



10 Jahre Identity Management Stand, Entwicklungen, Resümee

**Hartmut Hotzel, Andreas Böck
Hochschule München, ZaK**

**ZKI AK Verzeichnisdienste
2008-11-04**

Themen

Strategische Sicht (Hartmut Hotzel)

- Informationen zur Hochschule München
- Identity Management
- Positionierung innerhalb der Hochschule

Technische Sicht (Andreas Böck)

- *Systemkonzept*
- *Systembeschreibung*
- *Aktuelle Entwicklungen*

Resümee



Informationen zur Hochschule München

Hochschule für angewandte Wissenschaften

Munich University of Applied Sciences

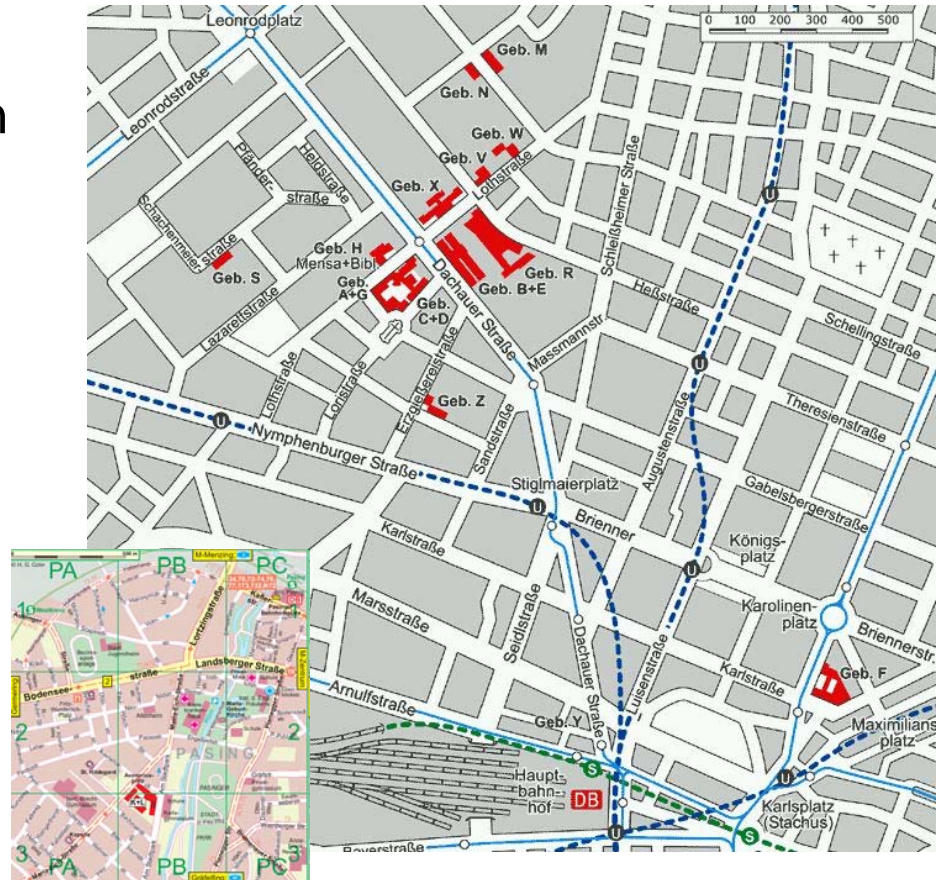
- Ca. 14.000 Studierende in 67 Studiengängen (Master, Bachelor, Diplom), Studienrichtungen Technik, Wirtschaftswissenschaften, Sozialwesen, Design
- Ca. 450 ProfessorInnen
- Ca. 420 MitarbeiterInnen („nicht-wissenschaftlich“)
- Keine festen wissenschaftlichen Mitarbeiter
- Ca. 800 Lehrbeauftragte

<http://www.hm.edu>



IT-Infrastruktur: Netz

- Zentralgelände und 6 größere Außenstellen im Stadtgebiet
- Glasfasernetz (WDM 100 Mbit/s bis 1 Gbit/s) für Daten und Telefon zwischen allen Außenstellen seit 2000
- Anbindung an das Münchner Wissenschaftsnetz / Internet über Leibniz-Rechenzentrum



3D-Darstellung aller Gebäude in Google Earth über www.hm.edu unter Standorte

eGovernance

IT Steuerkreis (seit 2008)

- 3 Dekane (von der erweiterten Hochschulleitung gewählt), Kanzler, Leiter Rechenzentrum
- Trifft verbindliche Entscheidungen für die gesamte Hochschul-IT
- Nimmt Funktionen eines CIO wahr

IT Arbeitskreis

- Vertreter aller Fakultäten, der Bibliothek, der Hauptabteilungen der Verwaltung, Vertreter des Rechenzentrums
- Beratende Funktion + Informationsverbreitung



Zuständigkeiten der zentralen IT

Zentrale IT umfasst

- Rechenzentrum incl. Netzwerk der Hochschule
- IT der Hochschulverwaltung (seit 2001)
- Telefonie (seit 2007)
- Endgeräte-/Endkunden-Betreuung der Fakultäten Betriebswirtschaft, Angewandte Sozialwissenschaften und Tourismus vor Ort (seit 2005)

Dienstleistungsangebote (Auszug)

- Basisdienste für alle Studierenden und Lehrenden (Plattformen, Mail, WLAN, Radius/VPN, Fileservices, Online-Dienste, Customer Self Services, ...)
- Campusmanagement-Software: Entwicklungskooperation PRIMUSS für Studierenden- und Prüfungsmanagement incl. Online-Verfahren (8 Hochschulen, abgekündigt)
- HIS FSV GX & COB, Diapers



Strategische Sicht

- Informationen zur Hochschule München
- **Identity Management**
- Positionierung innerhalb der Hochschule



Vorläufer des Identity Managements

10 Jahre ? Stand 1998:

- Vollständige automatische Erfassung aller Studierendendaten, manuelle Erfassung der Nicht-Studierenden nach Bedarf
 - Plattformübergreifendes Accounting (Unix, Novell, Windows)
 - Bereitstellung einer Hochschulmailadresse
 - Selbstbedienungsterminals an allen Standorten
-
- Mittelbar: Vorbereitung des ersten Online-Verfahrens (Prüfungsanmeldung)

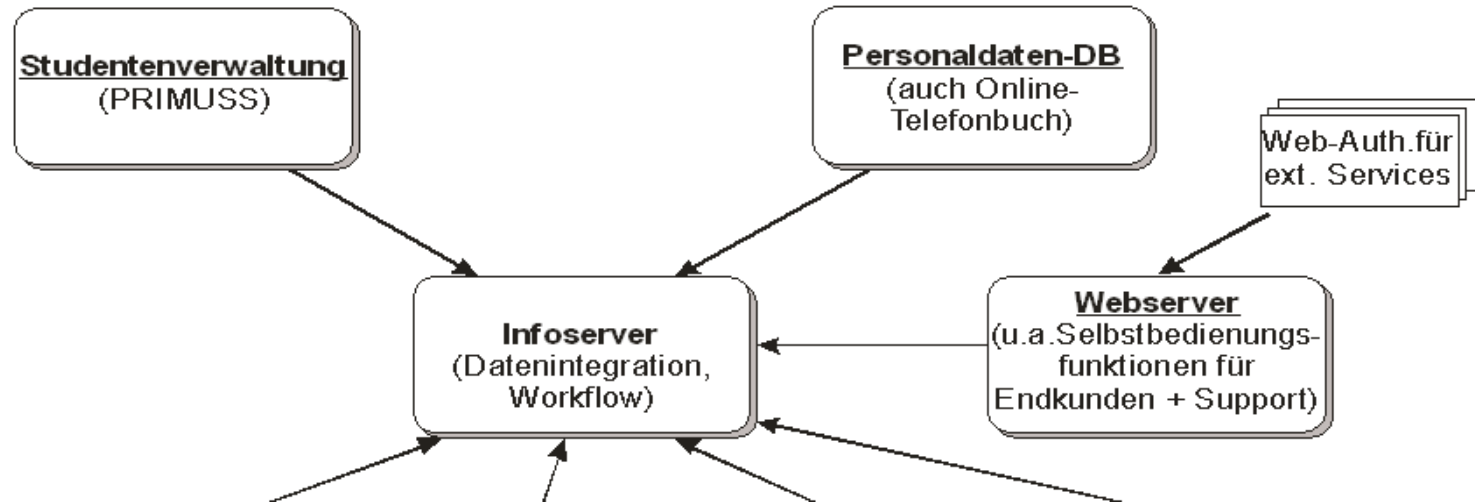


Quellsysteme

Quellsysteme für Personendaten (Ist-Stand)

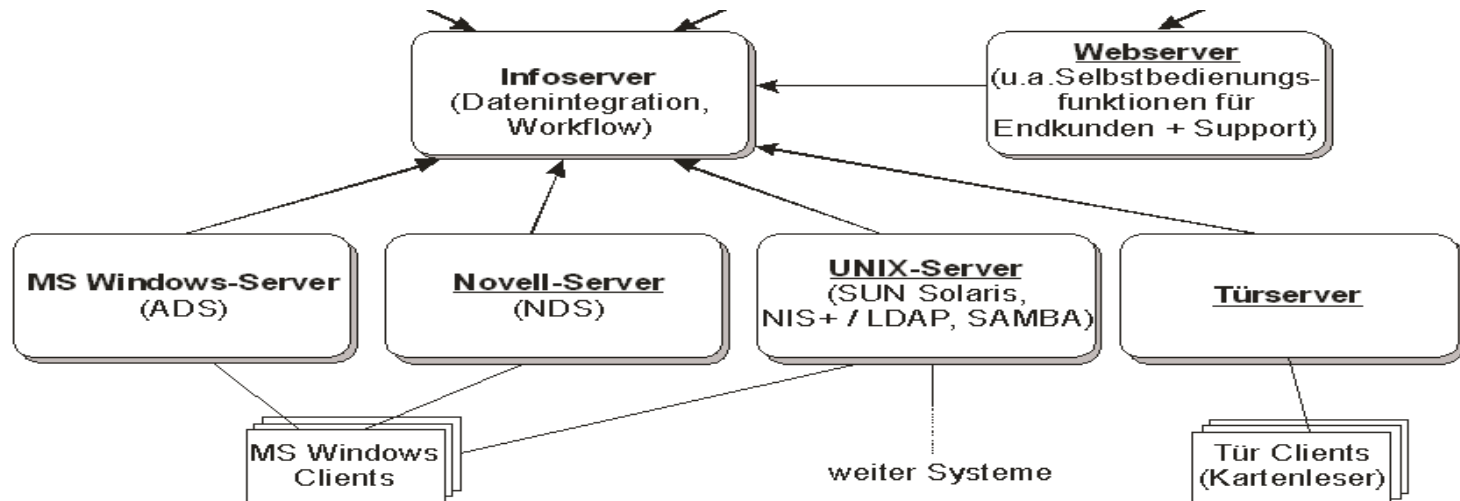
- Studierendenverwaltung – vollautomatisch
- ProfessorInnen und MitarbeiterInnen – halbautomatisch
einheitliche Personalverwaltung in Bayern in Vorbereitung SAP HR Viva Pro
- Lehrbeauftragte – halbautomatisch (workflow noch unvollständig)
- Gäste – nach Autorisierung und Datenerfassung

Alle Personen erhalten personalisierter Studierendenausweis bzw.
Mitarbeiter- oder Gastkarte mit berührungslosem Chip (Legic)

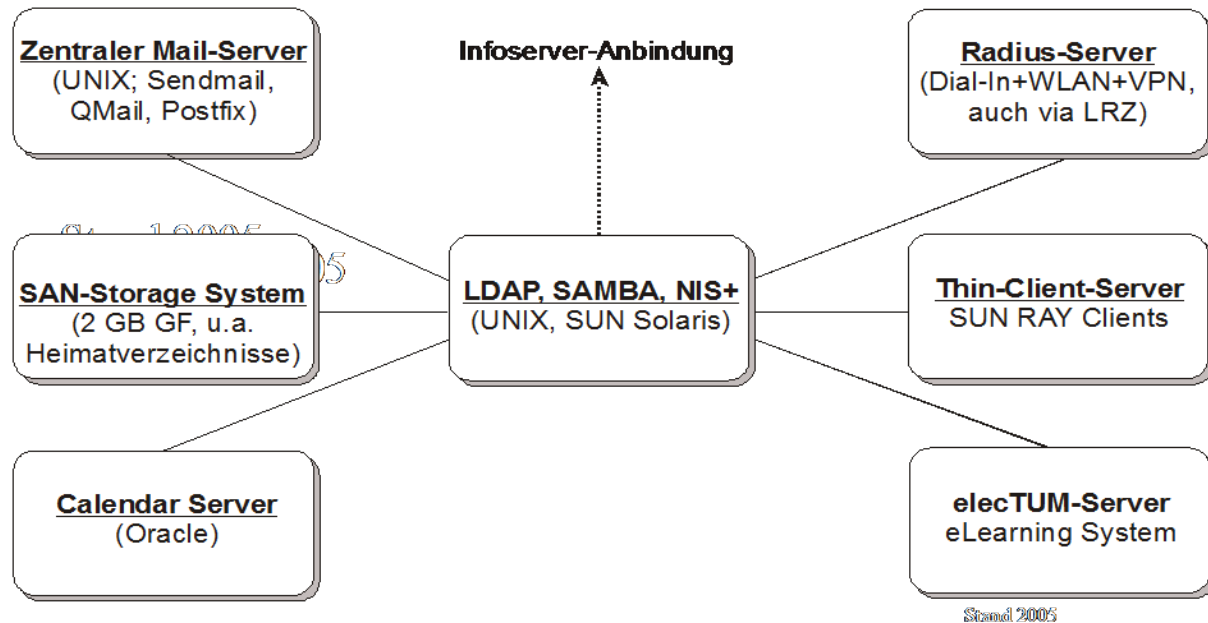


Provisionierung (1)

- Plattformen Unix (Solaris, Linux), Novell, MS AD
- Türzutritt für ca. 200 Labortüren (keine Außenhaut), zentral steuerbar (Nutzer, Zeiten, Räume), regelbasierend
- Online-Telefonbuch, Telefonlisten (intern)
- LDAP-Server mit weiteren Anbindungen



Provisionierung (2)



- Mail incl. Mailinglisten
- Zielgruppenorientiertes Rundmailtool (intern, tagesaktuell)
- Groupware Oracle Collaboration Suite
- Radius-Server / WLAN / Dial-In / VPN (Kooperation der Münchner Hochschulen mit dem LRZ)
- Sun Ray Thin Clients
- Externe Systeme (siehe hinten)

Strategische Sicht

- Informationen zur Hochschule München
- Identity Management
- **Positionierung innerhalb der Hochschule**



Positionierung innerhalb der Hochschule

- Hochschulleitung unterstützt zentrale Bereitstellung von Diensten
- Weitere Konzentration ist von der erweiterten Hochschulleitung beschlossen
- Integration von Diensten erfolgt schrittweise mit Berücksichtigung des Mehrwerts für Endanwender
- Datenschutzbeauftragter und Personalrat sind in aktuellen Entwicklungsprozess einbezogen
- Einbeziehung von externem Know-How



Technische Sicht

Strategische Sicht (Hartmut Hotzel)

- *Informationen zur Hochschule München*
- *Identity Management*
- *Positionierung*

Technische Sicht (Andreas Böck)

- Systemkonzept
- Systembeschreibung
- Aktuelle Entwicklungen

Resümee



Systemkonzept 1

- SQL-Datenbank
 - > Verfügbarkeit beim Start
 - > Datenintegration, Konsolidierung und Workflow über eingebaute Skriptsprache gut abbildbar
- Zugriff auf IDM-Kerndaten jederzeit und vollständig
 - > Nachhaltigkeit der Datennutzung
- Flexibilität: Sowohl Nutzung von Open Source als auch kommerziellen Systemen
 - > keine zu großen Herstellerabhängigkeiten



Systemkonzept 2

- “lose Koppung” zwischen IDM-Kern und Plattformen
-> ermöglicht u.a. Entkopplung der einzelnen Systemverfügbarkeiten
- Anbindung neuer Plattformen über deren native Funktionen (Schnittstellen oder Kommandozeile)
-> direkt mittels PERL-Agent
-> alternativ mittelbar über schon angebundene Plattform (z.B. LDAP)
- Weiter- und Neuentwicklung von Modulen auch unter Einbeziehung externer Partner gut abgrenzbar
- “customer self service”-Funktionen: Authentisierung via individuellem “Personal Identification Code” PIC

Technische Sicht

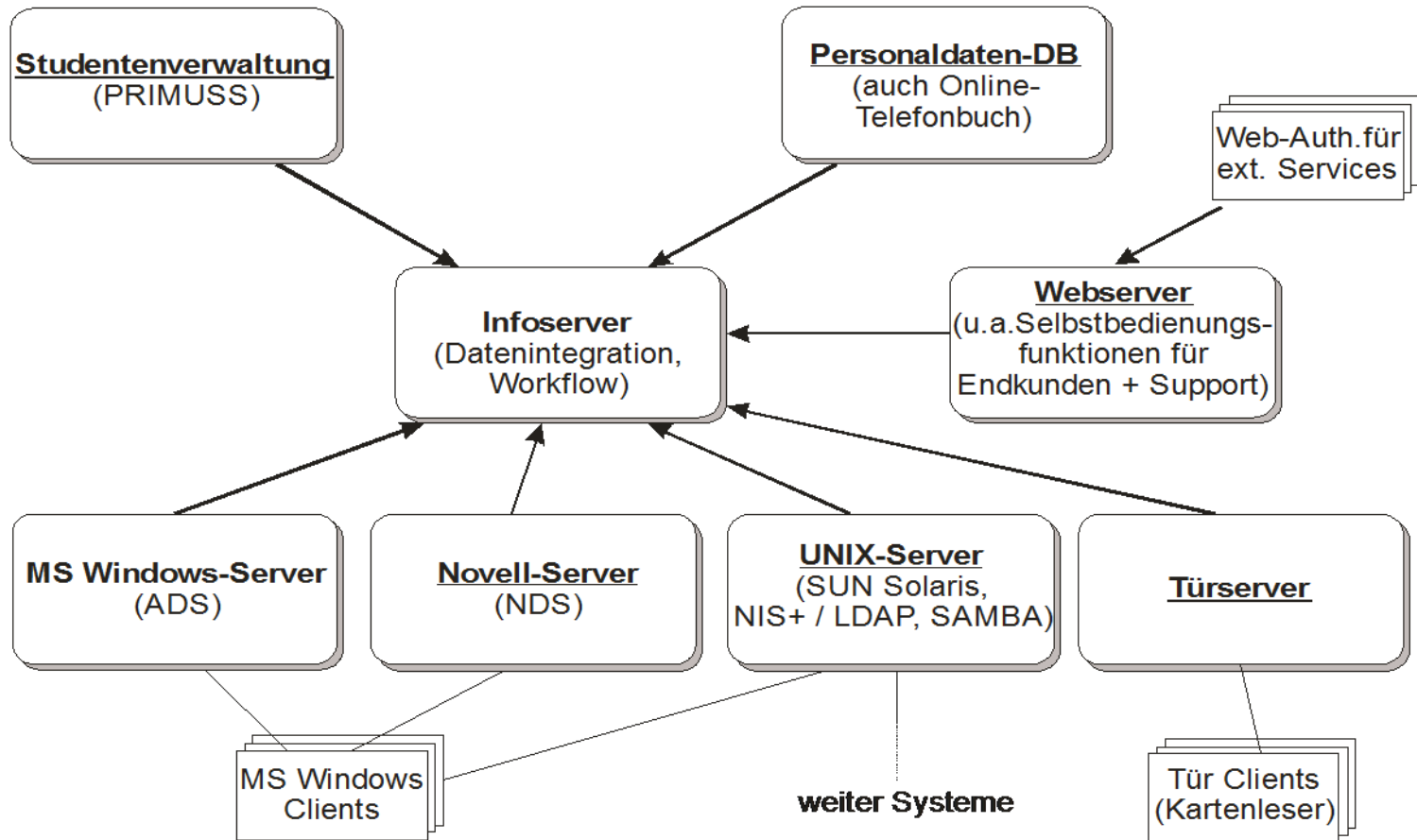
- Systemkonzept
- **Systembeschreibung**
- Aktuelle Entwicklungen

Systembeschreibung 1

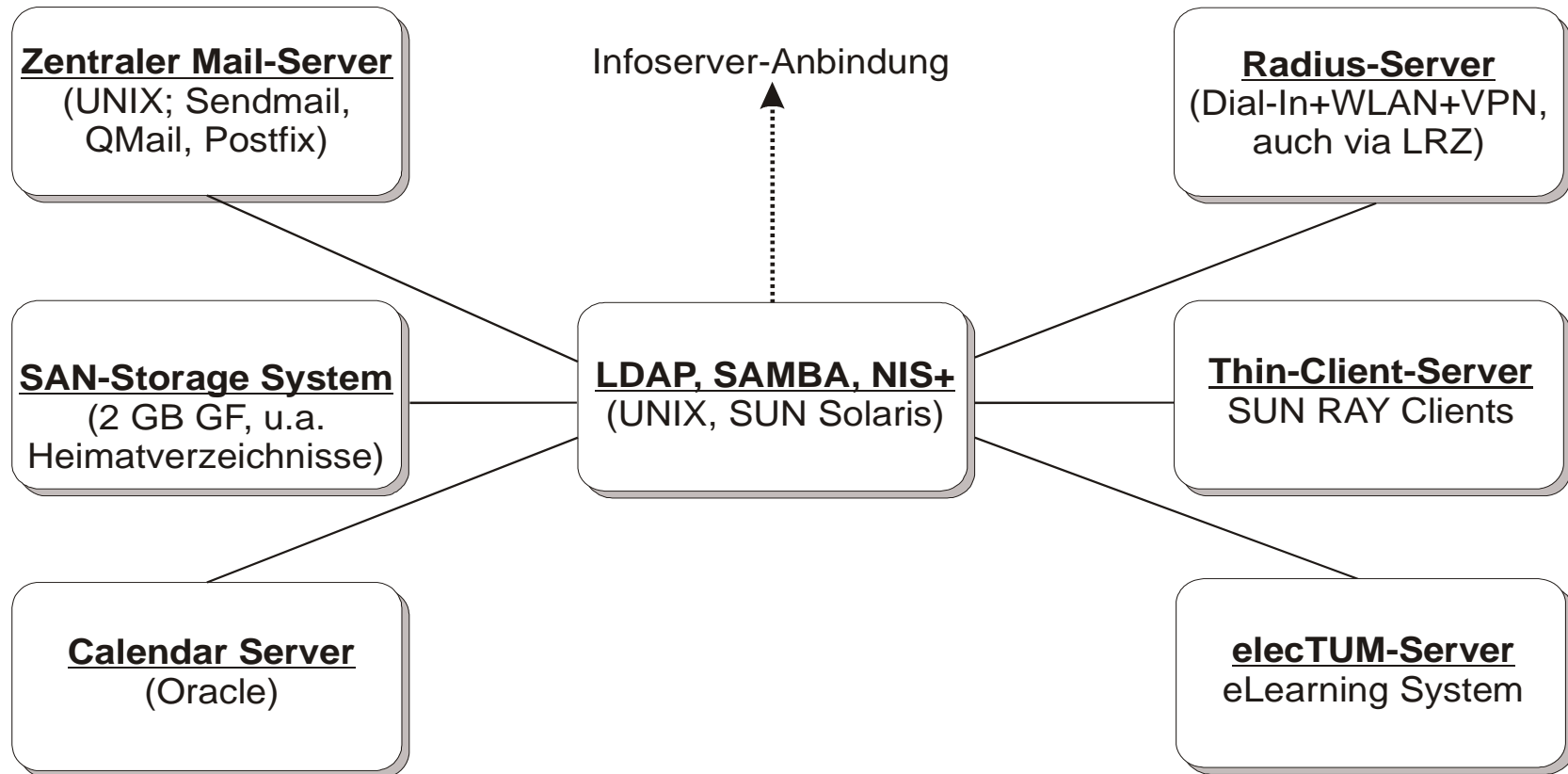
- IDM-Kern: PostgreSQL-Datenbank (“Infoserver/Infobase”)
- Datenimport und Konsolidierung aktionsgesteuert (PERL, PL/pgSQL)
- Workflow-Funktionen aktions- und zeitgesteuert
- Anbindung zu den Plattformen mittels PERL-Agent
- Anbindung der wichtigsten zentralen Dienste (Mail, Radius, Samba) über nachgeschaltete LDAP-Plattform (SUN-Solaris 10, SPARC, SUN-LDAP v5.2, mit eigenem plugin zur Zugriffssteuerung)
- Ausnahme (Direktanbindung):
 - > Anbindung des regelbasierenden Doorservers (campusweit derzeit ca. 200 Türen)
 - > webbasierendes „customer self service“-Interface



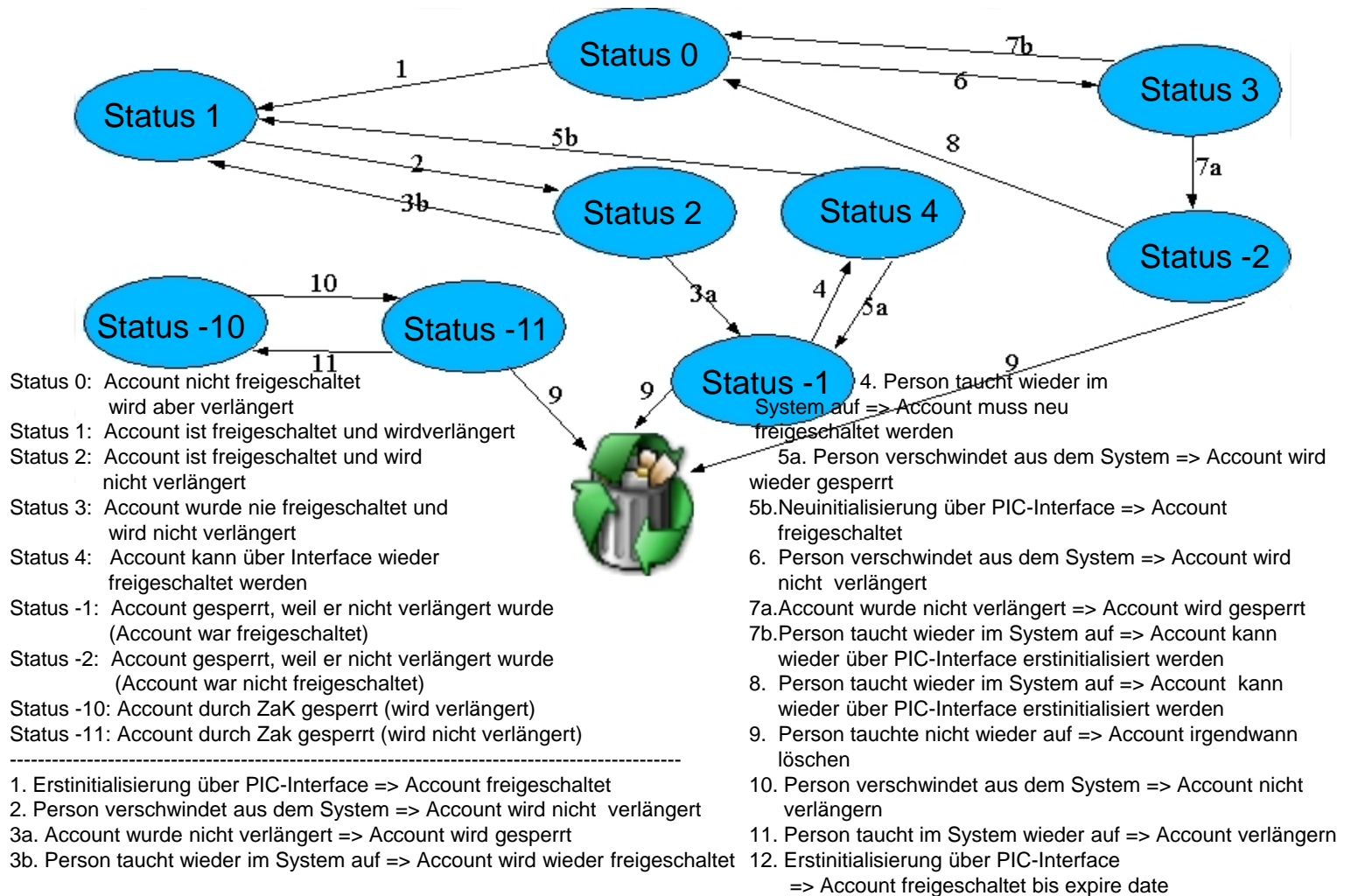
Systembeschreibung 2



Systembeschreibung 3



Systembeschreibung 4



Technische Sicht

- Systemkonzept
- Systembeschreibung
- **Aktuelle Entwicklungen**

Aktuelle Entwicklungen

Anbindung externer Systeme (Ist-Stand)

- Mehrere dezentrale Systeme der eigenen Hochschule
- LRZ (Radius)
- Zepelin: eLearning System der TUM (electum)
- Extern individual-programmiertes System (Auftrag von 3 Fakultäten vor einigen Jahren) mit Funktionen einer Fakultätsverwaltung bei externem Provider

In Vorbereitung

- Shibboleth: erste Testanwendungen + DFN Test-Föderation
- Anbindung der Bibliothek
- Langfristig: Einbindung anderer Organisationseinheiten

Organisatorisch

- DFN AAI, DFN PKI Infrastruktur



Resümee

- + Konzept
- + Integration (Datenquellen und Systeme)
- + Erfahrung im Massenbetrieb
- + Wartungsaufwand
- + Flexibilität

- o Langfristige Verfügbarkeit hinreichend qualifizierter MitarbeiterInnen

- Personal- und Haushaltsrecht

Vielen Dank für die Aufmerksamkeit



Fragen ?