

Identity Management im Münchner Wissenschafts-Netz:

Aktueller Stand der Projekte IntegraTUM und LRZ-SIM

ZKI-AK Verzeichnisdienste, 11. Oktober 2007
Wolfgang Hommel, Leibniz-Rechenzentrum

Übersicht

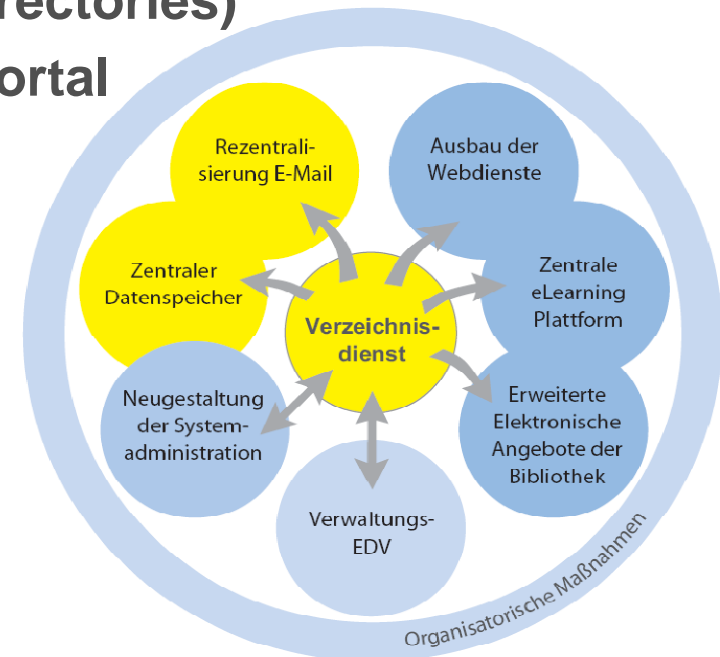
- DFG-Projekt IntegraTUM
 - **Aktuelle IM-Architektur**
 - **Schemavariationen**
 - **Gruppenverwaltung**
 - **Prozessanpassungen**
- Identity Management am LRZ
 - **Realisierte IM-Architektur**
 - **Werkzeuge zur Migration und Administration**
- Shibboleth-Aktivitäten
 - **Shibboleth an LMU und TUM**
 - **Shibboleth im Rahmen der Virtuellen Hochschule Bayern (vhb)**

Übersicht

- DFG-Projekt IntegraTUM
 - Aktuelle IM-Architektur
 - Schemavariationen
 - Gruppenverwaltung
 - Prozessanpassungen
- Identity Management am LRZ
 - Realisierte IM-Architektur
 - Werkzeuge zur Migration und Administration
- Shibboleth-Aktivitäten
 - Shibboleth an LMU und TUM
 - Shibboleth im Rahmen der Virtuellen Hochschule Bayern (vhb)

Rekapitulation: Ausgewählte IntegraTUM-Projektziele

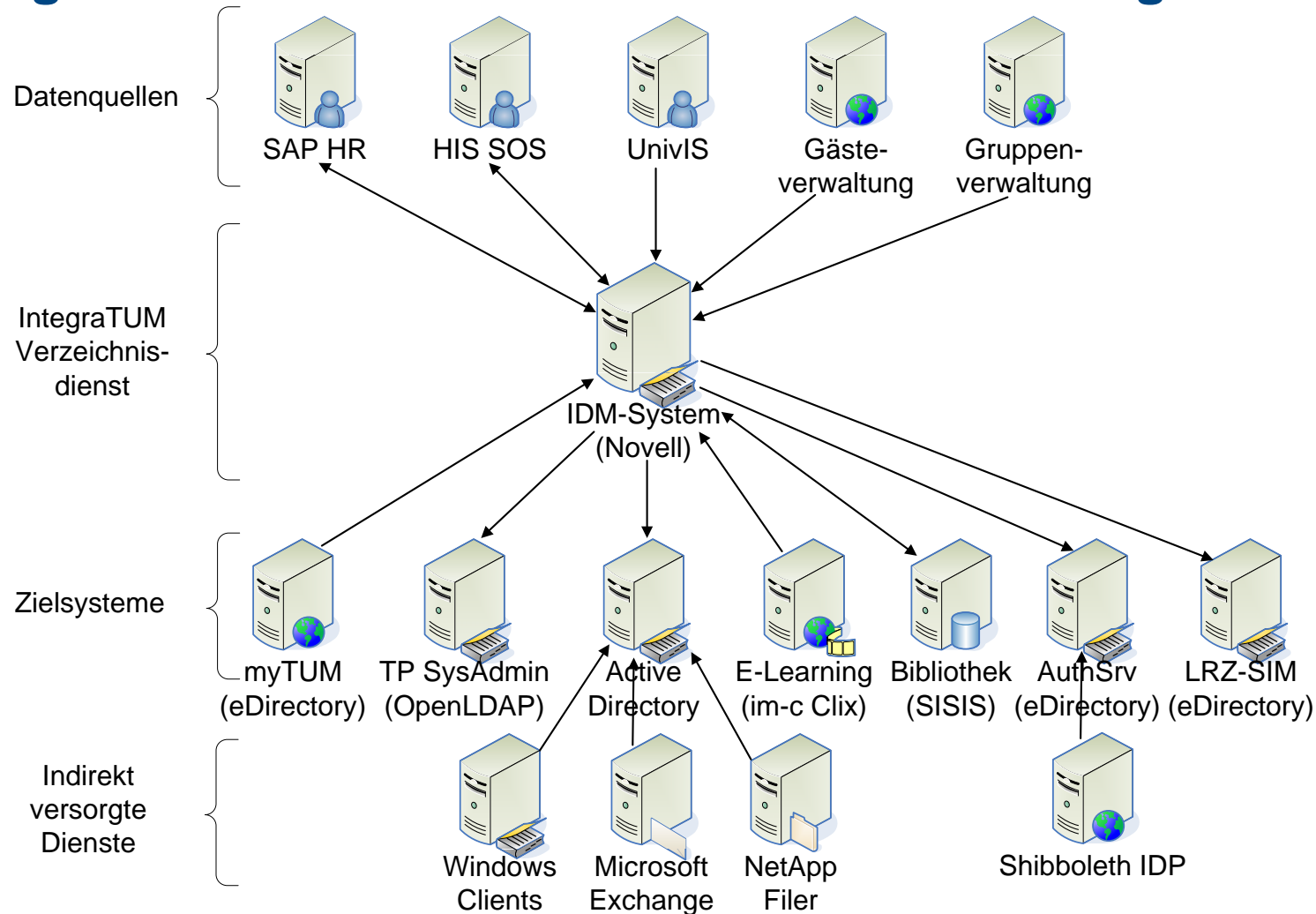
- Rezentralisierter Betrieb, dezentrale Administration
 - Mail-Server und Groupware
 - File-Server (Projektablagen, Home-Directories)
 - Web-Content Migration ins myTUM-Portal
- Ausbau elektronischer Dienste
 - E-Learning
 - Bibliotheksdienste
- Integration durch hochschulprozess-orientiertes Identity Management



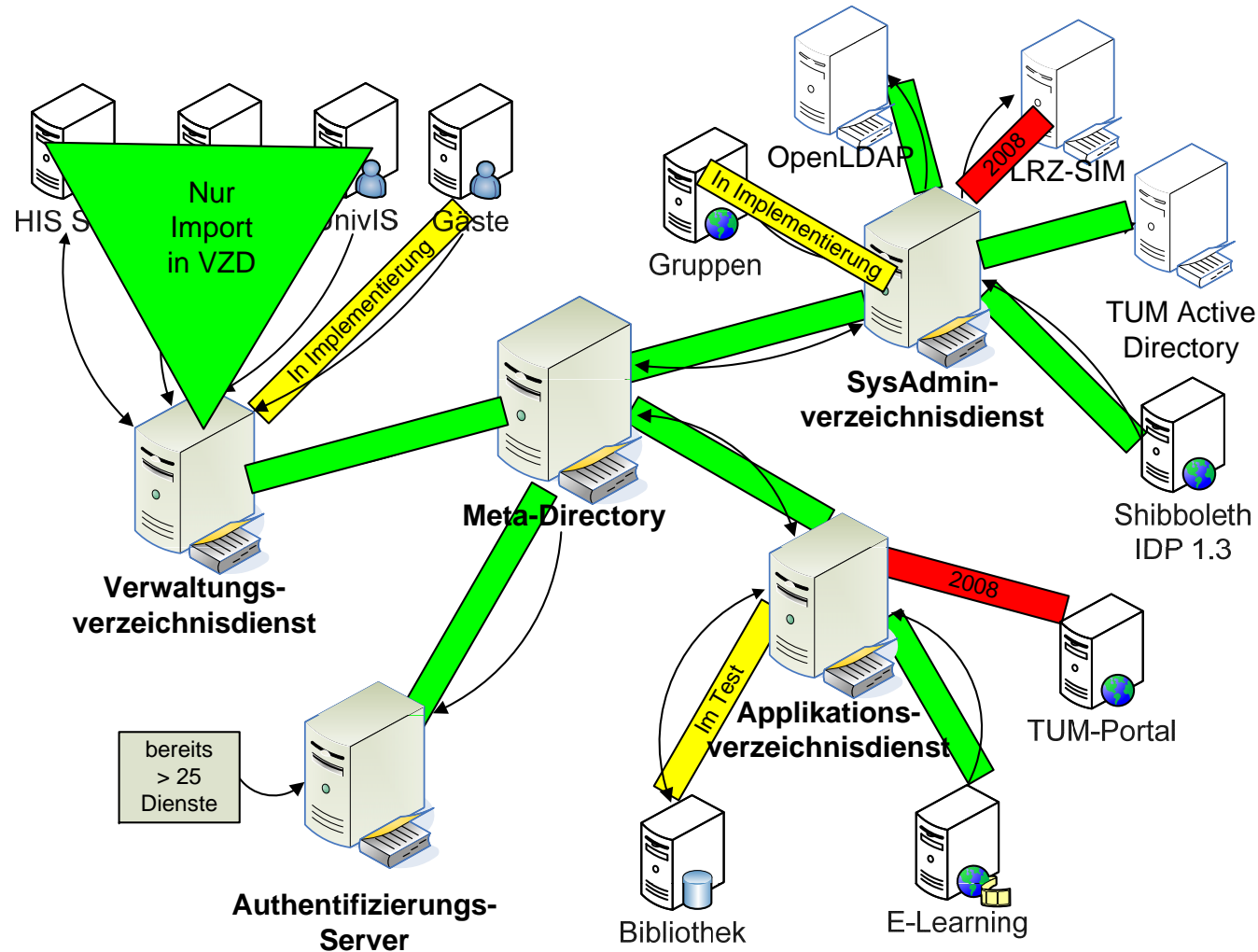
IntegraTUM: Eckdaten

- Projektlaufzeit 5 Jahre
 - Formal seit 07/2004
 - Real seit 02/2005
 - DFG-Begehung zur „Halbzeit“ erfolgreich
- Teilprojekt Verzeichnisdienst
 - 4 Projektstellen (je zur Hälfte DFG-/TUM-finanziert) am LRZ
 - Aufbau der Identity Management Infrastruktur
 - Mitwirken am TUM-weiten Deployment
 - Dauerhafter Betrieb am LRZ sichergestellt

IntegraTUM IM-Architektur: Aktuelle Zielsetzung



IntegraTUM IM-Architektur: Realisierung



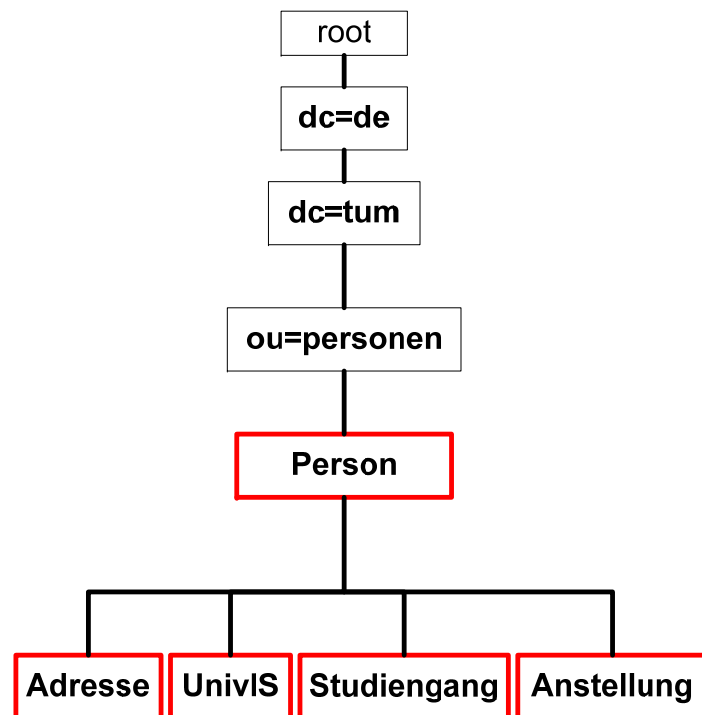
IntegraTUM: Hintergründe LDAP-Schema- und DIT-Design

- Anforderungen an das Identity Management
 - Aus Dienst-Perspektive einfache Anbindung
 - Skalierbarkeit bzgl. Anzahl angebundener Dienste
- Schema-Homogenität langfristig schwierig
 - Proprietäre Schemata, z.B. Active Directory, clixPerson
 - IETF-Schemata, z.B. inetOrgPerson, posixAccount
 - DFN-AAI Schema (eduPerson)
- Anforderungen aus Identity Management Sicht
 - Gute Eignung für Datenqualitäts-Prüfungen
 - Einfache Implementierung durch 1:1-Attributsmapping

IntegraTUM: IDM-intern verwendete LDAP-Schemata

„Hierarchische Variante“

Alle Attribute selbst definiert, z.B. itumNachname



Beliebig viele Unterobjekte, z.B. mehrere Adressen

„Flache Variante“

Hilfsklassen mit mandatory-Attributen

OC: itumPerson

iNachname „Max“
iVorname „Mustermann“
iKennung „ge99nug“
...

OC: itumStudent

iStudiengangliste „Stg1“ „Stg2“ „Stg3“ (multi-v)

OC: itumStg1{..N}

iStg1{..N}Fachsemester „6“ (single-v)
iStg1{..N}Bezeichnung „Informatik“ (single-v)
...

OC: itumMitarbeiter

iAnstellungsverzeichnis „Anst1“ „Anst2“ „Anst3“ (multi-v.)

OC: itumAnst1{..N}

iAnst1{..N}Einrichtung „Brandmeister“ (single-v.)

OC: itumGast

iGastverhaeltnisliste „Gast1“ „Gast2“ (multi-v)

OC: itumGastverh1{..N}

iGv1{..N}GastgeberID „012346789abcdef“ (single-v)
iGv1{..N}GastBeginDat „2006-11-29“ (single-v)
iGv1{..N}GastEndeDat „2006-11-29“ (single-v)

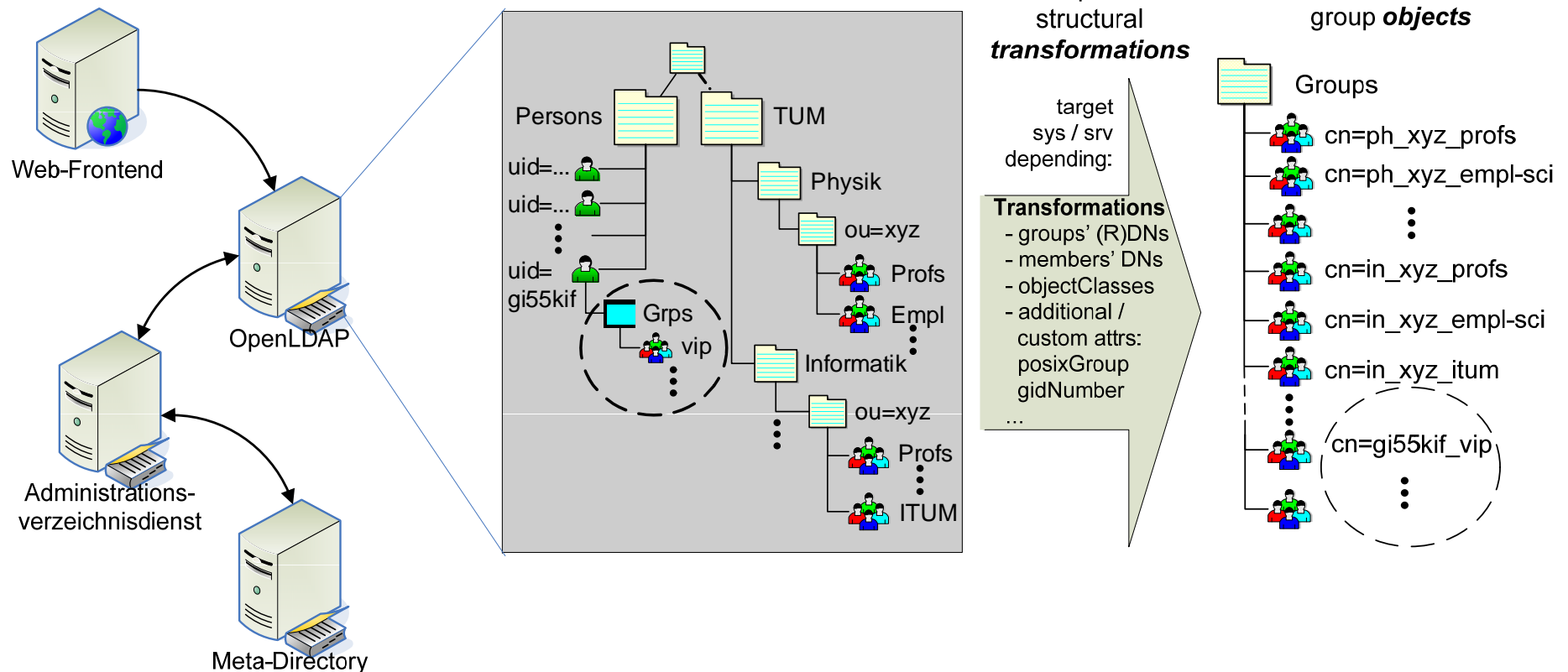
OC: itumAlumnus

iAlumnusliste „Alu1“ „Alu2“ (multi-v)
...

IntegraTUM: Bedarf an dienstübergreifender Gruppenverwaltung

- Gruppen als Basis für Autorisierungsmechanismen
- Dienstübergreifende Konsistenz notwendig, z.B. bei Projekten:
 - **Mailingliste**
 - **Gemeinsamer Filespace**
 - **E-Learning-Community**
 - **Interner Bereich des Webauftritts**
- Zwei grundlegende Arten von Gruppen
 - **Aus Attributen abgeleitet (automatisch generierbar)**
 - **Manuell gepflegt**

IntegraTUM: Gruppenverwaltung



- Siehe LDAPcon2007: Vortrag/Artikel von Daniel Pluta

IntegraTUM: Prozessanpassungen

- Vermeidung von Duplikaten durch SAP HR
- Ausgabe des Bibliotheksausweises bei Immatrikulation
- Zentrale Vergabe von Kennungen
 - Bei der Immatrikulation (über Studenten-Leporello)
 - Im Rahmen der Einstellungsunterlagen
- Zentraler Support (nicht nur) für rezentralisierte Dienste

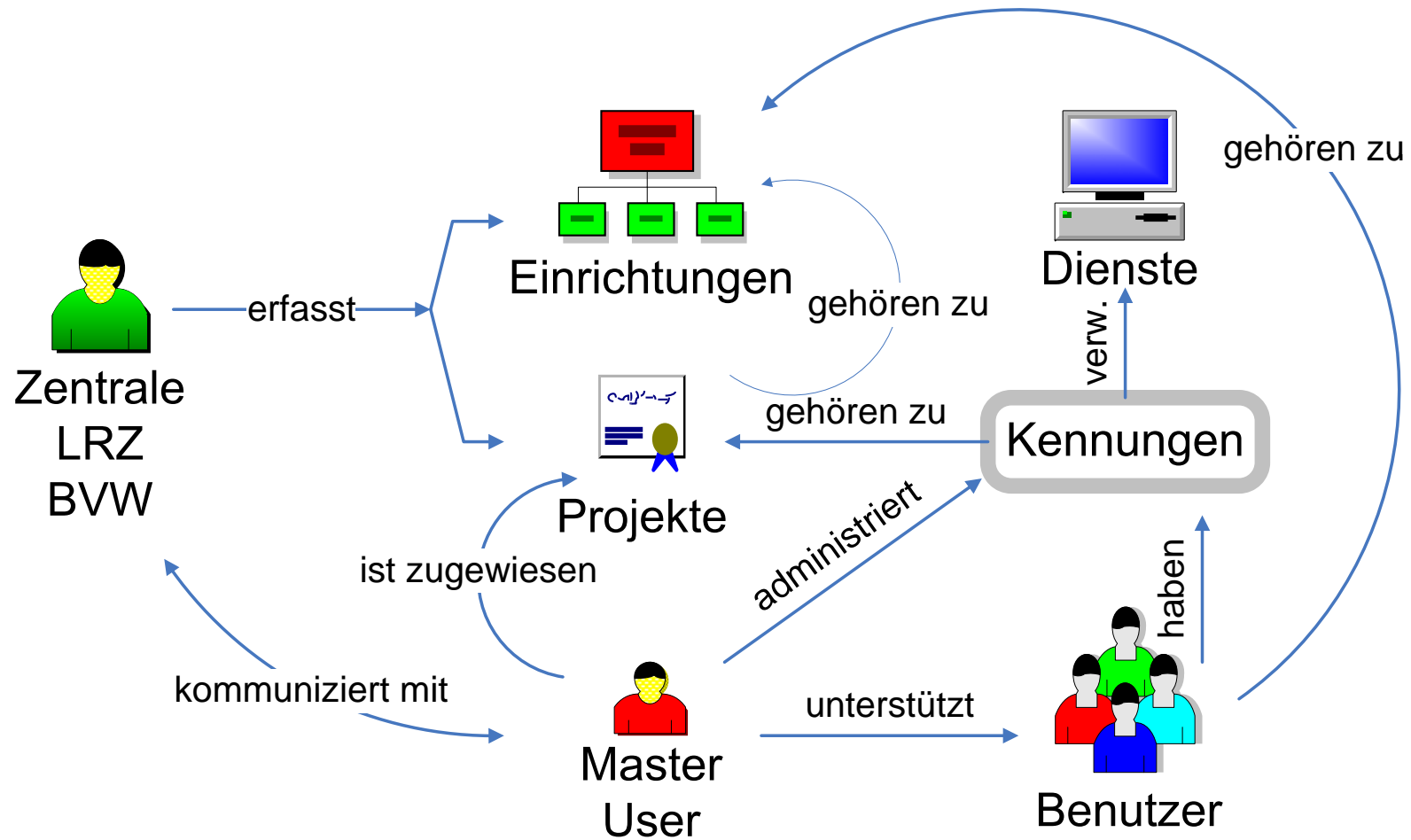
Übersicht

- DFG-Projekt IntegraTUM
 - Aktuelle IM-Architektur
 - Schemavariationen
 - Gruppenverwaltung
 - Prozessanpassungen
- Identity Management am LRZ
 - Realisierte IM-Architektur
 - Werkzeuge zur Migration und Administration
- Shibboleth-Aktivitäten
 - Shibboleth an LMU und TUM
 - Shibboleth im Rahmen der Virtuellen Hochschule Bayern (vhb)

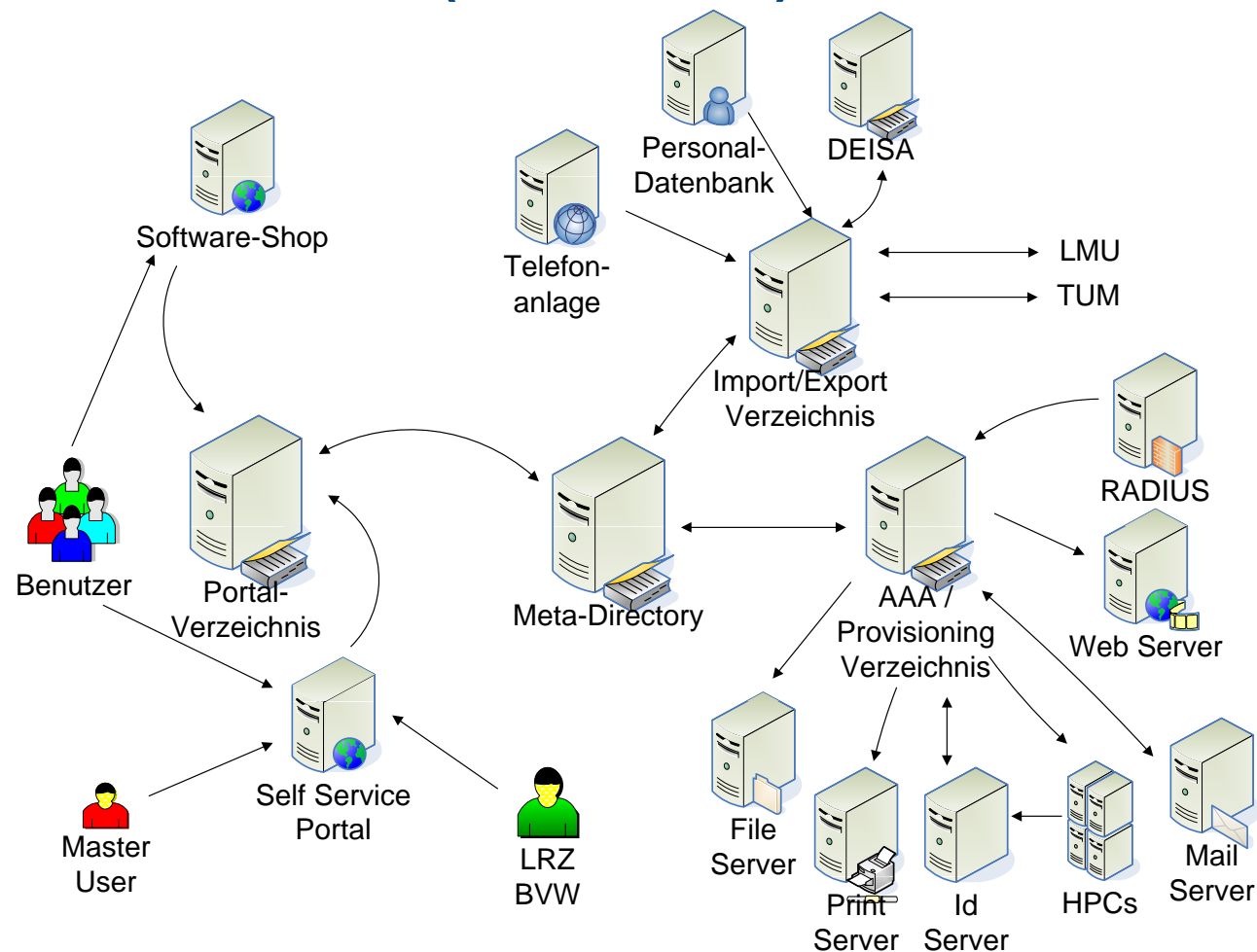
Projekt LRZ-SIM: Eckdaten

- > 100.000 Benutzer zu verwalten
 - **Münchner Hochschulrechenzentrum**
 - Studenten, Mitarbeiter
 - Alumni-Dienste, z.B. lebenslange Mail-Weiterleitung
 - **Höchstleistungsrechenzentrum**
 - HPCs für bayern- und deutschlandweite Nutzung
 - Europäische und internationale Grid-Projekte
- Accounting erfordert z.T. mehr als eine Kennung pro Person
- Schlüsselkonzept: Delegierte Administration

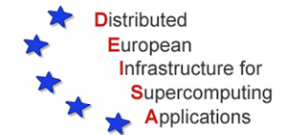
LRZ-SIM: Master User Konzept



LRZ-SIM: Architektur (vereinfacht)



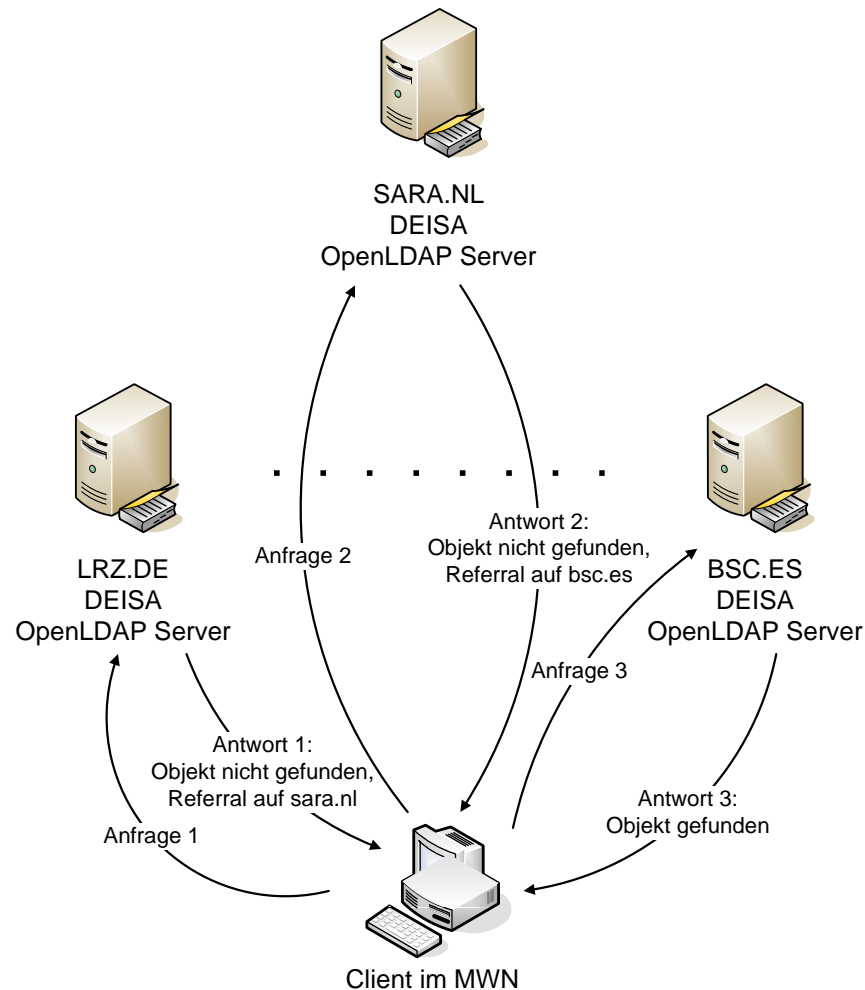
LRZ-SIM: Integration von DEISA Grid-Kennungen



Zentraler LDAP-
Server mit
Referrals auf die
LDAP-Server jeder
DEISA-Site

LDAP-Server pro
DEISA-Site

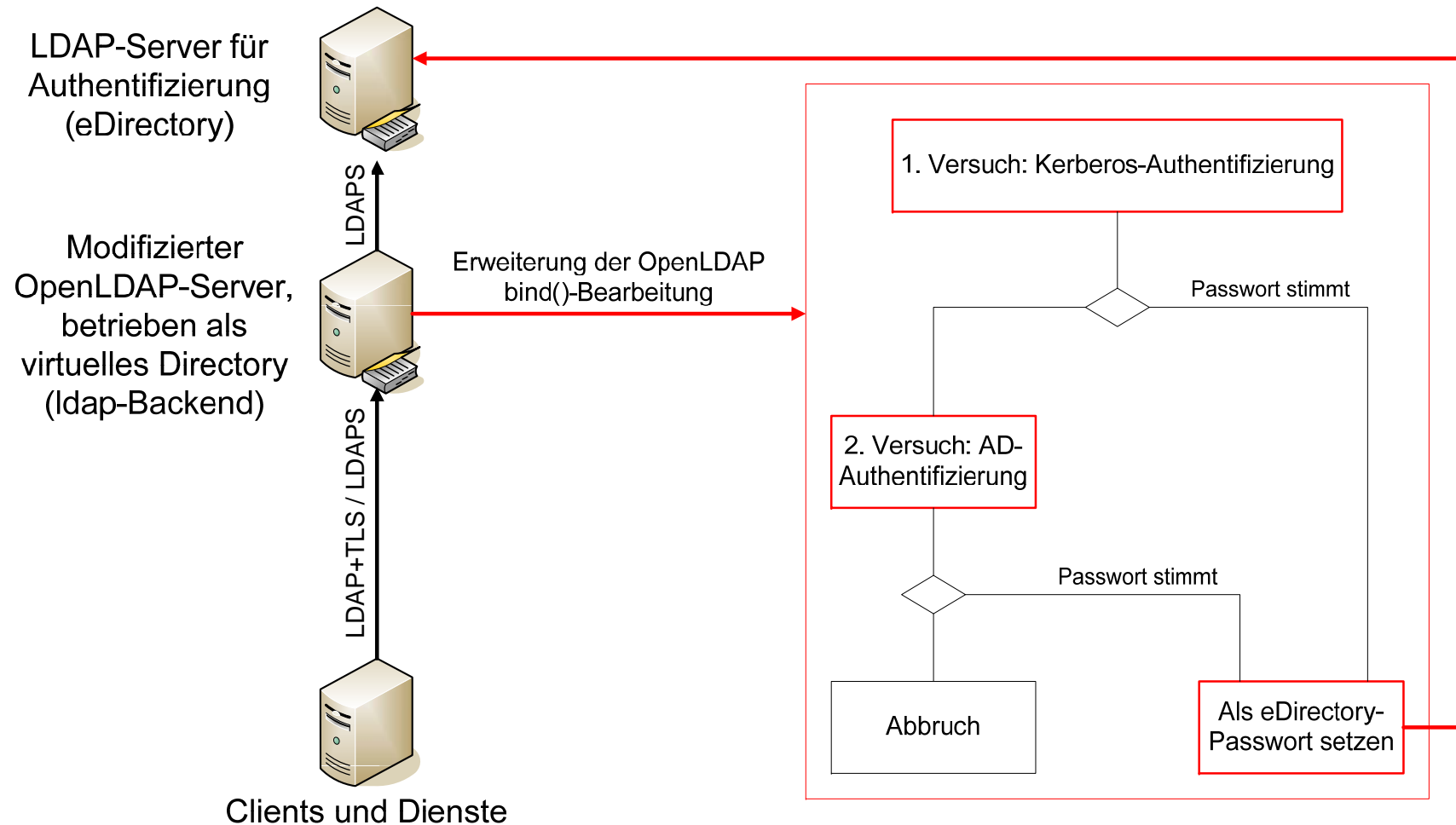
Clients




• Herausforderungen:

- Loginnamen / UIDs / GIDs werden extern vorgegeben
- Temporärer Ausfall des LDAP-Servers einer DEISA-Site darf nicht zum Löschen ihrer Kennungen führen

LRZ-SIM: Passwort-Migration AD/Kerberos → eDirectory



LRZ-SIM: Web-Frontend für Administration / Self Services


Identity Management Portal

DOKU
Impressum
Logout

Kennung: a2822bj; Benutzer: Herr Hommel

Benutzer-Verwaltung

Betreuer-Dienste

Einrichtung
[neu anlegen](#)
[anzeigen/bearbeiten](#)

Projekt
[neu anlegen](#)
[anzeigen/bearbeiten](#)
[HPCProjekt](#)

Person
[neu anlegen](#)
[anzeigen/bearbeiten](#)

Kennung
[neu anlegen](#)
[anzeigen/bearbeiten](#)

MasterUser-Dienste

Self Services

Admin-Dienste

Projekt anzeigen/bearbeiten

[\[Projekt \] => \[Projektdaten \] => \[Master User eintragen \] => \[Master User entfernen \] => \[Kontingente \] => \[Kennungsliste \] => \[Status/Bemerkung \]](#)

Gesamtzahl Kennungen (hell unterlegte Felder können geändert werden):

| | | |
|------------------|--------|------|
| Kennungen Gesamt | belegt | frei |
| Anzahl 30 | 30 | 0 |

| | | | | | | | | | |
|-------------------|--------|--------|--------------|--------|--------|----------------------|--------|------------|-----------|
| Anzahl Kennungen: | | | Quota in MB: | | | CPU-Zeit in Stunden: | | | |
| Dienst | Gesamt | belegt | frei | Gesamt | belegt | frei | Gesamt | verbraucht | verfügbar |
| AFS | 30 | 30 | 0 | 3000 | 3000 | 0 | | | |
| HLRB | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Linux | 0 | 0 | 0 | | | | | | |
| Mail | 30 | 30 | 0 | | | | | | |
| PC | 30 | 30 | 0 | 60000 | 60000 | 0 | | | |
| RVC | 0 | 0 | 0 | | | | | | |
| Sun | 30 | 30 | 0 | | | | | | |
| VPN | 30 | 30 | 0 | | | | | | |

Übernehmen und fortfahren
Speichern und beenden
Alles zurücksetzen

Projektdaten:

| | | | | | |
|-----------------------------------|------------------------------|------------------------------|------------------|-----------------------------|--|
| Projektbezeichnung: IntegraTUM | | | | Statistik-Kategorie: LRZ | |
| Projektname: a2836 | Projektbeginn: 2004-06-23 | Projektablauf: 2007-12-31 | Status: aktiv | Betreuer: Frau Schröder | Projekt-Maildomain: lrz-muenchen.de |

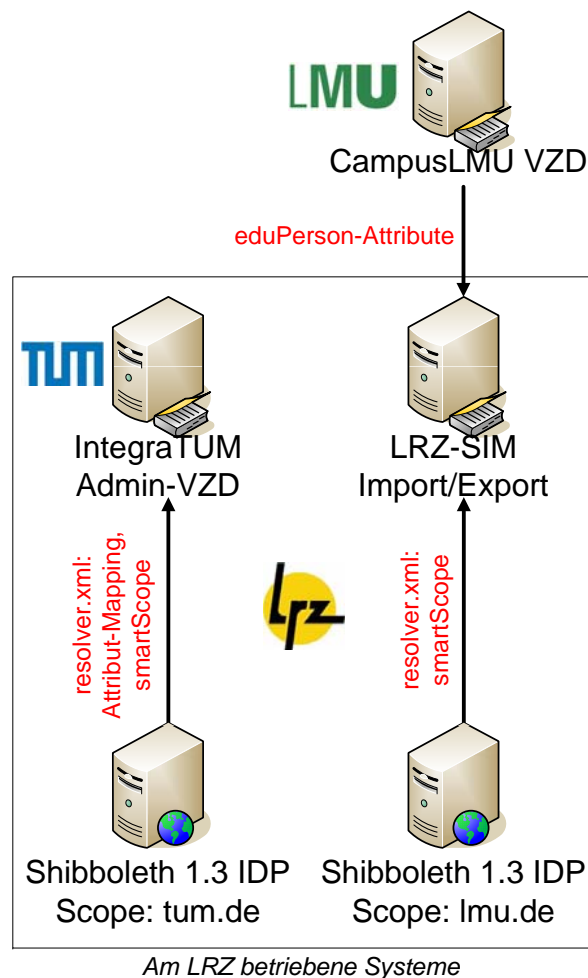
Übersicht

- DFG-Projekt IntegraTUM
 - Aktuelle IM-Architektur
 - Schemavariationen
 - Gruppenverwaltung
 - Prozessanpassungen
- Identity Management am LRZ
 - Realisierte IM-Architektur
 - Werkzeuge zur Migration und Administration
- Shibboleth-Aktivitäten
 - Shibboleth an LMU und TUM
 - Shibboleth im Rahmen der Virtuellen Hochschule Bayern (vhb)

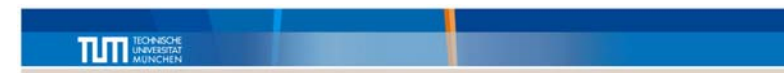
Shibboleth als (hochschul-internes) SSO-System der TUM

- Motivation:
 - SSO nicht nur HS-übergreifend, sondern auch TUM-intern
 - SSO + Corporate Design als sichtbares Integrationsmerkmal
 - Dienst-Anpassung „nur“ an Shibboleth erforderlich
- Beschluss der erweiterten Hochschul-Leitung
 - Investitionssicherheit für die Dienstbetreiber an TUM/LRZ
 - Kriterium bei der Einführung neuer Dienste
- Umsetzung wird pilotiert durch
 - E-Learning (Software im-c Clix, Plattform ZePeLin.org)
 - Bibliothek (Medienserver, Projekt mediaTUM)
 - myTUM-Webportal

Shibboleth: IDP-Hosting für LMU/TUM am LRZ

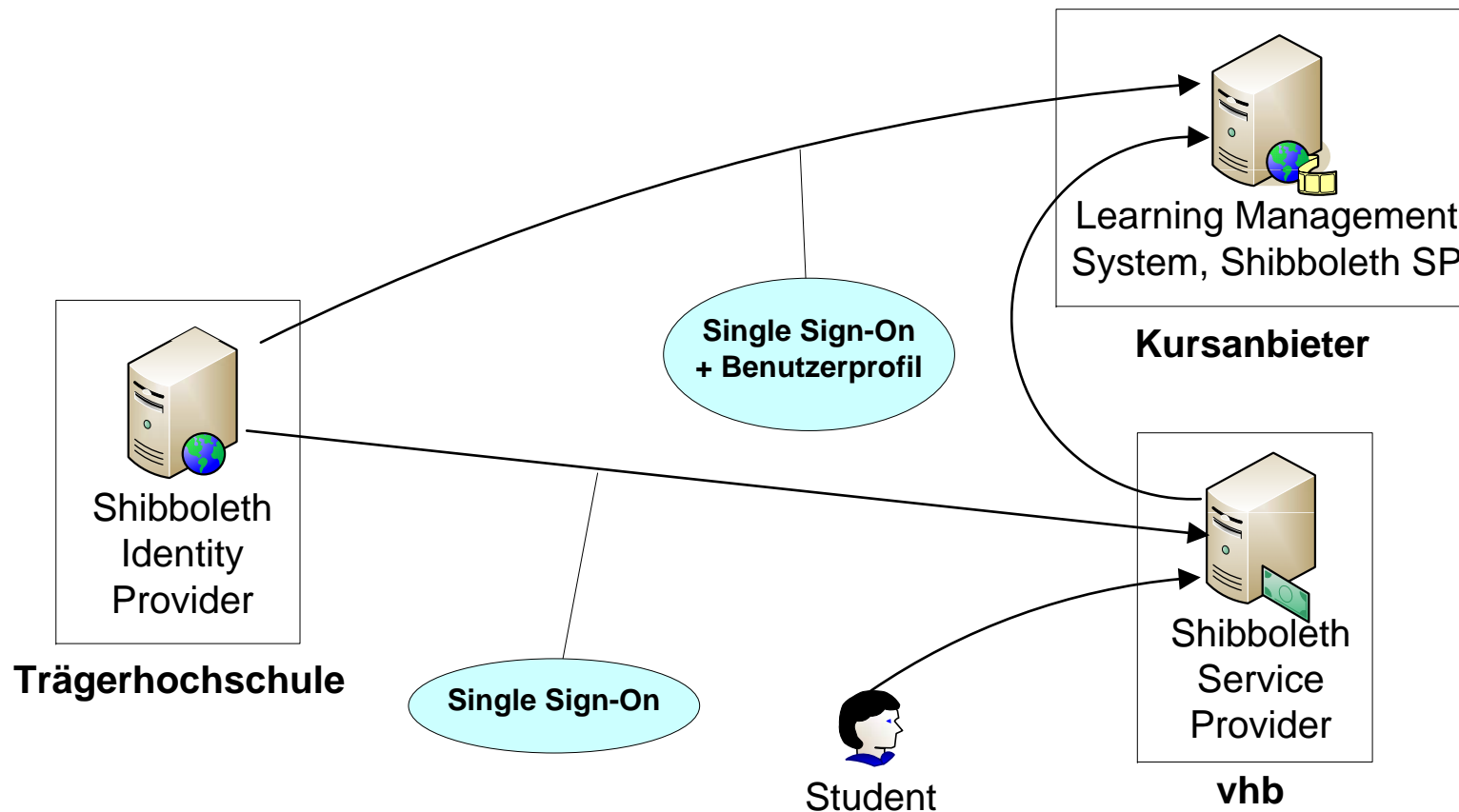


The screenshot shows the login page for the Ludwig-Maximilians-Universität München. The header includes the LMU logo and the text "LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN" and "DEUTSCHES FORSCHUNGSNETZWERK AUTHENTIZIERUNGS- UND AUTORSIERUNGS-INFRASTRUKTUR LOGIN". The main content area has the heading "Ludwig-Maximilians-Universität München" and a subheading "Bitte verwenden Sie Ihre CampusLMU-Kennung zur Anmeldung: Zulässig als Anmeldename sind E-Mail-Adressen der Domains @*.lmu.de.". Below this are input fields for "Benutzername:" and "Passwort:", and a "Anmelden" button. At the bottom, there is a note: "Um den angeforderten Dienst nutzen zu können, müssen Sie sich hier einloggen. Bei Rückfragen zur Authentifizierung im Rahmen der DFN Authentifizierungs- und Autorisierungsinfrastruktur wenden Sie sich bitte an den CampusLMU Helpdesk."



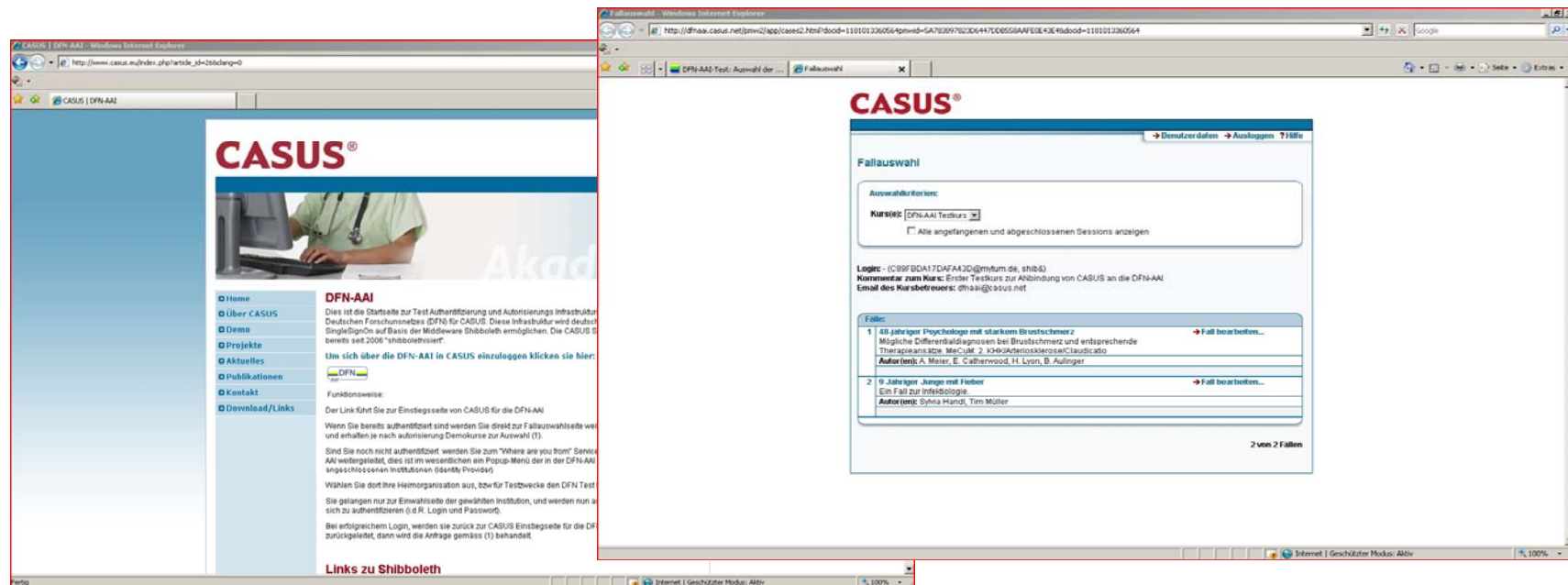
The screenshot shows the login page for the Technische Universität München (TUM). The header includes the TUM logo and the text "TECHNISCHE UNIVERSITÄT MÜNCHEN". The main content area has the heading "Bitte verwenden Sie Ihre myTUM-Kennung zur Anmeldung: Zulässig als Anmeldename sind E-Mail-Adressen der Domains @tum.de und @mytum.de.". Below this are input fields for "Kennung" and "Passwort:", and a "Login" button. At the bottom, there is a note: "Um den angeforderten Dienst nutzen zu können, müssen Sie sich hier einloggen. Bei Rückfragen zur Authentifizierung im Rahmen der DFN Authentifizierungs- und Autorisierungsinfrastruktur wenden Sie sich bitte an E-Mail an: support@tum.de".

Shibboleth im Rahmen der Virtuellen Hochschule Bayern



Herausforderung: Anbindung proprietärer LMS und Prüfungsverwaltungssysteme

DFN-AAI Prototyp CASUS: Medizin-LMS der LMU



- Motivation:
 - Gemeinsamer Studiengang Medizin LMU/TUM
 - Demonstration der Notwendigkeit weiterer Attribute (vgl. DFN-AAI Schema v0.8)

Zusammenfassung

- IntegraTUM – Besonderheiten
 - **Architektur mit Directory-Backbone**
 - **Flexibilität durch Schema-Variationen**
 - **Notwendigkeit dedizierter Administrations-Oberflächen**
- LRZ-SIM – Schwerpunkte
 - **HPC-Accounting und Integration von Grid-Benutzern**
 - **Transparente Passwort-Migration**
 - **Dedizierte Web-Oberfläche als wichtige Datenquelle**
- Shibboleth-Aktivitäten in München
 - **Shibboleth als strategische SSO-Plattform der TUM**
 - **Learning Management Systeme als Vorreiter**
 - **Nutzung der DFN-AAI im Rahmen der vhb**