Identitätsmanagement mit Open-Source-Software

M. Bachmann, Humboldt-Universität zu Berlin

8. Tagung der DFN-Nutzergruppe Hochschulverwaltung 7.-9- Mai 2007

Identitätsmanagement

- Was ist das?
- Wozu brauchen wir das?
- Was haben wir derzeit?
- Anforderungen
- Warum OpenSource?
- geplante Systemarchitektur

Was ist das?

- Identitätsmanagement: technische Verwaltung von Identitäten
- Zusammenführung von Nutzern aus verschiedenen Quellen und Bereitstellung in verschiedenen Endsystemen
- (digitale) Identität: Sammlung von Attributen, z.B. Name, Adresse, Matrikelnummer, Passwort, zugewiesene Rollen

Wozu brauche ich das?

- Authentifizierung und Autorisierung
- Passwortverwaltung und –synchronisierung
- Single Sign On Mechanismen (Shibboleth)
- Identitätszertifizierung mit Hilfe der PKI
- Rollenkonzepte und Berechtigungen
- Verwaltung des Zugriffs auf Ressourcen (Daten, Drucker, WLAN, Kopierer, Zutritt, ...)
-

Was haben wir derzeit?

- ca. 30000 Studierende, ca. 4000 Mitarbeiter (HIS: SOS, SVA)
- zentrale Accountdatenbank (ca. 38000 Einträge)
  - Reservierung von Accountnamen
- LDAP
  - Passworthash, Änderungsdatum
- Active Directory

Was haben wir derzeit?

- über 90 verschiedene IT-Dienste
- von **A**nmeldesystem Berufliche Weiterbildung bis **Z**utrittsystem
- ca. 1/3 zentral vom CMS verwaltet, 2/3 in den Fakultäten, Zentraleinrichtungen und Verwaltung
- steigende Anforderungen der Nutzer und Systembetreuer

Was soll erreicht werden?

- Serviceverbesserung durch einheitlichen Zugriff auf IT-Systeme
- Nutzerspezifische Sicht auf Dienste der HU (Portal)
- Hochschulübergreifende Nutzung der IT-Dienste ermöglichen
- Vereinfachung der Administration

Anforderungen

- Daten müssen aktuell, konsistent, verlässlich und ständig verfügbar sein
- Einbindung in vorhandene IT-Landschaft
- Integrierbar in bestehende Arbeitsabläufe
- Erweiterbar für zukünftige Anforderungen
- Datenschutz und Datensicherheit
- Auditierbarkeit

Anforderungen

- Orientierung an offenen Standards
- Benutzeroberflächen
- skalierbares Rollen- und Rechtekonzept
- unkomplizierter Betrieb
- Hochschulübergreifendes Identitätsmanagement (Föderation)

Warum Open-Source?

- Teil der Kerninfrastruktur
- Bindung an das Produkt eines Herstellers
- Anforderungen der Universität / Lösungen des Herstellers
- Anpassungsmöglichkeiten bei Oberflächen
- Erweiterungen und Weiterentwicklung

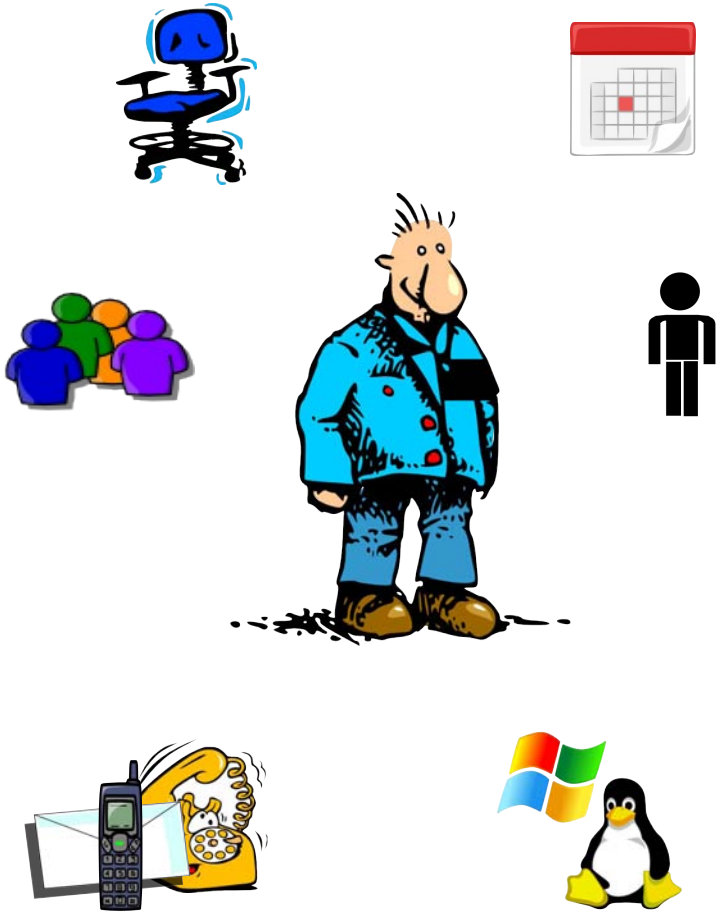
Warum Open-Source?

- konkrete Anforderungen / zukunftssichere Lösung
- Bildung internen Know-How's
- Sicherstellung des Weiterbetriebs
- Kosten

Designprinzipien

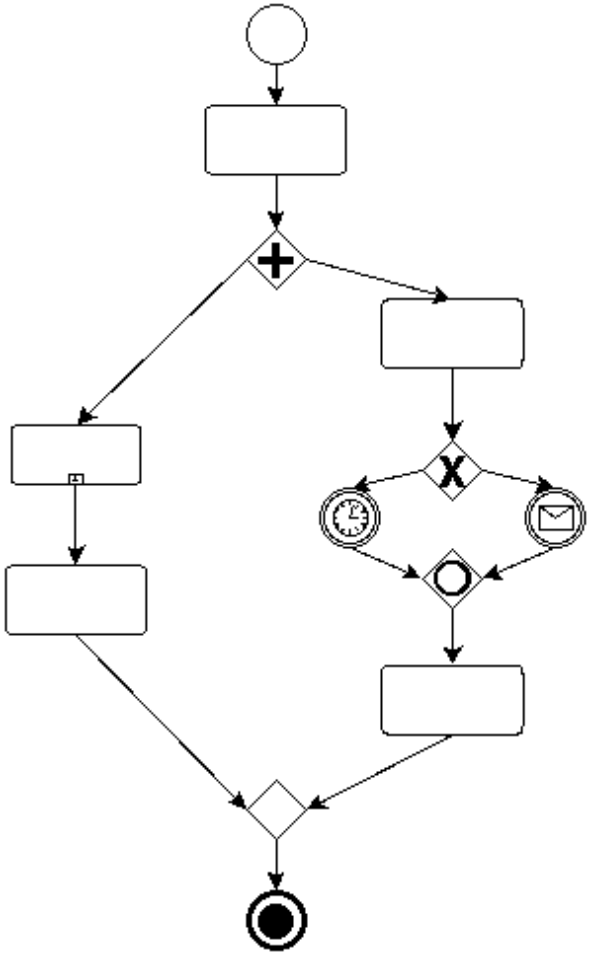
- Identität steht im Zentrum
- dynamische Attribute
- interne Workflow-Engine
- flexible I/O-Konnektoren

Designprinzipien



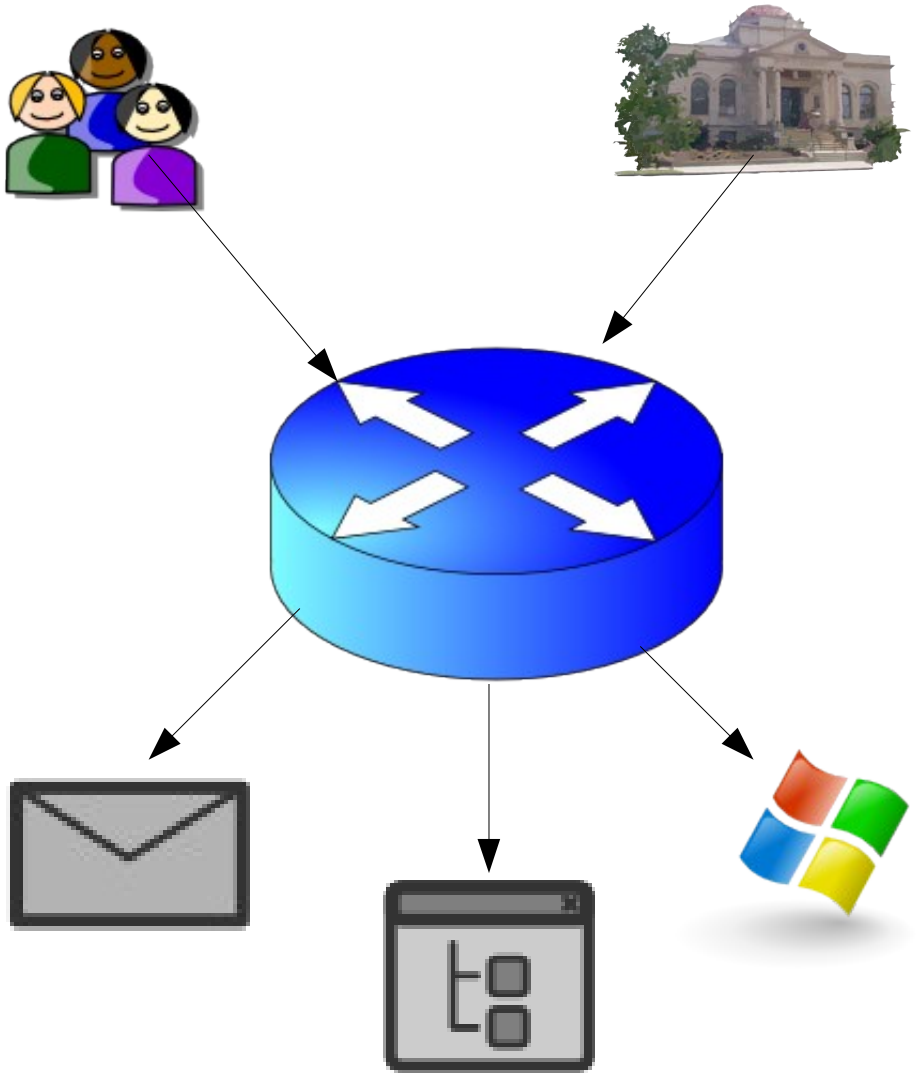
- Identität steht im Zentrum
- dynamische Attribute
- interne Workflow-Engine
- flexible I/O-Konnektoren

Designprinzipien



- Identität steht im Zentrum
- dynamische Attribute
- interne Workflow-Engine
- flexible I/O-Konnektoren

Designprinzipien

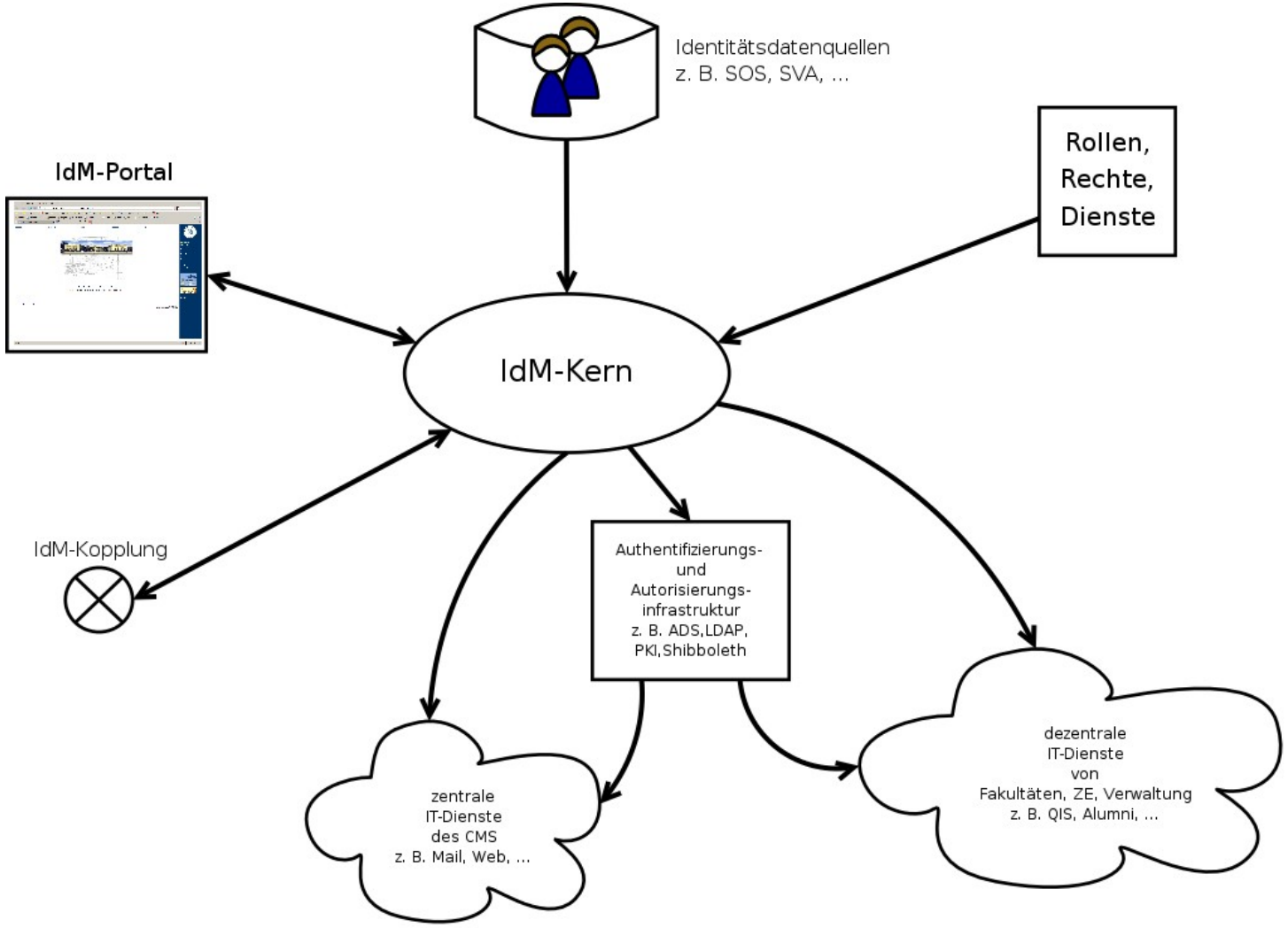


- Identität steht im Zentrum
- dynamische Attribute
- interne Workflow-Engine
- flexible I/O-Konnektoren

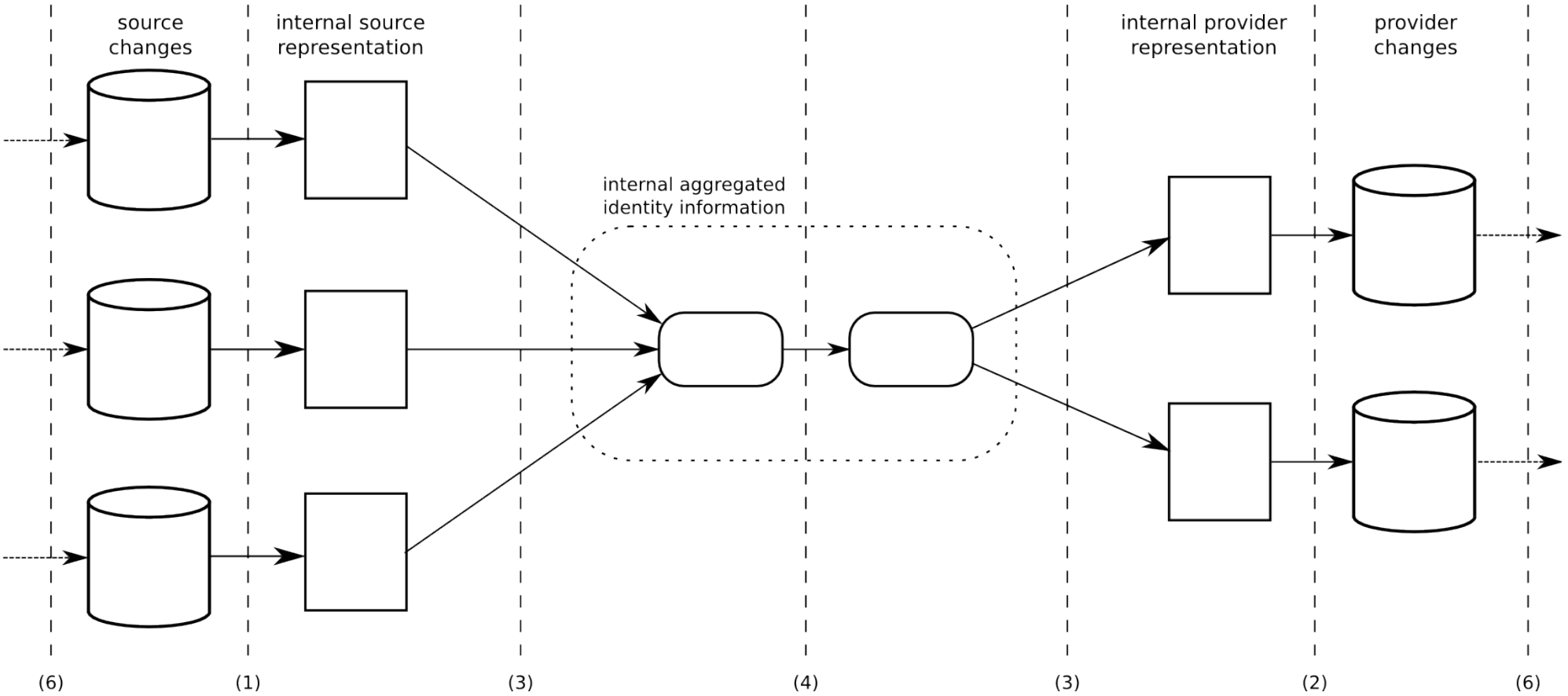
Systemarchitektur

- Java als System-Plattform
- Webservices als Systemschnittstellen
- RDMS als Backend
- Modularer Systemaufbau
- Verwendung von Standard-Komponenten
- Verwendung von Standard-Schnittstellen für Außenanbindungen (z.B. SAML, d.h. Shibboleth)

Prinzipskizze: HU-IAM



Prinzipskizze: IdM-Kern



Projektverlauf

- Haushaltfinianziertes Projekt, 3 Jahre
- 2 Projektstellen + Unterstützung aus CMS
- Januar 2007: Projektbeginn
- Herbst 2007: erste funktionsfähige Version, Konsolidierung der bestehenden Account-DB
- ab 2008: Integration zentraler und dezentraler Dienste, Erstellung von Synchronisationsmodulen

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
Michail Bachmann
m.bachmann@cms.hu-berlin.de