

# ZKI Workshop Verzeichnisdienste

---

Fachhochschule Köln

10. Juli 2003

**Dr. Werner Degenhardt, Armin Prosch**

LMU München, Referat Internet, <http://www.lmu.de/internet>

- Meta-Directory, warum?
- Directory Design Roadmap
- Anforderungsanalyse
- Datendesign
- Schemata
- Datenschutz und Datensicherheit

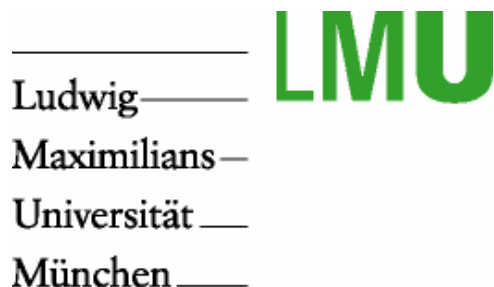


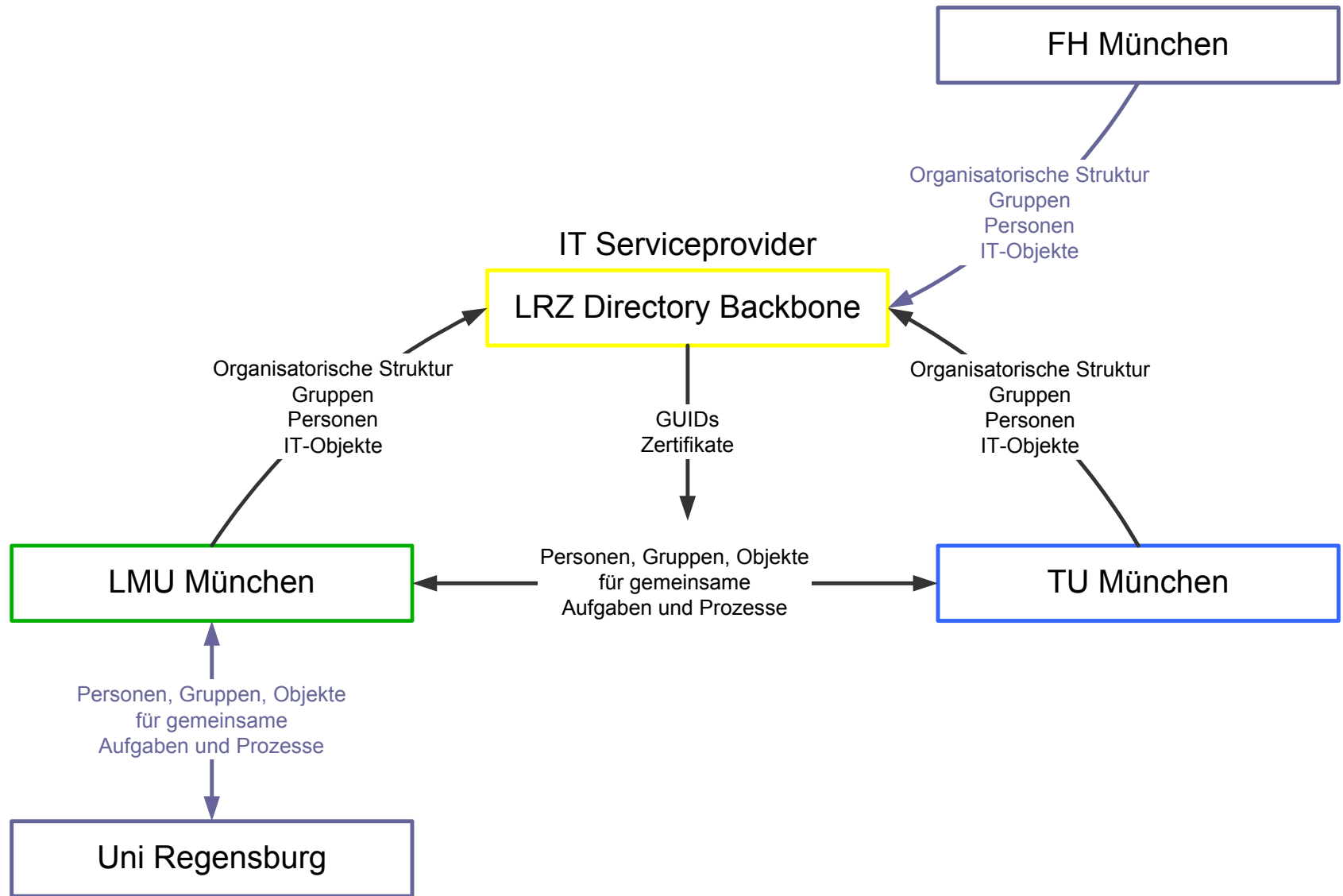
## Status-Quo

- gemeinsame Personen
- gemeinsame Prozesse
- gemeinsame Aufgaben
- gemeinsamer IT Provider

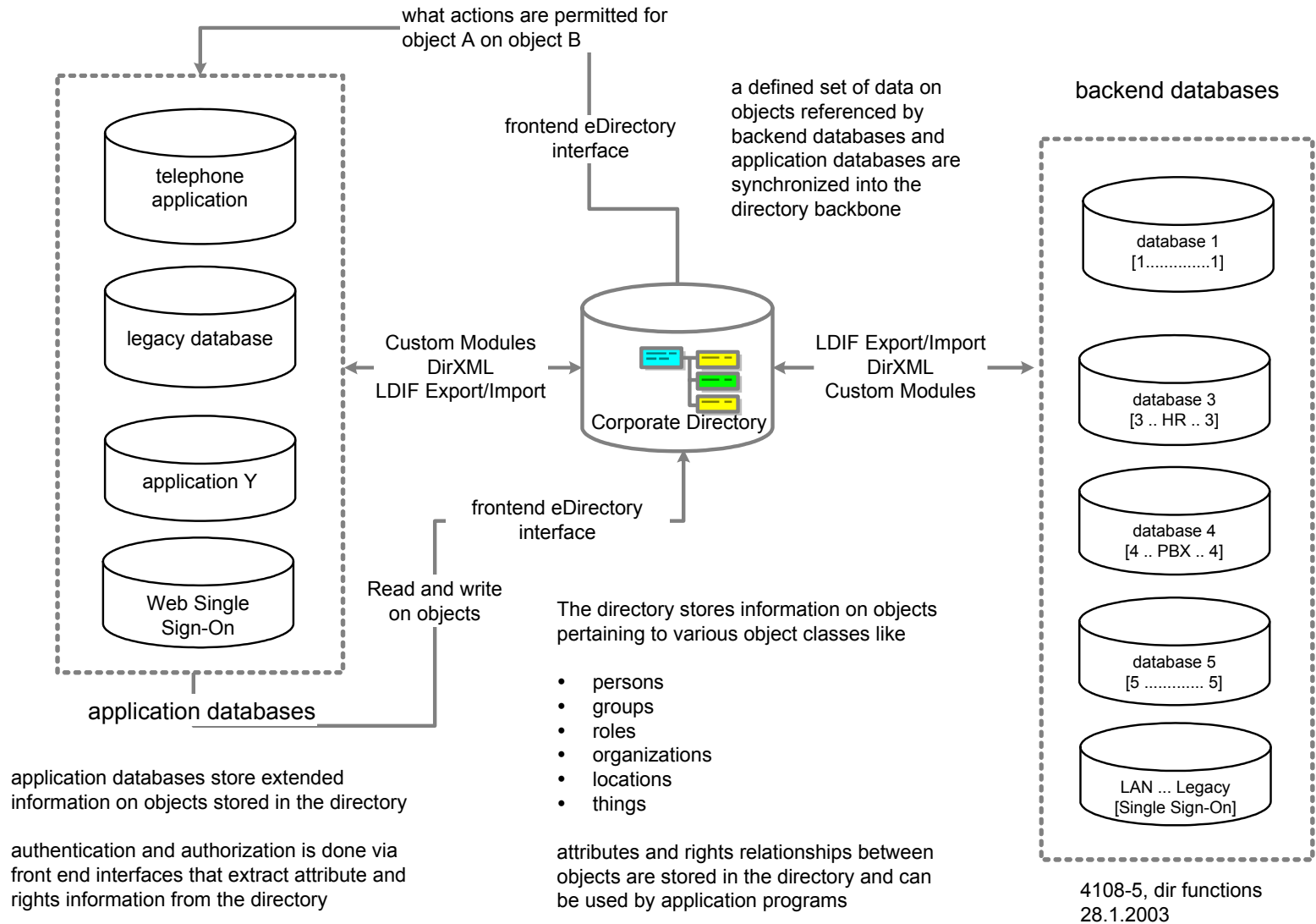
## Konsequenz

- Überschneidung in Kunden und Technik





# Identity Management



## Phasen

- Phasen im Design eines Directory-Service
  - Anforderungsanalyse
  - Datendesign
  - Data Policy Statement
  - Datenaustauschbeziehungen
  - Schema Design
  - Replikation
  - Sicherheit

## Weshalb ein Directory ?

- **A**uthentisierung
  - Authentisierung Portal
  - Single Sign-On
- **A**utorisierung
  - Single Sign-On
  - Autorisierung Portal
- **A**dministration
  - Outsourcing Mail zum IT-Provider
  - Organisationsübergreifende Benutzerverwaltung
  - Adressbuch

## Authentisierung am Portal

# Campus<sup>LMU</sup>

Anmeldung

Login:

Passwort:

**In den Eigenschaften Ihres Browsers müssen  
Cookies aktiviert sein.**



ludwig.maximilian

Logout

Modulauswahl

Anfragen

Neue Anfrage  
Anfrage verfolgen  
Anfragen zuordnen

Service

Feedback  
Campus Zugang  
Kontakt  
helpdesk-FAQs

Administration

Verwaltung

Anfragen verfolgen

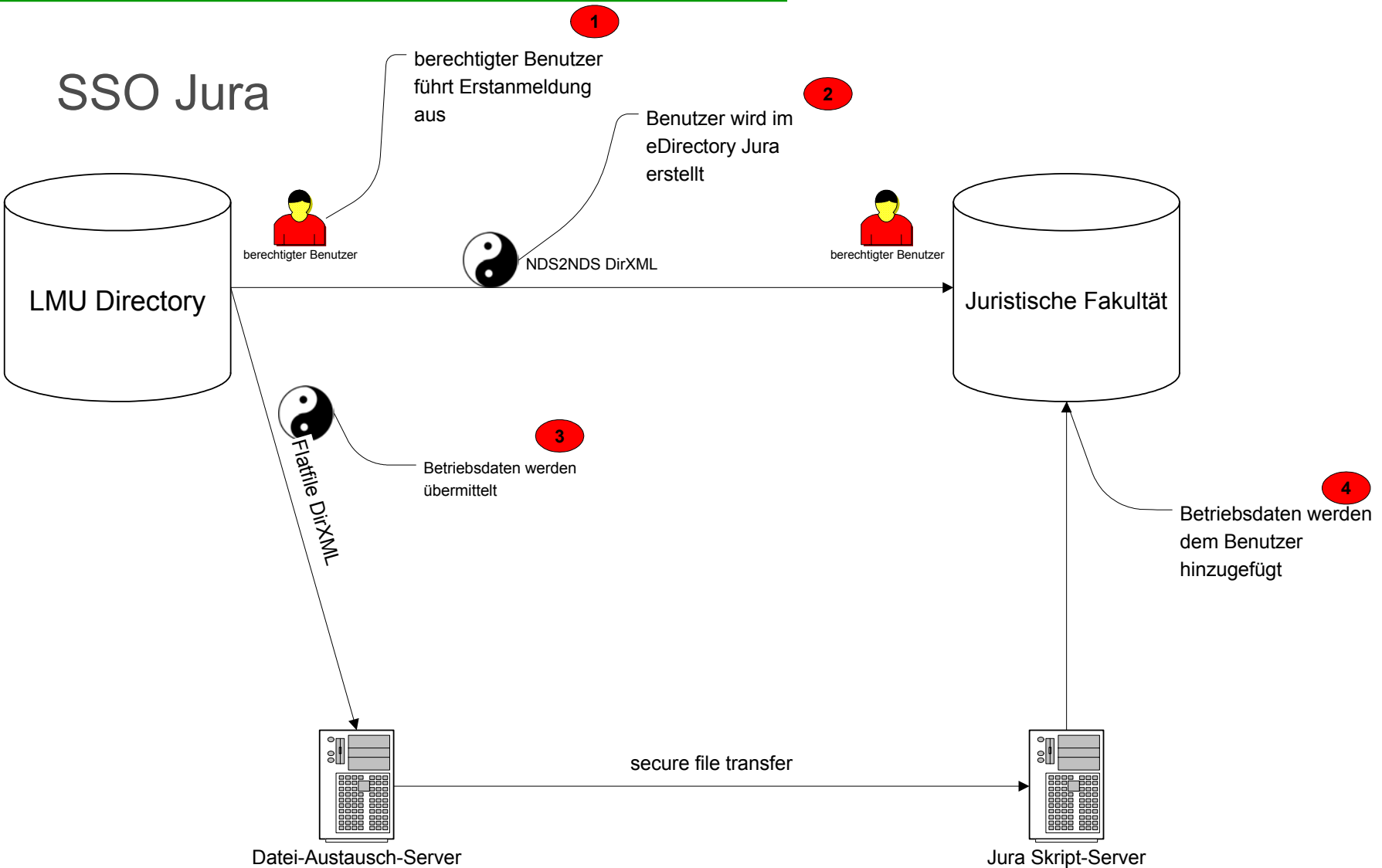
Ludwig Maximilian (ludwig.maximilian): Anfragen an das CampusLMU helpdesk

Suche nach:

Ihre Anfragen

| ID    | Eingang          | Thema                            | Status        |
|-------|------------------|----------------------------------|---------------|
| 12068 | 22.3.2001, 09:25 | Studienberatung und Fachberatung | abgeschlossen |
| 12076 | 22.3.2001, 10:20 | Proseminar II                    | abgeschlossen |
| 12245 | 26.3.2001, 15:21 | Login                            | abgeschlossen |
| 14218 | 3.5.2001, 11:51  | Passwort                         | abgeschlossen |
| 14223 | 3.5.2001, 13:02  | Behindertenhilfe                 | abgeschlossen |

# Anforderung: Single Sign-On

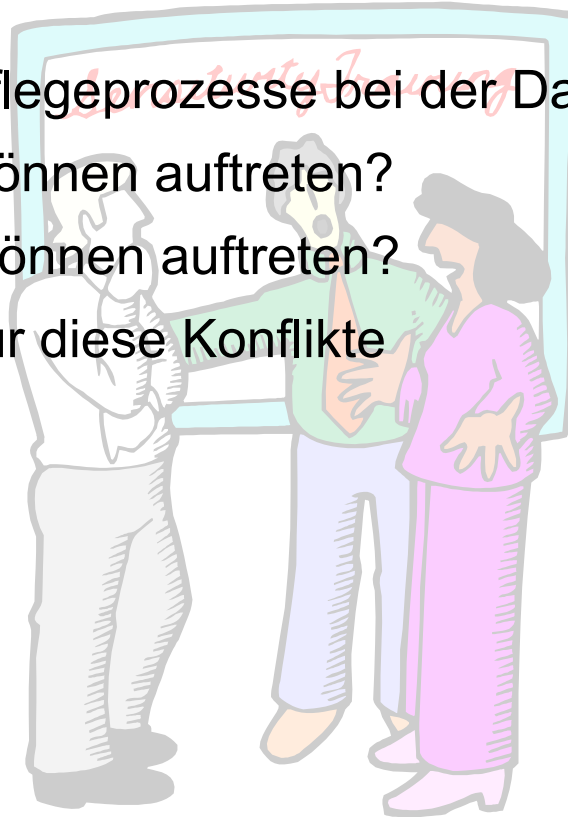


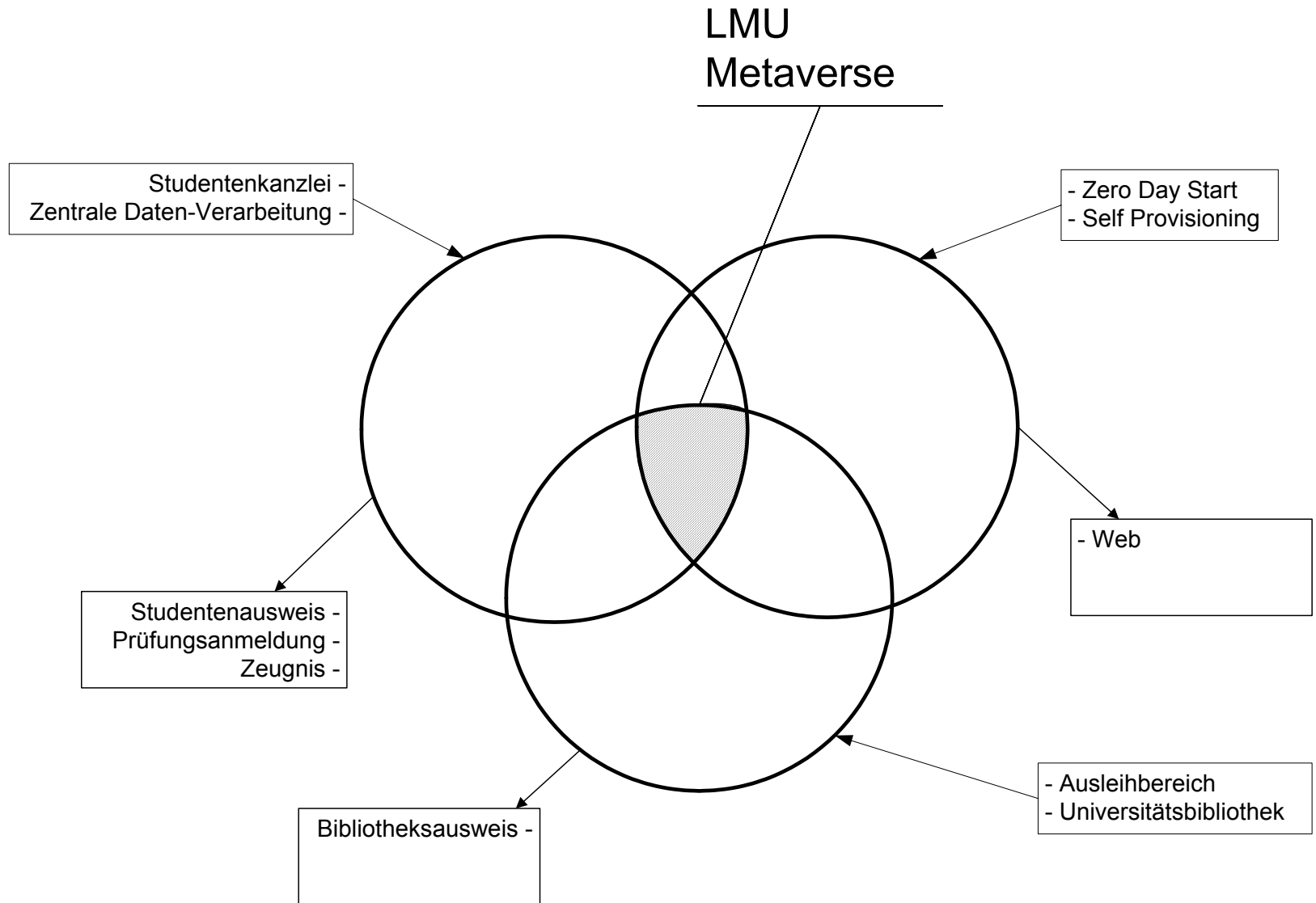
## Datenquelle → Directory → Datenziel

- Aufstellen der Erzeuger / der Verbraucher für jedes
  - Objekt
  - Attribut
  - Datenelement

## Data Policy Statement

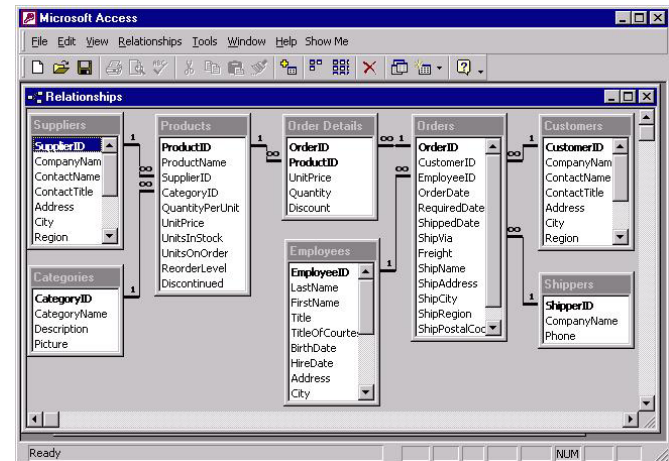
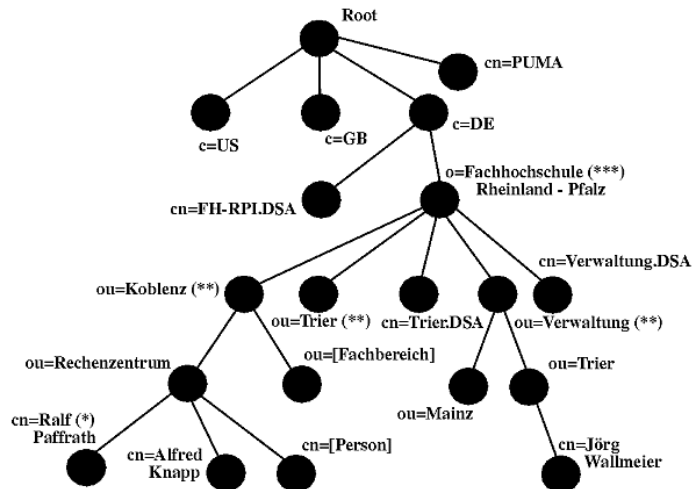
- Dateneigner, Einpflegeprozesse bei der Datenquelle
- Welche Formate können auftreten?
- Welche Konflikte können auftreten?
- Lösungsansätze für diese Konflikte

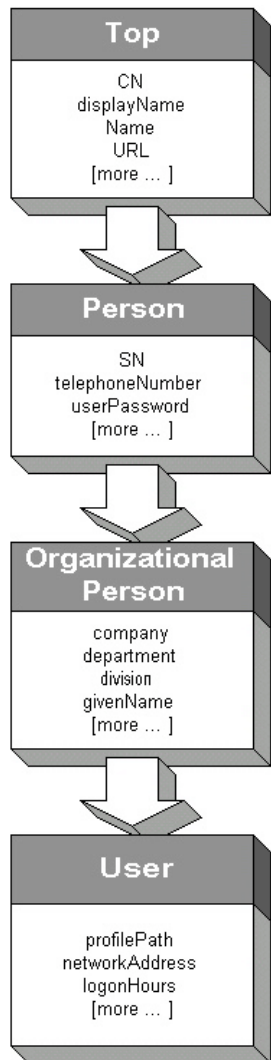




# Schema: Directory vs relationale Datenbank

| Directory                     | Relationale Datenbank    |
|-------------------------------|--------------------------|
| Datenbank                     | Datenbank                |
| objektorientiert-hierarchisch | (objekt)relational       |
| mehr lesen als schreiben      | mehr schreiben als lesen |
| „loosely consistent“          | Transaktionssicherheit   |





## Objektorientierung im X.500 Directory

- Jedes Objekt im Directory ist Instanz einer Klasse
- Die Klasse beschreibt die für ein Objekt verfügbaren Attribute
- Klassen erben ihre Eigenschaft von Super-Klassen
- Objekte
  - Container (O, OU, C, T, Group)
  - Leaf

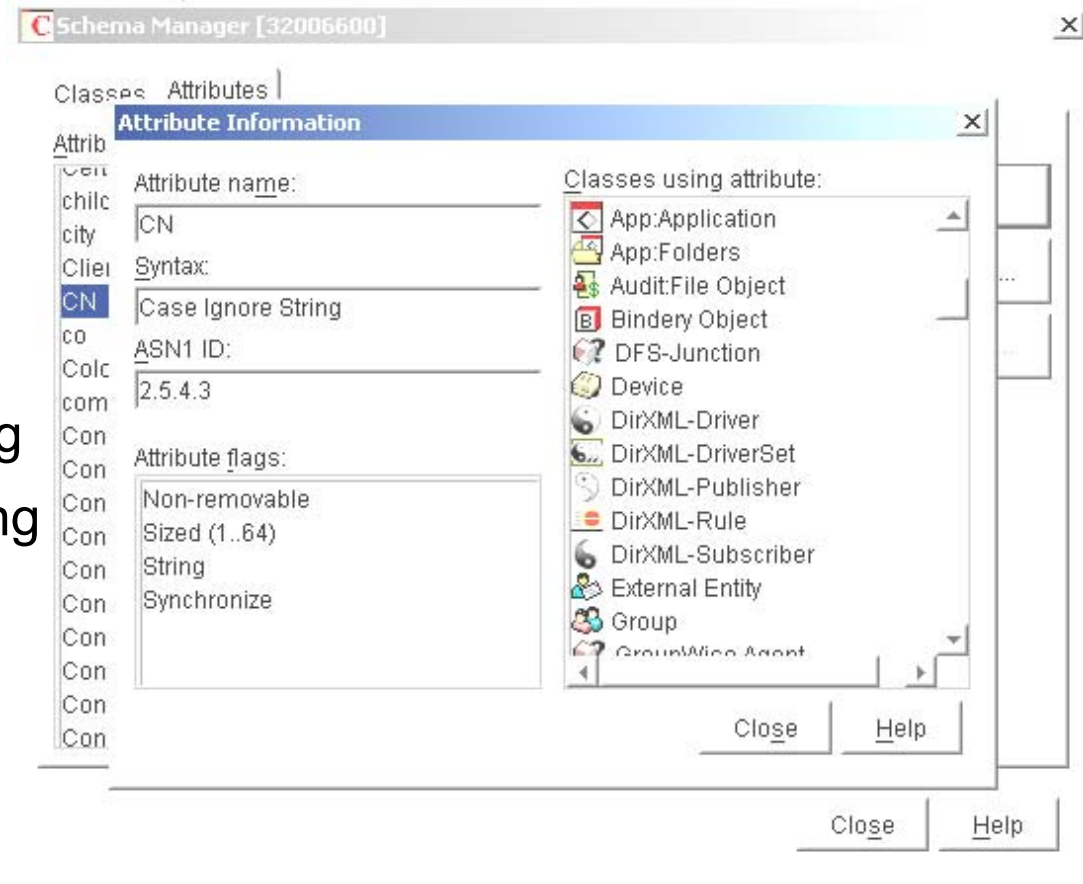
# Rechteverwaltung im eDirectory

- ACLs bis auf Attributebene
- Trustee
- Security Equals to
- Inherited Rights Filter
- Object Rights
  - Browse
  - Create
  - Rename
  - Supervisor
- Attribute Rights
  - Compare
  - Read
  - Write
  - Add-Self
  - Supervisor



# Schema Komponenten

- Object Class
- Attribute Type
- Attribute Syntax
  - Boolean
  - Case Exact String
  - Case Ignore String
  - Class Name
  - Integer
  - Timestamp
  - [...]



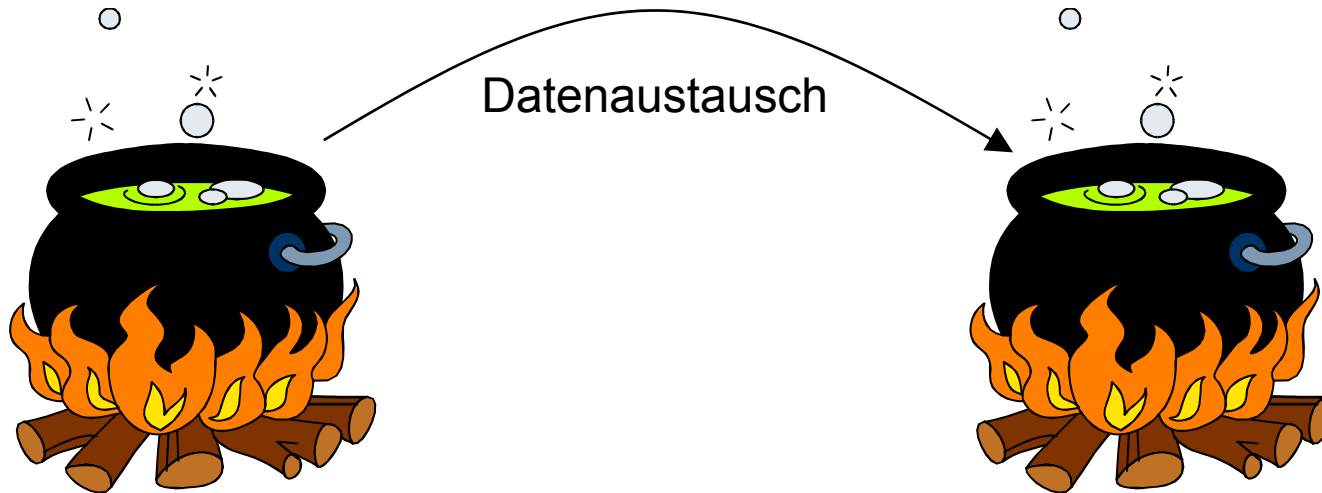
## Schema Klassen

- Name ImuPerson
- ASN.1 (Abstract Syntax Notation) 2.16.840.1.113719.2.206.0
- Typ
  - effective
  - abstract
  - auxiliary ✓
- Merkmale
  - mandatory
  - optional
  - naming

## Datenbank Struktur

- Strukturregeln
  - z.B. Verwendung von Auxiliary Classes
  - einheitliche Namensgebung für Attribute
- Container
- Leaf
- Flacher Namensraum vs. Hierarchie
- Gruppen
  - für die Zuordnung von Ressourcen
  - für die Zuordnung von ACLs
  - für die Abbildung von Hierarchien

Jeder soll sein eigenes Söppchen kochen!

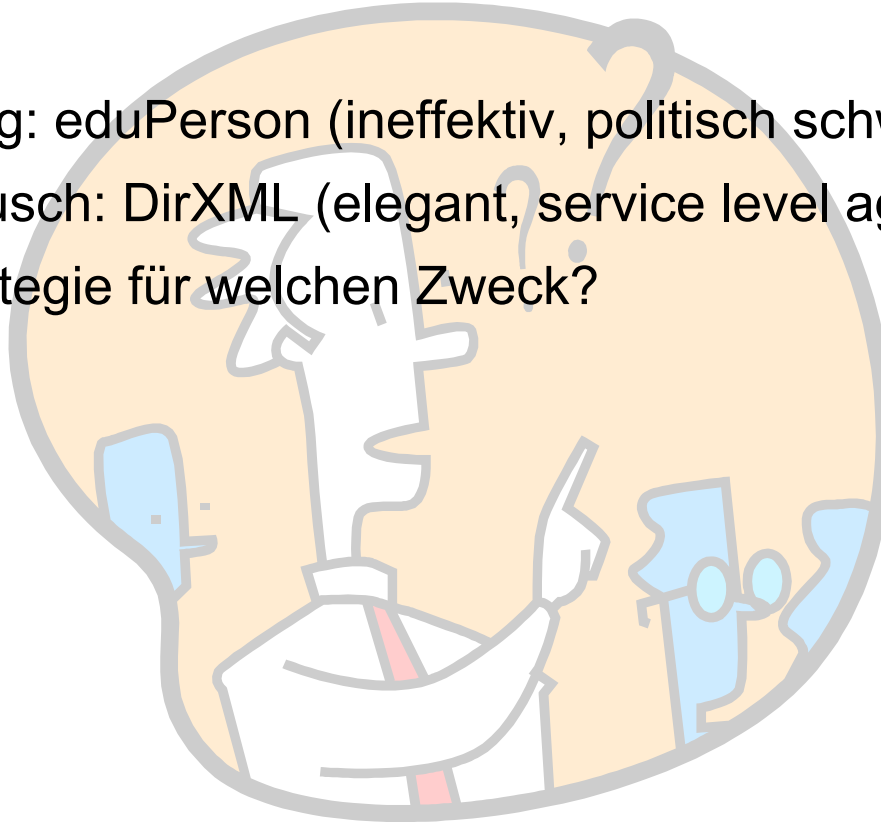


## Konsequenz

- Datenaustausch
- Zugriff über LDAP / NAM
- Keine föderierten Bäume

## Diskussion


- Datenhaltung: eduPerson (ineffektiv, politisch schwierig)
- Datenaustausch: DirXML (elegant, service level agreement)
- Welche Strategie für welchen Zweck?






- Herstellen von Vertrauen
  - Personen (Zugriff Dritter auf Personendaten)
  - Daten
    - Richtigkeit und Aktualität
    - Sicherheit
- Certificate Authority – dezentrale Datenpflege
- Datenschutz heißt auch: Datensicherheit beim Austauschpartner fordern

- Dienstvereinbarung mit dem Personalrat
- Informationelle Selbstbestimmung
  - gespeicherte Daten einsehen (Speicherung)
  - Freigabe zur Einsicht aktivieren und deaktivieren (Verwendung)
  - Übertragung in andere Datenbanken aktivieren und deaktivieren (Weitergabe)


## Profile, Gruppen, Freigaben

**mein profil**

ludwig.maximilian

Logout   

Campus<sup>LMU</sup>

Modulauswahl 

**Profilbereiche**

Meine Daten

**Personensuche**

Detailsuche

**Service**

Online-Hilfe  
Helpdesk  
Feedback

Daten anzeigen


Daten ändern

Freigabe verwalten


Gruppen verwalten

**Meine Daten - Anzeigen**

Welchen Datenbereich wollen Sie anzeigen?



Personendaten und Erreichbarkeit  
(z.B. Anschrift, Telefonnummer, etc.)



Studiendaten und Hobbys  
(z.B. Nebenfach, Hobbys, etc.)

Erstellt und betreut vom [Referat Internet und Virtuelle Hochschule](#)



## Backup

- `dsrepair.dib` bzw. DSDUMP
- Replikation
- LDIF
- Datenaustausch
- „normales Backup“
  - TSA-NDS
  - iManager
  - eMTool (Backup eDirectory Management Tool) *seit v. 8.7*



## physikalisch

- Nutzergemeinde
- Zugang zu dem Directory
- Netzwerkumgebung, Netzwerktopologie

## technisch

- Zugriffskontrolle / Authentisierung
  - ACLs
  - Anonymous
  - Simple password
  - Simple password over SSL
  - certificate authentication over SSL
  - SASL (Simple Authentication and Security Layer)

## Problematik

- Datenschutz
- Sicherheit
- Schutz vor Sniffen

## Datenaustausch

- PGP
- SSL

## Daten

- Secret Store
- Eigene Verschlüsselungsverfahren



Referat Internet

Oettingenstrasse 67

80538 München

Tel. +49 (0)89 2102 5979

Fax: +49 (0)89 2102 5980

# Questions & Answers

## Questions & Answers

[www.lmu.de/internet](http://www.lmu.de/internet)

[helpdesk@campus.lmu.de](mailto:helpdesk@campus.lmu.de)

