Fachhochschule Osnabrück
University of Applied Sciences

ZKI Tagung Verzeichnisdienste 08/09.02.10

Konzeption und Umsetzung von Identity Management an der FH-Osnabrück und der Vergleich zu anderen Hochschulen

Dipl.-Ing IT (FH) Jürgen Kuper

Gliederung

Fachhochschule Osnabrück
University of Applied Sciences

1. Historie
2. Aufbau META Verzeichnis
3. Struktur Benutzer-Rollen
4. Quellsysteme
5. Zielsysteme
6. Vergleich mit Projekten Uni-Jena und Uni-Oldenburg
7. Zusammenfassung

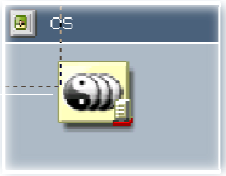
Historie

Fachhochschule Osnabrück
University of Applied Sciences

•Ca. 8300 Studierende
•Dezentrale IT Struktur (ohne RZ)
•In den Fakultäten eigenständige IT

•Seit 2001 zentrale Benutzerverwaltung
•Mit eDir als zentrales Verzeichnis

•Viele Dienste angeschlossen
•Sync. über Skripte bzw. manuell
•Eingeschränktes Rollenkonzept
•Erfahrungen in IDM Projekt eingeflossen



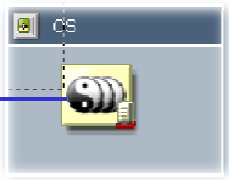
Zentrale Benutzer-verwaltung

Aufbau META Verzeichnis

Fachhochschule Osnabrück
University of Applied Sciences

•Seit 2007 IDM Projekt
•Aufbau META-OS
•Entwicklung Struktur und Rollensystem
•Anschluss ehemaliges zentr. Verzeichnis als Zielsystem

META-OS

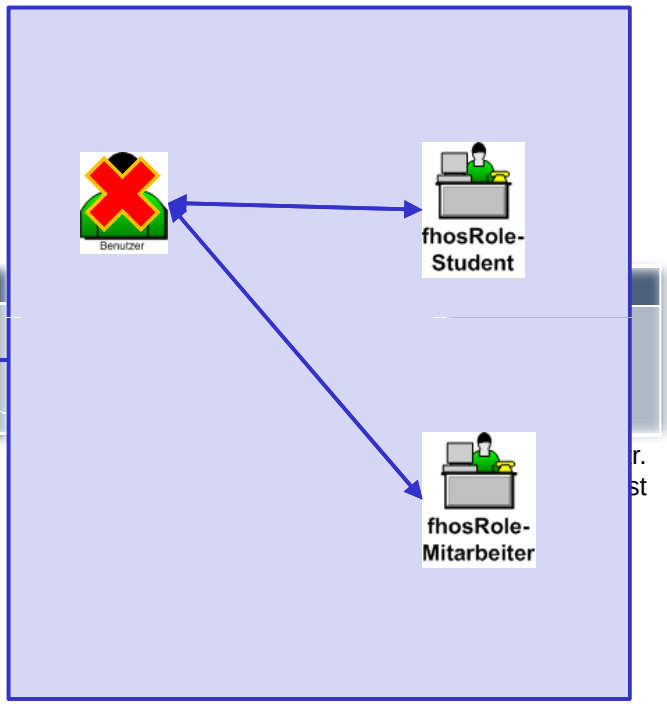


Ehemaliger zentr. Verzeichnisdienst

Struktur Benutzer - Rollen

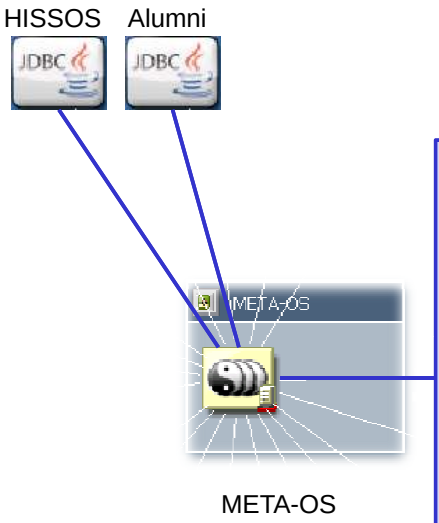
Fachhochschule Osnabrück
University of Applied Sciences

- Jede Identität ist im Verzeichnis enthalten
- Jede Identität hat mindestens eine Rolle (lt. ihrer Funktion)
- Wenn die Funktion nicht mehr gegeben ist wird die Rolle gelöscht (Rollenende erreicht)
- Hat eine Identität keine Rolle mehr, wird der Benutzer gesperrt
- Nach 90 Tagen wird dann das Benutzerobjekt gelöscht (außer es wird eine neue Rolle hinzugefügt)



Quellsysteme

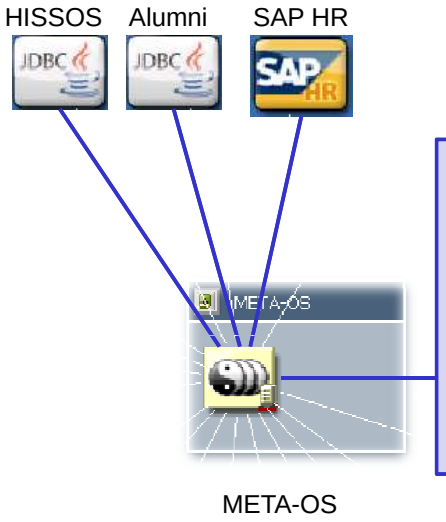
Fachhochschule Osnabrück
University of Applied Sciences



META-OS

- Das HISSOS System ist über DB Views angebunden
- Je einen für die Identität und einen für die Rolle
- Wg. Synchronisation wird der Rollendatensatz erst im DB View sichtbar wenn Attribute zurücksynchronisiert sind
- Das Rollenende steht auf Semester-ende
- Bei Exmatrikulation bzw. Rückmeldung wird das Rollenende angepasst.
- Der Alumnitreiber arbeitet analog

Quellsysteme

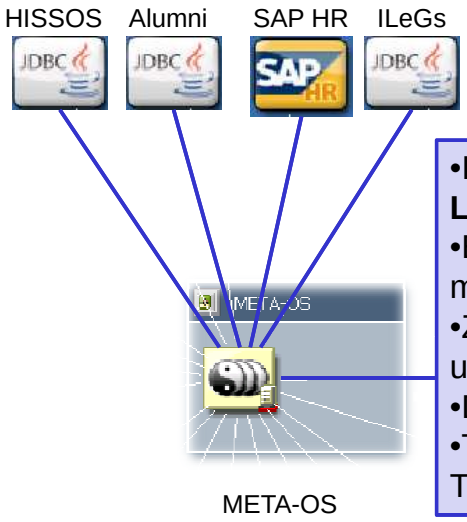


META-OS

- Es ist ein SAP Treiber in der IDM Software enthalten
- Im SAP HR System werden Professoren und Mitarbeiter verwaltet.
- Das Rollenende ist das konkrete Ausscheidungsdatum
- Emeritierte Professoren behalten die zugehörige Rolle

Verzeichnisdienst

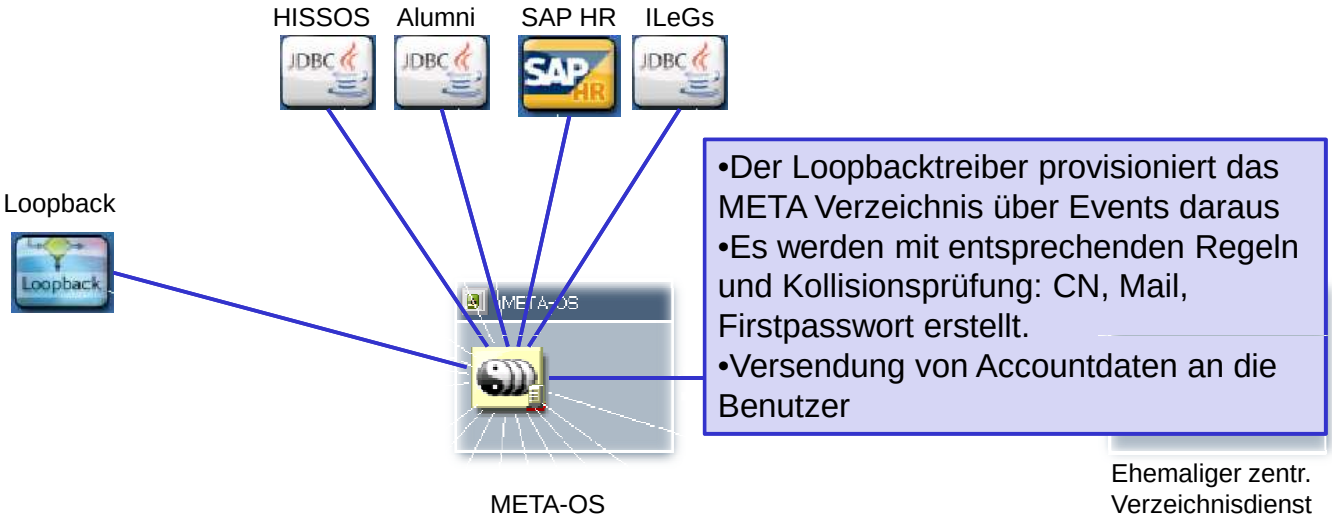
Quellsysteme



META-OS

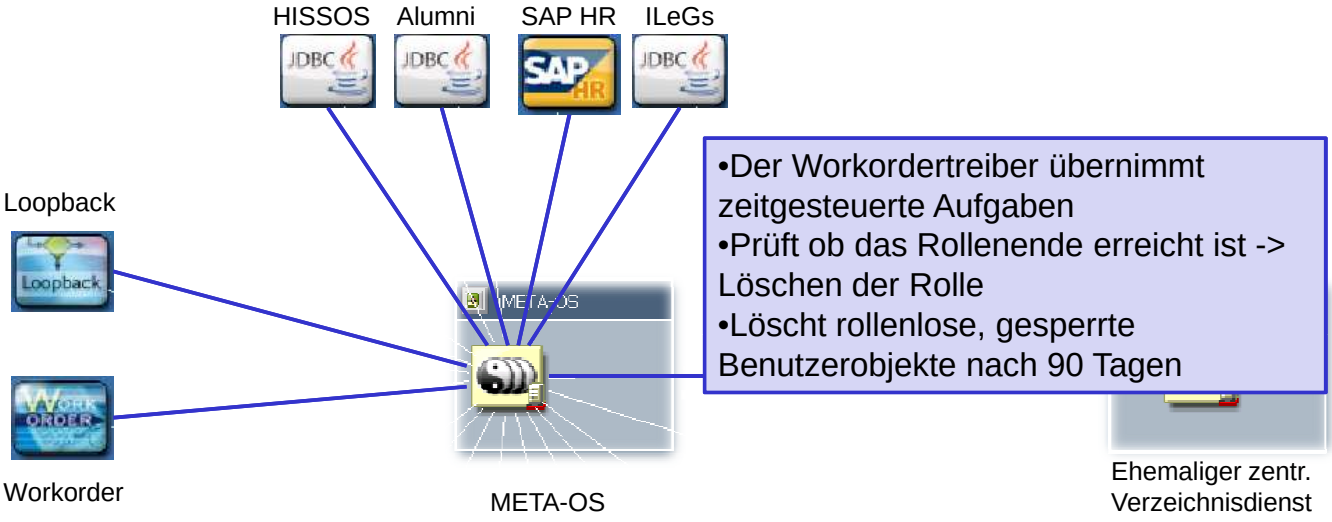
- ILeGs=**I**dentity Management für **Le**hrbeauftragte und **G**ä**s**te
- Eigenentwicklung um Identitäten möglichst früh im Prozess zu erfassen
- Zusätzlich: Workflow für‘s Management um Lehrbeauftragte bis zur Abrechnung
- Datenbankanwendung mit Webfrontend
- Treiber von der Struktur wie HISSOS Treiber

Zielsysteme



- Der Loopbacktreiber provisioniert das META Verzeichnis über Events daraus
- Es werden mit entsprechenden Regeln und Kollisionsprüfung: CN, Mail, Firstpasswort erstellt.
- Versendung von Accountdaten an die Benutzer

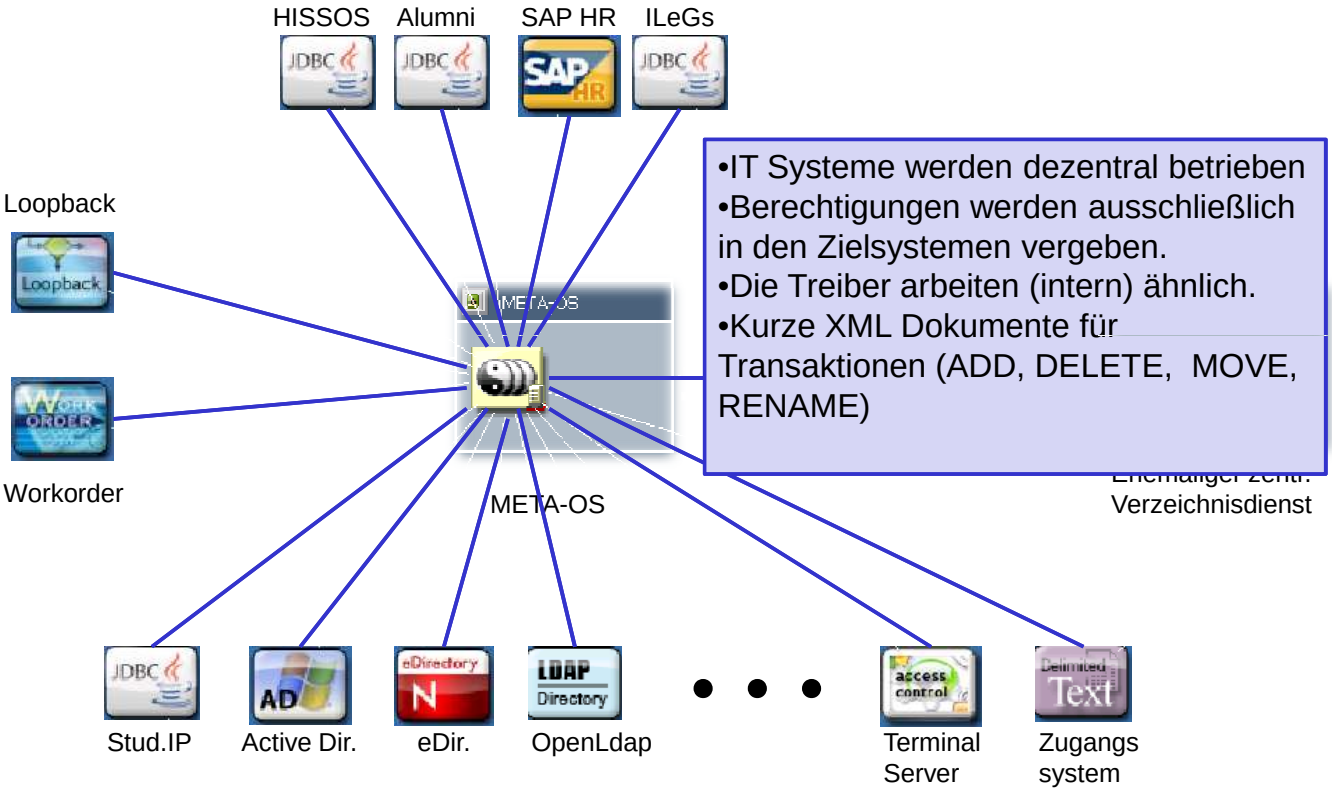
Zielsysteme



- Der Workordertreiber übernimmt zeitgesteuerte Aufgaben
- Prüft ob das Rollenende erreicht ist -> Löschen der Rolle
- Löscht rollenlose, gesperrte Benutzerobjekte nach 90 Tagen

Zielsysteme

Fachhochschule Osnabrück
University of Applied Sciences

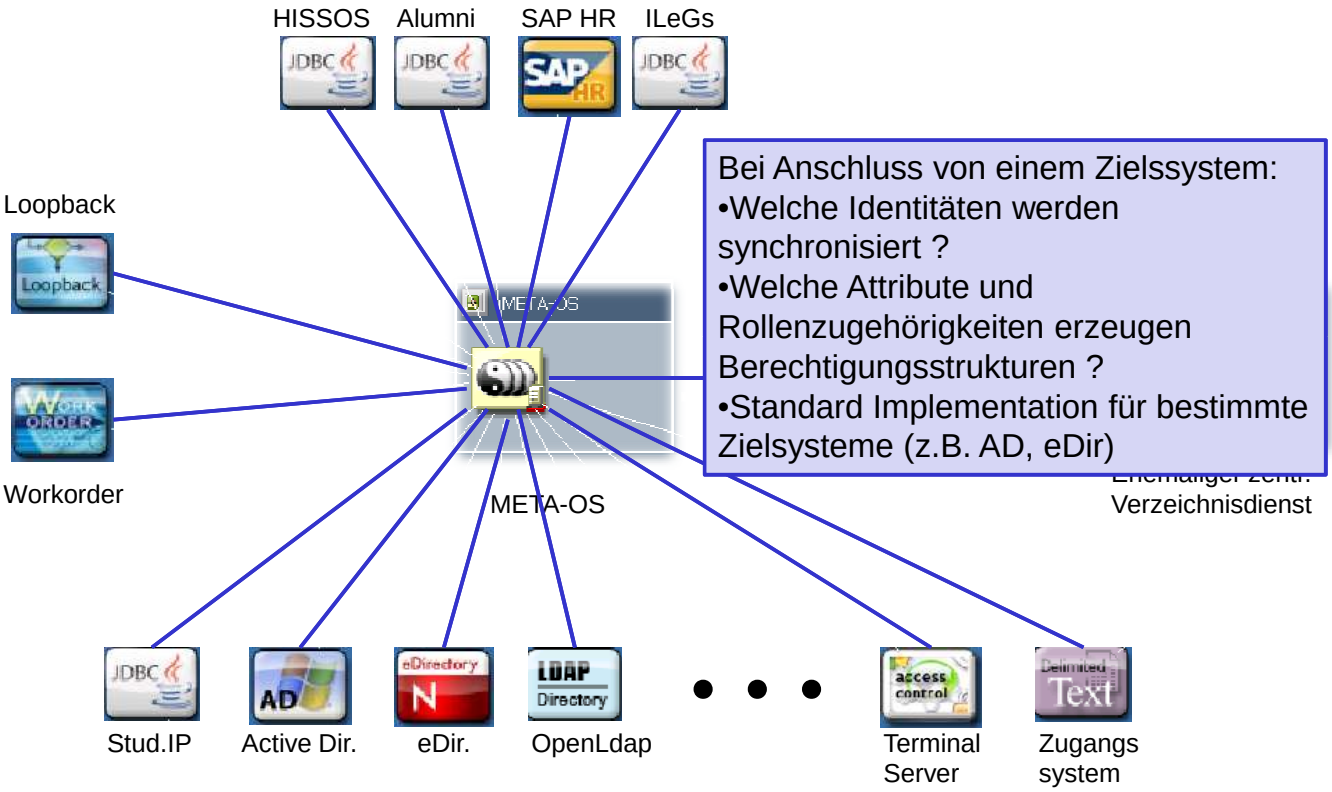


- IT Systeme werden dezentral betrieben
- Berechtigungen werden ausschließlich in den Zielsystemen vergeben.
- Die Treiber arbeiten (intern) ähnlich.
- Kurze XML Dokumente für Transaktionen (ADD, DELETE, MOVE, RENAME)

Verzeichnisdienst

Zielsysteme

Fachhochschule Osnabrück
University of Applied Sciences



Bei Anschluss von einem Zielssystem:
- Welche Identitäten werden synchronisiert ?
- Welche Attribute und Rollenzugehörigkeiten erzeugen Berechtigungsstrukturen ?
- Standard Implementation für bestimmte Zielsysteme (z.B. AD, eDir)

Verzeichnisdienst

Vergleich

Fachhochschule Osnabrück
University of Applied Sciences

- Ziel eines IDM Projektes ist immer gleich
- Trotzdem Unterschiede bei der Prozessumsetzung, durch:
  - Eigenheiten der eingesetzten IDM Software
  - Unterschiede in den Hochschulen
  - Abbildung von IT Prozessen
  - Ansätze zur Vergabe von Berechtigungen
  - Schwerpunkte bei der IDM Umsetzung
  - Ressourcen Einsatz im Projekt

Vergleich

Fachhochschule Osnabrück
University of Applied Sciences

- Vergleich von IDM Projekten mit gleicher Softwaregrundlage
- Dadurch Vergleich der konzeptionellen Ansätze
- Hier Einsatz ‚*Novell Identity Manager*‘
- Übersichtsdiagramme der IDM Struktur (nahezu) gleich

FH Osnabrück
•8300 Studierende
•12.000 Identitäten
•IDM Projekt: Seit 2007
•Siehe Oben

Uni Jena
•25.000 Studierende
•40.000 Identitäten
•Seit 2003 (produktiv 2007)
•Landesweites Projekt, jetzt betreibt jede HS ein eigenes META Verzeichnis

Uni Oldenburg
•10.000 Studierende
•15.000 Identitäten
•Seit 2005
•Mehrfache Mitarbeiterwechsel/ Projektänderung

*(Stand WS09/10)

Vergleich

Fachhochschule Osnabrück
University of Applied Sciences

- Ergebnis des Vergleiches:

  „Die IDM Projekte sind zu unterschiedlich.
  Ein konkreter Vergleich sprengt (hier) den Rahmen“

- Bei einem Vergleich kommt man schnell auf Implementierungs-Details, die an vielen Stellen im IDM System greifen
- Gerade diese Details beeinflussen die Struktur des Systems
- Details beinhalten die besonderen Gegebenheiten und Unterschiede

- Zwei Beispiele:

Beispiel: Strukturierung durch Rollen

Fachhochschule Osnabrück
University of Applied Sciences

FH Osnabrück

•7 Rollen

Uni Jena

•Zeitstudent
•Praktikant
•UKJ
•Kooperationspartner
•Gastwissenschaftler
•Student anderer Hochschule
•Studentenwerk
•Funktioneller Account

•16 Rollen (Rollentypen)

Uni Oldenburg

•4 Rollen

•Unterschiede direkt sichtbar
•Aber die Anzahl der Rollen lässt keinen Schluss auf die Qualität des IDM Systems zu
•Es zeigt lediglich die Stärke der Granulierung

•Bei näherer Betrachtung: Unterschiede bei der Nutzung der Rollen
Beispiel primäre/führende Rolle (Bei Benutzern mit mehreren Rollen):

Beispiel: Strukturierung durch Rollen

Fachhochschule Osnabrück
University of Applied Sciences

•Unterschiede direkt sichtbar
•Aber die Anzahl der Rollen lässt keinen Schluss auf die Qualität des IDM Systems zu
•Es zeigt lediglich die Stärke der Granulierung

•Bei näherer Betrachtung: Unterschiede bei der Nutzung der Rollen
Beispiel primäre/führende Rolle (Bei Benutzern mit mehreren Rollen):

FH Osnabrück

•Statische Berechnung der primären Rolle

•Durch Bewertung der möglichen Rollen
•Referenz auf die führende Rolle wird als Attribut gespeichert

Uni Jena

•Berechnung der führenden Rollen während der Laufzeit (bei Bedarf)

•Innerhalb eines IDM Treibers wird eine Javaklasse aufgerufen.
•Diese Klasse liefert für den Bedarfsfall eine Bewertung der eingenommenen Rollen

Uni Oldenburg

•Gleichberechtigte Rollen

Beispiel: Authentisierungscontainer

Fachhochschule Osnabrück
University of Applied Sciences

- Jedes IDM System betreibt (neben dem Meta Verzeichnis) einen weiteren Container mit allen Identitäten.

FH Osnabrück
•eDir
(ehem. Benutzerverwaltung)
•Historisch bedingt

Uni Jena
•eDir
(Verzeichnis A1)
•Zur Authentisierung (nur wenige Attribute vorhanden)

Uni Oldenburg
•Zentrales Active Directory

•Zur Authentisierung

- Bei näherer Betrachtung: Unterschiedliche Gründe und Nutzung.
- In Os.:“ legacy System“
- Bei den Anderen: Zentraler Baustein im IDM System
- Unterschiedliche Regeln: Hier Authentisierung

Vergleich und Austausch bringt neue Impulse !

Zusammenfassung

Fachhochschule Osnabrück
University of Applied Sciences

- Erfahrungen aus zentraler Benutzerverwaltung
- Ehemaliges zentrales Verzeichnis als Zielsystem (zum Erhalt ‚Status Quo‘)
- Neues META Verzeichnis
- Erweitertes Rollenmodell
- Loopback und Workordertreiber für verzeichnisinterne Aufgaben
- Quellsysteme: HISSOS, SAP und ILeGs (Eigenentwicklung)
- Verschiedene Zielsysteme mit Standard-Implementationen
- Provisionierung in den IDM Treibern, Berechtigungen in den Zielsystemen

- Ausblick:

Entscheidung über integriertes Campusmanagementsystem in OS

Bedeutung für IDM Projekt: Neue Quellsysteme. Das Quellsystem ist dann auch gleichzeitig Zielsystem…

Zusammenfassung

Fachhochschule Osnabrück
University of Applied Sciences

- IDM Projekte haben immer das gleiche Ziel
- Die grobe Struktur ist ähnlich
- In den Details große Unterschiede auch bei gleicher SW Grundlage
- Detaillierter Vergleich sprengt (hier) den Rahmen
- Austausch untereinander bringt neue Impulse

- Ausblick: Netzwerkbildung ?
  - Für Nutzer vom *‚Novell Identity Manager‘*
  - Konkretisierung von Ergebnissen des AK
  - Vielleicht Nutzertreffen mit konkreten Themen?
- Kontakt: j.kuper@fh-osnabrueck.de

Identity Management – Ein langer Weg

„Eine lange Reise beginnt immer mit dem ersten Schritt.“ - Konfuzius

Vielen Dank für Ihre Aufmerksamkeit