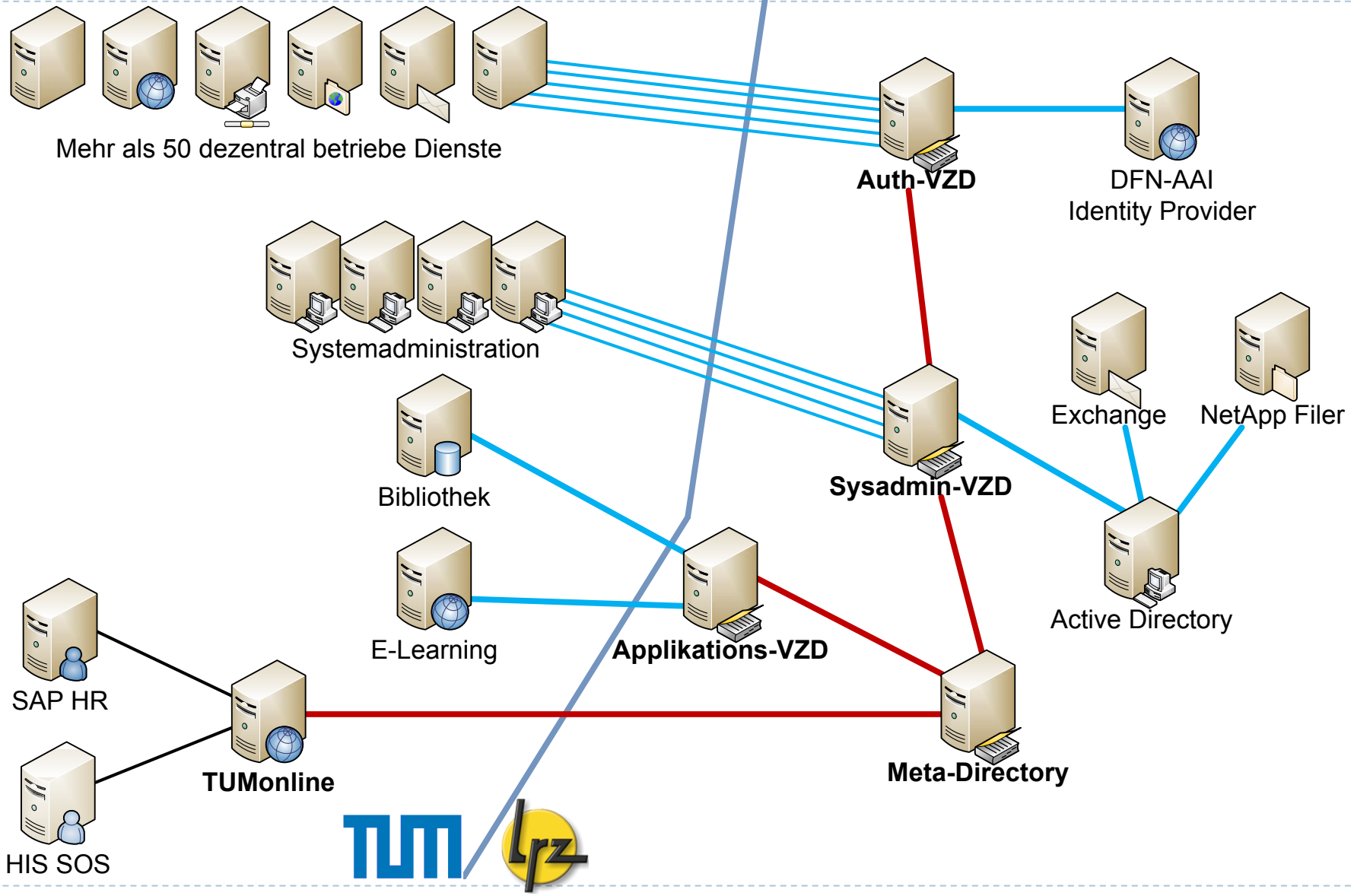
Identity & Access Management: Das Rückgrat der Hochschul-IuK-Infrastruktur

IntegraTUM – Teilprojekt Verzeichnisdienst

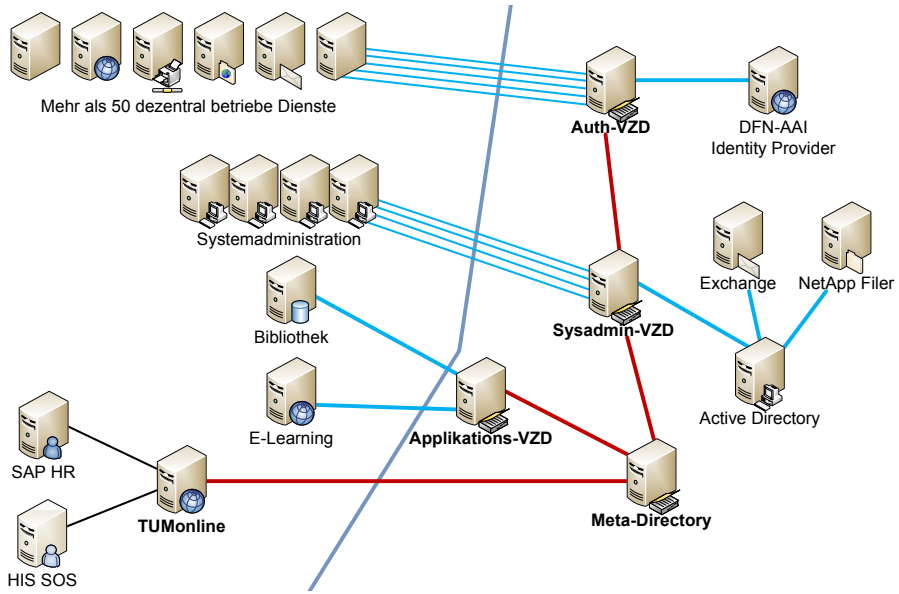
24. September 2009

Dr. Wolfgang Hommel, Leibniz-Rechenzentrum

IntegraTUM
Identity & Access Management Architektur



Mehrwert durch die I&AM-Architektur



Für die Benutzer

Für die Verwaltung

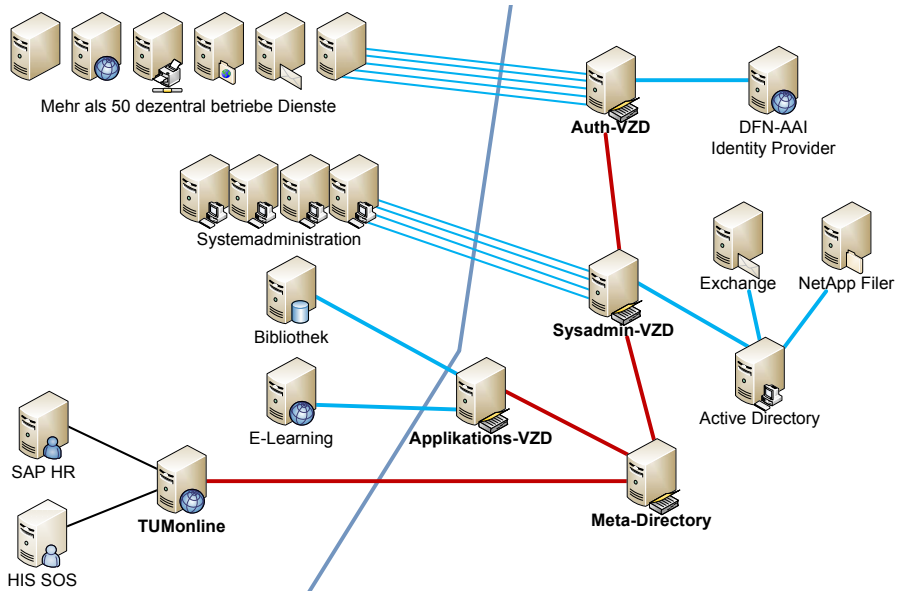
Für die Dienstanbieter

Nur eine Kennung (Loginname und Passwort) für alle IT-Dienste im Umfeld der TUM

Alle Dienste ab dem ersten offiziellen Tag an der TUM nutzbar

Stamm-/Kontaktdatenänderungen automatisch und schnell an alle IT-Dienste propagiert

Mehrwert durch die I&AM-Architektur



Für die Benutzer

Für die Verwaltung

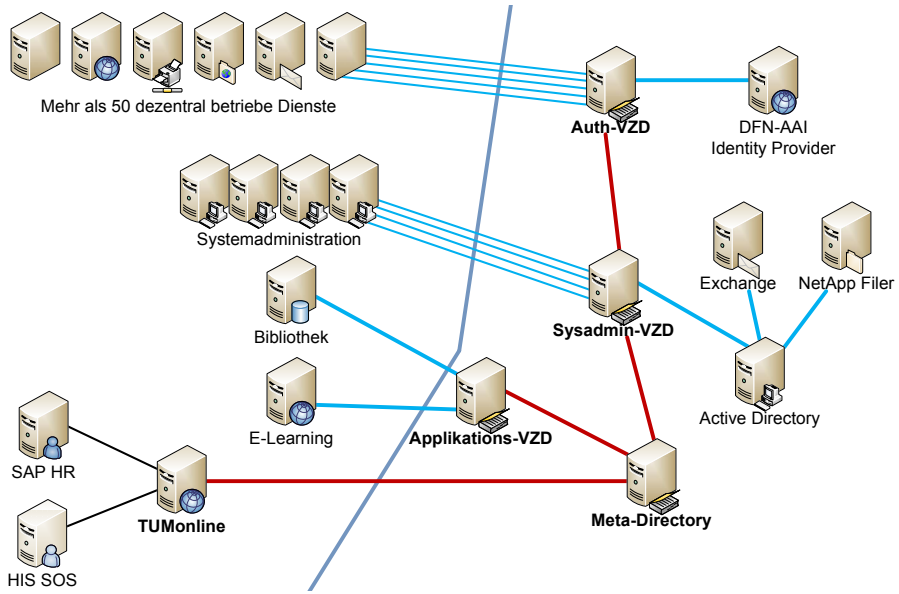
Für die Dienstanbieter

Nur noch ein einziges verwaltungsexternes System mit Benutzerdaten zu versorgen

Klare Zuständigkeiten durch Schnittstellenvereinbarung zwischen Verwaltung und technischem Identity Management

Nahtlose Integration in das Campus Management

Mehrwert durch die I&AM-Architektur



Für die Benutzer

Für die Verwaltung

Für die Dienstanbieter

Automatisierung von Anlegen, Freischalten, Aktualisieren und Löschen von Kennungen

Alle benötigten Benutzerdaten im richtigen Format und aus einer einzigen, autoritativen, dauerhaft verfügbaren Quelle

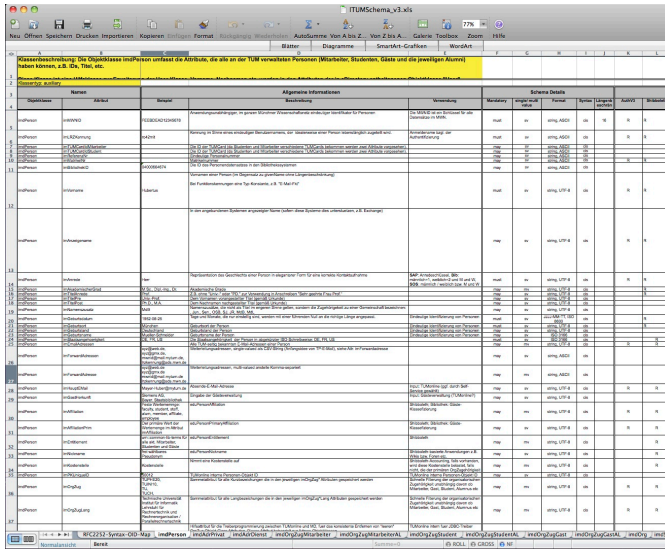
Verringerter Supportaufwand (z.B. vergessene Passwörter)

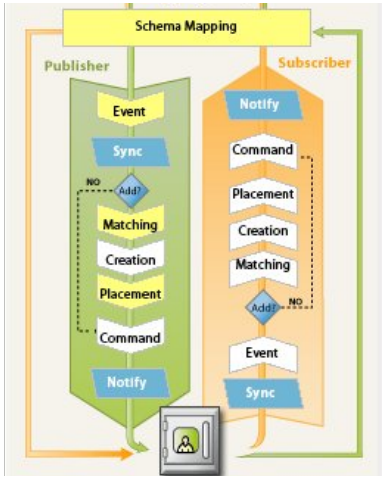
Design und Implementierung

Datenmodellierung pro Verzeichnisdienst:

Personen, Gruppen, Funktionskennungen, Organisationsstruktur und Studiengangs-informationen; Zugriffsberechtigungen

Produkte: Novell eDirectory und OpenLDAP





Konnektoren zwischen I&AM-System und Quellen/Zielen:

Uni- oder bidirektional, event- oder intervallgesteuert, Komplett- oder Delta-Transfer; Datenvolumen und -format

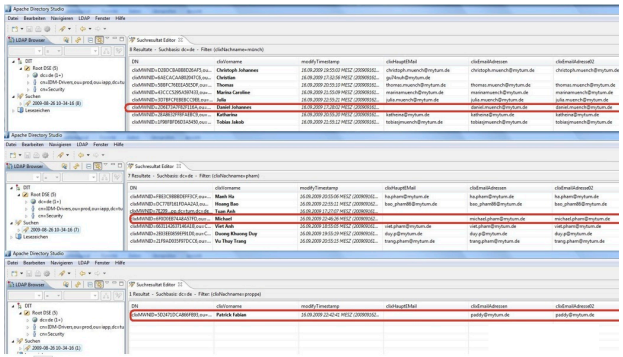
Produkt: Novell Identity Manager (DirXML)

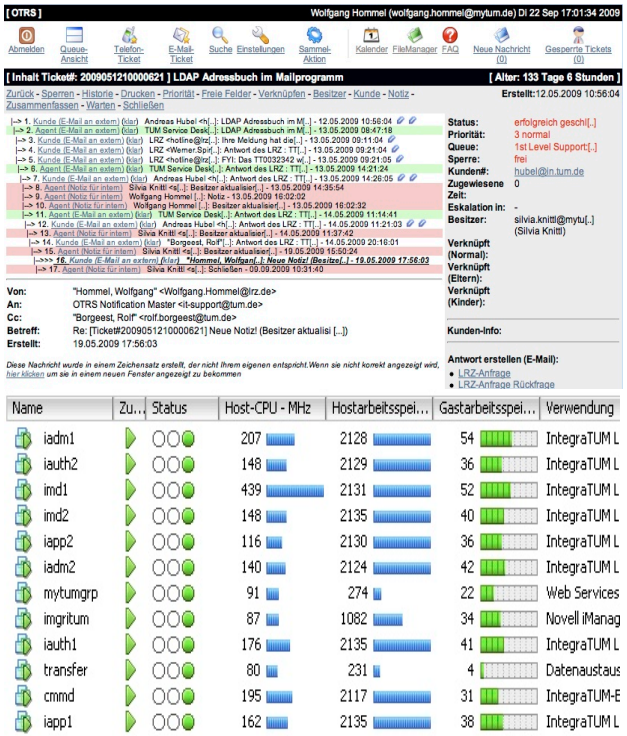
Herausforderungen im Betrieb

Unvollständige, in sich widersprüchliche oder veraltete Personendatensätze (Datenqualität)

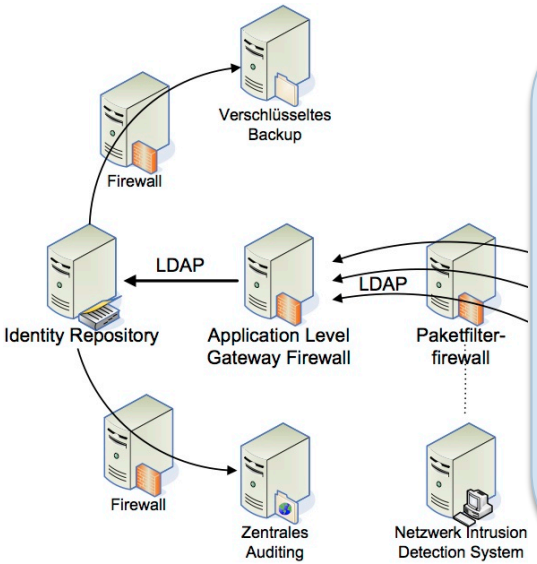
Zurücksetzen vergessener Passwörter, Registrieren von Gästen, Überprüfen von Berechtigungen (TUM IT Service Desk)

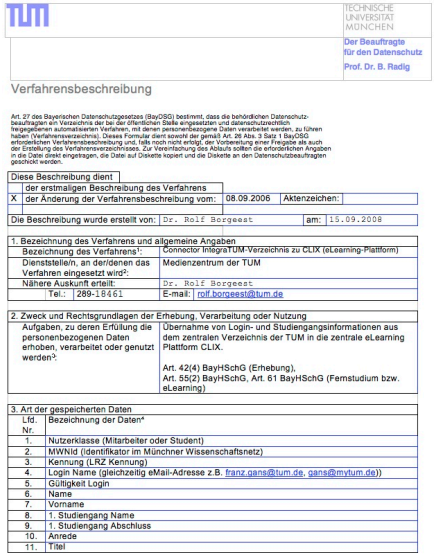
Performance an Stichtagen zur Account-Freischaltung, Initialabgleiche mit neuen Zielsystemen, Resynchronisation nach Ausfall





Sicherheit und Datenschutz





TUM — TECHNISCHE UNIVERSITÄT MÜNCHEN

Der Beauftragte für den Datenschutz
Prof. Dr. B. Radig

Verfahrensbeschreibung

Art. 27 des Bayerischen Datenschutzgesetzes (BayDSG) bestimmt, dass die behördlichen Datenschutzbeauftragten ein Verzeichnis der bei der öffentlichen Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, zu führen haben (Verfahrensverzeichnis). Dieses Formular dient sowohl der gemäß Art. 26 Abs. 3 Satz 1 BayDSG erforderlichen Verfahrensbeschreibung und, falls noch nicht erfolgt, der Vorbereitung einer Freigabe als auch der Erstellung des Verfahrensverzeichnisses. Zur Vereinfachung des Ablaufs sollten die erforderlichen Angaben in die Datei direkt eingetragen, die Datei auf Diskette kopiert und die Diskette an den Datenschutzbeauftragten geschickt werden.

Diese Beschreibung dient			
	der erstmaligen Beschreibung des Verfahrens		
X	der Änderung der Verfahrensbeschreibung vom:	08.09.2006	Aktenzeichen:

Die Beschreibung wurde erstellt von: Dr. Rolf Borgeest am: 15.09.2008

1. Bezeichnung des Verfahrens und allgemeine Angaben	
Bezeichnung des Verfahrens[1]:	Connector IntegraTUM-Verzeichnis zu CLIX (eLearning-Plattform)
Dienststelle/n, an der/denen das Verfahren eingesetzt wird[2]:	Medienzentrum der TUM
Nähere Auskunft erteilt:	Dr. Rolf Borgeest
Tel.: 289-18461	E-mail: rolf.borgeest@tum.de

2. Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung	
Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden[3]:	Übernahme von Login- und Studiengangsinformationen aus dem zentralen Verzeichnis der TUM in die zentrale eLearning Plattform CLIX. Art. 42(4) BayHSchG (Erhebung), Art. 55(2) BayHSchG, Art. 61 BayHSchG (Fernstudium bzw. eLearning)

3. Art der gespeicherten Daten	
Lfd. Nr.	Bezeichnung der Daten*
1.	Nutzerklasse (Mitarbeiter oder Student)
2.	MWNId (Identifikator im Münchner Wissenschaftsnetz)
3.	Kennung (LRZ Kennung)
4.	Login Name (gleichzeitig eMail-Adresse z.B. franz.gans@tum.de, gans@mytum.de))
5.	Gültigkeit Login
6.	Name
7.	Vorname
8.	1. Studiengang Name
9.	1. Studiengang Abschluss
10.	Anrede
11.	Titel

Integration ins LRZ-Serverbetriebskonzept (Zutrittskontrolle, OS-Updates, Patch-Management, ...)

LDAP Access Control Lists (ACLs)

LDAP-Zugriff bevorzugt im User-Kontext (ohne Proxy-User)

Datensparsamkeit: Auslieferung nur wirklich benötigter Benutzerdaten ans jeweilige Zielsystem

Verfahrensbeschreibungen, Zusammenarbeit mit TUM Datenschutzbeauftragtem und Gesamtpersonalrat

Selbstauskunft über TUMonline

Mehr als nur Technik…

Integration in die Hochschulprozesse

Individuelle Unterstützung bei der Dienstintegration

Erfahrungsaustausch und Kooperationen mit anderen europäischen Hochschulen

Integration der Thematik in Lehrveranstaltungen, wissenschaftliche Arbeiten

Ziele für die Weiterentwicklung

Flächendeckender Rollout

Anbindung aller Fakultäten an die Verzeichnisdienste zur Systemadministration

Integration weiterer dezentraler IT-Dienste

Münchenweite Prozesse

Durchgängige Datensynchronisation mit dem LRZ Identity Management

Gezielte Unterstützung hochschulübergreifender Studiengänge

Ausbau von Single Sign-On und DFN-AAI-Nutzung

Shibboleth-Anpassung weiterer zentraler und dezentraler Dienste

Öffnung ausgewählter Dienste für externe Nutzer