R|R|Z|N

Das Projekt SOI Niedersachsen - Service Orientierte Infrastruktur

Reinhard Obendorf
Systemtechnik, RRZN
Universität Hannover

ZKI-Arbeitstreffen Zentrale Verzeichnisdienste
Ilmenau, 15. - 16. Dez. 2004

Gliederung

[Formalia]
- Hintergrund
- Vorarbeiten
- Kooperation
- Ziele
- Organisation
- Risiken
- Phasen
- Arbeitspakete

[my 2¢]
- Rechte
- Namen
- Kiosk+WebISO

[Bericht]
- Inventur 0604 (RRZN)
- Betrieb 1204 (TU BS)
- Konzept (Sun)
- Zusammenfassung

Hintergrund

Die Entwicklungen im Informations- und Medienzeitalter führt die im nationalen und internationalen Wettbewerb stehenden Hochschulen zu neuartigen Herausforderungen im Felde der Lehr- und Lernkultur sowie der neuen bzw. entwickelten Formen der Wissensvermittlung und Kommunikation. Alle Bereiche einer Hochschule bedienen sich zur Bewältigung ihrer Aufgaben in Lehre, Forschung und Entwicklung sowie ihrer administrativen Aufgaben in vielfältiger Weise der Informationstechnologie und der neuen Medien. ...

... neuen Dienste erfordern

- eine Infrastruktur, die die Integration von Lehre, Lernen und Forschung sowie Verwaltungs-, Organisations- und Planungssysteme ermöglicht.
- Ein Planungs- und Management-System für alle Bereiche der Hochschule.
- Eine virtuelle Infrastruktur, die über die bisherige Infrastruktur der Hochschule hinausgeht (Zusammenspiel von Service-Einrichtungen untereinander, mit Fakultäten, Fachbereichen, Instituten und Verwaltung).
- ...

Aus „Vereinbarung zur Konzeptentwicklung und zum Aufbau einer Service-orientierten Infrastruktur an den niedersächsischen Hochschulen zwischen dem Niedersächsischen Ministerium für Wissenschaft und Kunst und der Sun Microsystems GmbH“

Vorarbeiten

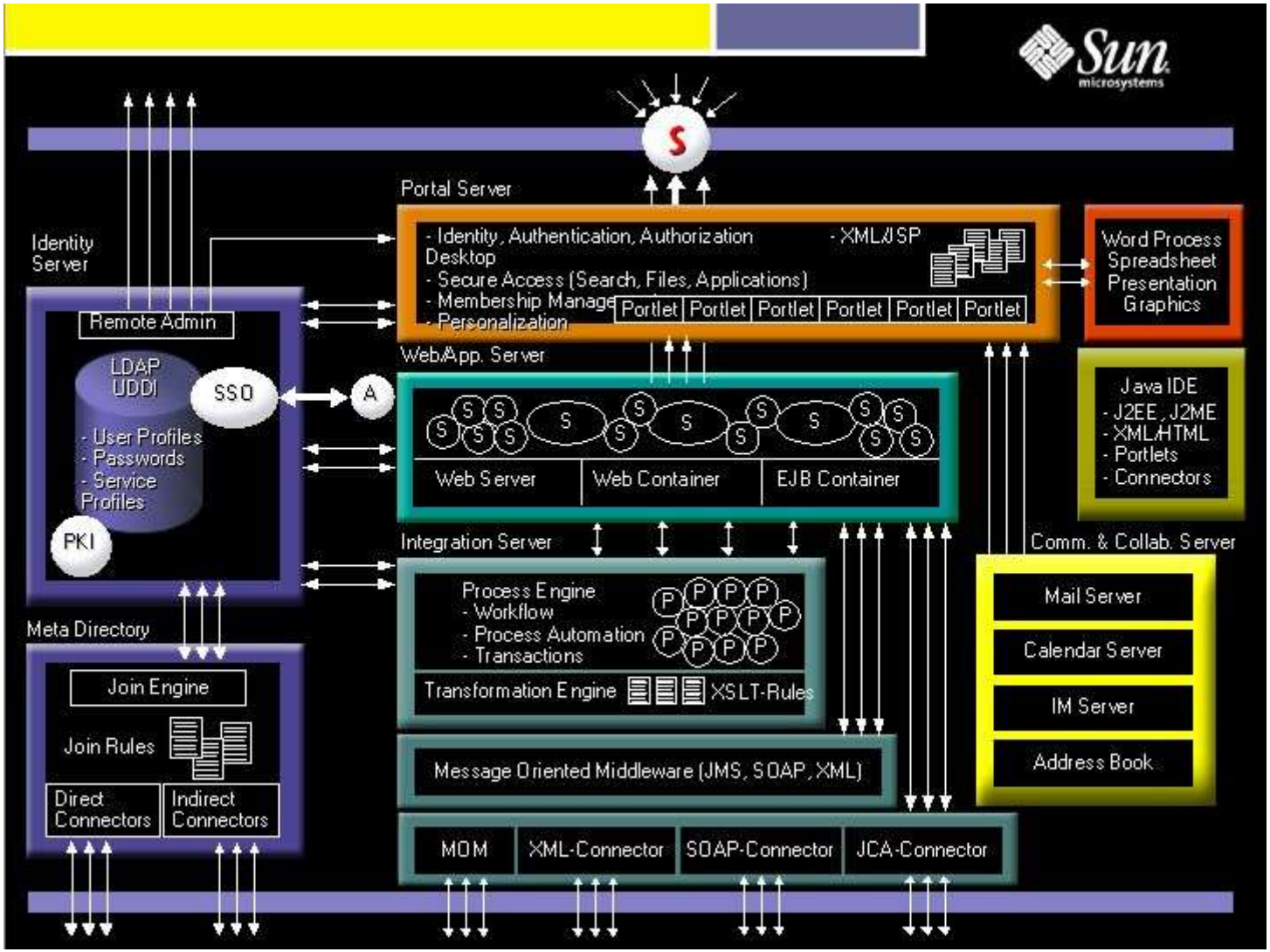
Konzept einer Service-orientierten Infrastruktur von Sun Microsystems

- Web-Services zur Integration von Anwendungen
- zentrales Identitätsmanagement für eine Site
- Network-Identity-Management zum Zugriff auf andere Sites

Erfahrungen in einer (mehr als) 18 Monaten laufenden Kooperation mit der FH Braunschweig/Wolfenbüttel als Center of Excellence

Vorstellung in einem Workshop am 26.11.2003 in Hannover mit Leitern der Hochschul-Rechenzentren in Niedersachsen

Am 07.05.2004 Start der Sun/NI Kooperation mit Sitzungen mit LANIT sowie UH (Präsidium), TIB, RRZN und Sun Microsystems



Java Enterprise System Architektur

Quelle: Vortrag Daniel Meyer, Senior Solution Architect, Sun Microsystems, RRZN Hannover, 26.11.2003

Kooperation

Projektpartner ist **Arbeitskreis des LANIT** [1] mit u.a. Vertretern

- der Universität Hannover,
- der Technischen Universität Braunschweig,
- der Technischen Universität Clausthal,
- der Universität Oldenburg und
- der Fachhochschule Braunschweig/Wolfenbüttel

Übernahme der Aufgaben eines **Kompetenz- und Pilotierungs-Zentrums** durch

- das Regionale Rechenzentrum für Niedersachsen an der Universität Hannover,
- das Rechenzentrum der Technischen Universität Braunschweig,
- das Rechenzentrum der Technischen Universität Clausthal und
- das Rechenzentrum der Fachhochschule Braunschweig/Wolfenbüttel

in Kooperation

[1] LandesArbeitskreis Niedersachsen für InformationsTechnik / Hochschulrechenzentren

Ziele

- Definition eines einheitlichen Identitäts-Management-Konzepts, das als Basis für eine Service-orientierte Infrastruktur dienen soll
- Definition eines gemeinsamen Kerns für ein Datenmodell (Schema), den damit verbundenen Prozessen und ein Rollenkonzept
- Entwicklung von „Best-Practice"-Konzepten
- Aufbau eines Support-Netzwerkes

Aus „Vereinbarung zur Konzeptentwicklung und zum Aufbau einer Service-orientierten Infrastruktur an den niedersächsischen Hochschulen zwischen dem Niedersächsischen Ministerium für Wissenschaft und Kunst und der Sun Microsystems GmbH"

Verantwortlichkeiten im Projekt

Lenkungsausschuss

- Abstimmung und Abnahme der Projektplanung/technischen Planung
- Entscheidung über Changes, Abnahmen, lokale Abnahmen
- Kommunikation mit anderen Bereichen der Hochschule

Technische Kontakte

- Realisierung der Arbeitspakete, Durchführung der Abnahmen

Projektleitung

- Project Initiation Document, Statusberichte, Issuelist
- Begleitung von Changes und Abnahmen

Organisation	Administrativer Kontakt	Technischer Kontakt
SOI-Arbeitskreis		
RRZN Hannover	Herr Schulze-Cremer	Herr Kamps, Herr Obendorf
TU Braunschweig	Herr Busch	Herr Dümpert, Herr Pilka
TU Clausthal	Herr Sarman	Herr Sarman
FH Braunschweig/Wolfenbüttel	Herr Franke	Herr Ludewig
U Oldenburg	Herr Sauer	Herr Weiss, Herr Reil
Andere Projektpartner		
Verbundzentrale des GBV	Herr Diedrichs	Herr Kinstler
Sun	Herr Kosnetzow, Frau Schiering (Projektleitung)	Herr Scherbach

Risikoumfeld des Projektes

- Verarbeitung personenbezogenener Daten
  - ständige Abstimmung mit Verantwortlichen der Hochschule
  - Verzögerungen des Projektes möglich
  - einzelne Dienste eventuell nicht realisierbar
- Anzahl der Projektpartner
  - 5 Hochschulen, VZG und Sun
  - Abstimmungen und Abnahmen gemeinsam

Phasen

Phase 1:

- Istaufnahme
  Klassifizierung vorhandener Systeme, statisches Modell basierend auf Istdaten
- Erstellung eines Feinkonzepts
  Definition Datenschema, Identitäten, Rollen, Attributen als Basis eines Autorisierungskonzepts
  Liste zu integrierender Anwendungen und Nutzerverwaltungen
  Synchronisations- und Provisionierungsregeln, Workflow
  Sicherheitskonzept
  Systemarchitektur, Testszenarien
  Produktvorschläge, auch Open-Source-Produkte
- ...

Phasen

Phase 1:

- Istaufnahme
- Erstellung eines Feinkonzepts
- Aufbau eines Kompetenz- und Pilotierungszentrums
- Dokumentation

Phase 2

- Umsetzung des entwickelten Feinkonzeptes in den einzelnen Hochschulen
- Unterstützung und Ressourcen des Pilotierungszentrums
- Angebote von Sun für Hardware und Software (Pauschale)

Arbeitspakete (Quelle PID)

- Vorschlag Architektur, Auswahl der Dienste, Auswahl der Standorte (MS 1)
  - Architektur
  - Evaluierung HIS, PICA, SAP/HR
  - Evaluierung LDAP-Proxy
  - Vorbereitung Realisierung Hochschulen
  - Sammlung Use-Cases (Hochschul-übergreifend)
  - Statisches Modell (MS 2)
    - Realisierung am Standort RRZN Uni Hannover (MS 3)
    - Realisierung am Standort RZ TU Braunschweig (MS 3)
    - Realisierung am Standort RZ TU Clausthal (MS 3)
      - Realisierung PICA, HIS, SAP/HR
      - Zusammenschalten der lokalen Piloten und Abnahme Use-Cases (MS 4)
        - Dokumentation und Präsentation der Ergebnisse (Projektabschluss)

[my 2¢] Rechte	= Berechtigungen zur Nutzung von Diensten für Angehörige der Hochschule
Grundrechte {	Benötigen
▪ Zugang Intranet/Internet	Bereitstellung Infrastruktur
▪ WLAN	+Sicherheit, VPN
▪ Surfen	+(Terminal-) Login
▪ Web-Mail (E-Mail) }	+remote IMAP(S), SMTP-Relay, Filter
Rollenrechte {	Benötigen
▪ Nutzung Rechner	Ressourcen-Management, Accounting
▪ E-Learning	+Bibliotheksnutzung
▪ Drucken }	+materielle Auslieferung
Sonderrechte {?}	Gastrechte für Gäste der Hochschule?
Vorrechte (Privilegien) {?}	Administrator der Administratoren?

[my 2¢] Namen

Authentifizierung:

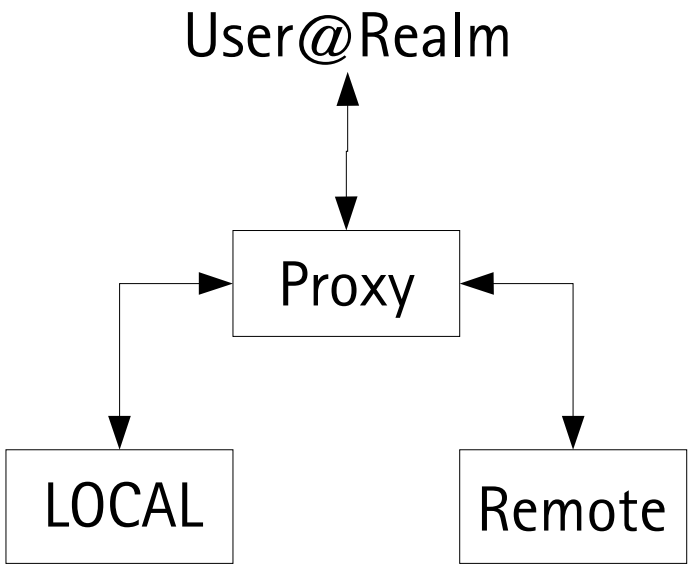
- username + password
- bei Unix, Windows, Anwendungen etc.

dazu Eingabefelder mit

- Syntax-Check, Zeichensatz, Längen
- Plausibilität (Forms)

PAM-gesteuerte Software

- LDAP, Radius > LDAP



mueller3[@uni-hannover.de]
meyer5[@institut.uni-hannover.de]

Mapping?
Meta-Mapping?

[my 2¢] Kiosk+WebISO

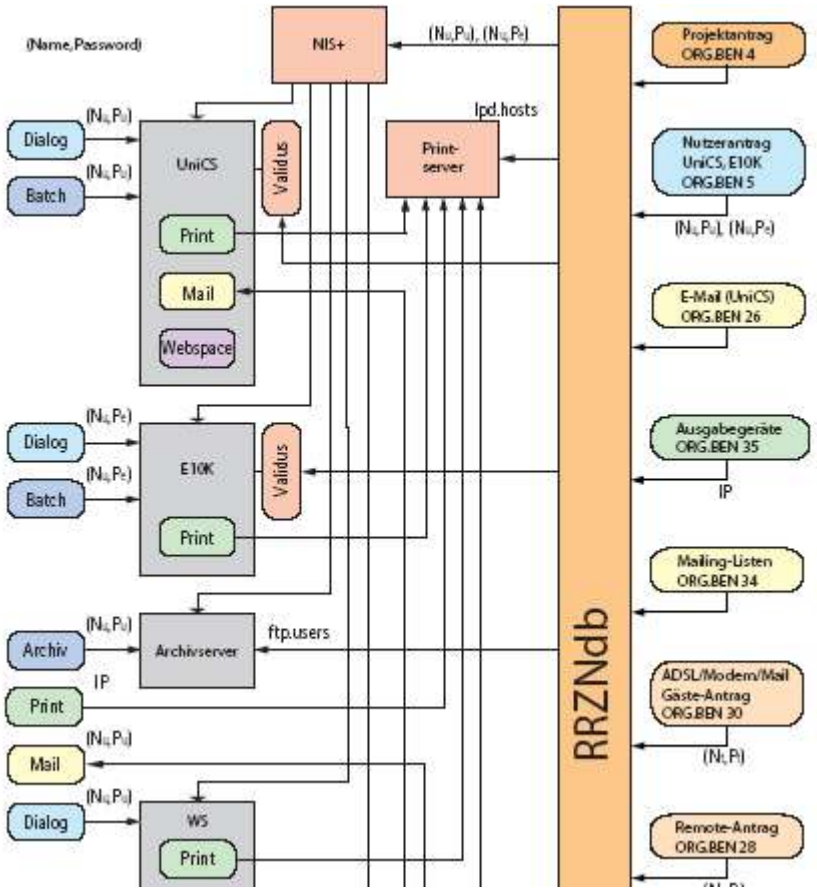
Services vornehmlich als Web-basierte Anwendungen einführen/umstellen

realisierbar mit den Methoden

- Kiosk - geschlossene Umgebung für spezielle Services
- WebISO - Web Initial Sign On (erzeugt Token/Cookies zur weiteren Verwendung, auch Domänen-übergreifend)
- Portal – Aufruf-Container für Web-Services (Servlets) kombinierbar mit Kiosk und WebISO

Probleme durch fremde Domänen:

- Cookies Domänen-abhängig <– Mapping auf latente, virtuelle ID@LOCAL
- Lebensdauer <– Messung von Inaktivität, vollständige Vernichtung
- Identity theft (Ausspähen, Shanghaien, Kenntnis von Bildungsregeln) <- gesicherte URLs, Ports, Zertifikate (User, Server)



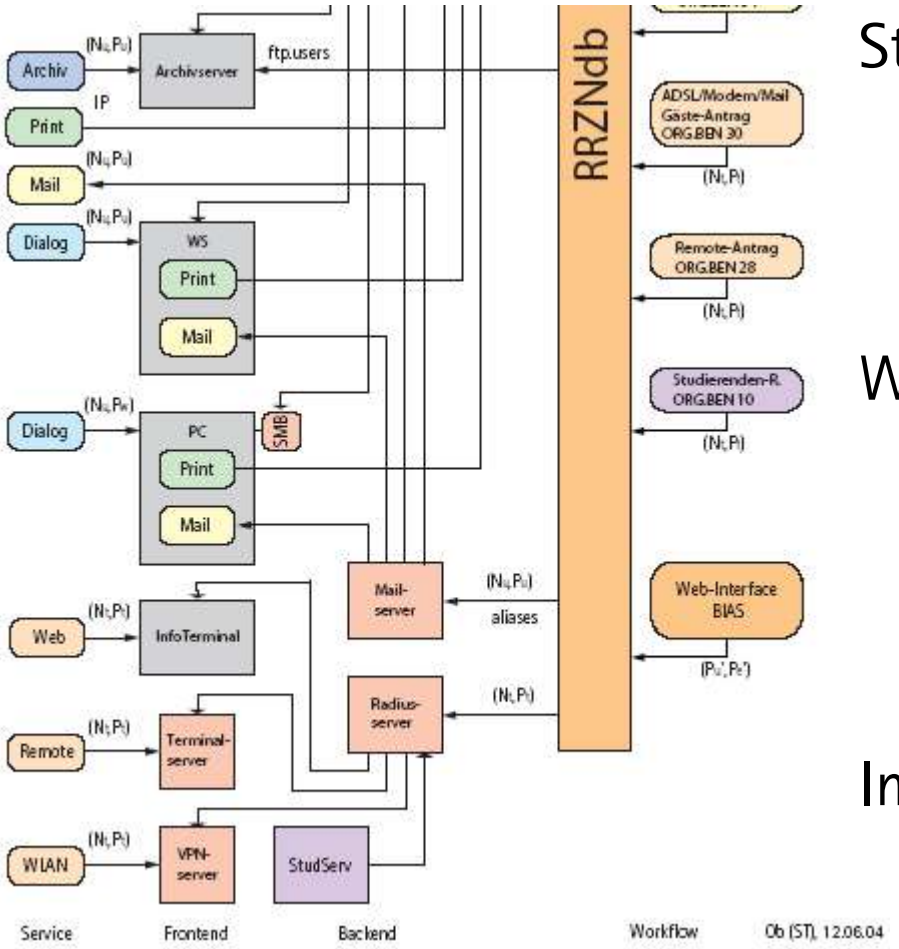
Service-Infrastruktur im RRZN

Stand Juni 2004

- Am Anfang steht der Projektantrag; zugeteilte Projektnummer ist Schlüssel der Oracle-Datenbank RRZNdb
- Anträge für Dienste basieren auf Projektantrag
- Kategorien für Nutzer
  - Projektmitarbeit
  - Institutszugehörigkeit
  - Studierendenstatus
  - Mit Einführung der CA erstmals *Person*

Service-Infrastruktur im RRZN

Stand Juni 2004



Studierende

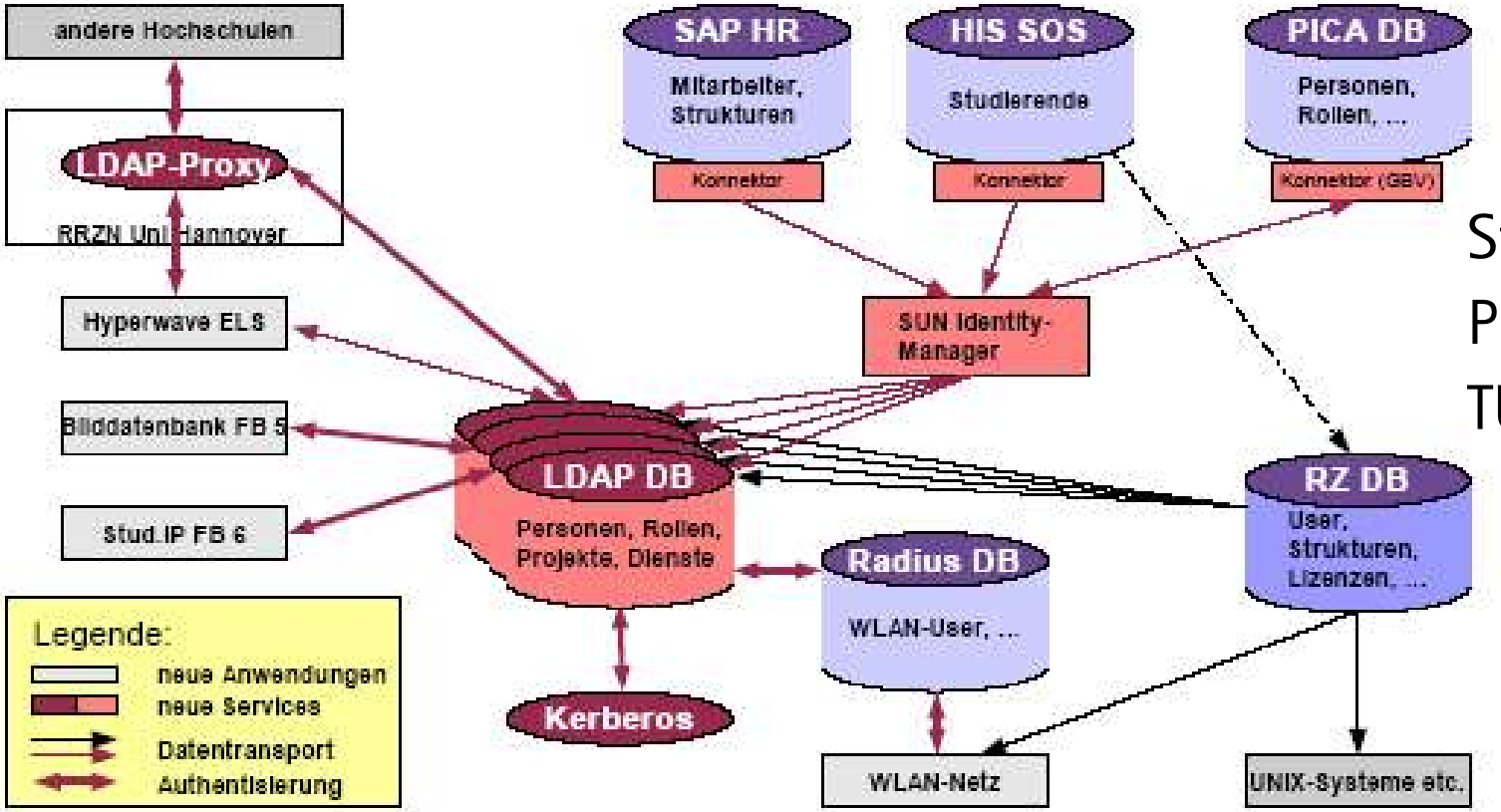
- Studierenden-Server seit 1996
- Internet-Zugang, Home, Mail, Software

Weitere interne User-DBs für

- CMS (Typo3),
- Zeiterfassung (GLAZ),
- Groupware (Ogo),
- diverse Sondernutzungen (Holobench)

InfoTerminals

RZ TU BS / LANIT Service-orientierte IT-Infrastruktur



Stand und Planung in TU Braunschweig

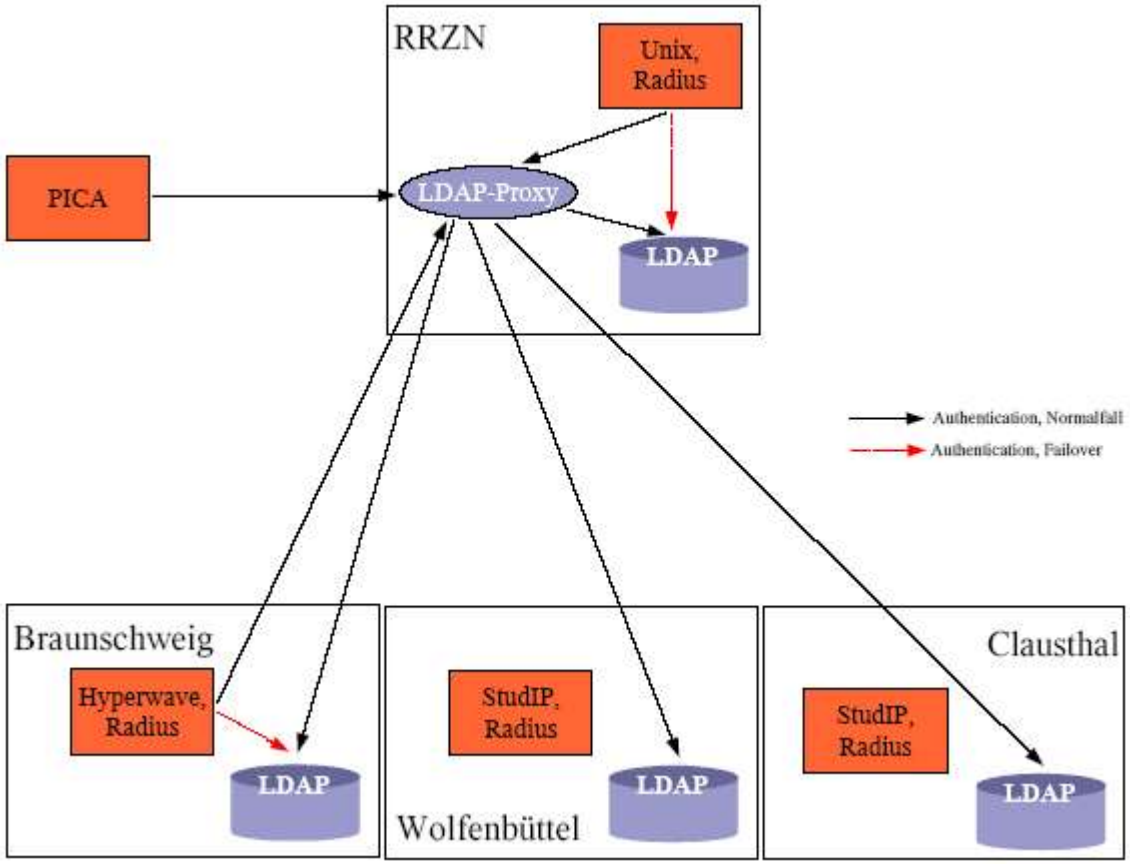
14.12.2004 1 Dr. Wolfgang Busch, Rechenzentrum TU Braunschweig

Stand 12.04

Hardware: 4 SunFire 210 (2 CPU 1 Ghz, 2 GB RAM, 2x36 GB Disk, 4 TP
2 SunFire 240 (2 CPU 1,28 Ghz, 2 BG RAM, 2x36 GB Disk, 4 TP
Aufstellung im RRZN, Integration mittels VPN nach BS und CLZ
VPN mit IPSec z.Zt. nicht realisierbar, Verschlüsselung mit SSL

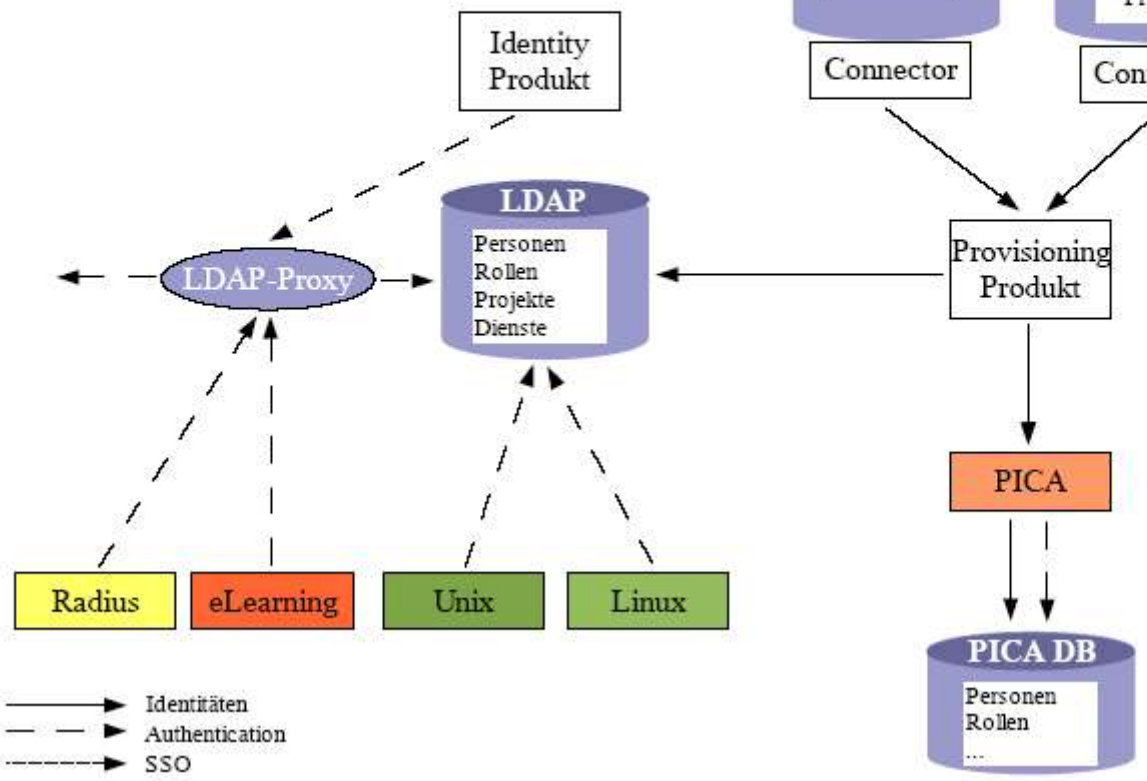
Software: Sun JES Access Manager (SSO, Policies, Adm. Access Management)
Sun JES Identity Manager (Connectoren, auto/manuell Provisioning)
Sun JES Directory Server (DB User+Konfig, Policies, Organisation)
Sun JES Web Server (Laufzeitumgebung für Access Manager)
Sun JES Application Server (Laufzeitumgebung für Identity Manager)
LDAP-Proxy (symLabs) Verteiler Authentisierungs-Requests
(Oracle 9i RDBMS (Konfigurations-DB für Identity Manager) für große Installationen)

Architektur für LDAP-fähige Anwendungen



Quelle: Klaus Scherbach, Architektur für SOI, 12/04

PoC - Authentication



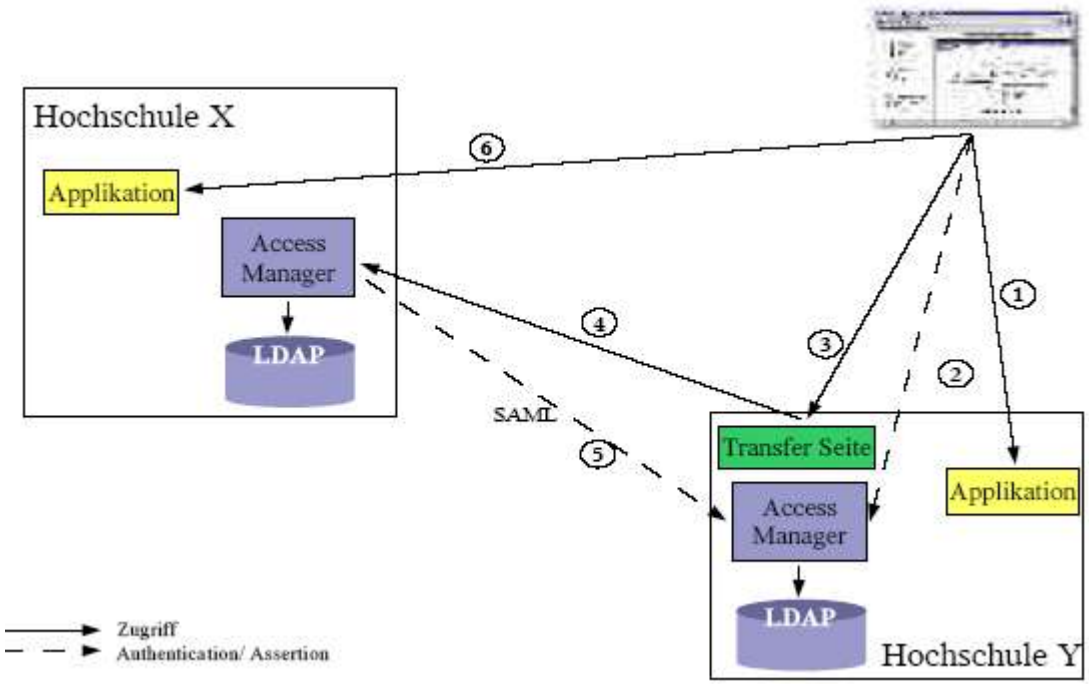
Anwendungen mit Authentisierung gegen eigene Nutzer-Datenbank

Erzeugen der Datensätze aus
- HIS-SOS für Studierende
- SAP/HR für Mitarbeiter

Nutzung über LDAP-Proxy für angeschlossene Hochschulen

Quelle: Konzeptvorschlag Klaus Scherbach, Senior Consultant, Sun Microsystems, 25.08.2004, Seite 21

Architektur für SSO-fähige Anwendungen (auch Standort übergreifend)



LOCAL:
Auswertung des SSO-Tokens;
initial Umlenkung auf Login-Seite des Access Managers

Remote:
SSO-Tokens mittels Cookies mit Bindung an DNS-Domain;
Access Manager auf Basis von SAML;
Mechanismus ähnlich Liberty, jedoch weniger komplex;
Transfer über abgestimmte URLs

Quelle: Klaus Scherbach, Architektur für SOI, 12/04

Zusammenfassung

- Gute Zusammenarbeit der beteiligten Rechenzentren mit Sun
- Jeweils Gespräche mit den einzelnen Verwaltungen (HIS und SAP/HR) und Bibliotheken (PICA), noch etwas interne Missionierung nötig, daher Proof of Concept angestrebt
- Bei Bibliotheken durch Mitarbeit der VerbundZentraleGöttingen Lösung für PICA in Aussicht, Interesse im Bereich statischer Dokumente und eLearning
- Unterstützung des MWK (Informationsmanagement, eLearning)
- Beginn der SW-Evaluierung, Abstimmungen
- Konzept mit Standort-übergreifender Funktionalität, daher adäquate Schemata „globalisieren“
- PoC, Ende der (Pilotierungs-) Phase 1, CeBIT ?
- ...