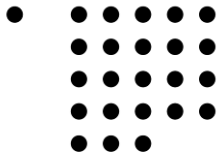

Fachhochschule Köln
University of Applied Sciences Cologne

Metadirectory-Lösungen an ausgesuchten Hochschulen

Stand: Juni 2009

Swen Hasberg, Patrick Odenwald, Thomas Krause

Datum	Bemerkung	Autor
31.07.2004	Erste Version	Swen Hasberg und Patrick Odenwald
30.06.2005	Aktualisierte Version (Juni 2005)	Swen Hasberg und Patrick Odenwald
25.06.2009	Aktualisierte Version (Juni 2009)	Thomas Krause

Inhalt

Einleitung

Dieses Dokument ist im Rahmen der Veranstaltung Verzeichnisdienste an der Fachhochschule Köln im Studiengang Wirtschaftsinformatik unter der Leitung von Prof. Dr. H. Stenzel begonnen worden und soll die Bemühungen ausgewählter Hochschulen im Bezug auf Metadirectory-Lösungen aufzeigen.

Anhand eines erstellten Kriterienkatalogs wurden die Daten aus uns vorliegenden Dokumenten und Präsentationen (ZKI-AK Verzeichnisdienste) zusammengetragen. Ein Teil der ermittelten Daten wurde von den verantwortlichen Personen der jeweiligen Hochschule verifiziert, aktualisiert und ergänzt. Dazu wurde den Personen ein Web-Interface zur Verfügung gestellt.

Im Sommersemester 2009 wurde das Dokument im Rahmen eines QQ2-Projekts aktualisiert.

Wir bedanken uns für die freundliche Unterstützung.

Die Autoren:

Swen Hasberg

Patrick Odenwald

Thomas Krause

RWTH Aachen

Stand: Mai 2006

Name des Projekts?

Identity Managment

Welche Inhalte werden im Meta-Directory gespeichert?

Personenstammdaten (Name, Anschrift, Emailadresse, Matrikelnummer)

Bislang erfolgt nur mit HIS SOS ein regelmäßiger Abgleich (je nach Änderungs-Frequenz in HIS SOS zwischen mehrmals pro Woche bis etwa einmal pro Monat). Abgleich mit HIS SVA erfolgt durch regelmäßige Übertragung von Name, Mitarbeiternummer und Nummer der Hochschuleinrichtung mit der ein Vertrag besteht. Diese Information wird nicht verwendet um Identitäten anzulegen, sondern um bestehende Identitäten oder neu anzulegende mit einer Identität in SVA zu verknüpfen. Außerdem lässt sich das Beschäftigungsende so erkennen.

Das Verzeichnis enthält auch die für die Provisionierung verschiedener Systeme erforderlichen Daten (UserId, Emailweiterleitungsadresse, Mailaliases, etc.).

Zentrale Authentifizierung (Single Sign On)?

Geplant (s.U.)

Welche Fremdsysteme müssen/mussten angebunden werden?

- Helpdesk System (Consol)
- Emailserver (Sun One)
- Campus Informationssystem (mit Veranstaltungsbuchung und HIS POS - Anbindung für Zugriff auf Prüfungsergebnisse durch die Studierenden)
- Pool (Windows/ADS)
- Webserver für Studierende
- HIS-SOS
- HIS-SVA
- TSM-Archivdienst
- MSDN AA
- Unix Cluster
- Windows/ADS für RZ-Mitarbeiter
- Grid Dienst
- Unified Messaging
- WLAN/VPN-Einwahl

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

- IBM Directory Integrator (IDI)
- ITIM Agenten
- eigene Scripte (vorrangig Java)

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

IBM Tivoli Identity Manager (ITIM)

Eigene Java Webanwendungen zur Realisierung spezieller Prozesse

Status (System geplant / in Testphase / fertiggestellt)?

Operativ seit Juli 2004 mit fast 135.000 Accounts die durch dieses System provisioniert werden!

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Solaris/SPARC (2 Systeme mit je 4 GByte Memory und je 2 Prozessoren).

Datenschutz und Systemsicherheit?

Die üblichen Sicherungsmaßnahmen wie Firewall, Hardening des Betriebssystems, Backup, besonders gesicherter Serverraum, Auditing, ...

Vorteile / Nachteile der Lösung?

Vorteile:

- Produkt hat seine Stärke bei der rollenbasierten Provisionierung, bei Bedarf Workflow gesteuert
- Weitere zu provisionierende Systeme lassen sich leicht anbinden

Nachteile:

- (normalerweise) teuer
- unbefriedigende webbasierte Bedienoberfläche für Kunden und Administratoren

Probleme bei der Planung / Entwicklung?

Es sind organisatorische Anpassungen in Rechenzentrum, Bibliothek und Verwaltung anzustreben die ihre Zeit benötigen.

Ausblick auf zukünftige Erweiterungen?

- Anbinding der Bibliothek (SISIS)
- Single Sign On (Shibboleth)
- Schnellere und teilweise bidirektionale Anbindung von HIS
- Unterstützung von Prozessen in der zentralen Hochschulverwaltung
- Umsetzung des bei IBM beauftragten Feinkonzeptes

Referenz

RWTH Aachen University
52056 Aachen
Rechen- und Kommunikationszentrum

Guido Bunsen
Email: bunsen@rz.rwth-aachen.de
Telefon: 0241/80-24882
Fax:

Freie Universität Berlin

Stand: Februar 2007

Name des Projekts?

FUDIS - Freie Universität (Berlin) Directory und Identity Service

Welche Inhalte werden im Meta-Directory gespeichert?

Keine Angaben

Zentrale Authentifizierung (Single Sign On)?

Geplant

Welche Fremdsysteme müssen/mussten angebunden werden?

Datenquellen:

- Studierendenverwaltung
- SAP-HR
- ERG
- Gastcard (Zentrum Weiterbildung)

Zielsysteme:

- Active Directory
- E-Mail
- Print Service
- Campus Managment
- …

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Datenquellen: Flat-File

Zielsysteme: primär LDAP, manchmal Flat-File oder andere Verfahren

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Keine Angaben

Status (System geplant / in Testphase / fertiggestellt)?

fertiggestellt

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Neue Systeme:

- Telefonanlage und VoIP-Pilotbetrieb
- Bibliotheken
- Teilnahme an DFN-AAI

Neue Anforderungen:

- SSO (Single Sign On)
- RBAC (Role Based Access Control)
- Dezentrale Administration von Rollen und Rechten
- Erweiterung des Portals um weitere Services
- Workflow-System

Referenz

Freie Universität Berlin
Zentraleinrichtung für Datenverarbeitung (ZEDAT)

Jörg Bechlars und Steffen Hofmann
Email: fudis@zedat.fu-berlin.de
Telefon:
Fax:

Technische Universität Berlin

Stand: Februar 2009

Name des Projekts?

TUBIS-Sphäre

Welche Inhalte werden im Meta-Directory gespeichert?

Keine Angaben

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

- CMS Typo3 (Webauftritt)
- Loga HCM (Personalverwaltung)
- SuperX (Reportsystem)
- LINF (Leistungsindikatoren in der Forschung)
- QIS/POS (Prüfungsanmeldung)
- asknet-Portal (Software Onlineshop)
- Hardware Onlineshop (TU Eigenentwicklung)
- Online Anträge (z.B. IP, Gäste, Exchangekonten)
- TUBIS Rollenverwaltung
- Schnittstelle zur informationellen Selbstbestimmung
- Selbstverwaltung (Passwörter, TANs etc.)
- Exchange
- Radius
- weitere in Vorbereitung

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Pull- und Push-Architektur

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung

Status (System geplant / in Testphase / fertiggestellt)?

fertiggestellt

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

- Neue Architektur
- Erweiterung der Pull- und Push-Dienste für Verzeichnisse
- Ereignissteuerung (zeitlich, Objektänderung, etc.)
- Neue Benutzungsschnittstelle (Webelemente können in Typo3 genutzt werden, Python-Interface für Scripte)
- Erstes RBAC-System mit xRE-Unterstützung

Referenz

Technische Universität Berlin

Christopher Ritter
Email: Christopher.Ritter@tu-berlin.de
Telefon: +49 30 314-78614
Fax:

Fachhochschule für Technik und Wirtschaft Berlin

Stand: Dezember 2008

Name des Projekts?

JUDIT

Welche Inhalte werden im Meta-Directory gespeichert?

Identität:

- Name
- Akademischer Grad/Titel
- Adresse
- Geburtstag/-ort
- Mailadresse
- Telefon

Beziehung/Funktion (Eine Identität kann mehrere Beziehungen zur FHTW haben):

- Funktion
- Studiengang
- Fachsemester
- Abschluss
- Hörerstatus
- Telefon/Fax
- Gebäude, Raum
- Matrikelnummer
- Personalnummer

Account (Mehrere Accounts pro Identität möglich)

- Login
- Passwort

Zentrale Authentifizierung (Single Sign On)?

Teilweise

Welche Fremdsysteme müssen/mussten angebunden werden?

- HIS-SOS/POS
- NIS
- NDS

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Treiber

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung auf Basis von Novell IDM

Status (System geplant / in Testphase / fertiggestellt)?

In Entwicklung

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

LDAP (mit Schemaerweiterungen)

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

In Entwicklung

Ausblick auf zukünftige Erweiterungen?

- weitere Systeme anbinden
- öffentliches Registrierungsinterface –auch für nicht-Studenten inkl. Approval (Personalstelle, Bibliothek)
- Integration offizieller(!) Organisationsstruktur

Referenz

Fachhochschule für Technik und Wirtschaft Berlin

Stefan Zech
Email:
Telefon:
Fax:

Universität Bielefeld

Stand: Februar 2007

Name des Projekts?

umfassendes Identity Management (TIM)

Welche Inhalte werden im Meta-Directory gespeichert?

Personendaten:

- Eindeutige, lebenslange Uni-Id
- Name (inkl. Titel und Zusätze)
- Geschlecht
- Geburtsdatum
- Adresse
- Email-Adresse
- …

Zentrale Authentifizierung (Single Sign On)?

später im Rahmen eines Portal-Projektes

Welche Fremdsysteme müssen/mussten angebunden werden?

Primärdaten:

- SISIS/PICA (Bibliothek)
- HIS-SVA (Peronaldezernat)
- HIS-SOS (Studentenverwaltung)
- BIS (Gästeverzeichnis)

Zu provisionierende Systeme:

- IT-Systeme in HRZ, UB und Verwaltung
- Verzeichnisse der dezentralen IT-Dienstleister (Fakultäten und Einrichtungen; später)

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Keine Angaben

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

vermutlich Tivoli-Produkte

Status (System geplant / in Testphase / fertiggestellt)?

- Grobkonzept im Rahmen einer Vorstudie mit externen Beratern (Fa. Comparex) entwickelt.
- Feinkonzept soll in Q3/04 von IBM entwickelt werden; dabei enge Abstimmung mit Du-E

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Dubletten zwischen den verschiedenen Quellsystemen, Lösung:

- Manuelle Bereinigung der Quellsysteme nach genauen Richtlinien (Normnamen)
- Plausibilitätsprüfung (z.B. Geburtsdatum)
- Abgleich von Vorname, Nachname, Geschlecht und Geburtsdaten
- Statistische Auswertungen um mögliche Dubletten zu finden
- Manuelle Bereinigung der gefundenen Probleme
- Mergen der Daten aus den verschiedenen Quellsystemen während der Initial-Befüllung

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

University Bielefeld

Frank Klapper
Email: frank.klapper@uni-bielefeld.de
Telefon:
Fax:

Ruhr Universität Bochum

Stand: Mai 2006

Name des Projekts?

RUBIKS

Welche Inhalte werden im Meta-Directory gespeichert?

- über eine einheitliche Schnittstelle sollen:
- Dienste von unterschiedlichen Anbietern abonniert werden können
- die entsprechenden Informationen abgerufen werden können
- Konfigurationen möglichst selbständig durchgeführt werden (ohne Aspekte der Datensicherheit zu vernachlässigen)

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

- HelpDesk- System (um möglichst schnell Fehler zu beseitigen)
- HIS SVA

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

- Perl-Skripte
- ldap

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung: das Projekt wurde im Sinne eines kundenorientierten Campus-übergreifenden Dienstleistungs-Management Systems konzipiert, indem ein Datenbank-gestütztes Informationssystem für alle anfallenden Vorgänge nutzbar ist

Status (System geplant / in Testphase / fertiggestellt)?

- Fertig gestellt
- nach der Fertigstellung wurden aus Sicherheitsgründen alle personenbezogenen Daten in eine eigene Datenbank transferiert (Name der Datenbank: iddb) [zentrale Autorisierungs-DB]
- dies führte zu der Möglichkeit, ohne großen Aufwand andere Einrichtungen einzubinden
- letztlich wurden Teile der iddb-Datenbank in den oiddb-Verzeichnisdienst gespiegelt, um der immer mehr zunehmenden ldap-Tauglichkeit vieler Anwendungen Rechnung zu tragen
- Später wurde ein Chipkartensystem zur Authentifizierung und Autorisierung mit digitaler Signatur entwickelt (Stand: 09.05.2006)

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- Oracle 8.1.7 Datenbank
- Oracle Web Application Server (Hinweis: die Idee war, dass die Schnittstellen zur Datenbank, ausschließlich über Web-Anwendungen implementiert werden sollten)

Welche Plattformen werden genutzt?

Unix-Systeme

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

University Bochum
Rechenzentrum

Ute Dederek-Breuer
Email: Ute.Dederek-Breuer@ruhr-uni-bochum.de
Telefon:
Fax:

Fachhochschule Bonn Rhein-Sieg

Stand: Juni 2005

Name des Projekts?

DIAS

Welche Inhalte werden im Meta-Directory gespeichert?

Die während des Workflows transportierten Daten

Zentrale Authentifizierung (Single Sign On)?

Nein

Welche Fremdsysteme müssen/mussten angebunden werden?

Mail,Telefon/Fax,Workflowsystem,Ausweisdruck,AD

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Über Workflows

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung

Status (System geplant / in Testphase / fertiggestellt)?

Teilweise umgesetzt

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Das Workflowsystem benutzt MS SQL-Server

Welche Plattformen werden genutzt?

Workflowsystem: MS Windows

Datenschutz und Systemsicherheit?

Daten werden nur für den begrenzten Zeitraum der Workflows und der Protokollierung gehalten.

Vorteile / Nachteile der Lösung?

Kurzfristige Umsetzung von kleinen Teilschritten.

Probleme bei der Planung / Entwicklung?

Viele Kleine.

Ausblick auf zukünftige Erweiterungen?

Schrittweise Anbindung an weitere Fremdsysteme. Umsetzen von bisher händischen, teilautomatischen Schnittstellen in teilautomatisch bzw. vollautomatisch Ablaufende.

Referenz

Fachhochschule Bonn-Rhein-Sieg
University of Applied Sciences
D-53757 Sankt Augustin

Dieter Weiß-Gräf
Email: dieter.weiss@fh-bonn-rhein-sieg.de
Telefon: +492241/865-8635
Fax: +492241/865-635

Fachhochschule Braunschweig/Wolfenbüttel

Stand: Januar 2003

Name des Projekts?

Serviceorientierte IT-Infrastruktur

Welche Inhalte werden im Meta-Directory gespeichert?

Personen, Studenten, Telefon, eMail-Service, Chipkarten-Informationen

Zentrale Authentifizierung (Single Sign On)?

Ja, für Webservices

Welche Fremdsysteme müssen/mussten angebunden werden?

HIS-SOS, HIS-POS, HIS-QIS, Portal, LMS, CMS, Apache, BSCW, Mail, Calendar, Pica

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Arbeiten auf Fremdsysteme (HIS) mit automatischem Abgleich zum Sun One Directory Service

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung mit SunOne Directory

Status (System geplant / in Testphase / fertiggestellt)?

fertiggestellt und seit Mitte 2003 im Regelbetrieb

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Sun One DirectoryService, File-Server, Samba-Server

Welche Plattformen werden genutzt?

Sun One, OpenLDAP

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Vorteile von SunOne:

- Integriertes Architekturkonzept.
- Im Kern des Konzeptes steht der Directory Service (Grundlage LDAP).
- Dafür gibt es verschiedene Lösungen (OpenLDAP oder herstellerabhängige Systeme).
- Directory Server ist gegenüber OpenLDAP skalierbar, d.h. nutzt die Leistung des Systems besser aus (Mehrprozessor).
- Directory Server bietet durch sog. multiple Master eine hohe Verfügbarkeit.
- Directory Server bietet die Möglichkeit der Konfiguration im laufenden Betrieb (keine Unterbrechung).
- Directory Server ist in allen Funktionalitäten sehr schnell (insert, search, delete) und hat auch mit mehreren Millionen Einträgen keine Performance-Probleme.
- Directory Server bietet die Möglichkeit der Delegation von Administrator-Funktionen.

Nachteile von SunOne:

- Directory Server ist kostenpflichtig.
- Directory Server ist kein OpenSource.
- Directory Server benötigt Sun Server Hardware
- Für Sun ONE Directory Server muss LDAP-Schemata von Drittanbietern geringfügig angepasst werden.

Probleme bei der Planung / Entwicklung?

- viele verschiedene Systeme
- viele Standorte
- verschiedene Endgeräte
- verschiedene Serversysteme
- Auswahl der Anwendungen fremdbestimmt
- Zugriff auf Daten von Anwendungen nicht oder nur schwer möglich
- Systeme müssen hochschulspezifisch sein bzw. bleiben (Profil der HS)

Ausblick auf zukünftige Erweiterungen?

- Identity Management und Portalservice für die Einbindung von Content-Management-Systemen und zum Dokumenten Management. Beides im weiteren Sinne, wobei Content alles umfassen wird.
- Integration intelligenter Suchmechanismen.
- Einbindung eines Systems zur Lehrevaluation

Referenz

Fachhochschule Braunschweig / Wolfenbüttel
Rechenzentrum

Email:
Telefon:
Fax:

Technische Universität Chemnitz

Stand: Februar 2009

Name des Projekts?

Produkt MoUSe - Management of User and Services

Welche Inhalte werden im Meta-Directory gespeichert?

in ca. 70 MySQL-Tabellen werden gespeichert:

- Personenstammdaten (Name; Anschrift; Geb.-datum; Zuordnung zu Einrichtung, Struktur und Persondentyp; Dauer der Nutzungsberechtigung)
- Daten zur Administration des Rechnerzugangs (NKZ, UID, k e i n e Paßwörter)
- Daten zur Verwaltung der Homeverzeichnisse (Quota, ...)
- Daten zum Management von E-Mailadressen, -aliases, Mailboxen und -domains
- Daten zur Kontenführung für kostenpflichtige Dienste
- Daten zur Steuerung Magnetkarten-Türzugang (Kartennumer, Mifare-ID, Zugangsbefugnisse, ...)
- Daten zur Verwaltung von Weiterbildungskursen (Teilnahme, Praktika, erreichte Punktzahlen, Zertifikate)
- Daten zur Zuordnung von Ressourcen aller Art zu Personen bzw. –gruppen (Softwarelizenzen, Handbücher, Magnetkarten, Speicherkapazitäten)
- Daten zum URZ-Haushalt (Titel, Kapitel, Aufräge, Rechnungen, ...)

Zentrale Authentifizierung (Single Sign On)?

nicht realisiert

z.Z. Testbetrieb

Welche Fremdsysteme müssen/mussten angebunden werden?

- AFS
- Heimdal (Kerberos)
- Windows NT
- Windows XP
- Linux (Verteilung der passwd-MAP ohne NIS)
- Mail-Server
- LDAP
- Türzugangssysteme Cronos und DACS (Eigenentwicklung)
- Kassensysteme des Studentenwerks
- LIBERO (Bibliothek) (wird noch in diesem Semester im Produktionsbetrieb eingesetzt werden)
- HELPDESK-System (Eigenentwicklung)
- URZ-Auftragsdatenbank (Eigenentwicklung)
- System zur Beschaffung von Standard-PC-Technik (Eigenentwicklung)
- Cisco UC Manager

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

ASCII-Schnittstellen über Files (Zugangssystem Cronos, Mailserver, Linux)

ASCII-Schnittstelle online (Kassensysteme)

Kommandoschnittstelle von Windows bzw. AFS (ASCII-Files)

alle Studentendaten werden vom Studierendensekretariat täglich als ASCII-File geliefert

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung

Status (System geplant / in Testphase / fertiggestellt)?

fertiggestellt

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- http (auch zum Printserver und zum Türzugangssystem DACS)
- MySQL Datenbank

Welche Plattformen werden genutzt?

Linux LAMP-System (Linux, Apache, MySQL, PHP)

Datenschutz und Systemsicherheit?

Kommunikation zwischen Web-Server und Web-Client über https

alle Web-Seiten über .htaccess geschützt

Zugriff zur MySQL-Datenbank nur vom MoUSe-Server (MySQL-Zugriffsrechte)

Vorteile / Nachteile der Lösung?

Vorteile:

- basiert auf kostenfreier Open-Source Software
- von jedem beliebigen Arbeitsplatz (plattformunabhängig), der über einen WebBrowser
- verfügt, sofort einsetzbar, ohne dass Software installiert werden muss
- einheitliche Nutzerkennungen über Systemgrenzen hinweg
- ein einziges Homeverzeichnis pro Nutzer, auf das von jedem System zugegriffen werden kann
- keine Wiedervergabe von Nutzerkennungen und UID
- keine Wiedervergabe von Mailadressen
- Bindung eines Kontos für kostenpflichtige Dienste an den Account
- offen für Erweiterungen
- einfach erweiterbar

Nachteile:

- Technologie (z.B. AFS als zentrales Filesystem) und Geschäftsabläufe der TU Chemnitz
- sind mit MoUSe relativ eng verknüpft und bestimmten den Leitungsumfang von MoUSe

Probleme bei der Planung / Entwicklung?

keine

Ausblick auf zukünftige Erweiterungen?

Verwaltung von Mitarbeiterdaten optimieren

Basis der TU Chemnitz für eine Gemeinsame Identifizierungsschnittstelle sächsischer Hochschulen

Datenbasis für VoIP-Projekt (Voice over IP)

Referenz

Technische Universität Chemnitz
D-09107 Chemnitz
Uni-Rechenzentrum TU Chemnitz

Dietmar Grunewald
Email: dietmar.grunewald@hrz.tu-chemnitz.de
Telefon: 0371/531-1724
Fax: 0371/531-1629

Technisch Universität Darmstadt

Stand: Juni 2005

Name des Projekts?

Meta-Directory

Welche Inhalte werden im Meta-Directory gespeichert?

Personen, Gruppen, Organisationen, Drucker, Rechner, Server-Zertifikate, Systemdaten. Jeweils mit einer Vielzahl von Attributen (Personendaten, Kontakt-Daten, Bezeichnungen, etc.). Nutzung für Abrechnungen/Accounting

Zentrale Authentifizierung (Single Sign On)?

Nein, aber „Single Passwort“. Für alle Dienste und Plattformen des HRZ ein Benutzername und Passwort.

Welche Fremdsysteme müssen/mussten angebunden werden?

Linux (ldap_pam) und AIX, Windows 2000/XP (Novell Client32), Mercury/32 Mailserver, Apache Webserver, Postfix MTA, FlexiTRUST (PKI), Learning Management Systeme (Clix, .LRN, WebCT), Radius.

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

LDIF Export/Import (Delimited Text), eigene Konnektoren über LDAP und JNDI, Weboberflächen für Benutzer (Self-Service für Benutzerkonten)

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Fertiges kommerzielles Produkt für Verzeichnisdienst (eDirectory). Eigenentwicklung bzw. PD-Software für:

- Anbindung an Fremdsysteme (Daten-Export)
- Web-Interface für Benutzer
- Datenimport von Studien- und Personalverwaltung.

Status (System geplant / in Testphase / fertiggestellt)?

Fertig gestellt, aber stetige Weiter-Entwicklung

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Native ODB von Novell. Protokolle: NDAP, LDAP, RADIUS

Welche Plattformen werden genutzt?

Novell NetWare für Verzeichnisdienst. Linux, AIX, Windows 2000/XP und NetWare für Datenabgleich und Benutzerinterfaces.

Datenschutz und Systemsicherheit?

SSL/TLS. 3 Industrie Standard-Server vor einem LoadBalancer.

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Komplexität, Strukturierung im Verzeichnis, Fragen zum Datenschutz (White Pages – Daten der Benutzer), Abgleich mit fremden Datenquellen (SAP/HR).

Ausblick auf zukünftige Erweiterungen?

- Chipkarte für Studierende: Schlüsselverzeichnis (PKI) für Benutzer (10/2005)
- „Single Password“ für HIS/QIS (11/2005)
- Abgleich mit SAP/HR der Personalverwaltung Workflow für Eintritt/Austritt von Bediensteten (2006)
- Erwerb einer kommerziellen Identity Management Software (2006)

Referenz

Technische Universität Darmstadt
D-64287 Darmstadt
Hochschulrechenzentrum (HRZ)

Dipl.-Ing. Ronny John
Email: Ronny.John@HRZ.TU-Darmstadt.de
Telefon: +496151/16-4573
Fax: +496151/16-3050

Technische Universität Dortmund

Stand: November 2008

Name des Projekts?

Keine Angaben

Welche Inhalte werden im Meta-Directory gespeichert?

Keine Angaben

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

HIS-SOS/POS

HIS-SVA

Universitäts Bibliothek

HRZ IDM in UniMail

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Keine Angaben

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Sun IDM als Basisprodukt

Status (System geplant / in Testphase / fertiggestellt)?

In Entwicklung:

- Entwicklungs-und Staging-Umgebung mit allen notwendigen Ressourcen (SOS, SVA, UniMail) aufgesetzt => erste Erfahrungen bzgl. der Datenqualität in den Quellsystemen können gesammelt werden
- Konzepte für Seeding und spätere Synchronisation der Datenbanken mit dem IDM werden entwickelt
- Geplantes IDM-System wird mit dem Datenschutzbeauftragten, dem Personalrat und den beteiligten Dezernaten diskutiert
- Grobkonzept für die Produktiv-Server

Projektende geplant: September 2009

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Vorteile:

- Flexibles, erweiterbares Framework
- Standardisierte Schnittstellen
- Weitgehend agentenlose => keine bis wenige Modifikationen an den vorhandenen Systemen
- Reporting, Auditing
- Resource Adapter für alle relevanten Systeme
- Skalierbarkeit

Nachteile:

- Open Source Version steht noch nicht zur Verfügung
- Hohe Einstiegshürde
- Proprietäre Prozessmodellierung
- OpenLDAP Resource Adapter muss noch implementiert werden
- WS Resource Adapter muss noch implementiert werden

Probleme bei der Planung / Entwicklung?

- Lernkurve steigt ziemlich steil an
    - Erste eigene Versuche dauert viel länger als geplant
    - Schon für kleinere Aufgaben ist ein breites Verständnis des IDM notwendig
    - Hohe Einstiegsanforderungen
- Teilnahme an den Kursen Deployment Fundamentals 1 & 2 ist dringend zu empfehlen
- Java, J2EE, SQL, XML, LDAP, AD, .. => Kein Einsatzgebiet für reine Java-Programmierer
- Kleinere Probleme mit SLES 10

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Technische Universität Dortmund

Jan Gellweiler
Email: jan.gellweiler@tu-dortmund.de
Telefon:
Fax:

Universität Duisburg-Essen

Stand: Februar 2007

Name des Projekts?

Identity Management

Welche Inhalte werden im Meta-Directory gespeichert?

- Nutzerdatenbank zur einheitlichen Authentifizierung
- Grobkonzept umfasst u.a.:
    - Standardisierbar, modular, Reporting
    - Zentraler Verzeichnisdienst
    - E-Mail Adresse
    - Authentifizierung und Kennwortsynchronisation
    - Autorisierung incl. Rollenkonzept
    - User Provisioning
    - Single Sign On
    - Webportal
    - Organisationsstruktur der Hochschule

Zentrale Authentifizierung (Single Sign On)?

Thema im Grobkonzept

Welche Fremdsysteme müssen/mussten angebunden werden?

- HIS-SOS
- HIS-SVA
- HIS-MBS
- HIS-LSF
- Telefonverzeichnis
- Benutzerverwaltung von Bibliothek, Rechenzentrum, Fachbereiche

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

- Alle Aktivitäten gehen vom IM aus
- Als Quellsysteme dienen HIS-SOS und HIS-SVA
- Es wird nicht in die Quellsysteme zurückgeschrieben
- Änderungen werden über Agenten auf den Zielsystemen geschrieben

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Produkt auf Basis von IBM/Tivoli

Status (System geplant / in Testphase / fertiggestellt)?

Feinkonzept durch IBM fertiggestellt

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

- Vorgespräche mit Personalräten haben stattgefunden in denen über den Umgang mit Mitarbeiterdaten diskutiert wurde
- Außerdem wird für die Zielsysteme dokumentiert wer welche Daten sehen kann

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

- Fusion Duisburg Essen: Prozesse müssen konsolidiert werden
- Schutz der Mitarbeiterdaten gewährleisten

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Universität Duisburg-Essen
Hochschulrechenzentrum

Herr Dr. Bruno Lix
Email: lix@hrz.uni-essen.de
Telefon:
Fax:

Universität Düsseldorf

Stand: Mai 2006

Name des Projekts?

Identity Managment an der Universität Düsseldorf

Welche Inhalte werden im Meta-Directory gespeichert?

Keine Angaben

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

Datenquellen:

- HIS-SVA
- HIS-SOS

Anzubindende Systeme:

- HIS-LSF
- E-Mail
- Selbstauskunft

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

- Der Transport von de Datenquelle zum Identity Vault erfolgt über Textdateien
- HIS-LSF ist über JDBC angebunden
- E-Mail wird über LDAP realisiert
- Die Selbstauskunft geschieht über Novell iManager

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Novell Identity Manager

Status (System geplant / in Testphase / fertiggestellt)?

Testsystem läuft; Produktivbetrieb geplant für September 2006

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Entwicklung weiterer Treiber in Kooperation mit RZ

Referenz

Heinrich Heine Universität Düsseldorf

Eric Humrich
Email:
Telefon:
Fax:

Universität Erfurt

Fachhochschule Erfurt

Technische Universität Ilmenau

Friedrich-Schiller-Universität Jena

Fachhochschule Jena

Fachhochschule Nordhausen

Bauhaus-Universität Weimar

Hochschule für Musik Franz Liszt Weimar

Stand: März 2008

Name des Projekts?

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

Welche Inhalte werden im Meta-Directory gespeichert?

Verwaltung von Identitäten und Rollen

stark begrenzte, für die Mehrzahl der Applikationen interessante Merkmale von Personen und ihren Rollen aus Studentenverwaltung, Mitarbeiterverwaltung, Bibliotheksbenutzerverwaltung und Benutzerverzeichnissen

Zentrale Authentifizierung (Single Sign On)?

Single Sign On für Portale und zentrale Dienste, wie Dial-In, VPN, E-Mail-Box

Welche Fremdsysteme müssen/mussten angebunden werden?

- HISSVA
- HISSOS
- PICA (Bibliotheksverwaltung)
- THUAPOS (Organisationssystem für andere Personen, z.B. Gäste)
- Authentifizierungssystem (LDAP, RADIUS)
- implizite Autorisierung

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

XML-basierende Schnittstelle

- zwischen HISSOS, HISSVA und Meta Directory per Staging-Tabellen, JDBC und DirXML
- zwischen PICA und Meta Directory per Delimited Text und DirXML
- zwischen THUAPOS, AA-system und Meta Directory per LDAP/eDirectory und DirXML

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung auf Basis des Produkts Nsure Identity Manager von Novell Inc.

Jede Hochschule pflegt ihr eigenes Meta Directory auf der Grundlage eines gemeinsamen Lösungsmusters

Status (System geplant / in Testphase / fertiggestellt)?

Fertiggestellt

Produktionsstart:

- Friedrich-Schiller-Universität Jena: 01.09.2007

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- MS Access JDBC/ODBC
- Informix JDBC, PostgreSQL JDBC
- LDAP
- eDirectory

Welche Plattformen werden genutzt?

Novell Netware, Sun Solaris, Suse Linux Enterprise Server

Datenschutz und Systemsicherheit?

- kein direkter Zugriff der Benutzer auf das Meta Directory
- in Abhängigkeit von den lokalen Gegebenheiten gesichertes Servernetz
- Verschlüsselung bei den Konnektoren

Vorteile / Nachteile der Lösung?

Vorteile:

- gute Konfigurierbarkeit durch den Einsatz eines Produktes
- flexibel bei Veränderungen und Erweiterungen

Nachteil:

- Lizenzkosten

Probleme bei der Planung / Entwicklung?

- hohe Komplexität des Problemraumes
- eintragsbezogenes Lizenzmodell der Verzeichnisanbieter

Ausblick auf zukünftige Erweiterungen?

- Autorisierungs- und Accounting-System
- Weitere Provisionierung bestehender Systeme
- Unterstützung der PKI

Referenz

Technische Universität Ilmenau

Jörg Deutschmann
Email: Joerg.Deutschmann@TU-Ilmenau.DE
Telefon:
Fax:

Universität Erlangen-Nürnberg

Stand: Februar 2009

Name des Projekts?

IDMone

Welche Inhalte werden im Meta-Directory gespeichert?

Daten zur Organisationsstruktur, Personen, Beschäftigungsverhältnissen, Rechten und Gruppen

Zentrale Authentifizierung (Single Sign On)?

Ja

Welche Fremdsysteme müssen/mussten angebunden werden?

- HIS SOS
- DIAPERS
- Studentische Prüfungsverwaltung ("Mein Campus")
- ADS
- NDS
- Radius (WLAN, VPN, …)
- RRZE (Abrechnung)

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Bereitstellung von Schnittstellen

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung mit Unterstützung durch Novell

Status (System geplant / in Testphase / fertiggestellt)?

Projekt beendet

- Übergang in Regelbetrieb
- Noch kein vollständiger Datenbestand
- Noch geringer Funktionsumfang

Bereits realisierte Funktionen:

- Provisionierung der studentischen Prüfungsverwaltung (‚Mein Campus‘)
- Provisionierung der bestehenden RRZE Benutzerverwaltung * Ablösung der Importe aus HIS SOS * Lieferung der Mitarbeiterdaten aus DIAPERS * Übergabe der Daten aus WAID
- User Self Service via WAID
- Admin Service via WAID
- Neuentwicklung des Web-Frontends (WAID) für den Self-Service
- Anbindung von Diapers (derzeit ohne Trigger)
- Lesende Anbindung von HIS SOS (derzeit ohne Trigger)
- Lesende Anbindung des Altsystems
- Zielsystemtreiber für ADS und NDS exemplarisch fertig

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

- Personelle Ausstattung
- Späte Vervollständigung des Teams

Ausblick auf zukünftige Erweiterungen?

- Aufbau der Gäste/Sonstigenverwaltung
- Anbindung von UnivIS
- Provisionierung von WLAN, VPN, SSO, …

Referenz

Universität Erlangen-Nürnberg

Dr. Peter Rygus
Email: peter.rygus@rrze.uni-erlangen.de
Telefon:
Fax:

Fern Universität Hagen

Stand: Juni 2005

Name des Projekts?

Identity Management bei der FernUniversität in Hagen mit Control-SA

Welche Inhalte werden im Meta-Directory gespeichert?

Benutzerdaten und Rechte

Zentrale Authentifizierung (Single Sign On)?

kein SSO (die Control-SA Infrastruktur sieht dies nicht vor)

Welche Fremdsysteme müssen/mussten angebunden werden?

- iPlanet Directory Server 5.1INFO:Mehrere Anwendungen fragen über das LDAP-Protokoll den Directory Server (iPlanet 5.1) ab. Da die ESS (noch) keine LDAP-Schnittstelle hat, werden Teile der Informationen aus der ESS in den bestehenden Directory Server übertragen. Zwar soll die ESS im Laufe des Jahres eine LDAP-Schnittstelle bekommen, aus Sicherheitsgründen wird die Architektur mit einem separaten Directory Server jedoch beibehalten. Dies hat auch den Vorteil, dass die Anwendungen, welche bisher den Directory Server abfragen, nichts von den Änderungen in der Infrastruktur mitbekommen werden.
- SOS DB (Zugriff nur lesend)
- PICA
- geplant Novell 6, Windows Active Directory, Solaris

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

In der ESS wird beispielsweise einem Benutzer das Recht zur Anmeldung auf einem „Solaris System“ zugestanden. Damit wird der User automatisch auf dem Zielsystem eingerichtet. Ändert der User nun sein Passwort, so kann Control-SA das Passwort auf allen angeschlossen Systemen auf den neuen Wert ändern (das ist kein SSO). Es existiert eine optionale Komponente „Control-SA/Passport“ zur benutzergeführten Passwordsynchronisation mittels Webschnittstelle.

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

fertiges Produkt:

- Enterprise security station 3.2 (kurz: ESS)
- Firma: BMC Software GmbH
- Produkt: Control-SA (ESS ist die zentrale Steuereinheit von Control-SA)

Status (System geplant / in Testphase / fertiggestellt)?

Fertiggestellt: Testsystem läuft seit Anfang November 2003

In Produktion: Auslesen der Daten aus der SOS DB und Anbindung iPlanet Directory Server

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- Sybase 12 und Oracle 8.1.7 (im Testsystem)
- Oracle 8.1.7 (im Produktivsystem)

Welche Plattformen werden genutzt?

Solaris 8 Plattform

Datenschutz und Systemsicherheit?

Firma BMC legt -nach eigenen Angaben- viel Wert auf Sicherheit (Internetquelle: www.bmc.com)

Vorteile / Nachteile der Lösung?

Vorteile:

- System läuft stabil
- sehr flexibel
- existierende Landeslizenz

Nachteile:

- Begriffe für Administratoren gewöhnungsbedürftig
- Fehleranalyse könnte besser unterstützt werden

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Neue Lasttests mit anderer Hardware

- Anbindung von selbst entwickelten Applikationen
- Einbindung Exchange-Server
- Test Control-SA/Web Console
- Einbindung von Mitarbeiterdaten

Referenz

Fern Universität Hagen
D-58084 Hagen
Universitätsrechenzentrum

Henning Mohren
Email: Henning.Mohren@FernUni-Hagen.de
Telefon: +492331/987-2856
Fax: +492331/987-19-2856

Hochschule für Angewandte Wissenschaft Hamburg

Hochschule für Bildende Künste Hamburg

Hochschule für Musik und Theater Hamburg

Technische Universität Hamburg-Harburg

Universität Hamburg

Stand: Oktober 2007

Name des Projekts?

eCampus

Welche Inhalte werden im Meta-Directory gespeichert?

Konsolidierte Personenidentitäten

Zentrale Authentifizierung (Single Sign On)?

Ja

Universität Hamburg: Auf Basis von Golem

Welche Fremdsysteme müssen/mussten angebunden werden?

- STiNE
- LBS
- LDAP-CD
- Bibliothekssystem
- …

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Über Konnektoren zwischen Quell- du Zielsystem

Auslösung durch Ereignisse

Konfiguration bestimmt welche Daten in welcher Form importiert oder exportiert werden

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigene Entwicklung auf Basis standardisierter Protokolle

Status (System geplant / in Testphase / fertiggestellt)?

Basisdienste vorhanden (eCampus I)

eCampus II ("Middleware" zwischen den Hochschulen / SSO) in Entwicklung

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

LDAP/LDIF, SAML (Liberty/Shibboleth), SOAP

Universität Hamburg: Golem zum Brokering von Autorisierungs-, Kontext- und Objektattributen zwischen WWW Anwendungen

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Vorteile:

- Automatische Erstellung, Verlängerung oder Löschung einer Zugangsberechtigung
- Automatische Bereitstellung von Email, Fileshare, Funknetz Zugang, etc.
- Schnelle Passwortänderungen und ggf. Neuvergabe
- Entlastung von organisatorischen Aufgaben
- Reduzierung von Komplexitäten im Verwaltungsumfeld durch hochschulübergreifende Strukturen.
- Automatische Erstellung einer Zugangsberechtigung, die die direkte Dienstaufnahme ermöglicht.
- Zeitnahe Änderungen an Personendaten mit unmittelbarer Provisionierung in die angeschlossenen Zielsysteme.
- Kostensenkung durch gemeinsame Ressourcennutzung, z.B. Abschluss gemeinsamer Software-Verträge für IDM-Komponenten.
- Erhöhte Sicherheit: Eine gemeinsame IDM-Lösung ermöglicht an zentraler Stelle eine Übersicht über Personen mit ihren Zugangs- und sonstigen Berechtigungen. Die IDM-Lösung schließt auch ein mögliches Sicherheitsrisiko durch nicht deaktivierte Accounts ausgeschiedener Personen aus.
- Verbesserte Integrierbarkeit weiterer Dienste wie z. B. Chipkarten- oder Gebäudezugangssysteme.
- Erhöhte Flexibilität bei der Umsetzung neuer Strukturen, z. B. bei der Anbindung neuer Einzelverzeichnisse oder neu zu schaffender Fakultätsinfrastrukturen
- uvm.

Probleme bei der Planung / Entwicklung?

- Generelles Problem der ersten Phase war die mangelnde Planbarkeit bedingt durch Abhängigkeiten von Datenlotsen / Campusnet
- Ein weiteres generelles Problem war und ist die dünne Ressourcendecke

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Universität Hamburg
Rechenzentrum

Dr. Stefan Gradmann
Email: stefan.gradmann@rrz.uni-hamburg.de
Telefon:
Fax:

Universität Heidelberg

Stand: Oktober 2005

Name des Projekts?

Heidelberger MetaDirectory Projekt

Welche Inhalte werden im Meta-Directory gespeichert?

Persondendaten:

- Nachname
- Vorname
- Institut
- Titel
- Anrede
- Anfangsdatum
- Endedatum
- Geschlecht
- Personalnummer
- Matrikelnummer
- Mail-Adresse

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

- HR-MA - Personalverwaltung (Oracle DB)
- HR-Stud - Studentensekretariat (Oracle DB)
- Email-Zentrale (Oracle DB)
- CA (Oracle DB)
- Email

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

- Über JDBC (Oracle DBs)
- Über LDAP (sonstige)

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Siemens DirX

Status (System geplant / in Testphase / fertiggestellt)?

Keine Angaben

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- LDAP-Server (MetaStore, User-Store)
- DirX EE
- DirXmetahub

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Abstimmung mit dem Datenschutz (ZENDAS)

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Universitätsrechenzentrum Heidelberg
Im Neuenheimer Feld 293
D-69120 Heidelberg

Prof. Michael Hebgen
Email: michael.hebgen@urz.uni-heidelberg.de
Telefon:
Fax:

Fachhochschule Köln

Stand: Juni 2004

Name des Projekts?

Zentraler Verzeichnisdienst

Welche Inhalte werden im Meta-Directory gespeichert?

Geplant: Personeninformationen aller Hochschulangehörigen

Zentrale Authentifizierung (Single Sign On)?

Nicht vorrangig geplant

Welche Fremdsysteme müssen/mussten angebunden werden?

HIS/SVA/SOS/POS, UnivIS, Telefonsystem, LDAP

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Keine Angaben

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

wenn möglich keine Eigenentwicklung

Status (System geplant / in Testphase / fertiggestellt)?

geplant

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Keine Angaben

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Verzögerungen, weil der Ressourcenbedarf die verfügbaren Mittel übersteigt

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Fachhochschule Köln
D-50678 Köln

Prof. Horst Stenzel
Email: stenzel@gm.fh-koeln.de
Telefon:
Fax:

Universität Mainz

Stand: März 2004

Name des Projekts?

Keine Angaben

Welche Inhalte werden im Meta-Directory gespeichert?

Projekt Anforderungen:

- Zentrales Verzeichnis
- Alle Daten sollen nur an einer Stelle gespeichert und verwaltet werden
- Passwort nur an einer Stelle gespeichert
- Delegation von einzelnen Aufgaben an FB oder Institute

Benutzerverwaltung umfasst:

- 4 Accounttypen (Mitarbeiter, Studierende, Nur Login, Nur Login und Druckkonto)
- Workflows

Zentrale Authentifizierung (Single Sign On)?

Ja

Welche Fremdsysteme müssen/mussten angebunden werden?

- Microsoft Active Directory
- Export zu SunOne Directory auf Mailserver (fertig)
- Export zu Applix Helpdesk (fertig)
- Synchronisierung mit UniVIS (?)
- Synchronisierung mit Telefonanlage (?)
- Synchronisierung mit FB Datenbanken (geplant)
- Unix – YP Tabellen via AD-Export
- Solaris – greift auf AD (aLDAP/Krb5) zu
- Import der Studentendaten (erfolgt über Textdatei)
- Import der Personaldaten

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Connectors

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

- Microsoft Identity Integration Server 2003 (MIIS)
- Microsoft Active Directory

Status (System geplant / in Testphase / fertiggestellt)?

- Testphase (Stand März 2004)
- MIIS Ende 2003 gekauft

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- LDAP (?)
- Kerberos (?)

Welche Plattformen werden genutzt?

Windows Server

Datenschutz und Systemsicherheit?

Kerberos (?)

Vorteile / Nachteile der Lösung?

Vorteil: Integration in bestehende IT-Landschaft der Uni-Mainz

Probleme bei der Planung / Entwicklung?

- Unixintegration – Probleme bei Windows 2003 Umstellung (UDP/TCP)
- Für NFSv4 auch Tickets unter Unix notwendig

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Universität Mainz

Email:
Telefon:
Fax:

Technische Universität München

Stand: November 2008

Name des Projekts?

IntegraTUM/TUMonline

Welche Inhalte werden im Meta-Directory gespeichert?

Alle Administrativen Daten auf Forschung und Lehre; insbesondere:

- Organisationsstruktur
- Personen
- Funktionen (Rechte)

Zentrale Authentifizierung (Single Sign On)?

Ja, mit Shibboleth

Welche Fremdsysteme müssen/mussten angebunden werden?

Datenquellen:

- HIS-SOS (Studentendverwaltung)
- SAP HR (Personalverwaltung)
- UnivIS (Gast Dozenten)
- Gästeverwaltungssystem (noch nicht implementiert)
- SISIS Elektra/SunRise (Bibliothek)

Angeschlossene Systeme:

- myTUM-Web-Portal (Novell eDirectory)
- Zentrale E-Mail-Server (BT/Syntegra Aphelion)
- Zentraler Storage (MS Active Directory)
- Authentifizierungsserver (MS AD, OpenLDAP)
- E-Learning System (imc CLIX)
- Bibliothekssystem (SISIS)
- Alumni-Datenbank (zu konsilidieren)

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Keine direkten DB Zugriffe!

Synchronisation erfolgt über LDAP, CSV, XML-RPC oder andere Schnittstellen

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Basierend auf fertigen Produkten, z.B. Anpassung von CAMPUSonline (TU Graz) an deutsche Anforderungen

Status (System geplant / in Testphase / fertiggestellt)?

In Betrieb, wird aber noch weiterentwickelt.

Bisher realisiert:

- Komplette Neuentwicklung der IT-Unterstützung für elektronische Bewerbung und Zulassung (inkl. Unterstützung für EFV (Fasttrack))
- Technische Infrastruktur (Produktiv-, Qualitätssicherungs-, Entwicklungs- und Backup-System)
- HIS SOS Schnittstelle in Betrieb
- SAP HR Schnittstelle in Betrieb
- Service-Desk in Betrieb (Basis: IT-Servicedesk IntegraTUM)
- Raumdatenübernahme läuft
- Einführung TUMonline Beauftragte läuft

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Novell eDirectory

Novell Nsure Identity Manager 2

Welche Plattformen werden genutzt?

Novell SuSE Linux Enterprise Server 9 + Open Enterprise Server

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Dubletten vermeiden

- Namen können sich ändern
- Tippfehler sind menschlich

Datenakquisition und Provisioning

- Proprietäre Schnittstellen z.T. fehlerhaft
- Read-only Zugriff / Export nicht ausreichend
- Konnektoren zu hochschulspezifischer Software
- Eigener Implementierungsaufwand hoch

Ausblick auf zukünftige Erweiterungen?

Ziel: TUMonline einziges Quellsystem u.a. für LV-, PV und Personendaten

Referenz

Technische Universität München

Hans Pongratz
Email: pongratz@tum.de
Telefon:
Fax:

Ludwig-Maximilians-Universität München

Fachhochschule München

Universität Regensburg

Stand: Januar 2003

Name des Projekts?

MUDS

Welche Inhalte werden im Meta-Directory gespeichert?

Personen, Gruppen, Rollen, Organisationen, Orte, Sachen, Telefon

Zentrale Authentifizierung (Single Sign On)?

Ja, über Campus Webportal

Welche Fremdsysteme müssen/mussten angebunden werden?

Keine Angaben

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

DirXML, LDIF Export/Import

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Eigenentwicklung mit Einbeziehung eines IT-Providers für Mail und Directory Backbone

Status (System geplant / in Testphase / fertiggestellt)?

Entwurf

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

LDAP, NAM, Prinzip der verteilten Systeme (Unterschiedlichste Systeme die Daten austauschen)

Welche Plattformen werden genutzt?

Keine Angaben

Datenschutz und Systemsicherheit?

PGP, SSL, Secret Store, Verschlüsselungsverfahren

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Datenschutz, Sicherheit, Akzeptanz

Ausblick auf zukünftige Erweiterungen?

Keine Angaben

Referenz

Ludwig-Maximilians-Universität München

Email:
Telefon:
Fax:

Universität Oldenburg

Stand: Mai 2006

Name des Projekts?

Identity-Managment

Welche Inhalte werden im Meta-Directory gespeichert?

Studierende

- Matrikelnummer
- Vorname
- Nachname
- Geburtstdatum
- Geschlecht
- Adresse
- Telefon
- Fax
- Handy
- Status
- Datum der Exmatrikulation
- Mail-Adressen

Zentrale Authentifizierung (Single Sign On)?

Keine Angaben

Welche Fremdsysteme müssen/mussten angebunden werden?

- SAP
- HIS

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

SAP über Novell SAP Konnektor

- Lesend mit IDoc‘s
- Schreibend mit JCO/BAPI

HIS über Novell JDBC Konnektor

- Lesen über Views (Studierenden- und Studiendaten)
- Schreiben direkt in die HIS Tabellen (nur Adressdaten)

Daten werden über Matching abgeglichen:

- Vorname
- Nachname
- Geburtsdatum
- Matrikelnummer
- Personalnummer

Über Schemaerweiterungen können zusätzliche Daten im Directory gespeichert werden

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Keine Angaben

Status (System geplant / in Testphase / fertiggestellt)?

In Entwicklung; Produktivbetrieb erwartet für August/September

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- eDirectory 8.7
- Identity Manager 2/3

Welche Plattformen werden genutzt?

- RedHat EL AS3

Datenschutz und Systemsicherheit?

Keine Angaben

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

Keine Angaben

Ausblick auf zukünftige Erweiterungen?

Migration geplant auf:

- Identity Manager 3
- eDirectory 8.8
- RedHat EL AS4

Aufsetzen von Novell Audit:

- Revisionsicheres Logging aller Vorfälle
- Auswertung durch DS Beauftragte
- Auswertung durch Revision

Anbinden weiterer Systeme:

- HICOM Telefonanlage
- Lehrveranstaltungsplaner (LVP)
- CAFM

Referenz

Carl von Ossietzky Universität Oldenburg
Ammerländer Heerstr. 114 – 118
26129 Oldenburg

Heiko Burchard
Email: h.burchard@uni-oldenburg.de
Telefon: +49 (0)441 798 4677
Fax: +49 (0)441 798 194677

Fachhochschule Osnabrück

Stand: Oktober 2007

Name des Projekts?

Identity Management an der FH Osnabrück

Welche Inhalte werden im Meta-Directory gespeichert?

Personenbezogene Daten zu Studenten und Mitarbeitern

Zentrale Authentifizierung (Single Sign On)?

Gibt es nicht überall, aber vielfach wird die Authentifizierung über LDAP genutzt

Welche Fremdsysteme müssen/mussten angebunden werden?

- HIS
- SAP
- webbasierte Dienste
- ein anderes eDirectory

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Aus dem HIS System werden csv Dateien an den Systemadministrator geschickt und diese werden dann ins eDirectory eingespielt. Aus dem SAP werden Emails für den Systemadminstratorgeneriert, sobald ein neuer Mitarbeiter eingetragen wird, oder es eine Änderung bei einem bestehenden Mitarbeiter gibt. Eine Synchronisation aus der NDS in die anderen Systeme gibt es noch nicht, ist aber angedacht. (z.B. die durch Selfservice gepflegte Anschrift für Studies) Für Lehrbeauftragte wird eine webbasierende Lösung entwickelt, um diese im eDirectory ein zu pflegen.

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Weitestgehend Eigenentwicklungen in Verbindung mit fertigen Tools

Status (System geplant / in Testphase / fertiggestellt)?

In Entwicklung; zuvor war nur ein zentraler Verzeichnisdienst vorhanden, der nun zu einem Identity Managment System ausgebaut werden soll

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

- EDirectory
- LDAP
- DirX

Welche Plattformen werden genutzt?

- Netware
- Linux

Datenschutz und Systemsicherheit?

Datenschutz über Zugriffsrechte, ansonsten nicht hinreichend gelöst

Vorteile / Nachteile der Lösung?

Probleme bei der Planung / Entwicklung?

Personelle Ressourcen

Ausblick auf zukünftige Erweiterungen?

DirXmL Einsatz zur Synchronisation bestimmter Daten mit einem anderen eDirectory; DirXmL als Synchronisation mit SAP und HIS, hier sind insbesondere Erfahrungen anderer Hochschulen interessant.

Referenz

Fachhochschule Osnabrück
D-49076 Osnabrück
EDV Verwaltung

Marion Krabbemeyer
Email: M.Krabbemeyer@fh-osnabrueck.de
Telefon: +49541/969-3048
Fax: +49541/969-13026

Universität Paderborn

Stand: Juni 2004

Name des Projekts?

Einführung eines Metaverzeichnisdienstes

Welche Inhalte werden im Meta-Directory gespeichert?

Zurzeit werden alle Identitäten in einem LDAP-Verzeichnis abgelegt, wobei initial nur ein minimaler (interner) Datensatz vorhanden ist, der vom Benutzer selbst aktiviert und ergänzt werden muss. Gespeichert werden verschiedene Daten, für verschiedene Benutzergruppen (Studierende, Mitarbeiter, Gäste), die sich grob wie folgt klassifizieren lassen:

- Benutzerdaten: Basisdaten (ID, Nachname, Vorname; werden mit den Verwaltungsdaten abgeglichen), Adressbuchdaten, …
- Accountdaten: Benutzerkennung, Passwort, Betriebssystemdaten (UID, GID, …)
- Verwaltungsdaten: Ablaufdatum, Sperrung,
- Daten einzelner LDAP-nutzender Anwendungen: E-Mail, WLAN-Zugang, Zur Speicherung der Daten werden soweit möglich LDAP-Standard-Schemata (person, inetOrgPerson, posixAccount, …) benutzt und diese ansonsten um wenige Paderborn-spezifische Schemata erweitert.

Zentrale Authentifizierung (Single Sign On)?

Ein einheitliches Passwort für angeschlossene Systeme (Crypt, MD5, Kerberos) ist realisiert. Später soll ein Identity-Server/-Manager zur Realisierung eines SSOs mit einmaliger Anmeldung für Web-Services und Portal-Anwendungen eingesetzt werden.

Welche Fremdsysteme müssen/mussten angebunden werden?

Datenquellen: SOS, HISSVA (weitere Daten werden über ein webbasiertes Selbstadministrationsskript erhoben)

Angebundene Zielsysteme: E-Mail (qmail), Benutzerauthentifizierung bei verschiedenen Betriebssystemen (Linux, Windows, Solaris, MacOS), WWW-Server, CMS, elektronisches Vorlesungsverzeichnis (HISLSF), Bibliothekssystem (Aleph), Portal-Server (geplant),

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Zurzeit erfolgt die Anbindung der Zielsysteme an das LDAP-Verzeichnis

- über das LDAP-Protokoll
- eine Authentifizierung auch über Kerberos
- Datenabgleiche mit Datenquellen und Zielsystemen über eigene Perl-Skripte

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Zurzeit wird openLDAP eingesetzt und zusätzlich werden eigene Perl-Skripte entwickelt. Der Einsatz einer kommerziellen Lösung für einen Metaverzeichnisdienst wird evaluiert.

Status (System geplant / in Testphase / fertiggestellt)?

Der openLDAP-Server als Verzeichnisdienst befindet sich im Produktiveinsatz. Für einen Metaverzeichnisdienst wurde ein Grobkonzept in Kooperation mit der Universität Bielefeld und mit externen Beratern (Fa. Comparex) entwickelt. Darüber hinaus findet eine Koordinierung/Erfahrungsaustausch mit anderen NRW-Hochschulen statt (Feinkonzept der Uni Duisburg-Essen durch Firma IBM).

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

Zurzeit wird das LDAP-Protokoll und ein openLDAP-Server genutzt.

Für die geplante Realisierung eines Metaverzeichnisdienstes kommen Produkte der Fa. SUN und IBM in betracht.

Welche Plattformen werden genutzt?

Der openLDAP-Server wird aktuell unter Linux betrieben. Es sind mehrere redundante Server über eine Lastverteilung erreichbar.

Datenschutz und Systemsicherheit?

Momentan erfolgt eine persönliche Zustimmung der Betroffenen zur Speicherung im Verzeichnisdienst. An einer Anpassung der rechtlichen Voraussetzungen (Einschreibungsverordnung, Dienstvereinbarung) wird gearbeitet. Der Verzeichnisdienst/LDAP-Server ist nur innerhalb der Hochschule zugreifbar und befindet sich in einem sicheren Subnetz, Anwendungen greifen auf (Teil-)Replika zu. Ein externer Zugriff erfolgt nur nach Authentifizierung über VPN.

Vorteile / Nachteile der Lösung?

Der aktuelle openLDAP-Server stellt eine kostengünstige Lösung dar, die zudem überschaubar und angepasst ist. Die Erweiterung, insbesondere der Skripte zum Datenabgleich und zur (Selbst-)Administration erfordern aber jeweils einen hohen Aufwand, sodass ab einer gewissen Komplexität (viele neue Systeme und dezentrale Administration) der Umstieg auf ein kommerzielles Metaverzeichnis und eine Provisioning-Komponente sinnvoll erscheint.

Probleme bei der Planung / Entwicklung?

Die eigentlichen Probleme bei der Verwaltung/Administration von Personenidentitäten sind Prozessprobleme, die in der ersten Projektplanung (Uni-Mobilis: Notebook-Universität) noch nicht genügend berücksichtigt wurden. So stellten die erstmalige Daten- und Prozesserhebung einen hohen Aufwand dar. Zudem mussten verschiedene Stellen von der Notwendigkeit einer konstruktiven Zusammenarbeit überzeugt und ein gemeinsames Vorgehen koordiniert werden. Die Klärung der rechtlichen Rahmenbedingungen (Änderung von Ordnungen, Beteiligung der Personalräte, Erstellung von Dienstvereinbarungen, datenschutzrechliche Dokumentation) erfordert ebenfalls einen hohen – zu Beginn des Projekts Uni-Mobilis nicht eingeplanten – Aufwand.

Ausblick auf zukünftige Erweiterungen?

In Paderborn steht momentan der Aufbau eines mit Verwaltungsdaten abgeglichenen Metaverzeichnisses im Vordergrund und weniger eine zentrale Provisioning-Komponente. Es ist aber abzusehen, dass die Komplexität der Datenflüsse, Rollen und Zugriffsrechte mit zunehmender Zahl der angebundenen Systeme nicht mittels eigener Skripte bewältigt werden kann. Die Uni Paderborn plant daher den Einsatz einer kommerziellen Lösung.

Referenz

Universität Paderborn
Paderborn
Zentrum IT-Dienste

Dr. Gudrun Oevel
Email: gudrun.oevel@uni-paderborn.de
Telefon:
Fax:

Universität Rostock

Stand: März 2008

Name des Projekts?

MetaDirectory

Welche Inhalte werden im Meta-Directory gespeichert?

Personendaten

Zentrale Authentifizierung (Single Sign On)?

zur Zeit nicht via MetaDirectory geplant

Welche Fremdsysteme müssen/mussten angebunden werden?

HIS-SVA, HIS-SOS, diverse ODBC-Quellen bzw. SQL-Server, ADS, LDAP-Server,

weitere sind geplant

Wie erfolgt Anbindung / Synchronisation mit Fremdsystemen?

Via Metadir-Connectoren/-Agenten (teilweise native, teilweise werden durch die Agenten POST bzw. PRE Skripte ausgeführt)

Handelt es sich um eine Eigenentwicklung / fertiges Produkt?

Siemens „DirX“

Status (System geplant / in Testphase / fertiggestellt)?

Seit Juli 2006 vollständig produktiv gemäß Konzept 1.1

Seit 2008 läuft zweite Phase

Welche Protokolle / Datenbanken werden für das Meta-Directory genutzt?

LDAP, ODBC, SMTP, SFTP, informix, mssql-srv

Welche Plattformen werden genutzt?

Windows 2003 Cluster (64 Bit)

Datenschutz und Systemsicherheit?

- System befindet sich hinter Firewall (Zugriff nur für best. IP und Portadressen erlaubt)
- Datenübertragung verschlüsselt
- ständige Abstimmung mit Datenschutzbeauftragtem

Vorteile / Nachteile der Lösung?

Keine Angaben

Probleme bei der Planung / Entwicklung?

- zeitlicher Verlauf bis zur Inbetriebnahme war schwer einschätzbar, da das RZ von sehr vielen Zuarbeiten (z.B. Verwaltung, Datenschützer, etc.) abhängig war, es gab erhebliche Verzögerungen (gegenüber der ursprünglichen Planung) in der Umsetzung seitens der Projekt-durchführenden Firma

- Eindeutige Zuordnung zwischen HR-Datensätzen und Personen
- Automatische Attribut Änderungen und deren Folgen (z.B. Zertifikate)
- zunehmende Anzahl von funktionellen Accounts
- u.a.

Ausblick auf zukünftige Erweiterungen?

Anbindung weiterer Fachbereiche, Telefonie, Zutrittssysteme, Bibliothek

Referenz

Universität Rostock
D-18051 Rostock
Rechenzentrum

Jörg Zerbe
Email: joerg.zerbe@uni-rostock.de
Telefon: 0381/498-5326
Fax: 0381/498-5302