technische universität
dortmund

IT & Medien Centrum
itmc

Erfahrungen mit dem Sun IDM sowie der aktuelle Stand bei der Einführung an der Technischen Universität Dortmund

Jan Gellweiler
LRZ, 03.11.2008

Agenda

- Vorstellung TU Dortmund
- IDM Projekt der TU Dortmund
- Bisherige Erfahrungen

Technische Universität Dortmund auf einen Blick

- Gegründet 1968
- 22.000 Studierende
- 2.200 Mitarbeiter

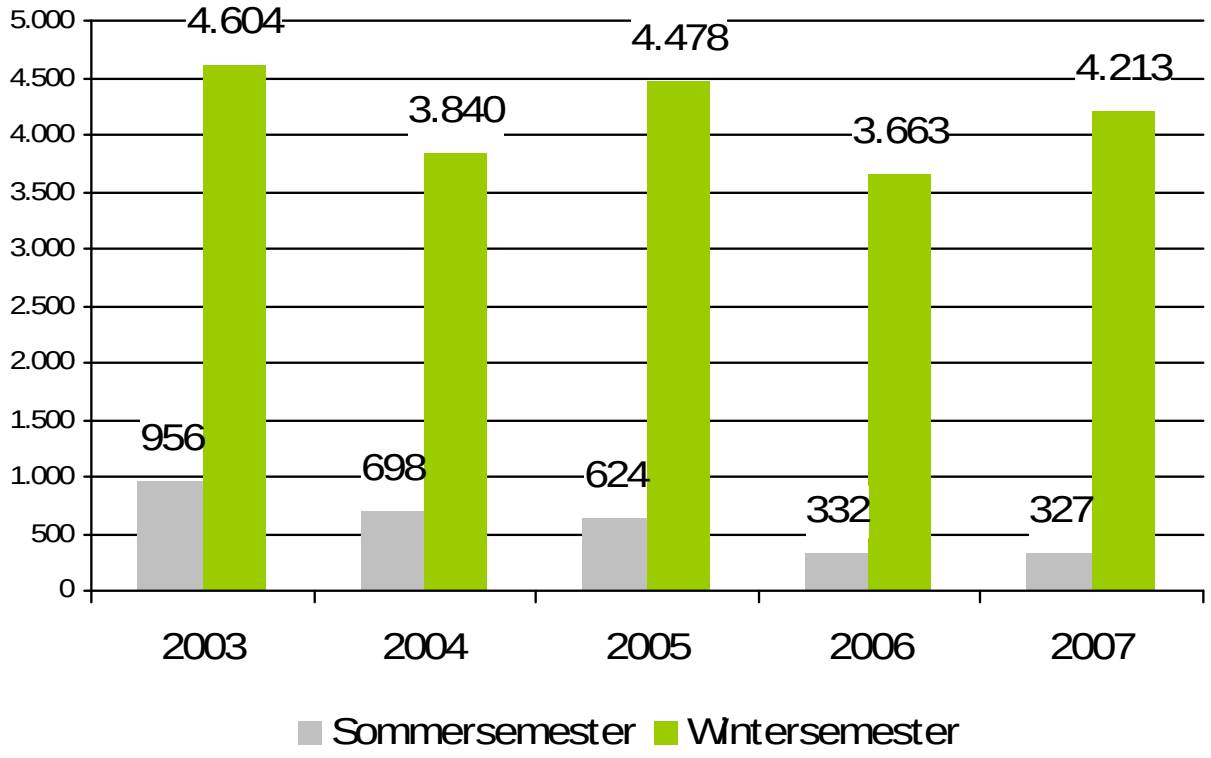
- 16 Fakultäten in den Wissenschaftsbereichen
  - Naturwissenschaften und Mathematik
  - Ingenieurwissenschaften und Informatik
  - Planungs- Bau- und Wirtschaftswissenschaften
  - Geistes-, Kultur-und Sozialwissenschaften

- 220 Mio. € Jahresbudget
- 40 Mio. € Drittmittel p.a.

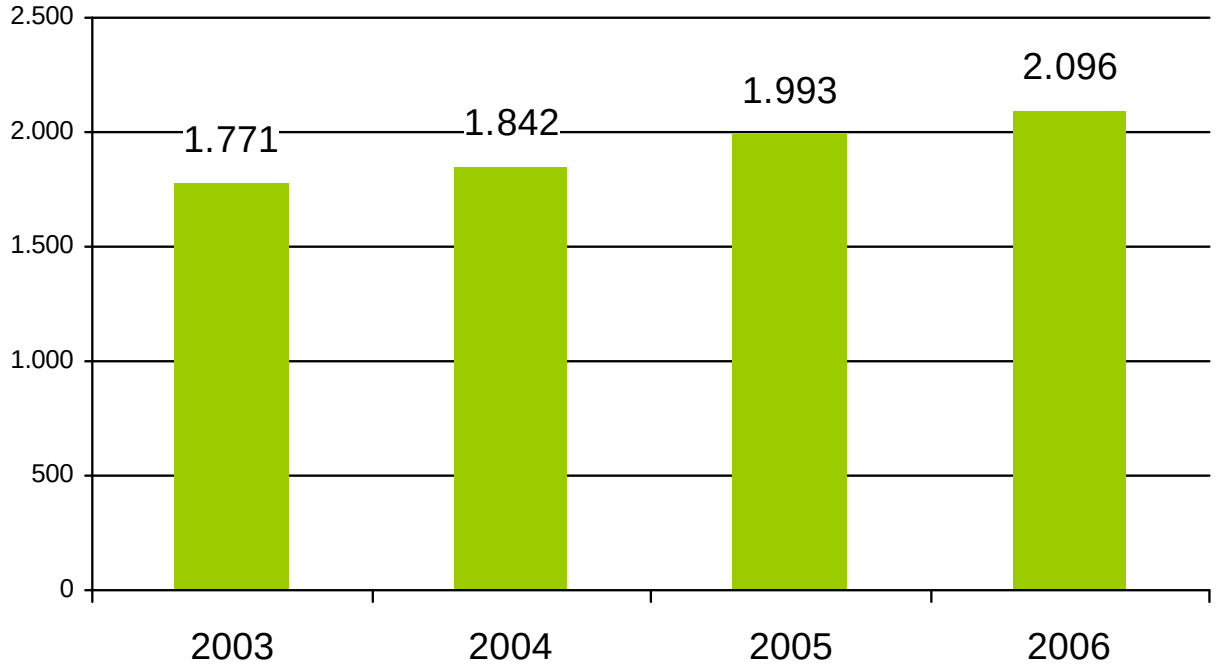
IT & Medien Centrum auf einen Blick

- 2007 aus Hochschulrechenzentrum und Medienzentrum zusammengelegt
- Ganzheitlicher Dienstleister für IT-Aufgaben an der TU Dortmund
- Bereitstellung einer modernen und leistungsfähigen IT-Infrastruktur für die Mitglieder der Universität
- Trägt konzeptionelle und operative Verantwortung für übergreifende elektronische IT und Mediendienste sowie das IT-Sicherheitskonzept
- Einzubeziehen bei der Entwicklung und Durchführung aller größeren IT-Projekte sowie bei der Vorbereitung größerer IT-Beschaffungen
- Ca. 70 Mitarbeiter

Daten: Neu- und Ersteinschreibungen (Kopfzahl)



Daten: Absolventen (ohne Promotionen)



Projektvorgaben

- Rektoratsprojekt
  - Bewilligt für 2 Mitarbeiter für 2 Jahre (Oktober 2007 - September 2009)
- Schaffung der Grundlage für künftige Mehrwertdienste
- IDM soll alle Identitäten, die im Uni-Raum vorkommen können, abdecken (Studierende, Mitarbeiter, Gäste, Externe, Projektpartner)
- Alle wesentlichen ID-tragenden Systeme sollen eingebunden werden (HIS-SOS/POS, HIS-SVA, Universitäts Bibliothek, HRZ IDM in UniMail)
- Flexibler Einsatz und Erweiterungsmöglichkeiten
- Einsatz einer offenen, möglichst standard-basierten Lösung
- Keine weitreichenden Verpflichtungen zu möglichen künftigen Lizenzkosten
- Berücksichtigung der UAMR

- Projektstart: Mai 2008
- Projektende: September 2009
- Aktuelles Projektteam: 1 MA (vollzeit), 1 SHK (12 Stunden/ Woche)

Ausgangssituation

- Der Dienst „UniMail“ ist zu einem Quasi-IDM ausgebaut
  - SOS- uns SVA-Daten sind in UniMail zusammengeführt und konsolidiert
  - Ergebnisse der Synchronisation werden nicht an SOS oder SVA zurückgegeben
  - UniMail provisioniert Drittsysteme (z.B. Radius, LSF-Authentifizierung)

- Hauptquellen für Identitäten sind:
  - HIS SOS für Studierendendaten
  - HIS SVA für Personaldaten
  - Bibliothek
  - UniMail

- Daneben gibt es noch eine Vielzahl weiterer Identitäts-tragender Systeme, z.B.:
  - Telefonanlage,
  - ZfW-Datenbank,
  - Domänen-Kontroller

Grobplanung

- Arbeitspaket 1: Einarbeitung Sun IDM / Machbarkeitsstudie anhand AM-Provisionierung (Mai – August 2008)
- Arbeitspaket 2: Analyse der wesentlichen Quellsysteme: Datenstrukturen, Rollenmodelle, Workflows (September – Oktober 2008)
- Arbeitspaket 3: Konsolidierung der Identitäten im IDM (bis Ende Januar 2009)
- Arbeitspaket 4: AM-Anbindung (Februar 2009)
- Arbeitspaket 5: Anbindung weiterer Quellsysteme (1. - 2. Quartal 2009)
- Arbeitspaket 6: Anbindung weiterer Zielsysteme (1.-3. Quartal 2009)
- Arbeitspaket 7: IDM Self-Service (2. Quartal 2009)

Ergebnisse Phase 1 & 2

- Sun IDM als Identity Management für die TU Dortmund ausgewählt
- Für globale Identitäten relevante Attribute in den Quellsystemen identifiziert
- Workflows, die auf diesen Attributen arbeiten, erfasst

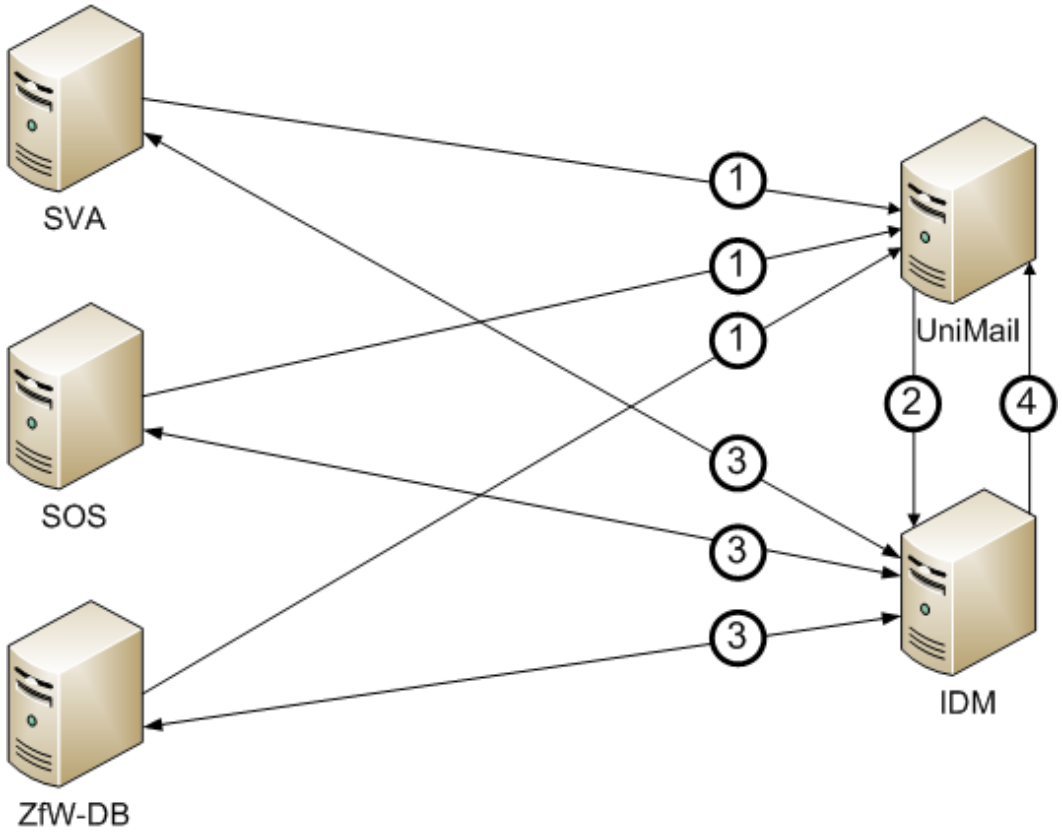
Aktueller Stand

- Entwicklungs- und Staging-Umgebung mit allen notwendigen Ressourcen (SOS, SVA, UniMail) aufgesetzt => erste Erfahrungen bzgl. der Datenqualität in den Quellsystemen können gesammelt werden
- Konzepte für Seeding und spätere Synchronisation der Datenbanken mit dem IDM werden entwickelt
- Geplantes IDM-System wird mit dem Datenschutzbeauftragten, dem Personalrat und den beteiligten Dezernaten diskutiert
- Grobkonzept für die Produktiv-Server

IDM Rollen an der TU Dortmund

- Start mit einem sehr eingeschränkten Rollenmodell
- Grundsätzliche Aufteilung in Studierende und MitarbeiterInnen
- Bei den Studierenden zunächst nur Rollen vom Typ „Studierender im Fachbereich XY“
  - Feingranularere Rollen hängen von den in SOS gepflegten Attributen ab
- Bei den MitarbeiterInnen erfolgt die grundsätzliche Gliederung nicht über Rollen sondern über die Organisationsstruktur (Datenquelle noch nicht geklärt, evtl. HIS-FSV oder Telefonbuch)
  - Rollen für z.B. Dezernenten oder Lehrstuhlinhaber werden bei Bedarf und nach Möglichkeit (Datenqualität!) aus SVA-Daten erzeugt

Seeding des IDM



Provisionierung von Ressourcen

- Drei grundsätzliche Varianten möglich:
  1. Das IDM provisioniert grundsätzlich alle in Frage kommenden Identitäten in die angeschlossene Ressource (z.B. Access Management)
  2. Vor der Provisionierung muss eine Registrierung durch den User erfolgen (z.B. DokuWiki der AStA)
  3. Direkte Ressourcenzuweisung durch Ressourcenverantwortlichen

- Für die Varianten 1 und 2 sind zusätzliche Approving-Schritte möglich.

- Bei den Studierenden soll die Provisionierung in ein System im Regelfall entsprechend der zweiten Variante erfolgen.

Erfahrungen

- Installation und erste Test verlaufen einfach und problemlos
- Danach steigt die Lernkurve ziemlich steil an
  - Erste eigene Versuche dauert viel länger als geplant
  - Schon für kleinere Aufgaben ist ein breites Verständnis des IDM notwendig
  - Hohe Einstiegsanforderungen
- Teilnahme an den Kursen Deployment Fundamentals 1 & 2 ist dringend zu empfehlen
- Java, J2EE, SQL, XML, LDAP, AD, .. => Kein Einsatzgebiet für reine Java-Programmierer
- Netbeans Plug-In besser als Eclipse-Plugin
- Kleinere Probleme mit SLES 10

Erfahrungen mit der AM-Provisionierung

- Stabiler Betrieb unter VMware
- Problemloses Backup & Recovery
  - IDM lässt sich jederzeit aus der Entwicklungsumgebung neu deployen
  - Backup & Recovery des DataStores erfolgt mit den üblichen DB-Werkzeugen
- Vollständige Reconciliation dauert für 25.000 Datensätze ca. 3,5 h
  - Optimierung aufgrund unseres Scenarios nicht möglich

Pro

- Flexibles, erweiterbares Framework
- Standardisierte Schnittstellen
- Weitgehend agentenlose
  => keine bis wenige Modifikationen an den vorhandenen Systemen
- Reporting, Auditing
- Resource Adapter für alle relevanten Systeme
- Skalierbarkeit

Contra

- Open Source Version steht noch nicht zur Verfügung
- Hohe Einstiegshürde
- Proprietäre Prozessmodellierung
- OpenLDAP Resource Adapter muss noch implementiert werden
- WS Resource Adapter muss noch implementiert werden

Vielen Dank!

- Kontakt:
  - jan.gellweiler@tu-dortmund.de

- Weitere Informationen:
  - http://www.itmc.uni-dortmund.de/de/projekte/unidoidm/index.html