Workshop 1: Bausteine für sicheres Informationsmanagement

Identity Management an Hochschulen

Dipl.-Math. Frank Klapper
IT-Manager
Universität Bielefeld

Gliederung

- **Motivation „Identity Management“**
- Begriffsklärung
- Vorgehen in einem Projekt

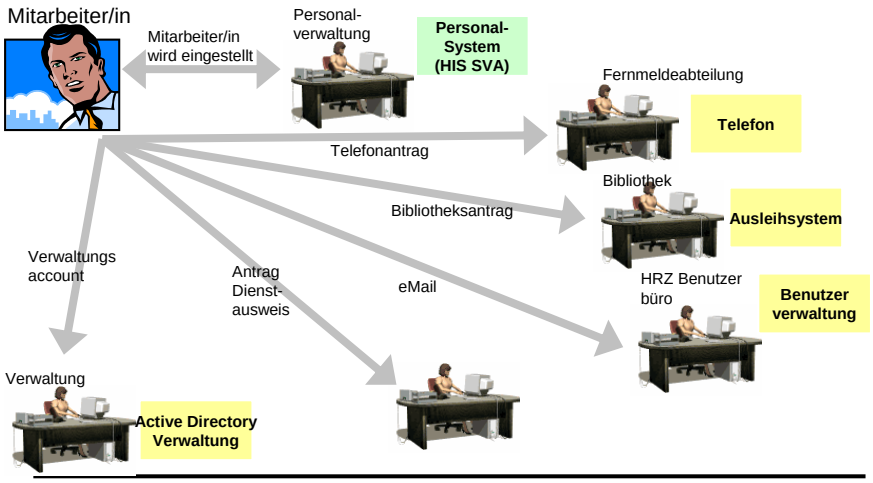
Motivation „Identity Management“

- Ansatz:
  - Universitätsweiter Service zur Bereitstellung von Daten, insbesondere Personendaten
- Strategische Ziele:
  - Verbesserung der Dienstleistungen der Universität für Studierende, Mitarbeiter und Gäste
  - Reduzierung der Infrastrukturkosten durch
    - Vereinfachung und Automatisierung der Administrationsprozesse
    - Verminderung von Datenredundanzen
    - Verbesserung der Qualität und Aktualität der Daten
    - Reduzierung der Administrationsaufwände für die Endbenutzer
    - Erhöhung der **Sicherheit**
    - Vereinfachung der **Integration** zukünftiger Anwendungen und Portale

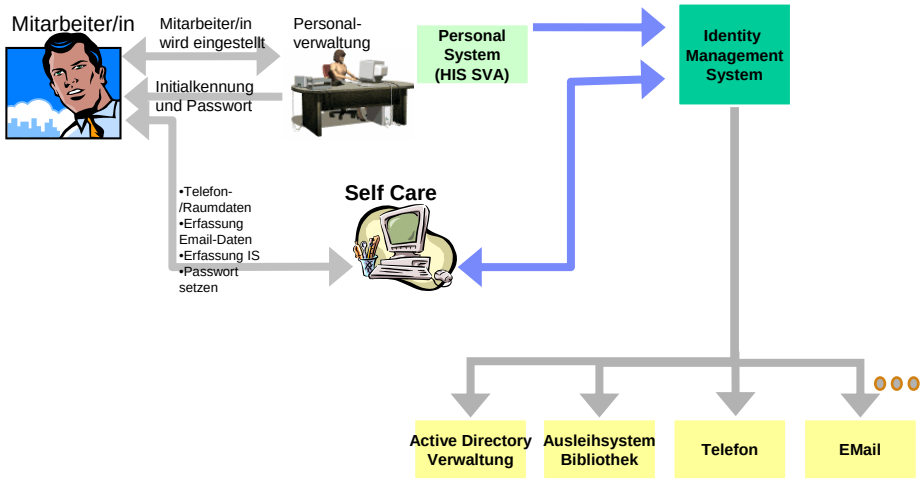
Motivation „Identity Management“

- **Heute:** Erfassung und Pflege von **Personenidentitäten** in verschiedenen I&K Systemen sind nicht abgestimmt:
  - Unvollständige, inkonsistente, veraltete und nicht vorhandene Datenbestände
  - Für Benutzer hochgradig unkomfortabel und unnötig kompliziert
  - Integration der Systeme nicht möglich
- **Lösung:** Einführung eines umfassenden **Identity Management Systems**, welches die Identitäts-Daten der einzelnen I&K Systeme / Verzeichnisse zusammenführt:
  - Vereinfachung der Datenverwaltung
  - Datenkonsistenz herstellen
  - Voraussetzung für integrierte Dienste schaffen

IST-Prozess: Wie kommt ein/e Mitarbeiter/in zu ihren/seinen Berechtigungen



Soll-Prozess: Wie kommt ein/e Mitarbeiter/in zu ihren/seinen Berechtigungen



Nutzen (1):
Nutzer (Reduzierung der Anlaufstellen)

- Die Studierenden und die Mitarbeiter bekommen bei der Immatrikulation oder Ihrer Einstellung sofort eine Benutzer-ID und ihr Initial-Kennwort. Dadurch erhalten sie praktisch umgehend auch ihre entsprechenden Zulassungen in den einzelnen EDV-Systemen (Directories)
- Je nach Prozess erfolgt dies eventuell erst nach der Anmeldung an der Self Care-Anwendung, damit keine überflüssigen Benutzerkonten in den Ziel-Systemen entstehen.
- Die Self Care-Anwendung ermöglicht dem Anwender selbst bestimmte Daten aktuell zu halten, damit er möglichst selten persönlich im Benutzerbüro erscheinen muss. Dies erhöht die Datenqualität in den angeschlossenen Systemen und verbessert damit die darauf basierenden Prozesse anderer Einrichtungen, wie z.B. der Bibliothek.

Nutzen (2):
Fachbereiche / Fakultäten

- Durch Schaffung von zentralen universitätsweiten Directories können den Fachbereichen die notwendigen Informationen über die Personen zur Verfügung gestellt werden.
- Anwendungen der Fachbereiche können diese Informationen nutzen und müssen keine eigenen redundanten Datenbestände, z.B. eigene Nutzerverwaltung aufbauen, deren Datenqualität aufgrund des hohen Administrationsaufwandes nur beschränkt wäre.
- Fachbereichsinformationen können dezentral eingepflegt werden und im Bedarfsfall auch anderen Fachbereichen zur Verfügung gestellt werden.

Nutzen (3):
Web-Portal (einheitlicher Dienstezugang)

- Ein Portal besteht aus einer Vielzahl von Anwendungen (Mail, Kalender, Bibliothekszugang, Prüfungsinformation, …), die dort in einer Benutzeroberfläche zur Verfügung gestellt werden.
- Diese Anwendungen nutzen eine Vielzahl von Datenbanken, Directories, Dateien, Drucker usw…
- Diese Ressourcen werden von verschiedenen Berechtigungssystemen geschützt.
- Durch die Vereinheitlichung von Benutzer-ID und Kennwort, können sich Anwender an einem Portal anmelden und dort unterschiedlichste Anwendungen starten ohne sich an jeder einzelnen Anwendung erneut anmelden zu müssen. (Single Sign-On)

⇨ Die Vereinheitlichung ist nur möglich, wenn durch ein Identity Management-Projekt die Basis geschaffen wurde.

Nutzen (4):
Telefonbuch / Adressbuch

- Das Identity Management ermöglicht ein ständig aktuelles Telefon- und Adressbuch.
- Durch klar definierte Prozesse und durch definierte Datenflüsse wird sichergestellt, dass die notwendigen Basisdaten immer aktuell gehalten werden und diese in die Zielsysteme kommen.
- Der Endanwender bekommt somit einen immer aktuellen Datenbestand zur Verfügung gestellt, der ihn bei seiner täglichen Arbeit unterstützt, z.B. beim Auffinden von E-Mail-Adressen, Telefonnummern oder der Raumnummern seiner Kollegen.
- E-Mail-Verteiler können leicht erzeugt und aktuell gehalten werden. Damit können zuverlässig alle Personengruppen über E-Mail erreicht werden.

Nutzen (5): Sicherheit und Datenschutz

- Das Niveau wird spürbar angehoben:
  - Dokumentation der Personenverzeichnisse, Datenflüsse und Zugriffsberechtigungen
    - •Schwachstellen werden aufgedeckt
  - Transparente und eindeutige Prozesse
  - Konsistente und aktuelle Datensätze
    - •**Die Löschung von Berechtigungen werden oftmals erst möglich**
  - Rollenbasierte Rechtekonzepte werden möglich
- Viele Anforderungen der **informationellen Selbstbestimmung** fallen quasi „nebenbei“ ab.
- Qualitativ hochwertige und gut strukturierte Daten ermöglichen den effizienten Einsatz von Sicherheitssoftware: Kennwortsynchronisation, Single Sign-On, Web Access Management, **Public Key** Infrastruktur, …

Nutzen (6): Wirtschaftlichkeit des Identity Managements

- Folgende Erfahrungswerte gelten im Identity Management
  1. Ab 3.000 Benutzer kann sich ein Identity Management lohnen
  2. Ab 10.000 Benutzern amortisiert sich der Aufbau eines automatisierten Identity Managements in jedem Fall
  3. Ab mehreren 10.000 Benutzern ist das Fehlen eines Identity Managements ein echter Wettbewerbsnachteil für jede Organisation.
- Eine Identity Management-Lösung kann im Universitätsumfeld „kostengünstig” aufgebaut werden, wenn diese Lösung mit den gleichen Produkten in möglichst vielen Universitäten aufgebaut wird. Gerade in der Implementierungsphase ergeben sich hier enorme Synergieeffekte zwischen den Universitäten.

➢ Quelle: IBM

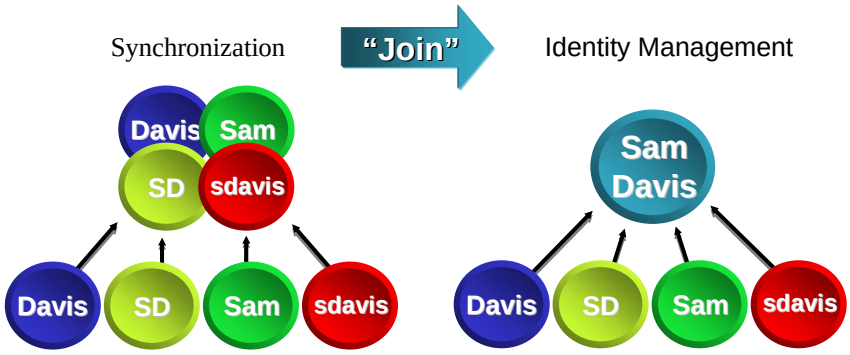
Gliederung

- Motivation „Identity Management“
- **Begriffsklärung**
- Vorgehen in einem Projekt

Was ist **Identity Management ?**

- Die konsistente Verwaltung von Personenidentitäten (Mitarbeitern, Kunden, Lieferanten) in IT-Systemen über mehrere heterogene Systeme, Anwendungen und Verzeichnisse.
  - Erstellen, Ändern und Löschen von Benutzerkonten und –profilen in den angeschlossenen Systemen.
  - Datensynchronisation von Benutzerkonten und –profilen zwischen den angeschlossenen Systemen.
  - Automatische Übernahme von Daten aus einem Quellsystem.

Identity Management



Was sind **Verzeichnisse / Directories** ?

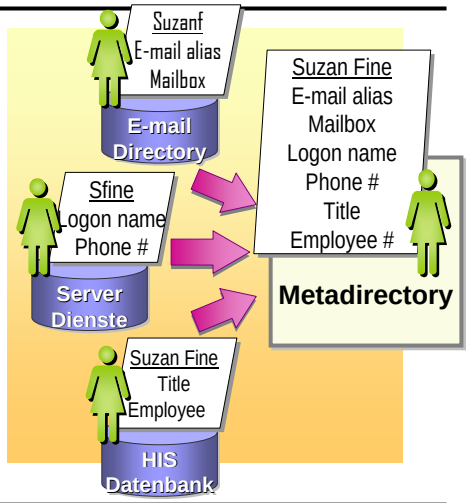
- Beispiele:
  - Telefonbuch
  - Fernsehzeitung
  - Versandhauskatalog
  - Kundenkartei
- Gemeinsame Eigenschaften:
  - Es sind Sammlungen von Einträgen
  - Änderungen der Einträge sind seltener als Abfragen
  - Es erfolgen häufig Anfragen nach bestimmten Einträgen
  - Die Einträge sollten sinnvoll gegliedert sein
- Fokus in diesem Vortrag:
  - Personen-/Nutzer-Verzeichnisse

Was ist ein **Meta-Directory** ?

- **Definition:** Meta-Directories ermöglichen den Zugang zu sämtlichen Informationen einer Organisation, die in unterschiedlichen Verzeichnissen gespeichert sind sowie deren Administration von einer einzigen Stelle aus (Burton Group, Februar 1996).
- Meta-Directories haben das Ziel:
  - Eine Teilmenge von Daten aus angeschlossenen Verzeichnissen zu synchronisieren, aggregieren und in einem zentralen Verzeichnis zu speichern.
  - Die Identitäten über alle angeschlossenen Verzeichnisse eindeutig, aktuell, vollständig und korrekt zu halten.
  - Das Erstellen, Ändern und Löschen von Benutzerkonten und –profilen in angeschlossenen Verzeichnissen zu automatisieren.

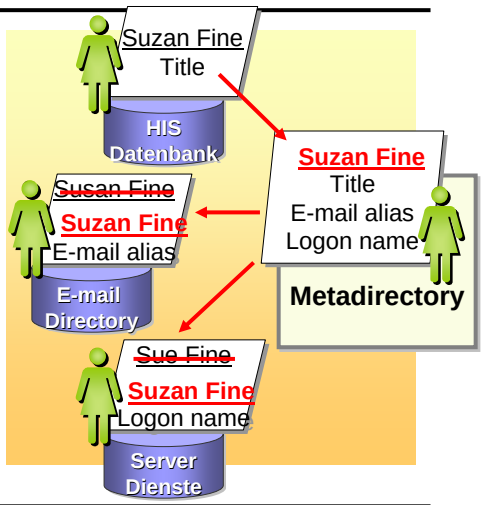
Meta-Directory

- Ein Meta-Directory erstellt eine Identität durch:
  - die Kombination von Informationen aus ver-schiedenen Verzeichnissen
  - die Präsentation **einer** Ansicht auf alle relevanten Objektdaten
- Es gibt eine zentrale Informations- und Administrationsschnittstelle



Identität – Meta-Directory

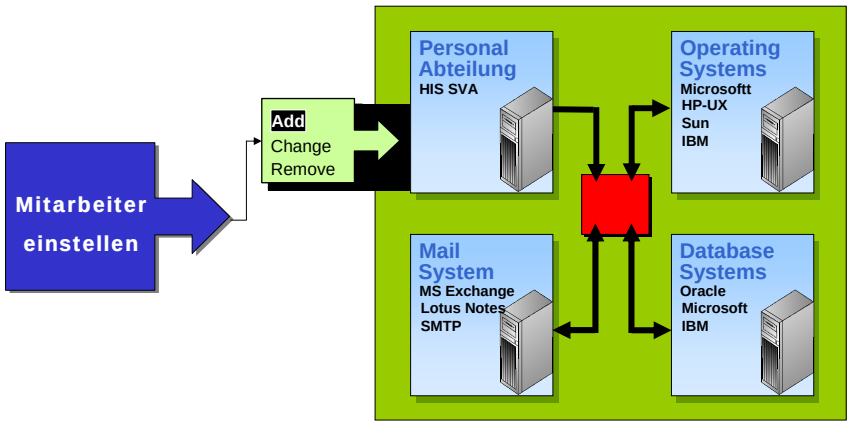
- Eine **Identität** ist die Summe aller Informationen zu einer Person
- Ein **Meta-Directory** :
  - Führt die Identitäts-Informationen zusammen
  - Managed die Identitäts-Informationen
  - Managed Veränderungen an Identitäts-Informationen
  - Managed die Integrität der Identitäts-Informationen



Was ist Provisioning ?

- Provisioning
  - Die Versorgung von Mitarbeitern mit all den Zugriffsberechtigungen zu den IT-Ressourcen, die sie für ihre Tätigkeit benötigen.
- De-Provisioning:
  - Entzug sämtlicher Zugriffsberechtigungen zu den IT-Ressourcen.
- Reverse Provisioning:
  - Den Status der Zugriffsrechte zum aktuellen, oder einem in der Vergangenheit zurückliegenden Zeitpunkt ermitteln.

Provisioning



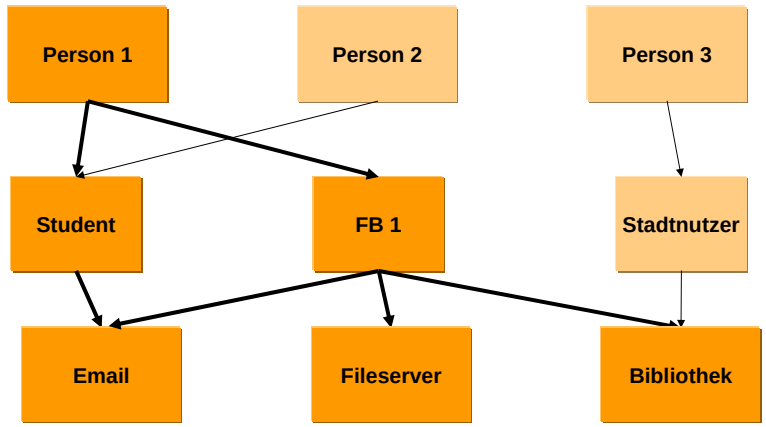
Funktionsumfang Provisioning

- Standard:
  - Anlegen, Verändern und Löschen von Benutzerkonten
- Erweitert:
  - Zentrale Rechtevergabe
    - Z.B. Zuordnung zu Gruppen
  - Tiefergehende Autorisierung von Berechtigungen in den angeschlossenen Systemen
    - Z.B. Schreibrecht auf Datenbanktabellen
  - **Rollen**basiertes Benutzermanagement
  - Workflow-Komoponenten
    - Genehmigungsverfahren, Eskalation, Benachrichtigung
  - Auditing, Reporting
- **Meta-Directories und Provisioning Systeme wachsen zusammen!**

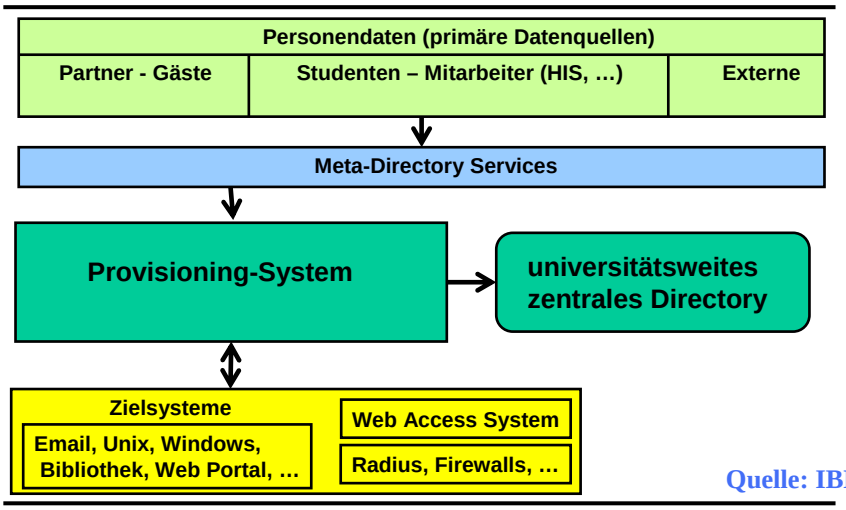
Was ist eine Rolle ?

- Eine Rolle
  - Wird durch einen bestimmten Satz von Attributen beschrieben
    - Funktionsbezogene Attribute: Student, Professor, Gasthörer, …
    - Organisatorische Attribute: Fakultätszugehörigkeit, andere Hochschule, …
  - Ist mit bestimmten Rechten verbunden
    - Die Rechte werden durch das Provisioning in den Zielsystemen eingestellt
  - Kann hierarchisch strukturiert sein
    - Mitarbeiter -> Professor
- Der Einsatz eines Rollenmodells beim Provisioning
  - verringert die Mengenproblematik beim Benutzermanagement
  - Führt zu einem konsistenten Berechtigungskonzept

Zusammenhang Identität – Rolle – Account

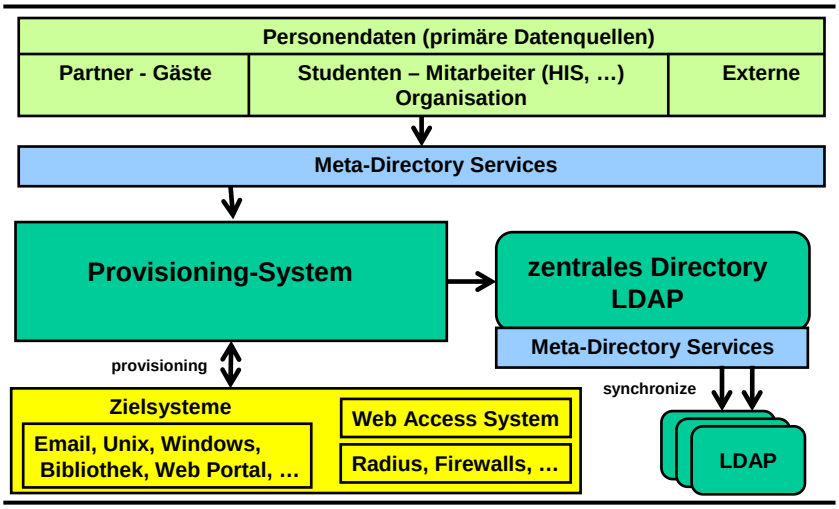


Architektur des Identity Management



Quelle: IBM

Architektur des Identity Management



Gliederung

- Motivation „Identity Management“
- Begriffsklärung
- **Vorgehen in einem Projekt**

Projektschwerpunkt

- Die Ursache für Probleme bei der Verwaltung/Administration von Personenidentitäten sind Prozessprobleme.
  - **Fokus im Projekt auf die Prozesse**
  - Und nicht auf Technik oder Produkte
- Es gibt auf Standards basierende Produkte am Markt.
- Der Aufbau eines Identity Managements ist also **primär ein organisatorisches und juristisches Problem.**
  - Dort liegt auch der Hauptaufwand.

➢ **Identity Management ist nicht „von der Stange“ zu haben, sondern ein sehr individuelles System entsprechend der Prozesse in der Hochschule.**

Projektphasen

- Vorstudie
  - Projektdefinition
    - Motivatoren definieren
    - Anforderungen definieren
    - Kontext definieren
    - Projektteam benennen
  - Analyse
    - Prozesse identifizieren
    - IST-Modellierung der Kernprozesse
    - **Schwachstellenanalyse**
  - Softwareauswahl
    - Marktanalyse
    - Anforderungsliste
    - Produktauswahl
- Hauptprojekt
  - Projektplanung/Projektleitung
  - IST-Analyse
    - Detaillierte Modellierung der Prozesse/Daten
    - **Schwachstellenanalyse**
  - Soll-Planung
    - **Soll-Modellierung** Prozesse/Daten
    - Endgültige Software-Auswahl
  - Implementierung
    - Design Technische Umsetzung
    - Teststellung
    - Technische Implementierung
    - Organisatorische Implementierung

Ansatzpunkte der Schwachstellenanalyse

- Können Verzeichnisse abgeschafft oder konsolidiert werden ?
- Werden Daten verwaltet, die nicht benötigt werden ?
- Wo existieren Mehrfacheingaben von Daten in verschiedenen Systemen ?
- Wo gibt es Medienbrüche ?
- Gibt es ein umständliches Formularwesen (übertrieben, lückenhaft) ?
- Wo sind überflüssige Prozesse ?
- Gibt es unzureichende Bearbeitungs- oder Entscheidungsverantwortung ?

Elemente der Soll-Modellierung

- Anzahl und Beschaffenheit der zu provisionierenden Systeme
- Soll-Zustände der Directories und Prozesse
- Datenflüsse zwischen den Directories
- Rollenbeschreibungen und zugeordnete Standardberechtigungen
- Datenhoheiten
- Datenpflegeprozesse
- Ableitungsregeln für Datenfelder
- Regeln zur Anlage und Löschung (Deaktivierung) von Benutzerkonten
- notwendige Datenbereinigungen

Projektkritische Faktoren

- **Entscheidung und Unterstützung der Hochschulleitung für ein solches Projekt**
- Aktive Beteiligung der Verwaltung
  - Von dort kommen fast alle Primärdaten
  - Zuständig für viele Prozesse im Projektkontext
- Kooperatives Zusammenarbeiten zwischen Verwaltung, Hochschulrechenzentrum, Bibliothek und dezentralen Einheiten
  - Gemeinsame IT-Strategie
  - Möglichst institutionalisiert
- Professionelle hochschulinterne Projektkoordination
- Frühzeitige Beteiligung von Personalräten und Datenschutzbeauftragten

Erfahrungen mit der externen Beratern

- Firma bietet Beratung, Coaching und Implementierung
- Firma moderiert Prozesse als unbeteiligter Partner
- Konflikte lassen sich mit externer Moderation einfacher lösen
- Hochschulen, ihre Struktur und ihre Produkte sind ein ungewohntes Terrain für Firmen
- Firma bringt Erfahrung mit ähnlichen Projekten im kommerziellen Bereich ein
- Projektabsprache muss geübt werden
- Zügiger Projektablauf

Produkte

- Critical Path
- IBM/Tivoli – Access 360
- Microsoft
- Novell DirXML
- Siemens DirX
- Sun - Waveset

Vielen Dank

Identity Management sorgt dafür, dass der richtige Anwender zum richtigen Zeitpunkt die angemessenen Zugriffsrechte erhält.