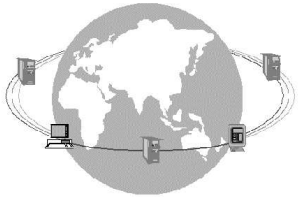
Integrierende Benutzer- und Ressourcenverwaltung an den Thüringer Hochschulen (Meta Directory)



Technische Universität Ilmenau
Universitätsrechenzentrum
Jörg Deutschmann

Gliederung

Einführung und Motivation

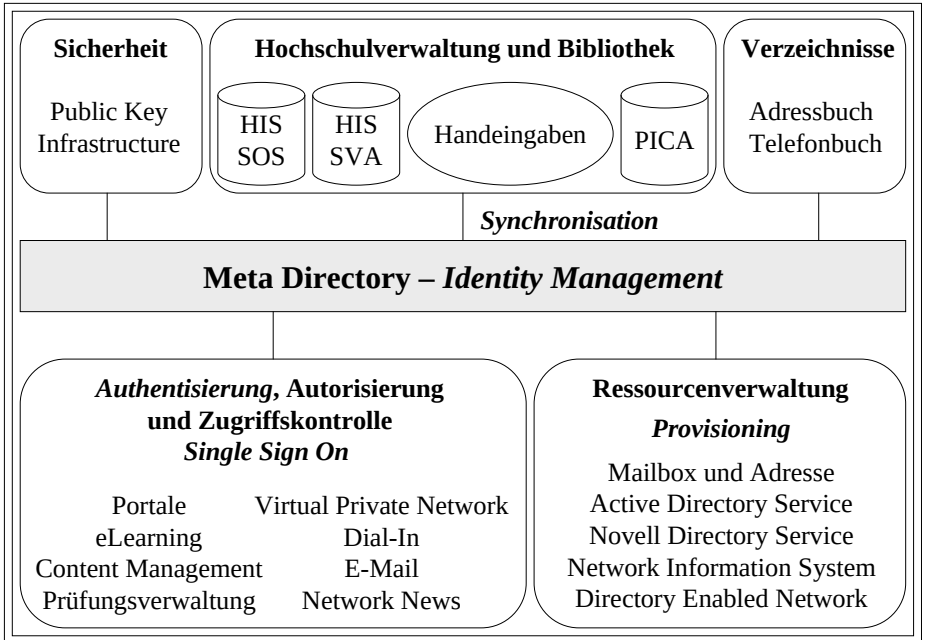
Szenario für einen integrierenden Verzeichnisdienst

Ergebnisse der Analyse- und Entwurfsphase inklusive entstandener Konzepte

Zusammenfassung und Ausblick

Einführung und Motivation

- Steigende Komplexität bei Administrationsprozessen
- Effizienteres Management der Hochschulressourcen
- Akademische Ressourcen 24 X 7 zur Verfügung
- Voraussetzung: integrierendes Identity Management
- LDAP für Benutzer- und Ressourcenverwaltung
- Paradigma des Meta Directory mit Integrationspotential
  - Rahmenwerk, dass durch Synchronisations-mechanismen die Integration unterschiedlicher Verzeichnisse und anderer Informationsressourcen innerhalb einer Organisation oder eines Unternehmens zu einem einzelnen globalen Verzeichnis gestattet und unterstützt



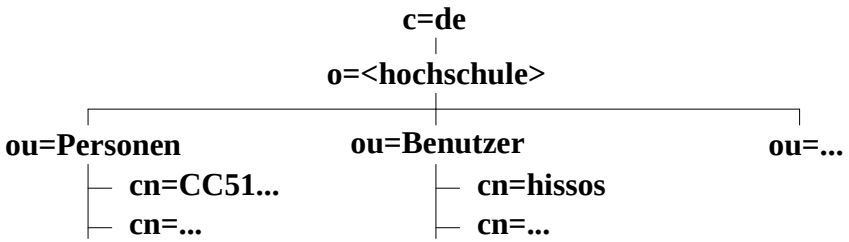
Analyse von Projekten im Umfeld

- **Definition of an European EduPerson** (DEEP) Trans-European-Research and Education Networking Association (TERENA)
- **eduPerson** Internet2 Middleware Architecture Committee Directory Working Group (MACE-Dir), Stand Oktober 2002
- **auEduPerson** West Australian Libraries Authentication Project (WALAP), Stand August 2002
- **gridPerson** Global Grid Forum

Synchronisation mit den operationellen Datenbanken

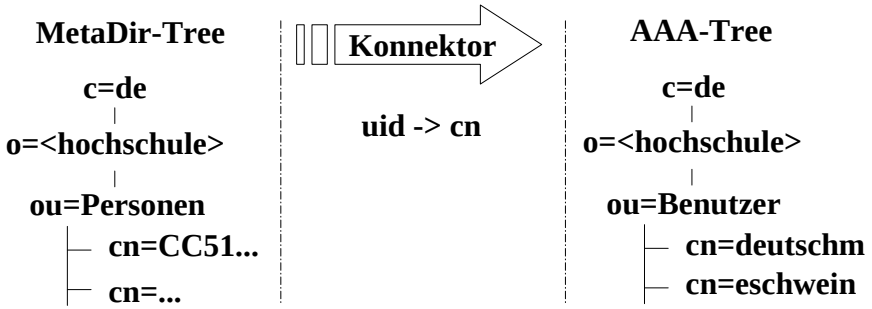
- Detaillierte Analyse von HISSOS und HISSVA und intensive Kommunikation mit den Verwaltungen
- Abbildung zwischen dem relationalen Datenbankmodell und der Verzeichnishierarchie des Meta Directory
  - Tabellen: Anwendung; Attribute HIS, Verzeichnis
- Ziel: direkte, ereignisgesteuerte Aktualisierung
- Problem: Eindeutigkeit der Abbildung
- Bei Erstübernahme von Identitäten Generierung von Daten: Identifikator, Login-Name und E-Mail-Adresse
- Zusammenarbeit mit der HIS GmbH vereinbart

Identitäten, Verzeichnis- und Datenstrukturen



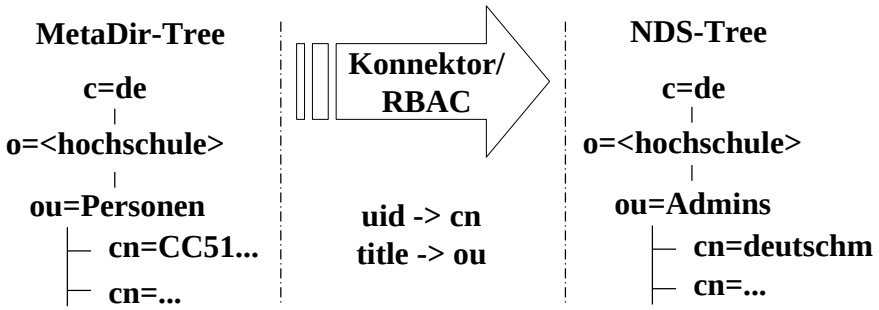
- Identifikation
  - Abstrakter, anwendungsunabhängiger Identifikator
- Objektklassen für Einträge unter Personen
  - person (X.521), organizationalPerson (X.521), inetOrgPerson (RFC 2798), eduPerson (MACE-Dir) und thuEduPerson (Entwurf)

Authentisierung und Single Sign On



- LDAP = zukünftiger Standard bei der Authentisierung
  - Single Sign On für Web-Applikationen und Portale, zentrale Mailboxen, eGroup und Network News, RADIUS, Dial-In, VPN

Provisioning, Rollen- und Gruppenkonzept



- Provisioning mit aufwendiger Routine verbunden
- Rollen: Mitarbeiter, Student, Gast, Alumni
- Verwaltung von Rechten ohne Kenntnis technischer Details der Zielsysteme

Sicherheitskonzept und Datenschutz

- Konstruktiver Datenschutz: Konsultation von Vertretern der Thüringer Landesdatenschutzbeauftragten und der Datenschutzbeauftragten der beteiligten Einrichtungen
- Sicherheitskonzept des Meta Directory
  - Aufnahme nur unbedingt notwendiger Daten
  - Kein direkter Zugriff der Benutzer
  - Verschlüsselung bei den Konnektoren
  - Mit geeigneten Maßnahmen gesichertes Servernetz
  - Informationelle Selbstbestimmung
- Information der Personalräte an den Einrichtungen

Evaluierung von Produkten

- Anforderungen an das Produkt
  - Verfügbare Konnektoren; Scriptsprache; LDAP-Unterstützung; Synchronisierung, Partitionierung, Replikation; Administrationsunterstützung; Referenzen und bestehende Umgebungen
- Betrachtete Produkte
  - Siemens DirXmetahub; Sun ONE Meta Directory; Novell DirXML; Microsofts Meta Directory Services; Critical Path Meta-Directory; MaXware Identity Management Suite; IBM Directory Integrator; Syntegra Global Directory Server / Meta Edition

Zusammenfassung und Ausblick

- Analyse und Entwurf als Ausgangspunkt für die Erstellung des Pflichtenhefts und zur Qualitätssicherung
- Produktentscheidung und intensive Consulting-Phase
- Implementierung entsprechend der Prioritäten parallel zum produktiven Betrieb
  - Pilotumgebung für HISSOS und HISSVA
  - Authentisierungsserver
- Testphase und Einführung in das produktive Umfeld
- Phase der Weiterentwicklung
  - Bibliotheksverwaltung PICA; Chipkarte und PKI; u.a.
  - Abbildung komplexer Regelwerke und Rollenmodelle