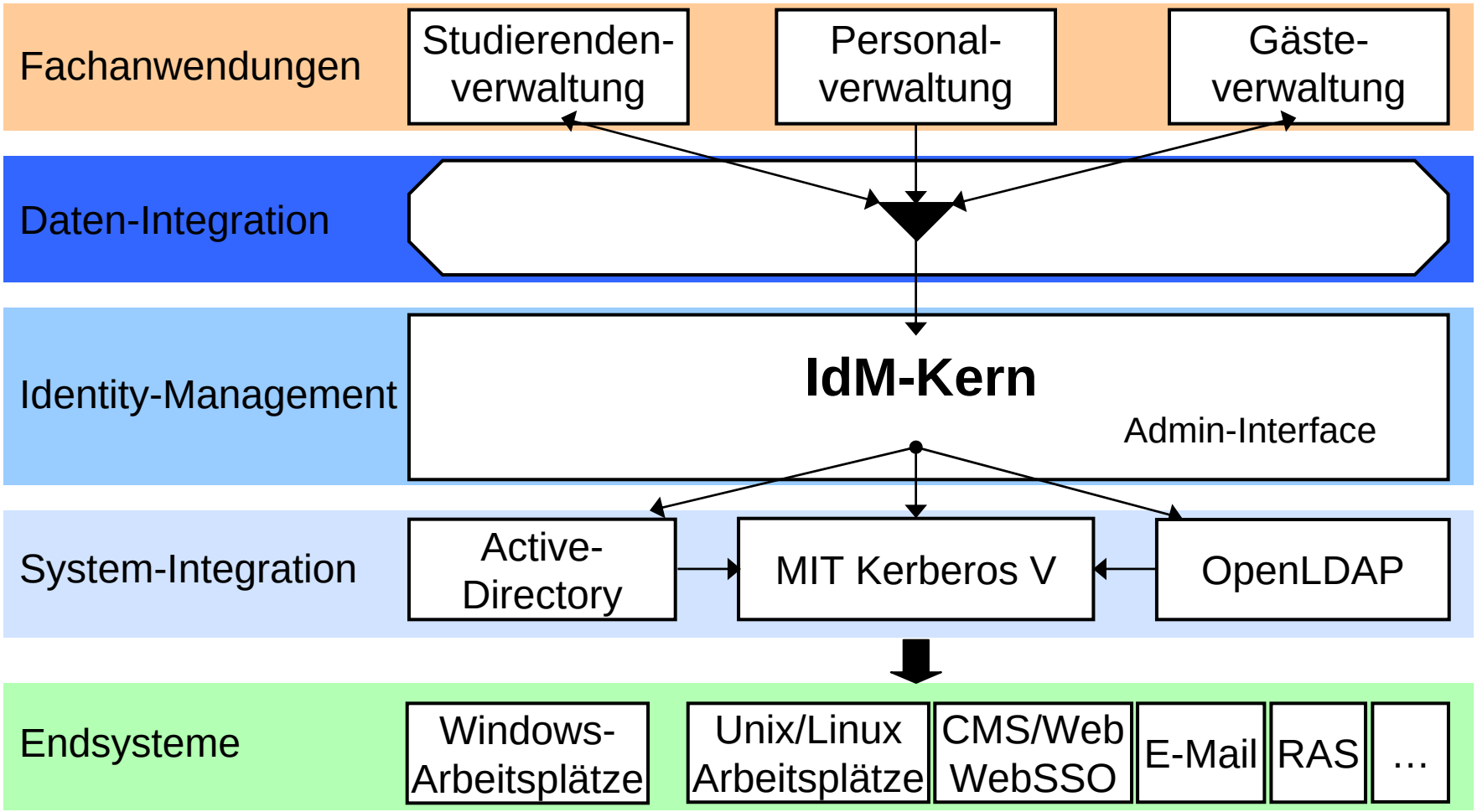
⇨ der kleine ALOIS (**A**ugsburger **L**eichtgewichtiges **O**ffenes **I**dentity-Management-**S**ystem)

IdM Grundsätze (2)

- keine Adressen, Telefonnummern, E-Mail-Adressen, …
- keine Abbildung eines formalen Organigramms
- bei wirklichem Bedarf: modulare Erweiterungen
- erleichtert Datenschutzfreigabe
- schafft Akzeptanz des Personalrats

⇨ Kein allumfassendes Auskunftssystem

Identity-Management Architektur



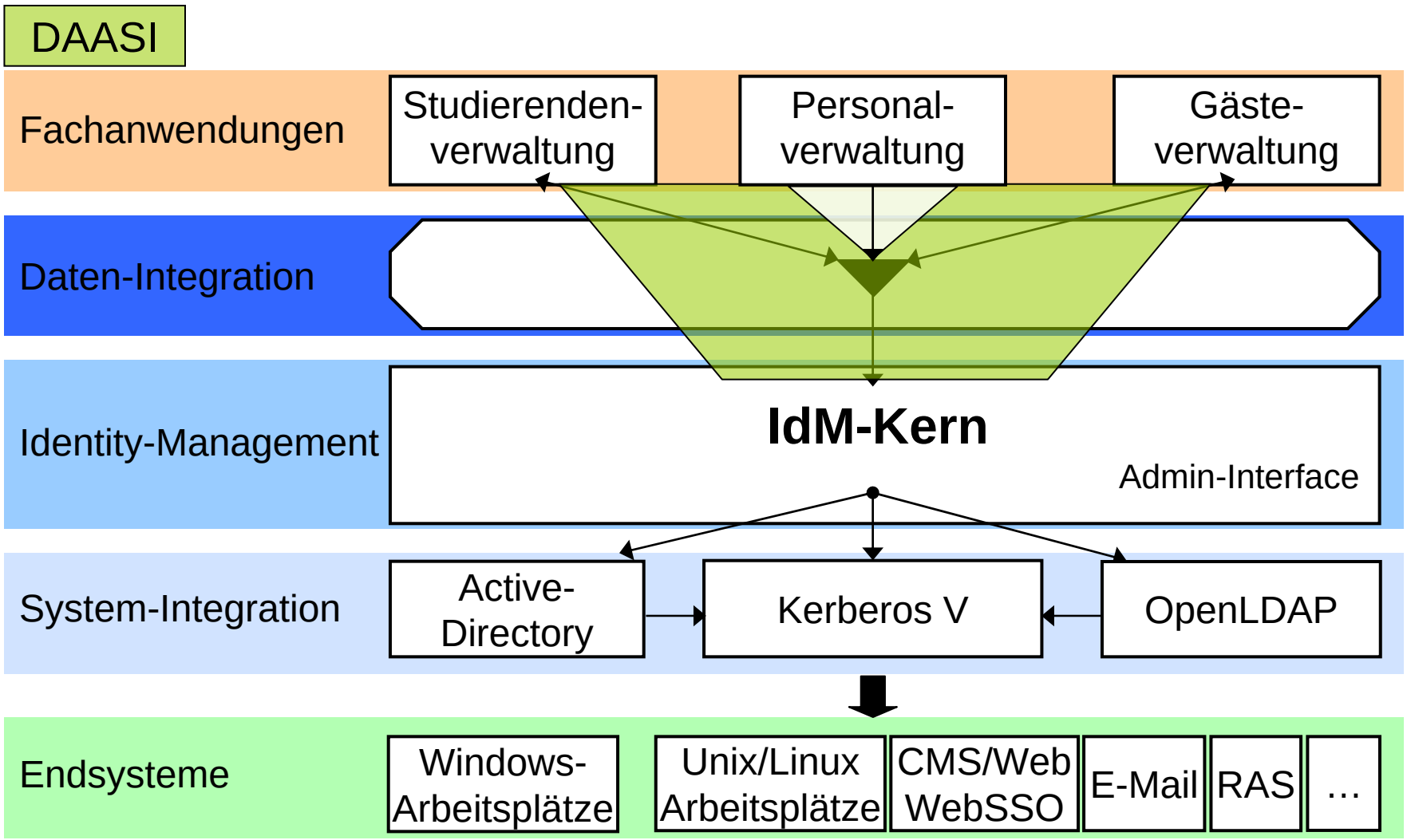
Kaufen oder Basteln?

- Kommerzielle Lösungen
  - gemischte Erfahrungsberichte anderer Hochschulen
  - großer Funktionsumfang, komplexe Systeme
  - Kosten nicht zu vernachlässigen (Beratung, Anschaffung, Betrieb)
  - viele systemspezifische Anpassungen notwendig
- Maßgeschneiderte Implementierung
  - Realisierung auf Basis von OpenLDAP gut machbar
  - vorhandene Expertise (Daten-/Systemintegration) nutzen
    - Benutzerverwaltung, Verzeichnisdienste
    - speziell Kerberos und Active Directory

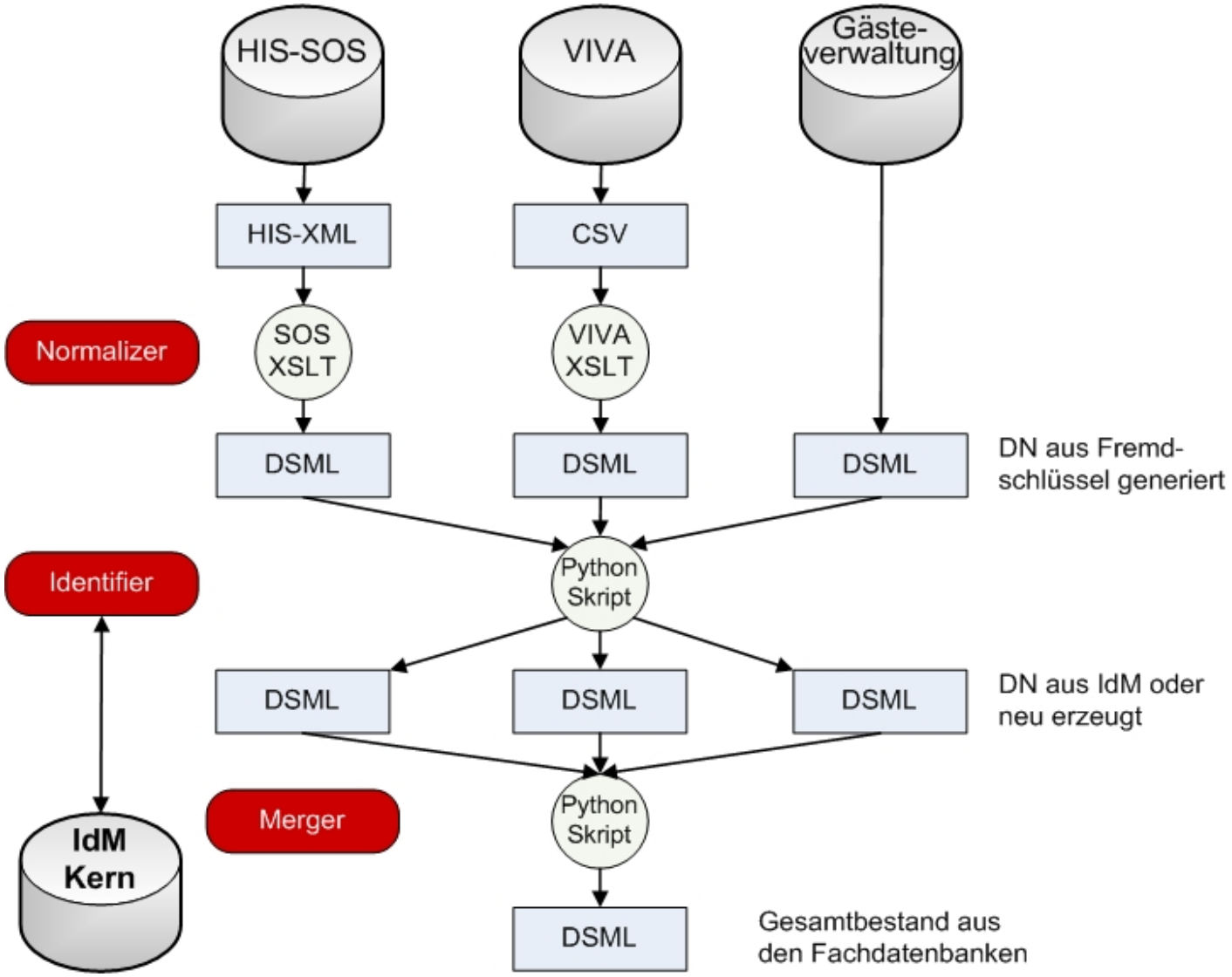
⇨ Weder Kaufen noch Basteln, sondern Mittelweg: Basis bauen lassen
  - Zusammenarbeit mit der Firma DAASI
    - Know-How
    - Open Source Lizenz, auch für Konnektoren

⇨ OpenLDAP-basierte Lösung in Kooperation mit der DAASI GmbH

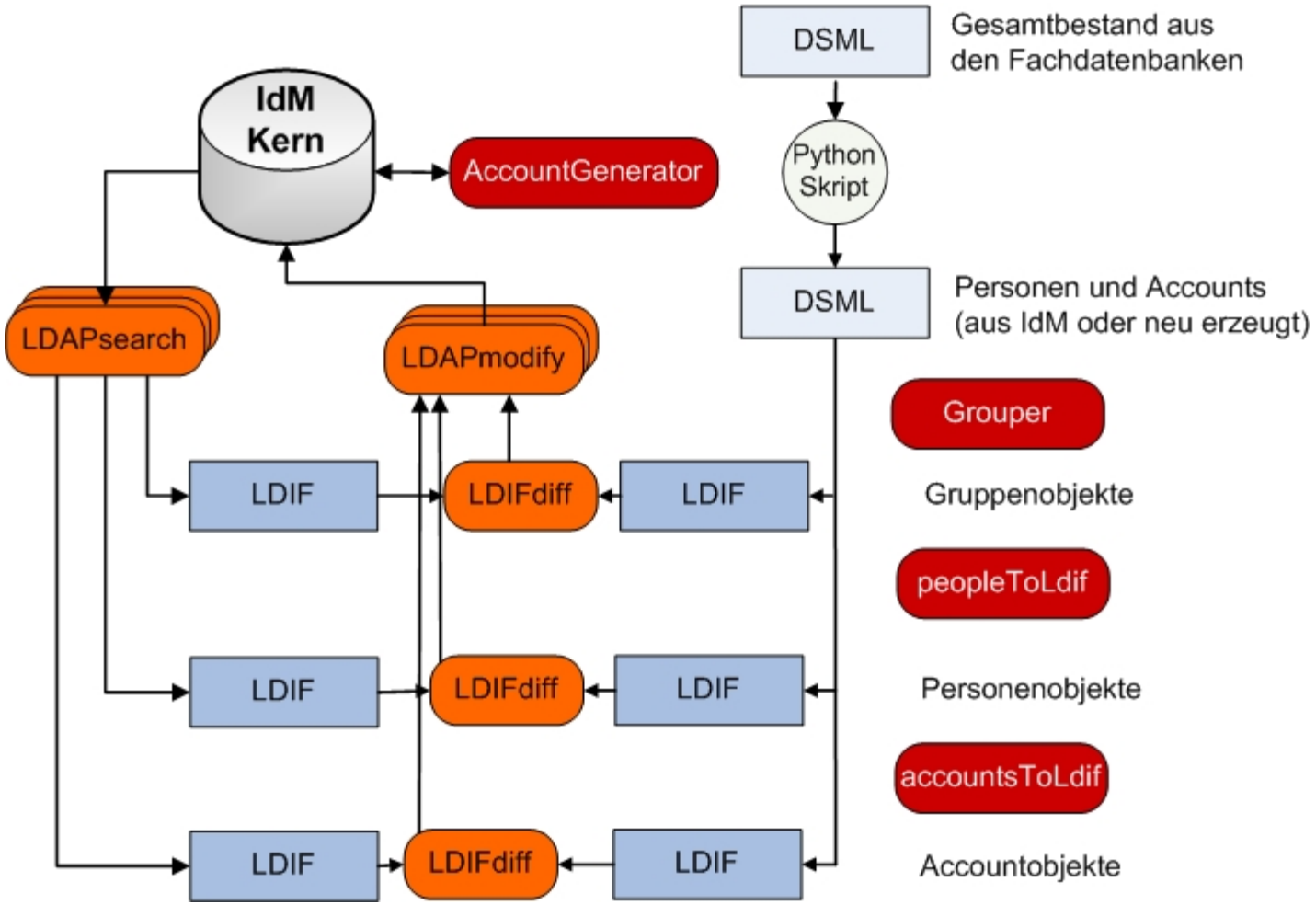
Identity-Management Architektur



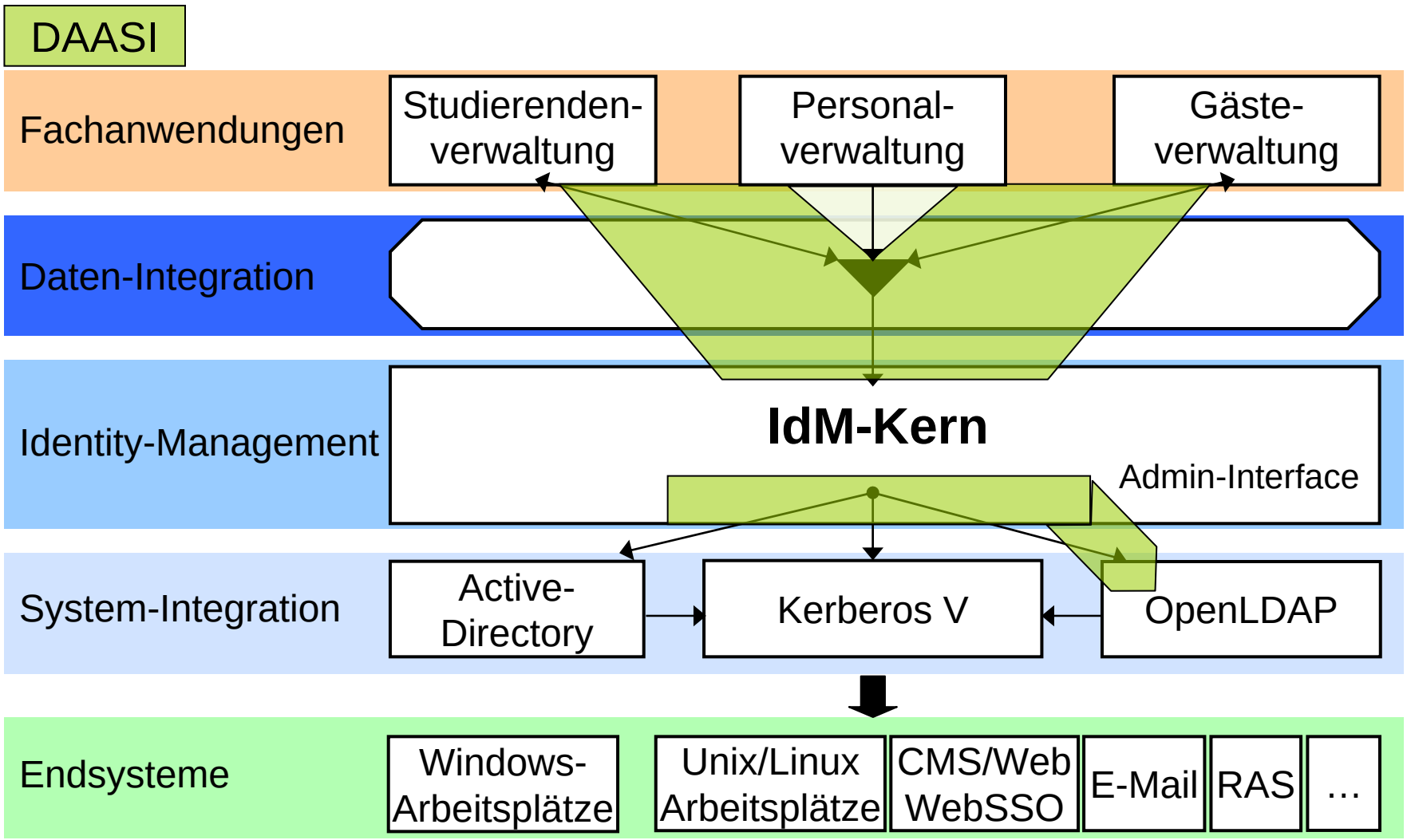
Befüllung (1)


HIS-SOS
VIVA
Gäste-verwaltung
HIS-XML
CSV
Normalizer
SOS XSLT
VIVA XSLT
DSML
DSML
DSML
DN aus Fremd-schlüssel generiert
Identifier
Python Skript
DSML
DSML
DSML
DN aus IdM oder neu erzeugt
Merger
Python Skript
IdM Kern
DSML
Gesamtbestand aus den Fachdatenbanken

Befüllung (2)

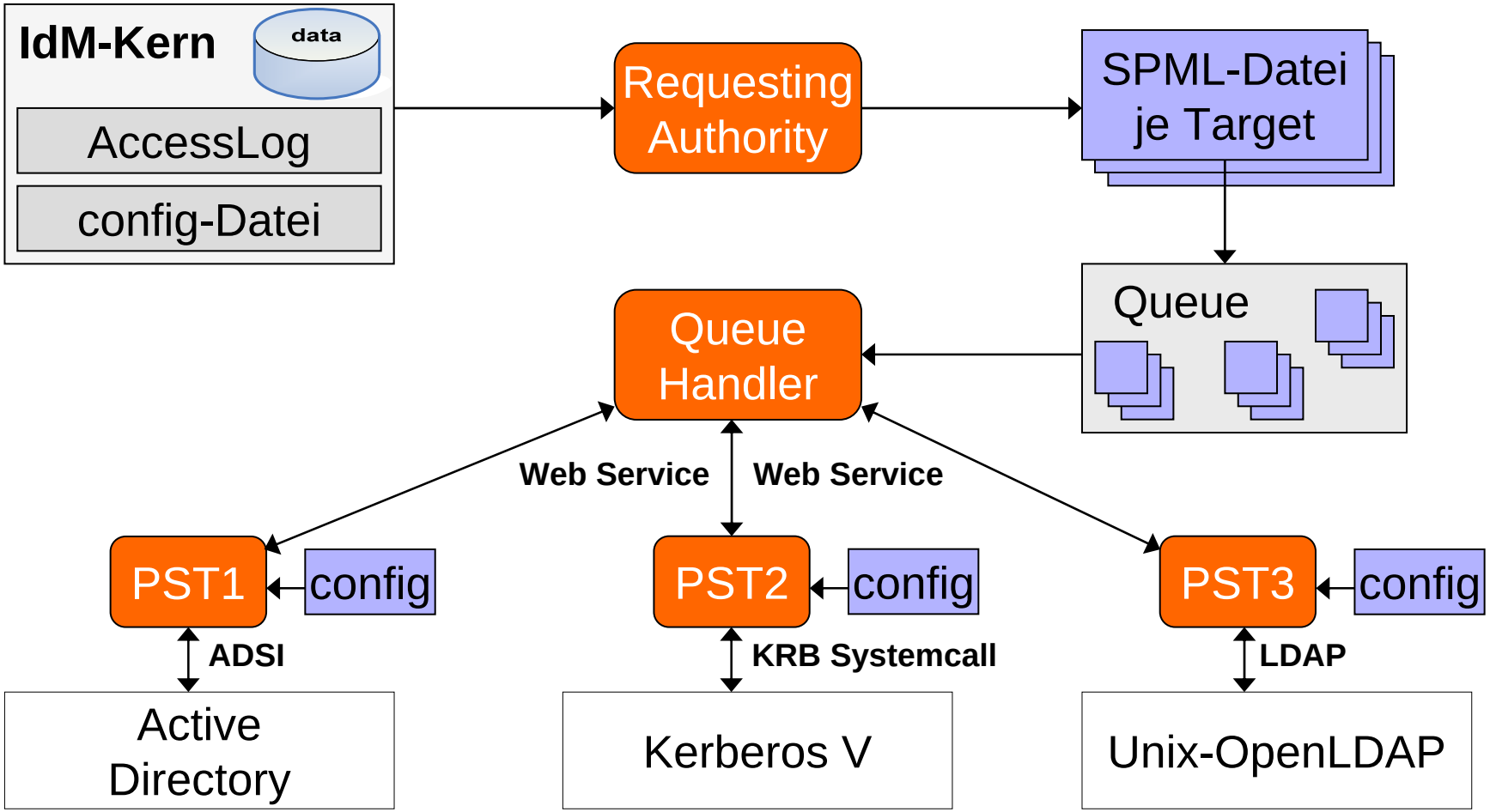

DSML
Gesamtbestand aus den Fachdatenbanken
IdM Kern
AccountGenerator
Python Skript
DSML
Personen und Accounts (aus IdM oder neu erzeugt)
LDAPsearch
LDAPmodify
Grouper
LDIF
LDIFdiff
LDIF
Gruppenobjekte
peopleToLdif
LDIF
LDIFdiff
LDIF
Personenobjekte
accountsToLdif
LDIF
LDIFdiff
LDIF
Accountobjekte

Identity-Management Architektur

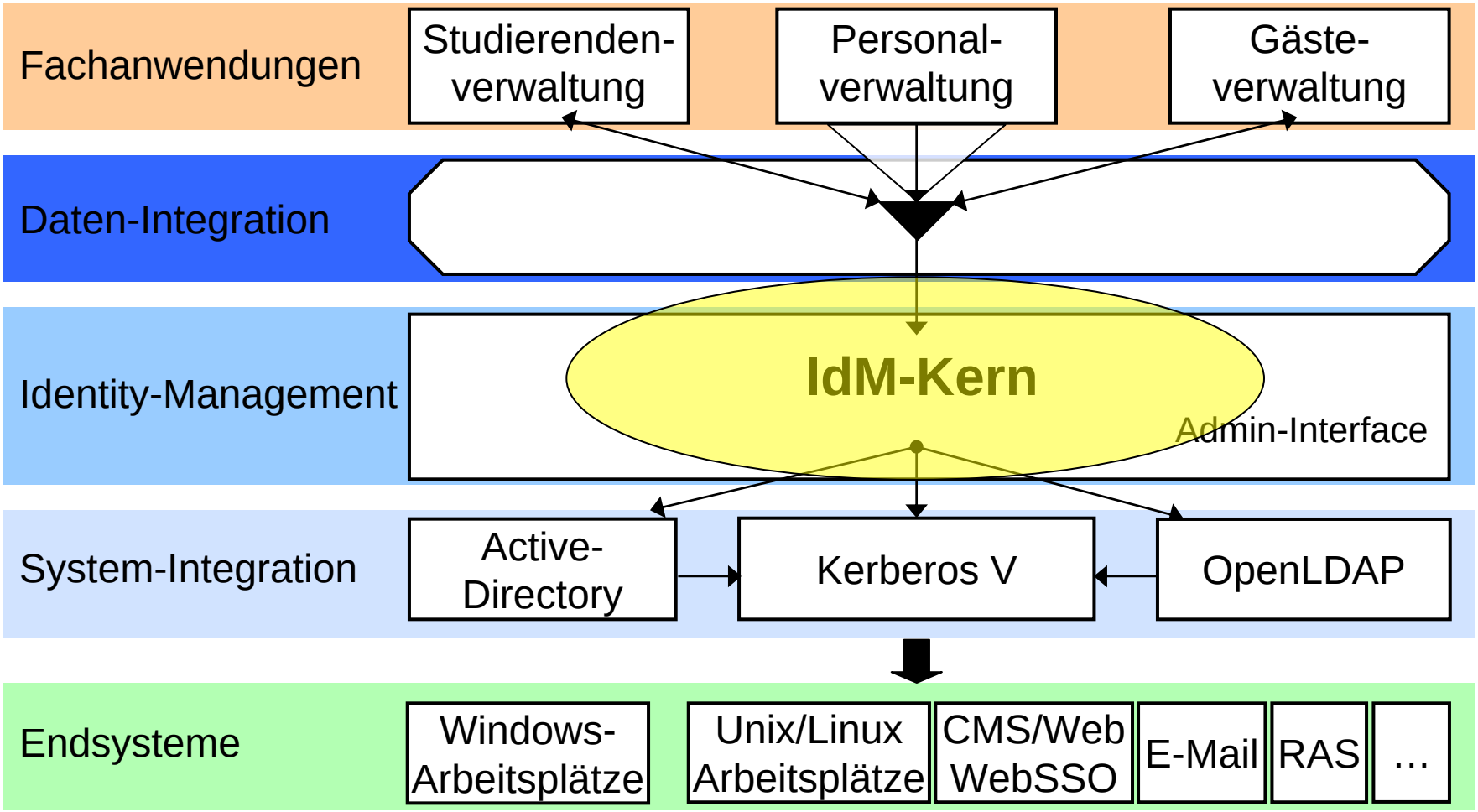


Provisionierung

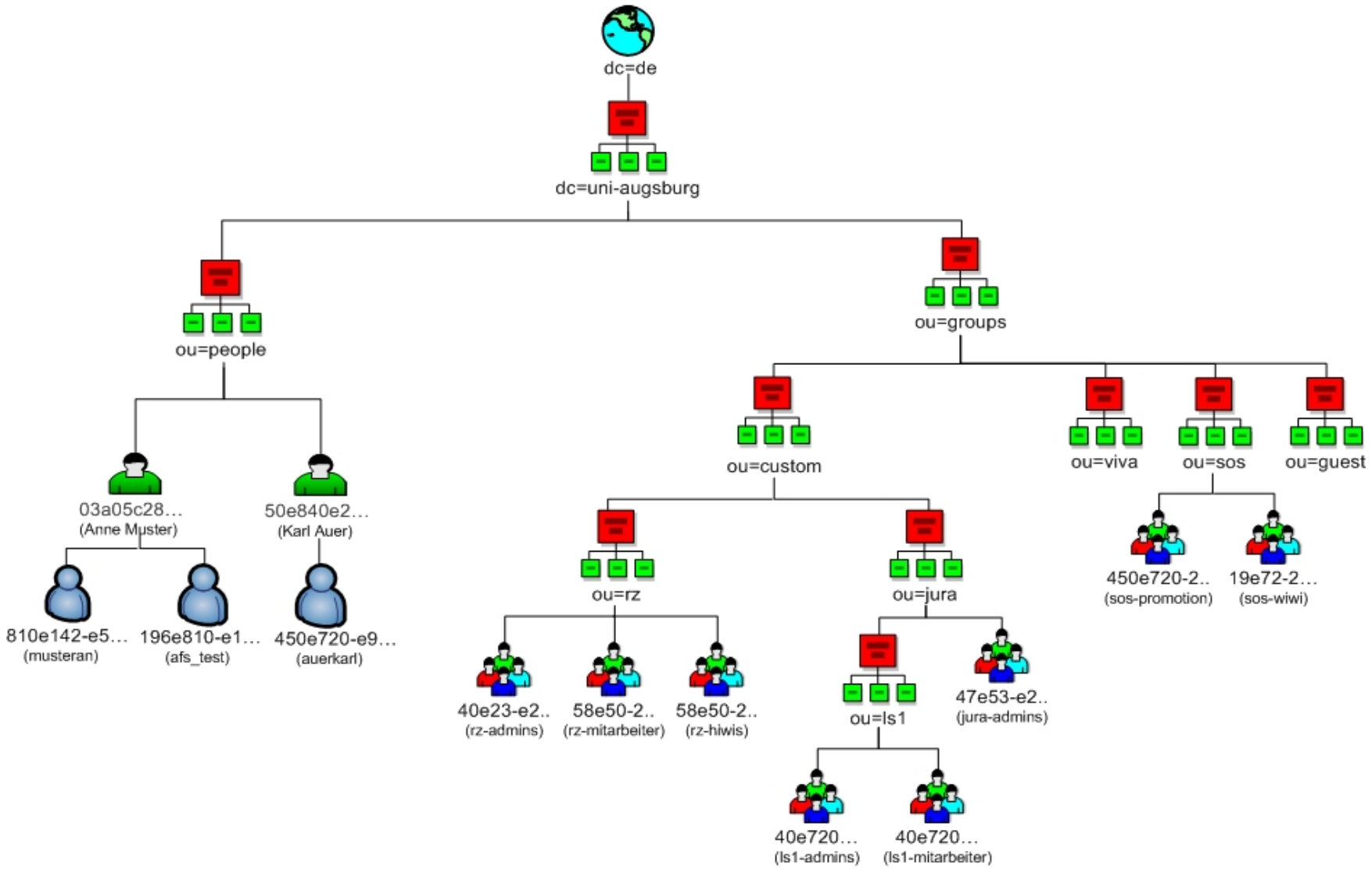
PST = Provisioning Service Target



Identity-Management Architektur



IdM-Kern DIT-Design



Verwaltung von Benutzergruppen

Universität Augsburg University

- Automatisierte Gruppenbildung (viva, sos, guest)
- Manuelle Gruppenbildung (custom)
  - Hierarchische OU-Struktur
  - entsprechend eines „gelebten“ Organigramms
  - Delegation der Verwaltung an Bereichsadministratoren
  - mit einheitlichem Berechtigungsmodell
  - nach fest vorgegebenen Standards
- Standard-Gruppen in jeder neuen OU
- „*ou-name*-admins“-Gruppe bekommt standardmäßig Administrationsrechte innerhalb dieser OU
- Berechtigungsvergabe über ACLs
- OUs kann nur der IdM-Admin administrieren

Mehrwert des IdM

- Mehrfachnutzung des Organigramms
- liefert Ordnung und Struktur
- für alle aktiven Verzeichnisdienste
- zur automatisierten Delegation von administrativen Aufgaben

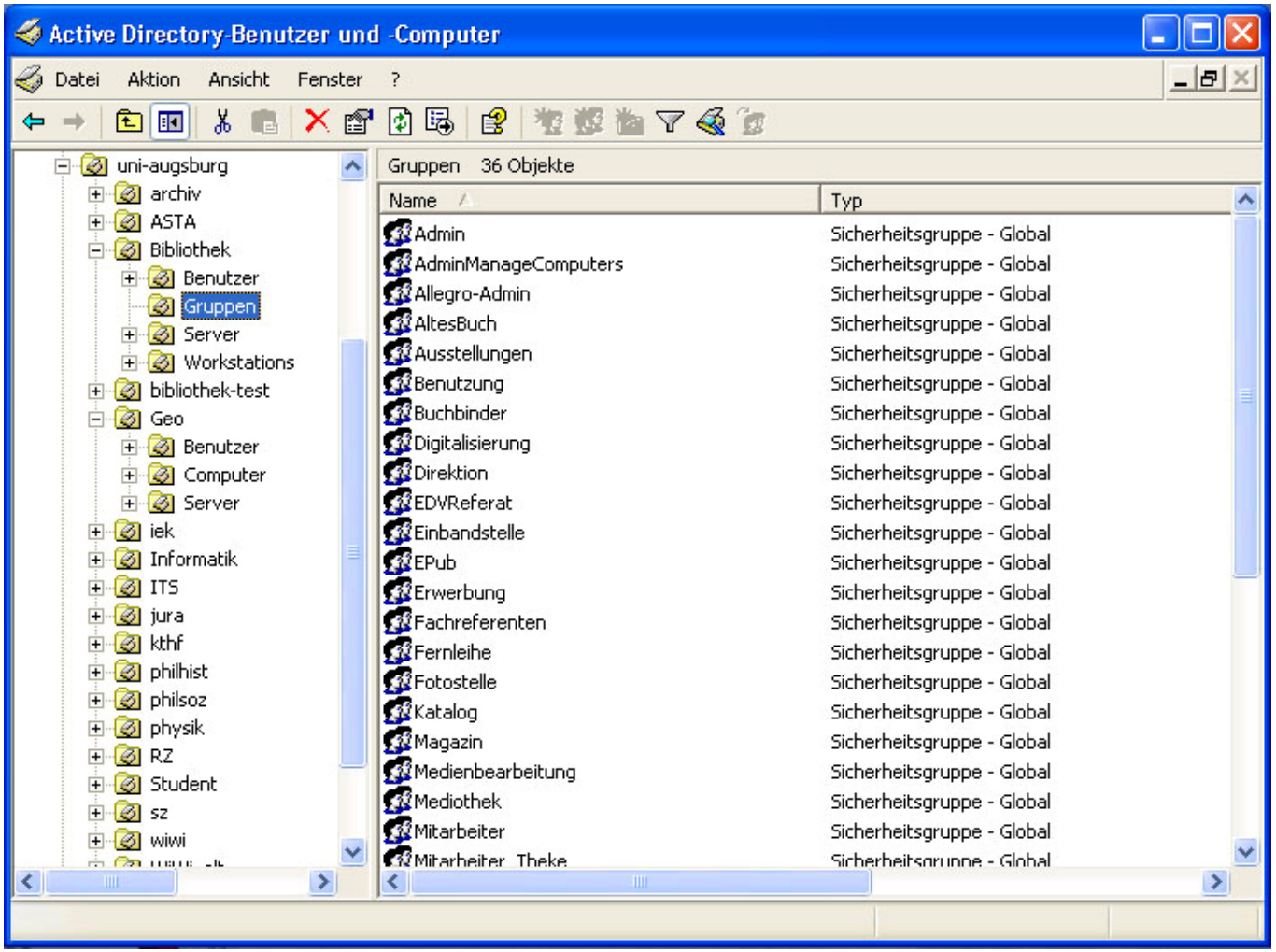
⇨ Mehrwert für die Systemintegrationsschicht

Beispiel: Provisionierung des Active Directory Systems

Active Directory an der Uni Augsburg

- Ursprünglich (bis Mitte 2003): NT-Domänen-Verbund
- Später (bis Mitte 2005): Active-Directory-Verbund
- Heute: eine Active-Directory-Domäne
  - Zusammenführung zu einer einzigen AD-Domäne
  - Gewisse administrative Freiheiten durch Delegation
  - Delegation auf Basis der AD-Struktur
- Derzeitiger Stand
  - Divergente Struktur
  - Unterschiedliche Berechtigungen
  - Viel passiert auf Zuruf
  - Dokumentation nicht aktuell
  - Funktioniert zwar, aber keiner blickt richtig durch

AD-Struktur heute



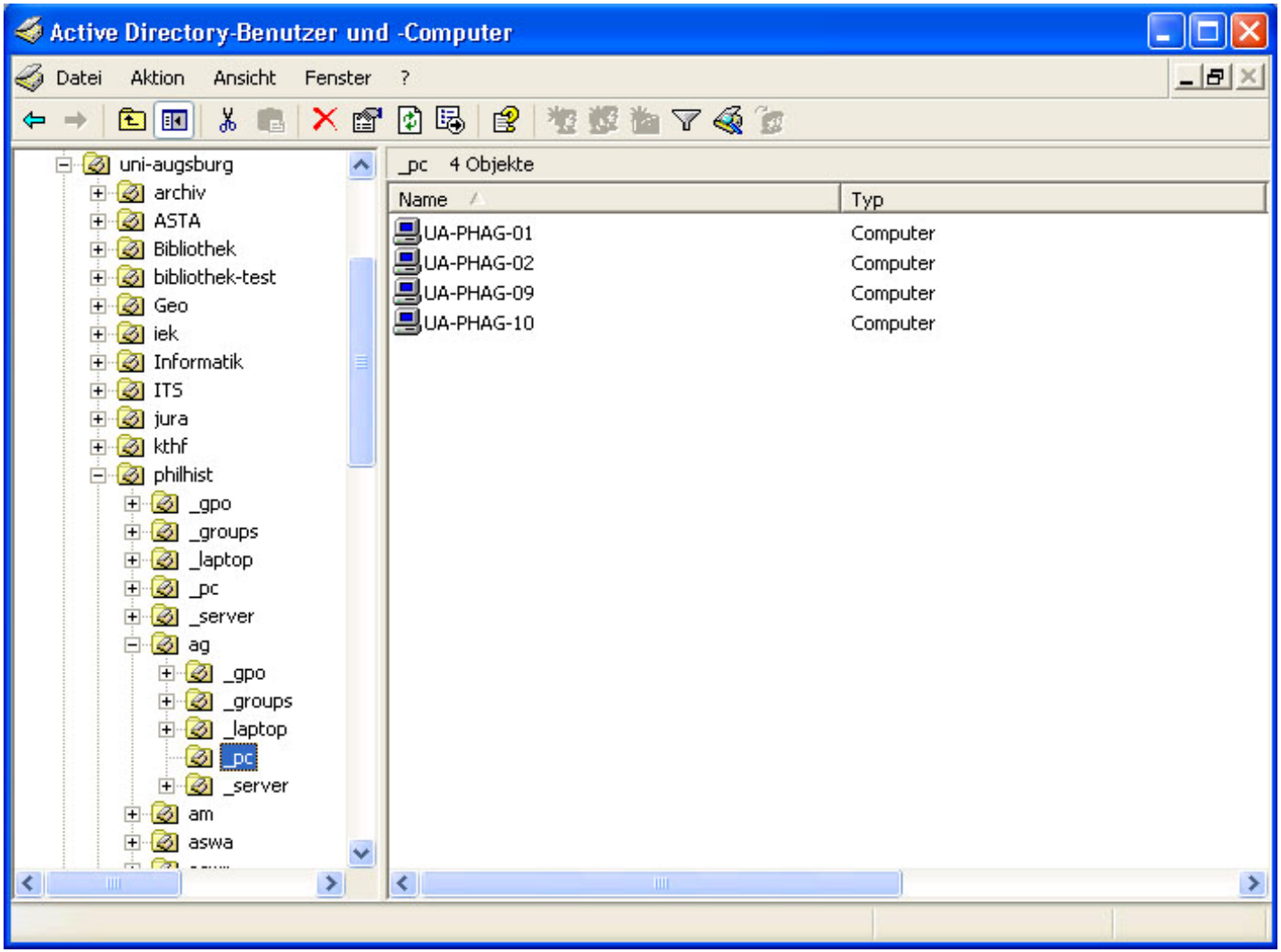
AD-Struktur in Zukunft

Universität Augsburg University

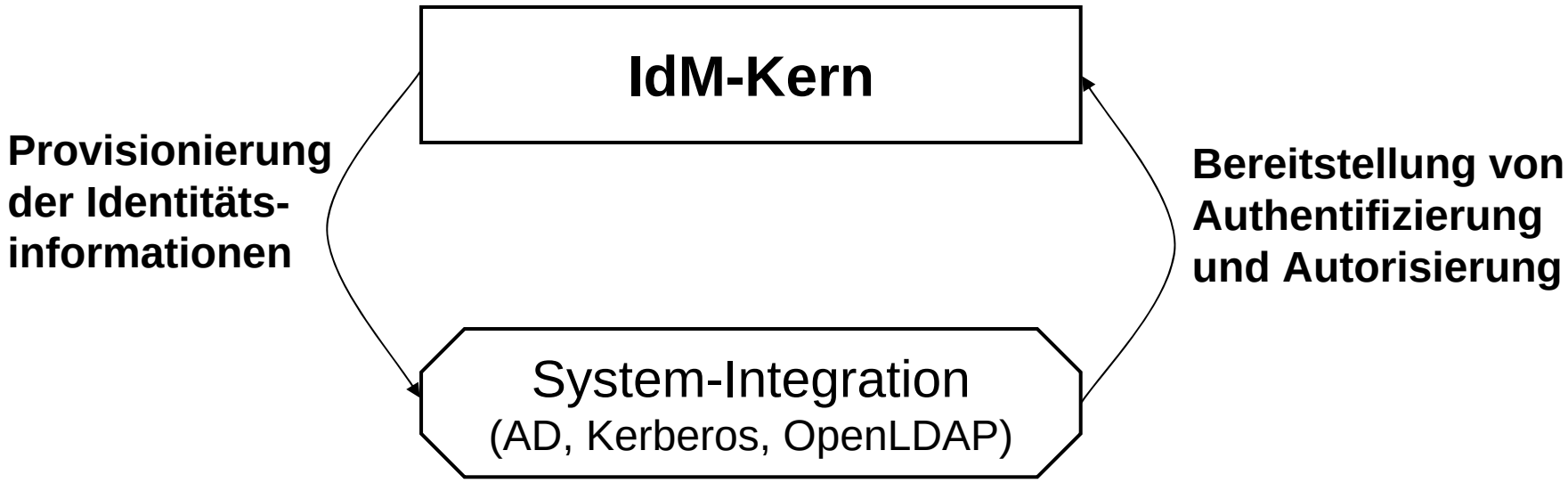
Idee: Strukturen aus dem IdM-Kern ins AD übertragen

- RZ-Benutzerkennungen kommen in Users-Container
  - darauf keinerlei Administrationsberechtigungen
- OU-Struktur wird in ou=uni-augsburg übertragen
- Standardisierte Unter-OUs
  - _gpo: Für Gruppenrichtlinienobjekte
  - _groups: Für die Gruppen aus dem IdM
  - _laptop: Für Computerkonten der Laptops
  - _pc: Für Computerkonten der Arbeitsplatz-PCs
  - _server: Für Computerkonten der Serversysteme
- Standardisierte Berechtigungen
- Festes Namensschema für AD-Objekte

AD-Struktur morgen



Identitätsrückkopplung



Fazit

- Der kleine ALOIS
  - Minimalistischer Identity-Management-Ansatz
  - Modular erweiterbare Funktionalität (Open Source)
  - Strukturierung anhand der Kooperationsbedürfnisse
- und der aktive Verzeichnisdienst
  - IdM-Struktur wird zur Delegation administrativer Aufgaben der Systemintegrationsschicht genutzt
  - Dezentrale Administration wird automatisiert: nachvollziehbar, verlässlich, dokumentiert

Und wenn sie nicht gestorben sind,

dann verwalten sie noch heute …

Universität Augsburg University

Danke für Ihre Aufmerksamkeit!