DFG-Projekt

IntegraTUM

Identity Management an Technischer Universität und Leibniz-Rechenzentrum München

Wolfgang Hommel
hommel@lrz.de

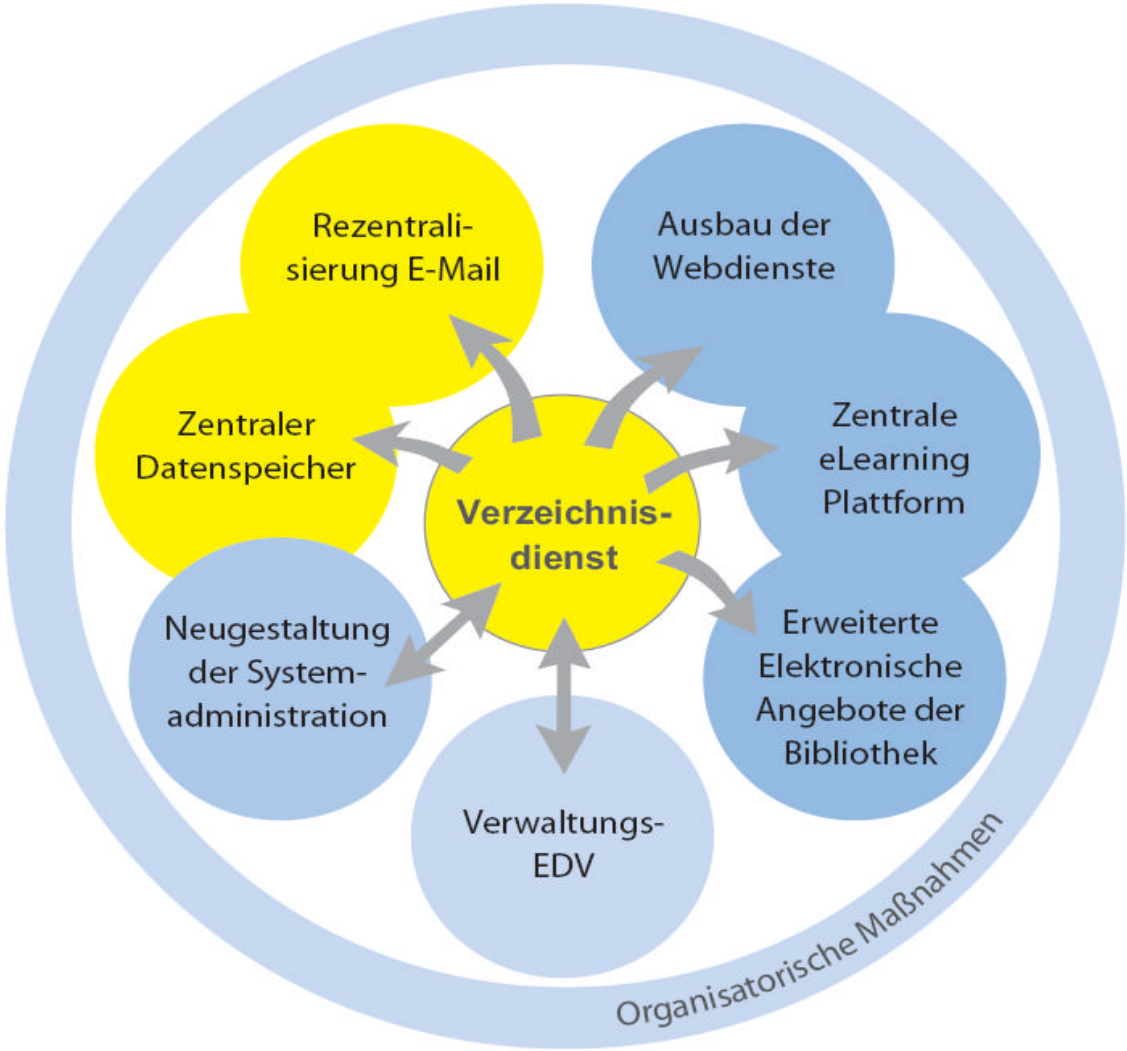
Agenda

- IntegraTUM-Überblick
- Teilprojekt Verzeichnisdienst
- Probleme, Lösungsansätze und Vorgehensweisen

Projekt IntegraTUM

Ein Überblick

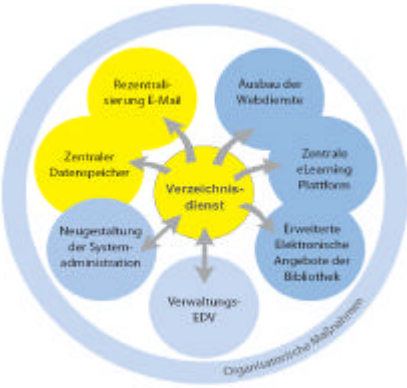
Teilprojekte



Prof. Dr. A. Bode
Vizepräsident /
CIO TUM

Einige Ziele des Gesamtprojekts

- Prämisse: Benutzerfreundliche und nahtlose IuK-Infrastruktur
- Rezentralisierter Betrieb, dezentrale Administration
  - Rezentralisierung von > 100 Mail-Servern
  - Zentraler File-Server für Home- und Projekt-Verzeichnisse (NAS-Filer + CIFS + Web-Interface statt AFS)
- Modernisierung der Software-Verteilung
- Migration von Web-Content ins myTUM-Portal
- Aufbau einer E-Learning Plattform
- Ausweitung elektronischer Angebote der Bibliothek



Zahlen zum Gesamtprojekt

- Projektbeginn 07/2004
- Geplante Laufzeit 5 Jahre
- Ca. 15 neue Projekt-Stellen
  - aus Mitteln der TUM
  - aus DFG-Förderung: Vorerst auf 2 Jahre begrenzt
- Stellenbesetzung erst 04/2005 abgeschlossen
- Ca. 20 weitere feste Projekt-Involvierte

Teilprojekt Verzeichnisdienst

Teilprojekt Verzeichnisdienst

- Eines der drei LRZ-Teilprojekte
- Ca. 4,5 Personen:
  - 4 Projektstellen, seit 12/2004 – 02/2005 besetzt
  - Teilprojektleiter
- Integriert ins Directory-Team des LRZ:
  - LRZ-Benutzerverwaltung und IM-Projekt
  - Betrieb myTUM-LDAP und IntegraTUM

Teilprojekt-Organisationsstruktur

LRZ-Abteilung „Benutzernahe Dienste und Systeme“

Gruppe „Directories, E-Mail“

Ado Haarer

Gruppenleiter

Wolfgang Hommel

Team-
/Teilprojektleiter

Latifa Boursas

Stefanie Winklmeier

Dr. Ralf Ebner

Technische Ziele TP LDAP (1/2)

- Aufbau eines zentralen Identity Repository und Provisioning-Systems

- Datenquellen:
  - HIS SOS (Studentenverwaltung)
  - SAP HR (Personalverwaltung)
  - UnivIS (Gast-Dozenten)
  - Gästeverwaltungssystem (zu implementieren)
  - SISIS Elektra/SunRise (Bibliothek)

Technische Ziele TP LDAP (2/2)

- Speisung angeschlossener Systeme:
  - myTUM-Web-Portal (Novell eDirectory)
  - Zentrale E-Mail-Server (BT/Syntegra Aphelion)
  - Zentraler Storage (MS Active Directory)
  - Authentifizierungsserver (MS AD, OpenLDAP)
  - E-Learning System (imc CLIX)
  - Bibliothekssystem (SISIS)
  - Alumni-Datenbank (zu konsolidieren)

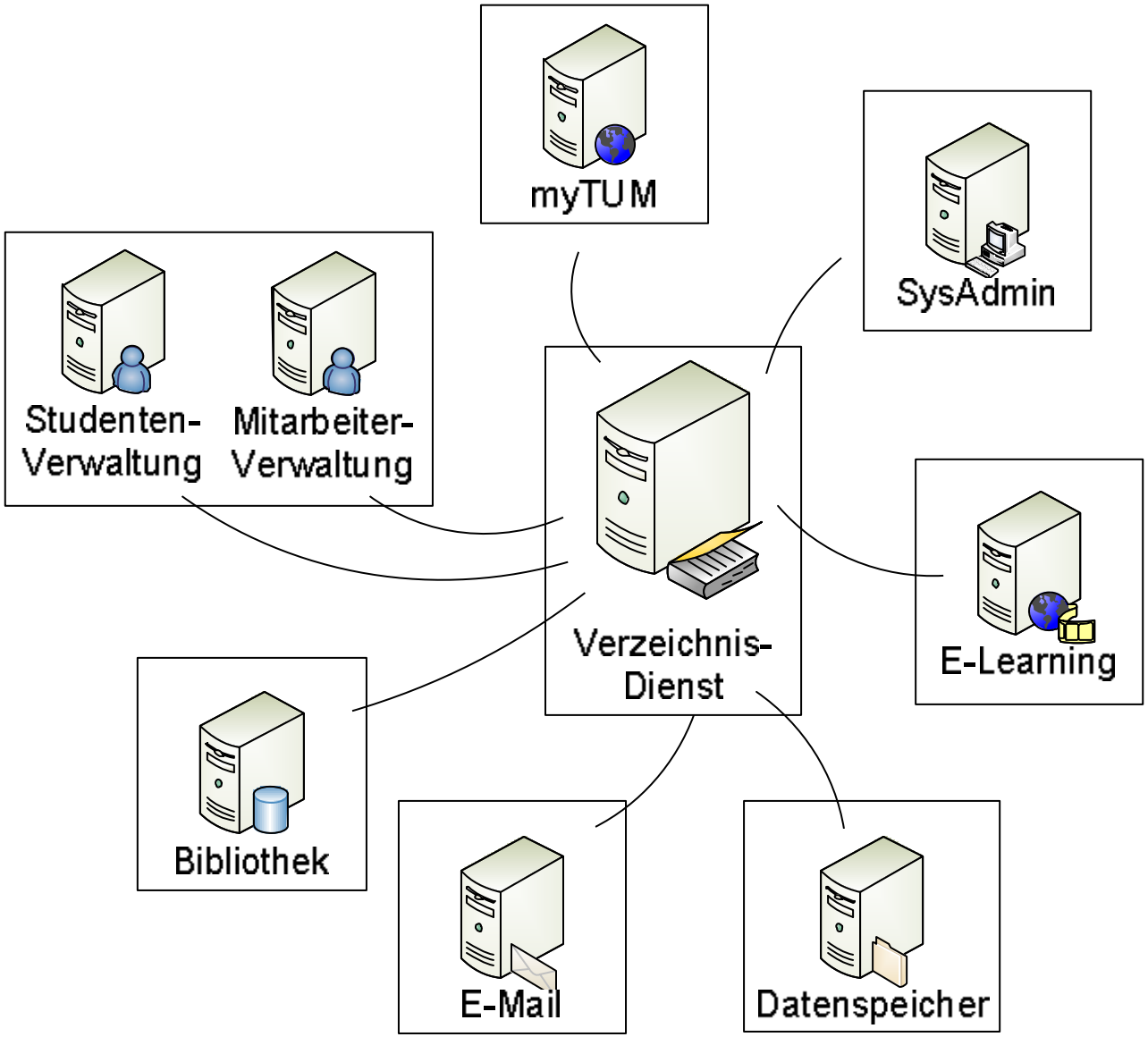
Weitere Ziele TP LDAP

- Prozessübergreifende Korrelation von Personen-Objekten
- Unterstützung der notwendigen dezentralen Administration

  ? Änderungen an bestehenden Prozessen notwendig! ?

- Selektiver Schreibzugriff auf Personal- und Studentenverwaltungs-Systeme
- Flexible Architektur für spätere Erweiterungen
- Grundlagen für hochschulübergreifenden Identitäts-Datenaustausch schaffen

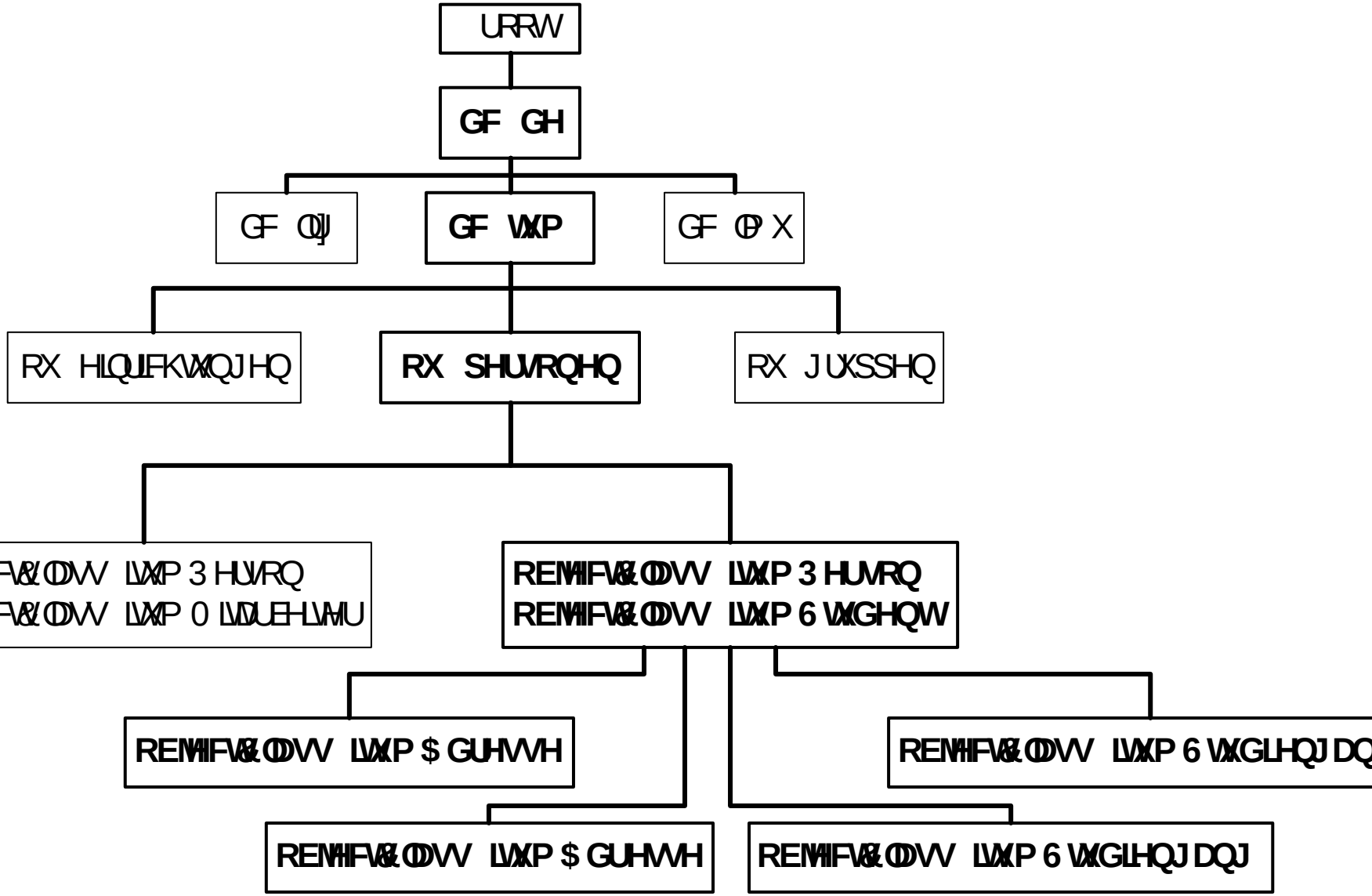
Architekturmodell (logisch)



Bisherige Tätigkeiten

- System- und Anforderungsanalyse
- Schnittstellendefinitionen:
  - Syntax und Semantik der Daten
  - Austauschfrequenz und –richtung
  - Protokoll / Transportweg
  - Definition autoritativer Datenquellen (u.U. mehr als eine pro Attribut!)
- Proof-of-Concept Testumgebungen
  ? Test-Datensätze häufig unrealistisch
- Prozessanalyse und Ist-Dokumentation
- Grobkonzepte für Gäste- und Gruppenverwaltung
- Eigenes Schema und Directory Information Tree

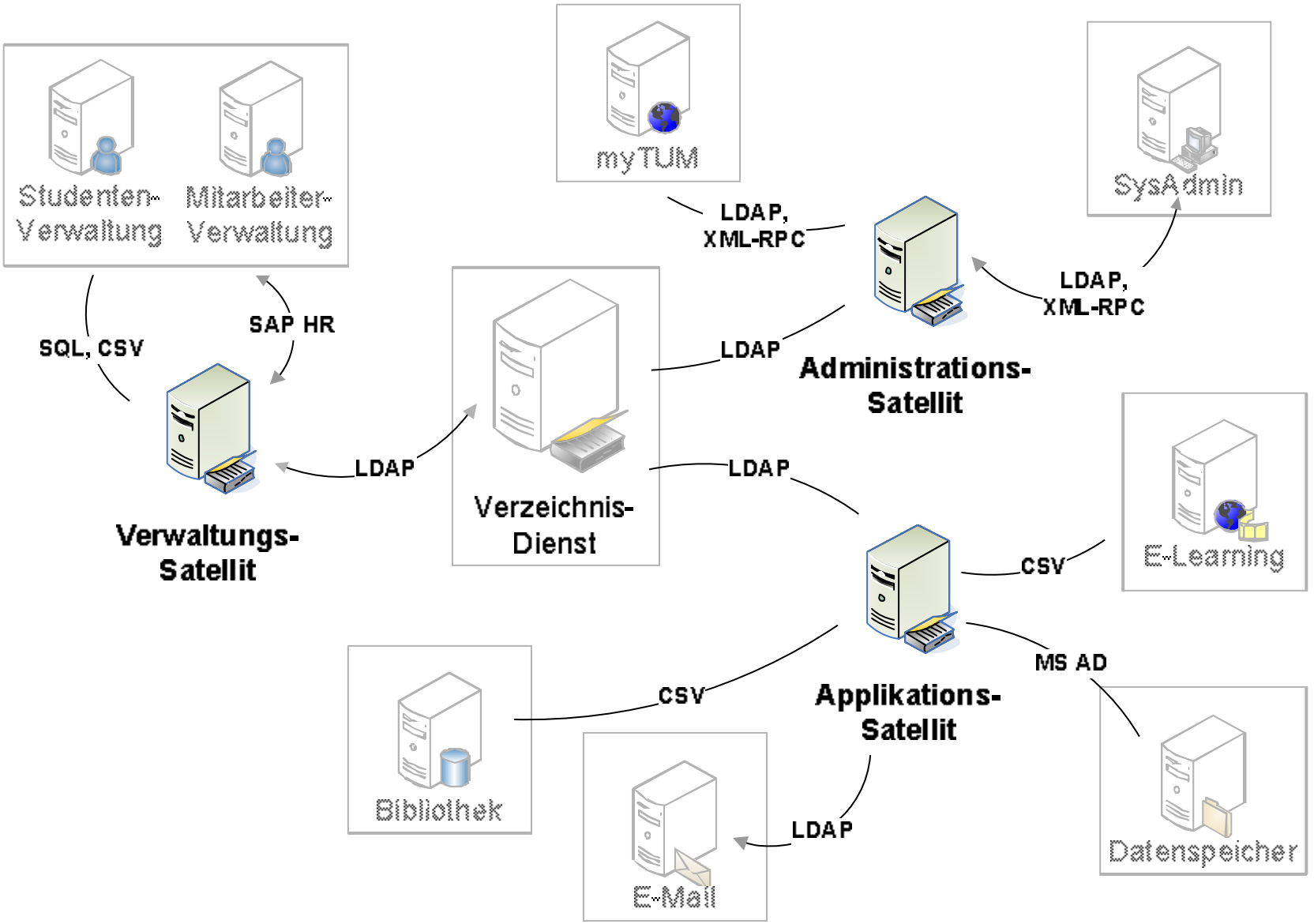
Directory Information Tree (DIT)



IntegraTUM LDAP Schemata

- Mehr als ein LDAP-Server im Einsatz:
  - Zentrales Repository: dediziertes Schema
  - LDAP-Server für direkten Zugriff:
    je nach Endsystemen „Standard-Schemata“
- 22 eigene Objektklassen mit 127 Attributen
- Spezifikation der autoritativen Datenquellen
- Dokumentation der Datenabnehmer

Architekturmodell (Realisierung)



Hochschulübergreifende MWN-Id

- MWN = Münchner Wissenschafts-Netz
  Infrastruktur für ca. 70.000 Endsysteme
- MWN-Id:
  Schlüsselattribut für technische Anwendungen
- Default E-Mail-Adresse für TUM-Angehörige:

  mwnid@mytum.de
- Auf Leporello gedruckt
- Nachteil: 16-stellige Hexzahl
  (Häufige Tippfehler, schlechte Merkbarkeit)

IntegraTUM Mail-Konzept

- Nur noch *eine* Mailbox pro Person
- Aliase für mwnid@mytum.de :
  - Self Service für Studenten: *@mytum.de
  - Self Service für Mitarbeiter: *@tum.de
  - Durch Fakultäts-Administratoren vergeben: *@xy.tum.de
- Lebenslange Mail-Weiterleitung: *@alumni.tum.de
- Funktions-E-Mail-Adressen (z.B. Webmaster, Sekretariate) über Shared IMAP Folders

LRZ-Kennungen

- LRZ vergibt Kennungen
  - fest an Studenten/Mitarbeiter der Münchner Universitäten
  - temporär an übrige Hochschul-Angehörige
  - an Nutzer von Hochleistungsrechnern aus Deutschland
  - im Rahmen europäischer Grid-Projekte

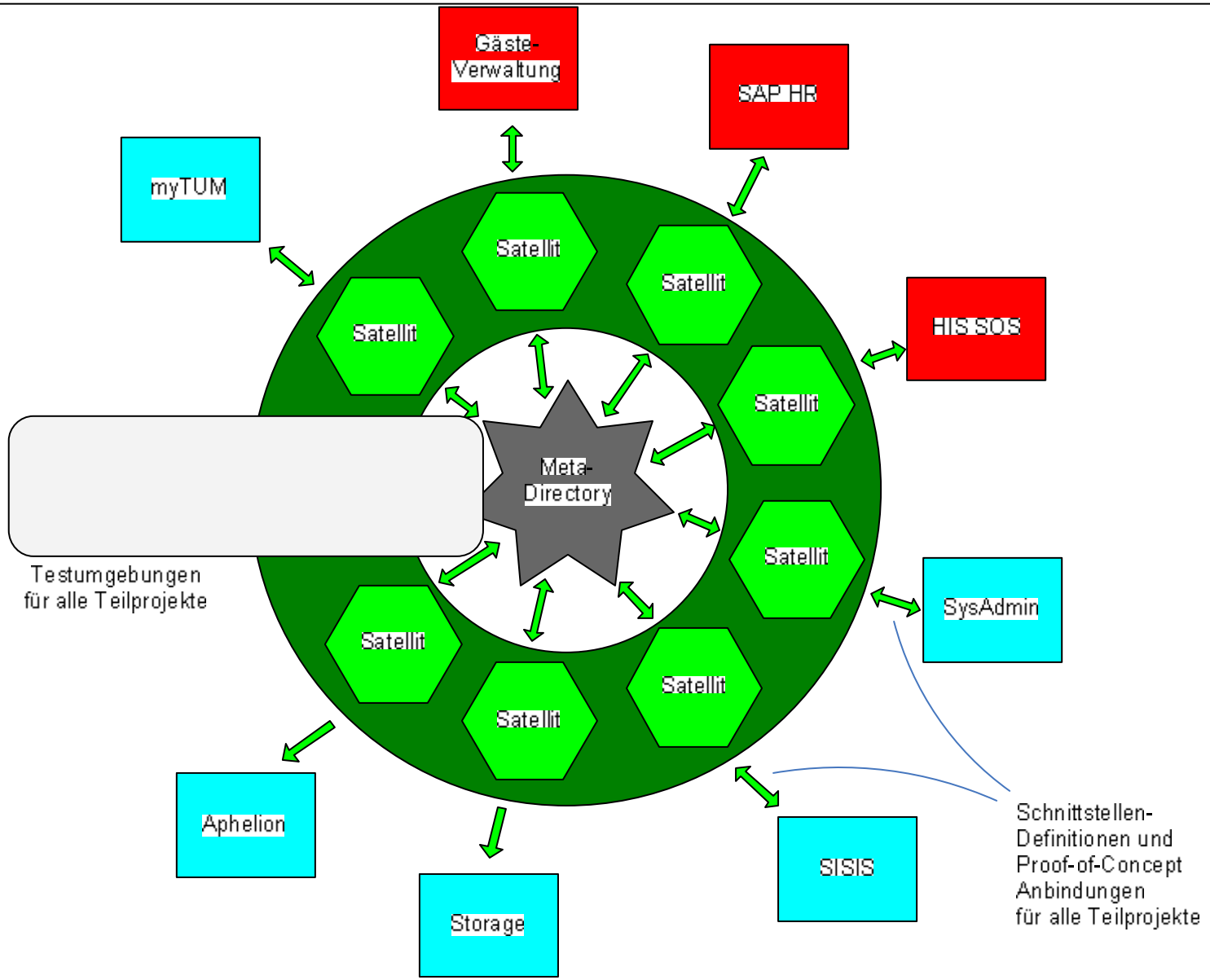
- „Nicht sprechendes“ Namensschema:

  K V Z Z K V K

  Beispiel: **me39liq** (Ca. 12 Mio. Möglichkeiten)
  Keine 0/1 wegen Verwechslungsgefahr mit O/l

- Ziele:
  - Konstanter Login-Name
  - ohne Bezug zum Realnamen der Person
  - Diktierbarkeit, Memorierbarkeit

Aufbau von Testumgebungen



Eingesetzte (LDAP-)Software

- Für den zentralen Verzeichnisdienst und die Satelliten-Verzeichnisse:
  - Novell eDirectory
  - Novell Nsure Identity Manager 2
  - Novell SuSE Linux Enterprise Server 9 + Open Enterprise Server

  Hintergrund:
  - Landeslizenzvertrag mit Novell
  - Jahrelanger Einsatz an LMU, TUM und LRZ
  - Fundiertes Produkt-Know-How im LRZ
- OpenLDAP / MS AD werden provisioniert

Probleme und Lösungsansätze

Vorgehensweisen

Korrelation von Personen-Objekten

Ist Student Müller == Mitarbeiter Müller ?

Schwierigkeiten:

- Namen können sich ändern (z.B. Heirat)
- Geburtsort und –datum können sich ändern ;-)
- Tippfehler sind menschlich
- Einhaltung von Datenschutz-Richtlinien

Gefahr:

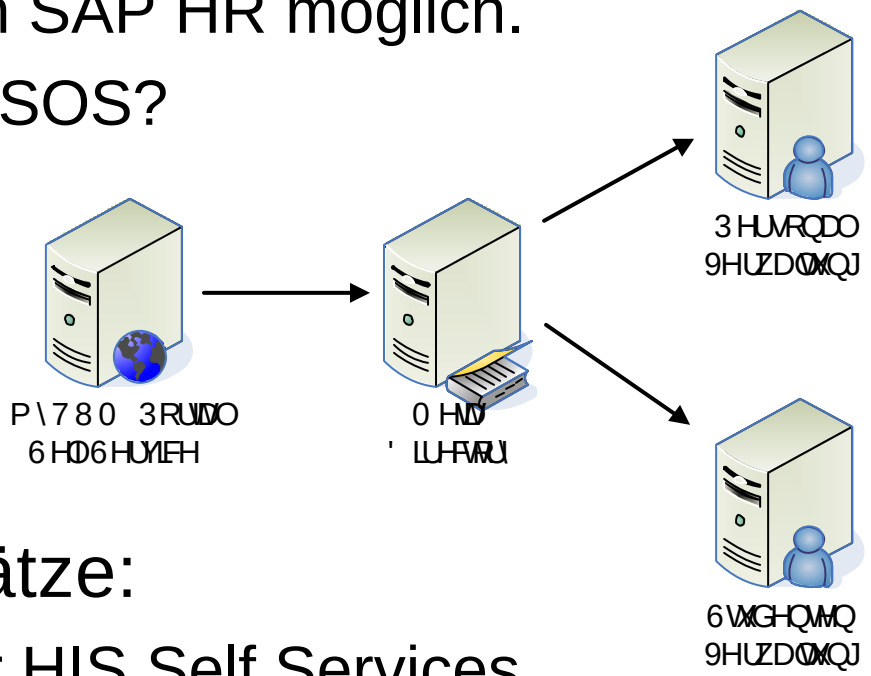
- „False Positives“ **müssen** vermieden werden

Lösungsansatz:

- Optionale Fuzzy-Suche, z.B. Geb-Datum +/- n Tage

Rollenübergreifende Self Services

- Für Adressänderungen und andere Formalia
- Wenn ein Student auch Mitarbeiter ist:
  - Schreiben in SAP HR möglich.
  - Aber in HIS SOS?



- Lösungsansätze:
  - Nutzung der HIS Self Services
  - Self Service verschickt Änderungsantrag an Verwaltung

Datenakquisition und Provisioning

Probleme bei anzubindenden Systemen:

- Werbeprospekte vs. Realität
- Proprietäre Schnittstellen z.T. fehlerhaft
- Read-only Zugriff / Export nicht ausreichend
- Konnektoren zu hochschulspezifischer Software?
- Eigener Implementierungsaufwand hoch

Lösungsansatz:

Heute selbst implementieren, was morgen

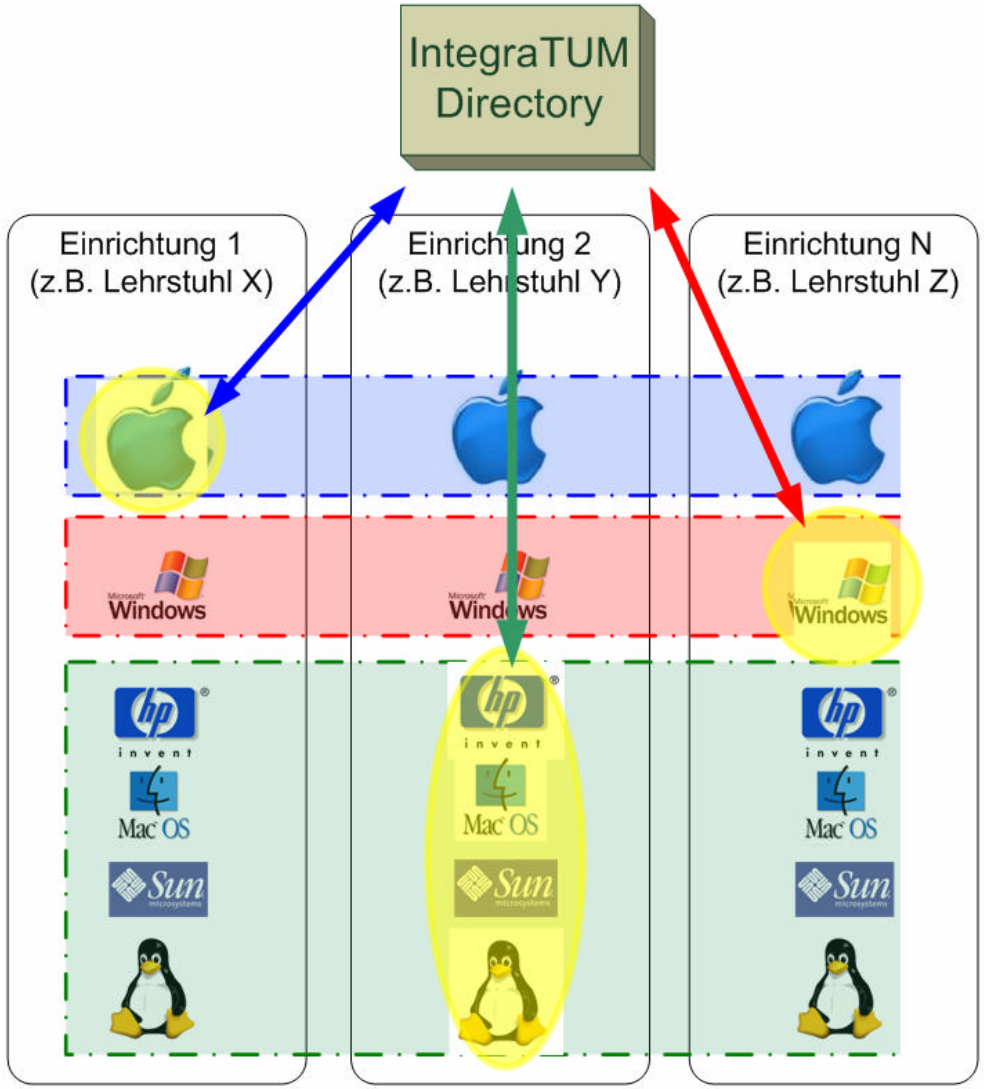
- nicht mehr benötigt oder
- zu kaufen sein wird

Provisioning-Skalierbarkeit

Anbindung von „Kompetenzzentren“ pro Fakultät und Betriebssystem-Gruppe

statt

Provisioning jedes einzelnen Rechnerpools/ Servers



Wissen erwerben und vermitteln

Probleme und Ist-Zustand verstehen:

- Bi- und multilaterale Gespräche
- Projektweite themenspezifische Workshops
  - Universitätsweite Gäste- und Gruppenverwaltung
  - Datenmodelle und Workflows
- Projektübergreifende Fragebogen-Aktionen

Ideen beschreiben und diskutieren:

- Missverständnisse ausräumen
- Vorteile aufzeigen
- Nachteile nicht verheimlichen

Wissen und Konzepte dokumentieren

- Ausführliche, vollständige und verständliche Dokumentationen erleichtern die Projektarbeit.

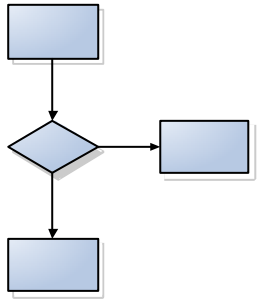
- „HowTo“-Dokumente für teaminternen und teilprojektübergreifenden Know-How-Transfer
  - Installation und Anwendung von OpenLDAP
  - Installation und Konfiguration von eDirectory
  - Umgang mit LDAPS/LDAP+TLS, OpenSSL und SSL-fähigen Java-Clients

- Schriftliche Dokumentation der Ist-Prozesse

Ziele:

- Erfassen, Verstehen und Dokumentieren der Ist-Prozesse
- Definition und Umsetzung von Soll-Prozessen

Prozess-Visualisierung:



- Flussdiagramme, Petri-Netze, ereignisgesteuerte Prozessketten, BPMN ?
- Wichtig ist der Inhalt, nicht die Auswahl vieler bunter Symbole!

Infrastruktur und Projektorganisation

Groupware:

- Mailingliste
- Ablagebereich auf Fileserver
- Subversion-Server
- MWN-weiter Gruppenkalender fehlt noch :-(

Organisation:

- Monatliche schriftliche Berichte
- Vier Vollversammlungen pro Jahr
- Workshops und projektweite Präsentationen bei Bedarf

Organisation und Erfahrungsaustausch

Organisation:

- Monatliche schriftliche Berichte
- Vier Vollversammlungen pro Jahr
- Workshops und interne Präsentationen bei Bedarf

Kooperation:

- Vielen Dank an alle Aktiven!
- Starkes Interesse an Kooperationen
  - Aktuell gesucht für Gespräche mit Herstellern: Anwender von SISIS und imc CLIX
- Unsere Konnektoren und Tools stehen auf Anfrage zur Verfügung

Zusammenfassung

- IntegraTUM ist noch am Anfang
- Vielversprechende Zwischenergebnisse
- Gemeinsame Probleme gemeinsam lösen – es bleiben genügend hochschulindividuelle übrig :-)
- Arbeitskreise sind wichtig!
- Arbeitsersparnis durch Vorarbeiten anderer
- Übertragbarkeit der IntegraTUM-Lösungen angestrebt