

# Identitätsmanagement als Baustein für ein gutes Campus Management

Campus Innovation Hamburg

20.11.2008

Dr. Rolf Borgeest, Technische Universität München

[rolf.borgeest@tum.de](mailto:rolf.borgeest@tum.de)

---

# Agenda

- Gutes Campus Management
- Ausgangslage, Kräfte
- Konsolidierung der Anwendungslandschaften
- Identity Management
  - Rechtevergabe / Entzug
  - Föderation / Shibboleth
- Besonderheiten an Hochschulen
- Fazit

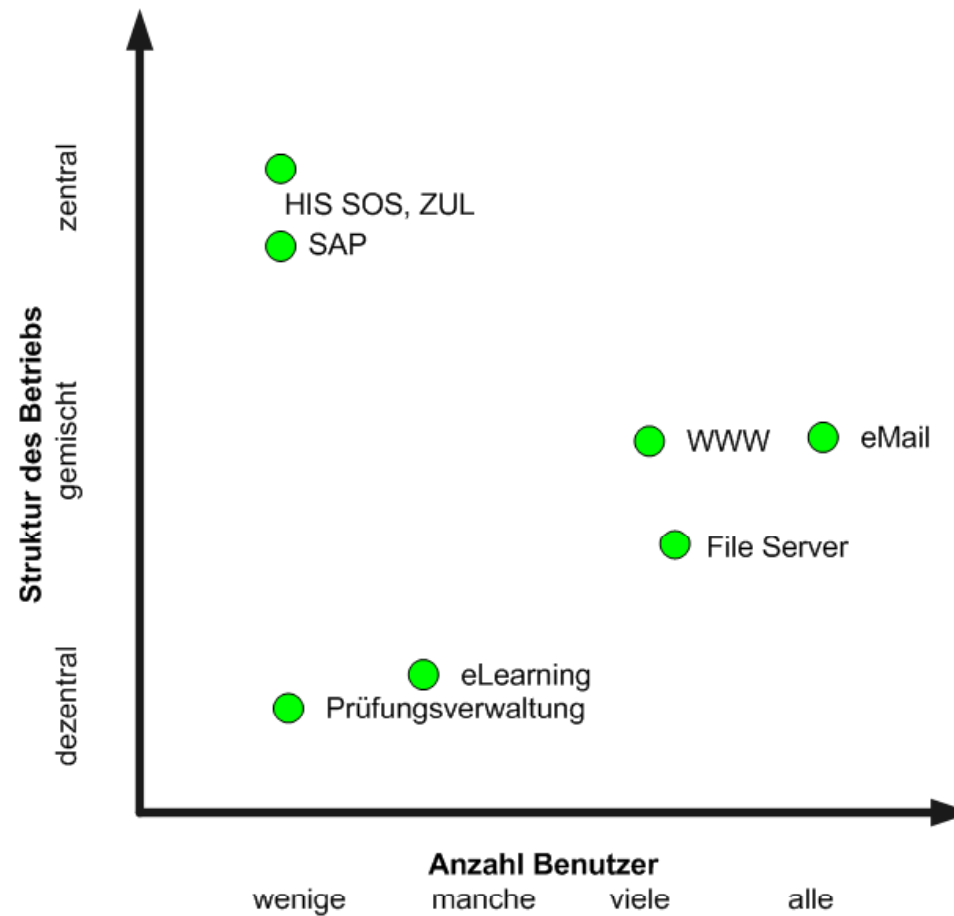
## Gutes Campus Management

- Verlässlich
- Sicher
- Transparent
- Einfach zu verstehen
- Durchgängig
- Webbasiert, vieles in Selbstbedienung zu erledigen
- Kein Selbstzweck
- Unterstützt die Mitglieder der Hochschule in
  - Studium
  - Lehre
  - Forschung
  - Verwaltung
- Begleitet die Mitglieder der Hochschule von Anfang bis Ende

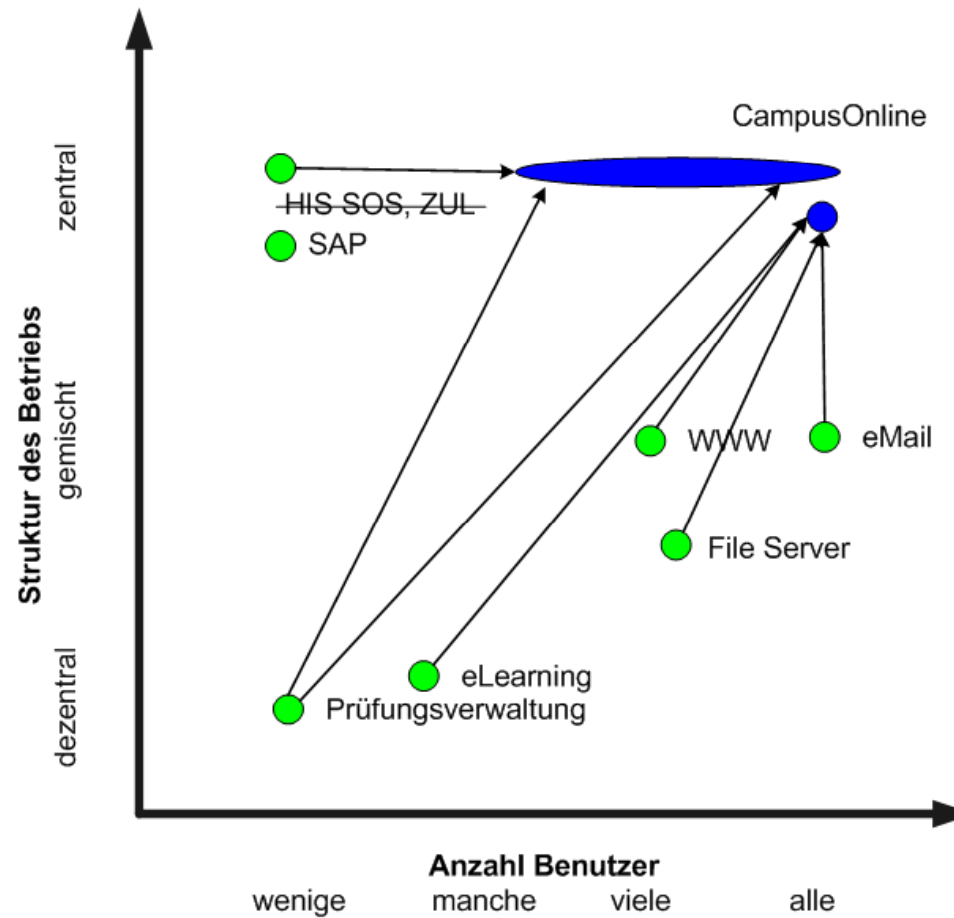
## Ausgangslage / Kräfte

- **Fachliche Aspekte**
  - Autonomie, Wettbewerb → Differenzierung durch gute Geschäftsprozesse, bei Auswahl von Studenten, Mitarbeitern
  - Bologna Prozess → Mehr Prüfungen, Höhere Fluktuation
  - Doppelte Abiturjahrgänge → Mehr Studenten
  - Geldknappheit, Lizenzierungsfragen → Zwang zu wirtschaftlichem Handeln
  - Gemeinsame Studiengänge, Organisationsübergreifende Zusammenarbeit → Föderationen
- **luK Aspekte**
  - Viele Dienste werden redundant angeboten
    - Gleiche Dienste mehrfach bzw. ähnlich Funktionalitäten in verschiedenen Anwendungen
    - Datenredundanz
  - Oftmals kleinteilige Organisation, Missbrauch von Wissenschaftlern als Systemadministratoren
  - Hohe, versteckte Aufwände
  - Rezentralisierung, Konsolidierung naheliegend

# Konsolidierung der Anwendungen



# Konsolidierung der Anwendungen



# Die Sicht des Studenten



Student Card



Intranet



Vorlesungsverzeichnis



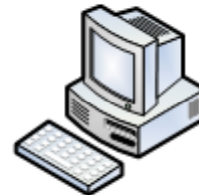
Prüfungsanmeldung



Fileserver



WLAN Zugang



CIP Pool



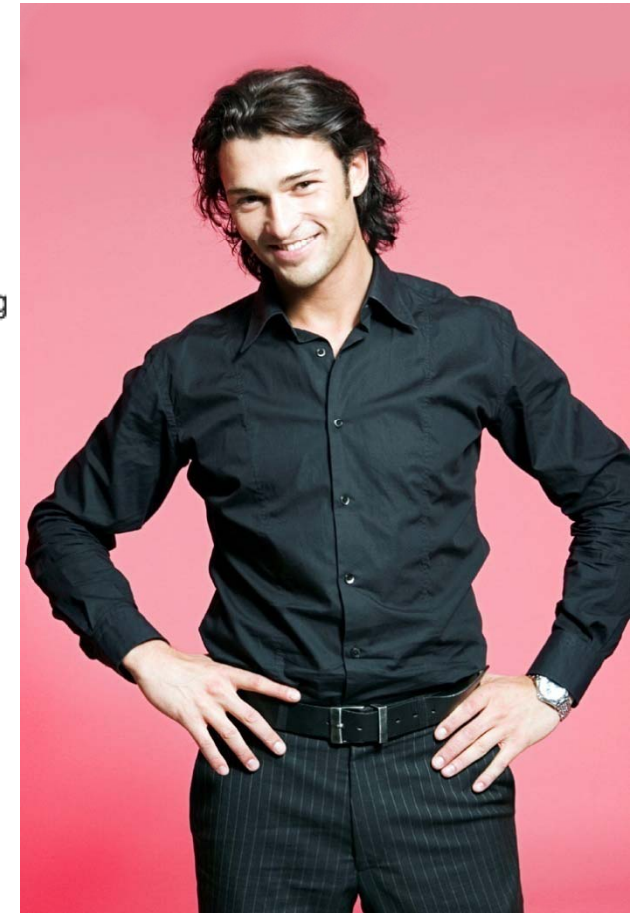
Mailserver



eLearning



Druckserver

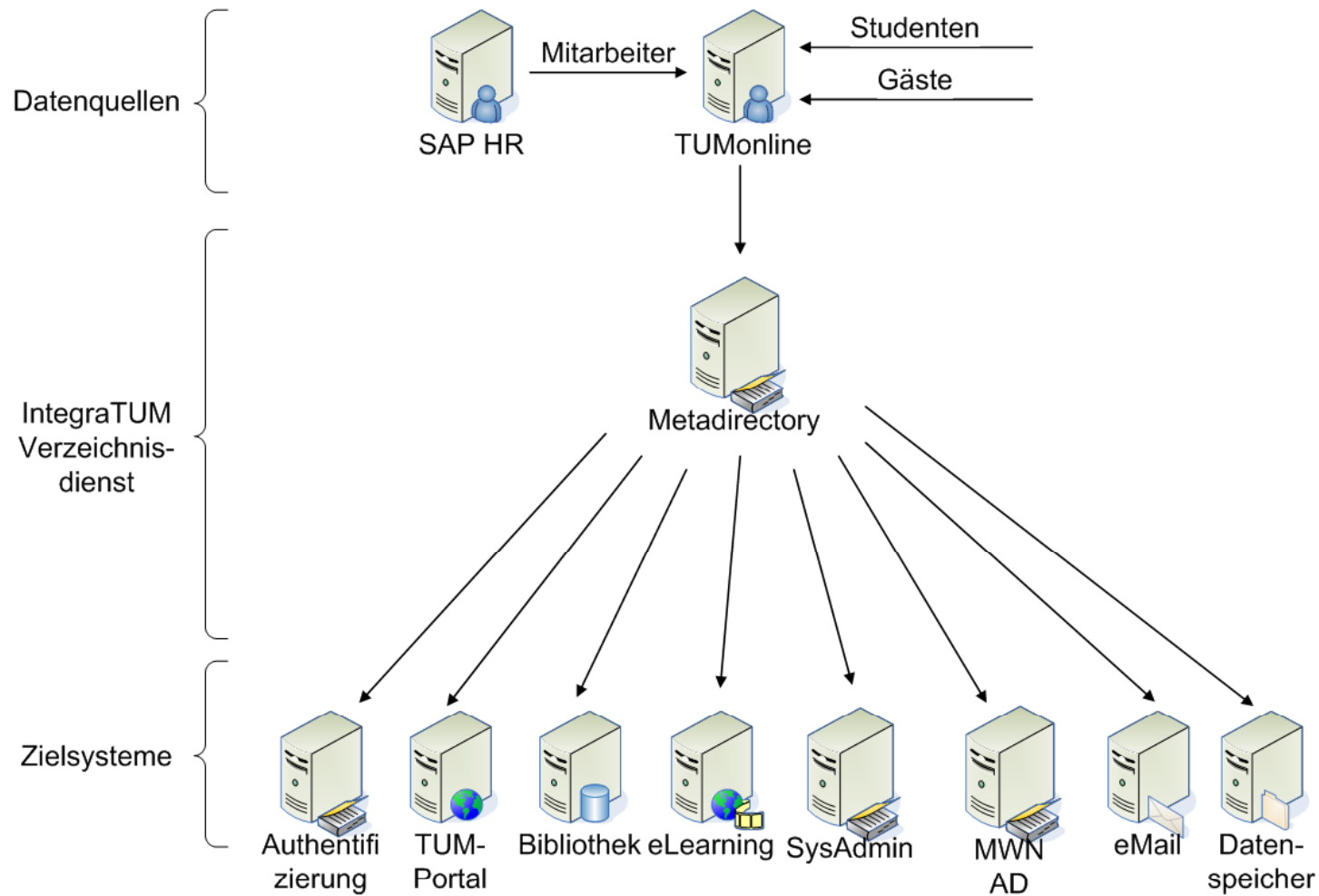


- Viele verschiedene Ansprechpartner
- Viele verschiedene Kennungen, Passwörter

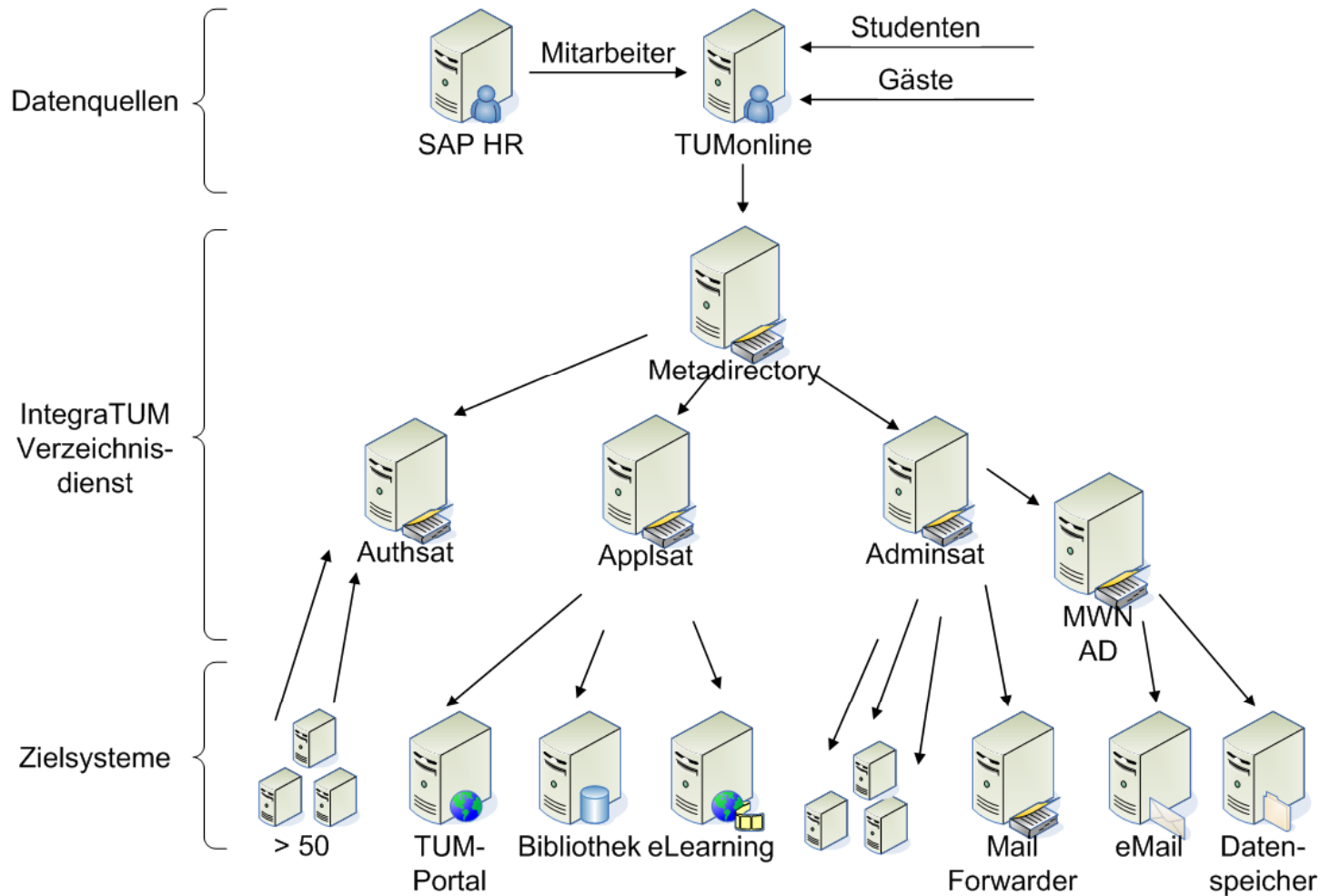
# Identity Management

- **Bestandteile**
  - Identifizierung / Authentifizierung - wer bist Du? / bist Du es wirklich?
  - Autorisierung – was darfst Du?
- **Bereitstellung eines**
  - zentralen, immer aktuellen, autoritativen**Datenbestands von Mitarbeitern, Studenten und Gästen**
- **(De-)Provisionierung von Diensten:**
  - Automatisierung der Benutzerverwaltungen
  - Einspeisung im der benötigten Daten, z.T. über eigene Schnittstellen, eigene Formate
  - Löschung der eingerichteten Rechte und Accounts sobald nicht mehr benötigt
- **Orientierung an den universitären Geschäftsprozesse**
  - z.B. Bewerbung, Immatrikulation, Exmatrikulation
- **Bereitstellung eines „Unified Login“**
  - Für alle benötigten Dienste
  - Mit passenden Rechten

# Identity Management – prinzipieller Aufbau



# Identity Management – etwas genauer



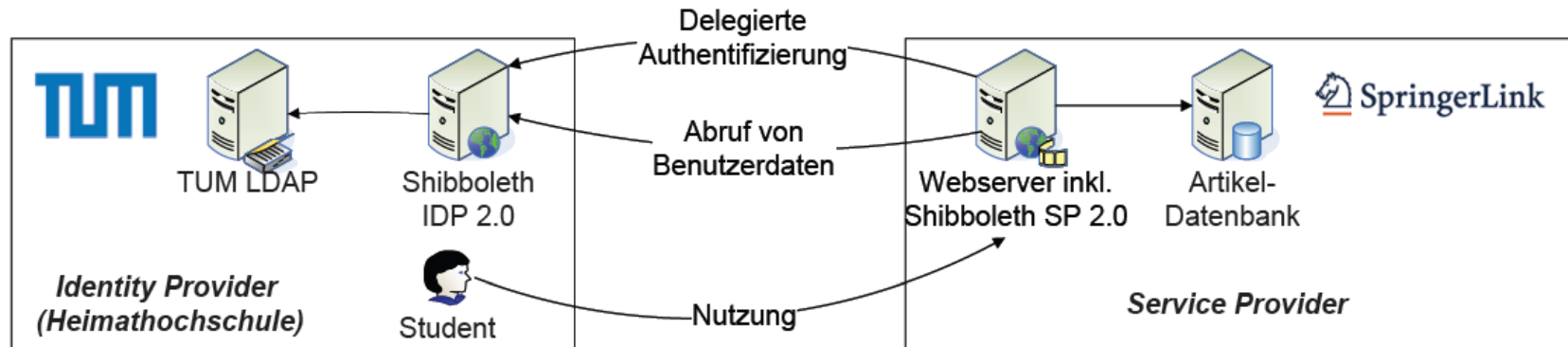
## Vergabe von Rechten / Autorisierung

- Automatische Versorgung mit Basisdiensten
  - Zugang zum Campus Management (z.B. Prüfungsanmeldung, Noteneinsicht (Studierende), Selfservices (alle))
  - eMail
  - eLearning
  - Persönlicher Speicher
  - Zugang elektronische Zeitschriften
  - Bibliotheksausweis
  - Auf Basis sehr grober Nutzerklassifikation
- Feinere Rechte entweder
  - Auf Basis von (automatisierten) Gruppen
  - Oder in den nachgelagerten Systemen
  - Jeweils in delegierter Administration
- Attribute der Quellsysteme zur Rechtevergabe nur eingeschränkt nutzbar
  - z.B. Kostenstelle nicht immer Spiegel der echten Organisationszugehörigkeit

## Entzug von Rechten

- Grundsätzlich enden alle Rechte mit
  - Exmatrikulation
  - Vertragsende
  - Ablauf eines Gaststatus
  - Karrenzeiten einstellbar, sofortiger Entzug muss ebenfalls möglich sein (bei Missbrauch)
  - Ausnahme: Erhalt der eMail Adresse für Alumni (Weiterleitung)
- Entzug von speziellen Rechten
  - Änderung von Gruppenzugehörigkeiten
  - Im nachgelagerten System

## Single Sign-On / Föderation / Shibboleth



Verlässliches Identity Management gestattet einfache Kooperation mit anderen Organisationen

- Technische Umsetzung: Shibboleth, speziell DFN-AAI
- Passwörter bleiben in der eigenen Organisation
- Öffnung eigener Dienste nach außen nach Belieben
- Auch lokal nutzbar
- Beispiele: springerlink.com, Microsoft Dreamspark
- Nur für webbasierte Dienste, jeweils Anpassungen nötig
- Begrenzte Semantik der Verfügbaren Daten (Org.zugehörigkeit, Mitarbeiter, Student); Erweiterungen (z.B. Studiengang) unterwegs

## Besonderheiten an Hochschulen

- Teilweise andere Datenquellen
  - Personalverwaltung (SAP HR)
  - Studierendenverwaltung (HIS SOS bzw. CAMPUSonline)
  - Gäste
  - Alumni
- Doppelrollen
  - Wissenschaftlicher Mitarbeiter ist zugleich Alumnus und Promotionsstudent
- Hohe Fluktuation
- Wer ist eigentlich Mitglied der Hochschule?
  - Studierende (im Vorkurs)
  - Studierende aus anderen Hochschulen im Rahmen gemeinsamer Studiengänge
  - Mitarbeiter
  - Gäste (Gastdozenten, Gastwissenschaftler, Stipendiaten, Mitarbeiter externer Firmen, Stadtbenutzer der Bibliothek...)
  - Mitarbeiter der Medizin (zumeist Klinikangestellte einer eigenen GmbH)
  - Alumni (wie erfolgreich muss ein Student sein, um Alumnus zu werden?)
  - Emeriti

## Datenschutz und Datensicherheit

- Sozial / Psychologisch
  - Frühe Einbeziehung von Datenschutzbeauftragten, Personalrat, Studierendenvertretern
  - Offene, ehrliche Kommunikation
- Gesetzlich
  - Gute Deckung durch BayHSchG (§42(4) (Studentendaten) §2(5) Alumni, §55(2) eLearning, IuK Unterstützung der Lehre)
  - Datenschuttfreigaben für
    - Verzeichnisdienst
    - Jeden einzelnen Zugriff auf Verzeichnisdienst (außer Authentifizierung)
- Fachlich - Datensparsamkeit!
- Technisch
  - Zentrale Systeme besser schützbar als dezentrale
  - Gefahren durch breite Nutzung Unified Login sind beherrschbar
    - Verwendung von SSL Protokollen Client → Server
    - Dezidiert abgesicherte SSL Protokolle Server ← → Server
    - Restriktive Vergabe von Leserrechten (nur für ausgewählte Attribute des sich anmeldenden Benutzers)

## Aspekte bei der Einführung

- **Alle Mitglieder betroffen**
  - Information der Nutzer
  - Ängsten begegnen
  - Support sicher stellen
- **Viele Einheiten betroffen**
  - Personalabteilung, Studiensekretariat, Fakultäten mit eigenen Kulturen
  - Gemeinsame Sprache / Domänen finden
    - Organisationsbezeichner
    - Studiengangsbezeichner
    - Aufgabenverteilung
  - Gelegenheit zur Geschäftsprozessmodellierung / Reengineering nutzen
- **Nach- und Neunutzung vorhandener Daten**
  - Datenqualität entspricht immer nur der aktuellen Nutzung
  - Attributnamen können irreführend sein
  - Anfänglich hohe Aufwände zur Datenkonsolidierung, Grundbedarf bleibt → „Identity Manager“
- **Änderungen im laufenden Betrieb – sorgfältige Planung, Test nötig**

## Fazit

- Identity Management ist die Voraussetzung für zentral bereit gestellte Dienste am Campus
- Begleitet das Mitglied der Hochschule von Anfang bis Ende
- Einführung aufwändig
- Notwendige Konsolidierung von
  - Prozessen
  - Systemen
  - Daten
- Vorteile
  - Schnelle Versorgung von neuen Mitarbeitern, Studenten mit allen nötigen Diensten
  - Reduktion der Anlaufschwierigkeiten für „Neue“
  - Reduktion der Administrationsaufwände
  - Verbesserung der Datenqualitäten
  - Besseres Campus Management