7.Tagung der
Nutzergruppe Hochschulverwaltung

HIS und Verzeichnisdienst

Ludwig Leute

HIS Hannover

www.his.de

Abt. Informationstechnologie in der Hochschulverwaltung

Gliederung

- Fragestellung
- Auflösung der Verwaltungsgrenzen
- Schnittstelle HIS-GX Stagingtabellen
- HIS-GX LDAP

Problem und Ausgangslage

- Ablage und Pflege von Personendaten innerhalb eines Unternehmens in verschiedensten Datenbanken
- durchschnittlich 190 separate Verzeichnisse, Tendenz zunehmend
- Zugänge und Veränderungen häufig, Überschneidung der Datenbestände
- Fehlender Abgleich führt zu Inkonsistenz

Auslöser: IT Benutzeradministration

systemorientierte Verzeichnisse:

z.B.
ADS (Microsoft Active Directory Services
NDS Novell Directory Services
NIS Network Information System (UNIX)

weltweit Akzeptanz:

LDAP = Light Directory Access Protokoll

Auflösung von Verwaltungsgrenzen

- Forderung: abgestimmte Verzeichnisse
- Verlässliche Personendaten: durch Regeln und Kontrollen im Rahmen von Verwaltungsprozessen
- Personendatenbanken der HS-Verwaltung > Reservoir für Verzeichnisdienste außerhalb der HS-Verwaltung
- Das Softwaresystem HIS-GX eröffnet die Nutzung von Personendaten der Verwaltungsdatenbanken

No.	Ao. 1913 Monat	Tag	Vor- und Zuname	Alter	Geburtsort	Stand und Wohnort des Vaters, der Mutter oder des Vormundes	Religion	Studium	Die zuletzt besuchte Universität	Taxe Mk.	Pf.
649	Nov	15	Hans Louis gen. Gebhardt [illegible]	21	Zoschwitz	Pfarrer Fr. dsgl.	ev.	jur. ~~[illegible]~~	Halle	12	
650			Kaspar Lindemann	26	Dortmund	Amtsgerichtsrat Breslau	kathol.	jur. et cam.	Breslau	12	
651			Nicolaus Spiegel	24	Kitzingen	Kaufmann dsgl.	kathol.	med.	Würzburg	12	
652			Paul Gies	21	Hamm	Pfarrer a. D. Heidelberg	evang.	philos.		20	
653			Elisabeth Wirtenberger	26	Gundelsheim	Rentner Eberbach	evang	philol.	Paris	12	
654	"	17.	Otto Levy	21	Hamburg	Kaufmann Hamburg	i.	jur.	Leipzig	12	
655	"	17.	Ernst Möller	24	Celle	Fabrikbesitzer Eisenach	evg.	med. dent.	Jena	12	
656			Hans Meyer	21	Heidelberg	Oberpostsekretär Heidelberg	evg.	jur.	–	20	
657			Gustav Wohl	28	Ochsenfurt	Landwirt Lampertheim	kath.	med.	—	20	
658		18.	Walter Dankwardt	22	Stralsund	verstorbener Kaufmann in Stralsund.	ev.	cam. et jur.	Berlin	12	
659			Kurt Schönfeld	24	Breslau	Kaufmann Breslau	jüd.	jur.	Breslau	12	
660			Jul. Medsch.	18	St. Petersburg	Kaufmann Petersburg	jüd.	Philosophie		20	
661			N. Katschzatscheff	23	Moscau	Fabrikant, Bacou	arm.-greg.	medic.	Moscau.	20	
662			Emanuel Gulmann	25	Baumholder	Kaufmann, Hanau	isr.	Zahnheilk.	Breslau	12	
663			Joseph Hermann	22	[illegible]	[illegible] [illegible]	~~kath~~	med.	Freiburg	12	
664		19.	Isidor Karl Kühn	27	Berg. Rothenfels	Steinbruchbes. u. Gutsbesitzer B. Rothenfels	kath.	nat.	Karlsruhe	12	
665		20.	Louis Ruegsegger	23	Genève	Genève Suisse (Kaufmann)	ev.	jur.	Genève	12	
666			Alexander Bernstein	19	Moskau	Moskau (Bankier)	evangelisch	jur	—	20	
667			Hans Glaeser	22	Kreuznach	Steele (Ruhr) Kgl. Bahnhofsvorsteher	kath.	jur.	Münster i/W	12	
668			Ludwig Luger	22	Durlach	Durlach, Kaufmann	ev.	jur.	Kiel	12	
669			Francis Maxwell	28	Java	Ingenieur, London	prot.	Natur-mat	Zurich	20	
670			Viktor Jakubowski	20	Posen	Baumeister, Posen	kath.	nat.-ök.		20	
671			Ludwig Lothar Steuer	19	Bad [illegible]	Steuer [illegible] Kreuznach	ev.	natök.	Bonn	12	

Personen-Verzeichnisse in Hochschulen

- Mitarbeiter
- Studierende
- Studienbewerber
- Alumni
- Chipkarteninhaber
- Kursteilnehmer
- eLearning-Teilnehmer
- RZ-Benutzer
- Gremienmitglieder
- Bibliotheksbenutzer
- Arbeitszeitregistrierung
- Zentrales Adressverzeichnis
- Telefonverzeichnis
- Türschlüssel-Inhaber
- Parkberechtigungen
- Geräteausleiher
- Zertifikats-Inhaber
- Softwarelizenz-Inhaber
- Freunde und Förderer
- Lieferanten
- Gäste

Personen-Verzeichnisse in Hochschulen

- Hinter den meisten Verzeichnissen stehen eigenständige Anwendungen
- in vielen Fällen eigene Erhebungs- und Pflegeroutinen für die Personengrunddaten
- Eine Abstimmung/Synchronisation der Datenbestände untereinander ist nicht der Standard.

Gliederung

Fragestellung

Auflösung von Verwaltungsgrenzen

Schnittstelle HIS-GX Stagingtabellen

HIS-GX LDAP

Staging Tabellen (Gliederung)

- Initiative Metadirectory Thüringen
- LDAP Schnittstelle HIS-GX Version 7.0
  für Personal und Studierende
- Daten der Staging Tabellen
- Verarbeitung/Update/Einschränkungen
- Komplexität der Verwaltungsdaten

Initiative für die Staging Tabellen:

Metadirectory Entwicklung Thüringen

Die Stagingtabellen in HIS-GX für die Module SOS und SVA sind in Absprache mit dem Metadirectory Vorschlag Thüringen implementiert worden

Staging Tabellen

LDAP Schnittstelle HIS-GX Version 7.0 (2004)
für Personal und Studierende

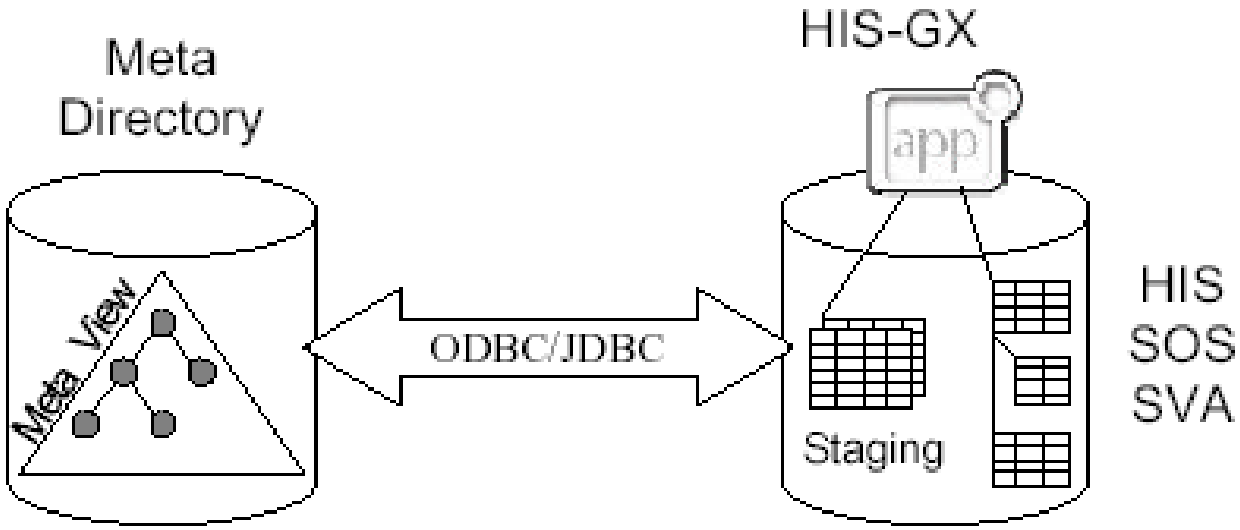

Abbildung 1: Prinzip der Staging-Tabellen

Quelle Metadirectory Thüringen

HIS und Verzeichnisdienst

- Je zwei Stagingtabellen in SOS und SVA mit identischen Feldern/Attributen

  Meta-Person und **Meta-Rolle**
  (1:n – Beziehung)

- Datenquelle bilden die Datenbanken der Personal- und Studierendenverwaltung

- Schutz der operativen Datenbanken

Daten der Stagingtabellen (SOS, SVA)

Meta-Person

Personal-Nr
Matrikel-Nr.
Familienname
Vorname
Post-Adresse
Akad. Grad
Geschlecht
Staat
Geburts-Datum
- Name
- Ort

Telefon Nr.
Fax Nr., eMail-Adr.

Meta-Rolle

(Personal)

Struktur/Org. Zugehörigkeit
Gruppenzugehörigkeit
Funktion
Kostenstellenzuordng
Beginn der Beschäftgg
Ende der Beschäftgg
Gebäude
Raum Nr.

(Studierende)

Studiengang
Fachsemester
Immatr. Datum
Exmatr. Datum

Aufbau der Staging Tabellen

- Jeder Satz in Meta-Person/-Rolle enthält einen Zeitstempel und Verarbeitungstempel
- Die Änderung eines Attributs wird in einem Attr.-flag (0/1) gekennzeichnet. Bei Löschung ist das Feld leer, das Attr.flag = 1
- Operationstypen: ADD, MOD, DEL
- MOD: eingeschränkt auf die zu ändernden Attribute mit flag=1
- Der Verarbeitungsstempel wird von HIS nicht bedient, für die Konnektoren vorgesehen

Update der Staging Tabellen Version 7.0

- Initial-Befüllung eines Directory ist über die Stagingtabellen nicht vorgesehen
- Stagingtabellen dienen der Aktualisierung des Metadirectory
- Einschränkung auf Daten, die in Dialogprozessen erfasst werden (Datenänderungen über Batchprogramme in SVA werden nicht übernommen)
- Daten, die in Form eines Schlüssels in SVA oder SOS verwaltet werden, werden im Klartext übermittelt. Keine systematische, nachträgliche Änderungen von Schlüsseltexten.

Update der Staging Tabellen Version 7.0

- Attribute sind in HIS-GX nicht frei konfigurierbar
- Identische Personen, in SOS und SVA, müssen über die Matrikel-Nr. in SVA identifiziert werden. Eine eindeutige ID-Nummer steht nicht zur Verfügung
- Stagingtabellen werden nicht geleert

  (geplant: konfigurierbare Löschbedingungen)
- Statusänderungen (z.B. Archivierung) werden nicht vermerkt
- Änderungen im Metadirectory werden derzeit nicht in die SOS bzw. SVA Datenbank übernommen

Schutz: Vermeidung nicht autorisierter DB-Zugriffe

- Umbenennung der Staging Tabellen
- Synonyme erzeugen für die ursprüngl. Staging Tab.
- Synonyme verweisen auf gleichnamige Tab. in einer anderen DB (META-DB)
- **Zum Lesen der Staging Tabellen sind keine Datenbankrechte für SOS- oder SVA notwendig**

Komplexität der Verwaltungsdaten

- Das ID-Management (Metadirectory/Verzeichnisdienst) benötigt klar strukturierte und einfache Attribute mit eindeutiger Aussagekraft. Z.B. Datum des Eintritts, der Immatrikulation, über das Studium, die Zugehörigkeit zu Hochschul-Institutionen ...
- Real kann ein Studirender bzw. eine Person z.B.

  gleichzeitig unterschiedliche Fächer studieren, mehrere Abschlüsse anstreben,

  gleichzeitig mehrere Beschäftigungsverhältnisse haben, die jeweils mehreren Kostenstellen zuzuordnen sind
- Die Komplexität der Verwaltung von Studierenden und Hochschulangehörigen muss dem ID-Mgmt verborgen bleiben.

Gliederung

Fragestellung

Auflösung von Verwaltungsgrenzen

Schnittstelle HIS-GX StagingTabellen

HIS-GX LDAP

HIS-LDAP (Gliederung)

- HIS-GX ID Nummer - Zusammenführung von rollen-unabhängigen Personendaten -
- Objektklasse hisPerson
- Anwendungsunabhängige HIS-GX Schnittstelle
- Berechtigungsmanagement für HIS-GX
- Zentrale Verwaltung übergreifender HIS-GX Schlüssel
- Authentifizierungsbasis für QIS und LSF
- ... z.B. zentrales Adressmanagement

HIS-GX ID Nummer

- Personendaten aus den Stagingtabellen in SOS (Studierende) und SVA (Beschäftigte) werden in HIS-LDAP zusammengeführt.
- Die Datenspeicherung ist redundant
- Die Erfassung zusätzlicher Personen direkt in LDAP
- Identitätsprüfung der Personendaten und Vergabe einer eindeutigen ID Nummer – Eliminierung von Duplikaten
- Freigabe mit HIS-GX-Version 8.0

hisPerson

Einführung einer (auxiliary) Objektklasse: hisPerson,

hisPerson ist abgeleitet aus der Standard Objektklasse eduPerson

Die Attributdefinitionen von eduPerson werden strikt beibehalten allerdings nur ein Teil der Attribute werden benutzt.

hisPerson wurde gegenüber eduPerson um zusätzliche Attribute erweitert, die keine Entsprechung in den LDAP Standard Objektklassen haben

hisPerson ist eine Schema Empfehlung

hisPerson umfasst mehr Attribute als die Stagingtabellen der HIS-GX Version 7.0

Das Update von HIS-LDAP erfolgt über Konnektoren, die auf die Stagingtabellen von SOS und SVA zugreifen

Objektklasse hisPerson, abgeleitet aus eduPerson

als relevant eingeschätzte Attribute der Standard Objektklassen:

person, organizationalPerson und inetOrgPerson

(**Vorschlag s. www.his.de von Peter Gietz, DAASI International GmbH Tübingen)**

sn / surname – Nachname
cn / commonName
(vollständiger Name einer Person)
userPassword (?)
telephoneNumber
facsimileTelephoneNumber
street (dienstl.)
postOfficeBox (dienstl. Postfach)
postalCode
postalAdress
physicalDeliveryOfficeName (?)
ou / organizationalUnitName

st / stateOrProvinceName (Bundesland)
l / localityName (Stadt)
department/Number
displayName (Vorname-blank-Nachname)
employeeNumber
employeeType
givenName (Vorname)
jpegPhoto (?)
mail
mobile (?)
roomNumber
uid (?) – login name

hisPerson – Attribute aus der eduPerson Objektklasse

Vorschlag s. www.his.de von Peter Gietz, DAASI International GmbH Tübingen

Relevante Attribute (zusätzlich zu Attributen aus den Objektklassen person, organizationalPerson und inetOrgPerson)

- eduPersonAffiliation (z.B. faculty, student, staff, alum, ...)
- eduPersonPrimaryAffiliation (Hauptzugehörigkeit)
- eduPersonOrgUnitDN (Zugehörigkeit zu Org.Einheiten)
- eduPersonPrimaryOrgUnitDN (Hauptzugehörigkeit)

Weniger relevante Attribute

- eduPersonEntitlement
- eduPersonNickname
- eduPersonOrgDN
- eduPersonPrincipalName
- eduPersonScopedAffiliation

hisPerson Attribute, die nicht in eduPerson enthalten sind

entsprechend der Standard Objektklasse naturalPerson (nP),
bzw. ohne Entsprechung in den Standard Objektklassen

- Person ID Nummer
- Namenserweiterungen
- Anrede
- Matrikel-Nr.
- Geschlecht (nP)
- Geburts-Datum (nP)
- - Name
- - Ort (nP)
- Staatsangehörigkeit (nP)
- Immatrikulationsdatum
- Datum des Ausscheidens
- akademischer Grad
- Studiengang / -Nr.
- Fach/Semester
- Kostenstelle
- Gebäude

HIS-LDAP : anwendungsunabhängige HIS-GX Schnittstelle

LDAP Replikation

Entwicklung und Aufbau eines HIS-GX Berechtigungsmanagements

- Die individuelle Rechtezuweisung in HIS-GX wird zukünftig durch rollengebundene Rechteprofile ersetzt.
- Für alle HIS-GX Module wird HIS-LDAP die zentrale Instanz zur Vergabe von Berechtigungen.
- Die Zuordnung eines Datenbank-Rechteprofils für eine Person (Zugriffe auf DB-Tabellen und Wertebereiche) erfolgt auf Modulebene zum Zeitpunkt der Synchronisation von LDAP-Server und jeweiligem Modul.

Übergreifende HIS-GX Schlüssel

- Die Pflege übergreifender Schlüssel (z.B. Kostenstellen) für die operativen HIS-GX Module erfolgt in HIS-LDAP.
- Durch Synchronisationsprozesse zwischen HIS-LDAP und den operativen Datenbanken erfolgt ein Schlüsselupdate in den Datenbanken.
- D.h. die übergreifenden Schlüssel werden redundant gehalten – in HIS-LDAP und in den HIS-GX Datenbanken.
- Der Betrieb von HIS-GX ist auch ohne HIS-LDAP möglich.

Authentifizierung

- Nutzung von HIS-LDAP zur Authentifizierung der Benutzer für die QIS-Module (Selbstbedienung/ eGovernment) und LSF.
- Die Hochschule legt fest, ob HIS-LDAP oder ein anderer Server für die Authentifizierung in QIS, LSF genutzt wird.
- Die Nutzung eines Authentifizierungsservers kann in den HIS-Modulen konfiguriert werden.
- Die Nutzung der Authentifizierungsfunktionen setzt geeignete Auth.-Attribute (Passwörter, Zertifikate) voraus.

HIS-LDAP Freigabe 1.10.2005 umfasst

- **Personendaten aus SOS und SVA**
- **Erfassungsmaske für zusätzliche Personendaten**
- **Identifikation: übergreifende ID Nummer**
- **Replikation**
- **Berechtigungsmanagement für ausgewählte HIS-GX Module**
- **Übergreifende Schlüssel**

Danke für Ihre Aufmerksamkeit