Verzeichnisdienste
–
Übersicht und Anwendungen

DFN Nutzergruppe Hochschulverwaltungen
„Auflösung der Verwaltungsgrenzen“

H. Stenzel, FH Köln
Braunschweig, 10.5.2005

Worum geht's?

- Personenbezogene Verzeichnisse in Hochschulen
- ZKI-Arbeitskreis Verzeichnisdienste
- Hochschulaktivitäten in Deutschland

Verzeichnisse und Identity Management in Hochschulen

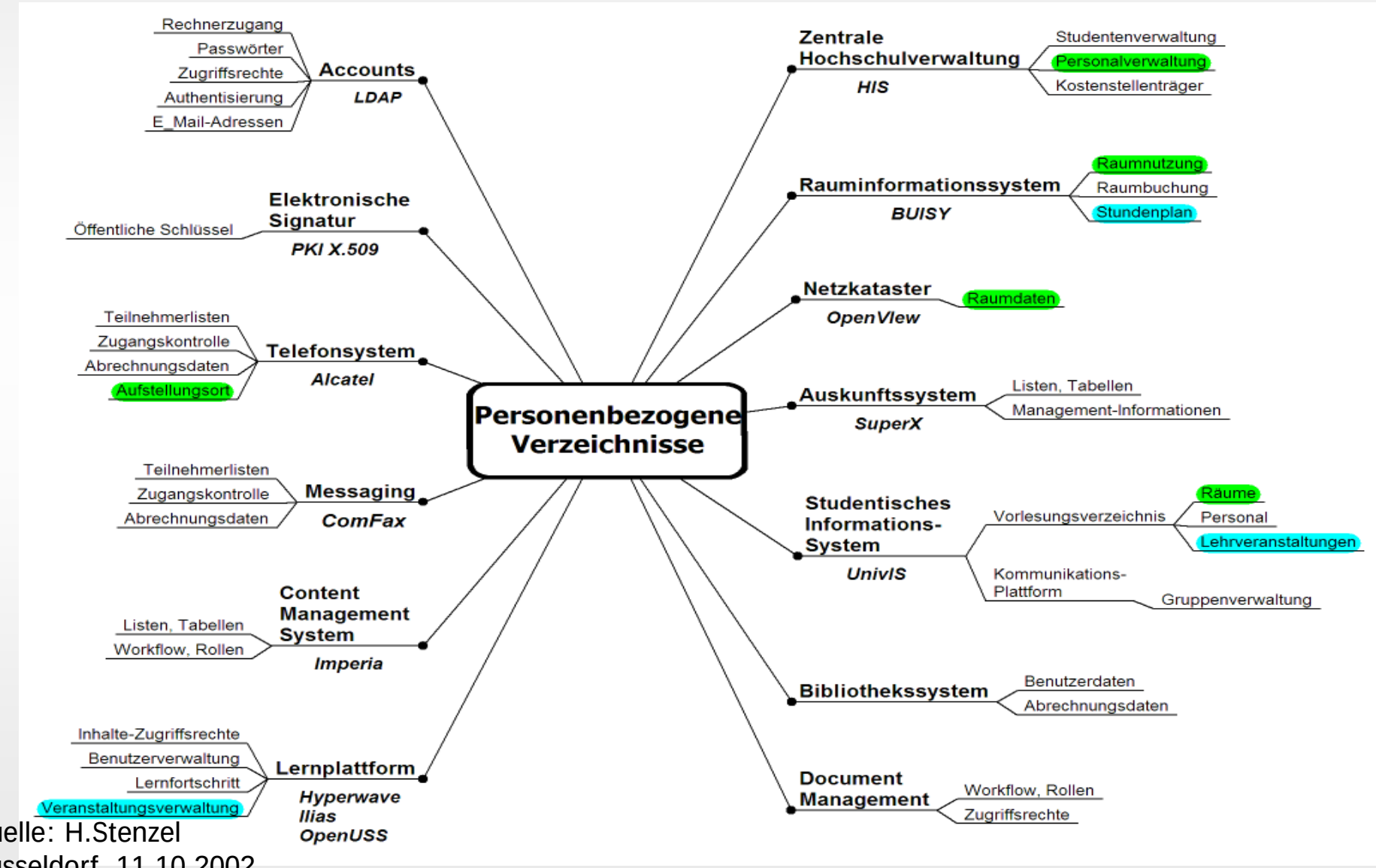
- Die Hochschulen stehen vor neuen Herausforderungen
  - Zunehmende Gestaltungsmöglichkeiten
  - Zunehmender Wettbewerb
  - Knappere Mittel
  - Wachsende Bedeutung digitaler Medien
  - Modularisierung
  - Internationalisierung
- Vorhandene IT-Strukturen sind nicht tragfähig für den Wandel Antworten:

  --> Serviceorientierung

  --> Konsolidierung

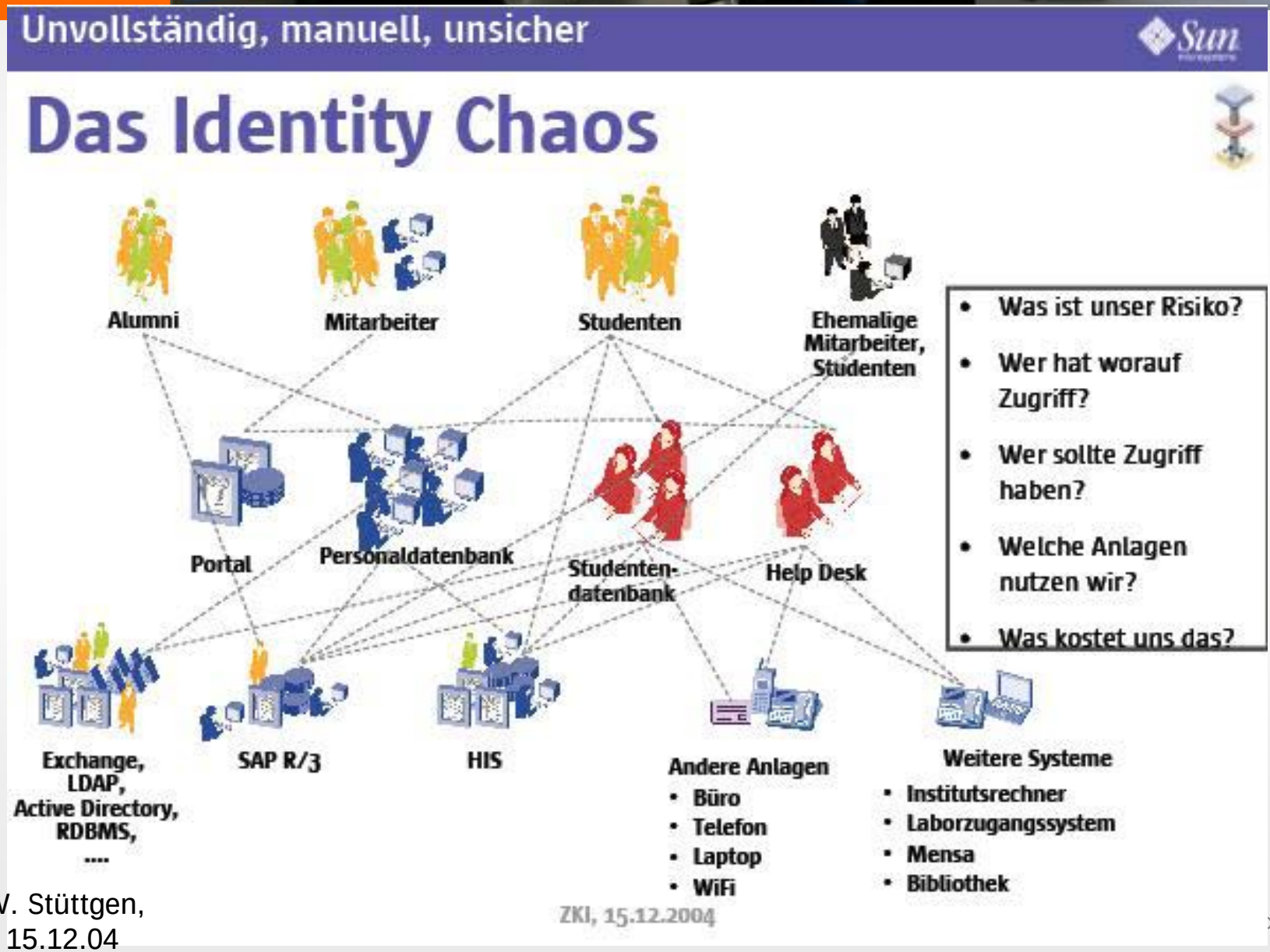
  --> Kooperation
- Identity-Management ist unbedingte Voraussetzung

Verzeichnisdienste in Hochschulen: Ist-Situation

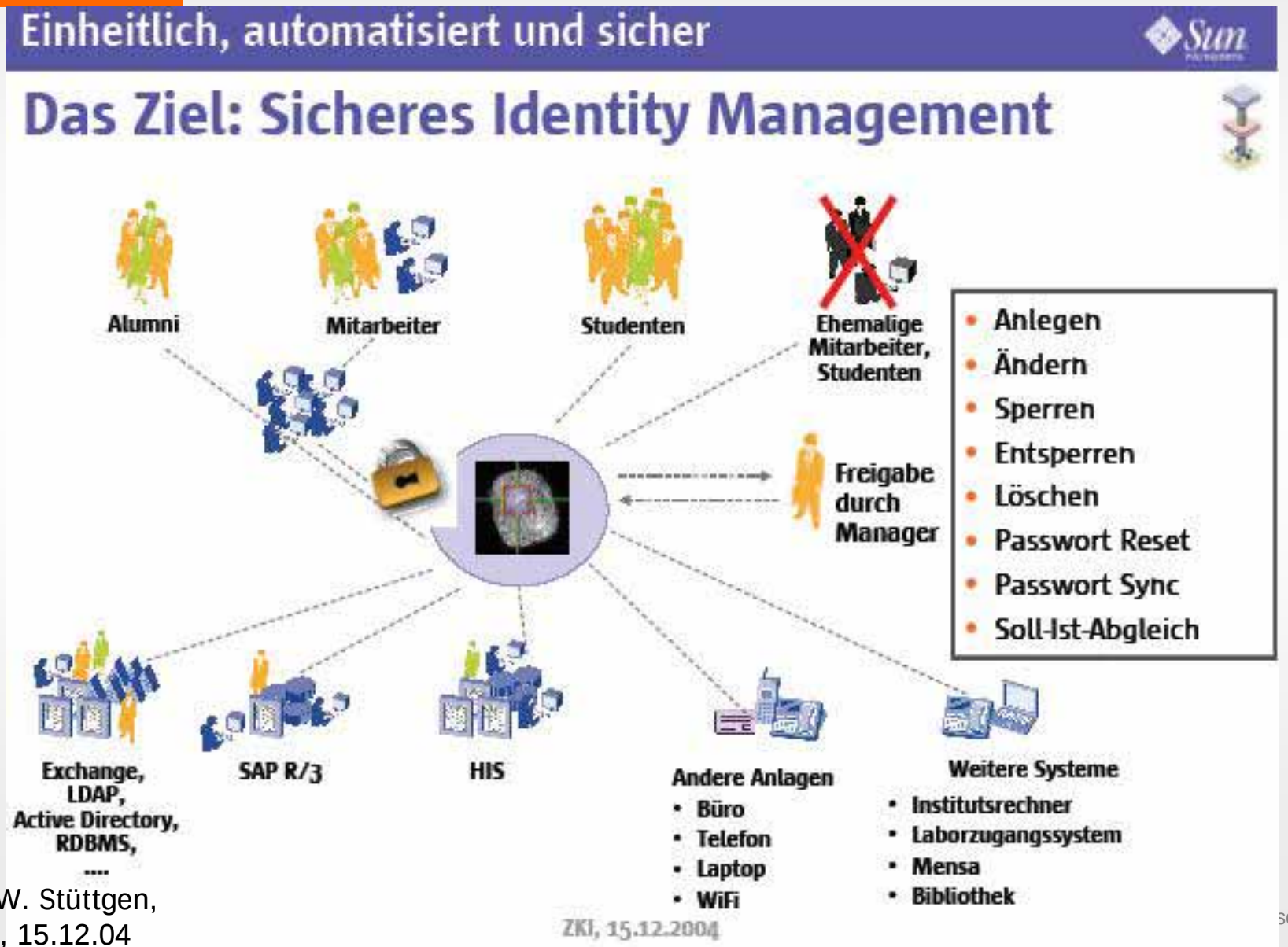


Quelle: H.Stenzel
Düsseldorf, 11.10.2002

Verzeichnisdienste in Hochschulen: Ist-Situation



Quelle: W. Stüttgen, Ilmenau, 15.12.04



Quelle: W. Stüttgen, Ilmenau, 15.12.04

Begriffe

- Benutzer-Verwaltung
  - login, Gruppenzugehörigkeit
  - Kombination von Authentisierung mit Rechtevergabe (= Autorisierung)
- Identitätsverwaltung
  - Personen statt Accounts, mit (wechselnden) Rollen und daraus abgeleiteten Rechten
  - ein Benutzer ←→ viele Funktionsbereiche (accounts)
  - (ein Account ←//→ viele Benutzer)
  - Zertifikate idR an Identitäten gebunden
- Directory = Benutzerverwaltung
  - Typischer Weise flach
- Verzeichnisdienst = Datenbank & Kommunikationsschnittstelle
  z.B. LDAP: Standardisiert, offen, hierarchisch gegliedert, verteilt
  proprietäre Verzeichnisse:
  - Microsoft Active Directory (sehr)
  - NDS (weniger)
- eduPerson:
  - Objektklasse Attributen für Personen in Hochschulinstitutionen
- Meta-Directory
  - Integration und Synchronisation der spezifischen Verzeichnisse
- Provisioning
  - Alle Mitglieder erhalten die für ihre Aufgaben notwendigen Ressourcen automatisiert - und nur die

KFR-Empfehlungen 2001-2005

Empfehlung der Kommission für Rechenanlagen der DFG 2001-2005, „Informationsverarbeitung an Hochschulen – Netze, Rechner und Organisation“, Aufgaben der Rechenzentren:

4.2.5 Verzeichnis-Dienste

„Die in Kapitel 2.1 geforderten „modernen, den Nutzer grundsätzlich nicht behindernden Techniken der Zugangskontrolle“, insbesondere in Verbindung mit Verschlüsselungstechniken, erfordern den Aufbau von Verzeichnissen mit Authentisierungs- und Autorisierungsinformation (IP-Adressen, Mail Adressen, Name-Server). Diese können zentral oder dezentral gepflegt werden; in beiden Fällen ist jedoch ein mindestens zentraler Zugriff zur Zugangskontrolle auf die zentralen Dienste erforderlich (z.B. LDAP). Die Koordination solcher Verzeichnisdienste unter gleichzeitiger Berücksichtigung der Funktionalität und des Datenschutzes wird zunehmend eine übergeordnete Aufgabe des Hochschulrechenzentrums sein.

ZKI

- „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung”
  - ca. 160 Mitglieder: Universitäten, Fachhochschulen, öffentlichen Forschungseinrichtungen, Firmen
  - 2 x jährliche Mitgliederversammlungen
  - Arbeitskreise:

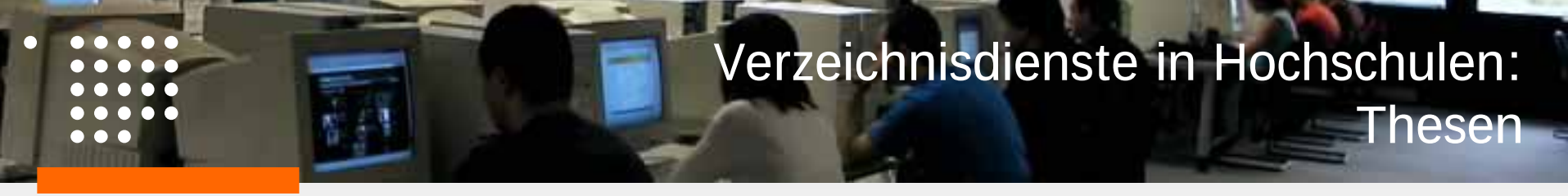
    Fachhochschul-Rechenzentren, Universitäts-Rechenzentren, Supercomputing, Netzdienste, Verteilte Systeme, Software-Lizenzen, Multimedia&Grafik, Kosten- und Leistungsrechnung, Verzeichnisdienste
  - Kommissionen zu besonderen Themen (z. B. G-WiN)
  - http://www.zki.de

ZKI Arbeitskreis Verzeichnisdienste

- Verzeichnisdienste: „Wesentliches technisches Mittel zur Erleichterung von Abläufen”
- Aktuelle Aufgaben:
  - Erfahrungsaustausch über die Einführung von Verzeichnisdiensten, Identity Management, Single Sign On, User Provisioning und verwandten Aufgaben
  - Förderung der Kooperation zwischen Verwaltungs-DV und Rechenzentren
  - Integration von PKI, sowie Domain-übergreifende Authentifizierung

ZKI Arbeitskreis Verzeichnisdienste: Aktivitäten

- 1/2-jährliche Treffen, Informationsaustausch und Diskussion:
  - Techniken
  - Projekte, Lösungen
  - Produkte
- Positions-Papier: „Operationelle Datenbanken der Hochschulverwaltung und das Identitäts- und Rollenmanagement”, August 2004
- http://gaia.zi.fh-koeln.de/zki-ak

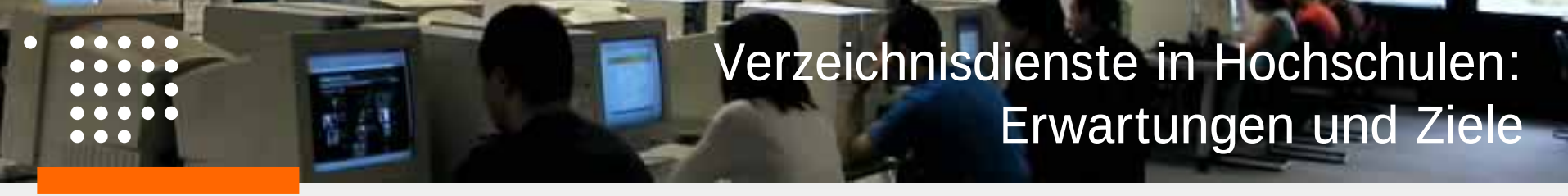


Verzeichnisdienste in Hochschulen: Thesen

- Ein integriertes Management der digitalen Identitäten wird benötigt
- Die Koordination mit der Verwaltungs-DV ist erforderlich
  Anforderung an Hochschulverwaltungsapplikationen:
  - Bereitstellung eindeutiger Objekt-Referenzen
  - Möglichkeit der Authentisierung über standardisierte Schnittstellen
  - Bereitstellung von Schnittstellen für die Rollen- und Rechteverwaltung
  - Möglichkeit des Im- und Exports von Daten auf Basis offener Standards

Entwicklung bei HIS

- Staging-Tabellen für SVA und SOS:
  offen: Import, API, Trigger
- Schnittstellen für Authentifizierung: LDAP, Secure IMAP, ...
- Eindeutige Benutzer-Identifikation: gleichbedeutend mit Authentifizierung gegen verschiedene Verzeichnisse? (Missverständnis ?)
- „HIS verwaltet alle Rollen selbst“,
  für jede Rolle ein eigener Account
- LSF als Frontend, Schnittstelle z.B. zu E-Learning-Systemen
- Zukünftige interessante Entwicklungen:
  - Eindeutige Personen-Kennung
  - integrierter LDAP, eduPerson



Verzeichnisdienste in Hochschulen: Erwartungen und Ziele

- Prozess-Orientierung (top down vs. bottom up)
  - Durchsetzung von Policies
  - Kontrollierte Erteilung und Entzug von Rechten
  - Nachvollziehbare Aktionen (Auditing)
- Innovationsmöglichkeit, Kostensenkung
  - Selbstbedienungsfunktionen
  - Vermeidung von Mehrfacharbeit
  - Zentralisiertes Helpdesk
  - Dienstebetreiber nicht gleichzeitig Benutzerverwalter
- Überörtliche Kollaboration
  - Schema
  - Kennung

Identity Management an Hochschulen

Umfrage an ausgewählten Hochschulen:

- Projektbezeichnung?
- Welche Inhalte werden im Meta-Directory gespeichert?
- Zentrale Authentifizierung (Single Sign On) ?
- Welche Fremdsysteme müssen/mussten angebunden werden?
- Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?
- Handelt es sich um eine Eigenentwicklung / fertiges Produkt?
- Status (System geplant / in Testphase / fertig gestellt)?
- Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?
- Welchen Plattformen werden genutzt?
- Datenschutz und Systemsicherheit?
- Vorteile / Nachteile der Lösung?
- Probleme bei der Planung / Entwicklung?
- Ausblick auf zukünftige Erweiterungen?

Stand an einigen deutschen Hochschulen

Hochschule	Projektstatus	Eigenentwicklung/Produkt
RWTH Aachen	Fertig gestellt, Ergänzungen geplant	IBM TIM, mit eigenen Java-Webanbindungen
Uni Bielefeld	Entwurf, Feinkonzept in Arbeit	vermutlich TIM
Ruhr-Uni Bochum	Fertig gestellt	Eigenentwicklung, Oracle
FH Braunschweig-Wolfenbüttel	Fertig gestellt	Eigenentwicklung mit SunOne Directory
Uni Braunschweig, RRZN Hannover, TU Clausthal, Uni Oldenburg	Feinkonzept erstellt, Pilotierungsphase	SUN
TU Chemnitz	Fertig gestellt	Eigenentwicklung
Uni Duisburg/Essen	Feinkonzept vorhanden, Umsetzung in Arbeit	TIM
FAU Erlangen-Nürnberg	Fertig gestellt, Erweiterungen geplant	GDS Server 2001 von BT Syntegra
Fern Uni Hagen	Fertig gestellt	Enterprise security station 3.2 (ESS), BMC Software GmbH , Control-SA
TU Ilmenau, Uni Jena, Uni Weimar	Erste Teile in Betrieb	Nsure Identity Manager (Novell)
Fachhochschule Köln	Entwurf, Feinkonzept geplant	openLDAP, iTIM geplant
Uni Mainz	Testphase	Microsoft Identity Integration Server
LRZ München	Testphase	Novel eDirectory + NIM2 + Eigenentwicklung
TU München	Entwurf	Voraussichtlich Novell-basiert
Uni Paderborn	Fertig gestellt	openLDAP, Umstellung auf ITIM geplant
Uni Rostock	teilweise fertig gestellt	Siemens „DirX“

Überörtliche Aktivitäten

- Thüringen: Codex
- Baden-Württemberg: PKI/LDAP
- Nordrhein-Westfalen: RV-NRW, 10er-Gruppe
- Niedersachsen: Service-orientierte Infrastruktur
- München: Info-Mgmt-Projekt

Einführungshindernisse

- Hochschulen sind keine Firmen
  - Komplexität der IT-Situation, Heterogenität, Menge
  - Hoher Regelungsgrad der Prozesse
  - Hohe Fluktuation, untypische Identitäten
- Ressourcen
- Vorschriften, Vorbehalte

Fazit

- Identity Management ist Basis-Technologie
- Zur Zeit besteht ein günstiges Zeitfenster
- Top-Down-Vorgehensweise ist erforderlich
- Alle müssen mitmachen → alle können profitieren

Alles klar?

Danke!