



Identity Management im Münchner Wissenschaftsnetz

**Aktueller Stand und Ergebnisse
des DFG-geförderten Projekts IntegraTUM**

ZKI Arbeitskreis Verzeichnisdienste
Herbsttagung 2009 – TU Dresden

Dr. Wolfgang Hommel, Leibniz-Rechenzentrum



Überblick



Übersicht:
IDM-Projekte im Münchener Hochschulumfeld

Identity Management am LRZ:
Erfahrungen nach 1,5 Jahren Produktivbetrieb

DFG-Projekt IntegraTUM:
Ergebnisse des Teilprojekts Identity Management

Shibboleth und DFN-AAI:
Aktivitäten und Pläne an den Münchener Universitäten



Die Rolle(n) des Leibniz-Rechenzentrums



Rechenzentrum für die
beiden Münchner Universitäten

Höchstleistungsrechenzentrum
mit Benutzern aus ganz Deutschland
sowie aus europäischen und internationalen Grid-Projekten

Wissenschaftliches Rechenzentrum –
separate Verwaltungs-IT an den Unis



IDM-Projekte an den Münchener Hochschuleinrichtungen



Ludwig-Maximilians-Universität: Campus^{LMU}

Technische Universität München: IntegraTUM, TUMonline

Hochschule München: Vgl. "10 Jahre Identity Management"

Leibniz-Rechenzentrum (BAdW): LRZ-SIM

In der letzten Spalte Gesamnnutzung wird eine daraus abgeleitete Einschätzung der Nutzung über alle Dienste hinweg angezeigt.

Betreuerdienste	Betreuer	F	Vorname	Nachname	Status	Rechte	AFS-Nummer	Rechte	Nutzung	PC	E-Mail	Anderer Dienst-Nutzung
Entwicklungs- und Bildungsinstitutionen												
	HR	HR	Dr.	Horst	stevo	-	-	3/3072	Linker	0/2048	ja	simonekr@lrz.de
	HR	HR	Dr.	Giese	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Grundler	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Krahn	[gesperrt]	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Lindner	[gesperrt]	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Leiß	stevo	-	-	3/3072	rein	0/2048	ja	johann.leiss@lrz.de
	HR	HR	Dr.	Müller	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Pongratz	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Römer	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Schäfer	[gesperrt]	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Seifert	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Wegner	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Wölfel	stevo	-	-	3/3072	rein	-	ja	Y
	HR	HR	Dr.	Kotz	[gesperrt]	-	-	3/3072	rein	0/2048	ja	InfoPoint.informatik@lrz.de
Projekt												
	Meta-Projekte											
	Alle Projekte											
	metaprojekte											
	unterstützen											
	Kungrätsche nominierten											
	Zugangsprojekt nominiert											
	Zugangsprojekt nominiert											
	HECProjekt											



Überblick



Übersicht:
IDM-Projekte im Münchener Hochschulumfeld

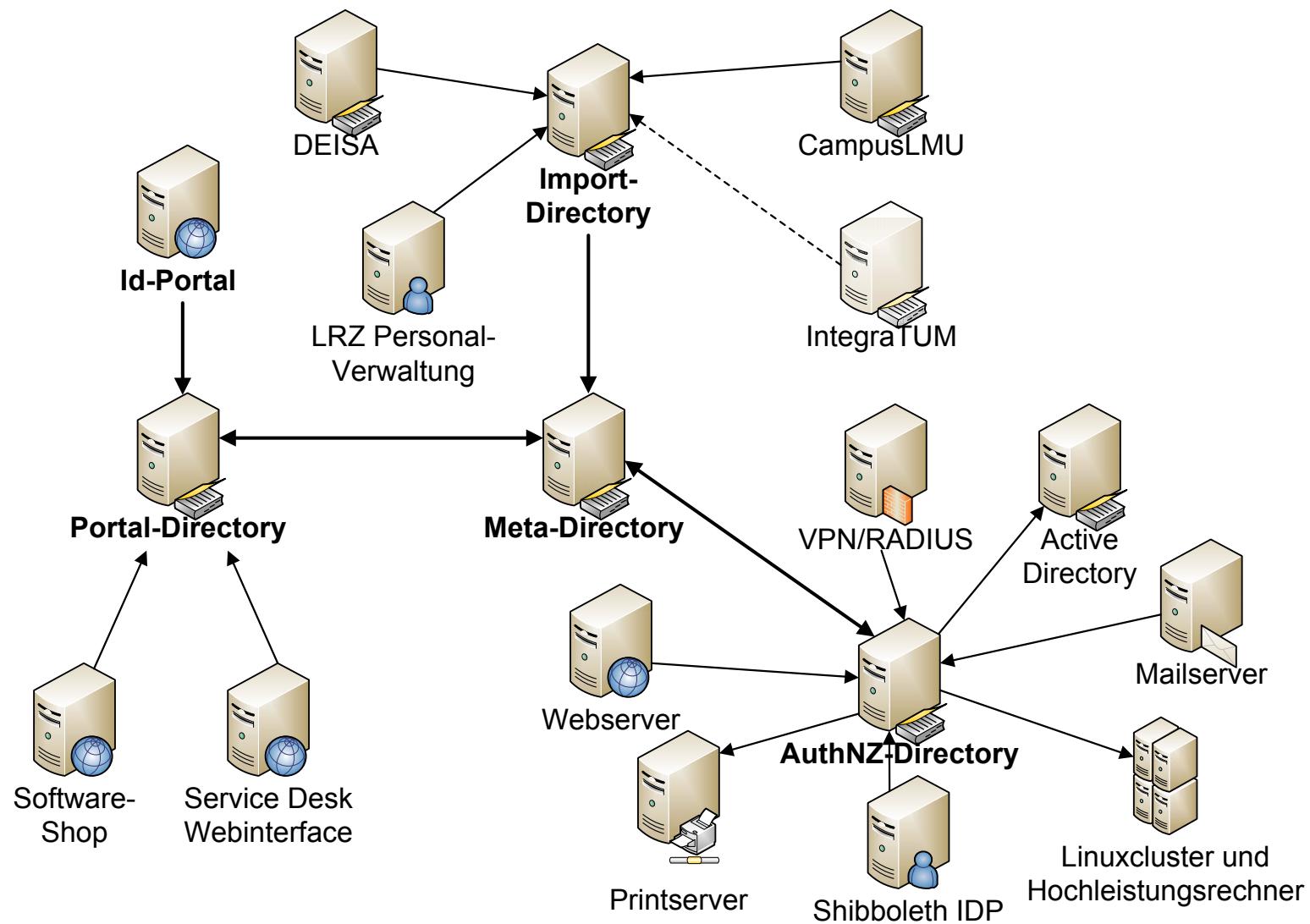
Identity Management am LRZ:
Erfahrungen nach 1,5 Jahren Produktivbetrieb

DFG-Projekt IntegraTUM:
Ergebnisse des Teilprojekts Identity Management

Shibboleth und DFN-AAI:
Aktivitäten und Pläne an den Münchener Universitäten

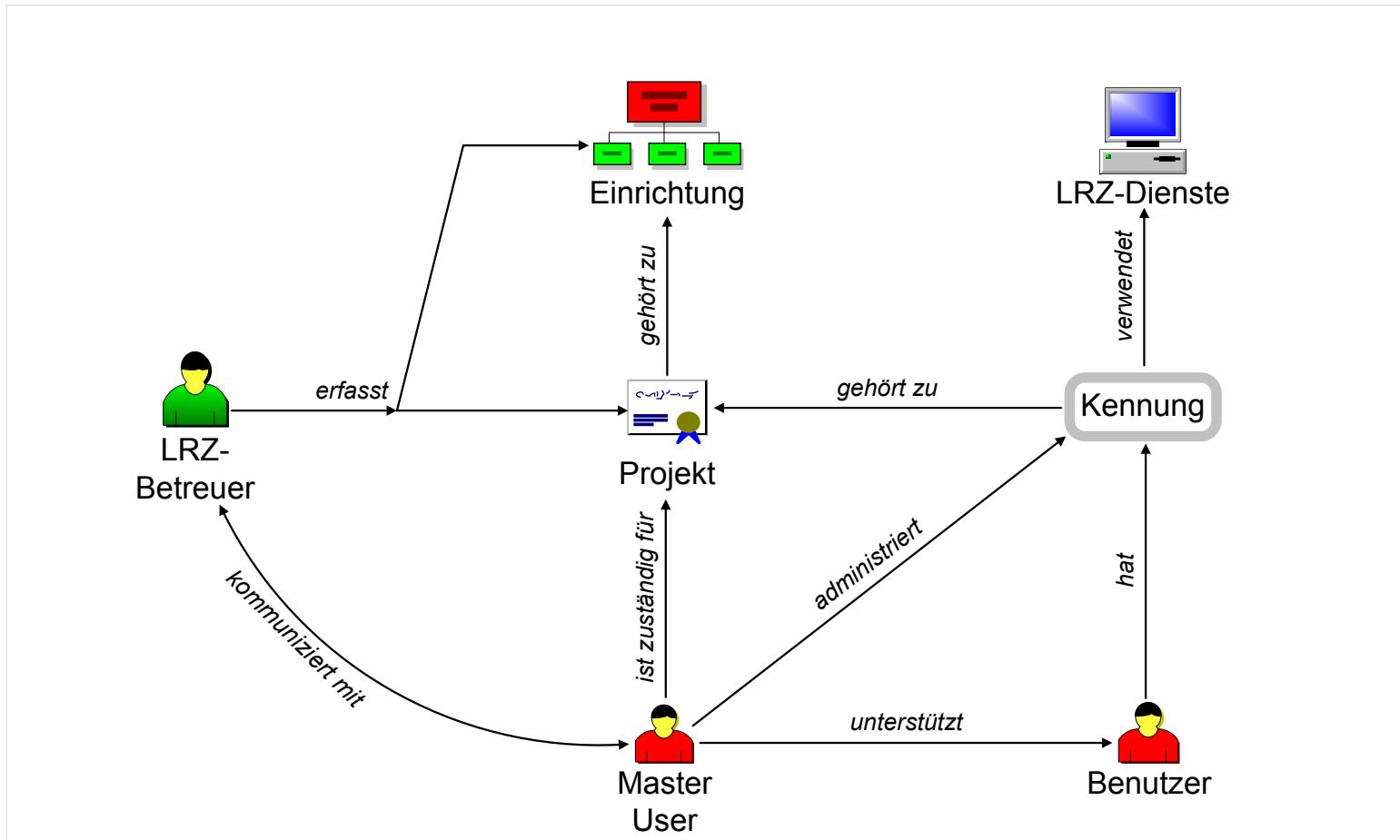


LRZ-SIM: Meta-Directory-Architektur



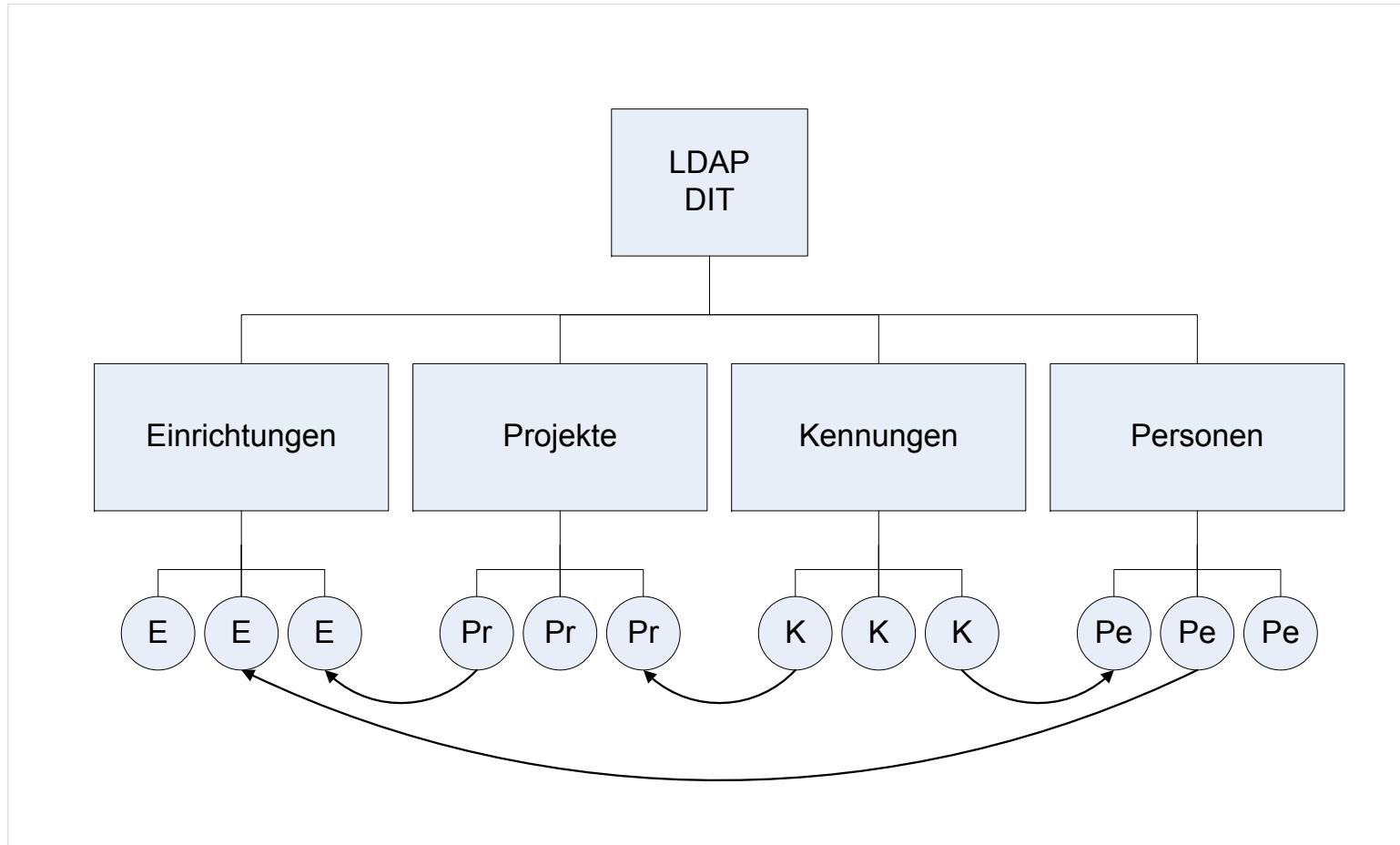


LRZ-SIM: Datenmodell und LDAP-DIT





LRZ-SIM: Datenmodell und LDAP-DIT





LRZ-SIM: Web-Frontend “Id-Portal”



Identity Management Portal

Kennung: a2822bj; Benutzer: Herr Dr. Hommel

[Impressum](#) [Logout](#)

Betreuerdienste

[Master User Dienste](#)

[Self Services](#)

Hotlinedienste

[Einrichtung anzeigen](#)

[Hierarchie anzeigen](#)

[Hierarchie erweitert](#)

[Hierarchie browsen](#)

Projekt anzeigen

Person anzeigen

Kennung anzeigen

[Admindienste](#)

Person anzeigen

[Person]=>[Personendaten]

Nachname:	Vorname:
Hommel	Wolfgang
Anrede:	Hochschul-Status:
Herr Dr. Hommel	Master User
Kontakt E-Mail-Adresse:	Telefon:
Wolfgang.Hommel@lrz.de	089-35831-7821
Benutzername:	
lu57hon	

Master-User von folgenden Projekten

a2836 E-Mail und Dateiablage für das Projekt IntegraTUM

gehört zu: Hochschulleitung TUM, CIO (t022)

Leitung: Herr Dr. Wülbbern

Weitere Herr Haarer

Master-User: Herr Haarer

Persönliche Kennungen

Kennung	Status	Datum der letzten Passwortänderung; Bearbeiter
---------	--------	--

LRZ-Betreuer

Master User

Self Services

Service Desk



LRZ-SIM: Nutzungsstatistik seit Anfang 2009



Über 500 Änderungen an Einrichtungen durch LRZ-Betreuer

Ca. 280 neue Master User, ca. 1200 alte Master User gelöscht

Über 40.000 Logins für Master User Dienste und Self Services

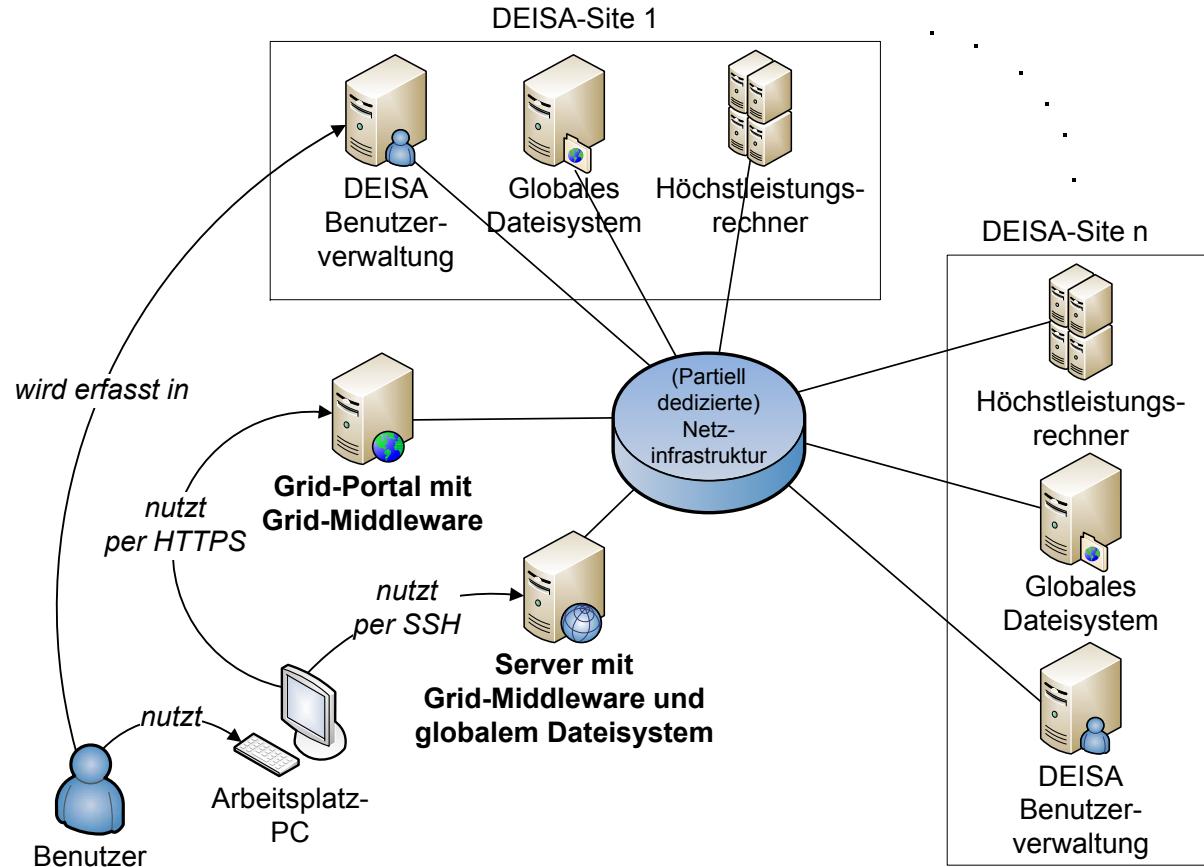
Über 10.000 Berechtigungsänderungen
an bestehenden Kennungen durch Master User

Rund 2.500 neue Kennungen angelegt,
rund 3.500 Kennungen gesperrt,
mehr als 6.500 Kennungen gelöscht

Self Services: Rund 2.500 Änderungen an Mail-Forwards,
rund 4.500 Abwesenheitsnotizen eingerichtet



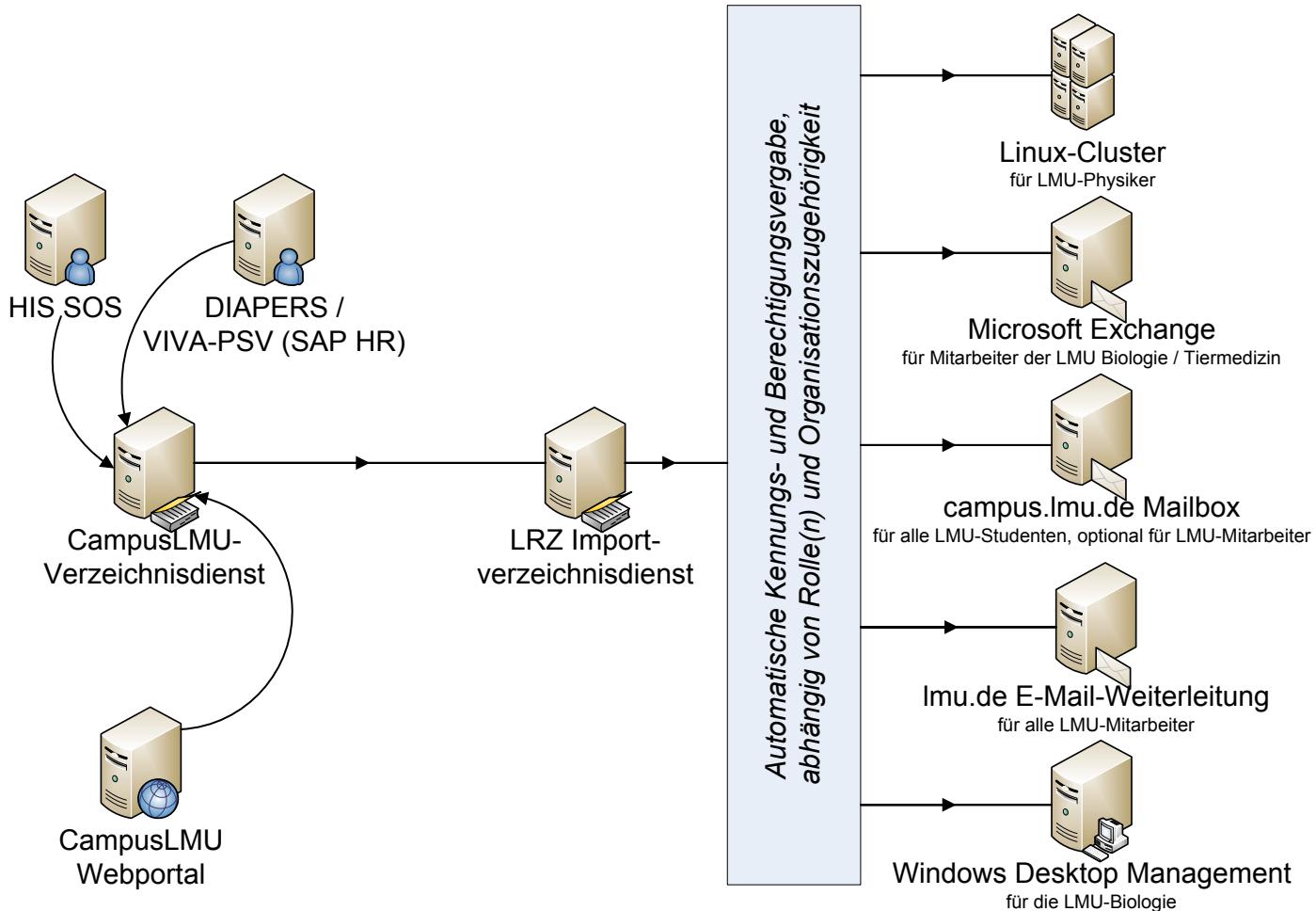
LRZ-SIM: Importschnittstellen



Grid-Projekt DEISA



LRZ-SIM: Importschnittstellen



Grid-Projekt DEISA

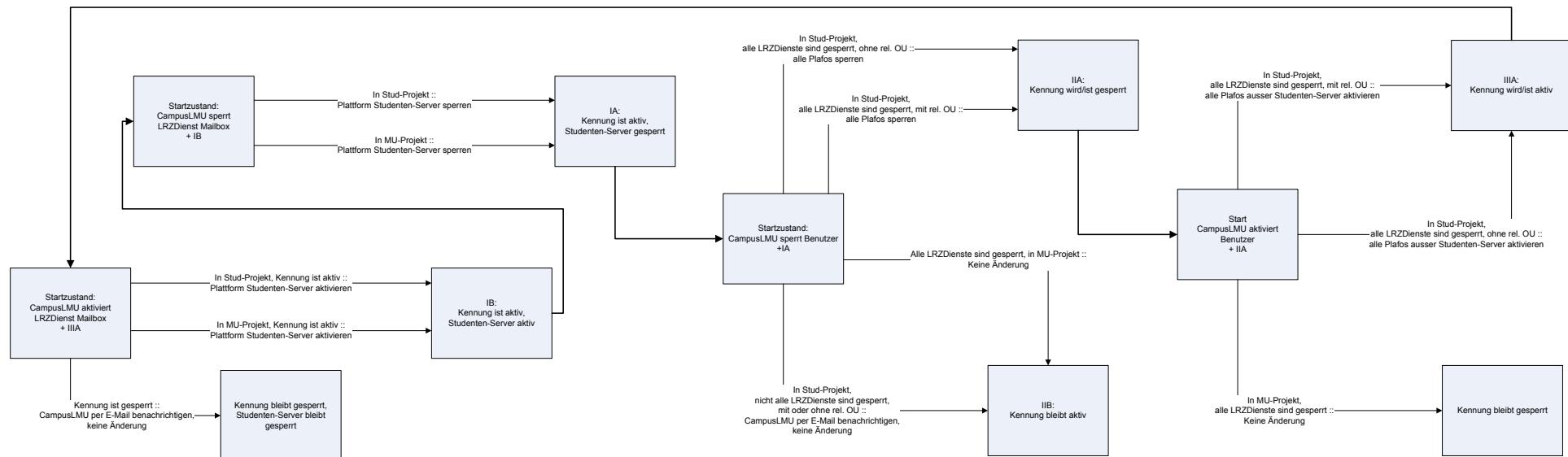
Campus^{LMU}



LRZ-SIM: Importschnittstellen



Komplexität:
Mapping der LMU-Kostenstellen auf LRZ-Projekte,
Überlappung mit Berechtigungsverwaltung durch Master User

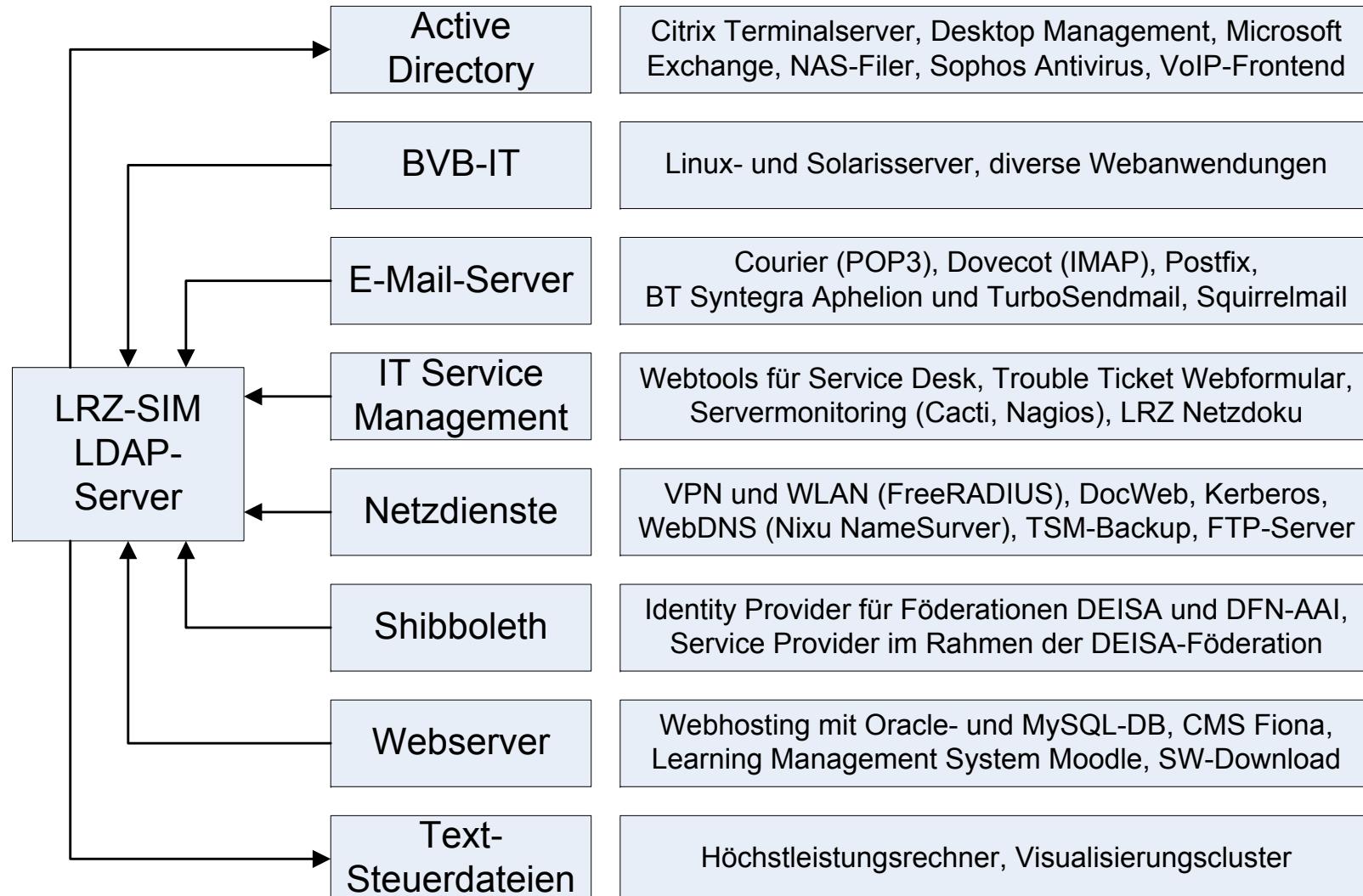


Grid-Projekt DEISA

Campus^{LMU}



LRZ-SIM: Angebundene Systeme





Überblick



Übersicht:
IDM-Projekte im Münchener Hochschulumfeld

Identity Management am LRZ:
Erfahrungen nach 1,5 Jahren Produktivbetrieb

DFG-Projekt IntegraTUM:
Ergebnisse des Teilprojekts Identity Management

Shibboleth und DFN-AAI:
Aktivitäten und Pläne an den Münchener Universitäten



IntegraTUM: IDM-Ausgangsbasis (2004/05)



LRZ-SIM Teilziel:
Direkte Kopplung mit Universitätsverwaltungen

Betrieb von LDAP-Servern für die TUM seit 2003

Gründung des LRZ Identity Management Teams
Ziel: Ausbau der IDM-Dienstleistungen

Gemeinsamer Projektantrag TUM / LRZ im Rahmen des DFG-Förderprogramms Leistungszentren für Forschungsinformationen



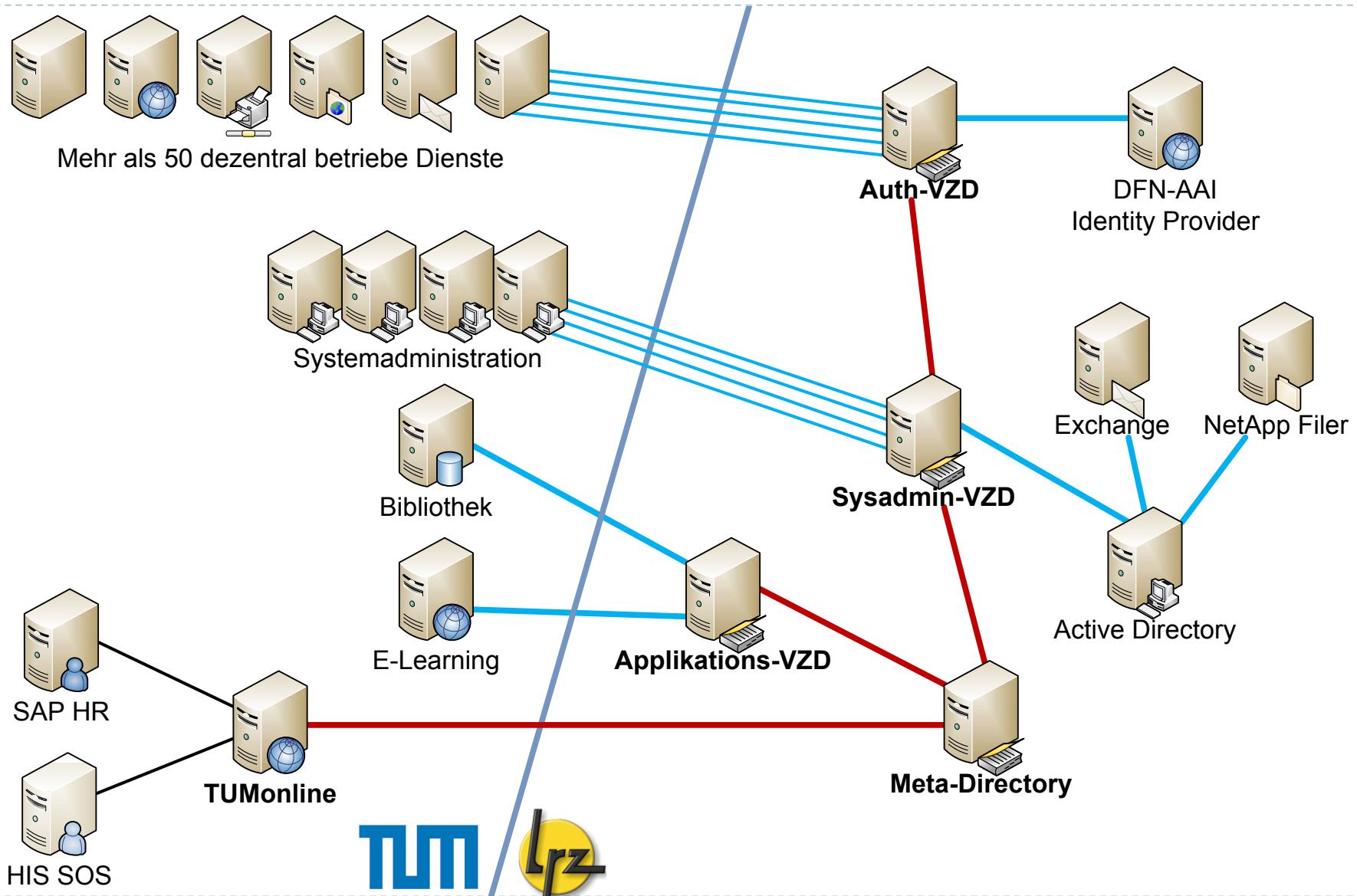
IntegraTUM: Projektstruktur



Seit 2007 zusätzlich:
SERVUS@TUM



IntegraTUM: IDM-Architektur 2009





IntegraTUM: Beispiele für die IDM-Prozessintegration



Online-Bewerbung
mit Accountvergabe (eingeschränkte Berechtigungen)

Vermeidung der Mehrfacherfassung von Personen
bereits in den Quellsystemen

Ausgabe des Bibliotheksausweises
im Rahmen der Immatrikulation / des Einstellungsverfahrens

Webbasierte Self Services,
z.B. zur Änderung der Privatanschrift (nur bei Studenten)



IntegraTUM: Angebundene Systeme



Zentrale Dienste

Bibliothek, E-Learning, Service Desk, TUMonline

Fakultätsweite Dienste

Webportale, z.B. E-Technik, Informatik, mediTUM, Physik, WiWi
Poolrechner/Arbeitsplätze, z.B. Chemie, E-Technik, Physik, WZW

Dezentrale Dienste

Diverse Webservices und Content Management Systeme
von Lehrstühlen und Fachschaften, MSDN AA



IntegraTUM: IDM-Konzepte und -Werkzeuge



ITUMSchema_v3.xls – OpenOffice.org Calc

Attributname	Attributbeschreibung	Schema-Daten		verwendet von															
		Attributtyp	Format	Type	Längen- beschränkung	Attribut Name	Attribut Name	Attribut Name	Attribut Name	Attribut Name									
14	intPerson	mv	mvLUP-2	dn															
15	intPersonName	mv	mvLUP-2	dn															
16	intPersonName	mv	mvLUP-2	dn															
17	intPersonName	mv	mvLUP-2	dn															
18	intPersonName	mv	mvLUP-2	dn															
19	intPersonName	mv	mvLUP-2	dn															
20	intPersonName	mv	mvLUP-2	dn															
21	intPersonName	mv	mvLUP-2	dn															
22	intPersonName	mv	mvLUP-2	dn															
23	intPersonName	mv	mvLUP-2	dn															
24	intPersonName	mv	mvLUP-2	dn															
25	intPersonName	mv	mvLUP-2	dn															
26	intPersonName	mv	mvLUP-2	dn															
27	intPersonName	mv	mvLUP-2	dn															
28	intPersonName	mv	mvLUP-2	dn															
29	intPersonName	mv	mvLUP-2	dn															
30	intPersonName	mv	mvLUP-2	dn															
31	intPersonName	mv	mvLUP-2	dn															
32	intPersonName	mv	mvLUP-2	dn															
33	intPersonName	mv	mvLUP-2	dn															
34	intPersonName	mv	mvLUP-2	dn															
35	intPersonName	mv	mvLUP-2	dn															
36	intPersonName	mv	mvLUP-2	dn															

RFC2252-Syntax-OID-Map

Tabelle 2 / 13

PageStyle

Summe=0

Google: IntegraTUM Schema

Schema-Design
in MS Excel

Automatisches
Erzeugen von
LDIF- und
Schema-Files,
LaTeX- und
HTML-Doku

Tools zum
Einspielen in die
LDAP-Server,
Schema-Diffs, ...



IntegraTUM-Gästeeverwaltung

Gast suchen | IntegraTUM - Gästeverwaltung 1.0.8.0 - n66mop - 1AC8FC82E30A0B0F - Hilfe

Stammdaten

MWNID:	eMail:	LRZ-Kennung:	Initial-Passwort:
C89FBDA17DAAFA43D		ne35ped	
Anrede:	Vorname:	Nachname:	Namenszusatz:
Herr	Wolfgang	Hommel	
Titel Pre:	Titel Mitte:	Titel Post:	Nationalität:
			Deutschland
Geburtsdatum:	Geburtsort:	Geburtsland:	Geburtsname:
28.06.1978	Gräfelfing		

Studium & Anstellung an der TUM

Studiengang ID	Studiengang	Abschluss	Studienform	Exmatrikulationsdatum
11	Informatik: NfElektrot	Diplom U	Erststudium	31.03.2004

Gastadresse

Straße:	Adresszusatz:	
Postleitzahl:	Ort:	Land:
Telefon:	Fax:	Postfach:

Typ	Straße	Adresszusatz	Postleitzahl	Ort	Land	Postfach	Telefon	Fax
HA	Hauzenberger 20/810	---	80687	München	---	---	57967862	---

Gastaufenthalt

[+]	All Aufenthalte beenden							
Auswählen	Beginn	Ende	Status	Herkunft	Einrichtung	Beschreibung	Eintragender	ID
	04.08.2008	04.02.2018	Gastwissenschaftler	TU-nahe Institution	TUIN	LRZ-Mitarbeiter; Auf Antrag von Silvia Knittl; TicketNr. 2008073110000182	SECB0970F872683A 1	

Buttons: Speichern, Zurücksetzen, Zurück

Gruppenverwaltungs-
LDAP-Backend

Heuristisches Identity
Matching per WS

Hochverfügbarkeit
und Load Balancing



Überblick



Übersicht:
IDM-Projekte im Münchener Hochschulumfeld

Identity Management am LRZ:
Erfahrungen nach 1,5 Jahren Produktivbetrieb

DFG-Projekt IntegraTUM:
Ergebnisse des Teilprojekts Identity Management

Shibboleth und DFN-AAI:
Aktivitäten und Pläne an den Münchner Universitäten



Motivation für den Shibboleth-Einsatz



Am LRZ:

Einheitliches Verfahren für völlig verschiedene Dienste

De-facto Standardsoftware, sehr guter Support
(Community, DFN-AAI, SWITCH-AAI)



Motivation für den Shibboleth-Einsatz



An LMU und TUM:

Stark vereinfachte Nutzung externer Dienste

Hochschulinternes (campusweites) Single Sign-On

Corporate Design +
Single Sign-On
=

Deutlich sichtbares
Integrationsmerkmal

Verbesserte
IT-Sicherheit,
da Reduktion
passwort-
verarbeitender
Stellen

Bei von Externen
nutzbaren Diensten nur
Anpassung an genau ein
SSO-System erforderlich



Shibboleth-Anpassung der angebotenen Dienste



Treibende Kraft an LMU und TUM: E-Learning

Eingesetzte Shibboleth-fähige Learning Management Systeme:

TUM:

im-c CLIX

LMU:

CASUS, Moodle, OLAT, (iTunes U)

Produktive Anwendungsgebiete:

Gemeinsame Studiengänge (z.B. Bio-Informatik, Medizin),
Kooperation LMU / Uni Zürich (Pathologie, Dermatologie)

Mittelfristige Ziele:
Kursabwicklung für Virtuelle Hochschule Bayern über DFN-AAI,
direkte Kursverlinkung aus CampusLMU und TUMonline



Zusammenfassung



Projekt LRZ-SIM:

Bereits sehr viele LRZ-Dienste integriert, eigenes Webfrontend, automatisierende Importschnittstellen

IntegraTUM IDM:

Kopplung von Campus Management und Meta-Directory, Integration in die Hochschulprozesse, diverse Werkzeuge

Intensive Zusammenarbeit von LMU, TUM und LRZ
(Motivation u.a. zentrale Dienste, gemeinsame Studiengänge)

Aktuelle und kommende Baustellen:

Direkte Kopplung der TUM- und LRZ-Verzeichnisdienste,
Ausbau der automatischen Berechtigungsvergabe für LRZ-Dienste (LMU/TUM),
Shibboleth-Anpassung der Webportale Campus^{LMU} und TUMonline,
Umsetzung des DFN-AAI E-Learning Profils in der VHB, ...