Tivoli Security Solutions

Ein Identity Management Prototyp für Hochschulen unter Benutzung von IBM Tivoli Identity Manager und IBM Tivoli Directory Integrator

Reinhard Stamms
IBM Tivoli Security Technical Sales
paul@de.ibm.com

02.06.2005

Warum ein Prototyp

Viele grundlegende Prozesse und Datenflüsse sind an Hochschulen ähnlich

- **Der Prototype erweitert das Standard-Produkt**
  - **Implementiert Datenmodell**
    - Modelliert alle Personentypen einer Hochschule in Superrollen
      - Rollenübergänge, zeitliche Befristung, Automation, Verlängerungsanträge
      - Datenübernahme von HIS, Identity Mapping (Vorname, Nachname, Geb.-Datum)
  - **Implementiert Organisationsstruktur & Admin-Konzept**
    - Zentrale Administration - Rollen, Policies, Provisioning
    - Bereichsorientierte Administration
      - Erfassung von Gästen & Provisioning Aufgaben
    - automatisierte Pflege der Bereichsstruktur & -berechtigungen
  - **Implementiert ein White Pages LDAP Directory**
    - Attributzugriff gesteuert durch Self Care: *Informationelle Selbstbestimmung*
    - automatisierte Pflege der LDAP Bereichsgruppen und ACLs
  - **Genereller Email Service – Qmail, Postfix, Sendmail**

Ziel: Eine Pilotumgebung kann schnell erreicht werden

Datenmodell

- **Ein Person-Objekt implementiert Superrollen**
  - Studierende, Mitarbeiter, Gäste, Externe
    - alle Superrollen gleichzeitig möglich
    - Superrollen zeitlich befristet
      - Erfassungsmasken Gäste & Externe
      - Self Care Verlängerung (Gäste & Externe)
      - Automation durch Workflows & Central Rules
        - einheitliche uid, customerID, Voreinstellungen
        - Beendigungsbenachrichtigungen …
        - … für alle Superrollen getrennt einstellbar

- **LDAP-Klasse UniPerson für Person-Objekt**
  - Attribute aus inetOrgPerson
  - Attribute für Studierende, Mitarbeiter, Gäste, Externe
  - Attribute für „Informationelle Selbstbestimmung“
  - Attribute zur Steuerung von HR Feed & Rules

- **erweiterbar**

Datenmodell - Superrollen

Superrolle	**Studierende**	**Mitarbeiter**	**Gäste**	**Externe Mitarbeiter**
Bestimmendes Attribut	**isRegistered** [true, false]	**isUniEmployee** [true, false]	**isGuest** [true, false]	**isExternal** [true, false]
Weitere Attribute	**courseOfStudy** **courseOfStudyExp** **courseOfStudyEx2** **studentDepartments**	**employeeType** **employeeTypeExp** **employeeTypeEx2** **departmentNumber**	**guestDepartment** **guestClassification** **workgroup** **workshop** **dateOfRemoval** **removalWarning** **guestSuspended** **canrenew** **noOfRenewals**	**extEmployeeType** **extDepartment** **dateOfRemovalExt** **removalWarningExt** **renewme** **noOfRenewalsExt**

Datenmodell – Attribute zur Zeitsteuerung

Person Objekt eines Studierenden vor/nach der Ende-Warnung

isRegistered	=	true
courseOfStudy	=	66#Mathematik#01
courseOfStudy	=	33#Biologie#02
courseOfStudyExp	=	200509290000Z#02
studentDepartments	=	07#01
studentDepartments	=	11#02

isRegistered	=	true
courseOfStudy	=	66#Mathematik#01
courseOfStudy	=	33#Biologie#02
courseOfStudyEx2	=	200509300000Z#200509290000Z#02
studentDepartments	=	07#01
studentDepartments	=	11#02

Person Objekt eines Gastes

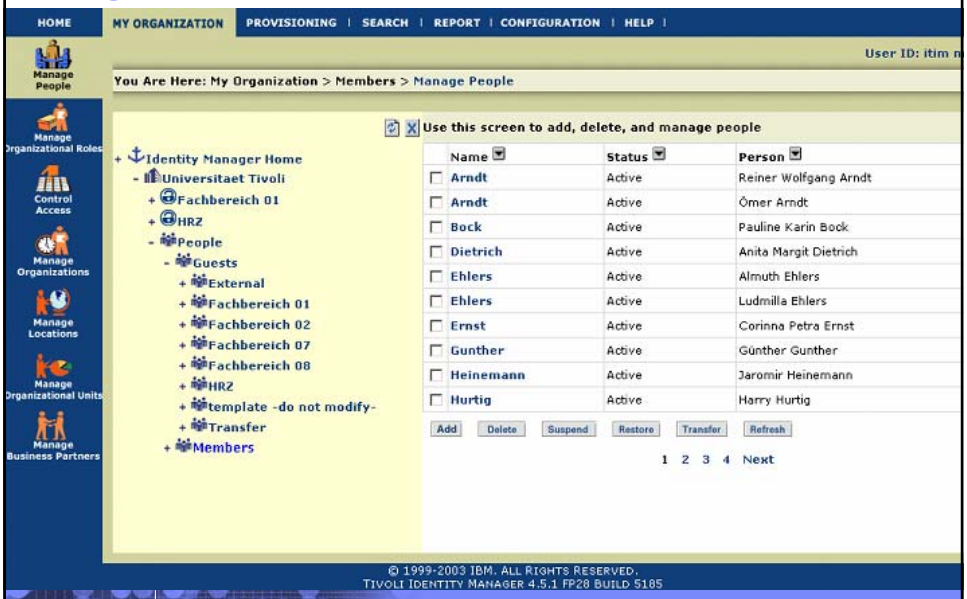
isGuest	=	true	guestDepartment	=	66#Mathematik
dateOfRemoval	=	200511290000Z	guestClassification	=	workgroup
canrenew	=	true	workgroup	=	wg1

Organisationsstruktur

- **Management von Provisioning**
  - flache Hierarchie von Admin Domains je Bereich
    - Provisioning Aufgaben, Services, Statische Rollen, BPPerson
  - einfaches Admin-Konzept: *Prinzipal Domain Administrator*
    - zentrale ACIs

- **Management von People**
  - bereichsorientierte Struktur für Gäste-Management
  - einfaches Admin-Konzept: *Group DomainAdmins + BereichAdmins*
  - automatisierte Pflege der Bereichssruktur + Bereichs-ACIs + BereichAdmins
    - Basis: Kostenstellendaten aus MBS

Organisationsstruktur - Screenshot



White Pages LDAP Directory

- Auskunftssystem
- Basis für Synchronisationen
- Repository für Anwendungen

- inetOrgPerson, eduPerson, UniAuxPerson

- Custom ITIM-Agent, Provisioning Policy, Dienstprogramm, LDIFs

- Implementiert Zugriffssteuerung für „Informationelle Selbstbestimmung“
  - dynamische Zugriffssteuerung auf Attributebene
  - Implementierung durch Filter-ACLs und LDAP-Gruppen
    - Gruppen: internet, uni, uni-sync, + Bereichs-Gruppen
  - Self Care im ITIM

- Dienstprogramm zur automatisierten Pflege
  - der Bereichs-Gruppen und Bereichs-ACLs
    - Basis: Kostenstellendaten aus MBS
  - Provisioning Policy wiest LDAP-Accounts die Gruppen zu

Implementierung Informationelle Selbstbestimmung

Eine Person kann in den 4 Kategorien …

Kategorie	Bedeutung	LDAP Attribut	Betroffene Attribute	
Identifikation	**Zugriff auf das gesamte Objekt**	**iselfidentification**	**alle**	[i,u]
Arbeitsbereich	**Zugriff auf Attribute, die den Arbeitsbereich betreffen**	**iselfwork**	**departmentNumber employeeType employeeNumber studentDepartments**	[i,u]
Adressen	**Zugriff auf Adreßangaben**	**iselfaddress**	**postalAddress postOfficeBox l street ou mail telephoneNumber facsimileTelephoneNu..**	[i,u]
Privat	**Zugriff auf private Daten**	**iselfprivate**	**homepostaladdress homephone mobile**	**[i,u,d,none]**

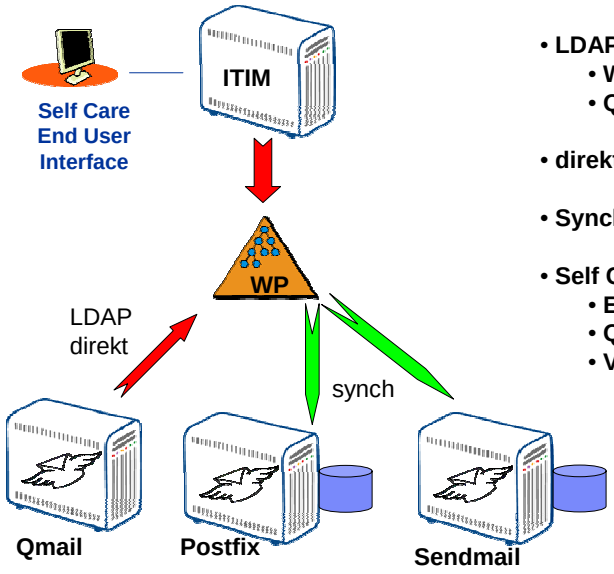
… folgende 4 Werte festlegen

i	→ Internet.	Anonymer Zugriff
u	→ Uni.	Hochschulweiter Zugriff
d	→ Department	Zugriff nur für den jeweiligen Bereich der Person
none	→ Kein Zugriff	(Attribute sind nicht vorhanden)

HISmulator

- Datenbank mit Tabellen konform zu HIS-SOS
  - Staging Tables, k_stg
- Bespieldaten
- Können mit ITDI DataFeed ins ITIM geladen werden

Genereller Email Service



- LDAP Repository
  - White Pages – standalone
  - Qmail Schema
- direkter LDAP-Zugriff
  oder
- Synchronisation in Dateien
- Self Care GUI
  - Email Adressen
  - Quota
  - Vacation Reply