Gaedke / Borgeest (Hrsg.)

Integriertes Informations-management an Hochschulen

Quo vadis Universität 2.0?

Tagungsband zum Workshop IIM 2007
Karlsruhe, 01.03.2007

universitätsverlag karlsruhe

Gaedke / Borgeest (Hrsg.)

Integriertes Informationsmanagement an Hochschulen

Quo vadis Universität 2.0?

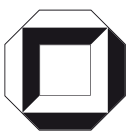
Tagungsband zum Workshop IIM 2007, Karlsruhe, 01.03.2007

Integriertes Informations-management an Hochschulen

Quo vadis Universität 2.0?

Tagungsband zum Workshop IIM 2007
Karlsruhe, 01.03.2007

Martin Gaedke
Rolf Borgeest
(Hrsg.)



universitätsverlag karlsruhe

Impressum

Universitätsverlag Karlsruhe
c/o Universitätsbibliothek
Straße am Forum 2
D-76131 Karlsruhe
www.uvka.de

Universitätsverlag Karlsruhe 2007
Print on Demand

ISBN: 978-3-86644-112-5

Vorwort

Stellt integriertes Informationsmanagement an einer Hochschule zukünftig die zentrale Schlüsselfunktion dar? Die Chancen durch integriertes Informationsmanagement (IIM) und der damit verbundene Paradigmenwechsel hin zur dienstleistungsorientierten Hochschule sind in vielerlei Hinsicht bestechend. Sie versprechen insbesondere eine Steigerung der Effektivität, Effizienz und Qualität bei der Umsetzung der Ziele einer Hochschule im globalisierten Wissensmarkt.

Die Schwierigkeiten bei der Realisierung eines integrierten Informationsmanagements sind allerdings ebenso vielfältig, wie die damit verbundenen Chancen. Sie sind geprägt von organisatorischen und informatisch/technischen Fragestellungen. Dabei erstreckt sich die Problematik auf den ersten Blick nur auf eine Vielzahl heterogener Datenquellen und -modelle sowie die Umsetzung organisationsübergreifender Prozesse und Transaktionen. Viele weitere Anforderungen und Problemstellungen, etwa im Rahmen der Gesetzgebung zum Datenschutz, des Identitätsmanagements und der Schnittstellen für spezielle Nutzungsszenarien, offenbaren sich erst durch Erfahrungen in realen Projekten.

Der Workshop findet dieses Jahr in Karlsruhe statt und nutzt zugleich das renommierte Forum der Konferenz Wirtschaftsinformatik 2007.

Der erste Workshop Integriertes Informationsmanagement an Hochschulen (IIM 2007) findet dieses Jahr in Karlsruhe im Rahmen der Konferenz Wirtschaftsinformatik 2007 statt. IIM 2007 versteht sich als Forum, um den aktuellen Stand der Technik und die damit verbundenen Erfahrungen in der Realisierung von integriertem Informationsmanagement vorzustellen. Das Leitthema „Quo Vadis Universität 2.0?“ diente dazu aktuelle Schwerpunkte in den Entwicklungen der Hochschulen zu identifizieren.

Trotz einer sehr kurzen Einreichungsphase von lediglich drei Wochen erhielten wir zahlreiche Beiträge, von denen wir letztendlich neun ausgewählt haben. Sie zeigen die zentralen Schwerpunkte des IIM in den Hochschulen auf und begegnen diesen Themen mit unterschiedlichen Ansätzen.

Ein Themenbereich sind Aspekte der grundlegenden Ordnung der IT an Hochschulen, ausgehend von einem eher technischen Ansatz zur Administration von Rechner Pools über die Anlagen von Softwarelandkarten als Mittel der Steuerung und Planung komplexer Softwarelandschaften bis zur einer Arbeit, die ganz grundsätzlich die Organisationsformen von Universitäten untersucht um daraus Anforderungen für das Integrierte Informationsmanagement

an Hochschulen abzuleiten. Ein weiterer Schwerpunkt ist das Identitätsmanagement – ein Trend, der auch in den IIM Szenarien der Wirtschaft derzeit viel diskutiert wird. Mit drei Beiträgen möchten wir dieses Thema daher beleuchten. Sie zeigen typische Problemstellungen und Lösungsansätze im universitären und intra-universitären Umfeld. Verschiedene Ansätze zur Integration von E-Learning in die Softwareumgebungen und Abläufe der Hochschulen bilden den letzen Themenkomplex des Workshops.

Darüber hinaus wird das Workshop-Programm durch einen außergewöhnlichen Sprecher abgerundet. John Gray behandelt das Thema IIM aus Sicht der Maturität einer Einrichtung und spricht über die „Innovative Universities Initiative“ von Microsoft.

Wir möchten uns bei allen bedanken, die zum Erfolg des IIM 2007 Workshops beigetragen haben. Besonderer Dank gilt hierbei insbesondere dem Organisationskomitee und Programmkomitee und vielen weiteren Helfern und Unterstützern. Ein besonderes Dankeschön richten wir auch an Brigitte Maier und Sabine Mehl vom Universitätsverlag Karlsruhe für ihre Unterstützung und Geduld bei der Herstellung der Druckversion. Allen Mitgliedern des Programmkomitees und den zusätzlichen Gutachtern gilt unser besonderer Dank für ihren Einsatz zwischen den Jahren; durch ihre Sorgfalt, Expertise und Gutachten gelang es uns ein interessantes und wegweisendes Programm zusammenzustellen.

Der größte Dank gebührt letztendlich den Autoren, die ihre Beiträge auf diesen Workshop eingereicht haben. Ihre Arbeit ist das Herz der IIM-Workshopreihe und setzt hoffentlich die Akzente, die wir für ein erfolgreiches integriertes Informationsmanagement an den Hochschulen benötigen. Danke!

Wir hoffen, dass Ihnen die Beiträge gefallen und Sie wertvolle Impulse für Ihre Arbeit, Forschung und Lehre erhalten.

Karlsruhe und München, im Januar 2007 Martin Gaedke und Rolf Borgeest

Organisation

Organisationskomitee

Prof. Dr. Sebastian Abeck, Universität Karlsruhe (TH)

Prof. Dr. Arndt Bode, TU München

Dr. Rolf Borgeest, TU München, Co-Chair

Dr.-Ing. Martin Gaedke, Universität Karlsruhe (TH), Co-Chair

Prof. Dr. Hannes Hartenstein, Universität Karlsruhe (TH)

Prof. Dr. Wilfried Juling, Universität Karlsruhe (TH)

Dipl.-Inform. Axel Maurer, Universität Karlsruhe (TH)

Prof. Dr. Andreas Oberweis, Universität Karlsruhe (TH)

Prof. Dr. Hartmut Schmeck, Universität Karlsruhe (TH)

Programmkomitee

Prof. Dr. Sebastian Abeck, Universität Karlsruhe (TH)

Prof. Dr. Hans-Jürgen Appelrath, Universität Oldenburg

Prof. Dr. Christian H. Bischof, RWTH Aachen

Prof. Dr. Arndt Bode, TU München (TUM)

Dr. Rolf Borgeest, TU München (TUM), Co-Chair

Prof. Dr. Walter Brenner, Universität St. Gallen

Dr. Andreas Degkwitz, TU Cottbus

Dr.-Ing. Martin Gaedke, Universität Karlsruhe (TH), Co-Chair

Dr. Stefan Gradmann, Universität Hamburg

Prof. Dr. Hans Peter Großmann, Universität Ulm

Prof. Dr. Hannes Hartenstein, Universität Karlsruhe (TH)

Dr. Wilhelm Held, Universität Münster

Prof. Dr. Lutz Heuser, SAP AG

Prof. Dr. Wilfried Juling, Universität Karlsruhe (TH)

Prof. Dr. Reinhard Keil, Universität Paderborn

Prof. Dr. Hartmut Koke, GWDG

Dipl.-Inform. Axel Maurer, Universität Karlsruhe (TH)

Prof. Dr. Andreas Oberweis, Universität Karlsruhe (TH)

Dr. Sabine Rathmayer,TU München

Prof. Dr. Peter Schirmbacher, Humboldt-Universität Berlin

Prof. Dr. Hartmut Schmeck, Universität Karlsruhe (TH)

Prof. Dr. Gerhard Schneider, Universität Freiburg

Prof. Dr. Thomas Tolxdorff, Charité Berlin

Prof. Dr. Klaus Turowski, Universität Augsburg

Prof. Dr. Theo Ungerer, Universität Augsburg

Zusätzliche Gutachter

Dr. Oliver Christ, SAP AG

Dipl.-Inform. Johannes Meinecke, Universität Karlsruhe (TH)

Dr. Philipp Rohde, RWTH Aachen

Dr. Orestis Terzidis, SAP AG

Inhaltsverzeichnis

Teil I

Aspekte grundlegender Ordnung von IT an Hochschulen

LDAP Site Management

Web/LDAP-basiertes Framework zur Administration von IP Netzen und Rechnerpools

Prof. Dr. Gerhard Schneider, Dirk von Suchodoletz, Tarik Gasmi

Institut für Informatik
Lehrstuhl für Kommunikationssysteme
Universität Freiburg
79104 Freiburg
{Gerhard.Schneider, Dirk.von.Suchodoletz, Tarik.Gasmi}@uni-freiburg.de

Abstract

Gerade in wissensintensiven Bereichen, wie Universitäten und Forschungseinrichtungen, hat die Zahl der computergestützten Arbeitsplätze und netzwerkbasierten Dienste rasant zugenommen. Gleichzeitig werden Datennetze immer breitbandiger und erlauben eine ganze Reihe neuer Betriebsszenarien. So könnten aus Pool- und Lehrmaschinen nachts Numbercrunsher werden, wenn sich die Geräte zentralisiert verwalteten und steuern lassen. Ziel ist die Nutzung von Remote-Boot-Services, um von einer festen Software-Installation hin zu On-Demand-Konfiguration und Betrieb zu kommen.

Um den Verwaltungsaufwand und Betriebskosten in einem vernünftigen Rahmen zu halten, muss die Administration in zunehmenden Maße auf Zentralisierung und Automatisierung setzen. Ein verteiltes, autonomes Managements der Ressourcen kann wichtige Informationen und Aufgaben wieder zusammenfassen, ohne dabei einerseits die dezentralen Einheiten zu entmündigen und andererseits die zentrale Administration zu überfordern.

Der folgende Beitrag beschreibt ein Management Framework zur Verwaltung von IP-Netzen und Rechnerpools im Rahmen größerer Umgebungen, etwa einer Universität. Das vorgestellte Framework ermöglicht eine lokale und autonome Administration der Basisdienste DNS und DHCP. Zusätzlich unterstützt es eine verteilte Verwaltung von PXE-Bootkonfigurationen für eine Reihe angebotener Remote Boot Services.

1 Motivation

Die Verwaltung einer zunehmenden Zahl von Rechnern, Diensten, und Netzwerk-Devices, hat die Administration heterogener, dezentraler Client/Server-Infrastrukturen in den letzten Jahren vor neue Herausforderungen gestellt. Schon in mittleren Organisationen und Unternehmen sind tausende von vernetzten Clients keine Seltenheit mehr, und ein umfassendes Client- und Service-Management ist von Hand nicht mehr effizient zu bewältigen. Der Betrieb und die Verfügbarkeit einer hohen Zahl von Rechnern und Diensten ist aufrecht zu erhalten und umfasst neben Installation und Wartung (*ITIL Configuration* und *Change* Management[1]), die Überwachung des Betriebs (Monitoring) und seine schnellstmögliche Wiederherstellung bei Ausfällen (*ITIL Incident* und *Problem* Management). Die Durchführung dieser Aufgaben durch eine Betreuung der einzelnen Geräte vor Ort ist nur unter hohem Arbeits- und Zeitaufwand, oder Einsatz von mehr Personal möglich. Den sprichwörtlichen „Turnschuh-Administrator mit Installations-CD“ kann sich keine Organisation selbst in mittleren IT-Umgebungen mehr leisten.

Informationen zu Menschen und Maschinen sind in solchen Umgebungen unabdingbar: Das zentrale Netzwerkmanagement möchte sehr schnell erfahren können, welche Maschinen wo in Betrieb sind und welche Personen in den einzelnen Bereichen die Verantwortung tragen. Traditionelle Konzepte benutzen dafür oft ein Nadelöhr: Der Anschluss neuer Maschinen und damit Ressourcen, wie IP-Adressen und Rechnernamen werden zentral beantragt und von einem Administrator direkt realisiert. Das bedeutet für den Administrator üblicherweise einiges an Aufwand und den Beantragenden einiges an Geduld. Das führt oft dazu, dass solche Prozesse ungenau ausgeführt oder im schlimmeren Fall einfach umgangen werden.

Die Entwicklung immer leistungsfähigerer Netzwerkinfrastrukturen erlaubt es Rechenzentren inzwischen immer stärker, zentralisierte Dienste an ihre Kunden zu bringen. Diskless Remote Boot, verschiedene Betriebssystem-Installationen oder Tools zum Hardware-Test vereinfachen Workflows erheblich. In dem Moment wo lokale Installation nicht mehr notwendig sind, lassen sich Geräte viel einfacher austauschen und unterschiedliche Betriebsarten auf einem Rechner erlauben. Lehrpools müssen nicht mehr für jeden Kurs aufwändig reinstalliert werden und lassen sich zudem in Randzeiten alternativ beispielsweise als Rechencluster wiederverwenden. Sehr viele Rechner können auf diese Weise aus einer einzigen oder wenigen und damit

[1] Die IT Infrastructure Library beschreibt IT Prozesse ganzheitlich und mit standardisierten Begriffen. In größeren IT-Infrastrukturen werden auf dieser Grundlage definierte IT-Prozesse eingesetzt, um beispielsweise Administrationsprozesse zu konzipieren, organisieren und zu koordinieren.

einfacher zu verwaltenden Installationen heraus betrieben werden. Vorteile ergeben sich auch für Arbeitsplatz-Maschinen von Mitarbeitern: In dem Augenblick wo sich jede Maschine beim Start erst einmal in der Zentrale „meldet“, kann diese bei Bedarf gut in den Startvorgang eingreifen und damit eine Reihe von Services, wie den Test der Maschine oder Installation von Betriebssystemen und Software ohne Vor-Ort-Administrator anbieten. Um genannten Ziele zu verwirklichen bedarf es neuer Herangehensweisen.

1.1 Neue Administrationskonzepte

In zahlreichen Verwaltungskonzepten arbeiten Automatisierung und Zentralisierung Hand in Hand. Die zentrale Speicherung von Daten, auf die einzelne Administrationsprozesse zugreifen, etwa Konfigurationsdaten von Diensten, bildet dabei die Grundlage. In vernetzten Umgebungen lassen sich dann mittels LAN-basierter Verwaltungswerkzeuge, Arbeiten von jedem beliebigen Rechner zentral durchführen. Zudem lassen sich Daten und Zugriff auf diese Weise einfacher kontrollieren und Administrationsabläufe zentral steuern. Damit schafft man zudem die Basis weitere Automatisierung von Administrationsprozessen zu erreichen.

1.1.1 Verteiltes und autonomes Management

Eine wichtige Möglichkeit den Verwaltungsaufwand der Administratoren zentraler Dienste zu reduzieren, besteht darin, bestimmte Teilaufgaben der Gesamtadministration und dafür benötigte Kompetenzen an andere zu delegieren.
Gerade zentrale Dienste einer Organisation, wie DNS, aber auch lokalere Dienste, etwa DHCP bieten sich dazu an. Ihre Konfigurationsdaten bestehen zu erheblichen Teilen aus lokal, etwa in einzelnen Abteilungen, vorliegenden Daten, klassischerweise Rechnernamen, IP-Konfigurationen und MAC Adressen. Diese Informationen können direkt, autonom von den lokalen Administratoren verwaltet und durch automatisierte Prozesse des Verwaltungssystems in die zentrale Konfiguration des Dienstes eingebunden werden, d.h. eine zentrale Administration wird in sich anbietenden Bereichen *re-dezentralisiert*. Die zentrale Speicherung aller Konfigurationsdaten erlaubt, durch geeignete Organisation bzw. Partitionierung der Daten, sowie mittels Access Control Mechanismen einen geregelten Zugriff auf Informationen. Durch Zuweisung entsprechender Zugriffsrechte auf definierte Daten an bestimmte Personen, kann dann die Delegation von administrativen Kompetenzen in einem gesteuerten Rahmen erfolgen.
Verwaltungssysteme zur Administration größerer IT-Umgebungen integrieren inzwischen weitgehend die angesprochenen Konzepte. Insbesondere zwei Lösungen dienten beim Entwurf

des Frameworks als Inspirationsquellen: *MS Active Directory* bietet u.a. ein umfassendes Client- und Service Management [Micr03],[2] das webbasierte Netzwerk-Registrierungssystem *NetReg* der Carnegie Mellon University, als Beispiel einer verteilten DNS und DHCP Verwaltung [CMU06].

2 Systemarchitektur und verwaltete Dienste

Kernstück des Frameworks ist ein LDAP Verzeichnis (Abb.1), welches einerseits der zentralen Speicherung aller Konfigurationdaten (Hostnamen, Domainnamen, IP-Adressen), Systemdaten und Benutzerdaten dient. Andererseits bildet es durch entsprechende Organisation der Daten hierarchische Verwaltungsstrukturen ab. Es dient auf diese Weise der Realisierung der vorgesehenen Delegationsmechanismen über ein rollenbasiertes Zugriffsmodell.

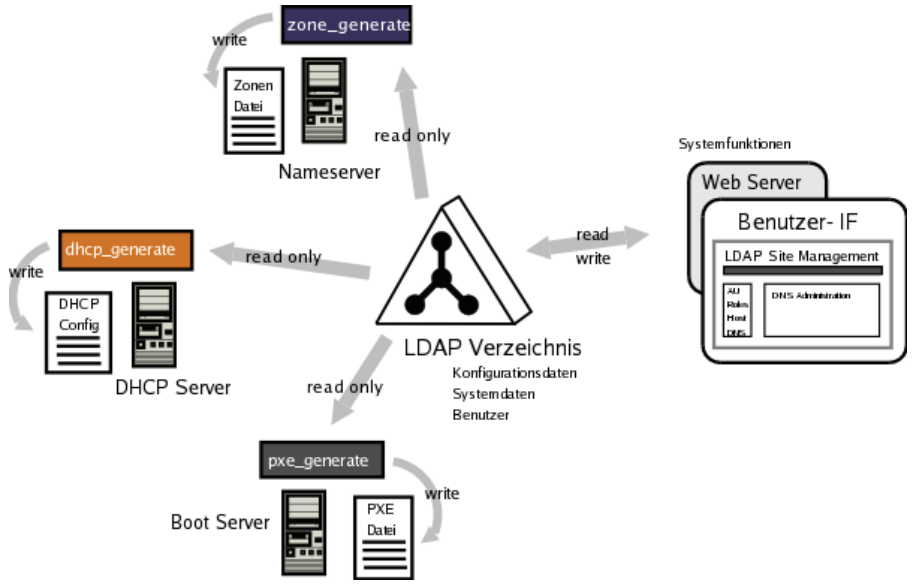


Abb. 1: Web/LDAP-basiertes Management Framework (Übersicht mit zentralen Komponenten Administrationsinterface, Datenbank und gesteuerte Dienste)

Das Web-basierte Benutzer-Interface bietet eine authentifizierte und benutzerfreundliche Administrationsumgebung, in welcher Verwaltungsaufgaben dezentral vorgenommen werden können. Dazu implementiert es Funktionen für alle vorgesehenen Verwaltungsprozesse und kontrolliert den Daten-Input. Ferner steuert es Aufbau und Organisation der Verzeichnisstruktur

[2] Das *eDirectory* von Novell bietet ein Lösung in ähnlichem Umfang. Wie Active Directory basiert es auf einer zentralen Speicherung aller benötigten Daten in einem LDAP Verzeichnis.

durch entsprechende Funktionen, d.h. Anordnung, Benennung von Objekten, und setzt Referenzierungen zwischen verteilten, aber logisch zusammengehörenden Datensätzen, etwa die Konfigurationsdaten eines spezifischen Dienstes. Weitere Funktionen sorgen bei Änderungen bestimmter an anderer Stelle im Verzeichnis referenzierter Daten für die Wahrung referentieller Abhängigkeiten und letztlich für die Integrität des gesamten Datenbestandes.
Die Konfiguration der Dienste erfolgt automatisiert und skriptgesteuert durch Konfigurations-Tools. Diese generieren asynchron, im Augenblick der Ausführung durch den Dienst-Administrator für den jeweiligen Dienst spezifische Konfigurationsdateien aus den verteilten und dezentral verwalteten Daten.

2.1 Verwaltung von Rechnerpools und der Basisdienste DHCP, DNS

Die Einbindung von Rechnern in die IP-Infrastruktur über die Basisdienste DNS und DHCP kann im Framework von zentralen Dienst-Administratoren an Vor-Ort-Administratoren der betreffenden Maschinen delegiert werden. Diese dürfen die Konfigurationsdaten ihrer Rechner wie Hostnamen, IP-Adressen in Eigenverantwortung verwalten und legen dazu im ihrem Verwaltungsbereich im LDAP Verzeichnis eigene Rechnerobjekte zur Speicherung der Informationen an. Der Weg über die zentrale Instanz bei Änderungen in diesen Daten, etwa von Rechnernamen (DNS) bzw. Netzwerkkarten (MAC Adresse, DHCP) oder bei Neuanschaffungen, erübrigt sich. Änderungen werden bei der nächsten Generierung der Konfigurationsdateien automatisch in die Dienstkonfiguration übernommen.
Durch das Framework kann die Administration zentraler DNS Dienste im Bereich der DNS Zonenverwaltung dezentralisiert werden, indem DNS Namenseinträge und ihre Resource Records verteilt und autonom verwaltet werden. Ferner können in einer Organisation auf Subnetzbasis dezentral betriebene DHCP Dienste, weiter zentralisiert und ihre Zahl reduziert werden. Lokale Administratoren verwalten das Netzwerk-Setup ihrer Rechner über entsprechende DHCP Optionen weiterhin autonom. Gleichzeitig bleibt die zentrale Kontrolle des Dienstes, u.a. Globale Optionen, in der Hand weniger Dienstverwalter. So ließen sich potentielle Fehler durch falsche Konfiguration lokal betriebener DHCP Dienste, die jedoch zu organisationsweiten Beeinträchtigungen des Netzwerkbetriebs führen können, etwa die fehlerhafte Vergabe bereits an anderer Stelle verwendeter IP-Adressen, reduzieren.

2.2 Verteilte Administration von Remote Boot Services

Remote Boot Services (RBS) bieten Client-Rechnern Betriebsressourcen, wie beispielsweise Betriebssystem, Software, Konfigurationen und Dateisystem, zentral über ein Netzwerk an, so dass diese beim Start eingebunden werden können. Das Bootkonzept definiert, welche Ressourcen zur Realisierung eines bestimmten Betriebskonzeptes beim Bootvorgang in welcher Kombination, von welchen Quellen und eingesetzten Serverdiensten eingebunden werden. Betriebskonzepte variieren in der anvisierten Funktionalität der Clients und in der Aufteilung von Rechenarbeit und Daten zwischen Client und Server im Betrieb.

2.2.1 Initiales Basis-Bootkonzept (PXE-DHCP-TFTP)

Meist kommt dabei das gleiche Bootkonzept zum tragen, welches den anfangs „nackten“ Client mit einer grundlegenden IP-Konfiguration und einer initialen Bootdatei versorgt, auf welcher alle weiteren Prozesse des Remote-Bootvorgangs zur Umsetzung verschiedenster Betriebskonzepte aufbauen. Dieses Basis-Bootkonzept wird durch Kombination der Dienste PXE,[3] DHCP und TFTP[4] realisiert. Anschließend lädt der Client die Bootdatei per TFTP vom Bootserver und bezieht dann erneut per TFTP die zum Client passende PXE-Bootkonfiguration, oder eine Default-Konfiguration, wenn keine speziellen Festlegungen getroffen wurden. Diese PXE-Konfigurationsdatei bestimmt den weiteren Verlauf des Bootprozesses und enthält Informationen zu den einzubindenden Betriebsressourcen oder komplette Submenüs.

[3] PXE (*Preboot eXecution Environment*) ist ein weit verbreiteter Standard der Firma Intel. Die PXE Software initialisiert durch entsprechende Boot-Einstellungen im BIOS, den Bootvorgang über das Netzwerk und bezieht vom DHCP Server Netzwerk-Setup und Informationen zur Quelle der initialen Bootdatei. Eine Open Source Lösung bietet das freie Boot-ROM-Porjekt Etherboot/gPXE [PXE06].

[4] DHCP Optionen *filename* (Name der Bootdatei) und *next-server* (TFTP Server-IP). TFTP ist ein stark vereinfachtes UDP-basiertes *File Transfer Protokoll*.

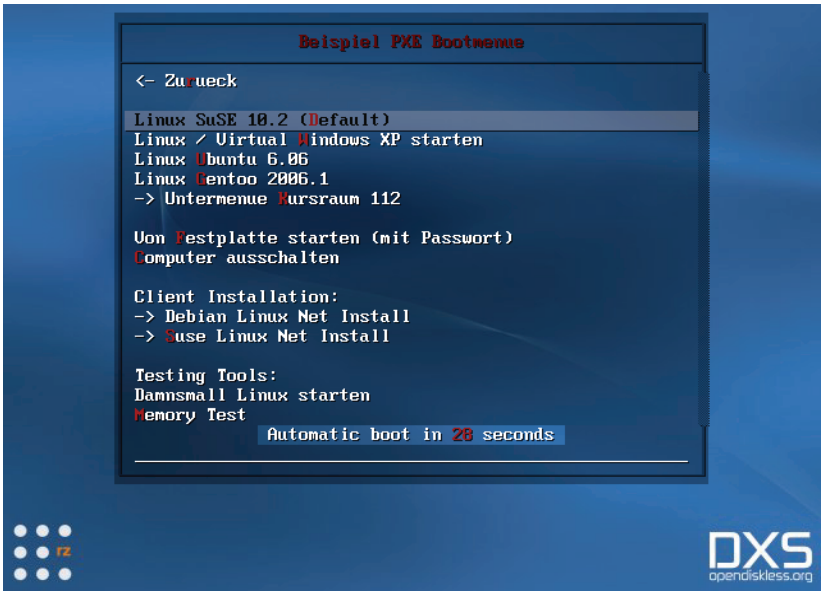


Abb. 2: Beispiel eines PXE Bootmenüs, welches eine Reihe verschiedener Betriebsarten einer einzigen Maschine erlaubt: Remote-Boot in unterschiedliche Linux-Varianten, Hardware-Test oder der Start von Festplatte[5]

2.2.2 Verwaltung eigener PXE-Konfigurationen und Bootmenüs

Das Framework unterstützt eine verteilte Administration von PXE Konfigurationsdateien. Lokale Administratoren können im System, aus dem Angebot zentraler RBS-Betreiber, für ihre Rechner PXE-Konfigurationen anlegen, etwa individuelle Bootmenüs zusammenstellen, und so ihren Rechnern diverse Betriebsmodi zuweisen und selbst verwalten. Zusätzlich bietet das Framework eine Zeitssteuerung von PXE-Konfigurationen. Dazu werden diesen Zeitspannen (Time Ranges) zugeordnet, in denen diese dann Gültigkeit haben. Auf diese Weise können den Clients in Abhängigkeit der Zeit, beispielsweise Montags zwischen 8 und 20 Uhr verschiedene PXE-Konfigurationen zugewiesen werden, die dann verschiedene *Betriebsmodi on Demand* erlauben.

2.2.3 RBS Betriebskonzepte

Mit dem geschaffenen Framework lassen sich folgende Remote Boot Services sehr gut zentral verwalten:

- *Automatisierte Remote OS/Software-Installation*
  Betriebsysteme und Software, lassen sich, individuell konfiguriert, zentral bereitstellen und remote von diesen Quellen installieren.[6] Dies erfolgt meist auf Grundlage des oben

[5] Diese oder textbasierte Menüs lassen sich mit der PXE-Komponente des Syslinux-Pakets [SYS06] erzeugen. Syslinux ist eine ganze Klasse von Bootloadern für Linux und andere Betriebssysteme.

beschriebenen initialen Basis-Bootkonzept. Auf diese Weise kann eine automatisierte Installation von Rechnern, durch einen Neustart initialisiert, zentral gesteuert und durchgeführt werden, etwa außerhalb von Kernarbeitszeiten. Dabei reduziert sich der Aufwand erheblich, wenn für eine größere Anzahl von Rechnern die gleiche Installation zentral verwaltet wird, etwa eine Standard-Arbeitsumgebung oder Kursumgebung. Softwareverteilungssysteme[7] integrieren meist zusätzlich eine Inventarisierung und ein zentrales Konfigurationsmanagement, sogenannte *Rollouts* sind mit weniger Aufwand verbunden.

- *Konfiguration und Betriebsmodus on Demand*

  Die remote einbindbare Ressourcen OS, Anwendungen und Konfigurationen können die komplette Installation eines Clients festlegen. Unterschiedliche Konfigurationen und Betriebsmodi für die Clients lassen sich so zentral einrichten und verwalten. Clients können nach Bedarf zu definierten Zeiten, durch einen Reboot, in einen anderen Betriebsmodus „umgeschaltet“ werden (*Betriebsmodus on Demand*). So können etwa Pool-Rechner tagsüber bestimmte Funktionen übernehmen, als einfache Workstations, Internet-PCs oder als spezielle Kursraum-Umgebungen [Such04], und nachts eine andere Funktion, etwa als Teil eines größeren GRID-Cluster zu Ausführung komplexer Rechnungen [DRBL06].

- *Diskless Clients (Net-PCs, Thin Clients)*

  Der vollständige Verzicht auf lokal gespeicherte Ressourcen führt zum Konzept der Diskless Clients.[8] Ausgangspunkt der Überlegungen ist die Erwartung, dass die bereits hohe Zahl zu verwaltender Pool- und Arbeitsplatzrechner in Zukunft noch zunehmen wird. Dieses Konzept bietet eine signifikante Aufwandsersparnis des Client-Management in mehrfacher Hinsicht:

  Zunächst wird durch Einbindung aller Ressourcen beim Booten ein Höchstmaß an Zentralisierung der Installationen und ihrer Administration erreicht. Dabei lassen sich sehr viele Rechner mit einer bzw. wenigen zentral verwalteten Installationen (Boot-

[6] Die meisten Linux-Distributionen bieten an das Betriebssystem über IP-Netze zu installieren, siehe dazu [LII06] für OpenSuSE, Ubuntu und Debian.

[7] Open Source Lösungen sind z.B. *Debian/Linux M23*, *Open PC Server Integration* (Linux, Windows OS-Installation). Verbreitete propritetäre Produkte sind *MS Remote Installation Services* als Erweiterung für Windows Server Systeme, *MS Systems Management Server* und *IBM Tivoli*.

[8] Der Client kann durchaus Betriebssysteme auf einem lokalen Speicher installiert haben. Der Begriff Diskless ist vielmehr als Boot-/Betriebskonzept zu sehen, welches auf lokalen Festspeichern abgelegte Ressourcen wie OS, Dateisysteme, Anwendungen beim Booten und im Betrieb nicht benötigt, denn als Hardware-Ausstattung.

Images) betreiben. Ferner erfolgt die komplette Installation, da die Ressourcen zur Laufzeit eingebunden werden, bei jedem Bootvorgang neu, *on the fly*, und nur für die Dauer des Betriebs, so dass die Clients auch als *stateless* bezeichnet werden. So lassen sich robustere mit weniger Administration verbundene Clients realisieren, da „Beschädigungen" der Installation während des Betriebs, beispielsweise durch den Benutzer oder Viren, durch einfachen Neustart (d.h. Neuinitialisierung) bereinigt sind.

Zusätzlich bietet das Diskless Client Konzept eine enorme Flexibilität bei der Definition individueller Betriebsmodi und Arbeitsumgebungen (siehe *Betriebsmodus on Demand*).

Als Beispiele seien das *Linux Terminal Server Project*, als einem der ältesten und aktivsten Linux-basierten Thin Client Projekte [LTSP06], und *OpenSLX* [OSLX06] als eine besonders flexible Open Source Lösung angeführt.[9] Daneben gibt es zahlreiche proprietäre Implementationen: Windows Server Systeme können im gewissen Umfang für dieses Boot- und Betriebskonzept eingesetzt werden, z.B. *MS Terminal Services*, wenn auch mit höheren Lizenzkosten und Einschnitten bei der Flexibilität.

- *Service-Mode*

  Beim Bootprozess können auch Programme zur Durchführung von Hardware-Tests, remote bezogen und direkt, meist ohne zwischengeschaltetes Betriebssystem, gestartet werden. Mit Hilfe von RBS Diensten lässt sich der Einsatz solcher Test-Suites zentral steuern, so dass große Rechnerzahlen zu beliebig definierbaren Zeiten, in einen Service-Mode gebootet werden können und dabei verschiedene Programme ausführen z.B. *memtest*, ein Speicher-Diagnose-Tool [MEM06].

3 Zentrale Features und Funktionen des Frameworks

Die Delegation von Aufgaben und daran geknüpfter Kompetenzen, ist ein zentrales Element vieler aktueller Management-Modelle. Angefangen beim grundlegenden Modell des

[9] *OpenSLX Linux Diskless Clients* wird im Rahmen eines Linux Diskless Client Projekts an der Universität Freiburg entwickelt. Weitere Open Source Lösungen sind das *PXES Thin Client Projekt* [PXES06], ähnlich LTSP nur deutlich kompakter, und das *Thin Station Project* [TSP06], Thin Client Projekt zur Unterstützung aller wichtigen Terminal-Server-Protokolle, wie Citrix ICA, NoMachine NX, 2X ThinClient, MS Windows Terminalservices (RDP), Cendio ThinLinc, Tarantella, X, Telnet, tn5250, VMS Term und SSH.

Management by Delegation[10] gefolgt von den darauf aufsetzenden, Weiterentwicklungen des *Management by Exception* und *Management bei Objectives*.

Delegation wird allgemein als Übertragung von Handlungskompetenz und damit verbunden von Entscheidungskompetenz bzw. Verantwortung, von einer Instanz, dem *Delegierenden*, an eine meist in der Hiearchie unterstellte Instanz, dem *Delegationsempfänger* verstanden. Teil der delegierten Kompetenzen kann auch die Kompetenz zur weiteren Delegation von Aufgaben sein. Delegation stellt ein probates Mittel zur Dezentralisierung und Auflösung starrer Strukturen in traditionellen Top-Down-Hierarchien dar, mit dem Ziel der Entlastung des Managements durch Teilung von Aufgaben und Verantwortung. Delegation setzt dabei eine klare Definition, von einander abgegrenzten Delegations- oder Kompetenzbereichen voraus.

Während der Delegationsempfänger die Handlungsverantwortung in seinem Kompetenzbereich trägt, verbleibt beim Delegierenden die zentrale Führungsverantwortung. Sie beinhaltet neben dem Formulieren grundsätzlicher Ziele und Treffen strategischer Entscheidungen, die Kontrollfunktion hinsichtlich delegierter Aufgaben, sowie die Rücknahme von Delegationen.

Delegationsmodelle werden auch in der IT-Verwaltung zunehmend aufgegriffen. Für die Administration größerer Umgebungen konzipierte, meist netzwerkbasierte Verwaltungssysteme verbinden ihre Verwaltungsfunktion mit einem Delegationsmechanismus und einer ausgereiften Rechteverwaltung und bieten so die Möglichkeit die Administration durch Delegation von Verwaltungssaufgaben zu dezentralisieren und zu entlasten (z.B. MS Active Directory).

Im vorliegenden Management Framework dienen Delegationsmechanismen der Realisierung einer verteilten und autonomen Administration der Dienste DNS, DHCP und PXE/RBS. Das zugrundeliegende Delegationsmodell und seine Umsetzung über Access Control Mechanismen soll im folgenden erläutert werden.

3.1 Delegationsmodell und interne Verwaltungsstruktur

Als Basis für ein Delegationsmodell wird eine hierarchische Verwaltungsstruktur aus voneinander abgegrenzten Verwaltungsbereichen, den administrative Units (AU), aufgebaut (Abb. 3a). Eine AU stellt den grundlegenden abgegrenzten Delegationsbereich dar, für den zur Abbildung administrativer Kompetenzen entsprechende Zugriffsrechte definiert werden können. Jede AU verwaltet autonom eigene Rechner und ihrer Einbindung in die verschiedenen Dienste. Ferner

[10] Auch als Harzburger Modell bekanntes in den 1960/70er Jahren weit verbreitetes Management-Konzept. Die Grundidee ist, Kompetenzen und Verantwortung für bestimmte Aufgaben, auf die unterste Hierarchieebene eines Unternehmens zu delegieren, mit dem Ziel selbstverantwortlich handelnder Mitarbeiter.

obliegt ihr die zentrale Administration eigens betriebener DNS, DHCP und RBS Dienste. Dazu wird sie in weitere entsprechende Administrationsbereiche unterteilt.
Der Aufbau der Verwaltungsstruktur erfolgt sukzessive (Abb. 3b), von oben nach unten, durch Anlegen von untergeordneter AUs.

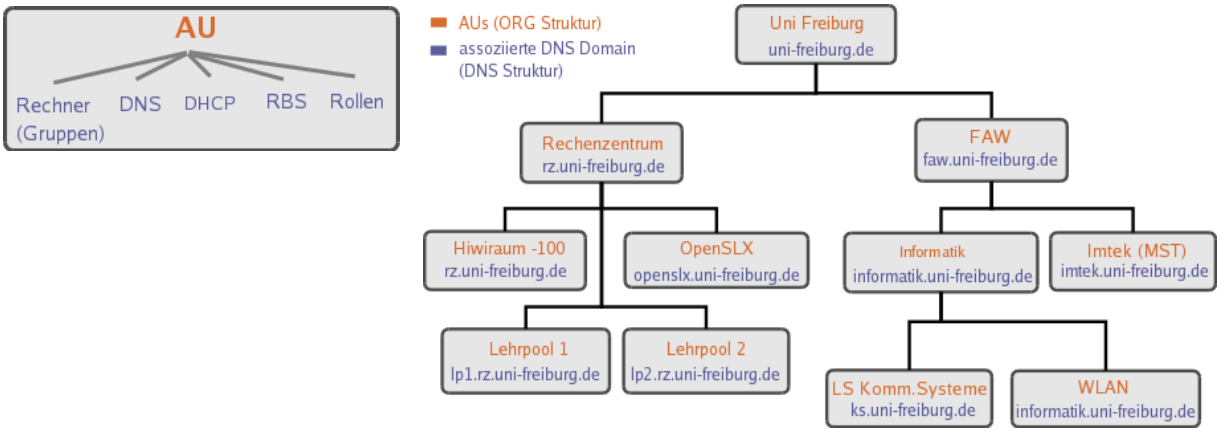


Abb. 3: (a) Administrative Unit (AU) mit weiteren partitionierten Unterbereichen, (b) Verwaltungsstruktur aus AUs aufgebaut (LDAP Verzeichnisbaum) und darin abgebildete DNS Struktur.

Dabei werden bestimmte Administrationskompetenzen „en-bloc“ an die festzulegenden Administratoren der neuen AU delegiert. Den oben beschriebenen Delegationsprinzipien folgend, übt eine AU die zentrale Kontrolle über ihre untergeordneten AUs aus. Durch bestimmen von Administratoren für die Unterbereiche kann auch innerhalb einer AU die Delegation bestimmter Teilaufgaben erfolgen, wie z.B. der Verwaltung von Rechnern oder des von der AU betriebenen DHCP Dienstes.
Der Verzeichnisbaum kann sich grundlegend an Verwaltungsstrukturen der Organisation orientieren. Die Definition von AUs ist dabei relativ frei und flexibel, so dass sie grundsätzlich jeden Bereich repräsentieren können, dem eine autonome Verwaltung bestimmter Ressourcen in Eigenverantwortung zugestanden wird, wie beispielsweise hochschul-öffentliche Computerräume, WLAN-Pools, oder auch bestimmte Projekte einer Abteilung.
Um die Unabhängigkeit zwischen Verwaltungs- und DNS Struktur zu wahren, wird der DNS Namensraum lediglich über den bestehenden Verzeichnisbaum verteilt. Jede AU wird einer DNS Domain zugeordnet, so dass Domainnamen als Ressource jedem verwalteten Hostnamen zugeordnet werden können. Dabei können mehrere AUs in der gleichen Domain sein.

3.2 Rollenbasierte Zugriffssteuerung

Die administrativen Kompetenzen des Verwaltungsbereich AU und seiner untergeordneten Bereiche werden im System über entsprechende Zugriffsrechte auf die jeweiligen Verzeichnisdaten abgebildet. Die Zugriffssteuerung erfolgt nach dem Modell der *Role Based Access Control* (RBAC), welches neben einem effizienten Autorisierungsmechanismus, vor allem mehr Flexibilität und eine Vereinfachung der Rechteverwaltung, dem *Access Control Management* bietet. Hier wurde auf das auch als *NIST Flat RBAC Model*[11] bekannte Konzept gesetzt, welches sich an einer gruppenbasierten Rechteverwaltung orientiert:

- Benutzer werden Rollen zugewiesen, *User Role Assignment* (URA).
- Rechte werden Rollen zugewiesen, *Permission Role Assignment* (PRA).
- Benutzer erhalten bestimmte Rechte als Mitglied einer bestimmten Rolle (URA), die über diese Rechte verfügt (PRA).

Ein Benutzer kann mehrere Rollen haben, und einer Rolle können mehrere Benutzer zugewiesen sein. Entsprechendes gilt für die Assoziation von Rechten mit Rollen.

Im System stehen die Rollen *MainAdmin*, den Hauptadministratoren einer AU mit entsprechenden Rechten, sowie für die AU-Unterbereiche die Rollen *HostAdmin* (Rechner), und *DhcpAdmin*, *DnsAdmin* und *RbsAdmin* (Verwaltung der jeweiligen Dienste) zur Verfügung. Die Rollen-Rechte-Zuordnung ist über die Access Control List (ACL) des LDAP Verzeichnisses in definierte Zugriffsrechte auf entsprechende Verzeichnisdaten festgelegt. Die Zuweisung von Rollen an bestimmte Benutzer erfolgt durch den MainAdmin der AU und stellt den eigentlichen Vorgang der Delegation von administrativen Kompetenzen dar. Abbildung 5 veranschaulicht schematich die Systemvorgänge, die im Zuge der Autorisierung eines zur Administration eines bestimmten Objekts geforderten Zugriffs ablaufen.

[11] Das *National Insititute of Standards and Technology* (NIST) hat verschiedene Formen von RBAC im standardisierten *NIST Model of RBAC* zusammengefaßt. Basismodell ist das Flache RBAC Modell, auf dem sukzessiv die erweiterten *Hierarchical*, *Constrained* und *Symmetric* RBAC Modell aufsetzen [NIST06], [SaFK03].

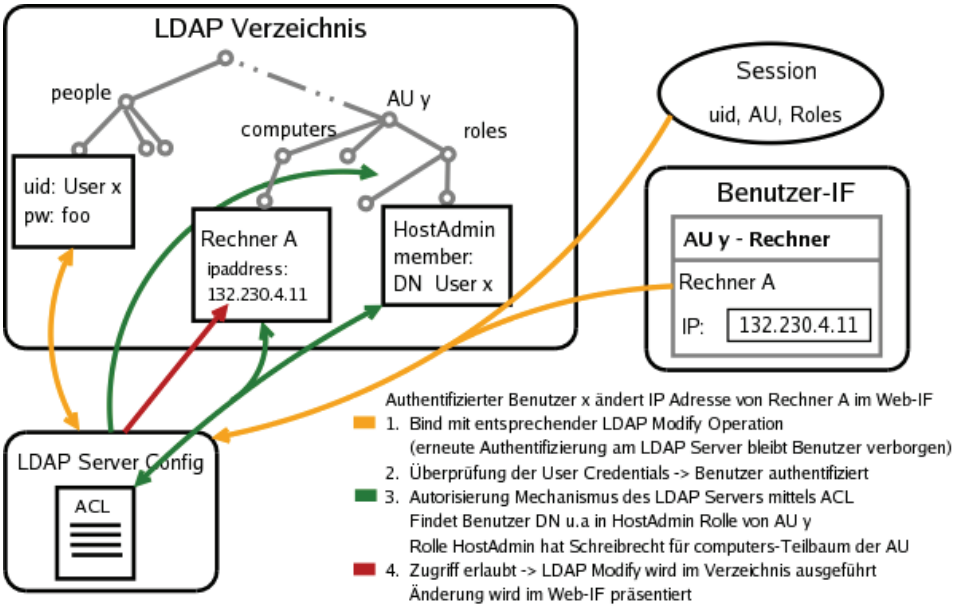


Abb. 5: Autorisierung von Zugriffen auf Verzeichnisdaten mittels RBAC

3.3 IP-Adressen Verwaltung

IP-Adressen stellen beim Netzwerk-Setup von Rechnern und bei der Konfiguration netzbasierter Dienste eine Schlüsselressource dar. Um das IP-Management effizienter zu gestalten, ist eine über Delegationsmechanismen zentrale gesteuerte und zugleich verteilte Verwaltung von IP-Adressen in das Framework integriert. IP-Adressen können von einer AU an direkt untergeordnete AUs delegiert und auf diese Weise in der gesamten hierarchischen Verwaltungsstruktur verteilt werden. Die von ihrer übergeordneten Instanz zugewiesenen IP-Adressen stehen einer AU dann zur Administration ihrer Rechner und Dienste, oder zur weiteren Delegation, direkt zur Verfügung. Die delegierende AU behält jederzeit die zentrale Kontrolle über alle delegierten IP-Adressen und kann diese bei Bedarf wieder zurückfordern. Davon können unter Umständen unterste Knoten des AU-Teilbaums betroffen sein, so dass die notwendigen Anpassungen im Verzeichnis rekursiv erfolgen.

3.4 Verteilte Dienste Administration

Zentral gespeicherte Konfigurationsdaten und ein gesteuerter Zugriff zur Kontrolle der administrativen Kompetenzen (LDAP, ACL) erlauben eine lokale Administration delegierter Teile der Konfiguration und ihre automatisierte Einbindung.

DNS: Die Verwaltung des meist zentral mit wenigen Servern betriebenen DNS einer Organisation wird durch Delegation der Verwaltung von Rechnernamen, d.h. DNS

Namenseinträge und zugehörigen Ressource Records (RR) verteilt. Lokale Administratoren haben über das Benutzer-Interface schreibenden Zugriff auf die DNS Namenseinträge ihre AU, die im System einer bestimmten DNS Domain zugeordnet ist. Die Generierung von Zonendateien erfolgt durch die Administratoren der Nameserver über das entsprechende Konfigurations-Tool. Es generiert die Zonendateien als einzelne Include-Dateien, eine für jede Subdomain der DNS Zone.

DHCP: Jede AU verwaltet seine eigenen DHCP Host und Subnet Objekte und darin angelegte DHCP Optionen, und kann diesen IP-Adressen aus dem der AU verfügbaren Adresspool verwenden zuweisen. Die Objekte sind im Verzeichnis über referenzierende Verweise einem bestimmten DHCP Dienst Objekt zugeordnet, in welchem der Dienst-Administrator die globale DHCP Optionen und Parameter des Dienstes festlegt. Die Generierung der Konfigurationsdateien erfolgt seitens des Dienstbetreibers durch das Konfigurationsskript, wiederum in Form von Include-Dateien für die Daten jeder AU, die einem spezifischen DHCP Dienst zugeordnet sind.

PXE/RBS: Das Framework unterstützt die Einrichtung von RBS Diensten und die Verwaltung von PXE-Bootkonfigurationen. RBS Betreiber können Server-spezifische PXE-Parameter in RBS-Dienstobjekten und Informationen zu ihren entfernt übers Netz beziehbaren Ressourcen (Kernel, Netzwerkdateisysteme) in Form von *generischen Bootmenüeinträgen* (GBM) ablegen. Nutzer des Dienstes können GBM verschiedener Anbieter zu vollständigen PXE-Konfigurationen erweitern und eigene PXE-Optionen hinzufügen. Auf diese Weise werden individuelle PXE-Bootmenüs aus dem Angebot von RBS-Diensten zusammengestellt und eigenen Rechnern zugewiesen. PXE-Konfigurationen sind einem RBS Dienst eindeutig zugeordnet. Das gleiche gilt für die darin abgelegten Bootmenüeinträge, die ein bestimmtes GBM im Verzeichnis referenzieren. Die Generierung der PXE-Konfigurationsdateien erfolgt analog zu DNS und DHCP auf dem entsprechenden Server (Abb. 6).

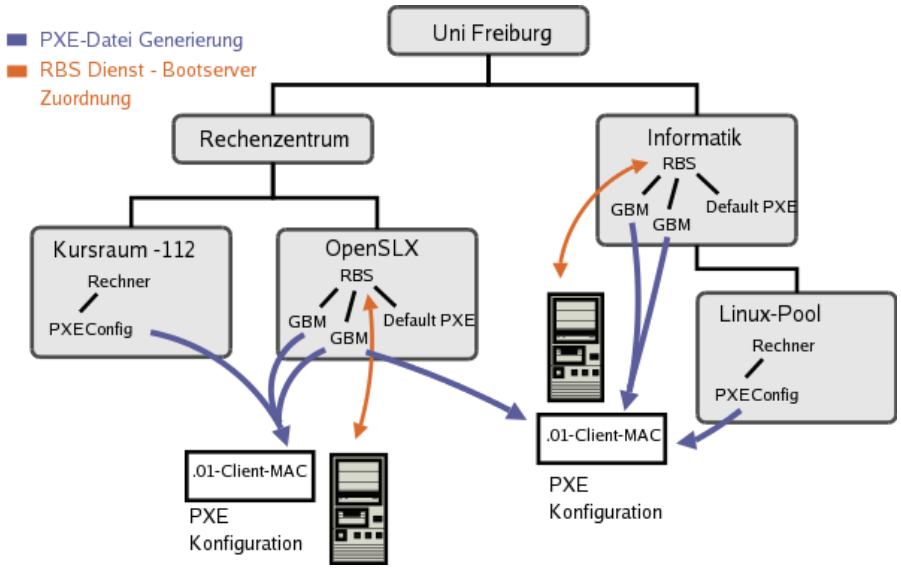


Abb. 6: Verteilte Organisation im Verzeichnis von PXE-Daten und Generierung von PXE-Konfigurationen für die in den verschiedenen Einheiten administrierten Clients

4 Fazit und Ausblick

Bisher gibt es an der Universität Freiburg eine ganze Reihe von Rechnerpools für verschiedene Anwendungen, wie Windows- oder Linux-Pools und Rechen-Cluster, die mit ihren eigenen dezentralen DHCP/TFTP-Einstellungen arbeiten. Diese Pools werden zuerst auf das Management-Framework umgestellt, da sich hier die Vorteile schnell einstellen können: Der Austausch von Hardware erfordert nun keine aufwändigen Workflows zum Ändern der MAC-Adressen mehr. Die Bootmenüs lassen sich flexibel erstellen und damit zeitgesteuert sehr verschiedene Betriebsarten realisieren. Damit sind dann sowohl die installierten Betriebssysteme als auch die Konfigurationsresourcen einer größeren Anzahl von Standardsystemen re-zentralisiert.

Der nächste Schritt wird die Übernahme heterogener Netze mit verschiedenen Arbeitsplatzsystemen in verschiedenen Einrichtungen sein: So bekommen lokale Administratoren statt statischer Adresszuweisungen die Möglichkeit weitgehend selbsttätig über ihren IP-Adress-Pool zu entscheiden. So soll in anderthalb Jahren mit einem ausscheidenden Mitarbeiter die manuelle DNS-Konfiguration komplett durch eine dezentrale Aktualisierung der Datenbank ersetzt werden.

Auf diese Weise lassen sich einige Routine-Aufgaben der Verwaltung von Rechnerpools bzw. Arbeitsplatzrechnern verteilen, ohne dass Dienst-Administratoren dabei die zentrale Kontrolle aus der Hand geben müssen, da sie weiterhin allein die Generierung der Konfigurationsdateien initiieren und steuern.

Literatur und Quellen

[Micr03] Active Directory Services, Microsoft, http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/

[CMU06] NetReg, Carnegie Mellon University, http://www.net.cmu.edu/netreg

[PXE06] Etherboot/gPXE, http://etherboot.sourceforge.net

[SYS06] Syslinux, PXELinux, http://syslinux.zytor.com

[LII06] Linux-Installation über Netzwerk/PXE:
Ubuntu, http://wiki.ubuntuusers.de/PXE-Installation
Debian, http://www.debian.org/releases/stable/i386/ch04.html.de
OpenSuSE, http://de.opensuse.org/SDB:Netzwerkinstallation_von_SuSE_Linux_ \
%C3%BCber_PXE-Boot

[Such04] D. v. Suchodoletz. *Linux Diskless Clients - eine Effizienzsteigerung im Kursbetrieb.* PIK 04/2004. Seite 246-250.

[DRBL06] DRBL - Diskless Remote Boot in Linux (National Center for High Performance Computing Taiwan), http://drbl.sourceforge.net

[LTSP06] LTSP - Linux Terminal Server Project, http://www.ltsp.org

[OSLX06] OpenSLX Linux Diskless Clients, http://www.openslx.org, und Linux Diskless Client Projekt an der Universität Freiburg (Lehrstuhl für Kommunikationssysteme) http://www.ks.uni-freiburg.de/projekte/ldc

[PXES06] 2X ThinClientServer PXES Edition, http://www.2x.com/pxes

[TSP06] Thin Station Project, http://thinstation.sourceforge.net

[MEM06] Memtest86+ Speicher Diagnose Tool, http://www.memtest.org

[NIST06] National Institute of Standards and Technology, *Role Based Access Control,* http://csrc.nist.gov/rbac

[SaFK03] R. Sandhu, D. Ferraiolo and R. Kuhn. *The NIST Model for Role Based Access Control: Towards a Unified Standard*. Proceedings, 5th ACM Workshop on Role Based Access Control, Juli 2003.

Die Landkarte – Rahmenwerk zur Unterstützung von Evolution und Betrieb serviceorientierter Architekturen

Frederic Majer, Johannes Meinecke, Patrick Freudenstein

IT-Management und Web Engineering Research Group
Institut für Telematik
Universität Karlsruhe (TH)
76128 Karlsruhe
{majer, meinecke, freudenstein}@tm.uni-karlsruhe.de

Abstract

Die technische Realisierung eines Integrierten Informationsmanagements an Hochschulen basiert zunehmend auf dem Konzept der serviceorientierten Architekturen. Die hochgradige Heterogenität und Komplexität der resultierenden Systemlandschaften begründet den Bedarf an systematischen Ansätzen zur Unterstützung der strategischen und technischen Weiterentwicklung sowie des Betriebs dieser Systeme. Der in diesem Beitrag beschriebene Ansatz – die Landkarte – basiert auf einem Informationsmodell zur umfassenden Modellierung serviceorientierter Architekturen. Entsprechend einer Landkarte nutzt das Rahmenwerk die Modellinformationen zur Laufzeit und dient verschiedenen Zielgruppen oder Systemen als Orientierungs- und Entscheidungshilfe. Neben der geeigneten Darstellung und Bewertung der relevanten Informationen über die Systemlandschaft unterstützt die Landkarte darüber hinaus den Betrieb serviceorientierter Architekturen, indem sie die einzelnen Systembestandteile gemäß ihrer spezifizierten Soll-Konfigurationen überwacht.

1 Einleitung

Dem Wunsch der durchgängigen Unterstützung der Geschäftsprozesse durch Anwendungssysteme wird in der Industrie [PKGS06] und an Hochschulen [GeMS06; HisG06] zunehmend mit dem Konzept der serviceorientierten Architektur begegnet. Ziel ist dabei die historisch gewachsene Systemlandschaft derart zu gestalten, dass Geschäftsprozesse durch die Aneinanderreihung von Serviceaufrufen realisiert werden können. Aufgrund der Integration und

Komposition unterschiedlichster Systemkomponenten und der Tatsache, dass verschiedene Einrichtungen und Organisationseinheiten zur Umsetzung beitragen, resultiert eine äußerst komplexe, heterogene und verteilte Systemlandschaft. In diesem Zusammenhang drängt sich die Frage nach geeigneten Konzepten zur Unterstützung der strategischen und technischen Weiterentwicklung sowie des Betriebs dieser Systeme auf. Einerseits benötigen die verschiedenen beteiligten Zielgruppen Informationen über die Fähigkeiten und die Konfiguration einzelner Komponenten sowie des gesamten Systems. Über geeigneten Sichten müssen die relevanten Daten derart aufbereitet sein, dass sie der Situation und den Bedürfnissen der Zielgruppe entsprechen. Andererseits werden Mechanismen benötigt, die ein Fehlverhalten bzw. Ausfälle einzelner Komponenten frühzeitig erkennen und gegebenenfalls Schritte zur Beseitigung der Betriebsbeeinträchtigung einleiten.

In diesem Beitrag wird ein systematischer und dedizierter Ansatz für die Evolution und den Betrieb höchstkomplexer, verteilter Systeme präsentiert. In Abschnitt 2 wird das zugrunde liegende Szenario vorgestellt und allgemeingültige funktionale Anforderungen an Unterstützungswerkzeuge für verschiedene Zielgruppen abgeleitet. In Abschnitt 3 wird ein Informationsmodell zur Modellierung serviceorientierter Architekturen bezüglich unterschiedlicher Aspekte eingeführt. Abschnitt 4 befasst sich mit der Vorstellung geeigneter Architekturkonzepte zur Unterstützung von Evolution und Betrieb solcher Systeme – der Fokus liegt hierbei auf der Beschreibung und Überwachung. Der Weiteren werden in Abschnitt 5 implementierte Unterstützungsfunktionalitäten und im darauf folgenden Abschnitt verwandte Ansätze der Wirtschaft und Forschung vorgestellt. Abschließend wird in Abschnitt 7 der Beitrag zusammengefasst und ein Ausblick auf zukünftige Arbeiten gegeben.

2 Problemstellung

Im folgenden Abschnitt werden die identifizierten funktionalen Anforderungen für die Unterstützung von Evolution und Betrieb von serviceorientierten Architekturen skizziert. Als Referenzarchitektur wurde der Anforderungsanalyse die serviceorientierte Architektur des Projekts „Karlsruher Integriertes InformationsManagement“ (KIM) [JuWi05] der Universität Karlsruhe (TH) zugrunde gelegt.

2.1 Karlsruher Integriertes InformationsManagement

Das Projekt Karlsruher Integriertes InformationsManagement der Universität Karlsruhe (TH) strebt eine ganzheitliche Betrachtung sämtlicher einrichtungsübergreifender Prozesse an der Hochschule an. Dieses Ziel wird mittels konsequenter Modellierung, Analyse und Verbesserung der Geschäftsprozesse sowie durch Schaffung einer übergreifenden prozessorientierten IT-Plattform verfolgt [FLMM06]. Entsprechend der dezentralen Verwaltungs- und Organisationsstruktur deutscher Hochschulen zeichnet sich die bestehende Systemlandschaft durch eine hochgradige Heterogenität aus. Um dennoch den standardisierten Zugriff auf Informationen und die Abwicklung von Geschäftsprozessen über verschiedene Organisationseinheiten hinweg zu ermöglichen, wird das Konzept der serviceorientierten Architekturen angewendet. Die resultierende integrierte serviceorientierte Architektur (iSOA) besteht aus den vier Integrationsschichten *Technische Infrastruktur*, *Basisdienste*, *Anwendungsdienste* und *Service-Portal* (vgl. Abb. 1).

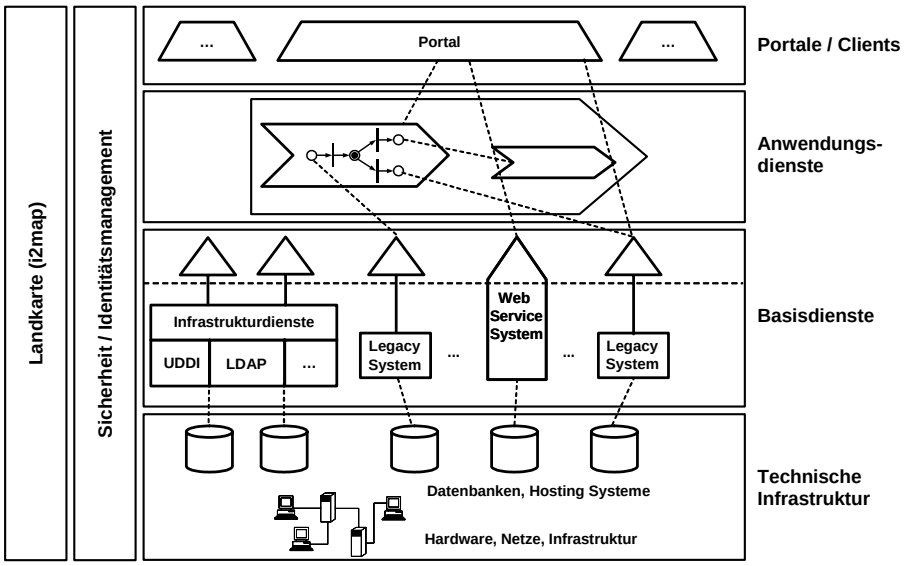


Abb. 1: Die integrierte serviceorientierte Architektur (iSOA)

Die Integrationsschicht Technische Infrastruktur befasst sich mit dem Betrieb und der Wartung der grundlegenden Infrastruktur. Die Schicht der Basisdienste beinhaltet hauptsächlich wiederverwendbare Komponenten in Form von Web Services, die als Wrapper den genormten und plattformunabhängigen Zugang zu den Daten aus (Alt)-Systemen oder Datenbanken bieten. Über das standardisierte CRUDS-Interface [IBMC05] stellt jeder Basisdienst Operationen zur Erstellung, Abfrage und Modifikation für eine begrenzte, semantisch stark kohäsive Menge an

Geschäftsobjekten zur Verfügung. Die Anwendungsdienste realisieren die Geschäftsprozesse, indem sie die Basisdienste zu höheren, prozessorientierten Diensten verknüpfen und selbst wiederum als CRUDS-Web Service publiziert werden. Beispielsweise werden beim Erstellen eines „Transcripts of Records“ (detaillierter Notenauszug eines Studierenden) die Basisdienste für Personen-, Prüfungsresultats- und Lehrveranstaltungsinformationen orchestriert. Die Schicht der Portale und Clients stellt den unterschiedlichen Benutzergruppen über verschiedene Formen von Benutzerschnittstellen wie Web Anwendungen und Portalen bis hin zu Büroanwendungen, zentrale und einheitliche Zugangspunkte auf die Geschäftsprozesse zur Verfügung.

Orthogonal zu den vier Schichten sind die Aspekte *Sicherheit / Identitätsmanagement* und *Landkarte (integrated information map – i2map)* angeordnet. Über einen föderativen Ansatz zur Authentifizierung und Autorisierung [MeNG05] sowie der Anwendung sicherer Kommunikationsmechanismen wird im Bereich Sicherheit und Identitätsmanagement der Datenschutz und die Integrität vertraulicher, personenbezogener Daten gewährleistet. Der Aspekt der Landkarte adressiert die in diesem Beitrag beschriebene Problematik der Unterstützung von strategischer und technischer Evolution und Betrieb der resultierenden hochkomplexen und stark verteilten Architektur. Hierfür sollen den verschiedenen Zielgruppen über geeignete Mechanismen und Sichten die relevanten Informationen über die Systemlandschaft als Orientierungs- und Entscheidungshilfe zur Verfügung gestellt werden.

2.2 Unterstützungspotenziale für Evolution und Betrieb serviceorientierter Architekturen

Für die Unterstützung von Evolution und Betrieb einer serviceorientierten Architektur wurden in Zusammenarbeit mit den unterschiedlichen Zielgruppen verschiedene funktionale Anforderungen an die Landkarte identifiziert. Die Nutzer charakterisieren sich durch verschiedene Informationsbedürfnisse und können im KIM-Projekt in die vier Gruppen *Anwender*, *Universitätsleitung*, *Entwickler* und *Betreiber* eingeteilt werden. Die Gruppe der Anwender subsumiert die Benutzer der universitären Informationssysteme wie Studierende, wissenschaftliche Mitarbeiter und Verwaltungsmitarbeiter der Hochschule. Die Universitätsleitung wurde hierbei aufgrund ihres besonderen Interesses an einem effizienten und reibungslosen Betrieb der gesamten Systemlandschaft und der damit verbundenen positiven Außenwirkung gesondert aufgeführt. Die Zielgruppe der Entwickler trägt entscheidend zur Evolution der gesamten Systemlandschaft bei, indem sie die Neu- und Weiterentwicklung von Komponenten und Funktionalitäten vorantreibt, wohingegen die Betreiber für den Betrieb der

existierenden serviceorientierten Architektur verantwortlich sind. Hierunter fallen Aufgaben wie die Überwachung der technischen Infrastruktur, der Legacy-Systeme sowie der im Zuge der iSOA entwickelten Komponenten und Schnittstellen, aber auch die Unterstützung der Anwender bei der Nutzung der Informationssysteme.

Grundsätzlich können die Informationsbedürfnisse der unterschiedlichen Zielgruppen und die daraus resultierenden funktionalen Anforderungen an die Landkarte in die Bereiche *Beschreibung* (A1 – A7) und *Überwachung* (A8 – A11) aufgeteilt werden. Tab. 1 stellt einen Überblick über die Funktionalitäten und die Nutzungshäufigkeit durch die einzelnen Gruppen dar.

	Anwender	Universitäts-leitung	Entwickler	Betreiber
A1: Überblick über Systemlandschaft	-	+	+	+
A2: Detaillierte Auskunft	+	+	+	+
A3: Suche nach Komponenten	o	o	+	+
A4: Protokollierung von Änderungen	-	-	+	+
A5: Momentaufnahme	-	-	+	+
A6: Simulation	-	o	+	+
A7: Speicherung des Betriebskonzepts	-	-	o	+
A8: Statusüberblick und Fehlererkennung	o	o	o	+
A9: Automatisches Testen / Auditing	-	-	+	+
A10: Auswertungen	o	+	+	+
A11: Benachrichtigungen	o	-	o	+
(+): Häufige Nutzung; (o): Seltene Nutzung; (-): Keine Nutzung				

Tab. 1: Nutzung der Landkartenfunktionalitäten

Im Folgenden werden die einzelnen funktionalen Anforderungen an die Landkarte kurz skizziert.

A1 – Überblick über die Systemlandschaft: Zur (strategischen) Weiterentwicklung der iSOA soll die Landkarte dedizierte Sichten auf die Systemlandschaft bieten. Speziell die Visualisierung von Beziehungen zwischen den Komponenten steht hierbei im Vordergrund.

A2 – Detaillierte Auskunft: In Abhängigkeit der Zielgruppen sollen neben detaillierten allgemeinen, organisatorischen und funktionalen Beschreibungen auch Informationen bezüglich der Aspekte Sicherheit und Qualität über die iSOA-Komponenten verfügbar sein.

A3 – Suche nach Komponenten: Um die Wiederverwendung von Komponenten in dem hochkomplexer System zu forcieren, sollen umfassende Suchmechanismen angeboten werden.

A4 – Protokollierung von Änderungen: Die Landkarte soll einen zentralen Zugangspunkt zu allen protokollierten Änderungen an Komponenten des Gesamtsystems darstellen.

A5 – Momentaufnahme: Um die Fehleranalyse in der iSOA zu unterstützen, sollen historische Beschreibungs- und Konfigurationsinformationen des Gesamtsystems zur Verfügung stehen.

A6 – Simulation: Die Auswirkungen von Veränderungen in Form von Modifikationen existierender Systembestandteile sowie das Hinzufügen oder Entfernen von Komponenten soll anhand der Beschreibungsinformationen simulierbar sein.

A7 – Speicherung des Betriebskonzepts: Als zentrales Medium in der iSOA soll die Landkarte den Zugriff auf das Betriebskonzept ermöglichen.

A8 – Statusüberblick und Fehlererkennung: Neben der Abfrage des Soll-Zustands einer Komponenten (A2) soll die Landkarte diesem den tatsächlichen Ist-Status gegenüberstellen. Darüber hinaus sind die Informationen auszuwerten bzw. zu dokumentieren.

A9 – Automatisches Testen / Auditing: Die Landkarte soll allgemeine Verfahren bereitstellen, um einzelne Komponenten vor und während ihres Einsatzes hinsichtlich der Erfüllung von Anforderungen und Richtlinien (Standardkonformität, Sicherheit, Dienstleistungs-vereinbarungen etc.) zu untersuchen.

A10 – Auswertungen: Kontinuierlich soll die Art und der Umfang der Nutzung einzelner Systembestandteile ausgewertet und dokumentiert werden.

A11 – Benachrichtigungen: Die Landkarte soll Mechanismen zu Verfügung stellen, um Personen oder (externe) Systeme über aktuelle Ereignisse (wie z.B. Systembeeinträchtigungen durch Ausfälle) in der iSOA zu benachrichtigen.

Neben der grundsätzlichen Aufgabe mit der Landkarte als Unterstützungssystem für Evolution und Betrieb einer serviceorientierten Architektur die gewünschten funktionalen Anforderungen zu erfüllen, liegt eine weitere Herausforderung darin, den verschiedenen Zielgruppen entsprechend ihrer Interessen dedizierte Zugangspunkte und Sichten auf die relevanten Informationen zur Verfügung zu stellen.

3 Modellierung serviceorientierter Architekturen

Die Analyse der in Kapitel 2 spezifizierten Anforderungen führt zu dem Schluss, dass, unabhängig von der Umsetzung der einzelnen Anforderungen in funktionale Basisbestandteile

eines Unterstützungssystem, detaillierte Informationen über die in der Gesamtarchitektur enthaltenen Komponenten und deren Beziehungen untereinander benötigt werden. Neben beschreibenden Aspekten, um beispielsweise Evolution in Form von Komposition oder Wiederverwendung existierender Komponenten zu unterstützen, sind vor allem Laufzeitinformationen aller Komponenten für den reibungslosen Betrieb von Interesse.

[ABCF02; ScDR03] definieren den Spezifikationsrahmen für (Fach)-Komponenten in die Ebenen *Vermarktung*, *Aufgabe*, *Terminologie*, *Qualität*, *Abstimmung*, *Verhalten* und *Schnittstelle* und demonstrieren die Übertragbarkeit auf Web Services. Um die umfassende Beschreibung und Überwachung einer gesamten serviceorientierten Architektur zu ermöglichen, wurden bei unserem Ansatz basierend auf den Erfahrungen aus dem KIM-Projekt die verschiedenen grundlegenden Bausteine identifiziert und in einem nächsten Schritt deren relevante Attribute in entsprechenden Dimensionen definiert.

Das resultierende Informationsmodell in Form eines UML-Klassendiagramms beinhaltet als zentrale Klasse die Definition von *iSOAComponent*, welche die Attribute beinhaltet, die alle Bausteine der iSOA gemeinsam haben. Diese abstrakte Oberklasse vererbt ihre Eigenschaften zum einen den Komponenten der technischen Infrastruktur (*TechnicalInfrastructure-Component*) wie Server, Datenbanken und Altsysteme und zum anderen den spezifischen Bausteinen einer serviceorientierten Architektur (*SOAComponent*). Die Gruppe SOAComponent beinhaltet Komponenten und damit verbundene Typdefinitionen der Portalschicht (beispielsweise *Application*, *Domain*, *ControlFunction*, *Audience*), eine abstrakte Klasse für Web Services und speziellen Klassen wie etwa dem *SecurityRealm* zur Modellierung des Geltungsbereichs einer Organisationseinheit. Der Typ *WebService* teilt sich wiederum in Anwendungsdienste (*ApplicationService*), Basisdienste (*CoreService*) und Infrastrukturdienste (*InfrastructureService*). Letztere dienen vor allem der Spezifikation fundamentaler Infrastruktur-Basisdienste einer SOA, wie zum Beispiel dem *Identity Provider* oder *Security Token Service*, zur Unterstützung eines föderierten Identitätsmanagements.

Abb. 2 gibt einen Ausschnitt des Informationsmodells mit dem zentralen Typ iSOAComponent sowie einigen damit verbundenen Typdefinitionen wieder. Grundsätzlich wird jede Komponente über einen eindeutigen Bezeichner identifiziert und es können (Meta)-Informationen wie die Beschreibung (*Description*), Schlagwörter (*Tags*) oder die Schichtenzugehörigkeit (*Layer*) spezifiziert werden. Der *Status* bezeichnet dabei nicht den gegenwärtigen operativen Zustand einer Komponente, sondern ermöglicht die Zuordnung einer

Komponente zu den Phasen ihres Entwicklungszyklus (z.B. entwickelt, getestet, betriebsbereit, abgeschaltet). Dementsprechend besteht auch die Möglichkeit Kontaktinformationen für Ansprechpartner bezüglich unterschiedlicher Belange zu spezifizieren bzw. die Änderungshistorie (*ChangeLog*) zu hinterlegen und auf die technische Dokumentation (*Documentation*) zu verweisen.

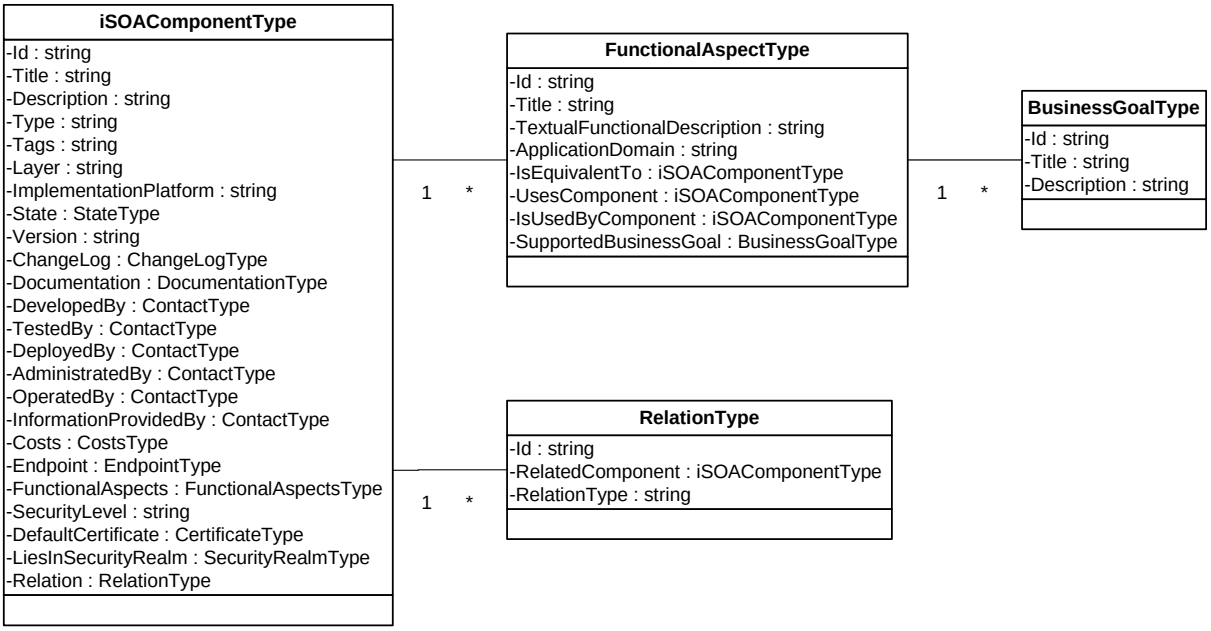


Abb. 2: Auszug aus dem Informationsmodell für serviceorientierte Architekturen

Einige allgemeingültige Sicherheitsaspekte wie die Spezifikation der Sicherheitsstufe (*SecurityLevel*) oder des Standardzertifikats (*DefaultCertificate*) einer Komponente sind direkt in iSOAComponent enthalten. Weiterführende Sicherheitsaspekte wie beispielsweise die Spezifikation von Autorisierungsrichtlinien für Operationsaufrufe oder die Transport- und Nachrichtensicherheit sowie eine umfassende Beschreibung der Schnittstelle werden über die Definition von Endpunkten (*EndpointType*) realisiert. Der Freiheitsgrad mehrerer Endpunkte ermöglicht, dass eine Komponente über mehrere Zugangspunkte mit unterschiedlichen Protokollen und Sicherheitsrichtlinien (z.B. Zertifikate) verfügen kann.

Der Typ *FunctionalAspectType* ermöglicht die Beschreibung der funktionalen Aspekte einer Komponente. Wie in Abb. 2 ersichtlich, kann die generelle Funktionalität, die Anwendungsdomäne sowie der durch die Komponente unterstützte Zweck beschreiben werden. Über Attribute wie *IsEquivalentTo*, *UsesComponent*, *IsUsedByComponent* können funktionale Beziehungen bzw. Abhängigkeiten zu anderen Bausteinen der iSOA modelliert werden, um beispielsweise während des Betriebs einen schnellen Überblick über die Auswirkungen von

Ausfällen einzelner Systembestandteile zu erhalten. Darüber hinaus besteht auf Ebene der iSOAComponent die Möglichkeit mittels des Typs *RelationType* beliebige weitere Beziehungen zu anderen Komponenten zu definieren.

4 Landkartenarchitektur zur Unterstützung von Evolution und Betrieb serviceorientierter Architekturen

Die in Kapitel 2 spezifizierten Funktionalitäten zur Unterstützung von Evolution und Betrieb serviceorientierter Architekturen sollen den verschiedenen Zielgruppen über dedizierten Sichten auf die relevanten Informationen innerhalb eines i2map-Portals oder durch die Einbindung in andere, bereits existierende Portale oder Client-Anwendungen zugänglich gemacht werden. Durch die Ausrichtung einzelner funktionaler Anforderungen auf einerseits beschreibende und andererseits überwachende Aspekte werden im Folgenden die jeweiligen zur Realisierung benötigten Bausteine und Konzepte der Landkartenarchitektur getrennt beschreiben. Aufgrund der Tatsache, dass die Landkarte einen Aspekt der iSOA darstellt, orientiert sich deren Konzeption konsequent an der bereits vorgestellten Gesamtarchitektur.

4.1 Unterstützung von Beschreibung

Um die beschreibenden Funktionalitäten realisieren zu können, werden die einzelnen Komponenten (*Verwaltete Objekte*) der iSOA an einem zentralen Verzeichnis (*KIM-Registry*) angemeldet. Hierbei werden die dem Typ der Komponente entsprechenden relevanten Informationen gemäß dem Informationsmodell spezifiziert und in der Registry abgelegt. In Abhängigkeit der Managementfähigkeit der jeweiligen Komponente kann dieser Schritt automatisiert durchgeführt werden. Die Registry stellt, als zentrales datenhaltendes System, verschiedene Schnittstellen in Form von Web Services für den Zugriff auf die Daten zur Verfügung. Neben der Schnittstelle für den umfassenden Zugriff auf die Komponenteninformationen gemäß dem Informationsmodell (*Registry*) können Untermengen der Informationen gemäß dem UDDI-Standard [BCEH02] oder für andere Modelle wie z.B. WAM [MGMB06] abgerufen und dediziert genutzt werden (vgl. Abb. 3). In diesem Zusammenhang ist für Szenarien mit autarken Organisationseinheiten die Föderation mehrerer Verzeichnisse denkbar, um die lose Kopplung serviceorientierter Architekturen zu

gewährleisten und dennoch beschreibende (und überwachende) Funktionalitäten über die Grenzen der eigenen Zuständigkeit hinaus zu unterstützen.

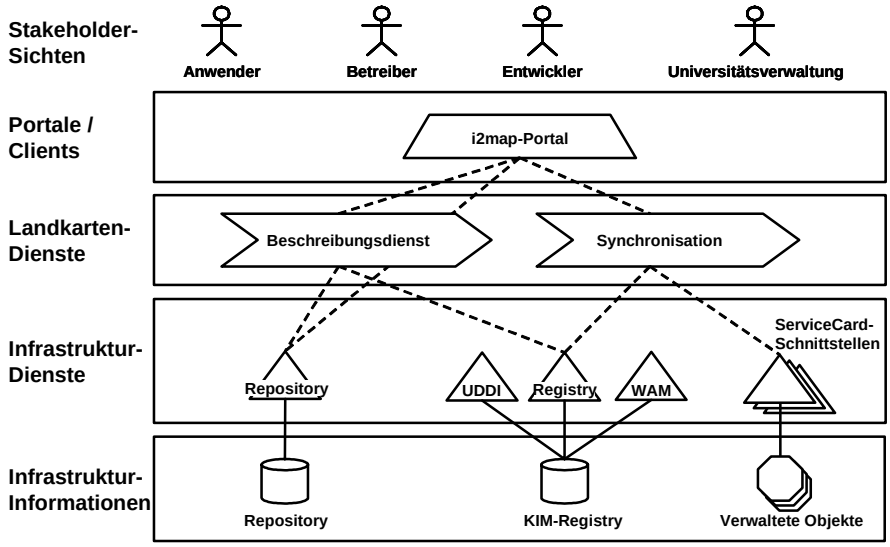


Abb. 3: Basisarchitektur für den Bereich Beschreibung

Für die Umsetzung der eigentlichen Landkartenfunktionalität ist der *Beschreibungsdienst* zuständig. Dieser Anwendungsdienst ruft gemäß der Nutzeranfrage aus dem i2map-Portal die benötigten Informationen über den Registry-Basisdienst ab und bereitet diese den Nutzerbedürfnissen entsprechend auf. Zur Bereitstellung mit bestimmten Komponenten assoziierter Dokumente (beispielsweise technische Dokumentation) greift der Anwendungsdienst auf ein Repository zu, welches diese zur Verfügung stellt.

Um Konsistenz zwischen den gespeicherten Daten in der Registry und den Informationen, die managementfähige Komponenten über sich publizieren, zu gewährleisten, existiert ein Synchronisationsdienst. Einerseits propagiert dieser Veränderungen, die direkt an Komponenten der iSOA vorgenommen werden (z.B. Änderung der Schnittstelle durch Entwickler). Andererseits werden Aktualisierungen der Registry-Einträge, die über das i2map-Portal getätigt werden (z.B. veränderte Zuständigkeiten), an die Komponenten weitergeleitet und dort verarbeitet.

4.2 Unterstützung von Überwachung

Neben den beschreibenden Informationen ist das Echtzeitverhalten einzelner Komponenten und des Gesamtsystems zur Gegenüberstellung der Soll- und Ist-Werte von Interesse. Hierbei ist der Realisierungsgrad der funktionalen Anforderungen aus Kapitel 2 bezüglich der Überwachung von Komponenten stark an deren Managementfähigkeit gekoppelt.

In der Landkartenarchitektur stellt der Anwendungsdienst *Monitoring & Ereignisauswertung* den zentralen Baustein dar (vgl. Abb. 4). Über den Zugriff auf die KIM-Registry erhält dieser die Bezeichner und Zugangspunkte der zu überwachenden Komponenten. Gemäß seiner Konfiguration nutzt er zur eigentlichen Überwachung verschiedene Agenten. Diese Agenten sind als CRUDS-Basisdienste realisiert und stellen für gewisse Komponententypen dedizierte Überwachungsmetriken zur Verfügung. Diese Indirektion hat zum einen den Vorteil, dass der Ansatz beliebig skalierbar ist und eine Parallelisierung der Statusabfragen des Gesamtsystems ermöglicht. Zum anderen erhöht die Kapselung der Logik zur konkreten Überwachung der Komponenten die Flexibilität und Mächtigkeit. Denkbar ist hierbei, dass verschiedene Agenten für einen Komponententyp zuständig sind und sich durch unterschiedliche Überwachungsaspekte und -verfahren auszeichnen oder bestimmte Agenten sich bereits existierender Überwachungssysteme bedienen (z.B. für den Bereich der technischen Infrastruktur).

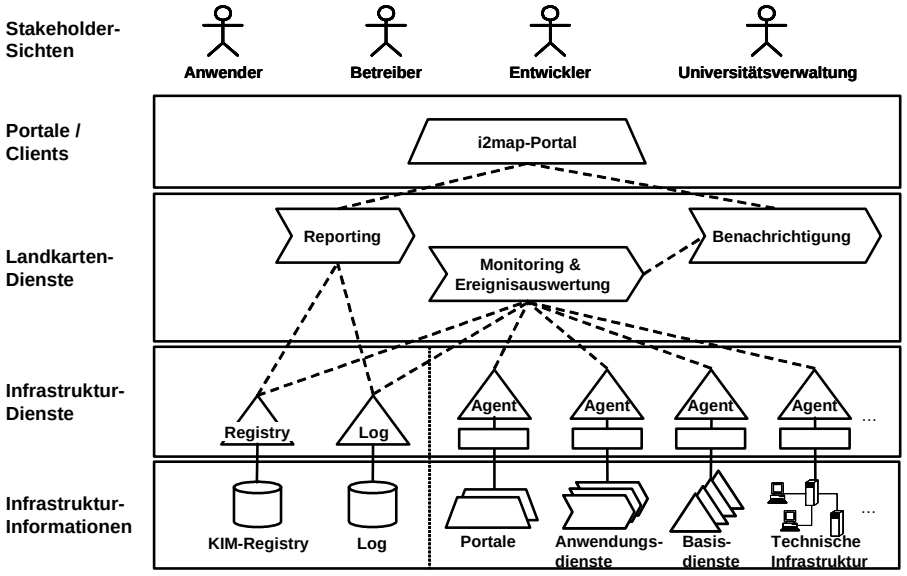


Abb. 4: Basisarchitektur für den Bereich Überwachung

Die Ergebnisse der kontinuierlichen Statusabfragen und Tests der einzelnen Agenten werden durch den Anwendungsdienst Monitoring & Ereignisauswertung anhand definierter Regeln ausgewertet und in ein Log geschrieben. Identifizierte Systembeeinträchtigungen werden über eine separate Benachrichtigungskomponente (*Benachrichtigung*) den zuständigen Personen oder anderen Systemen mitgeteilt.

Den Zugriff auf die Laufzeiteigenschaften des gesamten Systems über das i2map-Portal wird durch den *Reporting*-Anwendungsdienst realisiert. Dieser stellt die Daten und Auswertungen wie beispielsweise die durchschnittliche Verfügbarkeit oder die Nutzungsstatistik einer Komponente über dedizierte Sichten zur Verfügung.

5 Implementierung von Landkartenfunktionalitäten

Nach der Einführung des Informationsmodells sowie der allgmeingültigen Landkartenkonzepte für Beschreibung und Überwachung serviceorientierter Architekturen, wird nun der Einsatz im Rahmen des Projekts Karlsruher Integriertes InformationsManagement vorgestellt. Mit dem Projektziel der technologischen Umsetzung einer durchgängigen Integration der Geschäftsprozesse und der damit einhergehenden Einbindung verschiedenster Softwaresysteme entsteht eine im hohen Maß verteilte Gesamtarchitektur, die es zu beherrschen gilt.

In diesem Zusammenhang ist die Existenz von Informationen über die einzelnen Komponenten die Basis für die Unterstützung von Evolution und Betrieb der gesamten Architektur. In einem ersten Schritt wurden die hierfür vorgesehenen Managementoperationen *getServiceCard* und *getStatus* der bereits existierenden Basis- und Anwendungsdienste derart implementiert, dass die Komponenten Auskunft über sich – in Form einer beschreibenden Visitenkarte (*ServiceCard*) – und über ihren Zustand (*Status*) geben können. Die Daten können dabei in verschiedenen Detaillierungsstufen abgefragt werden und entsprechen dem Informationsmodell. In einem weiteren Schritt wurden alle relevanten Komponenten an einer zentralen Registry angemeldet und die beschreibenden Informationen dort abgelegt. Bei nicht oder nur begrenzt managementfähigen Komponenten des Gesamtsystems wurden die Informationen manuell eingepflegt. Für die Überwachung der Basis- und Anwendungsdienste wurden Agenten implementiert, die den Status gemäß etablierter Standards zurückliefern. Für das Monitoring von Komponenten der technischen Infrastruktur sowie weiterer Komponenten wie beispielsweise dem Microsoft BizTalk Server 2006 bedienen sich andere Agenten des bereits im Rechenzentrum im Einsatz befindlichen Überwachungssystem Nagios [GalsoJ] und des Microsoft System Center Operations Manager 2007 [Micr06].

Schlussendlich werden den Nutzern über Zugriffe auf verschiedene Anwendungsdienste die gewünschten Landkartenfunktionalitäten in dem auf Basis des Microsoft Office SharePoint Server 2007 implementierten i2map-Portal (vgl. Abb. 5) zur Verfügung gestellt. Dabei nutzen

die Gruppe der Entwickler vor allem die Möglichkeit nach Diensten zu suchen sowie deren detaillierte (Schnittstellen-)Beschreibungen abzurufen. Neben den Betreibern, die vor allem die Übersicht über den gesamten Systemzustand benötigen, ist auch die Universitätsverwaltung an den Auswertungen bezüglich der Nutzungsintensität der verschiedenen Dienste interessiert. Für die Gruppe der studentischen Anwender wurde darüber hinaus im Studierendenportal eine Sicht auf anstehende Wartungsarbeiten an Diensten sowie eine Liste der aktuell ausgefallenen Dienste erstellt.

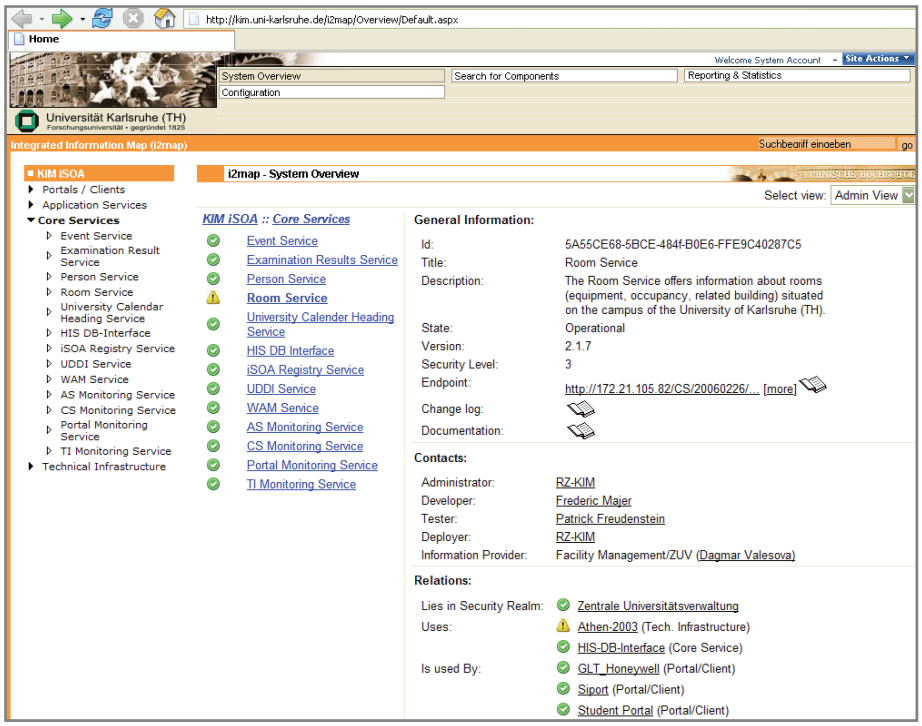


Abb. 5: Administrationssicht des i2map-Portals

6 Verwandte Ansätze

Der folgende Abschnitt soll einen kurzen Überblick über verwandte Ansätze, die sich mit der Unterstützung von Evolution und Betrieb serviceorientierter Architekturen befassen, geben.

Neben Ansätzen zur Modellierung einzelner, domänenspezifischer Aspekte von Systemkomponenten wie beispielsweise das Qualitätsverhalten von Web Services [OASI05a], bestehen auch umfassendere Standards, die sich mit komplexen Systemen und allen darin enthaltenen Komponenten und deren Beziehungen untereinander auseinandersetzen. In

abstrakter Art und Weise spezifiziert die OASIS in ihrem Referenzmodell [OASI06] grundlegende Bausteine und Konzepte serviceorientierter Architekturen, um unabhängig von konkreten Implementierungen und Technologien ein gemeinsames Verständnis und eine klare Terminologie zu etablieren. Andere Ansätze wie [Kirc03] ordnen konkret Systembausteine einzelnen Architekturschichten zu und stellen erste Modelle zu deren Beschreibung zur Verfügung. [WiBW03] stellt darüber hinaus ein Unterstützungswerkzeug mit Sichten auf die modellierte Architektur zur Verfügung, fokussiert aber den Bereich der Krankenhaus-informationssysteme und berücksichtigt somit nicht den organisations- bzw. unternehmens-übergreifenden Aspekt einer serviceorientierten Architektur.

Für den Bereich der Überwachung bietet [OASI05b] ein Framework zum Management von Komponenten, im Speziellen für Web Services. Des Weiteren existieren andere Lösungen für das Monitoring von Portalen oder der technischen Infrastruktur (z.B. ManageEngine, [AdveoJ]). Die Dynamic System Initiative von Microsoft strebt die Vision der ganzheitlichen Unterstützung von Design, Installation und Betrieb von verteilten Systemen an [Turn06]. Über das System Definition Model, das zukünftig durch die Service Modeling Language ersetzt wird, sollen abstrakt gewisse Aspekte von Systemen modelliert und beispielsweise durch den System Center Operations Manager 2007 überwacht werden.

7 Zusammenfassung und Ausblick

Mit der zunehmenden Umstrukturierung der bestehenden IT-Infrastrukturen gemäß dem Paradigma einer serviceorientierten Architektur steigt der Bedarf an dedizierten Ansätzen zur Gewährleistung von Evolution und Betrieb der resultierenden Systeme. Identifizierte funktionale Anforderungen für ein Unterstützungskonzept und -system stellen hierbei die implizite Berücksichtigung beschreibender und überwachender Aspekte dar. Das in diesem Beitrag präsentierte Informationsmodell als Grundlage zur Modellierung der charakteristischen Aspekte serviceorientierter Architekturen in Verbindung mit den Konzepten der Landkarte, die für die verschiedenen Zielgruppen über dedizierte Sichten auf die relevanten Informationen als Orientierungshilfe fungiert, stellt ein Rahmenwerk dar, das den gewünschten Anforderungen begegnet. Eine darauf basierende Implementierung erster Funktionalitäten in den Bereichen Beschreibung und Überwachung und deren Integration in das Landkarten-Portal im Rahmen

des KIM-Projekts an der Universität Karlsruhe (TH) zeigte das praktische Unterstützungspotenzial.

Für die Zukunft ist die Entwicklung weitererführender Funktionalitäten im Bereich der Beschreibung wie die Momentaufnahme (A5) sowie die Simulation (A6) vorgesehen. Des Weiteren soll der Bereich der Überwachung fokussiert werden, damit umfassende Funktionalitäten für den im Rahmen des KIM-Projekts für das zweite Quartal 2007 vorgesehenen Pilotbetrieb des Studierendenportals und aller damit in Beziehung stehender Komponenten zur Verfügung stehen. Dies umfasst vor allem die Entwicklung weiterer Agenten mit dedizierten Überwachungs- und Testmetriken (A9) für bestimmte Komponententypen sowie die damit verbundene Erweiterung der Ereignisauswertung. Darüber hinaus wäre die Integration weiterer Managementfunktionalitäten zur direkten Verwaltung der Komponenten über das Portal sowie die Erarbeitung von Konzepten zur Selbstheilung serviceorientierter Architekturen durch die automatische Rekonfiguration einzelner Komponenten wünschenswert.

Literaturverzeichnis

[ABCF02] Ackermann, J.; Brinkop, F.; Conrad, S.; Fettke, P., et al.: Vereinheitlichte Spezifikation von Fachkomponenten. http://www.wi2.info/downloads/gi-files/MEMO/Memorandum-final-2-44-mit-literatur-Web.pdf. (02.12.2006)

[AdveoJ] AdventNet Inc.: Advent Homepage. http://www.manageengine.com/ (05.12.2006).

[BCEH02] Bellwood, T.; Clément, L.; Ehnebuske, D.; Hately, A.: UDDI Version 3.0, UDDI.org. http://uddi.org/pubs/uddi-v3.00-published-20020719.htm.

[FLMM06] Freudenstein, P.; Liu, L.; Majer, F.; Maurer, A., et al.: Architektur für ein universitätsweit integriertes Informations- und Dienstmanagement. in Tagungsband zur INFORMATIK 2006 - Informatik für Menschen, 36. Jahrestagung der Gesellschaft für Informatik. 2006. Dresden. S. 50-54.

[GalsoJ] Galstad, E.: Nagios Homepage. http://www.nagios.org/ (05.12.2006).

[GeMS06] Gehrke, M., Meyer, M., and Schäfer, W., Eine Rahmenarchitektur für verteilte Lehr- und Lernsysteme - 2006), Arbeitsgruppe CampusSource: http://www.campussource.de/projekte/docs/rahmenarchitektur.pdf (28.11.2006).

[HisG06] His Gmbh, Planung zur neuen Softwaregeneration von HIS, 06.07.2006.

[IBMC05] IBM Corporation: Elements of Service-Oriented Analysis and Design, IBM Homepage. http://www-128.ibm.com/developerworks/webservices/library/ws-soad1/ (29.05.2005).

[Juli05] Juling, W.: KIM Project Homepage, University of Karlsruhe. http://www.kim.uni-karlsruhe.de/ (25.05.2005).

[Kirc05] Kirchner, L.: Cost Oriented Modelling of IT-Landscapes: Generic Language Concepts of a Domain Specific Language. In Workshop on Enterprise Modelling and Information Systems Architectures (EMISA ´05). 2005. Klagenfurt, Austria. S. 166-179.

[MeNG05] Meinecke, J.; Nussbaumer, M.; Gaedke, M.: Building Blocks for Identity Federations. In Fifth International Conference for Web Engineering (ICWE2005), Sydney, Australia 2005. Springer, S. 203-208.

[MGMB06] Meinecke, J.; Gaedke M.; Majer F.; Brändle, A.: Capturing the Essentials of Federated Systems. In 15th International World Wide Web Conference (WWW), Edinburgh, UK 2006.

[Micr06] Microsoft Corporation: Microsoft Homepage. http://www.microsoft.com/mom/evaluation/beta/opsmgroverview.mspx (05.12.06).

[OASI05a] OASIS: Quality Model for Web Services. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsqm. (26.05.2005).

[OASI05b] OASIS: Web Services Distributed Management. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm (28.05.2005).

[OASI06] OASIS: Reference Model for Service Oriented Architecture 1.0. http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.html (05.12.2006).

[PKGS06] Phifer, G., Kenney, L.F., Genovese, Y., Smith, D.M., et al., Hype Cycle for Web Technologies, Research Report. 2006, Gartner Research: Stanford, CT.

[ScDR03] Schmietendorf, A.; Dumke, R.; Reitz, D.: Fettke, P.; Loos, P.: Erfahrungen im Umgang mit der Spezifikation von Web Services. In K. Turowski (Hrsg.): Tagungsband des 3. Workshops Modellierung und Spezifikation von Fachkomponenten. S. 30-45.

[Turn06] Turner, M.: Microsoft System Center takes on enterprise IT management market leaders. http://download.microsoft.com/download/6/A/0/6A0B048D-D2B2-409B-9468-F3749B2DDD00/OvumSummit_SC_MMS06_WEMD_Group.pdf.

[WiBW03] Winter, A.; Brigl, B.; Wendt, T.: Modeling hospital information systems. The revised three-layer graph-based meta model 3LGM. In Methods of information in medicine, Schattauer, Stuttgart 2003. S. 544-551.

Analyse von Risikofaktoren bei der Einführung, Integration und Migration von integrierten Informationssystemen an mittelgroßen deutschen Hochschulen

Bettina Bazijanec, Oliver Gausmann, Sebastian Klöckner, Klaus Turowski

Lehrstuhl für Wirtschaftsinformatik und Systems Engineering
Universität Augsburg
86159 Augsburg
{bettina.bazijanec, oliver.gausmann, sebastian.kloeckner, klaus.turowski}
@wiwi.uni-augsburg.de

Oliver Beran

Zentralverwaltung Universität Augsburg
Universität Augsburg
86159 Augsburg
oliver.beran@zv.uni-augsburg.de

Abstract

Zahlreiche Fallstudien und Strukturierungsansätze dokumentieren sowohl mögliche Vorgehensweisen bei der Einführung integrierter Informationssystemarchitekturen als auch die damit einhergehenden Chancen und Risiken. Die Gestaltung der Architektur selbst wird durch die Aufbauorganisation, die Ablauforganisation sowie die bereits vorhandene IT-Architektur maßgeblich beeinflusst. Hierbei fokussiert sich ein Großteil der veröffentlichten Untersuchungen auf das industrielle Umfeld. Verschiedene Projekte und Forschungsarbeiten zu integrierten Informationssystemen (IIM-Systeme) im Hochschulumfeld dokumentieren jedoch, dass auch im Bereich von Universitäten umfangreiche Projekte zur Einführung von Informationssystemarchitekturen mit service-basierten Ansätzen existieren, die durch organisationsübergreifende Prozesse wie der Nutzung von Value-added Campus Services motiviert sind. Vielfach wird dabei den zu berücksichtigenden Organisationsformen kaum oder gar keine Beachtung geschenkt. Dabei scheint zunächst offensichtlich, dass universitäre Organisationsstrukturen (bezogen auf die Aufbau- und Ablauforganisation) teilweise deutlich von industriellen Strukturen abweichen. In der wissenschaftlichen Literatur finden sich

allerdings kaum Hinweise darauf, in welcher Weise sich universitäre von typischen industriellen Organisationsstrukturen unterscheiden und welche Implikationen dies auf die Einführung, Migration und Integration von Informationssystemen hat. Die Erkenntnisse aus dem DFG-geförderten Forschungsprojekt im Innovationswettbewerb „Leistungszentren für Forschungsinformation – integriertes Informationsmanagement“ werden daher im Rahmen dieses Beitrags zum einen dazu genutzt, die Aufbauorganisation einer typischen mittelgroßen Hochschule strukturiert zu beschreiben, zum anderen werden die während des Forschungsprojekts vollständig dokumentierten Prozesse einer mittelgroßen deutschen Hochschule in Kategorien eingeteilt, um gemeinsam mit den Ausprägungen organisationaler Strukturmuster einen Bogen aufzuspannen, in dem die relevanten organisationalen Einflussfaktoren auf die IT-Architekturgestaltung im Hochschulumfeld erklärt und spezifische Charakteristika für verschiedene ablauf- und aufbauorganisatorische Gegebenheiten herausgearbeitet werden. Diese Charakteristika beschreiben Potentiale und Herausforderungen bei Einführung, Integration oder Migration von IS-Architekturen mit Referenzcharakter.

1 Gestaltung und wissenschaftliche Einordnung des Analyserahmens

Welche Merkmale unterscheiden die Aufbau- und Ablauforganisation mittelgroßer deutscher Hochschulen von denen typischer Industrieunternehmen und welche Hinweise lassen sich daraus auf die Gestaltung integrierter Informationssystemarchitekturen im Hochschulumfeld identifizieren? Diese zentrale Forschungsfrage soll auf Basis der Ist-Analyse eines realen Forschungsprojektes an einer mittelgroßen, deutschen Hochschule beantwortet werden. Ziel des Beitrags ist die Erarbeitung eines Strukturierungs- und Erklärungsmodells in Form eines konzeptuellen Analyserahmens, der in seinen Analyseeinheiten und Dimensionen theoretisch geprägte Konstrukte enthält, die eine Aufstellung von über Einzelfälle hinaus gehenden Aussagen erlauben [Kubi76]. Ein solcher Analyserahmen kann dann als Orientierungshilfe für die weitere Informationssystemgestaltung dienen [Kirs71]. Über den rein theoretischen Erklärungsansatz hinaus ermöglicht der Analyserahmen durch die Verknüpfung mit dem Zielsystem an mittelgroßen Universitäten pragmatische Aussagen und hilft bei zukünftigen Gestaltungsaufgaben [Hach05]. Die Erstellung des Analyserahmens findet zweistufig statt: Zunächst wird ausgehend von Arbeiten Chandlers [Chan62; Chan77; Chan90] die Aufbauorganisation einer mittelgroßen, deutschen Hochschule in Organisationsstrukturtypen

eingeordnet. Dazu werden die einzelnen Einrichtungen sowie die Beziehungen zwischen diesen Einrichtungen den jeweiligen Strukturtypen zugeordnet. Im zweiten Schritt werden die an der Hochschule identifizierten Prozesse in Kernprozesse, direkte Supportprozesse sowie indirekte Supportprozesse eingeteilt. Ausgehend von der Prozesseinteilung Porters in Kernprozesse und unterstützende Prozesse [Port84] betonen verschiedene Autoren die Wichtigkeit der unterstützenden Prozesse (Supportprozesse) für die Kernprozesse [BeKa05; Rump99; Stau01]. Im Rahmen dieses Beitrags sollen die Supportprozesse nochmals in direkte Supportprozesse und indirekte Supportprozesse unterschieden werden. Während die direkten Supportprozesse einen unmittelbaren und relativ kurzfristigen Einfluss auf die erfolgreiche Durchführung der Kernprozesse besitzen, haben die indirekten Supportprozesse nur begleitende und langfristige Einwirkungen auf die Kernprozesse. Diese Dreiteilung wurde im Rahmen des durchgeführten Forschungsprojektes vorgenommen, um eine feingranularere Bewertung hinsichtlich der Merkmale Informationsbedarf, Aktualität und Verfügbarkeit von Prozessen vornehmen zu können. Abb. 6 veranschaulicht den grundsätzlichen Aufbau des Analyserahmens, der durch die Verknüpfung der im folgenden Kapitel erläuterten Organisationsstrukturtypen (M-Form, U-Form und H-Form) mit den drei bereits beschriebenen Prozesstypen entsteht. Die spezifischen Charakteristika beziehen sich auf die typischen Aufgaben bei der Einführung, Integration und Migration rechnergestützter Informationssysteme in den jeweiligen organisatorischen Szenarien.

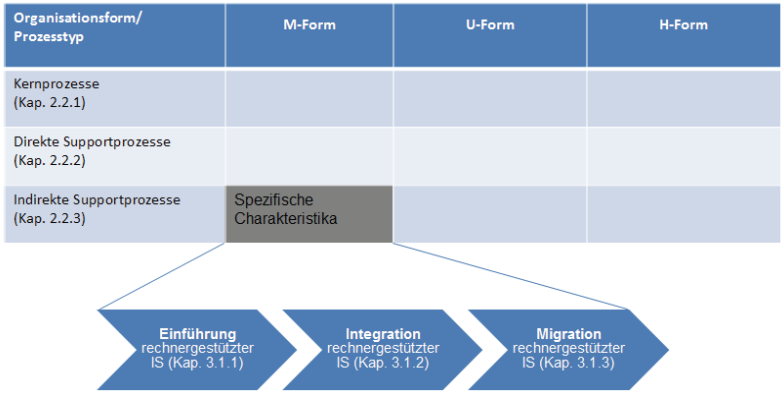


Abb. 6: Grundsätzlicher Aufbau des Analyserahmens

Im Folgenden werden zunächst die verschiedenen Hochschuleinrichtungen und deren Beziehungen zueinander den Organisationsstrukturtypen zugeordnet. Darauf aufbauend wird auf Grundlage der im Projekt untersuchten und dokumentierten Ablauforganisation die Einteilung der Prozesse in Kernprozesse sowie direkte und indirekte Supportprozesse vorgenommen. Abschließend werden die resultierenden, hochschulspezifischen Charakteristika

für die drei Aufgabentypen Einführung, Integration und Migration unter Verwendung des Analyserahmens identifiziert und diskutiert.

2 Analyse der Aufbau- und Ablauforganisation einer mittelgroßen, deutschen Hochschule

Auf den ersten Blick werden Universitäten als direkt vergleichbar mit Industrieunternehmen betrachtet [Hild06]. Diese externe Beurteilung von Universitäten greift allerdings zu kurz, da Universitäten zwar einerseits als öffentlich-rechtliche Organisationen, die dem öffentlichen Dienst- und Haushaltsrecht unterliegen, betrachtet werden können, andererseits aber der im Grundgesetz verankerte Anspruch von „Freiheit von Forschung und Lehre“ und das damit einhergehende Selbstverständnis der akademischen Einheiten diesen große Freiheiten und Entscheidungsbefugnisse einräumt [DeSc06]. Folglich unterscheiden sich die Merkmale von Unternehmen und Universitäten insbesondere durch die interne Beziehungsstruktur der einzelnen Einheiten, aber auch durch die rigiden Vorgaben des Landes sowie des Bundes für öffentlich-rechtliche Organisationen, stark. Die besonderen Merkmale und ihre Auswirkungen auf eine integrierte Informationssystemstruktur werden im Folgenden anhand der Aufbau- sowie der Ablauforganisation dargestellt.

2.1 Struktur der Aufbauorganisation

Die Analyse der Aufbauorganisation und ihre Rolle im Hinblick auf die Einführung eines IIM an Universitäten beruht auf den theoretischen Arbeiten von Chandler [Chan62; Chan77; Chan90]. Chandlers frühe Studien lieferten verschiedene Organisationsstrukturtypen: Zum einen die funktionale Struktur (U-Form), die sich durch eine zentralisierte und funktional-abteilungsorientierte Gestaltung auszeichnet, bei der Entscheidungs- und Koordinationsverantwortung durch eine kleine Gruppe des Topmanagements wahrgenommen wird. Zum anderen die multidivisionale Struktur (M-Form), die durch eine Zerlegung anhand von kundenorientierten, produktorientierten oder geographischen Kriterien in semi-autonome operative Einheiten gekennzeichnet ist. Williamson [Will75; Will85] prägte darüber hinaus einen dritten Organisationsstrukturtyp, die Holding-Struktur (H-Form), die wie die M-Form einen divisionalen Ansatz verwendet, wobei jedoch der Zentrale eine verhältnismäßig schwache Stellung zukommt. Jede dieser drei kurz dargestellten Organisationsstrukturen besitzt im

Hinblick auf ihre Informationsverarbeitungskapazität, Koordinationsfähigkeit sowie ihre Anreizkompatibilität aufgrund ihrer Konfiguration, Koordination und Aufgabenteilung sowohl Stärken als auch Schwächen. Diese sind in Tab. 1 in Anlehnung an Berkovitz [BFFB01] dargestellt und erläutert:

Organisationsstruktur	Informations-Verarbeitungskapazität	Koordinationsfähigkeit zwischen einzelnen Bereichen	Anreizkompatibilität zwischen einzelnen Bereichen
U-Form	Begrenzt durch die Kapazitäten der Zentrale, da die Notwendigkeit der Entscheidungen durch das Topmanagement zu Engpässen führt.	Die Koordinationsfähigkeit aufeinander folgender Aufgaben ist aufgrund der vertikalen Kontrollstrukturen verhältnismäßig stark	Die Bestimmung einheitenorientierter Anreize, die sowohl mit anderen Einheiten als auch mit den Zielen der Gesamtorganisation übereinstimmen, ist schwierig
M-Form	Die dezentralisierte Entscheidungsfindung erhöht die allgemeine Informationsverarbeitungskapazität innerhalb der einzelnen Einheiten	Die starke Position der Zentrale erlaubt eine angemessene einheitenübergreifende Koordination von „oben nach unten"	Stark einheitenorientierte Anreize, d.h. eine problematische Teilzielorientierung, können durch starke Bindungen an die Gesamtorganisation ausgeglichen werden
H-Form	Die dezentralisierte Entscheidungsfindung erhöht die allgemeine Informationsverarbeitungskapazität	Die schwache Position der Zentrale erlaubt nur eine eingeschränkte einheitenübergreifende Koordination von „oben nach unten"	Stark einheitenorientierte Anreize, d.h. eine problematische Teilzielorientierung, sind aufgrund der schwachen Bindungen an die Gesamtorganisation kritisch zu betrachten
Legende	Organisationsstruktur hat negativen Einfluss auf den jeweiligen Faktor	Organisationsstruktur hat leicht positiven Einfluss auf den jeweiligen Faktor	Organisationsstruktur hat stark positiven Einfluss auf den jeweiligen Faktor

Tab. 1: Einfluss der Organisationsstruktur auf Verarbeitungskapazität, Koordinationsfähigkeit und Anreizkompatibilität

Aus den oben dargestellten Organisationsstrukturen können bestimmte Auswirkungen auf die Einführung eines IIM-Systems abgeleitet werden:

- Teilzielorientierungen bzw. Anreizinkompatibilitäten behindern bzw. verhindern die Einführung eines IIM-Systems
- Dezentrale Entscheidungsfindung erhöht die Notwendigkeit eines IIM
- Die Koordinationsfähigkeit zwischen den Bereichen wirkt in direktem Maße auf die Komplexität der Einführung eines IIM

Verwendet man diese oben dargestellten, generischen Organisationsstrukturen für die Analyse der Aufbauorganisation einer mittelgroßen, deutschen Universität, so stellt man fest, dass prinzipiell alle drei Strukturformen anzutreffen sind. So folgt die Struktur der Zentralverwaltung weitestgehend dem Modell der U-Form, zentrale Einheiten wie das Rechenzentrum, die Bibliothek oder das Weiterbildungsinstitut sind Elemente der M-Form und die Fakultäten mit ihren Lehrstühlen entsprechen dem Modell der H-Form. Diese sollen im Folgenden genauer dargestellt werden.

2.1.1 Universitätsleitung und Zentralverwaltung

Die interne Aufbauorganisation der Zentralverwaltung einer Universität kann grundsätzlich als Anwendung der U-Form, d.h. als zentralisierte und funktional-abteilungsorientierte Struktur, charakterisiert werden. Dies zeigt sich unter anderem sehr deutlich an der klaren Abteilungsbildung und dem eindeutigen Liniensystem wie beispielsweise bei [UnAu06] und den daraus resultierenden Dienstwegen. Darüber hinaus weist auch das Verhältnis zu dem verantwortlichen Wissenschaftsministerium klare hierarchische Organisationsstrukturen auf, da durch das Wissenschaftsministerium erlassene Verordnungen und Ausführungsbestimmungen durch die Zentralverwaltung umgesetzt werden müssen. Zwischen der Zentralverwaltung und den zentralen Einheiten muss die Aufbauorganisation als M-Form typisiert werden, da die einzelnen Einheiten einen semi-autonomen Status besitzen und sich nach produkt- und zum Teil kundenorientierten Kategorien gruppieren lassen. So lassen das Rechenzentrum, das Sportzentrum, das Sprachenzentrum als auch die Bibliothek eine klare Produktorientierung erkennen (vgl. beispielsweise [UnAu06b]), während z.B. der Alumniservice eine starke Kundenorientierung aufzeigt. Das Verhältnis zwischen der Zentralverwaltung und den einzelnen Fakultäten muss aufgrund der hohen Freiheitsgrade der Fakultäten und der Bestimmungen des bayerischen Hochschulgesetzes als H-Form eingeordnet werden.

2.1.2 Zentrale Einheiten

Wie bereits in 2.1.1 dargestellt, muss das Verhältnis zwischen Zentralverwaltung und zentralen Einheiten als M-Form charakterisiert werden, wobei die zentralen Einheiten die Rolle der einzelnen Divisionen übernehmen. Basierend auf dem Organisationsstrukturverhältnis zwischen Zentralverwaltung und zentralen Einrichtungen muss auch die strukturelle Verbindung zwischen den einzelnen zentralen Einheiten als Anwendung der M-Form interpretiert werden, da die einzelnen zentralen Einheiten als einzelne Divisionen zueinander im Verhältnis stehen. In Bezug auf die einzelnen Fakultäten der Universität könnte die Verbindung zu der Zentralverwaltung als M-Form oder als H-Form beschrieben werden. Eine Einordnung als H-Form erscheint zweckmäßiger, da die Fakultäten hohe Freiheitsgrade in Bezug auf die Zentralverwaltung besitzen und sich dies folglich auch auf die „Divisionen“ der Zentralverwaltung auswirkt. Unter Zugrundelegung des Verhältnisses zwischen der Zentralverwaltung und den zentralen Einheiten könnte die Organisationsstruktur in Bezug auf die Lehrstühle, ebenso wie bei den Fakultäten, sowohl als M-Form, aber auch als H-Form

charakterisiert werden. Aufgrund der hohen Freiheitsgrade der Lehrstühle erscheint eine Einordnung als H-Form adäquater.

2.1.3 Fakultäten

Wie in 2.1.1 dargestellt, muss das Verhältnis zwischen Zentralverwaltung und den Fakultäten als H-Form bezeichnet werden, wobei die Fakultäten die Rolle der einzelnen, weitestgehend unabhängigen Divisionen übernehmen. Das Organisationsstrukturverhältnis zwischen Fakultäten und zentralen Einheiten muss ebenso als H-Form beurteilt werden. Die zentralen Einheiten nehmen hierbei die Position der semi-autonomen und die Fakultäten die Position der weitgehend unabhängigen Einheiten wahr. Die organisatorische Beziehung zwischen den einzelnen Fakultäten entspricht aufgrund des Beziehungsverhältnisses zur Zentralverwaltung der H-Form, wobei sich die Fakultäten zueinander im Sinne weitestgehend unabhängiger Divisionen beschreiben lassen. Das Verhältnis zwischen Fakultäten und Lehrstühlen wird durch das landeseigene Hochschulgesetz sowie das ebenfalls landesspezifische Hochschulpersonalgesetz bestimmt und kann als H-Form charakterisiert werden.

2.1.4 Lehrstühle

Das Verhältnis der Lehrstühle zu der Zentralverwaltung, den zentralen Einheiten und den Fakultäten ist als H-Form zu beurteilen. Dementsprechend muss auch das Verhältnis der einzelnen Lehrstühle untereinander als H-Form charakterisiert werden, wobei die einzelnen Fakultäten den Status der einzelnen weitestgehend unabhängigen Divisionen übernehmen.
Zusammenfassend lassen sich die einzelnen organisationsstrukturbedingten Beziehungsverhältnisse an einer Hochschule wie folgt zusammenfassen:

Verhältnis zwischen:	Zentralverwaltung	Zentrale Einheiten	Fakultäten	Lehrstühle
Zentralverwaltung	U-Form	M-Form	H-Form	H-Form
Zentrale Einheiten		M-Form	H-Form	H-Form
Fakultäten			H-Form	H-Form
Lehrstühle				H-Form

Tab. 2: Organisatorische Beziehungsverhältnisse zwischen Hochschuleinrichtungen

2.2 Struktur der Ablauforganisation

Basierend auf den oben aufgeführten Definitionen sollen nun die verschiedenen Prozesstypen unter Berücksichtigung der vorhandenen Organisationsstrukturen betrachtet werden.

2.2.1 Kernprozesse

Die Kernprozesse einer Universität sind in erster Linie die Lehr- und Forschungsprozesse, wie es Art. 2 Abs. 1 Satz 4 „Die Universitäten dienen vornehmlich der Forschung und Lehre und verbinden diese zu einer vorwiegend wissenschaftsbezogenen Ausbildung.“ des bayerischen Hochschulgesetzes zum Ausdruck bringt. Art. 9, Satz 1 des BayHSchPG detailliert dies: „Professoren und Professorinnen nehmen die ihrer Hochschule jeweils obliegenden Aufgaben in Wissenschaft, Kunst, Forschung, Lehre und Weiterbildung nach näherer Ausgestaltung ihres Dienstverhältnisses selbstständig wahr“. Aus diesen Vorgaben lässt sich bereits erkennen, dass vornehmlich die Lehrstühle und Fakultäten für diese Kernprozesse verantwortlich sind. Im Folgenden soll der Einfluss der Organisationsstruktur auf diese genauer betrachtet werden.

Lehrprozesse:

Im Rahmen dieser Darstellung werden die Gesamtprozesse zur Durchführung von Vorlesungen, Hausarbeiten, (Projekt-)Seminararbeiten, Diplomarbeiten und Doktorandenseminaren als Lehrprozesse verstanden. Wie bereits dargestellt, nehmen die Professorinnen und Professoren ihre Aufgaben im Hinblick auf die Lehre selbstständig war. Dies entspricht hinsichtlich der einheitenübergreifenden Organisationsstruktur weitgehend den Eigenschaften der H-Form, da die Zentrale, hier die Universitätsleitung, aufgrund der gesetzlichen Vorgaben nur einen relativ geringen bzw. indirekten Einfluss auf die entsprechenden Prozesse (Lehrorganisation) bzw. Produkte (Lehrveranstaltungen) besitzt. In Hinsicht auf die einheiteninterne Struktur sollte eine hierarchische Organisationsstruktur existieren, da die Professorinnen und Professoren die direkten disziplinarischen Vorgesetzten ihrer Mitarbeiter sind. Diese Vermutung wurde auch durch die Prozessanalysen an den verschiedenen Einrichtungen der untersuchten Universität bestätigt. Gleichzeitig stellte sich allerdings heraus, dass, obwohl eine weitgehende Freiheit im Hinblick auf die Prozessgestaltung möglich ist, sich die verschiedenen Vorgehensmodelle durchaus ähneln und weitgehend ähnliche Strukturen aufweisen. Die Vorgehensmodelle selbst besitzen dabei außerordentlich leistungsfähige Eigenschaften, was sich beispielsweise an der zumeist äußerst effizienten Veranstaltungsorganisation oder auch der internen Aufteilung der einzelnen Prozessverantwortlichkeiten zeigte. Dies war insbesondere auf die vorhandenen hierarchischen Strukturen sowie die überschaubare Größe der Organisationseinheiten zurückzuführen. Parallel hierzu weist die einheitenübergreifende H-Form allerdings weitere Merkmale im Hinblick auf den hohen Koordinationsaufwand sowie Anreizinkompatibilitäten zwischen den Bereichen auf. Diese Merkmale konnten im Verlauf der Prozessanalysen

weitgehend bestätigt werden. Dies ist unter anderem der Grund für eine relativ geringe Anzahl einheitenübergreifender sowie interdisziplinärer Lehrveranstaltungen, obgleich dies im Sinne einer ganzheitlichen Lehre wäre. Der Einsatz eines IIM-Systems kann hierbei insbesondere im Bereich der Koordinationsaufwandsminimierung äußerst sinnvoll sein, da sowohl der Kenntnisstand über weitere Veranstaltungsinhalte als auch die direkte operative Koordination der Veranstaltungen verbessert wird. Gleichzeitig könnte die Einführung eines IIM-Systems aufgrund eventuell bestehender Anreizinkompatibilitäten, insbesondere hinsichtlich entstehender Informationstransparenzen, mit gewissen Schwierigkeiten verbunden sein.

Forschungsprozesse:

Im Rahmen dieser Betrachtungen werden die Gesamtprozesse der Erstellung von Veröffentlichungen, der Durchführung von Reviews, der Anfertigung von Forschungsanträgen sowie die Bearbeitung von Forschungsvorhaben verstanden. Auch diese Aufgaben werden vornehmlich von den Professorinnen und Professoren sowie ihren Mitarbeiterinnen und Mitarbeitern wahrgenommen. Dementsprechend muss auch hier von einer hierarchischen Struktur im einheiteninternen Bereich sowie einer H-Form im einheitenübergreifenden Bereich ausgegangen werden. Diese Annahmen wurden im Rahmen der durchgeführten Prozessanalysen bestätigt. Parallel hierzu zeigte sich, dass viele der untersuchten Einheiten bereits Ansätze eines IIMs besitzen. So verfügen beispielsweise einige Einheiten über gemeinsame Referenzbibliotheken für die Erstellung von Veröffentlichungen. Im Gebiet einheitenübergreifender Forschungsprozesse zeigten sich vergleichbare Merkmale wie im Bereich der Lehrprozesse. So sind zwar einige einheitenübergreifende Forschungsprozessinstanzen vorhanden, jedoch sind diese mit einem hohen Koordinationsaufwand verbunden. Darüber hinaus werden manche einheitenübergreifende Forschungsprozessinstanzen aufgrund unterschiedlicher Teilzielorientierung im Hinblick auf Forschungsgebiete nicht realisiert. Der Einsatz eines IIMs kann auch im Aufgabenkreis der Forschungsprozesse sinnvolle Unterstützung liefern. So könnten durch eine Integration von Referenzbibliotheken Skaleneffekte realisiert werden. Ferner würde bspw. eine gemeinsame Kooperationsplattform sowohl der einheiteninternen als auch einheitenübergreifenden Forschung sehr behilflich sein. Gleichzeitig muss allerdings hier, wie auch im Bereich der Lehrprozesse, bei der Einführung eines IIMs aufgrund der eventuell vorhandenen Anreizinkompatibilitäten sowie des zu erwartenden Umstellungsaufwands innerhalb der Einheiten mit gewissen Schwierigkeiten gerechnet werden.

2.2.2 Direkte Supportprozesse

Die erfolgreiche Umsetzung der Kernprozesse ist, wie bereits dargestellt, nur durch die Unterstützung der notwendigen Supportprozesse möglich. Dies ist auch an Universitäten der Fall. So ist weder eine erfolgreiche Lehrveranstaltung noch eine effiziente Forschung ohne eine adäquate Personal- und Raumplanung möglich. Auch hier lässt sich, wie bei den Kernprozessen, vermuten, dass innerhalb der Organisationseinheiten aufgrund der hierarchischen Strukturen relativ gute Koordinations- und Anreizmechanismen vorhanden sind. Zwischen den Organisationseinheiten sollten aufgrund der vorhandenen M- und H-Formen allerdings Optimierungspotentiale im Hinblick auf Koordinations- und Anreizformen erkennbar werden. Diese Hypothesen wurden durch die durchgeführten Prozessanalysen bestätigt. So funktionieren beispielsweise die einheiteninternen Personalplanungsprozesse für Veranstaltungen weitestgehend reibungslos, da diese zwischen den Professoren und Mitarbeitern zumeist direkt abgestimmt werden und im Rahmen der Prozessanalysen als problemlos bezeichnet wurden. Bei der einheitenübergreifenden Raumplanung kommt es zum einen aufgrund fehlender oder unvollständiger Information zu hohen Koordinationsaufwand und in Einzelfällen zu Fehlplanungen, zum anderen aufgrund unterschiedlicher Teilziele der einzelnen Einheiten zu ineffizienter Ressourcenauslastung. Auch war erkennbar, dass auftretende Schwierigkeiten der Kernprozesse in vielen Fällen auf Hindernisse innerhalb der direkten Supportprozesse, wie zum Beispiel Raumplanung, Prüfungsabwicklung oder auch anderweitige Koordinationsprobleme, zurückzuführen sind. Darüber hinaus stellte sich heraus, dass die Verwalter der für den Prozess wichtigsten Ressourcen einen erheblichen Einfluss auf den Prozessablauf haben und somit organisationsstrukturbedingte Koordinationsstrukturen beeinflussen können. So können teilweise vorhandene Hindernisse aufgrund der existierenden Organisationsstrukturen durch persönliche Kontakte zu den ressourcenverantwortlichen Aufgabenträgern vermindert bzw. aufgehoben werden. Hinsichtlich einer möglichen Verwendung eines IIM-Systems deuten diese Ergebnisse insbesondere im Bereich des bereichsübergreifenden Informationsflusses und des Koordinationsaufwands auf ein hohes Optimierungspotential hin, da ein IIM die aktuellen Schwächen der fehlenden oder unvollständigen Information als auch der ineffizienten Ressourcenauslastung beheben würde. Aufgrund der vorhandenen Teilzielvarianten, aber viel mehr noch durch die Veränderung der Informations- und Kontrollstrukturen als Resultat der steigenden Informationstransparenz, ist mit Hindernissen und Akzeptanzrisiken bei der Umsetzung eines IIM-Systems zu rechnen.

2.2.3 Indirekte Supportprozesse

Wie dargestellt, haben die indirekten Supportprozesse nur begleitende und langfristige Einwirkungen auf die Kernprozesse. Gleichwohl ist ohne die wirksame Funktionsfähigkeit der indirekten Supportprozesse die Durchführung der Kernprozesse nicht möglich. Zu dieser Prozessart werden im Rahmen dieser Betrachtung insbesondere die Infrastrukturprozesse, wie zum Beispiel die Schlüsselverwaltung, als auch die allgemeinen Verwaltungsprozesse, wie die der Haushalts- und Personalprozesse, gezählt. Diese Prozessarten werden hauptsächlich durch die zentrale Verwaltung wahrgenommen. Basierend auf den vorhandenen Strukturbeziehungen zwischen Zentralverwaltung, zentralen Einheiten sowie den Fakultäten und Lehrstühlen muss davon ausgegangen werden, dass die Prozesse vornehmlich durch die Eigenschaften der M- und H-Form beeinflusst werden. Diese Annahme konnte im Verlauf der Prozessanalysen jedoch nicht bestätigt werden. Vielmehr zeigte es sich, dass die Eigentümer der für den Prozess wichtigsten Ressource maßgeblichen Einfluss auf den Prozessablauf ausüben können. Da diese vornehmlich in der Zentralverwaltung verortet sind, zeigten sich die Eigenschaften der U-Form, die teils durch gesetzliche Regelungen des Landes sowie des Bundes unterstützt werden. Dies offenbart sich unter anderem in den vorhandenen Formularen, Fristen sowie Informationswegen. Im Hinblick auf ein IIM ist dies insbesondere im Bereich der Redundanzvermeidung sowie der Steigerung der Informationstransparenz und -verfügbarkeit empfehlenswert.

3 Identifikation spezifischer Charakteristika unter Verwendung des Analyserahmens

Basierend auf den oben dargestellten Kriterien der Aufbau- und Ablauforganisation an deutschen Hochschulen lassen sich im Hinblick auf die Einführung, Integration und Migration eines IIM-Systems bestimmte Potentiale und Risiken ableiten. Unter Einführung von IIM-Systemen wird im diesem Beitrag vornehmlich davon ausgegangen, dass existierende, nicht oder nur begrenzt rechnergestützte Informationssysteme bzw. -prozesse, wie beispielweise die Erstellung eines Vorlesungsverzeichnisses, durch rechnergestützte Informationssysteme, wie beispielsweise ein Veranstaltungsmanagementsystem, weitgehend ersetzt und automatisiert werden. Als Integration rechnergestützter Informationssysteme wird in diesem Beitrag die

Zusammenführung bestehender und autonom arbeitender Informationssysteme mit dem Ziel einer einheitlichen, redundanzfreien und aktuellen Daten- und Funktionsbasis verstanden [Buss02]. Hierbei können sowohl konsolidierte als auch föderative Konzepte in Betracht gezogen werden. Die Migration eines integrierten Informationsmanagementsystems beinhaltet schließlich die Erweiterung eines vorhandenen integrierten Informationssystems, die den Anwendern zusätzliche Informationen bzw. Funktionalitäten zur Verfügung stellen. Die in Tab. 3 zusammengefassten Merkmale werden im Folgenden genauer dargestellt und um weitere Beispiele ergänzt.

Organisationsform / Prozesstyp	U-Form		M-Form		H-Form	
Kernprozesse (Kap. 2.2.1)	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	gemeinsame Referenzbibliothek Einheiten intern Aufwandsreduktion Keine Installation und Schulung Datenübernahme Umstellungsaufwand ++	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Fortbildungsmanagementsystem Zentrale Einheiten - Zentralverwaltung Informationsverfügbarkeit keine Akzeptanzprobleme Datenübernahme Umstellungsaufwand +	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Veranstaltungsinformationssystem Lehrstuhl - Lehrstuhl Interdisziplinäre Aktivitäten Anreizinkompatibilitäten Akzeptanzprobleme Mehraufwand, Nutzenverlust Desintegration +
Direkte Supportprozesse (Kap. 2.2.2)	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Gruppenkalender Einheiten intern Informationsverfügbarkeit, Planbarkeit Datenaktualität Installation und Schulung nicht notwendig Umstellungsaufwand ++	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Help Desk Zentrale Einheit - Zentralverwaltung Prozessstörungsminimierung Akzeptanzprobleme Anforderungsvielfalt Strukturelle Komplexität Umstellungsaufwand +	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Raumplanung Lehrstuhl –Fakultät Vollständige Information hoher Koordinationsaufwand Informationstransparenzen ggf. Vielzahl Systeme Desintegration +++
Indirekte Supportprozesse (Kap. 2.2.3)	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Reisekostenabrechnung Zentralverwaltung – Lehrstuhl Prozessgeschwindigkeit gering Systemkomplexität gering gering ++	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Infrastruktursysteme Zentrale Einheit - Zentralverwaltung Datenintegrität technischer Natur Akzeptanzprobleme Kompatibilität divergierende Altsysteme +	Beispiel: Beziehung: Vorteil: Hindernisse: Einführung: Integration: Migration: Häufigkeit:	Struktur häufig durch gesetzliche Vorgaben überlagert

Tab. 3: Organisationsstruktur- und prozesstypbedingte Potentiale und Risiken als Grundlage für Umsetzungsstrategien eines integrierten Informationsmanagements an Hochschulen

3.1 Einführung rechnergestützter Informationssysteme

Die Neueinführung rechnergestützter Informationssysteme bedeutet zumeist eine Ablösung existierender, nicht rechnergestützter Informationssysteme. Diese Umstellung auf rechnergestützte Informationssysteme ist häufig mit einer Umverteilung der Arbeitslast innerhalb als auch zwischen einzelnen Organisationseinheiten verbunden, sodass die bestehenden Organisationsstrukturen und Prozesstypen erheblichen Einfluss auf die erfolgreiche Einführung solcher Systeme haben können. Im Falle einer hierarchischen Organisationsstruktur ist eine Systemeinführung mit geringeren Schwierigkeiten verbunden, da das Management in kritischen Fällen direkte Anweisungsbefugnis besitzt und die Unterstützung aller Beteiligten gewährleisten kann. Diese Hypothese konnte sowohl im Rahmen der Analysen aber auch auf Basis früherer Systemeinführungen bestätigt werden. Wenn jedoch eine Organisationsstruktur der H-Form als Rahmenbedingung einer Systemneueinführung vorliegt,

so gestaltet sich die Implementierung solcher Systeme aufgrund eventuell vorhandener Anreizinkompatibilitäten sowie komplexerer Koordinationsmechanismen deutlich schwieriger. Folglich müssen in diesem Fall die Teilziele der einzelnen beteiligten Einheiten berücksichtigt und entsprechend kompatible Anreizsysteme bzw. Anreize geschaffen werden. Dabei kann es von entscheidender Bedeutung sein, dass der Aufgabenträger, der die bedeutendsten Ressourcen der betroffenen Prozesse verwaltet, die Einführung eines solchen Informationssystems unterstützt, da er im Zweifelsfall seine Entscheidungskompetenz über diese Ressourcen im Sinne einer erfolgreichen Systemeinführung verwenden kann. Gleichzeitig muss der Koordination der einzelnen Einheiten besonderes Augenmerk geschenkt werden, da Fehlsteuerungen einen Korrekturaufwand bei allen Beteiligten und damit ggf. Akzeptanzprobleme verursachen können. Im Hinblick auf die Existenz einer Organisationsstruktur der M-Form ist aufgrund der analogen Anreizkompatibilitätsstrukturen ein vergleichbares Muster wie bei der H-Form zu erwarten. Allerdings bestehen aufgrund der Kontrollstrukturen der Zentrale geringe Risiken im Bereich der Koordination. Gleichzeitig sollte aber auch hier die Unterstützung des bedeutendsten Ressourcenverwalters sichergestellt sein, um diese im Konfliktfall zielführend nutzen zu können. Diese These konnte jedoch bisher weder im Rahmen der Prozessanalysen noch auf Basis vergangener Erfahrungen bestätigt werden.

3.2 Integration rechnergestützter Informationssysteme

Die Integration existierender Systeme unterscheidet sich grundlegend von der Neueinführung rechnergestützter Informationssysteme. Dies ist vor allem dadurch begründet, dass bei einer Neueinführung vollständige Anwendungssysteme mit geringem bzw. keinem Adaptionsaufwand zum Einsatz gebracht werden können. Bei der Integration bestehender Systeme hingegen müssen sowohl Daten als auch Funktionen, die zum Teil tief in bestehenden Systemen verankert sind, integriert werden. Dies ist nur durch grundlegende Veränderung bzw. Abschaltung einzelner Teilsysteme möglich, was jedoch in hohem Maße sowohl von der bestehenden Organisationsstruktur sowie den betroffenen Prozessen abhängig ist, da die entsprechenden Verantwortlichen in beiden Fällen diesem Vorgehen zustimmen müssen.

Bei einer hierarchischen Organisationsstruktur (U-Form) sollte es zu geringen koordinations- und anreizorientierten Schwierigkeiten kommen, da das Top-Management über die Integration der verschiedenen Systeme entscheidet und aufgrund der gegebenen Kontrollstrukturen auch über die Anpassung oder Abschaltung der Systeme und Prozesse bestimmen kann. Diese

Annahme wurde durch verschiedenste Integrationsprojekte innerhalb einzelner Lehrstühle bestätigt. Für den Fall des Vorhandenseins einer Organisationsstruktur in H-Form erzeugt die Integration verschiedener Systeme äußerst komplexe Herausforderungen, da es sowohl zu Koordinationsschwierigkeiten als auch zu Anreizinkompatibilitäten kommen kann. Hierbei ist diese Merkmalsausprägung die wohl am häufigsten auftretende Form an Universitäten. Unter der Annahme, dass jede der betroffenen Einheiten der Integration bereits eigene Systeme besitzt, würde die Integration bei allen Beteiligten einen direkten Mehraufwand aufgrund der notwendigen Veränderungen der Daten- und Funktionsstrukturen verursachen. Gleichzeitig besteht die Gefahr, dass durch die Integration Funktionalitäten einzelner Systeme verloren gehen, da diese nicht in ein Gesamtkonzept übernommen werden können. Dies führt bei den betroffenen Einheiten zu einem Nutzenverlust aufgrund der Integration, sodass sogar negative Anreize in Hinblick auf die Integration entstehen können. Gleichzeitig besteht die Gefahr, dass nicht ein, sondern mehrere Ressourcenverwalter existieren, sodass eine Ausnutzung der Entscheidungskompetenzen im Sinne der Integration nur erschwert möglich ist. Somit müsste sich die Integration im schlechtesten Fall auf ein föderatives Datenkonzept beschränken, welches auch das unveränderte Fortbestehen der bereits existierenden Systeme erlaubt. Diese Fragestellung wurde im Rahmen der Konzeption eines integrierten Raumplanungssystems genauer untersucht und bestätigt. Im Hinblick auf die Existenz einer divisionalen Organisationsstruktur an Universitäten sollten die durch eine Integration verursachten Herausforderungen im Vergleich zu Organisationsstrukturen der H-Form einen geringeren Komplexitätsgrad aufweisen, da die einzelnen Einheiten aufgrund ihrer unterschiedlichen kunden- oder produktorientierten Ausrichtung, abgesehen von gemeinsam benötigten Basisdaten und -funktionen, nur geringe Berührungspunkte aufweisen. Zum anderen kann die Zentrale in Konfliktfällen durch die ihr innewohnende Autorität zwischen den Einheiten vermitteln. Diese These konnte allerdings im Rahmen der Prozessanalysen bisher noch nicht belegt werden.

3.3 Migration rechnergestützter Informationssysteme

Die Migration bestehender rechnergestützter Informationssysteme sollte im Vergleich zu der Einführung und der Integration rechnergestützter Informationssysteme minimale Fragestellungen aufwerfen, da bereits ein integriertes Informationssystem einschließlich eines entsprechenden Verantwortlichen existiert. Dieser kann bei Bedarf prinzipiell ohne Rücksichtnahme auf die vorhandenen Organisationsstrukturen und deren Einheiten die

Umstellung von einem Altssystem auf ein neues System veranlassen. Jedoch muss hierbei darauf geachtet werden, dass alle angeschlossenen Einheiten das neue System problemlos verwenden können, da ansonsten die Gefahr der Desintegration aufgrund von Akzeptanzschwierigkeiten besteht.

4 Fazit und weiterer Forschungsbedarf

In diesem Beitrag wurden die unterschiedlichen Organisationsstrukturtypen sowie die grundlegenden Prozesskategorien der Ablauforganisation dargestellt und ihr Auftreten an deutschen Universitäten analysiert. Die Ergebnisse dieser Analyse zeigen, dass sich der gesamtorganisatorische Aufbau deutlich von in Unternehmen häufig vorzufindenden hierarchischen Strukturen unterscheidet. Diese Unterschiede üben einen nicht zu vernachlässigenden Einfluss auf die Prozesse einer Universität sowie die unterstützenden Informationssysteme aus und müssen daher bei der Einführung, Integration und Migration von Informationsmanagementsystemen mit in Betracht gezogen werden. Der Beitrag liefert hierzu einen ersten Analyserahmen, der in weiteren Forschungsarbeiten weiter ausgebaut werden wird. Insbesondere müssen bei der Analyse auch quantitative Faktoren, wie die Anzahl der betroffenen Prozessinstanzen, die potentiellen Kosteneinsparungen, aber auch qualitative Merkmale, wie beispielsweise der Variantenreichtum einzelner Prozesse oder die zeitliche Stabilität als Kriterien, berücksichtigt werden. Darüber hinaus muss die Gültigkeit der dargestellten Eigenschaften und Einflussfaktoren für artverwandte Institutionen wie Fachhochschulen oder Berufsakademien sowie der Einfluss der Größe einer Institution auf die dargestellten Faktoren überprüft werden.

Literatur

[UnAu06] Augsburg, U.: Organisationsstruktur der Universität Augsburg. Augsburg, 2006.

[UnAu06b] Augsburg, U. (Hrsg.): Rechtssammlung der Universität Augsburg. http://www.verwaltung.uni-augsburg.de/sammlung/download/100.pdf, Abruf 2006-12-14.

[BeKa05] Becker, J.; Kahn, D.: Der Prozess im Fokus. In Becker, J.; Kugeler, M.; Rosemann, M.: Prozessmanagement. Springer, Berlin 2005. S. 3-16.

[BFFB01] Berkovitz, J.; Feldman, M.; Feller, I.; Burton, R.: Organizational Structure as Determinant of Academic Patent and Licensing Behavior: An Exploratory Study of Duke, Johns Hopkins, and Pennsylvania Universities. In: Journal of Technology Transfer 26, S. 21-35.

[Buss02] Bussler, C.: B2B Integration Technology Architecture. 4th Int'l Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems. 2002.

[Chan62] Chandler, A. D.: Strategy and structure: Chapters in the history of the American industrial enterprise (1962), S. 463.

[Chan77] Chandler, A. D.: The visible hand : the managerial revolution in American business. Harvard Univ. Press, Cambridge 1977.

[Chan90] Chandler, A. D.: Scale and scope: the dynamics of industrial capitalism. Belknap Press of Harvard Univ. Press, Cambridge 1990.

[DeSc06] Degkwitz, A.; Schirmbacher, P.: Informationsinfrastrukturen im Wandel. Informationsmanagement an deutschen Universitäten. 1. Aufl., Deutsche Initiative für Netzwerkinformation e.V. (DINI), Göttingen 2006.

[Hach05] Hach, H.: Evaluation und Optimierung kommunaler E-Government Prozesse. Dissertation, Universität Flensburg. Flensburg, 2005.

[Hild06] Hildebrand, I. (Hrsg.): "Unternehmen Hochschule": UNIK sieht Erfolge bestätigt. http://idw-online.de/pages/de/news186725, Abruf 2006-11-24.

[Kirs71] Kirsch, W.: Entscheidungen in Organisationen. Bd. 3, Wiesbaden 1971.

[Kubi76] Kubicek, H.: Heuristische Bezugsrahmen und heuristisch angelegte Forschungsdesigns als Elemente einer Konstruktionsstrategie empirischer Forschung. Berlin 1976.

[Port84] Porter, M.: Wettbewerbsstrategie: Methoden zur Analyse von Branchen und Konkurrenten (Competitive strategy). 2. Aufl., Campus-Verlag, Frankfurt/Main 1984.

[Rump99] Rump, F. J.: Geschäftsprozeßmanagement auf der Basis ereignisgesteuerter Prozeßketten. Teubner Verlag, 1999.

[Stau01] Staud, J. L.: Geschäftsprozeßanalyse. Springer, Berlin 2001. S. XI, 377.

[Will75] Williamson, O. E.: Markets and Hierarchies: Analysis and Antitrust Implications. A Study in the Economics of Internal Organization. Free Press, New York 1975.

[Will85] Williamson, O. E.: The economic institutions of capitalism. The Free Press, New York 1985.

Teil II

Identitätsmanagement

Integriertes Informationsmanagement an einer großen Universität

Konzeption einer Informations-Infrastruktur, erste Erfahrungen mit den verwendeten Technologien sowie Überlegungen zu deren Einführung

Gunnar Dietz, Martin Juhrisch, Dirk Kußmann,

Frank Schumacher, Stanislav Stoytchev, Martin Stracke

DFG-Projekt MIRO
Westfälische Wilhelms-Universität Münster
48149 Münster
{gunnar.dietz, juhrisch, dirk.kussmann, stanislav.stoytchev,
frank.schumacher, martin.stracke}@uni-muenster.de

Abstract

Effektive wie effiziente Versorgung und Verwaltung von Informationen gehören zu den wesentlichen Grundbedingungen für eine zukunftsfähige Forschung und Lehre an Hochschulen. Für den Erfolg in Wissenschaft und Bildung spielt die schnelle und einfache Verfügbarkeit von Informationen eine ebenso wichtige Rolle wie ihre sach- und fachgerechte Verwertbarkeit.

Die Westfälische Wilhelms-Universität Münster (WWU) konnte mit dem durch die Deutsche Forschungsgemeinschaft (DFG) geförderten Projekt *MIRO* (Münster Information System for Research and Organization) die Entwicklung eines umfassenden Systems für das integrierte Informationsmanagement forcieren, das wissenschaftliche und organisatorische Informationen mit einheitlichem Zugriff und individuellem Verteilungsmodus integriert bereitstellt**.** Der vorliegende Bericht informiert über die Inhalte und Ziele des Projektes, skizziert die bisherigen konzeptionellen Arbeiten zum Aufbau einer Informations-Infrastruktur und fasst erste Erfahrungen mit den verwendeten Technologien sowie Anmerkungen zur Einführung und Inbetriebnahme der neuen Infrastruktur und den darauf basierenden Anwendungen zusammen.

Im Rahmen dieses Beitrags stehen konkrete Aspekte bei der Umsetzung dieses sehr umfangreichen Vorhabens im Vordergrund; auf eine Zusammenstellung und Diskussion der wissenschaftlichen Grundlagen wird bewusst verzichtet.

1 Inhalte und Ziele des Projekts MIRO

In dem seit November 2005 im Rahmen des Förderprogramms *Leistungszentren für Forschungsinformation*[12] von der Deutschen Forschungsgemeinschaft (DFG) geförderten Projekt *MIRO* (Münster Information System for Research and Organization) wurde zunächst schwerpunktmäßig mit dem Aufbau einer Informations-Infrastruktur für integriertes Informationsmanagement begonnen. Zu ihren Kernkomponenten zählen ein umfassendes *Identitätsmanagement*, die Bereitstellung von *effizienten Arbeitsumgebungen* mittels moderner Portaltechnologie, ein *Single Sign-On (SSO)* bzw. *Accessmanagement* sowie eine Universitätssuchmaschine, welche moderne Verfahren des *Information Retrieval* bereitstellt. Flankiert wird der Aufbau dieser Komponenten von tiefgreifenden Maßnahmen zur *Sicherheit*, *Qualität* und *Verlässlichkeit* der informationsverarbeitenden Systeme, damit u. a. eine hohe Verfügbarkeit der neuen Infrastruktur von Beginn an gewährleistet ist und sich bei den zukünftigen Nutzern entsprechendes Vertrauen aufbauen kann. Erste Anwendungen mit Beispielcharakter, welche die neue Informations-Infrastruktur nutzen, werden zur Verankerung der Infrastruktur-Komponenten in die IT-Anwendungslandschaft der Universität beitragen.

Ziel von MIRO ist die möglichst vollständige Erschließung und (rollenspezifische) Bereitstellung von wissenschaftlichen und organisatorischen Informationen, die an der Universität Münster vorliegen, sowie von weiteren, externen wissenschaftlichen Informationsquellen in Zusammenarbeit mit Kooperationspartnern wie z. B. der Universitätsbibliothek Bielefeld oder dem Hochschulbibliothekszentrum (hbz) in Köln. Die erschlossenen Informationen können mit Hilfe der in effiziente Arbeitsumgebungen integrierten Anwendungen bedarfsgerecht zusammengeführt, bereitgestellt und vor allem schnell und zielgerichtet verfügbar gemacht werden, ohne dass der jeweilige Nutzer Detailwissen über die Struktur der Universität oder den Ablageort bestimmter Daten besitzen muss. Wir sind aufgrund der bisherigen Erfahrungen heute sicher, dass es uns gelingt, ein nutzerorientiertes Informationsmanagement aufzubauen, welches nicht zuletzt auch für die Ausbildung der Studierenden von großer Bedeutung sein wird.

[12] siehe http://www.dfg.de/forschungsfoerderung/wissenschaftliche_infrastruktur/lis/projektfoerderung/foerderziele/leistungszentren.html

2 Konzeption der Informations-Infrastruktur und erste Erfahrungen mit den verwendeten Technologien

2.1 Identitätsmanagement

Ein zentrales Identitätsmanagement bildet eine wichtige Grundlage für den von uns gewählten Ansatz für ein integriertes Informationsmanagement. Das Ziel, einem Benutzer Inhalte unter Berücksichtigung seiner Rechte und Rollen zur Verfügung zu stellen, kann nur erreicht werden, wenn zuverlässige, aktuelle Benutzerdaten vorliegen. Die an der WWU bislang eingesetzte, 15 Jahre alte Benutzerverwaltung entsprach vor diesem Hintergrund nicht mehr den Anforderungen. Primäres Ziel der Einführung des Identitätsmanagements ist es, jeder Person genau eine, eindeutige (digitale) Identität in der IT-Landschaft zuzuordnen. Gerade im Hinblick auf die Realisierung eines Single Sign-On, aber auch in Hinblick auf die Datensicherheit ist dies unerlässlich. Des Weiteren bietet das Identitätsmanagement (siehe Abb. 1) eine rollengesteuerte Zugriffskontrolle und unterstützt das Management von Identitäten und Accounts durch ein Workflow-System.

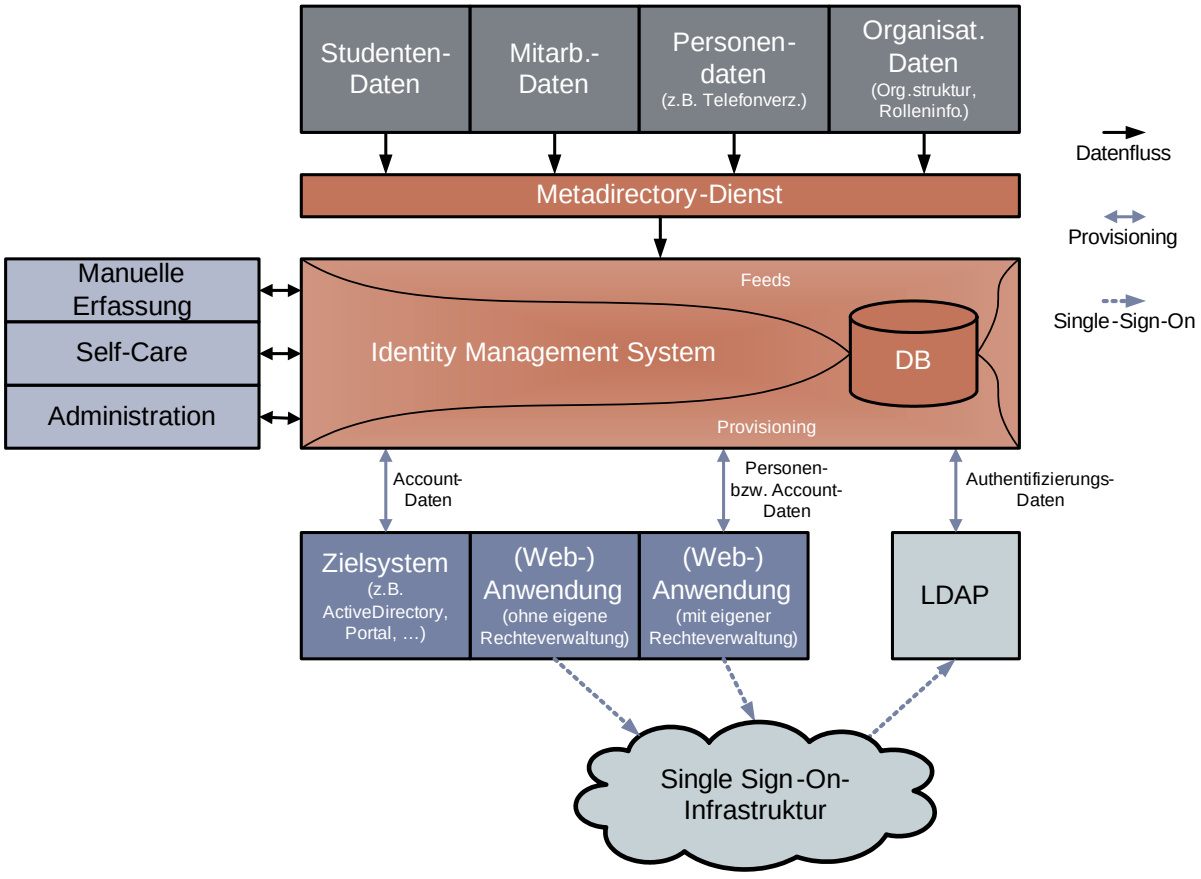


Abb. 1.: Aufbau des Identitätsmanagements

Das Identitätsmanagement-System wird aus verschiedenen Quellen mit Personendaten und organisatorischen Daten gespeist (*Feeds*). Die Rollen einer Identität können sich automatisch aus den Attributen der Identität ergeben, aber auch manuell hinzugefügt werden. Diese Rollen bilden die Entscheidungsgrundlage für das *Provisioning*, d. h. die automatische Versorgung der Zielsysteme mit Accountdaten. Außerdem können auf manuellem Wege weitere Personen (z. B. Gäste der Universität) oder zusätzliche Daten zu bestehenden Personen erfasst werden. Ebenso bietet es den Benutzern *Self-Care-Mechanismen*, wie z. B. Dateneinsicht (im Sinne der informationellen Selbstbestimmung), Datenänderungen oder Beantragung von zusätzlichen Accounts.

Im Rahmen einer Konsortiallizenz des Landes NRW wurde der IBM Tivoli Identity Manager (ITIM) lizenziert. Die WWU beteiligt sich im Rahmen dieser Lizenz an einem landesweiten Projekt zum Identitätsmanagement. Zurzeit befinden wir uns noch in der Testphase mit dem ITIM, der produktive Einsatz wird zum zweiten Quartal 2007 erfolgen.

Es hat sich herausgestellt, dass die Einführung eines Identitätsmanagements trotz der Unterstützung durch eine mächtige Software sehr aufwändig ist. Die Rechte, die an einer Hochschule die Zugriffserlaubnis zu Ressourcen oder Informationen regeln, sind vielfältig und hochkomplex. In der bestehenden Benutzerverwaltung werden zur Zeit ca. 2000 Benutzergruppen mit unterschiedlichen Rechten gepflegt, eine im Vergleich mit anderen Universitäten hohe Zahl, welche die Bedürfnisse des bereits über viele Jahre zentral betriebenen Verfahrens widerspiegelt.

Ziel des neu einzuführenden Rollenkonzepts zur Steuerung dieser Rechte ist es, mit einer vergleichsweise kleinen Zahl von Rollen auszukommen, damit u. a. der Wartungsaufwand überschaubar bleibt. Dieser Ansatz bedingt zunächst, dass detaillierte Rechtestrukturen weiterhin außerhalb des Identitätsmanagement-Systems abgehandelt werden müssen; hierzu wird in einem ersten Schritt der Teil der alten Benutzerverwaltung, mit dem die vorhandenen Gruppen gepflegt werden, parallel zum ITIM weiter betrieben. Der Umstand, dass Benutzer teilweise mehrere Kennungen auf *einem* Zielsystem besitzen (z. B. für eine zusätzliche Rolle als Administrator), sorgt für zusätzliche Schwierigkeiten bei der Konzeption, da die eingesetzte Software diese Funktionalität so nicht vorsieht und daher von uns entsprechend angepasst werden musste.

Die Beachtung von Datenschutzvorschriften führte zu einem außerordentlichen organisatorischen Aufwand, der weit höher war als zunächst geplant. Zusätzlich zu einer bereits vorliegenden, ausführlichen Datenschutzvorabkontrolle musste die Nutzungsordnung geändert werden, um die notwendige Rechtssicherheit herzustellen. Die Zusammenführung von bislang verteilt vorliegenden personenbezogenen Daten ist in jedem Fall ausführlich zu begründen; es muss klar erkennbar sein, dass der angestrebte Zusatznutzen nur auf diesem Wege zu erreichen ist.

2.2 Effiziente Arbeitsumgebungen

An der Universität Münster existiert eine Vielzahl von unterschiedlichen webbasierten Anwendungen – dazu gehören sowohl der Zugang zu Webinhalten (Content) als auch umfangreiche DV-Anwendungen, die über eine Webschnittstelle verfügen. Bestehende Anwendungen und neu zu realisierende Dienste sollen zukünftig auf einer gemeinsamen Integrationsplattform konzentriert und nutzerfreundlicher bereitgestellt werden. Es sollen personalisierbare Arbeitsumgebungen (Portale) entstehen, die dem Anwender effizientes Arbeiten ermöglichen, indem ein zentraler Einstiegspunkt zur Nutzung unterschiedlicher Dienste geboten wird. Der Integrationsgedanke ist zusätzlich durch die Realisierung einer Single Sign-On-Infrastruktur zu unterstützen.

Im Rahmen der Evaluationsphase wurde ein Testportal auf der Basis des IBM *WebSphere Portalserver 6.0* realisiert. Dieses basiert auf J2EE-Technologie, wobei die einzelnen Portalanwendungen als Java-Portlets vorliegen. Neue Anwendungen können direkt an diese technischen Rahmenbedingungen angepasst werden (siehe Abb. 2 – Neuentwicklung von Portlets). Mit WSRP (*Web Services for Remote Portlets*) lassen sich bereits bestehende Portlets leicht integrieren. Mittels dieser Funktionalität werden Mehrwerte für Nutzer zum einen durch Verknüpfung von Informationsquellen aber auch durch eine durchgängige Unterstützung von Prozessen bzw. Workflows geschaffen. Anders verhält es sich bei der Integration bestehender Webanwendungen. Diese sind häufig auf der Basis von Skriptsprachen wie zum Beispiel PHP oder Perl implementiert, so dass sie nicht ohne weiteres in Java-Portlets überführt werden können.

Generell können bei der Integration bestehender Anwendungen drei weitere Fälle unterschieden werden, die hauptsächlich von der jeweiligen technischen Realisierung abhängen. Im ersten Fall

lassen sich Webservices entwickeln, die als Schnittstellen zu Anwendungen genutzt und sehr flexibel in die neue Arbeitsumgebung integriert werden können.

Eine weitere Möglichkeit besteht darin, Webanwendungen über portalspezifische *Portletbridge*-Verfahren einzubinden. Beim *Portletbridging* im ursprünglichen Sinne handelt es sich um eine JSR-168-konforme Technik[13], bei der ein Portlet als Proxy für die Zugriffe auf ein externes HTML-Webinterface fungiert. Als Ergebnis einer Anfrage über die Portletbridge wird in der Portaloberfläche der Inhalt des BODY-Tags der externen Webseite dargestellt.

Ein drittes Verfahren ergibt sich durch die Möglichkeit, externe Webseiten über IFrame-Objekte einzubinden. Dies ist allerdings eine Technik, deren Unterstützung über den JSR-168 explizit ausgeschlossen wird! Mit einem IFrame-Objekt im Portal wird quasi ein eigenes HTML-Fensterobjekt erzeugt, wobei sich der Inhalt des IFrames komplett der Steuerung durch die Portalanwendung entzieht.

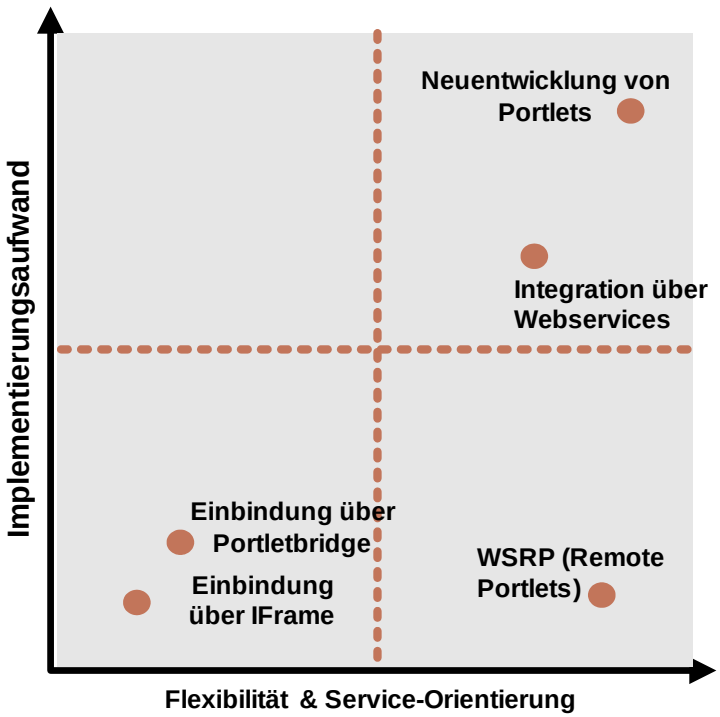


Abb. 2: Integration von bestehenden und Entwicklung neuer Webanwendungen

Über das *Webclipping* bietet der IBM-Portalserver die Möglichkeit, ein Webinterface über IFrame oder über eine Portletbridge einzubinden. Beide Mechanismen implizieren technische Schwierigkeiten, welche vor allem durch die geringe Portalintegrationsstufe und die damit

[13] JSR = Java Specification Request; speziell für den JSR-168 siehe z.B. http://developers.sun.com/prodtech/portalserver/reference/techart/jsr168/pb_whitepaper.pdf

eingeschränkte Möglichkeit der Einflussnahme auf den Datenaustausch der Anwendungen verursacht werden. Mit Blick auf das SSO-Infrastrukturkonzept stellt sich beispielsweise das Portletbridging als problematisch dar, weil der Schutz einer Anwendung durch einen vorgeschalteten Ressourcenmanager technisch nicht realisierbar wäre. Bei Verwendung der IFrame-Technologie setzt man demgegenüber auf eine nicht JSR168-konforme Technologie. Doch stören in diesem Fall oft Login- und/oder Logout-Funktionalität der externen Webanwendungen den reibungslosen Dialogablauf im Sinne der SSO-Implementierung. Technische Hürden ergeben sich zudem sehr leicht durch Fremdeinflüsse bei der Bearbeitung externer Ressourcen. Eingebettete META-Tags (z. B. REFRESH), absolut positionierte DIV-HTML-Elemente oder auch die skriptgesteuerte Erzeugung von HTML-Fragmenten können leicht zu einer im Portal nicht lauffähigen Webseite führen. Zwar ließe sich bei Einsatz einer Portletbridge ein Teil dieser Probleme eventuell durch eine XSLT-basierte Filterung des HTML-Quelltextes beheben, allerdings wäre ein solches Verfahren bei der großen Anzahl von externen Webanwendungen und ihrer Heterogenität unter gleichzeitiger Berücksichtigung regelmäßiger Updates ein sehr aufwändiges und fehleranfälliges Unterfangen. Aus diesen Gründen haben wir uns entschlossen, bestehende Anwendungen vorzugsweise über Webservice-Schnittstellen zu integrieren.

2.3 Accessmanagement und Single Sign-On webbasierter Anwendungen

Zentrale Voraussetzung für die Implementierung eines Single Sign-On (SSO) für bestehende webbasierte Intranetdienste ist ein Identitätsmanagement. Auf dieser Grundlage wird ein LDAP-Directory[14] mit den erforderlichen Daten für ein zentrales SSO provisioniert.

Abb. 3 verdeutlicht die SSO-Architektur. Die verschiedenen Anwendungen werden als Ressourcen beschrieben, deren Zugriffe jeweils durch Ressourcenmanager geschützt werden. Die eigentliche Zugangsprüfung erfolgt durch einen zentralen Authentifizierungsmanager, mit dem die einzelnen Ressourcenmanager kommunizieren. Nach dem Schlüssel-Schloss-Prinzip repräsentiert jeder Ressourcenmanager das Schloss zur Anwendung. Der passende Schlüssel wird technisch als (digitales) Ticket, beispielsweise verpackt in einem Browser-Cookie, vom Authentifizierungsmanager geliefert.

[14] LDAP = Lightweiht Directory Access Protocol; siehe z. B. http://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Der Zugriff auf eine beliebige Ressource führt also grundsätzlich über den Ressourcenmanager. Ist der Benutzer bereits bekannt und zugriffsberechtigt, leitet der Ressourcenmanager die Anfrage direkt zur Anwendung weiter. Wenn kein gültiges Ticket für die Nutzung der Ressource vorliegt, wird der Authentifizierungsmanager involviert. Nach erfolgreicher Authentifizierung erzeugt dieser ein Ticket. Nach einmaliger erfolgreicher Authentifizierung stehen dem Anwender alle webbasierten Anwendungen zur Verfügung, deren Zugang zentral gesteuert wird.

SSO kann also in einer beliebigen serviceorientierten Architektur (SOA) benutzt werden. Das gilt natürlich auch für Portale. Durch die Aggregation von Anwendungen im Portal wird somit ein wesentlicher Mehrwert geschaffen. Anwendungen, die aus technischen oder aus dienstlichen bzw. inhaltlichen Gründen nicht für eine Integration in das Portal in Frage kommen, können dennoch in den SSO-kontrollierten Pool von Ressourcen eingegliedert werden.

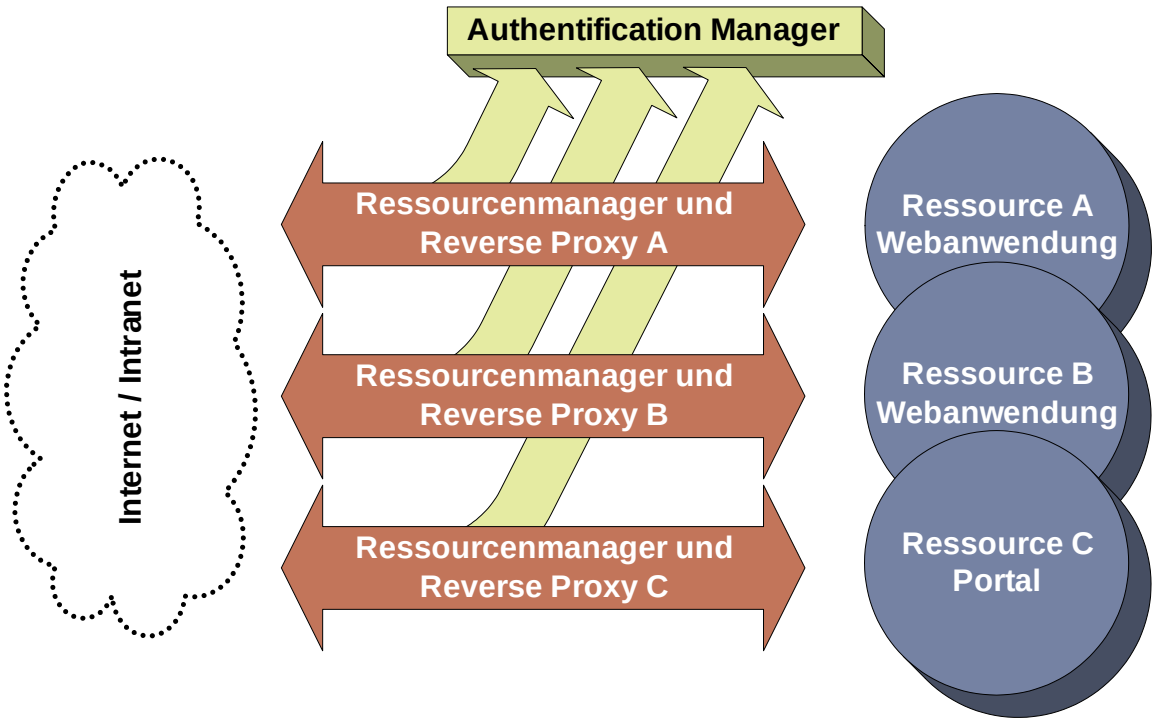


Abb. 3: Single Sign-On Infrastruktur

Zur Realisierung einer webbasierten SSO-Infrastruktur wurden der IBM *Tivoli Access Manager* (TAM) in Verbindung mit dem Reverse Proxy *Webseal*[15] und die Open-Source-Lösung *Shibboleth*[16] untersucht. Die grundsätzlichen Prinzipien und Funktionen, die dem Schutz webbasierter Ressourcen dienen, sind in beiden Produkten ähnlich realisiert, da die Zugriffe auf einzelne Webanwendungen jeweils über Ressourcenmanager gelenkt werden. Diese kommunizieren bidirektional mit einem zentralen Authentifizierungsmanager, wodurch bei berechtigtem Zugriff ein digitales Ticket erzeugt wird, das als Schlüssel zu allen Anwendungen im SSO-Verbund dient. Bei Verwendung von Shibboleth übernimmt ein *Service Provider* die Aufgabe des Ressourcenmanagers und ein *Identity Provider* dient als Authentifizierungsmanager. Zur Authentifizierung eines Benutzers verwendet der Identity Provider ein externes Benutzerverzeichnis (z. B. LDAP).

Als Ergebnis der Evaluation haben wir uns in einem *Proof of Concept* für eine auf Shibboleth basierende SSO-Lösung entschieden. Hierbei konnte die Portalanwendung (WebSphere-Portalserver) erfolgreich eingebunden werden. Shibboleth weist aufgrund seiner offenen Schnittstellen, der gebotenen Flexibilität und einer großen Internet-Community viele Vorteile gegenüber der proprietären Lösung von IBM auf und bietet weiterhin bekanntermaßen die Möglichkeit, Dienstleistungen auch organisationsübergreifend zur Verfügung zu stellen. Daher wird Shibboleth bereits von einigen anderen Universitäten und öffentlichen Einrichtungen getestet bzw. eingesetzt, um in Zukunft auch Dienste im Rahmen einer Föderation bzw. Kooperation anbieten zu können.

Beim Accessmanagement wird zwischen den Begriffen Zugangskontrolle und Zugriffskontrolle unterschieden. Zugangskontrolle – oder Accessmanagement im engeren Sinne – steht für einen Mechanismus, der bestimmt, ob einem Anwender der Zugang zu einer Ressource überhaupt gestattet wird oder nicht. Unter Zugriffskontrolle dagegen wird der Mechanismus verstanden, der die Art und Weise bestimmt, wie auf Ressourcen zugegriffen werden kann. Mit einem universitätsweiten Single Sign-On wird die Basis für eine zentrale Zugangskontrolle geschaffen. In der oben diskutierten Web-Infrastruktur kann der Zugang zu Informationsressourcen rollenbasiert geregelt werden, indem dafür geeignete Attribute im Identitätsmanagement zentral verwaltet werden.

---

[15] siehe z.B. http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/ de_DE/HTML/ am51_webseal_guidet000.htm

[16] siehe z. B. http://shibboleth.internet2.edu/

Für die zentrale Zugriffskontrolle benötigt man eine Softwarekomponente, die alle Zugangs- und Zugriffsinformationen in Form von Zugriffskontrolllisten (*Access Control Lists*, ACLs) verwaltet (siehe [SaSa94]). Anwendungen müssen dazu gebracht werden, die in diesem Register gespeicherten Metadaten richtig auszulesen und die Zugriffsinformationen durchzusetzen.

Nach einer umfassenden, praktischen Erprobung eines auf dem Markt führenden Access-Management-Systems (Tivoli Access Manager) sowie nach der Untersuchung ähnlicher Systeme haben wir erkannt, dass die Einführung eines solchen Systems in einer bestehenden heterogenen Landschaft zurzeit noch sehr aufwändig ist. Diese Aufgabe wurde daher zunächst zurückgestellt, denn die Anbindung an TAM bedeutet bei den meisten existierenden Systemen u. a. einen tiefen Eingriff in die Anwendungslogik.

2.4 Suchraumkonzept und Einbindung erster Datenquellen

Die neu einzuführenden Methodiken und Verfahren im Bereich *Information Retrieval* werden sowohl wissenschaftliche als auch organisatorische Informationen sowie Lehr- und Lernmaterialien durchsuchbar und rollenspezifisch verfügbar machen. Um dieses Ziel zu erreichen, ist eine enge Kopplung zwischen der einzuführenden Suchmaschinentechnologie und den in den vorherigen Abschnitten bereits beschriebenen Technologien vorgesehen. Die Universität Münster hat sich nach einer Evaluation der am Markt befindlichen Produkte für die *Enterprise Search Platform* der Firma *FAST Search & Transfer*[17] entschieden.

2.4.1 Suchraumkonzept

Strategische Überlegungen zur Interoperabilität und zum Kooperationspotenzial der Suchmaschine spielten bei der Produktauswahl eine entscheidende Rolle, da bei der Suche nach wissenschaftlichen Informationen Datenquellen aus dem *lokalen* Suchraum an der Universität Münster sowie dem *erweiterten* Suchraum gleichzeitig durchsucht und nach Relevanz sortiert werden müssen (siehe Abb. 4).

[17] siehe http://www.fastsearch.com/

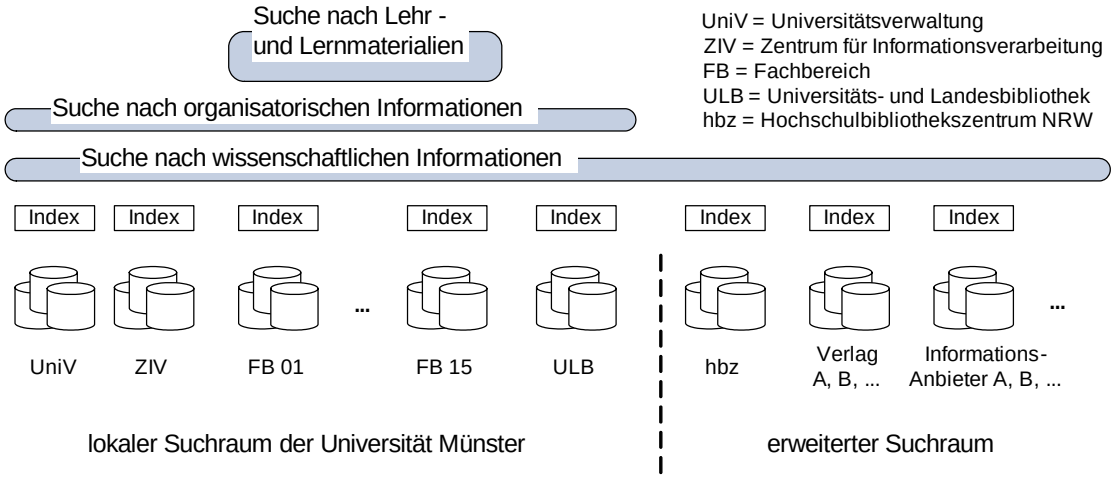


Abb. 4: Suchraumkonzept an der Universität Münster

Eine weitere Besonderheit unseres Suchraumkonzeptes besteht in der Unterstützung von Arbeitsgruppen durch Einbeziehung von noch nicht publizierten (wissenschaftlichen) Informationen, die in großer Zahl auf Servern und persönlichen Rechnern vorhanden sind. Dabei spielt natürlich ein verlässliches Zugriffs- bzw. Berechtigungskonzept eine große Rolle (auf diesen Aspekt wird im folgenden Abschnitt genauer eingegangen). Daneben werden selbstverständlich die „klassischen“ wissenschaftlichen Informationen, welche üblicherweise in Katalogen bzw. Datenbanken von Bibliotheken vorliegen, sowie organisatorische Informationen, die z. B. zur Steuerung und zur Administration der Universität benötigt werden, eingebunden. Somit müssen neben den auf (öffentlichen) Webservern vorhandenen Daten vielfältige Formate aus anderen Datenquellen (Fileserver, Mailarchive, Datenbanken usw.) durchsucht und indexiert werden.

Zur Verbindung von Suchräumen verschiedener Suchmaschinen bestehen unterschiedliche Möglichkeiten. Bei der *Metasuche* wird eine Suchanfrage an andere Suchmaschinen weiter gegeben; die jeweiligen Ergebnislisten werden nacheinander angezeigt. Bei der *föderierten Suche* werden verschiedene Indizes im Rahmen einer Suchanfrage miteinander kombiniert, wobei sich die Integration verschiedener Indizes unterschiedlicher logischer oder inhaltlicher Struktur mitunter als schwierig herausstellen kann (siehe dazu u. a. [CFKN06]). Trotzdem stellen die Möglichkeiten des zuletzt genannten Verfahrens die aus unserer Sicht favorisierte Lösung dar, da die Qualität der Suchergebnisse bei entsprechender vorheriger Aufbereitung der Daten und Indizes deutlich besser ausfällt als bei der Metasuche. Wir wollen also wo immer möglich die föderierte Suche einsetzen bzw. implementieren.

2.4.2 Einbindung erster (XML-basierter) Datenquellen

Für die Einbindung der vielfältigen Datenquellen stehen bei den zurzeit am Markt verfügbaren Produkten unterschiedliche Werkzeuge zur Verfügung. Die auf Webservern vorhandenen Daten werden mit *Crawlern* durchsucht; bei Fileservern, Mail- und Newsservern, Dokumentenmanagementsystemen sowie Datenbanken kommen jeweils spezielle *Konnektoren* zum Einsatz, welche der Suchmaschine den Zugriff auf die jeweilige Datenquelle ermöglichen. Besteht die Notwendigkeit, bestimmte neu eingestellte Dokumente sehr schnell in den Index aufzunehmen, kann dies mit Hilfe von *Push-Mechanismen*, die man den Datenquellen zuordnet, realisiert werden. Alle Dateien bzw. Dokumente durchlaufen vor der eigentlichen Indexierung eine umfangreiche Analyse, das *Document Processing*.

Abb. 5 zeigt exemplarisch einige Verarbeitungsschritte bei der Einbindung von Daten, die in diesem Fall über die OAI-PMH-Schnittstelle[18] (siehe dazu [VNLW04]) eines OAI-Repository-Servers in einem bestimmten XML-Format geliefert werden. Voraussetzung für die Bearbeitung von XML-Datenquellen über eine Schnittstelle ist die Einigung auf ein einheitliches Format für die Abbildung der Objektstrukturen der jeweiligen Datenquelle (Verarbeitungsschritt 1). Eine erste Implementierung erfolgt mit dem vom Hersteller *Fast* vorgeschlagenen *FastXML*-Format (siehe [Kost04]). Die Verarbeitungsschritte 2 und 3 verdeutlichen das Mapping und die Verarbeitung der XML-Objekte auf die im Indexprofil definierten Indexfelder, welche sich an den Fast-Standardfeldern und den vom *Dublin-Core*-Metadatenschema[19] vorgegebenen Feldern orientieren. Bei einer Suchanfrage (Verarbeitungsschritt 4) wird dann über die *Search API*[20] auf diesen Index zugegriffen, entweder im Rahmen einer Einzelsuche (*Front Ende Services* in Abb. 5) oder einer föderierten Suche (*Federated Search*).

[18] OAI = Open Archives Initiative; siehe z.B. http://www.openarchives.org/
[19] siehe z.B. http://dublincore.org/
[20] API = Application Programming Interface (Programmierschnittstelle)

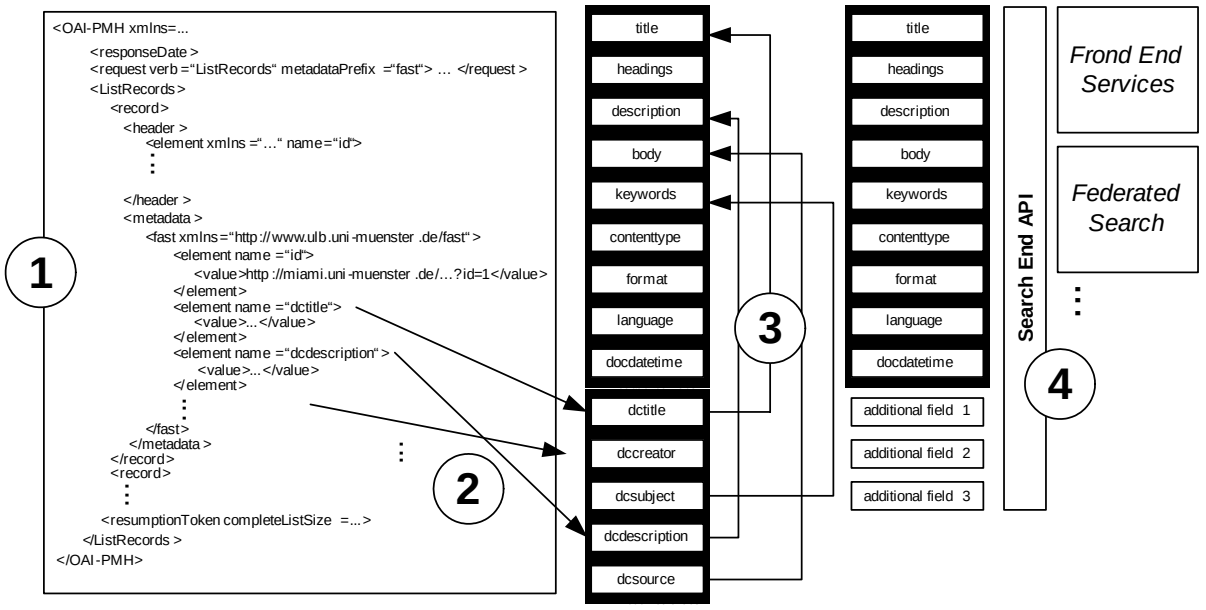


Abb. 5: Verarbeitungsschritte bei der Einbindung von (XML-) Datenquellen

Zur Überprüfung der im vorherigen Abschnitt bereits angesprochenen Problematik der Zugriffssicherung sind in ersten Prototypen Access-Control-List-Informationen (ACLs) in die systeminterne Dokumentbeschreibung aufgenommen worden. Die verwendete Suchmaschine verfügt über ein entsprechendes Security Access Modul (SAM) und ist daher ist in der Lage, die Berechtigungen, welche der jeweilige Dateneigner zuvor festgelegt hat, auszuwerten. Dem Nutzer werden auf diese Weise bei seiner Suche nur die Informationen angezeigt, auf die er ohnehin zugreifen darf.

3 Anmerkungen zur Einführung (Roll-out) der neuen Technologien

Ein Projekt der Größenordnung und Komplexität wie MIRO soll am Ende allen Mitgliedern der Universität Nutzen bringen. Deshalb ist von Anfang an zu bedenken, wie die entwickelten Systeme und Infrastruktur-Komponenten konkret ein- und in den Regelbetrieb überführt werden sollen. Die folgenden Abschnitte fassen die Überlegungen zu diesem *Roll-out*-Prozess zusammen, wobei zunächst die organisatorischen Rahmenbedingungen skizziert werden.

3.1 Informationsverarbeitung an der Universität Münster

Um die Arbeitsergebnisse von MIRO in den Produktionsbetrieb zu übernehmen, muss auf vorhandene Organisationsstrukturen der Informationsverarbeitung zurückgegriffen werden, die den Roll-out-Prozess maßgeblich unterstützen können. Dazu sind die Voraussetzungen in Münster seit Jahren vorhanden und haben sich bewährt. Dies betrifft zum einen dezentrale, professionell arbeitende IV-Teams in den Fachbereichen, IV-Versorgungseinheiten (IVVen) genannt, die vor 10 Jahren eingeführt wurden. Dadurch wurden die unkoordinierten und viel zu kostspieligen Betreuungsmodelle in den Fachbereichen beendet, bei denen jede noch so kleine Einrichtung auf unterschiedliche Weise die vor Ort anfallenden IV-Themen mehr oder weniger selbständig erledigte. Zum anderen besteht eine enge Zusammenarbeit der drei zentralen Einrichtungen, des *Zentrums für Informationsverarbeitung (ZIV)*, der *Universitätsverwaltung (UniV)* sowie der *Universitäts- und Landesbibliothek (ULB)*, die als *IKM-Service* (Information, Kommunikation, Medien) institutionalisiert und vom Rektorat dauerhaft eingerichtet ist. Der IKM-Service bündelt die Kräfte in überlappenden Themenfeldern und hilft Doppelarbeiten zu vermeiden.

Insgesamt existieren 8 IVVen für 15 Fachbereiche und je eine für UniV und ULB. Diese arbeiten eng mit dem ZIV zusammen. Mit Vorrang obliegen ihnen fachspezifische und regelmäßig anfallende Aufgaben zur Betreuung der Nutzer, Arbeitsplatzsysteme und Server vor Ort. Sie arbeiten eigenverantwortlich, fachlich fundiert, zügig und erreichen durch ihre direkten Kontakte in den Fachbereichen, zu denen sie gehören und die sie gut kennen, eine hohe Kundenzufriedenheit. Sie haben nicht nur die Aufgabe, universitätsweit einzuführende Neuerungen der Informationsverarbeitung dezentral umzusetzen, sondern sorgen auch dafür, dass dezentral vorhandene Bedürfnisse an zentraler Stelle Gehör finden und koordiniert werden können.

Alle Rechnernetze sind vollständig dem ZIV unterstellt. Rechner- und Betriebssysteme sowie Anwendungssysteme mit zentralem Charakter, welche die Ressourcen sowie die damit verbundenen Versorgungskonzepte, Verfahren und Betriebskonzepte bzw. die Unterstützung einzelner Nutzer und Nutzergruppen umfassen, werden vom ZIV vorgehalten. Server mit fachspezifischen Aufgaben werden von den IVVen betrieben. Die Kooperation zwischen

IVVen und ZIV wurde verbindlich geregelt.[21] Die Ergebnisse spiegeln sich in vielen gemeinsam und erfolgreich angegangenen Entwicklungen wider[22].

Übergeordnetes Organ für alle IV-Fragen ist der IV-Lenkungsausschuss (IVL), dem die Rektorin (vertreten durch einen Prorektor), die Kanzlerin, der Vorsitzende der IV-Kommission sowie drei weitere Experten angehören, die auf dem Gebiet der IV besonders ausgewiesen sind. Die Direktorin der ULB und der Direktor des ZIV nehmen an den Sitzungen beratend teil. Der IVL nimmt CIO-Aufgaben wahr, indem er den nutzergerechten und wirtschaftlichen Betrieb des IV-Gesamtsystems sicherstellt, die dazu notwendigen Grundsatzentscheidungen trifft, die Ziele und Aufgaben auf der zentralen und der dezentralen Ebene festlegt sowie die Entscheidungs- und Betriebsabläufe und die Ergebnisse der Arbeit kontrolliert.

Die hier skizzierten organisatorischen Aspekte spielen nicht zuletzt auch für die Deutsche Forschungsgemeinschaft (DFG) im Rahmen der Förderung dieses Projektes eine wichtige Rolle, da ohne *spezialisiertes technisches und organisatorisches Wissen […] unterstützende Dienstleistungen für Forschung und Lehre in einer dem neuen medialen Umfeld entsprechenden Form* nicht angeboten werden können[23].

3.2 Roll-out und Change Management

An der WWU Münster werden die zwischen IKM-Service und IVVen festzulegenden Roll-out-Schritte durch gemeinsame Aktionen koordiniert. Auf diese Weise können neue Software-Komponenten verbreitet und bestehende Anwendungen modifiziert werden, um z. B. (Web-) Anwendungen auf eine Authentifizierung via Shibboleth umzustellen und auf diese Weise an den universitätsweiten Single Sign-On-Mechanismus anzudocken. Diese Strukturen sind weiterhin hilfreich, um etwa dezentrale Datenquellen der Fachbereiche zu erschließen und in die universitätsweite Informations-Infrastruktur einzubringen. Die IVVen werden dabei im Sinne des *Change Managements* das Wissen über den Nutzen von MIRO durch Schulung und Beratung begleiten und die Ausweitung durch gute Anwendungsbeispiele fördern. Sie sind bereits mit MIRO vertraut gemacht und vom Nutzen des integrierten Informationsmanagements überzeugt worden; selbstverständlich werden sie regelmäßig über die aktuellen Entwicklungen auf dem Laufenden gehalten. Die IVVen unterstützen die Initiierung und Autorisierung der

[21] siehe hierzu http://www.uni-muenster.de/ZIV/Organisation/KooperationIVVundZIV.html
[22] Beispiele sind Systemmanagement, Backup und Archivierung, Softwareverteilung in Paketen, Maßnahmen zur IV-Sicherheit und Rezentralisierung der E-Mailserver.
[23] siehe http://www.dfg.de/aktuelles_presse/download/leistungszentren_04.pdf

einzelnen Veränderungsmaßnahmen und wirken mit bei der Implementierung, Überwachung und Prüfung in ihren Fachbereichen. Die hierfür erforderlichen Prozesse werden innerhalb von MIRO entwickelt und ausführlich dokumentiert, um ihre Wiederverwendbarkeit an anderen Stellen zu gewährleisten. Dabei dürfte es in der Praxis unproblematisch sein, wenn sich im Laufe der Entwicklung von MIRO herausstellen sollte, dass einzelne Ressourcen auch von den IVVen betrieben werden müssen, weil dies z. B. aus Gründen der Kapazitäts- und Lastverteilung oder der Systemadministration notwendig werden sollte. Dies könnte die Universitätsportale betreffen, die möglicherweise als virtuelle Portale mit Zugriff auf zentrale Dienste eingesetzt werden müssen. Dies könnte sich auch für die Suchmaschine ergeben, die als generelles Navigationsinstrument einen deutlich höheren Stellenwert als bislang erhalten wird.
Mit Vertretern der Dekanate wurde bereits über das Projekt MIRO ausführlich gesprochen. Da wir dabei überall große Zustimmung erfahren haben, sind wir zuversichtlich, dass der Roll-out-Prozess gelingt. Dennoch wird der Aufwand groß und nicht in kurzer Zeit zu bewerkstelligen sein. Durch ein weiter zu verstärkendes Marketing und viele positive Anwendungsbeispiele wollen wir Schneeballeffekte auslösen, die uns auf dem Weg zu einem integrierten Informationsmanagement voranbringen.

Literaturverzeichnis

[CFKN06] Chernov, Sergey; Fehling, Bernd; Kohlschütter, Christian; Nejdl, Wolfgang; Pieper, Dirk; Summann, Friedrich: Enabling Federated Search with Heterogeneous Search Engines – Combining FAST Data Search and Lucene. (Federated Search Project Report); März 2006. URL: http://base.ub.uni-bielefeld.de/download/FedSearchReport.pdf

[SaSa94] Sandhu, R. S.; Samarati, P.: Access control: principle and practice. In: Communications Magazine, IEEE, Fairfax, VA, 1994.

[SBHT05] Schmidt, Jürgen; Böhm, Bettina; Held, Wilhelm; Tröger, Beate: Integrierte Bereitstellung, einheitlicher Zugang und individuelle Verteilung – Informationsmanagement einer großen Universität. (Projektvorschlag MIRO – Münster Information System for Research and Organization); Januar 2005. URL: http://www.uni-muenster.de/ikm/miro

[Kost04] Kostädt, Peter: Indexierung der HBZ-Verbunddaten mit Fast Data Search. In: Proceedings of the 8th InetBib-Tagung, Bonn 2004.

[VNLW04] Van de Sompel, Herbert; Nelson, Michael L.; Lagoze, Carl; Warner, Simeon: Resource Harvesting within the OAI-PMH Framework. In: D-Lib Magazine, 2004.

Föderatives und dienstorientiertes Identitätsmanagement im universitären Kontext

Thorsten Höllrigl, Frank Schell, Horst Wenske, Hannes Hartenstein

KIM / Rechenzentrum
Universität Karlsruhe (TH)
Zirkel 2
76128 Karlsruhe
{hoellrigl, schell, wenske, hartenstein}@kim.uni-karlsruhe.de

Abstract

Eine Universität, die wettbewerbsfähig operieren will, muss ihre Dienste und Geschäftsprozesse IT-basiert in durchgängiger Weise unterstützen. Grundlage hierfür ist ein universitätsweites Identitätsmanagement, um einen sicheren instituts- und einrichtungsübergreifenden Ressourcenzugriff zu ermöglichen. Die vorliegende Arbeit führt unseren Ansatz des föderativen und dienstorientierten Identitätsmanagements weiter, diskutiert darauf aufbauende Konzepte und legt hierbei gewonnene Erfahrungen dar. Darüber hinaus demonstrieren wir konzeptionell in diesem Workshopbeitrag anhand eines exemplarischen Anwendungsdienstes wie die von uns identifizierten Identitätsmanagementdienste in diesen integriert werden.

1 Einleitung und Motivation

Eine moderne Universität, welche national und international erfolgreich und wettbewerbsfähig operieren will, muss ihre Dienste und Geschäftsprozesse für Studium, Lehre und Weiterbildung, Forschung und Entwicklung, Informationsversorgung sowie zur eigenen Verwaltung IT-basiert in durchgängiger Weise unterstützen. Dabei kommt dem Identitätsmanagement (IdM) eine fundamentale Rolle zu, damit Identifikation und Authentifikation von Personen als auch Autorisation für den Zugriff auf unterschiedliche Ressourcen über Organisationsgrenzen hinweg gewährleistet werden kann. In unserer früheren Arbeit [HMSW06] haben wir hierzu die Grundlagen und die Architektur eines föderativen und dienstorientierten Identitätsmanagements vorgestellt, welche im folgenden

Absatz nochmals in Kürze motiviert werden. Der Fokus der hier vorliegenden Arbeit liegt nun auf der konkretisierten Darstellung und Diskussion der zugehörigen Dienste des Identitätsmanagements bzw. auf der Beantwortung der Frage, mit welchen Identitätsmanagementdiensten eine solche Föderation ausgebildet werden kann. Dieser Workshopbeitrag umfasst sowohl eine technische Konzeption als auch aktuelle Erfahrungen aus dem Aufbau eines integrierten Identitätsmanagements im Rahmen des Vorhabens „Karlsruher Integriertes InformationsManagement“ (KIM).

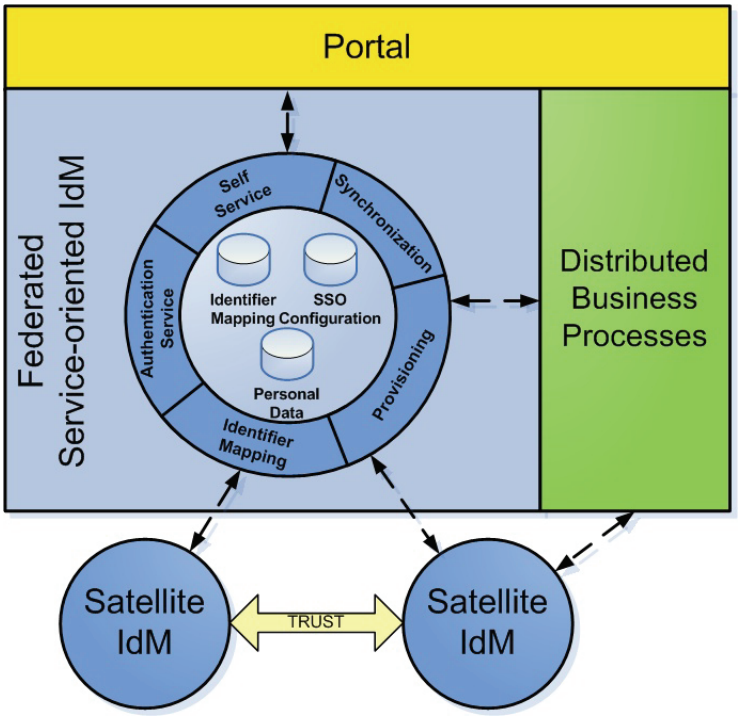


Abb. 7: Zusammenschluss von Satelliten über Identitätsmanagementdienste

In einer größeren, heterogenen Systemlandschaft, wie sie an vielen Universitäten vorzufinden ist, sind die einzelnen Institute und Einrichtungen, die im Laufe der Jahre unabhängig voneinander evolutionär gewachsen sind, in der Regel untereinander weder harmonisiert noch sind IT-gestützte, übergreifende Geschäftsprozesse etabliert. Um der Herausforderung universitätsweiter und IT-basierter Geschäftsprozesse zu begegnen, verfolgt ein föderatives, dienstorientiertes IdM einen kooperativen und integrierenden Ansatz. In diesem Zusammenhang stellt eine Föderation ein Zusammenschluss unabhängiger organisatorischen Einheiten (Satelliten) mit einer eigenen Identitätsbasis dar, welche eine Vertrauensbeziehung zueinander haben. Dabei ist zu betonen, dass ein föderatives IdM nicht das lokale Identitätsmanagement der Satelliten ersetzt, sondern auf diesen aufbaut (Abb. 7).

Die wesentlichen Beweggründe, diesen Ansatz zu verfolgen, liegt in der Aufrechterhaltung der Eigenständigkeit der Institute und Einrichtungen bei gleichzeitiger Wahlfreiheit der eingesetzten Systeme und Fortbestand bestehender lokaler Prozesse. Dadurch wird eine höhere Akzeptanz bei den Partnern erreicht, da sie ihre bestehenden Intra-Satellitenprozesse weiter betreiben können und weiterhin funktionsfähig sind, selbst wenn zentrale Dienste ausfallen sollten. Auch die Verantwortung der Daten (z.B. Datenpflege und Zugriffberechtigungen) und der lokalen Geschäftsprozesse bleibt bei den Satelliten, die ihre spezifischen Anforderungen und Rahmenbedingungen am Besten kennen. Dadurch können die Satellitenbetreiber weiterhin schnell und flexibel lokale Prozesse, die keinerlei Auswirkungen auf die anderen Satelliten der Föderation haben, anpassen.

Diese Flexibilität auf Ebene der Satelliten wird auf Ebene organisationsübergreifender Geschäftsprozesse, die sowohl erweiterbar als auch auf Bedarf anpassbar sein müssen, durch eine Dienstorientierung im Rahmen einer Service-orientierten Architektur (SOA) unterstützt. Eine SOA basierend auf Web Services bietet Mechanismen, um existierende Systeme und Applikationen unabhängig von ihrer Sprache und Plattform zu integrieren [ZiKG04]. Übertragen auf ein Identitätsmanagement bedeutet dies die Bereitstellung identitätsbezogener Daten über dezentrale Dienste. Diese Identitätsmanagementdienste, die im Laufe der Arbeit noch weiter betrachtet werden, können von anderen Applikationen wiederverwendet werden, um komplexere Anwendungsszenarien bzw. umfangreichere Funktionalitäten umzusetzen. Darüber hinaus ist eine Integration beliebiger Informationsdienste, die über die Universität verteilt angeboten werden, realisierbar. Dies bietet die Grundlage dafür, dass die Daten nur in den assoziierten Systemen gespeichert werden müssen, und eine zentrale Replikation dieser Daten nicht notwendig ist [HoRe05], wodurch Änderungen der Datenschemata oder Zugriffsberechtigungen ausschließlich lokal durchzuführen sind. Der weitgehenden Eigenständigkeit der Partner in einer Föderation steht als „zentralistische“ Komponente die Einigung auf ein Regelwerk für das Bündnis entgegen. Die Erstellung dieses föderativen Regelwerkes ist ein dynamischer Prozess, und liegt in den Händen von definierten organisatorischen Strukturen. Dadurch soll sichergestellt werden, dass sich das Regelwerk neuen Gegebenheiten anpassen und mit neuen Mitgliedern wachsen kann. Bei konsequenter Verfolgung der ausgeführten Leitgedanken wird dieses „Regelwerk“ durch föderative Identitätsmanagementdienste definiert; ein Vorschlag hierzu ist Gegenstand der weiteren nun folgenden Abschnitte. Im nächsten Abschnitt wird eine Übersicht über die Dienste gegeben, die weiteren Abschnitte

gehen dann detailliert auf die einzelnen Dienste ein. Zuletzt betrachten wir die Anwendung der Identitätsmanagementdienste zur Realisierung eines Erreichbarkeitsdienstes.

2 Identitätsmanagementdienste

Für das dienstorientierte Identitätsmanagement haben wir für die erste Entwicklungsphase grundlegende Identitätsmanagementdienste identifiziert. Die Dienste und ihre Interaktionspartner, nämlich die Portale, Satelliten und verteilte Geschäftsprozesse, sind in Abb. **7** dargestellt. Diese vom Identitätsmanagement bereitgestellten Dienste bilden den „Kitt“ der Föderation, welcher grundsätzlich in unterschiedlichen Graden hinsichtlich Zentralität oder Dezentralität ausgeprägt werden könnte. Wir geben im Folgenden den von uns gewählten „Betriebspunkt“ in diesem Raum der Freiheitsgrade an.

Die Dienste werden als „Identity Shared Services“ (ISS) bezeichnet und in zwei Klassen unterteilt (Abb. 8). Die ISS Klasse der Selbstbedienungsdienste (Self Services) bietet einen zentralen Zugangspunkt für Studenten und Mitarbeiter zur individuellen Konfigurationen und Datenänderungen. Dadurch wird einem Nutzer unbürokratisch, schnell und flexibel ermöglicht, Anpassungen wie z.B. eine Adressänderung vorzunehmen, wodurch der Support und Administrationsaufwand in einer größeren Organisation handhabbar bleibt. Die zweite ISS Klasse bietet Identitätsinfrastrukturdienste („Infrastructure Services“) an, die von Satelliten bzw. Anwendungsdiensten in Anspruch genommen werden können. Dadurch kann zum einen ein Entwickler bzw. Betreiber eines identitätsbezogenen Anwendungsdienstes sich auf die Kernfunktionalität des Dienstes konzentrieren, und kann z.B. für notwendige Authentifikationsfunktionalitäten in seinem Dienst auf den Authentifikations Dienst („Authentication Service“) der Identity Shared Services zugreifen. Zum anderen bieten die Identitätsinfrastrukturdienste föderative Basisfunktionalitäten an, die nicht von einem einzelnen Anwendungsdienst innerhalb eines Satelliten erbracht werden können. Hierbei ist insbesondere der föderative Synchronisationsdienst zu nennen, der die Synchronisation kongruenter Datensätze zwischen Satelliten durchführt, so dass Dateninkonsistenzen vermieden werden. Ebenso ist hier ein Abbildungsdienst („Identifier Mapping“) beheimatet, der lokale Account-Identifikatoren einer Identität bei den verschiedenen Satelliten aufeinander abbilden kann.

Für die Nutzung der Identity Shared Services ist es pro Entität notwendig, föderative Informationen, die lokal in einem Satellitenkontext nicht auftreten, zu erfassen. Es sind hierbei

zwei Möglichkeiten gegeben. Zum einen können die bestehenden Satelliten-Accounts benutzt und mit föderativen Informationen angereicht oder ein neuer Föderations-Account für einen Nutzer zusätzlich angelegt werden. Da die Identity Shared Services das verbindende Element der Föderation darstellen, muss eine gewisse Unabhängigkeit zu den einzelnen Satelliten gewahrt werden, damit die Föderation auch bei Umstrukturierungsprozessen operationsfähig bleibt. Deshalb haben wir uns für einen dedizierten, neuen Föderations-Account entschieden. Dadurch sind wir beispielsweise bei der Wahl der Passwort-Policy, des benutzten Datenschemas und der Auswahl der gehaltenen Datenattribute frei von satellitenspezifischen Zwängen. Nach den abgeleiteten Anforderungen stellt der Betreiber der Identity Shared Services eine eigene organisatorische Einheit mit Identitätsbasis dar, und kann als weiterer Satellit in die Föderation aufgenommen werden.

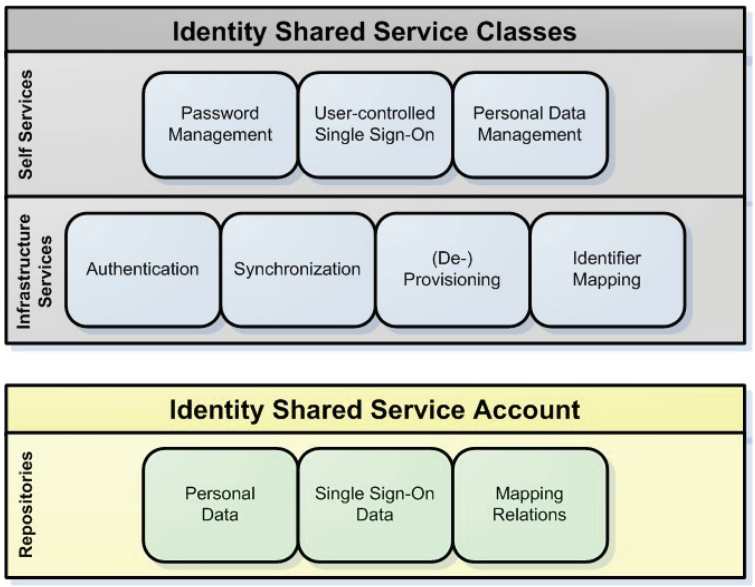


Abb. 8: Klassifizierung der Identitätsmanagementdienste

Damit eine Entität an der Föderation teilnehmen kann, ist eine initiale Authentifikation und Konfiguration notwendig. Die Erstellung eines IIS-Accounts kann mit dieser initialen Phase verbunden werden („Bootstrapping“). Die IIS-Accounts sollen dabei keine andere Form eines Meta-Directorys darstellen: die Datenattribute des IIS-Accounts sollen auf ein Minimum reduziert sein, da eventuelle Zusatzinformationen für organisationseinheitenübergreifende Geschäftsprozesse von den jeweils verantwortlichen Informationsdiensten bezogen werden können.Basierend auf einer von uns durchgeführten Analyse sind die zwingend notwendigen Elemente eines IIS-Accounts ein universitätsweit eindeutiger Identifikator, die individuelle

Single Sign-On Konfiguration zusammen mit den Identifier Mappings. Darüber hinaus können optional Emailadresse, Vorname oder Nachname in dem Identity Shared Service Repository, welches die notwendigen Daten zum Betrieb der Identity Shared Services zur Verfügung stellt, gespeichert werden (Abb. 8). Nachfolgend gehen wir ausführlicher auf die Funktionalitäten der betrachteten Identitätsmanagementdienste ein, diskutieren Problemstellungen und präsentieren Lösungsansätze.

2.1 Identifier Mapping

Innerhalb der Universität Karlsruhe haben die einzelnen organisatorischen Einheiten über einen längeren Zeitraum unabhängig voneinander jeweils eine eigene Datenbasis mit eigenen Identifikatoren für ihre lokal zu verwaltenden Identitäten entwickelt. Hierdurch können organisationsübergreifende Geschäftsprozesse nicht ohne Unterstützung auf die Dienste der entsprechenden Satelliten zugreifen, da die automatisierte Zuordnung einer Entität zu den lokalen Identitäten nicht immer möglich ist. Im universitären Kontext werden größtenteils personalisierte Dienste, wie beispielsweise Bibliotheksdienste, angeboten, wodurch ein föderatives Rollen Mapping nicht ausreicht. Die Herausforderung liegt damit in einem Identifier Mapping, das alle lokalen Identifikatoren zu einer Entität erfasst. Hierbei lassen sich folgende Probleme identifizieren. Zum einen ist ein automatisiertes Mapping nicht möglich, da in der Regel nur eine ungenügende Anzahl von Attributen bei den verschiedenen Satelliten existieren, die für einen eindeutigen Abgleich dienen können. Zum anderen ist ein durch die Administration durchgeführtes manuelles Mapping der lokalen Identitäten zur globalen Identität aufgrund der großen Anzahl von Identitäten praktisch nicht durchführbar. Ein von uns verfolgter Lösungsansatz besteht in einem Mapping der lokalen Identifikatoren auf einen globale ID, die eine Entität universitätsweit eindeutig identifiziert. Die manuelle Zuweisung der verschiedenen lokalen Identitäten zu einer globalen ID wird durch den Nutzer selbst erbracht, indem der Nutzer sich an der jeweiligen lokalen Datenbasis authentifiziert. Durch diesen authentifizierten Vorgang kann zum einen die Abbildung lokale ID auf globale ID ermittelt und zum anderen sichergestellt werden, dass nur ein berechtigter Nutzer diese Zuordnung durchführen kann. Dies geschieht während des initialen Registrierungsvorgangs und der Freischaltung des ISS-Accounts eines Nutzers. Um eine höhere Sicherheit zu erreichen, ist es möglich, einen gemeinsamen Verweis (Handle) für eine Entität zwischen Identity Mapping Service und Satellit zu generieren. Dieses Handle wird vom Identifier Mapping Service auf die jeweilige globale ID und von dem Satelliten auf seine jeweilige lokale ID abgebildet. Dies hat

den Vorteil, dass jeder Dienstanbieter nur sein eigenes datensatzspezifisches Handle kennt und dadurch nicht auf andere Handles von anderen Dienstanbietern schließen kann. Dies setzt jedoch voraus, dass ein Satellit die Handles in seine lokale Datenbasis aufnehmen kann.
Die Einführung eines zusätzlichen globalen Identifikators bzw. mehrerer Handles ist notwendig, da eine einfache Harmonisierung aller lokaler Identifier zu einer gemeinsamen globalen ID häufig nicht möglich ist. Das liegt darin begründet, dass organisatorische Einheiten unterschiedliche Anforderungen an ihre lokalen Identifikatoren stellen z.B. eine Mindestlänge oder spezielle Präfixe, wodurch ein globaler Identifikator nicht einfach die vorherige lokale ID ersetzen kann. Letztlich ermöglicht ein Identifier Mapping durch die Zuordnung von allen lokalen Identifikatoren zu einer gemeinsamen Identität nicht nur organisationsübergreifende Geschäftsprozesse, sondern auch den automatisierten Datenabgleich bei Änderungen und eine personalisierte Single Sign-On Funktionalität über Satellitengrenzen hinweg. Hierbei erfolgt die Einbindung des Identifier Mapping Service über eine Web Service Schnittstelle, wodurch dessen flexible Nutzung in Anwendungen oder Einbindung in Web Service Orchestrierungen ermöglicht wird.

2.2 Provisionierung

Ein weiterer Identitätsmanagementdienst ist die Provisionierung bzw. die Deprovisionierung. Ersteres stellt hierbei die initiale Phase des Identity Lifecycle Managements dar, wogegen letzteres dessen abschließende Phase bezeichnet. Durch die Provisionierung werden nach dem Anlegen eines neuen Accounts in einer organisatorischen Einheit weitere Satelliten automatisiert mit den für sie relevanten Daten versorgt. Das Identitätsmanagement sorgt somit dafür, dass ein neuer Mitarbeiter nach seiner Einstellung bzw. ein Student nach seiner Immatrikulation in allen relevanten Satelliten bekannt ist, und das mehrmalige Anlegen von Accounts und das wiederholte Angeben persönlicher Daten entfällt. Weitaus bedeutender als die Effizienzsteigerung durch die Provisionierung ist das Erhöhen der Sicherheit durch die Deprovisionierung. Verwaiste Accounts stellen ein hohes Sicherheitsrisiko dar, denn ehemalige Mitarbeiter können sich ansonsten noch mit ihren alten Accountdaten einloggen und eigentlich unautorisierten Zugriff auf Ressourcen erlangen. Durch die Deprovisionierung wird diese Sicherheitslücke geschlossen. Hierbei werden beim Verlassen der Föderation automatisiert alle vorhandenen Accounts eines Benutzers gelöscht bzw. wird den einzelnen Föderationspartner das Ausscheiden mitgeteilt. Der bereits vorgestellte Identitätsmanagementdienst Identifier

Mapping wird hierbei zur Realisierung der Provisionierung und Deprovisionierung benötigt, um sicherzustellen, dass die angelegten Accounts einer Entität zugeordnet werden können. Neben den bereits im Bereich des Identifier Mappings angesprochenen Problemen muss beim Anlegen neuer Accounts, die entsprechende Passwort-Policy und die zwingend notwendigen Attribute der jeweiligen organisatorischen Einheiten beachtet werden. Die dafür notwendigen Richtlinien müssen durch ein in der Föderation definiertes „Regelwerk“ festgelegt werden.

2.3 Synchronisation

Die verschiedenen organisatorischen Einheiten einer Universität verfügen über unterschiedliche Datenbanken und Verzeichnisdienste, die unter anderem personenbezogene Daten speichern. Diese Daten lassen sich in zwei Klassen unterteilen. Es gibt zum einen satellitenrelevante Daten, die nur im Satellitenkontext von Bedeutung sind und zum anderen satellitenübergreifende Daten, die in allen Satelliten konsistent sein sollen. Der föderative Synchronisationsdienst ermöglicht, dass kongruente satellitenübergreifende Daten in den verschiedenen Satelliten synchronisiert werden können. Der Synchronisationsdienst bedient sich des Identifier Mapping Service um sicherzustellen, dass die richtigen Datensätze miteinander synchronisiert werden. Außerdem werden die Synchronisationsdatenflüsse konfiguriert und für ein späteres Auditing und Reporting überwacht. Dabei wird durch das „Regelwerk“ in der Föderation festgelegt, für welche Datenattribute ein Satellit die autoritative Quelle repräsentiert, also berechtigt ist, bestimmte Attributinformation eines Datensatzes bei den anderen Satelliten zu überschreiben. Dadurch wird sichergestellt, dass klar geregelt ist, welcher Satellit für welche Attribute die Verantwortung hat, und dass die Daten aktuell und korrekt sind. Eventuelle Inkonsistenzen durch Race Conditions bei Datenaktualisierung werden dadurch vermieden. Für die Erstellung der Synchronisationsdatenflüsse werden Modellierungs- und Überwachungswerkzeuge benötigt, damit vereinbarte Synchronisationsrichtlinien zwischen den Satelliten auch wirklich berücksichtigt werden. Zusätzlich werden für die Synchronisation Konnektoren für die einzelnen Datenquellen benötigt. Diese Datenkonnektoren müssen einen konsistenten Lese- und Schreibzugriff auf die unterschiedlichsten Datenquellen ermöglichen. Darüber hinaus muss für den Zugriff eine entsprechende Transaktionsverwaltung gegeben sein.
Bei der Kapselung einer Datenquelle durch einen Web Service ist es aus Sicht des Datensynchronisationssystems ein Vorteil, dass zu den unterschiedlichsten Datenquellen eine feste Schnittstelle vorhanden ist, über die beruhend auf Standards beispielsweise Zugriffsrichtlinien und Sicherheitsstandards generisch unabhängig vom Typ der Datenquelle umgesetzt werden

können. Aus Sicht des Satelliten bietet ein Web Service zum einen den Vorteil, dass kein direkten Zugriff auf seine Datenbasis gewährt wird, sondern über den Web Service kontrolliert wird, welche Daten aktualisiert werden. Zum anderen kann das Datensynchronisationssystem ausgetauscht werden, ohne satellitenseitige Änderungen vornehmen zu müssen. Darüber hinaus kann der Satellit selbstständig die Datensynchronisation den lokalen Gegebenheiten anpassen, und vor und nach der Synchronisation lokale Geschäftsprozesse auslösen.

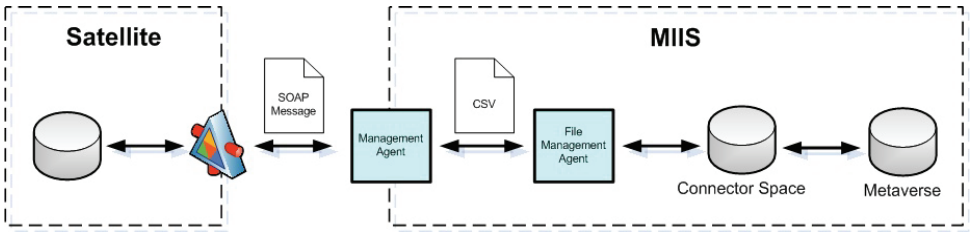


Abb. 9: MIIS Web Service Konnektor

Prototypisch wurde ein Web Service Konnektor für den Microsoft Identity Integration Server 2003 (MIIS) und auf Seite des Satelliten für eine PostgreSQL Datenbank ein Web Service entwickelt (Abb. 9). Auf eine ausführlichere Beschreibung der Prototypen verzichten wir aufgrund des gegebenen Rahmens der Arbeit. Während der Entwicklung des Prototyps hat sich herausgestellt, dass der MIIS ohne zusätzliche Erweiterungen von Drittanbietern ein reines Datensynchronisationswerkzeug darstellt. Weitere von uns geforderten Funktionalitäten, wie beispielsweise Unterstützung von Geschäftsprozessen, Unterstützung von in diesem Gebiet relevanten Standards (z.B. SPML und XACML) und umfangreichen Auditing und Report Funktionalitäten hat uns dazu bewogen, die SUN Identity Management Suite zu evaluieren. Diese bietet ein umfangreiches Spektrum an Werkzeugen von der Datensynchronisation über Zugriffsmanagement bis zur Selbstbedienungskomponente an und wird zukünftig als Open Source zur Verfügung stehen, wodurch eine Universität befähigt wird, individuelle Erweiterungen durchzuführen.

2.4 Authentifikation

Ein Ziel des Identity Managements ist es, eine Grundlage zur möglichst einfachen und schnellen Integration neuer Dienste zu realisieren. Identitätsbezogene Dienste können jedoch nicht ohne Authentifikation und einer sicheren Gewährleistung der Identität des Nutzers

angeboten werden. Das föderative und dienstorientierte Identitätsmanagement stellt für diesen Zweck die entfernte Authentifikation unter anderem über einen Web Service zur Verfügung. Dies vereinfacht die Integration neuer Dienste, da Dienstanbieter nicht dazu gezwungen sind, eine eigene Benutzerverwaltung aufbauen und administrieren zu müssen. Es wäre denkbar, dass ein Benutzer mit Hilfe dieser Authentifikation auch Dienste außerhalb des universitären Kontexts nutzen kann, solange diesen Dienstanbietern erlaubt ist, den Authentifikationsdienst zu nutzen. Hier muss die Frage geklärt werden, wer diesen Dienst nutzen darf. Der Authentifikationsdienst ist nicht zum Einsatz für private Webseiten gedacht, da hierdurch der Anschein eines offiziellen Dienstes entstehen könnte. Dies kann durch die Verwendung auf Transportebene wie SSL mit Client-Authentication eingeschränkt werden, aber auch durch eine personenbezogene Zugriffskontrolle. In einem heterogenen Umfeld wie es an einer Universität vorzufinden ist, müssen mehrere Standardschnittstellen, wie z.B. LDAP und Web Services, angeboten werden. Vor allem die Bereitstellung einer Web Service Schnittstelle stellt eine Herausforderung dar, denn die Entwicklung der Web Service Technologien befindet sich im Bezug auf Sicherheitsfragen noch in einem frühen Stadium. Die WS-* Architektur, welche eine Vielzahl von Spezifikationen enthält, spielt hierbei eine zentrale Rolle, da hier Standards zu Sicherheit, Zuverlässigkeit und Transaktionen von Web Services realisiert werden [FSLS03]. WS-Security ist hierbei die Grundlage aller weiteren WS-* Spezifikationen und definiert Erweiterungen von SOAP. Zum einen dient WS-Security zur Gewährleistung von Vertraulichkeit und Integrität von SOAP Nachrichten, zum anderen spezifiziert WS-Security die Verwendung von Security Tokens, die zum sicheren Austausch von Identitätsdaten, Authentifikations- und Autorisationsinformationen in SOAP Nachrichten verwendet werden. Durch den Einsatz von diesen und weiteren Standards, wie WS-Metadataexchange, WS-SecurityPolicy, WS-Trust und WS-Federation, kann der von uns bereitgestellte Authentication Service eine sichere Authentifikation und Ausstellung eines Security Tokens gewährleisten. Problematisch hierbei sind sowohl die noch nicht vollständige Umsetzung aller Spezifikationen als auch die mangelnde Interoperabilität zwischen den implementierten Standards in verschiedenen Frameworks, wie beispielsweise in .Net und Java. Am weitesten Fortgeschritten ist die Umsetzung der WS-* Architektur mit der Windows Communication Foundation (WCF) in .Net. [Micr06]. Da in Java bisher nur rudimentäre Implementierungen von WS-* Standards vorhanden sind, beschäftigt sich aktuell SUN im Projekt Tango mit deren weiteren Umsetzung zur Erstellung der Web Service Interoperability Technology (WSIT) in Zusammenarbeit mit

Microsoft [HaCa06]. Die vollständige Integration dieser Technologien in Produkte ist auch bei Microsoft noch nicht abgeschlossen. Von uns benötigte Funktionalitäten, wie das Active Requestor Profile der WS-Federation Spezifikation zur aktiven Security Token Anfrage durch einen SOAP-fähigen Client, wird in Microsofts Implementierung von WS-Federation – Active Directory Federation Services (ADFS) – nicht unterstützt. Da frühestens 2008 mit einer Umsetzung zu rechnen ist, wurde im Rahmen unserer Arbeit eine Eigenimplementierung eines WCF-basierten Authentifikationsdienst umgesetzt. SUN ist in einem aktuellen Projekt – OpenSSO – im Moment dabei, WSIT in ihren SUN Access Manager zu integrieren und versucht somit die mangelnde WS-* Unterstützung zu überwinden [JNET06]. Letztlich ist es ein Ziel unserer Arbeit die Interoperabilität dieser beiden Welten zu gewährleisten (Abb. 10).

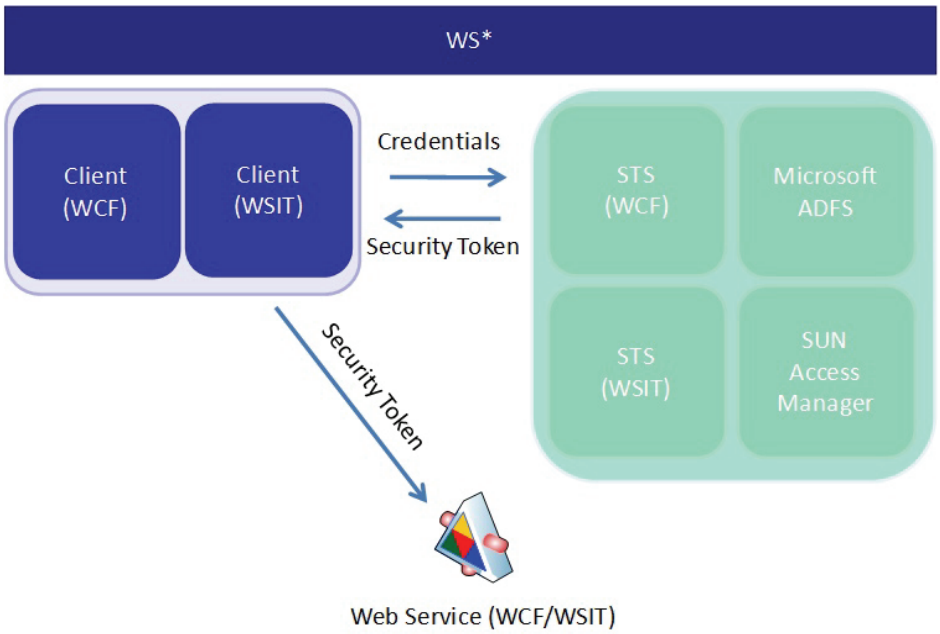


Abb. 10: Interoperabilität zwischen Microsoft und SUN Technologien

2.5 Self Service

Das Identitätsmanagement stellt nicht nur Infrastrukturdienste zur Verfügung, sondern auch Selbstbedienungsfunktionalität zur eigenverantwortlichen Verwaltung dieser Dienste. Die Selbstbedienung kann in mehrere Bereiche gegliedert werden. Zunächst wird dem Nutzer die Kontrollmöglichkeit, für welche Satelliten ein Single Sign-On erlaubt ist, gegeben und angeboten, seine persönlichen Daten zu aktualisieren. Der Nutzer stellt die autoritative Quelle für beispielsweise den aktuellen Wohnsitz dar. Diese Informationen werden nach der Eingabe

durch den Nutzer in die relevanten Satelliten synchronisiert, womit dieser nun immer unter der aktuellen Anschrift schriftlich für Mitteilungen der Universität, wie z.B. Mahnungen der Universitätsbibliothek, erreichbar ist. Weiterhin können leicht neue Funktionen, wie beispielsweise ein zukünftiges Passwortmanagement, in die Selbstbedienung integriert und angeboten werden. Diese Dienste werden im Rahmen des KIM-Projekts entstehenden Microsoft Office Sharepoint Services 2007 Portals integriert werden, um für den Nutzer an einer zentralen Stelle, alle Selbstbedienungsfunktionalitäten zu bündeln. Die Nutzung des Portals setzt einen ISS-Account voraus, der nur durch eine zuvor definierte harte Authentifikation angelegt wird.

2.5.1 User-Controlled Single Sign-On

In einer größeren heterogen Systemlandschaft, wie sie eine Universität darstellt, verfügt eine Entität in der Regel über mehrere Accounts, über die diese auf verschiedene Ressourcen zugreifen kann. Der Zugriff auf diese Ressourcen gestaltet sich mühsam, wenn sich eine Entität bei jedem neuen Ressourcenzugriff neu authentifizieren muss, damit ihr der Zugriff gewährt wird. Darüber hinaus benötigen verteilte Anwendungen, die in Namen einer Entität auf verschiedene Ressourcen zugreifen müssen, einen Mechanismus, der es ermöglicht, ohne wiederkehrende Reauthentifikation einen kontrollierten Zugriff zu erlauben.

Der kontrollierbare Single Sign-On Dienst bietet einen Mechanismus, über den ein sicherer Ressourcenzugriff ohne wiederkehrende Reauthentifikation realisiert wird. Der Benutzer authentifiziert sich initial mit dem ISS Account am Authentication Service, der nach erfolgreicher Authentifikation einen Security Token ausstellt.

Mit Hilfe dieses Security Tokens kann die Entität bzw. die in seinem Namen agierende Applikation sich bei anderen Diensten authentifizieren und auf die jeweiligen Ressourcen zugreifen. Da die potentielle Gefahr besteht, dass eine Applikation mit Hilfe des Security Tokens im Hintergrund auf sensitive Ressourcen zugreift und nicht beabsichtigte Veränderungen durchführt, soll der Benutzer in der Lage sein, den Single Sign-On Mechanismus einzuschränken. Hierzu bietet der ISS Single Sign-On Dienst dem Benutzer die Möglichkeit, individuell einzustellen, auf welche Systeme respektive Dienste die SSO Einschränkungen wirksam sein sollen. Der SSO Dienst kann für komplette Satelliten deaktiviert bzw. mit weiteren Authentifikationsmechanismen (z.B. PIN/TAN Abfrage) abgesichert werden. Dabei müssen die Konsequenzen der jeweiligen SSO Einschränkungen für den Benutzer klar und verständlich dargestellt werden. Darüber hinaus stellt der ISS Account für einen

eventuellen Angreifer ein attraktives Ziel dar, da über ihn Zugriff auf verschiedene Systeme erlangt werden kann. Daher sollte die Passwort Policy des ISS Accounts mindestens so restriktiv sein wie die restriktivste Passwort Policy der erreichbaren Systeme. Sollte ein potentieller Angreifer Zugang auf einen ISS Account erlangt haben, würden ihn noch die individuellen SSO Einstellungen einschränken, weshalb diese ebenfalls mit einem weiteren Schutzmechanismus versehen werden sollten.

3 Anwendungsdienste

Basierend auf den föderierten Identitätsmanagementdiensten erlauben Anwendungsdienste die Etablierung organisationsübergreifender Geschäftsprozesse. In der ersten Phase wurde der Bedarf an einem generellen Dienst zur Auslieferung von Nachrichten an frei spezifizierbare Gruppen identifiziert. Im nächsten Abschnitt wird auf die Konzeption dieses Dienstes und dessen Interaktion mit unseren Identitätsmanagementdiensten eingegangen.

3.1 Erreichbarkeit

Einer der ersten Dienste, die die Infrastruktur des Identitätsmanagements nutzen, stellt der Erreichbarkeitsdienst (Recipient Service) dar. Dieser Dienst ermöglicht die Übermittlung einer Nachricht via Email an eine individuell spezifizierbare Gruppe von Empfängern, die nach vorgegebenen Kriterien ausgewählt werden kann. Dem Erreichbarkeitsdienst, der als Web Service implementiert wird, kann hierbei authentifiziert, signiert und verschlüsselt eine Nachricht gemeinsam mit der Spezifikation der Zielgruppe übermittelt werden. Abb. 11 zeigt die Systeme und Identitätsmanagementdienste, mit denen der Recipient Service interagiert. Durch die Einbindung dieses Dienstes in ein Portal kann ein Nutzer diesen Dienst aufrufen. Hierfür wird der Nutzer zunächst über das Portal authentifiziert, wodurch dieses einen Token erhält, mit dem beispielsweise der Erreichbarkeitsdienst aufgerufen werden kann. Hierfür müssen die Dienste untereinander eine Vertrauensbeziehung eingehen. Der Nutzer kann nach erfolgreicher Authentifikation eine Nachricht an eine Zielgruppe senden. Die Beschreibung der Zielgruppe erfolgt über vordefinierte Parameter, wie Alter, Geschlecht, Mitarbeiter, Student, Alumni, Angehöriger eines bestimmten Instituts, usw. Eine Orchestrierung von Web Services erledigt daraufhin die Besorgung der Informationen, um alle Mitglieder der Zielgruppe erreichen zu können. Zum Zugriff auf die unterliegenden Information Services benötigt der

Recipient Service ein Security Token, das er vom Authentication Service erhält. Jedem Informationsdienst werden die für ihn spezifischen Attribute übermittelt, worauf diese in ihren jeweiligen Datenquellen nach den Einträgen suchen und letztlich deren Identifikatoren an den Erreichbarkeitsdienst zurücksenden. Die Identifikatoren werden je nach Art der Handhabung durch den Identifier Mapping Service in globale Identifikatoren überführt.

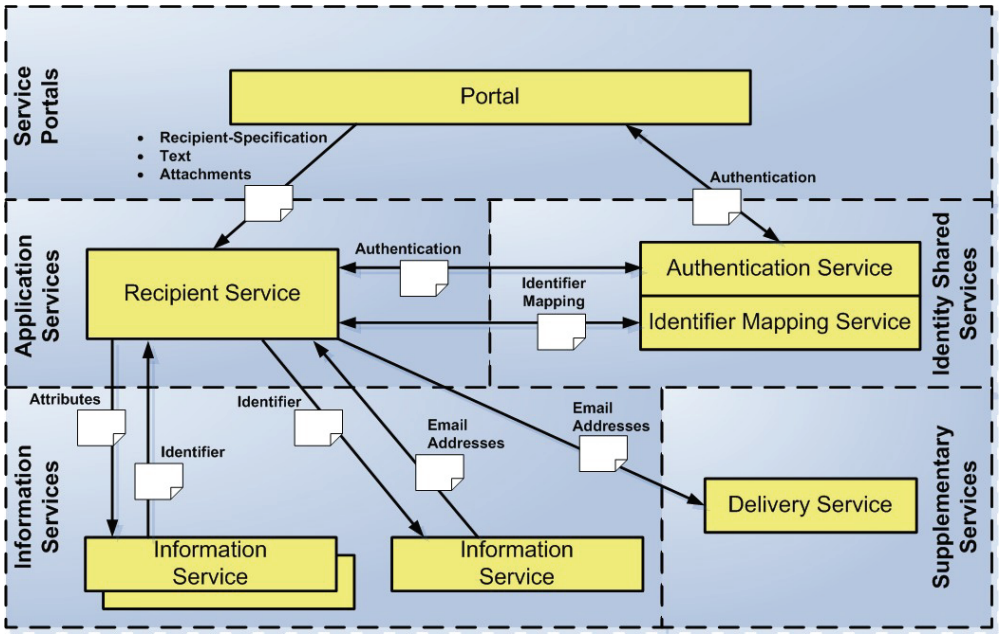


Abb. 11: Interaktionen des Recipient Service

Diese werden einem dedizierten Informationsdienst übergeben, der dem Recipient Service die zugehörigen Email-Adressen zurückliefert. Abschließend wird einem weiteren Dienst, der zur Ausstellung von Emails dient, die Email-Adressen und die Nachricht übermittelt. Dieser versendet die Nachricht an alle Email-Adressen über einen universitätseigenen SMTP-Server.

4 Zusammenfassung & Ausblick

In diesem Beitrag wurde aufbauend auf den grundlegenden Leitgedanken der Föderation und Dienstorientierung eine Konkretisierung der notwendigen Identitätsmanagementdienste vorgestellt. Diese Dienste bieten eine Grundlage für organisationsübergreifende Geschäftsprozesse in einer heterogenen Umgebung. Durch Mechanismen, wie die entfernte Authentifikation, (De-)Provisionierung und Synchronisation wird sowohl die Sicherheit, als auch die Aktualität der Datenbestände innerhalb der Föderation gewährleistet. Dabei wurde bei

der Umsetzung eine aktuelle Interoperabilitätsproblematik im Bezug auf Web Service Sicherheit festgestellt, welche die Interaktion unserer Dienste erschwert und zurzeit nur durch Eigenentwicklungen überwunden werden kann. Wir haben anhand eines exemplarischen Anwendungsdienstes demonstriert, wie die von uns identifizierten Identitätsmanagementdienste integriert werden. Die Bereitstellung der Identitätsmanagementdienste und deren Integration in weitere Anwendungsdienste fördert eine lebendige Dienstevielfalt, wodurch IT-gestützte Prozesse und Dienste in Lehre, Forschung und Weiterbildung flexibel unterstützt werden.

Literaturverzeichnis

[FSLS03] Ferguson, Donald F.; Storey, Tony; Lovering, Brad; Shewchuck, John: Secure, Reliable, Transacted Web Services: Architecture and Composition. http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/wsoverview.asp, 2003, Abruf am 2006-12-08.

[HaCa06] Carr, Harold: Sun's Project Tango. http://java.sun.com/developer/technicalArticles/glassfish/ProjectTango/index.html, 2006-06-01, Abruf am 2006-12-08.

[HMSW06] Höllrigl, Thorsten; Maurer, Axel; Schell, Frank; Wenske, Horst; Hartenstein, Hannes: Dienstorientiertes Identitätsmanagement für eine Pervasive University. Dresden, 2006.

[HoRe05] Hommel, Wolfgang; Reiser, Helmut: Federated Identity Management: Die Notwendigkeit zentraler Koordinationsdienste, Kaiserslautern, 2005.

[Micr06] Microsoft .Net Framework: Windows Communication Foundation, http://wcf.netfx3.com/index.html, Abruf am 2006-12-08.

[JNET06] Java.Net: OpenSSO Project, https://opensso.dev.java.net/ index.html, Abruf am 2006-12-08.

[ZiKG04] Zimmermann, Olaf; Krogdahl, Pal; Gee, Clive: Elements of Service-Oriented Analysis and Design - An interdisciplinary modeling approach for SOA projects. http://www-128.ibm.com/developerworks/webservices/library/ws-soad1/index.html, 2004-06-02, Abruf am 2006-12-08.

IDM@eCampus.HH

Identity Management am Hochschulstandort Hamburg

Prof. Dr. Martin Gennis

Hochschule für Angewandte Wissenschaften Hamburg
20099 Hamburg
martin.gennis@bui.haw-hamburg.de

Dr. Stefan Gradmann

Regionales Rechenzentrum
Universität Hamburg
20146 Hamburg
stefan.gradmann@rrz.uni-hamburg.de

Stefanie Winklmeier

Multimedia Kontor Hamburg GmbH
22083 Hamburg
s.winklmeier@mmkh.de

Abstract

Ziel des Hamburger Identity Management (IDM) Projektes eCampus II ist der Aufbau eines gemeinsamen Identity Management Systems, im Zuge dessen ein konsolidierter Bestand der Studierenden- und Mitarbeiter-Identitäten der Hamburger Hochschulen bereit gestellt und grundlegende Verfahren für das Management dieser Identitäten etabliert werden sollen. Der Fokus liegt zunächst auf einem technischen Kommunikationsrahmen, der Implementierung gemeinsam genutzter IDM-Komponenten und dem Aufbau eines gemeinsamen Organisationsmodells. In der Folge werden gemeinsam nutzbare Verfahren für die Anbindung der jeweiligen ‚Corporate Directories' entstehen, der notorisch ‚abgekapselte' Bibliotheksbereich eingebunden und die Hamburger Hochschulen in das bundesweit im Aufbau befindliche Trust-Szenario DFN-AAI gemeinsame eingebunden.

Ausgangspunkt dieses Vorhabens war das vorangegangene Projekt eCampus I, in dessen Rahmen die Hamburger Hochschulen gemeinsam mit dem Multimedia Kontor Hamburg

(MMKH) die hier dargestellte und nunmehr zur Umsetzung vorgesehene Konzeption entwickelt haben [Ecam03].

Das Folgeprojekt eCampus II ist Teil einer Gesamtstrategie, welche die möglichst nahtlose und effiziente Integration der Hamburger Hochschulen in die digitale Neuformationen der Lehr-, Lern- und Forschungsumgebungen ermöglichen soll und damit die Chancen des Hochschulstandorts Hamburg insgesamt in den Bereichen eLearning und eScience deutlich fördert.

1 Das eCampus-Projekt und seine Entstehung

Im Rahmen des E-Learning-Förderprogramms der Behörde für Wissenschaft und Forschung der Freien und Hansestadt Hamburg (BWF) entstand im Frühjahr 2004 ein Konzeptpapier des MMKH mit dem Titel „eCampus 2010 - Auf dem Weg zu einer integrierten IT-Dienste-Infrastruktur der Hamburger Hochschulen“. Die Studie ergab, dass eine IT-gestützte, hochschulübergreifende Erneuerung der Organisation und Verwaltung der Hamburger Hochschulen nicht nur unabdingbar für ein modernes, flexibles und leistungsfähiges Hamburger Wissenschaftssystem ist, sondern auch die Voraussetzung für innovative und attraktive Studien- und Weiterbildungsangebote aus den Hochschulen.

Mit Blick auf diesen Bedarf wurde das Projekt eCampus I als ein gemeinsames Vorhaben der öffentlichen Hamburger Hochschulen und der BWF ins Leben gerufen [Haus05]. Hierbei sollten in erster Linie durch einen hochschulübergreifenden Erfahrungsaustausch Kooperations- und Synergiepotentiale zu IT-Infrastrukturen und Services, sowie zur gemeinsamen Strategieentwicklung zu Verfahren, Systemen und Organisationsprozessen ausgelotet werden. Damit sollten zukünftige Modernisierungsvorhaben unterstützt und hamburgweite Interoperabilität und Ressourcensharing ermöglicht werden.

2 AG Basisdienste – Themenauswahl

Da das Projekt eCampus I einen sehr umfassenden Ansatz verfolgte und daher schnell eine hohe Komplexität des Aufgabengebiets erkennbar war, wurden Arbeitsgruppen mit unterschiedlichen thematischen Schwerpunkten gegründet (AG Best-Practice und Benchmarking, AG Prüfung

und Veranstaltung, AG Studierende, AG Webauftritt, AG Basisdienste). Die Gesamtstruktur des Projektes ist schematisch in untenstehender Abb. 1 dargestellt.

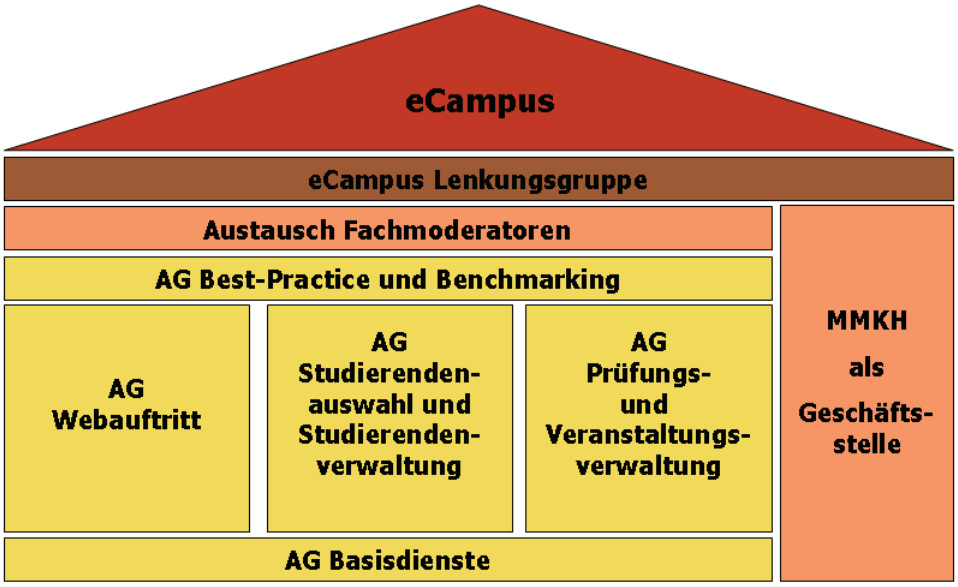


Abb. 12 Projektarchitektur eCampus I

Beteiligt waren am Projekt eCampus I neben dem MMKH als Geschäftsstelle die folgenden Hochschulen:

- Universität Hamburg
- Hochschule für Angewandte Wissenschaften Hamburg
- Technische Universität Hamburg-Harburg
- Hochschule für Bildende Künste Hamburg
- Hochschule für Musik und Theater Hamburg

Dabei kam der Arbeitsgruppe Basisdienste eine schon in ihrer Benennung angedeutete grundlegende Funktion zu: Ihre Zielsetzung war es, durch Zusammenarbeit mit den Hamburger Hochschulen die Anforderungen zentraler oder zumindest gemeinsamer IT-Basisdienste zu identifizieren und die inhaltlichen und strategischen Voraussetzungen für die Entwicklung angemessener Lösungen zu schaffen.

Für die AG Basisdienste rückte nicht überraschend das Thema „triple A“ (Authentifizierung, Autorisierung und Accounting) als strategische Querschnittstechnologie rasch in den zentralen

Fokus. Sie setzte sich daher das Ziel, eine Hamburg-weite Identity Management Lösung zu entwerfen.

Die Hauptmotivation für die Befassung mit diesem Thema war der Wunsch, die Grundlagen für eine echte Single Sign-On (SSO) Lösung zu schaffen und damit den Abschied von der Erfordernis einzuleiten, für jeden Dienst ein eigenes Passwort verwalten zu müssen. Dieser Zustand ist aus Nutzersicht extrem unkomfortabel und stellt Administratoren regelmäßig vor praktisch unbeherrschbare Situationen. Sich mit einem Passwort anzumelden und alle Services nutzen zu können, war und ist eine der mit der Einführung eines Hamburg-weiten Identity Management Systems verbundene Zielvorstellung. Darüber hinaus sollten die Dienste allen denjenigen, die sie benötigen, automatisiert bereit gestellt werden. Nach dem erfolgreichen Abschluss des Studiums bzw. nach Beendigung des Arbeitsverhältnisses sollten die Zugangsberechtigungen auch automatisch wieder entzogen werden. Die Einführung eins IDM stellt also einen echten Mehrwert dar – nicht nur für Studierende, sondern auch für Alumni, Lehrende, Forschende und Verwaltungsmitarbeiterinnen und -mitarbeiter. Über diesen für den Endnutzer unmittelbar offensichtlichen Nutzen hinaus bedient ein Identity Management System eine Reihe weiterer administrativer Anforderungen von Hochschulen, beispielsweise im Bereich des Datenschutzes und der Datensicherheit [Wind05].

2.1 Marktsichtung und verwandte Projekte

Als erster Schritt der AG Basisdienste wurde die Situation in Bezug auf vorhandene IT-Infrastruktur, Verzeichnisdienste und Authentifizierungslösungen der Hamburger Hochschulen untersucht. Daran anschließend wurde auf Basis der verfügbaren Vorarbeiten (namentlich einer Arbeitsgruppe zu Authentifizierung und Autorisierung (Au²) am RRZ der Universität Hamburg) eine Marktsichtung in Bezug auf vorhandene IT-Produkte und Lösungen durchgeführt. Parallel dazu wurde der Kontakt zu Identity-Management-Projekten an Hochschulen und verwandten Initiativen im Hochschulumfeld gesucht.

Um einen Überblick über den aktuellen Stand der technischen Umsetzungen zu erlangen, wurden folgende marktführende Hersteller von IDM-Lösungen zu Präsentationen und Demonstrationen eingeladen:

- Sun (Identity Manager)
- Novell (eDirectory)
- Microsoft (AD/MIIS)

- Siemens (DirX)

Um von bereits vorliegenden Erfahrungen zu profitieren und bereits bekannte Fehler vermeiden zu können, erfolgte außerdem ein Austausch durch Besuche bzw. Einladungen nach Hamburg mit folgenden bekannten IDM-/Authentifizierungsprojekten:

- SWITCH-AAI (Zürich) [Swit06]
- AAR (Universität Freiburg) [Ober06]
- OFFIS (Universität Oldenburg) [Offi07]
- SOI (mehrere Hochschulen und Rechenzentren in Niedersachsen) [Schu05]
- IntegraTUM (Technische Universität München) [Inte06]
- NRW-Landesprojekt [Reso05]

2.2 hhEduPerson-Schema und Hamburg-weit einheitlicher Benutzeraccount

Zur Entscheidungsfindung für einen eigenen Lösungsansatz wurden die (Quasi-)Standards LDAP, LDIF, Liberty, Shibboleth, SAML, SOAP sowie eduPerson betrachtet. Für die Attribut-Spezifikation wurde das hhEduPerson-Schema auf Grundlage des eduPerson-Schemas [Educ07] sowie weiterer bestehender nationaler und internationaler Schemata (swissEduPerson, schac-Schema der TERENA [Tere07]) erarbeitet. Die Attributmenge hhEduPerson stellt die gemeinsam festgelegte Schnittmenge an Standardattributen dar, die über die Grenzen der Hochschulverzeichnisse hinweg bekannt und transportierbar sein sollen. Bei der Attributspezifikation wurde ein eher minimalistischer Ansatz verfolgt.
Weiter wurden Syntax und Bildungsregeln für Hamburg-weit einheitliche Benennungen von Benutzeraccounts vereinbart.
Vor allem aber wurde hinsichtlich der grundlegenden Systemarchitektur eines gemeinsamen Identity-Management-Ansatzes ein gemeinsamer Konsens hergestellt. Die dabei diskutierten Alternativen und das erreichte Ergebnis sind im folgenden Abschnitt dargestellt.

3 Diskussion der Identity Management-Ansätze

Schon zu Beginn der Zusammenarbeit stellten sich Heterogenität und Verteiltheit als bestimmende Faktoren am Hochschulstandort Hamburg heraus. Die AG Basisdienste

diskutierte daher mehrere technische Linien als mögliche Lösungsansätze der zukünftigen Identity Management-Systemarchitektur.

3.1 Peer to Peer (P2P) Ansatz

Die in den Hochschulen aufgebauten Verzeichnisse werden in diesem Szenario Teil einer virtuellen LDAP-Infrastruktur, wie sie in Abb. 2 (P2P Ansatz) dargestellt ist. Die Directories verfügen dabei über den gemeinsamen Attributrahmen und hochschulübergreifende User-IDs und können über Verweisstrukturen (Referral) oder das so genannte ‚chaining' aufeinander Bezug nehmen und Attributwerte austauschen.

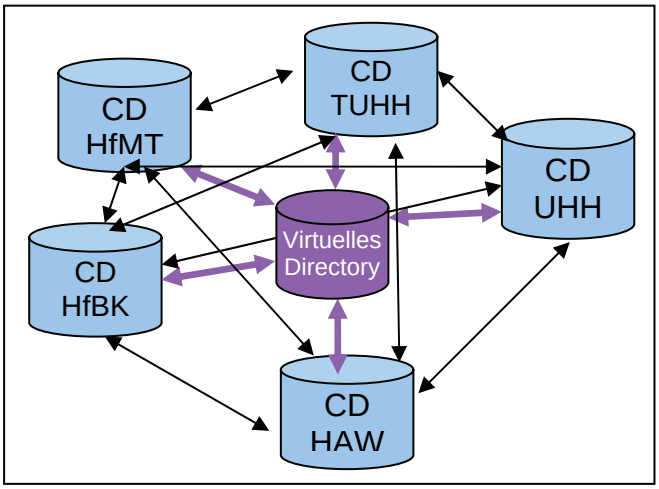


Abb. 13 P2P Ansatz

Konsolidierung und Provisionierung verlaufen in diesem Ansatz rein lokal über die jeweiligen Hochschulverzeichnisse. Einen höheren Integrationsgrad erhielte dies Szenario durch den zusätzlichen Aufbau eines ‚Virtual Directory', für das mehrere Implementierungsvarianten denkbar sind. Die Zuständigkeit für die gespeicherten Daten verbleibt in den Hochschulen; dies betrifft den funktionalen Betrieb wie auch den Datenschutz.
Ein solches Virtuelles Directory unterstützt beispielsweise den wechselseitigen Zugriff auf eLearning-Plattformen, ein hamburgweites Adressbuch der Hochschulmitarbeiter und Self-Services für die Änderung von vordefinierten Attributinhalten.

3.2 Metadirectory-Ansatz

Der Metadirectory-Ansatz geht bezüglich des Integrationsgrades und der daraus resultierenden Funktionalität erheblich über das erste Szenario hinaus und ist in Abb. 14 dargestellt. Eine Identity-Management-Lösung (IDM) führt dabei Informationen aus bestehenden

Benutzerverwaltungen zu Identitäten zusammen. Jede Identität steht in einer 1:1- Beziehung zu einer natürlichen Person. Damit steht zu jedem Zeitpunkt allen vom IDM versorgten Systemen ein integrer Stammdatenbestand von Benutzer-Identitäten zur Verfügung.

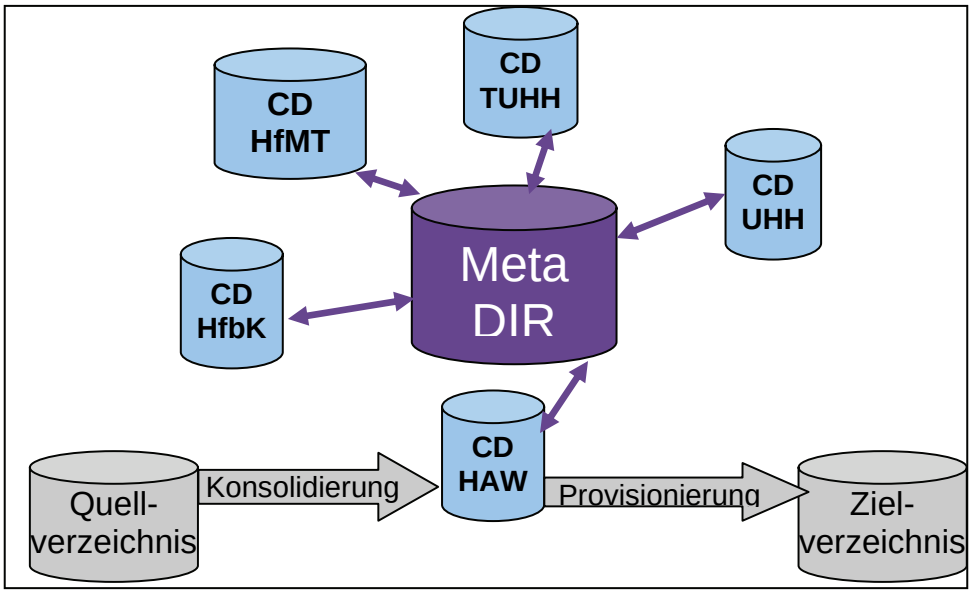


Abb. 14: Metadirectory-Ansatz

Konsolidierung und Provisionierung verlaufen jedoch auch in diesem Ansatz rein lokal über die jeweiligen Hochschulverzeichnisse.

3.3 Föderierter Ansatz

Dieser Ansatz ist zu den beiden vorher dargestellten Szenarien komplementär: Er zielt auf die Integration des hamburgweiten Authentifizierungsmodells in großflächigere, überregionale oder gar transnationale Kooperationsszenarien. Eine Schlüsselrolle nimmt dabei das auf dem SAML-Standard basierende Shibboleth-Modell [Shib07] ein.

Das Modell unterscheidet im Wesentlichen zwei Hauptrollen – die eines Anbieters von Authentifizierungsinformationen (sog. „ID-Provider“) und diejenige eines Anbieters von Diensten („Service-Provider“). Klärungsbedürftig war, ob die Hamburger Hochschulen als ID-Provider gemeinsam angesprochen werden (Abb. 15) oder ob jede Hochschule separat als ID-Provider auftritt (Abb. 16), bei dem sich ein Hochschulangehöriger in gewohnter Weise authentifizieren kann. Damit zusammen hängt ggf. die Entscheidung für ein sog. virtuelles Directory oder Metadirectory und für die Einführung einer hochschulübergreifenden Public-Key Infrastructure (PKI), über die der Nutzer zertifikatsbasiert Zugang zu den WWW-Diensten

der anderen Kooperationspartner erhalten könnte. Zugleich können Hochschulen als Service-Provider auftreten, die mit bestimmten Identity-Providern ein Vertrauensverhältnis eingehen. Die Mittlerrolle übernimmt ein Where-Are-You-From-Dienst (WAYF), der den Service-Providern zugeordnet oder zentral betrieben werden kann.

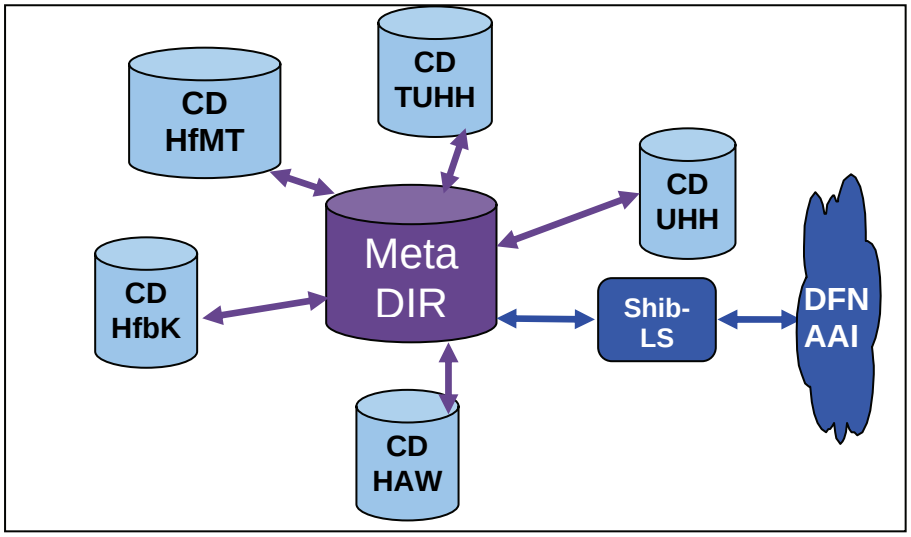


Abb. 15: Variante 1 - Hamburger Hochschulen als ein gemeinsamer ID-Provider

Service-Provider können von Identity-Providern zusätzliche Attribute anfordern, um über den Zugriff auf Ressourcen zu entscheiden. Anzustreben ist die Implementierung eines so genannten 'Local Service' entweder für alle Hamburger Hochschulen gemeinsam oder für jede der Hochschulen als separaten Identity-Provider, dessen Authentifizierungsinformationen vom lokalen Verzeichnisdienst geliefert werden, oder eine Direktanbindung der Hochschulverzeichnisse an einen gemeinsam betriebenen Identity-Provision-Service.

Die Hochschulen werden dabei Teil einer – nach den Plänen des DFN-Vereins [Kaeh06] deutschlandweiten – Föderation, in der die Universitäten protokollbasiert Trust-Beziehungen untereinander aufbauen und den Mitgliedern anderer Hochschulen Zugangsrechte zu den eigenen WWW-Diensten gewähren können. Die Zuständigkeit für die gespeicherten Daten verbleibt in den Hochschulen. Shibboleth gibt Nutzern die Möglichkeit, zu bestimmen, welche persönlichen Daten die heimische Organisation weitergeben darf und genügt damit dem Kriterium der informationellen Selbstbestimmung.

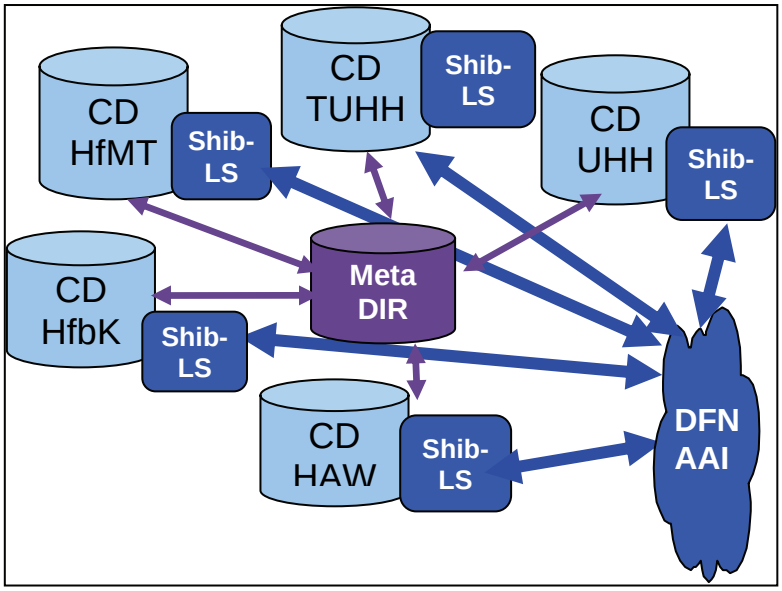


Abb. 16:Variante 2 - jede Hamburger Hochschule ist ein eigener ID-Provider

3.4 Hamburger Ansatz (eCampus II)

Für den Hochschulstandort Hamburg mit seinen spezifischen Bedingungen war nach Bewertung der AG Basisdienste eine besondere Variante des Metadirectory-Ansatzes die angemessenste Lösung. Bei diesem Ansatz betreiben die Hochschulen ein gemeinsames Identity-Management-System (IDMS) als Back-Office-Funktion, aus dem heraus die jeweiligen Corporate Directories der Hochschulen als die eigentlichen Authentifizierungsinstanzen provisioniert werden. Die untenstehende Abb. 17 deutet dies für das Beispiel der Hochschule für Angewandte Wissenschaften (HAW) an.

Das IDM wertet die Quellsysteme der Hochschulen in fest definierten Intervallen aus und generiert daraus die eindeutigen Personendatensätze. Jeder Personendatensatz repräsentiert die Identität einer Person, welche im IDM eine oder mehrere Rollen zugewiesen bekommt. Die einer Identität zugewiesenen Rollen steuern die automatisierte Vergabe von Rechten in den vom IDM zu befüllenden Zielsystemen.

Prinzipiell sind Zielsysteme alle Systeme der beteiligten Hochschulen, die von dem IDM Daten erhalten. Bei einem Zielsystem kann es sich z.B. um ein Verzeichnis handeln, das von unterschiedlichen Anwendungen zur Benutzerauthentifizierung abgefragt wird. Ein Verzeichnis mit dieser Funktion wird als Corporate Directory bezeichnet. Das IDM kann genutzt werden, um weitere Zielsysteme (z.B. Verzeichnisse) einer Hochschule/ eines Standortes/einer Fakultät mit konsistenten Identitätsdaten zu befüllen, die dort z.B. zur Steuerung des lokalen Zugriffs auf

Datei- und Druckdienste dienen. Zielsysteme können auch Datenbanksysteme oder andere IT-Systeme sein, die über eine eigene Benutzerverwaltung verfügen. Das IDM kann diese Benutzerverwaltungen mit Hilfe geeigneter Konnektoren fortlaufend mit aktuellen Benutzerdaten provisionieren.

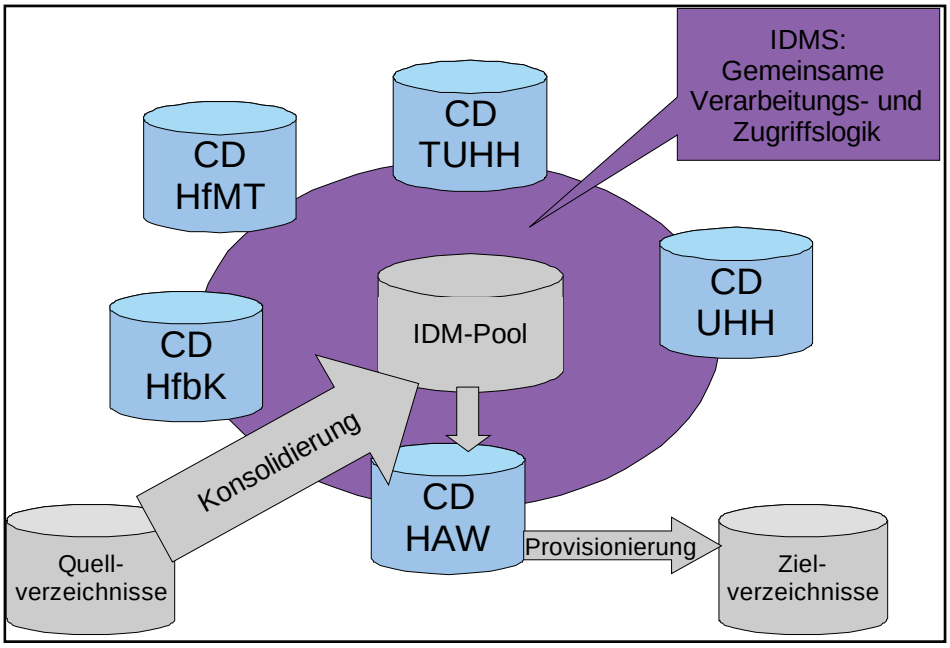


Abb. 17: Der eCampus-Ansatz

Diese Lösung stellt eine zukunftsweisende, sehr weitgehende Konzeption mit einem hohen Synergiepotential dar. Denn durch die Einführung einer gemeinsamen Identity-Management-Lösung für alle Hamburger Hochschulen sind unmittelbare und mittelbare Vorteile auf unterschiedlichen Ebenen und für die verschiedenen beteiligten Gruppen erreichbar.

Die Studierenden werden ebenso davon profitieren wie die Lehrenden und Forschenden, das Personal im technischen Umfeld ebenso wie die Beschäftigten im Verwaltungsbereich. Ein Mehrwert ist zu verzeichnen auf der Benutzungsebene, auf der IT-Administrationsebene, auf der Verwaltungsebene für Studien- und Forschungsprozesse und nicht zuletzt auf der entwicklungsorientierten Infrastrukturebene. In Zeiten knapper werdender Ressourcen mit gleichzeitig steigenden Anforderungen sind die zu erwartenden Synergieeffekte nicht zu vernachlässigen. Die folgende Aufzählung zeigt eine Auswahl der zu erwartenden Vorteile.

Vorteile für Studierende:

- Automatische Erstellung einer Zugangsberechtigung unmittelbar nach der Immatrikulation. Damit kann die Studentin bzw. der Student sofort die

Kommunikationsstrukturen und die von ihr/ihm benötigten Dienste der Hochschule nutzen.

- Automatische Verlängerung der Berechtigungen nach erfolgreicher Rückmeldung bzw. automatische Löschung dieser Zugangsberechtigungen beim Verlassen der Hochschule.
- Bereitstellung bestimmter Dienste unter Verwendung des Accounts z.T. noch vor Studiumsantritt:
- Automatisch bereitgestellter E-Mail Zugang,
- Ortsunabhängiger Zugriff auf einen zentralen Datenspeicher *(Homedirectory)*,
- Department- und Fakultäts-*Fileshare* (aufgrund der Departmentzugehörigkeit erhält der Studierende automatisch Zugriff auf diese beiden öffentlichen Speicherbereiche),
- Funknetz-Zugang (Zugriff auf das Netzwerk über die WLAN-Infrastruktur),
- Schnelle und unkomplizierte Passwortänderungen und ggf. Neuvergabe von jeder internetfähigen Arbeitsstation aus mit automatischer und zeitnaher Verteilung an alle angeschlossenen Zielsysteme *(Self-Services)*.

Vorteile für Lehrende und Forschende:

- Entlastung von organisatorischen Aufgaben, speziell auch am Anfang und Ende eines Semesters.
- Vereinfachte Kommunikationsmöglichkeiten mit den eigenen Studierenden durch standardisierte eMail-Adressen, aufgabenorientierte Autorisierungsverfahren, wie etwa Zugriffssteuerung auf studienrelevante Applikationen und Daten.
- Einfache und sichere Bereitstellung von Studienmaterialien durch eine zentrale Datenhaltung.
- Standardisierte und einfache, zeit- und ortsunabhängige Nutzung gemeinsamer Daten im Forschungsumfeld.

Vorteile für alle Beschäftigten der Hamburger Hochschulen:

- Reduzierung von Komplexitäten im Verwaltungsumfeld durch hochschulübergreifende Strukturen.
- Nutzung des Intranets mit der standardisierten Zugangsberechtigung zur Optimierung bestimmter Arbeitsprozesse in zentralen Bereichen – wie z.B. beim Personalservice.
- Automatische Erstellung einer Zugangsberechtigung, die die direkte Dienstaufnahme ermöglicht.
- Zeitnahe Änderungen an Personendaten mit unmittelbarer Provisionierung in die angeschlossenen Zielsysteme. Hierdurch ergeben sich wesentlich kürzere Verarbeitungszeiten.

Vorteile für die IT-Administration der Hamburger Hochschulen:

- Senkung des Administrationsaufwandes für die angeschlossenen Zielsysteme. Die den Departments nun zusätzlich zur Verfügung stehende Zeit kann zur weiteren Verbesserung des Benutzerservice mit seinen ständig steigenden Anforderungen genutzt werden.
- Kostensenkung durch gemeinsame Ressourcennutzung, z.B. Abschluss gemeinsamer Software-Verträge für IDM-Komponenten.

Allgemeine und zukünftige Vorteile für die Hamburger Hochschulen:

- Erhöhte Sicherheit: Eine gemeinsame IDM-Lösung ermöglicht an zentraler Stelle eine Übersicht über Personen mit ihren Zugangs- und sonstigen Berechtigungen. So ist es möglich, diese Berechtigung an zentraler Stelle schnell und sicher zu entziehen. Verlässt ein/e Studierende/r die Hochschule, wird der Account für einen bestimmten Zeitraum gesperrt, bis er nach einem weiteren definierten Zeitraum komplett gelöscht wird. Hiermit wird sichergestellt, dass kein an das IDM-System angeschlossener Dienst mehr missbräuchlich genutzt werden kann. Die IDM-Lösung schließt somit ein mögliches Sicherheitsrisiko durch nicht deaktivierte Accounts ausgeschiedener Personen aus.
- Verbesserte Integrierbarkeit weiterer Dienste wie z. B. Chipkarten- oder Gebäudezugangssysteme in bestehende Organisationsstrukturen.

- Erhöhte Flexibilität bei der Umsetzung neuer Strukturen, z. B. bei der Anbindung neuer Einzelverzeichnisse oder neu zu schaffender Fakultätsinfrastrukturen

Schon die hier aufgeführten Punkte zeigen, welcher Mehrwert durch die Einführung eines IDM für alle Hamburger Hochschulen geschaffen werden kann. So wird das IDM-System zum einen ein indirektes Hilfsmittel bei der Positionierung der Hamburger Hochschulen im bundesweiten und internationalen Wettbewerb darstellen, zum anderen aber auch eine direkte Wirkung im nationalen und internationalen Vergleich bei großen und anspruchsvollen IT-Projekten zeigen.
Dieses Synergiepotential kann die Lösung jedoch wirklich erst dann entfalten, wenn sie in eine institutionalisierte Kooperation der Hochschulen auf einer gemeinsamen technischen Basis eingebettet ist. Auch bedingt sie für das zentrale IDM eine von allen Hochschulen getragene Entscheidung für ein gemeinsam einzusetzendes technisches Werkzeug für den Verzeichnisaufbau, die Konsolidierung von Identitäten und deren (De-)Provisionierung.

4 eCampus II

Die im vorangehenden Abschnitt genannten Voraussetzungen sind inzwischen geschaffen und ermöglichen nunmehr den Start eines Projektes zur Umsetzung der in eCampus I erarbeiteten Verfahrensansätze. Die Entscheidung für den Einsatz von eDirectory (Novell) und der zugehörigen Komponenten für das Identity Management ist inzwischen getroffen. Sie ist hauptsächlich dadurch begründet, dass es sich um einen der technischen Marktführer unter den standardbasierten IDM-Lösungsanbietern handelt, und dass an den Hamburger Hochschulen auf existierende Erfahrungen beim Einsatz von eDirectory-Verzeichnisdiensten zurückgegriffen werden konnte. Außerdem haben die Hamburger Hochschulen und die Staats- und Universitätsbibliothek eine Rahmenvereinbarung bezüglich der arbeitsteiligen Kooperation in zentralen Bereichen der IT-Versorgung abgeschlossen, die als einen Kooperationsschwerpunkt das gemeinsame Verfahren für das Identity Management vorsieht und damit Voraussetzungen für eine institutionalisierte und dauerhafte Kooperation schafft.
Zudem ist durch außerplanmäßig bereitgestellte Mittel der BFW und durch Eigenfinanzierung aus den Mitteln der beteiligten Hochschulen ein finanzieller Handlungsrahmen geschaffen worden, der eine Umsetzung der Konzeption zumindest in einem ersten Entwurf erlaubt.

Am Umsetzungsprojekt eCampus II werden neben den an eCampus I beteiligten Hochschulen zusätzlich die Hafen City Universität Hamburg und die Staats- und Universitätsbibliothek Hamburg beteiligt sein.
Im Einzelnen ermöglichen diese Voraussetzungen die in den nachfolgenden Abschnitten dargestellten Schwerpunktsetzungen im Projekt eCampus II.

4.1 Verfahrensaufbau gemeinsames IDM

Es ist geplant, im Jahr 2008 den Prototyp eines gemeinsamen IDM-Pools der Hamburger Hochschulen verfügbar zu machen, der die in der nachstehenden Abb. 18 skizzierte Grundfunktionalität bereitstellt.
Das gemeinsam betriebene System für das Identity-Management empfängt dabei die Personenidentitäten aus den Quellsystemen, konsolidiert diese im Fall von Mehrfachvorkommen, fügt die für die hochschulübergreifend eindeutige Zugangsberechtigung notwendigen Attribute hinzu – auch ggf. Rollenattribute nach Maßgabe eines zentral erstellten und administrierten Regelwerks – und provisioniert die generierten Identitäten in die Zielsysteme.
Quellsysteme können dabei beliebige Verzeichnisdienste (wie etwa im Virtuellen Campus der Universität), aber auch Verwaltungssysteme vom Typ STiNE/CampusNet, HISSOS oder Paisy oder auch die (über einen Identity-Proxy) angebundene Benutzerverwaltung des Pica-Bibliothekssystems sein. Die in der Abbildung aufgeführten Quellsysteme stellen nur eine Auswahl möglicher Umgebungen dar.
Zielsysteme wiederum können prinzipiell alle Systeme sein, die an den einzelnen Hochschulen loziert sind, die dezentrale hochschulspezifische Versorgung mit Diensten übernehmen, ihre Benutzerdaten jedoch aus dem IDM erhalten und bei Bedarf z.B. applikationsabhängig ergänzen. Der Datenaustausch zwischen den Quellsystemen und dem IDM bzw. zwischen dem IDM und den Zielsystemen erfolgt über sogenannte (Software-) Konnektoren.
Allerdings ist angestrebt, die Zahl der Zielsysteme dergestalt zu beschränken, dass idealerweise nur ein System pro Hochschule direkt aus dem gemeinsamen Identity-Pool provisioniert wird. Dies wird typischerweise das Corporate Directory der jeweiligen Hochschule sein, das dann seinerseits eine Unterverteilerrolle übernimmt, so dass sich eine auch unter betrieblichen Aspekten vorteilhafte kaskadierte Provisionierungskette ergibt.

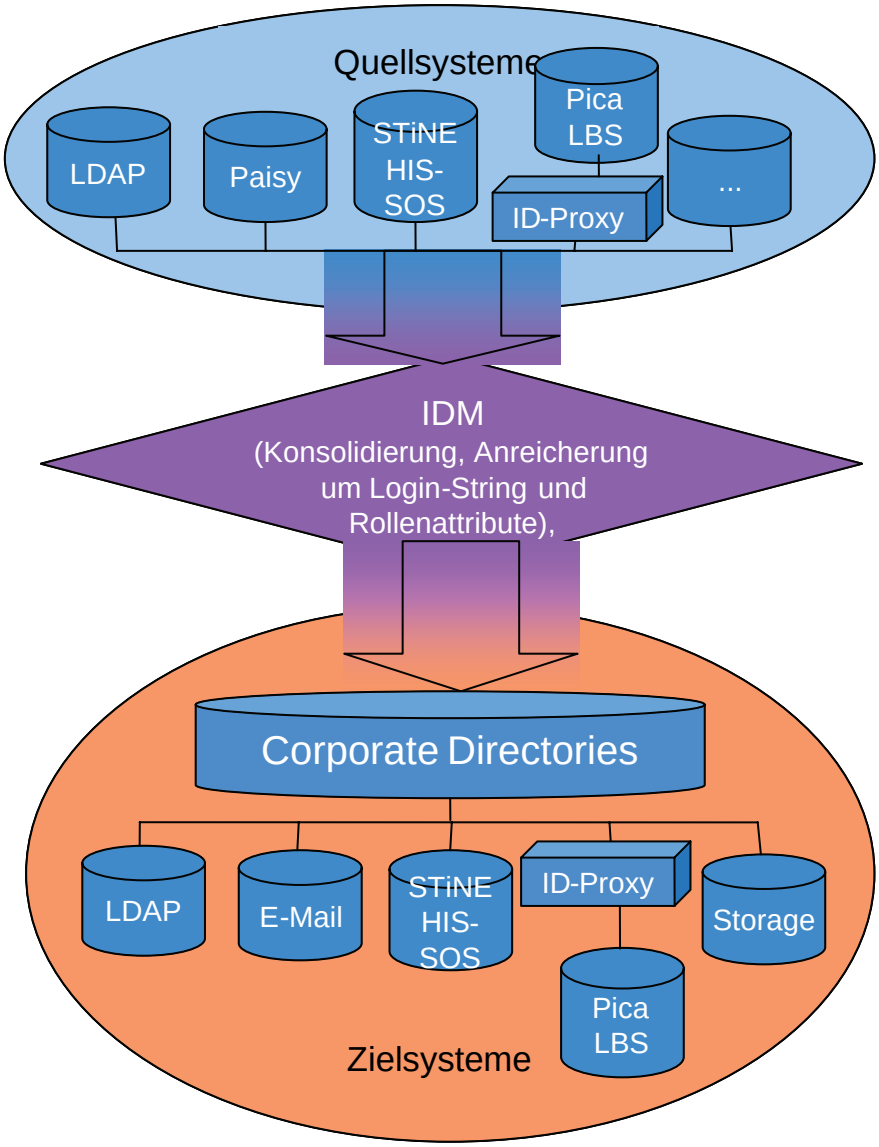


Abb. 18 Grundfunktionalität IDMS HH

4.2 Spezifische Vorteile des eCampus-Ansatzes

Über die weiter oben schon dargestellten Mehrwerte hinaus weist unser Verfahrensansatz drei spezifische Vorteile auf, die ihn möglicherweise auch über den Hochschulstandort Hamburg hinaus interessant machen und ihm ein gewisses Übertragbarkeitspotential verleihen. Diese drei Spezifika seien daher an dieser Stelle abschließend dargestellt.

Es handelt sich um einen im echten Sinne hochschulübergreifenden Verfahrensansatz. In diesem Sinne gehen wir weiter als verwandte Kooperationen wie etwa in Thüringen oder Nordrhein-Westfalen, indem nicht nur gemeinsame Daten- und Produktstandards vereinbart wurden, sondern auch das IDMS als einen gemeinsam betriebenen Verfahrenskern aufgesetzt

werden soll. Allerdings ist dieses Vorgehen möglicherweise nur unter den Randbedingungen eines Stadtstaats praktikabel und erweist sich in einem Flächenland so zumindest in naher Zukunft als nicht durchführbar.

Mit der Einbeziehung des neuen IDM-Konnektor-Produktes von OCLC Pica / Sisis [OCLC06] kann eine Einbindung des schwer integrierbaren Bibliotheksbereichs geleistet werden, die bisher aufgrund der mangelnden Offenheit vieler Systeme für die Bibliotheksautomation mit ihren in der Regel gekapselten Systemen für die Benutzerverwaltung nicht realisierbar schien. Das Pica-Lokalsystem LBS wird in Hamburg für mehrere Hochschulen gemeinsam vom RRZ zusammen mit der Staats- und Universitätsbibliothek betrieben, so dass durch die Verbindung des gemeinsamen Identity-Pools mit dem LBS weitere Synergien geschaffen werden können: es wird solcherart nicht erforderlich, mehrere Separatverbindungen zwischen Teilinstanzen des Bibliothekssystems und den jeweiligen lokalen Corporate Directories zu implementieren und zu pflegen.

Es ist beabsichtigt, den Einsatz des IDM-Connectors im Zuge eines Pilotvorhabens vorzunehmen, so dass am Standort Hamburg Erfahrungen und Know-how aufgebaut werden können, die zumindest im Bereich der Pica-Anwender auch deutschlandweit von Interesse sein dürften.

Schließlich erlaubt unser Lösungsansatz eine Einbindung der Hamburger Hochschul- und Bibliothekslandschaft in das Shibboleth-basierte AAI-Verfahren, das derzeit vom DFN aufgebaut wird. Die Hamburger Hochschulen können in einem solchen System im Sinne der oben unter 3.3 dargestellten Alternativen als ein gemeinsamer Identity-Provider auftreten, was die aufwändige Mehrfachimplementierung von ‚Local Services' obsolet macht.

Das besondere Potential und zugleich die zentrale Herausforderung des Projektes eCampus II liegen in dessen hochschulübergreifendem Ansatz. Alle Beteiligte sind sich der Bedeutung einer regelmäßigen Abstimmung und des Austauschs miteinander bewusst, der sie durch entsprechend angepasste Strukturen und Abläufe gerecht werden.

Literatur und WWW-Ressourcen

[Ecam03] Homepage des Projektes eCampus unter http://www.ecampus-hamburg.de/

[Educ07] Homepage von EDUCAUSE/Internet 2 unter http://www.educause.edu/content.asp?SECTION_ID=30&bhcp=1

[Haus05] Stephanie Haussner, Ulrich Schmid, Martin Vogel: Vom e-Learning zum eCampus. Hamburgs Hochschulen auf dem Weg zu einer integrierten e-Learning- und IT-Dienste-Infrastruktur. In: Zeitschrift für Hochschuldidaktitk (ZFHD), April 2005, S. 33-46, online unter http://www.zfhd.at/resources/downloads/ZFHD_03_03_Haussner__eCampus_HH_1000343.pdf

[Inte06] IntegraTUM. Bericht 2004-2006, Antrag 2006-2009. online unter http://portal.mytum.de/iuk/integratum/dokumente/index_html/vortrag_DFG.pdf

[Kaeh06] Ulrich Kähler: Sicherer Umgang mit geschützten Ressourcen. DFN-AAI nimmt Gestalt an. In: DFN-Mitteilungen 71, Dezember 2006, S. 11-14. Online unter http://www.dfn.de/content/fileadmin/5Presse/DFNMitteilungen/DFN_71.pdf

[Ober06] Bernd Oberknapp: AAI for German higher education - The library's perspective online unter http://www.switch.ch/proxy/aai/support/presentations/infoday-2006/AAI-ID06-50-AAR.pdf

[OCLC06] Informationsflyer von OCLC zum neuen Produkt Identity Management Connector unter http://www.oclcpica.org/dasat/images/2/100782-idm-flyer.pdf

[Offi07] Homepage des Identity Management Projektes von OFFIS unter http://www.offis.de/projekte/projekt.php?id=108

[Reso05] Ressourcenverbund NRW. Homepage unter http://www.rv-nrw.de/

[Schu05] Steffen Schulze-Kremer: Service-orientierte IT-Infrastruktur an niedersächsischen Hochschulen. Abschlußbericht. Online unter http://soi.lanit-hrz.de/export/sites/default/de/download/soi-abschlussbericht.pdf

[Swit06] Homepage von Shibboleth unter http://www.switch.ch/aai/

[Shib07] Homepage von SWITCH AAI unter http://shibboleth.internet2.edu/

[Tere07] Homepage von TERENA unter http://www.terena.org/

[Wind05] Phillip J. Windley: Digital Identity. O'Reilly 2005

Teil III

Integration von E-Learning

Erweiterung eines LMS um hochschultypische Softwaresysteme

Markus Schmees, Hans-Jürgen Appelrath, Dietrich Boles, Norbert Kleinefeld

Department für Informatik
Universität Oldenburg
26121 Oldenburg
{markus.schmees, hans-juergen.appelrath, dietrich.boles, norbert.kleinefeld}
@informatik.uni-oldenburg.de

Abstract

Hochschulen setzen zunehmend eine Reihe dedizierter Softwaresysteme ein, um Prozesse u.a. in Lehre, Studium und Verwaltung zu unterstützen. Diese Systeme haben spezifische Aufgabenbereiche, arbeiten meist unabhängig voneinander und sehen eine Integration in weitere Hochschulsysteme i.d.R. nicht vor. Eine wichtige Voraussetzung, um z.B. komplexere Verwaltungsprozesse zu automatisieren, ist der systemübergreifende Austausch von Daten und Nachrichten. Zu dem Zweck ist Interoperabilität zwischen den unterschiedlichen Systemen herzustellen (im Sinne einer serviceorientierten Softwarearchitektur oder über wohldefinierte Schnittstellen wie Web Services), die sie im Regelfall nicht besitzen. Zur Lösung dieses Problems stellt der vorliegende Artikel einen Ansatz vor, der verschiedene Funktionen und Daten unterschiedlicher Hochschulsysteme in ein zentrales Lernmanagementsystem (LMS) integriert. Am Beispiel der Universität Oldenburg wird eine heterogene Anwendungslandschaft präsentiert und darauf aufbauend die Erweiterung des universitären LMS um weitere Hochschulsysteme beschrieben. Das derart erweiterte LMS befindet sich - nach meist unvermeidlichen Startschwierigkeiten - im produktiven Einsatz und dient als Grundlage zur Integration weiterer Hochschulsysteme und Informationsdienste. Der gewählte Ansatz scheint aber dank seines „generischen Konzeptes“ auf andere Integrationsprojekte übertragbar.

1 Einleitung

Informations- und Kommunikationstechnologien (IKT) helfen dabei, sich wiederholende Abläufe zu standardisieren, zu automatisieren und zu rationalisieren. Dadurch können ihre

Anwender angestrebte Ergebnisse einfacher, schneller und bequemer erreichen, was i.d.R. zu Akzeptanz und unumkehrbarer Nutzung führt. Eine aktuelle Untersuchung zur IT-Nutzung für den deutschen Hochschulbereich bietet [KlSc06]. Im Rahmen von Technology Enhanced Learning (TEL) unterstützen IKT Prozesse in Studium, Lehre und Verwaltung. Hochschulen setzen zu diesem Zweck verschiedene Softwaresysteme ein, die meist in unterschiedlichen Programmiersprachen entwickelt wurden, auf verschiedenen Plattformen eingesetzt sind und im Regelfall unabhängig voneinander arbeiten. Häufig findet man sog. Lernmanagementsysteme (LMS), die an zentraler Stelle unter einheitlicher Oberfläche u.a. digitale Lern- und Arbeitsmaterialien bereitstellen und die Kommunikation zwischen Studierenden und Lehrenden fördern. Bestehende Studien- und Prüfungsordnungen bleiben auch unter Einsatz solcher Systeme gültig, darin enthaltene und durchaus individuelle Regelungen einer Hochschule sind dabei einzuhalten. Darüber hinaus verstärkt die Einführung von Studienbeiträgen in einigen Bundesländern die Forderung nach effizienteren und schlankeren Verwaltungsprozessen.

Dieser Artikel erläutert ein Konzept, das verschiedene Hochschulsysteme und Informationsdienste in ein zentrales LMS integriert und so ein umfassenderes Campus Management gestattet. Am Beispiel der Universität Oldenburg wird eine heterogene Hochschulsystemlandschaft vorgestellt und auf Grundlage des zentralen LMS die Anwendung dieses Konzepts beispielhaft beschrieben. Der folgende Abschnitt 2 geht zunächst auf Besonderheiten von LMS ein, die im Folgenden die Basis zur Integration weiterer Hochschulsysteme darstellen. Abschnitt 3 stellt verschiedene Typen von Softwaresystemen vor, die häufig an einer Hochschule zu finden sind. Daraufhin erläutert Abschnitt 4 unterschiedliche Ansätze, um Systeme in ein zentrales LMS zu integrieren. Die Anwendung dieser Möglichkeiten am Beispiel des weit verbreiteten LMS Stud.IP stellt Abschnitt 5 dar. Abschnitt 6 geht auf verwandte Arbeiten ein, bevor Abschnitt 7 diesen Artikel mit einer Zusammenfassung abschließt.

2 Lernmanagementsysteme

LMS sind auch als Lernportale oder -plattformen bekannt. Sie bieten eine einheitliche Oberfläche, unter der sie zur Unterstützung von Kommunikation, Koordination und Kooperation eine Vielzahl aufgabenspezifischer Komponenten vereinen. Aus technischer Sicht sind LMS serverseitig installierte Softwaresysteme, die aus einer Menge aufrufbarer und ausführbarer Funktionen bestehen. Sie erlauben z.B. die Verwaltung und Organisation von Veranstaltungen,

deren Teilnehmern und die Bereitstellung von Lernmaterialien. Der Zugriff darauf erfolgt i.d.R. über einen Webbrowser, so dass Anwender keine Zusatzsoftware auf ihren Rechnern installieren müssen und die bereitgestellten Funktionen „von überall aus“ aufrufen können. LMS bieten u.a. Kursumgebungen zur Vermittlung von Wissen. Diese erlauben Kursplanung, Interaktionen zwischen Beteiligten sowie Selbststudium und räumen ihren Anwendern die Möglichkeit ein, sich persönlich zu präsentieren. LMS sind im Regelfall in unterschiedlichen Programmiersprachen entwickelt und auf verschiedenen Plattformen installiert. Ein gemeinsames Verständnis, welche Funktionsbereiche ein LMS bieten sollte, existiert nach [BHMH02] nicht, gewisse „Trends/Standardisierungen“ sind aber in Referenzmodellbildungen erkennbar. [MüDü02] identifizieren die folgenden wesentlichen Funktionsbereiche eines LMS:

- **Kursverwaltung**: In diesen Bereich fallen Funktionen, die mit der Planung und Organisation von Online-Kursen zusammenhängen, z.B. Einrichten und Beschreiben neuer Kurse, Festlegen von Formalitäten zur Kursanmeldung, Aufbau von Kurskalendern und Nutzungsstatistiken, Einteilung von Gruppen oder Archivierung beendeter Kurse.
- **Content-Verwaltung**: Weitere Aufgabe eines LMS ist die Verwaltung und Bereitstellung von Inhalten, die für Lehre und Studium wichtig sind. Dabei handelt es sich u.a. um digitale Lehr- und Lernmaterialien wie Präsentationen, Skripte oder Vorlesungsaufzeichnungen, aber auch um allgemeine Informationen zu Kursen wie organisatorische Hinweise oder Termine.
- **Nutzerverwaltung**: Dieser Bereich umfasst Funktionen zur Verwaltung einzelner Anwender, z.B. persönliche Daten, stellt Möglichkeiten zur An- und Abmeldung am LMS bereit, bietet Einstellungen im Rahmen einer „Personalisierung“, erlaubt die Erstellung individueller Stundenpläne und unterstützt bei der Umsetzung von Rechte- und Rollenkonzepten.
- **Kommunikation**: Eine wichtige Aufgabe von LMS ist die Unterstützung bei der Kommunikation, sowohl zwischen Lehrenden und Studierenden als auch zwischen Studierenden untereinander. Dazu kann es elektronische Hilfsmittel wie z.B. Foren, Chats, das Versenden interner Nachrichten, die Annotation von Lernmaterialien oder das Einstellen aktueller Ankündigungen bereitstellen.

- **Evaluation**: Dieser Bereich umfasst Funktionen zur Abfrage bzw. zur Überprüfung von Wissen bzw. Lernerfolg. Dazu zählen z.B. Tests, deren Auswertung automatisch stattfinden kann, aber auch die Durchführung von Evaluationen im Anschluss an eine Lehrveranstaltung. Durch Umfragen können Lehrende die „Stimmungen und Vorstellungen“ ihrer Studierenden abfragen und sie direkt an der Planung und Gestaltung von Veranstaltungen beteiligen.
- **Information**: Über das "reine Lernen" hinaus stellen LMS i.d.R. weitere Funktionen zur Verfügung, mit denen ihre Anwender Zusatzinformationen beziehen können. Dazu gehören z.B. eine Übersicht über das gesamte Kursangebot, allgemeine Hochschulinformationen oder Veranstaltungshinweise.

Im Jahr 2005 gab es bereits mehr als 140 LMS auf dem Markt[24]. Einige Systeme bilden besonders gut bestehende Strukturen einer Hochschule nach und unterstützen z.B. deren Verwaltungsprozesse, während andere Systeme ihren Schwerpunkt auf die Erstellung von Lerneinheiten oder eine einfache Navigation darin legen. Um LMS miteinander vergleichen, Vor- und Nachteile herausarbeiten und ein geeignetes System auswählen zu können, wurden Marktstudien erstellt, z.B. von [HeKo03], und verschiedene Evaluationen[25] durchgeführt, u.a. von [BHMH02]. Weit verbreitet sind z.B. die Open Source Systeme Stud.IP[26] und Moodle[27] oder die kommerziellen Systeme CLIX[28] und Blackboard[29]. Neben LMS setzen Hochschulen zur Bewältigung ihrer Aufgaben weitere Softwaresysteme ein. Der folgende Abschnitt beschreibt Besonderheiten und verschiedene Typen der von ihnen unterstützten Applikationen.

3 Heterogene Hochschulsystemlandschaft

Neben einem oder mehreren LMS kann man an einer einzelnen Hochschule eine Vielzahl verschiedener Softwaresysteme finden, die jeweils unterschiedliche Prozesse unterstützen. Nachfolgend sind mit Bezug zur Systemlandschaft der Universität Oldenburg wesentliche Applikationstypen und ihr Einsatzbereich beschrieben sowie zugehörige Beispiele aufgeführt.

[24] Eine aktuelle Marktübersicht bietet z.B. http://www.c3-initiative.info/peter/directory/27
[25] Eine Auswahl von Evaluationen ist zu finden unter http://www.evaluieren.de/infos/links/plattfor.htm
[26] http://www.studip.de/
[27] http://moodle.org/
[28] http://www.im-c.de/138/Lernplattform-CLIX/
[29] http://www.blackboard.com/products/academic_suite/learning_system/index.Bb

- **Nutzerverwaltung**: Eine Hochschule „lebt“ von Studierenden, deren Daten bez. Immatrikulation, Belegung von Modulen, Rückmeldung, Studiengang, Fachsemester usw. i.d.R. vom Immatrikulationsamt verwaltet werden. Dieses kann zur Unterstützung z.B. das Studentenorganisationssystem[30] (SOS) der Hochschul-Informations-System (HIS) GmbH einsetzen sowie Moveon[31] der Firma Unisolution, um z.B. Auslandssemester und Austauschstudierende zu verwalten.
- **Prüfungsangelegenheiten**: Das Prüfungsamt einer Hochschule muss die Einhaltung von Prüfungsordnungen sicherstellen, Prüfungsdaten, insbesondere Prüfungsleistungen verwalten, Prüfungsberechtigte bestimmen, Prüfungstermine vergeben, An- und Abmeldungen zu Prüfungen handhaben und schließlich Auskünfte zu erzielten Leistungen erteilen. Zur Unterstützung dieser Aufgaben findet man z.B. das Prüfungsorganisationssystem[32] (POS) der HIS GmbH.
- **Veranstaltungsverzeichnis**: Hochschulen bieten verschiedene Typen von Veranstaltungen an, z.B. Seminare, Vorlesungen oder Praktika. Zur Verwaltung dieser Veranstaltungen, inzwischen meist Module genannt, ihres Typs, inhaltlicher Beschreibungen, erreichbarer ECTS-Punkte, Räume, Zeiten und zur Festlegung der Modulverantwortlichen setzt die Universität Oldenburg einen von der Universität Bremen entwickelten Lehrveranstaltungsplaner[33] (LVP) ein.
- **Bibliothekskatalog**: Hochschulbibliotheken halten meist ein zentrales elektronisches Verzeichnis der erfassten Literatur zur Literaturrecherche vor. Darüber hinaus setzen sie häufig weitere Systeme ein, die eine Verwaltung der Ausleihe erlauben und z.B. Daten zum Ausleihstatus eines Buchs liefern und Möglichkeiten zur Vormerkung oder zur Verlängerung einer Ausleihe bieten. In Oldenburg findet man dazu z.B. das Oldenburger Regionale Bibliotheks- und Informationssystem[34] (ORBIS).

[30] http://www.his.de/Abt1/HISSOS
[31] http://de.unisolution.de/moveon/
[32] http://www.his.de/Abt1/HISPOS
[33] http://www.uni-oldenburg.de/dezernat3/veranstaltungsverzeichnis/lvp_info/manual/man_toc.html
[34] http://katalog.bis.uni-oldenburg.de/

- **Dienste des Rechenzentrums**: Die Informations-, Bibliotheks- und IT-Dienste (IBIT) stellen verschiedene Applikationen bereit, z.B. ein E-Mail-System zur Kommunikation oder persönlichen Webspace, den Studierende und Mitarbeiter zur Selbstdarstellung nutzen können. Eine zentrale Benutzerdatenverwaltung gestattet die Diensteanmeldung mit jeweils gleichen Zugangsdaten. Ein **Central Authentication Service35** (CAS) ermöglicht darüber hinaus Single Sign On (SSO), d.h. den Wechsel zwischen den Diensten ohne erneute Anmeldung.
- **Lernmanagementsysteme**: Die Universität Oldenburg setzt Stud.IP[36] als zentrales LMS ein. Darüber hinaus sind weitere und ganz unterschiedliche LMS zu finden, die individuelle Anforderungen einzelner Fachbereiche erfüllen. Dazu zählen z.B. Campus Virtuell[37], Physik Multimedial[38] und Ecedon[39].
- **Gebäudemanagement**: Zur Vergabe und Verwaltung von Räumen wie z.B. Hörsälen setzt das Raumbüro ein System zur Raumplanung ein, das ursprünglich von der Universität Bremen entwickelt wurde. Für Baumanagement und zur Instandhaltung findet man Systeme der Firma Speedikon Facility Management[40].
- **Klassische ERP-Dienste**: Darüber hinaus nutzt die Verwaltung der Universität klassische ERP-Systeme wie z.B. SAP R/3. Hier sind zugehörige Module für Finanzen (SAP R/3 FI), Anlagenbuchhaltung (SAP R/3 AM), Budgetverwaltung (SAP R/3 PSM), Controlling (SAP R/3 CO), Einkauf (SAP R/3 MM) sowie Personal Abrechnung und Organisation (SAP R/3 HR) zu finden.
- **Informationsdienste**: Schließlich stellen einzelne Institute, Departments und Abteilungen, aber auch Lehrende, Fachschaften und Studierende auf ihren Webseiten unterschiedliche Informationen zur Verfügung. Die Stabsstelle „Presse & Kommunikation“ ist u.a. für die Veröffentlichung von Veranstaltungsinformationen, die Einhaltung des Corporate Designs (CD) sowie den Webauftritt der Universität zuständig. Das aktuelle Vorlesungsverzeichnis wird jeweils direkt aus dem Datenbestand des LVP generiert.

[35] https://cassrv01.uni-oldenburg.de:9443/cas/
[36] http://elearning.uni-oldenburg.de/
[37] http://www.campus-virtuell.de/
[38] http://www.oldenburg.physik-multimedial.de/
[39] http://lspace5.via-on-line.de/
[40] http://www.speedikonfm.com/

Hochschulen wie die Universität Oldenburg setzen zu unterschiedlichen Zwecken eine Vielzahl verschiedener Softwaresysteme ein. Diese sind i.d.R. in verschiedenen Programmiersprachen erstellt, auf unterschiedlichen Plattformen installiert und arbeiten meist unabhängig voneinander. Um z.B. komplexe Verwaltungsprozesse zu automatisieren, redundante Datenhaltung zu vermeiden, den Austausch und Abgleich von Daten zu ermöglichen oder das Einhalten von Ordnungen sicherzustellen, ist eine Kopplung dieser Systeme sinnvoll, mitunter sogar zwingend. Aufgrund der angesprochenen Verschiedenartigkeit gestaltet sich diese Verbindung jedoch schwierig. Daher stellt der folgende Abschnitt einen Ansatz vor, um Funktionalität und Daten unterschiedlicher Systeme in ein zentrales LMS zu integrieren.

4 Integration von Lern- und Hochschulmanagement

Der Trend geht dahin, verschiedene Hochschulsysteme miteinander zu koppeln. Aber bereits die Wartung, Anpassung und Erweiterung von LMS ist mühsam, da diese i.d.R. zu verschiedenen Zwecken entwickelt, in verschiedenen Programmiersprachen geschrieben und auf unterschiedlichen Plattformen eingesetzt sind. Systeme wie CLIX oder Blackboard sind kommerzielle Applikationen, die laufende Lizenzgebühren verlangen und keine Veränderungen an Quellcode oder Datenbankstrukturen erlauben. Andere wie z.B. Moodle oder Stud.IP sind hingegen frei erhältlich und gestatten ausdrücklich die Anpassung ihrer Programmierung, binden aber natürlich entsprechendes Personal. Eine Diskussion bez. des Einsatzes von Open Source Software im E-Learning liefern z.B. [CoNe04], Erfahrungen beim Einsatz von Open Source LMS haben u.a. [ABK+06] thematisiert. Ein Ansatz, um verschiedene Hochschulsysteme zusammenzubringen und einen gewissen Grad an Interoperabilität herzustellen, ist ihre Integration in ein zentrales und erweiterbares LMS, nicht zuletzt aus der Überlegung heraus, dass sich in einem LMS die Alleinstellungsmerkmale und Profilierungsmöglichkeiten einer Hochschule deutlich eher zeigen als bei Systemen etwa zur Anlagenbuchhaltung, Personalabrechnung oder Gebäudemanagement. Dazu sind verschiedene Optionen vorstellbar, angefangen bei der Verlinkung von Inhalten, über eine Vereinheitlichung von Datenaustauschformaten und Schnittstellen bis hin zur Herstellung der Erweiterbarkeit eines LMS. Eine Erläuterung der einzelnen Ansätze folgt, ihre jeweilige Anwendung wird im nächsten Abschnitt beschrieben.

- **Einfacher Verweis**: Eine einfache Möglichkeit, um externe Inhalte einzubeziehen, ist ihr direkter Abruf bzw. ein einfacher Verweis darauf. Dafür notwendig ist die Internetadresse, unter der diese Informationen abrufbar sind. So stellen z.B. Nachrichtenanbieter RSS-Feeds bereit und Wetterdienste liefern Wetterinformationen zu fast allen Standorten weltweit. Auf diese Weise können Daten wie z.B. Nachrichten, Bilder oder Stylesheets in den Auftritt des LMS oder an passende Stellen eines enthaltenen Kurses integriert werden. Durch einen solchen Verweis ist aber auch z.B. die automatische Weiterleitung eines Webbrowsers in ein externes System möglich. Ist darüber hinaus ein SSO-Dienst beteiligt, muss sich der Anwender im Zielsystem nicht erneut authentifizieren und bekommt im günstigsten Fall „von dieser Umleitung nichts mit".
- **Einheitliches Datenaustauschformat**: Durch eine Vereinheitlichung des Datenaustauschformats können verschiedene Systeme mit dem gleichen Datenbestand arbeiten und diesen oder Teile davon untereinander austauschen. Die Daten werden zu diesem Zweck aus einem System exportiert, in einem maschinenles- und -interpretierbaren Format abgespeichert und können daraufhin von einem weiteren System, das sich konform zu diesem Format verhält, gelesen und verarbeitet werden. Das leistet z.B. das Sharable Content Object Reference Model[41] (SCORM) als Standard für digitale Lernmaterialien.
- **Einheitliche Schnittstellen**: Sollen nicht nur Daten, sondern auch Funktionalität eines externen Systems einbezogen werden, muss diese in einheitlicher Weise zum Ansprechen zu Verfügung stehen. So bieten z.B. Web Services eine Möglichkeit zum entfernten Prozeduraufruf. Um dabei unabhängig von Plattformen und Programmiersprachen zu bleiben, tauschen die Systeme i.d.R. mit Hilfe des Simple Object Access Protocols[42] (SOAP) XML-basierte Nachrichten aus. Eine Beschreibung der angebotenen Funktionen, ihrer Parameter, auszutauschende Nachrichten sowie zu erwartende Antworten beschreibt im Regelfall die Web Services Description Language[43] (WSDL).

[41] http://www.adlnet.gov/scorm/index.cfm
[42] http://www.w3.org/TR/soap
[43] http://www.w3.org/TR/wsdl

- **Plugin-Integration**: Verschiedene Softwaresysteme sind i.d.R. unterschiedlich aufgebaut. Um ein einzelnes LMS um unterschiedliche Komponenten zu erweitern oder eine bereits erstellte Komponente einfach in verschiedene LMS integrieren zu können, bietet sich ihre Erweiterung um eine einheitliche Erweiterungsschnittstelle an. Die jeweiligen Komponenten können dann an diese Schnittstelle angepasst werden und lassen sich im Sinne von Plugins direkt integrieren. Das vereinfacht zudem einen Austausch von Komponenten zwischen verschiedenen LMS und vermeidet ihre Anpassung bei LMS-Updates.

Regeln einer serviceorientierten Architektur (SOA), wie sie z.B. [HeHV06] beschreiben, vereinfachen die Integration verschiedener Komponenten und Systeme in ein Gesamtsystem. Da Komponenten damit plattform- und programmiersprachenunabhängig angekoppelt sind, können sie bei Bedarf leicht einbezogen oder ausgetauscht werden. Voraussetzung ist, dass sich sowohl Serviceanbieter als auch -nutzer auf bestimmte Schnittstellen einigen und diese konsequent implementieren. Die meisten Hochschulsysteme stellen ihre Dienste jedoch nicht nach außen, insbesondere nicht z.B. als Web Services zur Verfügung. Um sie dennoch in eine solche SOA einbeziehen zu können, ist ihre Erweiterung ist unumgänglich. Zwar kann das innerhalb einer Hochschule z.B. vom Präsidium politisch gewollt und damit getrieben sein. Dennoch ist die Erweiterung einzelner Hochschulsysteme nicht in jedem Fall möglich oder z.B. aus lizenzrechtlichen Gründen nicht erlaubt. Hinzu kommen externe Systeme, die z.B. durch Kooperationsverträge oder den Austausch von Lehrveranstaltungen einzubeziehen sind. Man kann also nicht generell davon ausgehen, dass diese Systeme anpassbar/erweiterbar sind oder gar die verlangten Schnittstellen einhalten. Aus dem Grund verfolgt diese Arbeit einen pragmatischen Ansatz, der verschiedene Integrationsoptionen berücksichtigt. Der folgende Abschnitt stellt am konkreten Beispiel der Universität Oldenburg ihre Anwendung bei der Integration unterschiedlicher Hochschulsysteme in das zentrale LMS Stud.IP vor.

5 Anwendung am Beispiel des LMS Stud.IP

Ein zentrales Kompetenzzentrum sollte an einer Hochschule für Betrieb, Administration und Erweiterung der LMS sorgt und ihre Anwender bei der Arbeit beraten und unterstützen. In

Oldenburg übernahm das Labor für Content Engineering[44] (CELab) bis 2006 und ihm folgend das IBIT diese Aufgabe. Es betreibt das zentrale Stud.IP-System und versucht, verschiedene E-Learning-Geschäftsprozesse wie z.B. das Einrichten neuer Module und eine Zuordnung der jeweiligen Modulverantwortlichen zu automatisieren. Auf Grundlage der im vorigen Abschnitt beschriebenen Ansätze wurden zu dem Zweck verschiedene Hochschulsysteme integriert. Weitere LMS und ihre Inhalte wurden durch einfache Verweise angesprochen, Nutzerverwaltungen und das Prüfungssystem über einheitliche Schnittstellen eingebunden, Lehrveranstaltungsdaten durch ein Synchronisationstool übernommen und Plugins für den Import von Nachrichten und Export von Evaluationsergebnissen integriert. Die nachfolgende Abb. 1 skizziert das derart erweiterte LMS und die angebundenen Systeme. Eine Erläuterung des jeweiligen Vorgehens und der im Einzelnen erzielten Ergebnisse folgt im Anschluss daran.

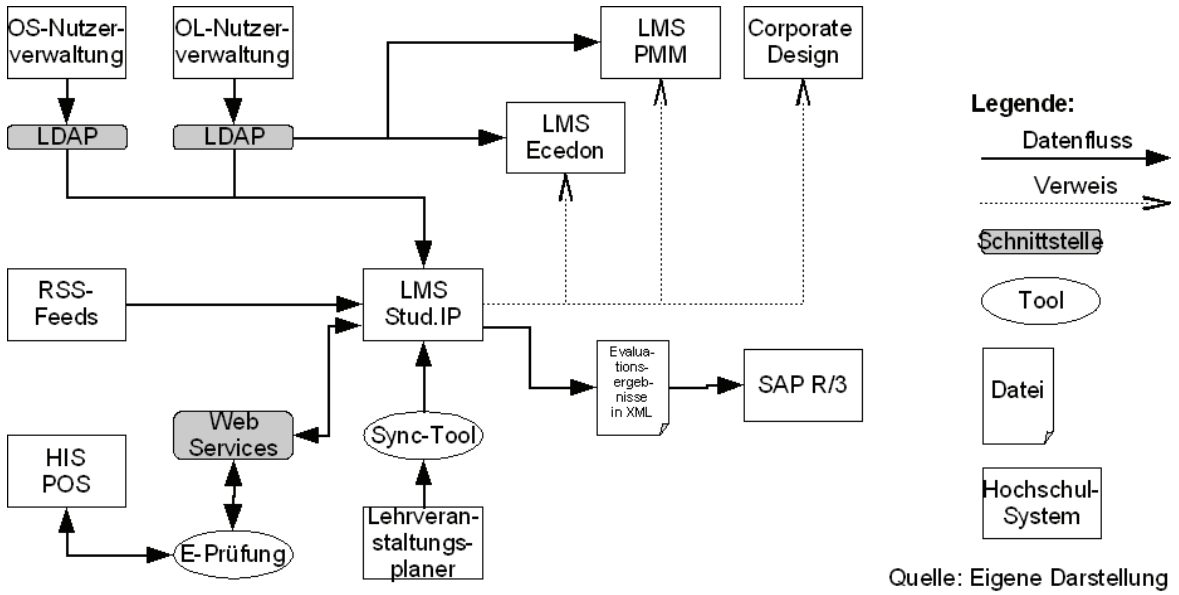


Abb. 19: Integration verschiedener Daten und Hochschulsysteme in ein zentrales LMS

- **Authentifizierung**: Damit sich Studierende und Mitarbeiter mit ihren bekannten Zugangsdaten, die i.d.R. aus Matrikel- bzw. Mitarbeiternummer und Passwort bestehen, beim LMS anmelden können, wurde die zentrale Benutzerverwaltung des Oldenburger IBIT unter Verwendung des Lightweight Directory Access Protocol (LDAP) angebunden. Sobald ein Anwender korrekte Zugangsdaten eingibt und die Benutzerverwaltung diese bestätigt, gilt er für das LMS als authentifiziert. Name, E-Mail-Adresse und anfänglicher Status (Dozent/Student)

[44] http://www.celab.de/

werden nach erfolgreicher Authentifizierung in das LMS übernommen. Weil im Rahmen eines Lehrveranstaltungsaustausches mit der Universität Osnabrück einige Veranstaltungen hochschulübergreifend stattfinden und die Studierenden Zugriff auf zentral bereitgestellte Lehrmaterialien erhalten sollten, wurde in gleicher Weise die Benutzerverwaltung der Universität Osnabrück angebunden.

- **Single Sign On**: Um ohne erneute Authentifizierung in weitere Oldenburger Hochschulsysteme wechseln zu können, wurde der CAS-Server des IBIT integriert. Greift ein nicht authentifizierter Anwender auf das LMS zu, prüft es zunächst, ob dieser bereits gegenüber des CAS-Servers authentifiziert ist. In dem Fall kann es die jeweils notwendigen Benutzerdaten übernehmen. Ansonsten muss sich der Anwender entweder beim CAS-Server oder beim LMS direkt anmelden, um diesen Zugriff zu erhalten. Sind weitere Systeme an den CAS angebunden, wie z.B. Physik Multimedial (PMM), kann ein Anwender zwischen diesen Systemen ohne erneute Anmeldung hin- und herwechseln.
- **Veranstaltungsdaten**: Das zentrale LMS einer Universität soll sämtliche Veranstaltungen unterstützen. Um dies zu erreichen und den Lehrenden die Verwaltung ihrer Kurse so praktisch wie möglich zu gestalten, wurde der zentrale Lehrveranstaltungsplaner in das LMS integriert. Ein Werkzeug, in der vorangehenden Abb. 1 als „Sync-Tool“ bezeichnet, gleicht automatisch einmal täglich die Daten des LVP mit den Kursdaten des LMS ab, richtet dabei neue Kurse ein, übernimmt deren Titel, Termine sowie Beschreibungen und ordnet ihnen die angegebenen Lehrenden als Dozenten zu. Lehrende finden diese Kurse daraufhin in der Übersicht über die eigenen Veranstaltungen und können sie administrieren. Studierende können einen Kurs im Kursverzeichnis des LMS suchen, sich daran anmelden und ihn auch ohne Beteiligung des Lehrenden nutzen, um z.B. im Forum zu diskutieren, Veranstaltungstermine in den persönlichen Kalender einzutragen oder einen Stundenplan erstellen zu lassen.
- **E-Prüfung**: Um die Prüfungsformalitäten zu vereinfachen, wurde das POS des Prüfungsamtes in das LMS integriert. Die dazu notwendige Funktionalität wurde vom Prüfungsamt implementiert, in Form von Web Services auf einem zentralen Application Server bereitgestellt und in die Funktionalität des LMS eingebettet.

Studierende können sich durch Eingabe von Transaktionsnummern, die sie bei der Immatrikulation erhalten, online bei Modulprüfungen an- und wieder abmelden. Sie erhalten eine Übersicht über bisher abgelegte Prüfungen und können ihre jeweiligen Leistungen einsehen. Modulverantwortliche können die jeweiligen Prüfungsteilnehmer abfragen, darüber den zu erwartenden Aufwand abschätzen und im Anschluss eine Bewertung/Benotung online vornehmen.

- **Externer Content**: LMS wie z.B. Physik Multimedial oder Ecedon stellen spezialisierte Inhalte zur Verfügung, die einige Lehrende in ihren Veranstaltung einsetzen möchten. Weil die Studierenden hauptsächlich Stud.IP nutzen und dies nun auch „Hochschulstandard“ ist, wurden die externen Systeme und ihre Inhalte durch einfache Querverweise in die gewünschten Kurse integriert. Dieses Verfahren bietet sich vor allem bei den Systemen an, die ebenfalls an das zentrale SSO angebunden sind, so dass ein Wechsel zwischen den Systemen ohne erneute Anmeldung stattfinden kann.
- **SAP-Integration**: Am Ende eines Semesters findet i.d.R. eine Evaluation von Lehrveranstaltungen statt. Die Universität Oldenburg führt diese Evaluation elektronisch mit Hilfe des Stud.IP-Systems durch. Um diese Ergebnisse im Anschluss einfacher auswerten und archivieren zu können, werden sie in das universitäre SAP-System überführt. Die Erstellung von Fragen und Erhebung von Daten erfolgen über das LMS, das sie in einem eigens dafür entwickelten XML-Format abspeichern kann. Das SAP-System kann dieses Format lesen, interpretieren und damit die Evaluationsergebnisse übernehmen. Sobald sie vom Lehrenden freigegeben sind, zeigt das LMS ebenfalls diese Ergebnisse an.
- **Designanpassung**: Die Presse- und Kommunikationsstelle der Universität schreibt ein offizielles Corporate Design vor, das sämtliche Fakultäten, Institute und Abteilungen/Lehrstühle bei ihren Webauftritten verwenden müssen. Dieses ist daher auch in das zentrale LMS zu integrieren. Zu diesem Zweck werden Formatvorlagen und Stylesheets an zentraler Stelle bereitgestellt. Weil die Stud.IP-Entwickler Darstellung und Funktionalität ursprünglich nicht strikt getrennt hatten, mussten Umstellungen auf das neue Design manuell durch eine Verlinkung bzw. direkte Anpassung vorgenommen werden. Zusätzliche „externe Informationen“ wie z.B. die aktuelle Temperatur, Luftdruck und Aussichten

werden bei ihrem Anbieter abgefragt und eingeblendet. Für eine Übersicht über aktuelle Schlagzeilen wurde zunächst der RSS-Feed der Tagesschau eingebunden. Dieser wurde ab Stud.IP-Version 1.4 von einem personalisierbaren RSS-Reader abgelöst, der abonnierte Nachrichten auf der Startseite darstellt.

- **Plugin-Schnittstelle**: Die Kursumgebung des Stud.IP-Systems sieht vor, dass ein Dozent einzelne Komponenten wie z.B. Forum, Wiki oder Dateibereich passend zur jeweiligen Veranstaltung aktivieren bzw. deaktivieren kann. Um funktionale Erweiterungen neu einfügen und derart benutzen zu können, sind Änderungen an zahlreichen Stellen und Dateien des Programmcodes notwendig. Daher wurde das System um eine allgemeine Plugin-Schnittstelle erweitert, die diese manuellen Änderungen vermeidet. Neue Komponenten können auf diese Weise leicht auf System-, Administrations- und Kursebene integriert werden und sind zudem zwischen verschiedenen Stud.IP-Installationen und damit Standorten austauschbar. Bestehende Erweiterungen, z.B. ein Tool zur Anmeldung und Belegung von Tutorien, können in das vorgegebene Plugin-Format überführt und dann einfach in ein Stud.IP-System integriert werden. Ergebnisse der jeweils durchzuführenden Lehrveranstaltungsevaluationen können so in einem einheitlichen Format exportiert und zur Archivierung sowie zur Bereitstellung für SAP-Nutzer, z.B. für Dezernenten, in ein R/3-System importiert werden.
- **Statistikfunktionen**: Um die Aktivität innerhalb von Veranstaltungen ermitteln zu können, z.B. wie stark die Anwender in Foren diskutieren, Ankündigungen benutzen oder Dateien herunterladen, wurden komplexe Statistikfunktionen in das LMS integriert. Auf dieser Grundlage kann dann z.B. das Präsidium einen Preis für besonders aktive E-Learning-Veranstaltungen vergeben oder die Ergebnisse bei der Verteilung von Studienbeiträgen berücksichtigen.

Eine Kopplung von Hochschulsystemen gestaltet sich schwierig, da sie eine Anbindung weiterer Systeme i.d.R. nicht vorsehen und viele Hochschulen darüber hinaus jeweils unterschiedliche Applikationen einsetzen. Verwenden sie hingegen gleiche Systeme, liegen diese zumeist in unterschiedlichen Versionen vor, was diese Kopplung ebenfalls erschwert. Aus verschiedenen Gründen bot sich das Stud.IP-System als Grundlage für diese Integration an. Zum einen ist es das zentrale LMS der Universität und bildet hochschultypische Strukturen

nach. Zum anderen handelt es sich um Open Source Software, die es den Mitarbeitern des CELab ermöglichte, neue Anforderungen ihrer Hochschule an das System relativ zeitnah umzusetzen. Der folgende Abschnitt grenzt diese Arbeit von verwandten Ansätzen ab.

6 Verwandte Arbeiten und Ansätze

Der vorgestellte Ansatz beschreibt die Integration von Daten und Funktionen unterschiedlicher Hochschulsysteme in ein zentrales und anpassbares LMS, nämlich das Open Source System Stud.IP. Das Spektrum verwandter Integrationsansätze reicht von kleinen Hochschulen, z.B. regional ausgerichteten Fachhochschulen, die kein LMS einsetzen und bestehende Systeme unabhängig voneinander betreiben, bis hin zu Projekten wie dem E-Learning Academic Network[45] (ELAN) in Niedersachsen, die als geförderter Verbund eine Vernetzung ihrer Systeme sowohl innerhalb der beteiligten Hochschulen als auch hochschulübergreifend vorantreiben. Das Potential des Einsatzes von Open Source Software im E-Learning, insbesondere ihre Erweiterbarkeit, thematisieren [CoNe04]. Auf die Erweiterung und Anpassung des Open Source LMS Stud.IP im Speziellen gehen [ABK+06] ein. Eine Integration kostenpflichtiger digitaler Lernmaterialien in Lernportale beschreiben [ReAp04]. Sie koppeln die Auslieferung ausgewählter Dateien mit elektronischen Bezahlsystemen. Sobald ein Anwender darüber eine bestimmte Gebühr bezahlt hat, darf er die zugehörige Datei herunterladen. Ein allgemeines Verfahren zur Integration des elektronischen Handels in Softwaresysteme wie LMS ist u.a. in [Schm06] erläutert. In diesem Fall stellen die Konzepte und Technologien des E-Commerce über den reinen Handel hinaus zudem die Einhaltung organisatorischer Vorgaben sicher. Die Ableitung derartiger Vorgaben aus Prüfungsordnungen wird z.B. von [Hack06] mit Hilfe von Ontologien thematisiert. Voraussetzung, um solche Regeln umzusetzen, ist eine Zusammenarbeit der verschiedenen Hochschulsysteme. Dazu hat diese Arbeit einen pragmatischen Ansatz beschrieben, den die Universität Oldenburg beschreitet, der aber grundsätzlich auf andere Hochschulen übertragbar scheint. Der folgende Abschnitt fasst noch einmal wesentliche Ergebnisse/Erkenntnisse zu einem Fazit zusammen.

[45] http://www.elan-niedersachsen.de/

7 Fazit und Ausblick

Im Rahmen des Bologna-Prozesses stellen Hochschulen ihre Veranstaltungen nach und nach auf bez. ECTS-Punkten einheitlich bewertete Module um, die studienbegleitend geprüft werden. Da im Vergleich zu den „klassischen“ Veranstaltungen dabei u.a. deutlich mehr Modulprüfungen anfallen, entsteht ein höherer Verwaltungsaufwand. Gerade bei großen Veranstaltungen (z.B. mit mehr als 400 Studierenden) sind Formalitäten wie das handschriftliche Ausfüllen von Bewertungsbögen kaum noch „nebenher“ von Lehrenden zu bewältigen. Zudem können bei der manuellen Übernahme dieser Daten im Prüfungsamt leicht Fehler entstehen, von denen der Lehrende im Folgenden nichts mitbekommt. Daher ist eine Unterstützung solcher Prozesse durch IKT wie z.B. LMS sinnvoll. Die Integration weiterer Hochschulsysteme kann den Funktionsumfang eines solchen LMS erweitern, die systemübergreifende Automatisierung von Geschäftsprozessen erleichtern und damit den individuellen Anforderungen einer Hochschule entsprechen. Dabei ist zu beachten, dass die Funktionalität des Gesamtsystems immer auch von der Funktionsbereitschaft der integrierten Teilsysteme abhängt. Je mehr Systeme integriert werden, umso größer ist die Gefahr, dass eines davon ausfällt. Als Betreiber des Stud.IP-Systems hat CELab die Erfahrung gemacht, dass Anwender i.d.R. die inneren Strukturen eines solchen Systems nicht kennen und damit auch nicht wissen, welche weiteren Systeme angebunden sind. Für die Anwender stellen sich die integrierten Teilsysteme als Funktionalität des LMS dar. So kommt es z.B. beim Ausfall der Prüfungsfunktionalität häufiger zu Beschwerden, dass das LMS nicht korrekt funktioniert, wobei man dann nur an das zuständige Prüfungsamt verweisen kann. Fallen hingegen zentrale Dienste wie die Benutzerauthentifizierung aus, ist darüber hinaus nicht nur kein Zugriff auf das LMS, sondern auch auf weitere daran angebundene Dienste mehr möglich. In diesem Zusammenhang sind z.B. Service- oder Wartungszeiten unterschiedlicher Abteilungen aufeinander abzustimmen, Notfallpläne zu erstellen oder ein notwendiger Informationsfluss abteilungsübergreifend zu koordinieren.

Literaturverzeichnis

[ABK+06] Hans-Jürgen Appelrath, Dietrich Boles, Norbert Kleinefeld, et al. Einsatz des Open-Source-Lernmanagementsystems Stud.IP zur Unterstützung der

Präsenzlehre der Universität Oldenburg. In Christian Hochberger und Rüdiger Liskowsky (Hrsg.): *Informatik 2006: Informatik für Menschen*, ISBN: 978-3-88579-188-1, S. 53-58. Köllen Druck+Verlag, Bonn, 2006.

[BHMH02] Peter Baumgartner, Hartmut Häfele, und Kornelia Maier-Häfele. E-Learning Praxishandbuch: Auswahl von Lernplattformen: Marktübersicht – Funktionen - Fachbegriffe. ISBN: 3-70651-771-X, Studienverlag, Innsbruck, 2002.

[CoNe04] Chris Coppola und Ed Neelley. Open Source - opens learning: Why open source makes sense for education. 2004. http://www.rsmart.com/assets/OpenSource-OpensLearningJuly2004.pdf, abgerufen am 29.11.2004.

[Hack06] Richard Hackelbusch. Handling Heterogeneous Academic Curricula. In A Min Tjoa und Roland R. Wagner (Hrsg.): Proceedings of the 17th International Workshop on Databases and Expert Systems Applications (DEXA 2006), ISBN: 0-76952-641-1, S. 344-348. IEEE Computer Society Press, Los Alamitos, 2006.

[HeHV06] Andreas Hess, Bernhard Humm und Markus Voß. Regeln für serviceorientierte Architekturen hoher Qualität. In Arndt Bode et al. (Hrsg.): Informatik Spektrum, Band 29, Heft 6, ISSN: 0170-6012, S. 395-411. Springer Verlag, Berlin, 2006.

[HeKo03] Alexander Hettrich und Natascha Koroleva. Learning Management Systeme (LMS) und Learning Content Management Systeme (LCMS). Fraunhofer Institut für Arbeitswirtschaft und Organisation, ISBN: 3-81676-237-9, 2003. http://www.iltec.de/downloads/IAOLMSLCMSStudie.pdf, abgerufen am 28.09.2006.

[KlSc06] Bernd Kleimann und Ulrich Schmid. eReadiness deutscher Hochschulen: Sind Deutschlands Hochschulen „fit“ für die Informationsgesellschaft? Auswertung der Umfrage „IT-Management und E-Learning an deutschen Hochschulen“. eUniversity – Update Bologna, Campus Innovation, Bonn, 2006.

[MüDü02] Roman Müller und Johannes Dürr. Plattformen und Programme – Grundlegende Verfahren und Tools des E-Learning. In Ute Scheffer und Friedrich W. Hesse

(Hrsg.): E-Learning: Die Revolution des Lernens gewinnbringend einsetzen, ISBN: 3-60894-332-3, S. 164-184. Klett-Cotta Verlag, Stuttgart, 2002.

[ReAp04] Dennis Reil und Hans-Jürgen Appelrath. Kostenpflichtiger Content in Lernportalen. In Gregor Engels und Silke Seehusen (Hrsg.): DeLFI 2004: Die 2. e-Learning Fachtagung Informatik, ISBN: 3-88579-381-4, S. 91-102. Köllen Druck & Verlag, Bonn, 2004. http://www-is.informatik.uni-oldenburg.de/publications/1144.pdf, abgerufen am 09.03.2005.

[Schm06] Markus Schmees. Organizing Technology Enhanced Learning. In Bruce Spencer, Mark S. Fox, Weichang Du, Donglei Du, und Scott Buffett (Hrsg.): Proceedings of the Eigth International Conference on Electronic Commerce (ICEC'06), ISBN: 1-59593-392-1, S. 139-150. ACM Press, New York, 2006.

Effizientes und nachhaltiges eLearning an der RWTH Aachen durch das integrierte Lehr- und Lernportal L²P und das CAMPUS-Informationssystem

Michael Gebhardt[1], Philipp Rohde[2], Ulrik Schroeder[2]

[1] Rechen- und Kommunikationszentrum
[2] Centrum für integrative Lehr- und Lernkonzepte (CiL)
RWTH Aachen
52056 Aachen
gebhardt@rz.rwth-aachen.de
{rohde,schroeder}@cil.rwth-aachen.de

Abstract

Die Auswertung der eLearning-Strategien deutscher Hochschulen [KlWa05] zeigt, dass eLearning-Prozesse und -systeme nahtlos in die bestehende Hochschul-IT eingebunden werden müssen, um den Einsatz von eLearning nachhaltig und erfolgreich einzuführen. Die RWTH Aachen setzt seit 2001 das integrierte CAMPUS-Informationssystem ein, das zahlreiche Prozesse in den Bereichen Veranstaltungsorganisation, Verzeichnisdienste und Organisationsabläufe der Universität als webbasiertes Informationssystem unterstützt. Es umfasst Webanwendungen und Portale wie beispielsweise das online verfügbare Vorlesungs- und Organisationsverzeichnis, den persönlichen Studienplaner, Lehrevaluation oder Beschaffungsportale. Funktionen des eLearning für die Durchführung der eigentlichen Lehrveranstaltungen bietet CAMPUS indes nicht. Um diese Lücke zu schließen, entwickelt das Centrum für integrative Lehr- und Lernkonzepte (CiL) zusammen mit dem Rechen- und Kommunikationszentrum der RWTH in einer Kooperation mit Microsoft Deutschland GmbH das hochschulweite Lehr- und Lernportal L²P, welches nahtlos mit den administrativen Prozessen von CAMPUS integriert wird. L²P ermöglicht den effizienten Masseneinsatz didaktisch innovativer Methoden bei der Begleitung von Lehrveranstaltungen, insbesondere durch die Bereitstellung digitaler Lehrinhalte sowie Kommunikations- und Kollaborationsfunktionalität für Lehrende und Lernende.

1 Der Hintergrund

Das CiL (Centrum für integrative Lehr- und Lernkonzepte) wurde als zentrales Service-, Kompetenz- und Supportzentrum rund um das Thema eLearning eingerichtet mit dem primären Ziel einer Qualitätsverbesserung der Präsenzlehre an der RWTH Aachen durch Ergänzung mit digitalen Lehrangeboten und computerunterstützten Kommunikations- und Kollaborationselementen („Blended-Learning“). Das CiL ist Impulsgeber für die Entwicklung und Umsetzung innovativer Lehr- und Lernmodelle. Eine der wesentlichen Aufgaben des CiL ist die Entwicklung und Einführung einer zentralen eLearning-Plattform und die Bereitstellung effektiver Begleitmaßnahmen. Dabei setzt das CiL auf die Strategie, die Einstiegshürde zur Nutzung der eLearning-Funktionalität so gering wie möglich zu halten und möglichst alle Studierenden und Lehrenden der RWTH von Anfang an zu erreichen. Dies wird unter anderem durch die Einbindung der eLearning-Plattform in die bestehende administrative Hochschul-IT erreicht.

Um die große Zahl administrativer Prozesse mit ihren ca. 30.000 Studierenden und ca. 10.000 Mitarbeitern bewältigen zu können, setzt die RWTH seit 2001 das CAMPUS-Informationssystem ein, siehe [GeBi04] und [BiGS05]. CAMPUS bündelt viele administrative Dienste einer Universität als webbasiertes Informationssystem: Es umfasst mehr als ein dutzend Webanwendungen und Portale in den bisher drei Anwendungsbereichen Veranstaltungsorganisation, Verzeichnisdienste und Organisationsabläufe. CAMPUS deckt als administrative Unterstützung indes keine Funktionen des eLearning oder Blended-Learning für die Durchführung der eigentlichen Lehrveranstaltungen der RWTH ab. Um diese Lücke zu schließen, wird der neue, vierte Anwendungsbereich eLearning in CAMPUS ergänzt. Dazu entwickelt das CiL zusammen mit dem Rechen- und Kommunikationszentrum der RWTH in einer Kooperation mit Microsoft Deutschland GmbH das Lehr- und Lernportal L²P. Begleitend bietet das CiL allgemeine und spezifische Beratung und Qualifizierung zu eLearning und Blended-Learning, informiert über mögliche Einsatzszenarien und vermittelt gegebenenfalls bestehende Expertise an der RWTH.

Als hochschulweites Lehr- und Lernportal unterstützt L²P die Präsenzlehre der RWTH und steht als zentraler Dienst allen Studierenden und Lehrenden zur Verfügung. Es ermöglicht didaktisch innovative Methoden bei der Begleitung von Lehrveranstaltungen, insbesondere durch die Bereitstellung digitaler Lehrinhalte sowie Kommunikations- und Kollaborationsfunktionalität für Lehrende und Lernende. Ziel ist die breite Unterstützung der regulären Präsenzlehre, deren

Anreicherung durch eLearning und Blended-Learning sowie die Unterstützung und Vereinfachung der begleitenden Prozesse für Lehrende und Lernende. L²P soll dabei sowohl den möglichst einfachen Einstieg in eine elektronisch unterstützte Lehre für diejenigen Dozenten bieten, die bisher wenig Erfahrung mit dem Einsatz von eLearning haben, als auch komplexere didaktische Abläufe für fortgeschrittene eLearning-Szenarien ermöglichen.

Obwohl sich alle Beteiligten einig sind, dass eLearning wesentlich zur Verbesserung der Qualität der Lehre beitragen wird, kann dessen Einführung unter den aktuellen Rahmenbedingungen nicht mit einem dauerhaft erhöhten Aufwand einhergehen. Eine Lösung, die nachhaltig effiziente Prozesse unterstützt, ist deshalb essenziell. Um Redundanzen zu vermeiden und Synergien zu nutzen, baut L²P auf den etablierten zentralen Diensten der RWTH auf: Die Entwicklung von L²P erfolgt auf Basis des CAMPUS-Informationssystems, in dessen administrative Prozesse es nahtlos integriert ist. Ebenso wird das vorhandene Aachener Identity Management bei der Realisierung von L²P einbezogen.

Als webbasierter Dienst ist der Zugang zu L²P jederzeit und von jedem Ort aus möglich. Als geschlossener Dienst mit entsprechender Authentifizierung erfolgt die Darstellung aller Inhalte personalisiert und auf den entsprechenden Nutzer abgestimmt. Durch die Verwendung klar strukturierter Lernräume zu allen Veranstaltungen ist ein homogener und einheitlicher Zugriff auf alle Dienste und Materialien in L²P gewährleistet.

2 Das CAMPUS-Informationssystem

CAMPUS ist das integrierte Informationssystem der RWTH Aachen. Das webbasierte Informationssystem unterstützt wesentliche Kernprozesse der Hochschule über organisatorische, Nutzergruppen- und Systemgrenzen hinweg. Im Jahr 2001 startete das Vorlesungs- und Organisationsverzeichnis. Heute werden mehr als ein Dutzend unterschiedlicher Dienste von „A“ wie Auszubildendenverwaltung bis „Z“ wie virtuelles Zentrales Prüfungsamt in Zusammenarbeit zwischen dem Rechen- und Kommunikationszentrum mit Kooperationspartnern in Verwaltung, zentralen Einrichtungen und den Fachbereichen angeboten. Mehr als 1.500 Mitarbeiter in 700 Organisationseinheiten tragen aktiv in ihren spezifischen CAMPUS-Rollen wie z.B. Dozent, Fachstudienberater oder Rollenverwalter dazu bei, alle Studierenden und Mitarbeiter der RWTH zu unterstützen.

2.1 Anwendungsportfolio

CAMPUS gliedert sich in vier Anwendungsbereiche, siehe Abbildung 1. Neben den Bereichen Veranstaltungsorganisation, Verzeichnisdienste, und Unterstützung von Organisationsabläufen kommt durch das L²P-Projekt der Bereich eLearning hinzu. Jeder der vier Anwendungsbereiche umfasst mehrere Anwendungen, die jeweils eine Reihe von Prozessen unterstützen. Alle Anwendungen nutzen die gemeinsame technische Betriebs- und Supportinfrastruktur des CAMPUS-Informationssystems.

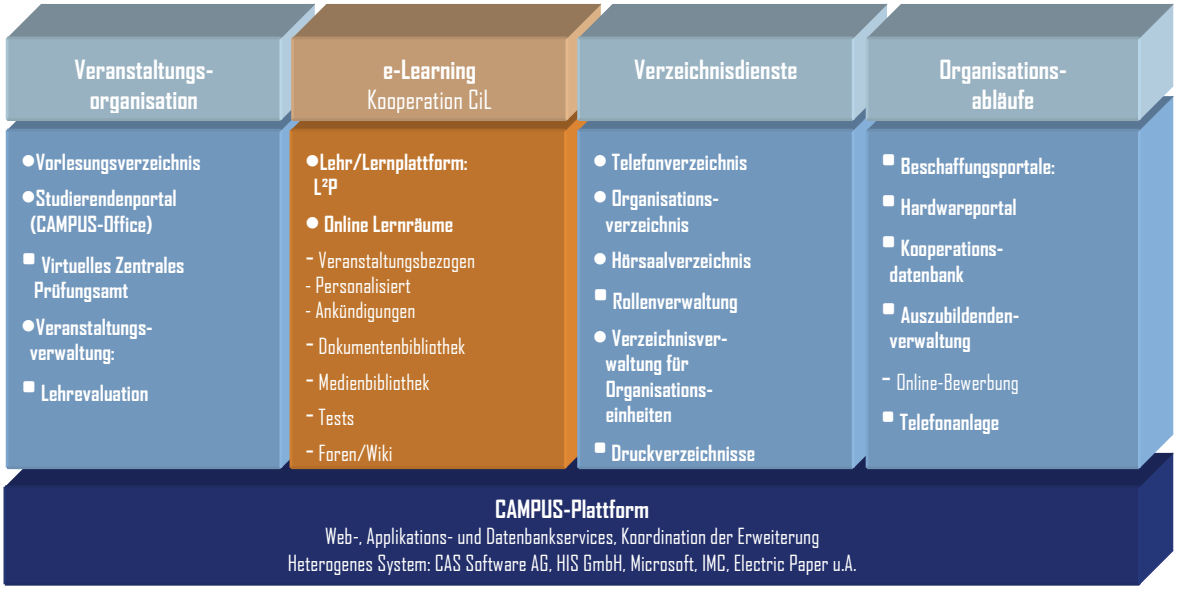


Abb. 1: Anwendungsportfolio des CAMPUS-Informationssystems

Der Anwendungsbereich *Veranstaltungsorganisation* umfasst das öffentliche Vorlesungsverzeichnis inkl. Raumbuchung und Semesterplanung, die Vorlesungsplanung für Studierende (CAMPUS-Office), das Virtuelle Zentrale Prüfungsamt, die personalisierten Zugänge für Dozenten, Fachstudienberater und Dekane und die studentische Lehrveranstaltungsbewertung (Lehrevaluation). Dieser Bereich umfasst auch die im Projekt Modul-IT realisierte Unterstützung modularisierter Studiengänge für den europäischen Bolognaprozess.

Der in Kooperation mit dem CiL betriebene Anwendungsbereich *eLearning* umfasst die Entwicklung und den technischen Betrieb des integrierten Lehr- und Lernportals L²P.

Der Anwendungsbereich *Verzeichnisdienste* umfasst das öffentliche Telefon- und Organisationsverzeichnis, das Hörsaalverzeichnis sowie den personalisierten Zugang für die Organisationseinheiten zur Verwaltung der Verzeichnisse. Alle Verzeichnisse sind

untereinander verbunden. So ist es möglich, ausgehend von dem Belegungsplan eines Hörsaals zu einer Veranstaltung über deren Dozenten zu dessen Organisationseinheit zu navigieren und sich dort über die Veranstaltungsliste der Organisationseinheit wiederum zu einem Studiengang zu bewegen.

Im Anwendungsbereich *Unterstützung von Organisationsabläufen* sind eine Reihe recht unterschiedlicher Anwendungen zusammengefasst. Dazu zählen die vereinfachte Beschaffung von standardisierten Arbeitsplatzrechnern über das Hardwareportal, die Kooperationsdatenbank DACOR zur Anbahnung von Kooperationen, eine Auszubildendenverwaltung, die Anbindung an die Telefonanlage und die Anbindung des Softwareportals zur hochschulweiten Beschaffung von Software zu Hochschulkonditionen. Weitere Prozesse sind die Erstellung gedruckter Verzeichnisse sowie zahlreiche regelmäßige Datenexporte zu lose gekoppelten Systemen in und außerhalb der Hochschule.

2.2 Zielgruppen

Die drei größten Zielgruppen der Dienste des CAMPUS-Informationssystems sind die Studierenden, die Dozenten und die neun Fachbereiche der RWTH. Für die Studierenden bietet das CAMPUS-Informationssystem den speziellen personalisierten Zugang CAMPUS-Office. Der Onlinestudienplaner ermöglicht jedem Studierenden die individuelle Vorlesungsplanung und den direkten Zugriff auf die persönlichen Vorlesungs- und Veranstaltungsdaten. Mit CAMPUS-Office können sie ihre Termine organisieren, sich zu Veranstaltungen und Prüfungen anmelden, E-Mails lesen und versenden, Dokumente speichern und vieles mehr; und dies von zu Hause aus, an der Universität, während eines Praktikums im In- und Ausland oder sogar im Urlaub.

Dozenten können über ihren persönlichen Zugang zum CAMPUS-Informationssystem ihre Vorlesungen, Übungen, Seminare etc. verwalten und im Online-Vorlesungsverzeichnis ankündigen. Die Dozenten pflegen dabei die Angaben ihrer eigenen Veranstaltungen und die Zuordnung der Veranstaltungen zu Studiengängen. Gleichzeitig mit der Eintragung in das Vorlesungsverzeichnis ist auch die verbindliche Buchung von geeigneten Hörsälen für die gewünschten Termine möglich. Richtet der Dozent Anmeldeverfahren für seine Veranstaltungen ein, erhält er durch die Online-Anmeldung der Studierenden über CAMPUS-Office individuell für jede Veranstaltung Anmelde- und Teilnehmerlisten mit Kontaktdaten, Studiengang und Fachsemester der Studierenden. Diese Daten kann er für die weitere

Veranstaltungsorganisation exportieren; über die integrierte E-Mail-Funktion kann er die Teilnehmer direkt per E-Mail anschreiben.

Die Fachbereiche pflegen über die Rolle des Fachstudienberaters ihre Studiengänge, Prüfungsordnungen, Studienpläne sowie die Zuordnung der Veranstaltungen. Über die Rollenverwaltung können die Einrichtungen der Fachbereiche ihre Mitarbeiter für die unterschiedlichen Dienste autorisieren. Die Einrichtungen nutzen über ihre autorisierten Mitarbeiter die übrigen Dienste des CAMPUS-Informationssystems, indem Sie z.B. elektronische Beschaffungen über das Hardwareportal durchführen oder die Kooperationsangaben in der Kooperationsdatenbank DACOR pflegen. Über das Hardwareportal können Einrichtungen standardisierte PC-Systeme, Monitore und Laptops in einem vereinfachten und beschleunigten Beschaffungsverfahren ohne Durchführung eines eigenen Preisvergleichs bestellen. Der Preisvergleich wird dabei durch ein Online-Bieterverfahren ersetzt. Für die Produkte wird jeweils der günstigste Bieter alle 2 Wochen neu ermittelt. Die Bestellung erfolgt online durch autorisierte Mitarbeiter der Einrichtungen.

2.3 Eckdaten und Nutzung

Das offizielle Veranstaltungsverzeichnis wird an allen neun Fachbereichen der RWTH flächendeckend eingesetzt. Der Bestand des Veranstaltungsverzeichnisses umfasst im Wintersemester 2006/2007 insgesamt 7.537 Veranstaltungen für 9 Fachbereiche in 136 Studiengängen. Diese sind verbunden mit 87.430 Raumbuchungen. An den Veranstaltungen sind 3.873 unterschiedliche Dozenten beteiligt. In über 1.500 Anmeldeverfahren wurden 56.000 Anmeldungen von Studierenden zu Veranstaltungen und Prüfungen durchgeführt. Die online verfügbaren, historischen Semester seit 2001 haben jeweils einen ähnlichen Umfang. Im aktuellen Semester werden ca. 17.000 Notenspiegel pro Monat über das Virtuelle Zentrale Prüfungsamt abgerufen und darüber mehr als 12.000 Bescheinigungen online erstellt. Der aktuelle Datenbestand des Mitarbeiter-, Adress- bzw. Organisationsverzeichnisses umfasst ca. 25.000 Einträge. Das Hardwareportal machte im Jahr 2006 über 500.000 € Umsatz. Auch für alle weiteren Dienste des CAMPUS-Informationssystems werden kontinuierlich vergleichbare statistische Daten erhoben.

Abbildung 2 zeigt die Nutzung des Gesamtsystems. Diese wächst seit 2003 mit einer kontinuierlichen Wachstumsrate von ca. 50% pro Jahr. Im Zusammenhang mit den Erweiterungen zum Leistungs- und Teilnehmermanagement für den europäischen Bolognaprozess und einer Integration mit dem hochschulweiten Lehr- und Lernportal L²P wird

für 2007 noch ein verstärktes Wachstum erwartet. Der Betrieb der Plattform erfolgt auf einer Webfarm in 3-Schichtenarchitektur, mit aktuellen Technologien z.B. für Lastbalanzierung, automatisiertem Deployment und kontinuierlichem Monitoring unter Einsatz eines komplexen Softwarestacks von der Firewall über Web- und Applikationsserver bis zur Datenbank. Die Webfarm wird unter Microsoft Windows betrieben. Die gemessene effektive Verfügbarkeit der Plattform erreichte 2005 einen Wert von 99,9% bei einer „Rund um die Uhr"-Servicezeit von 365 Tagen á 24 Stunden pro Jahr.

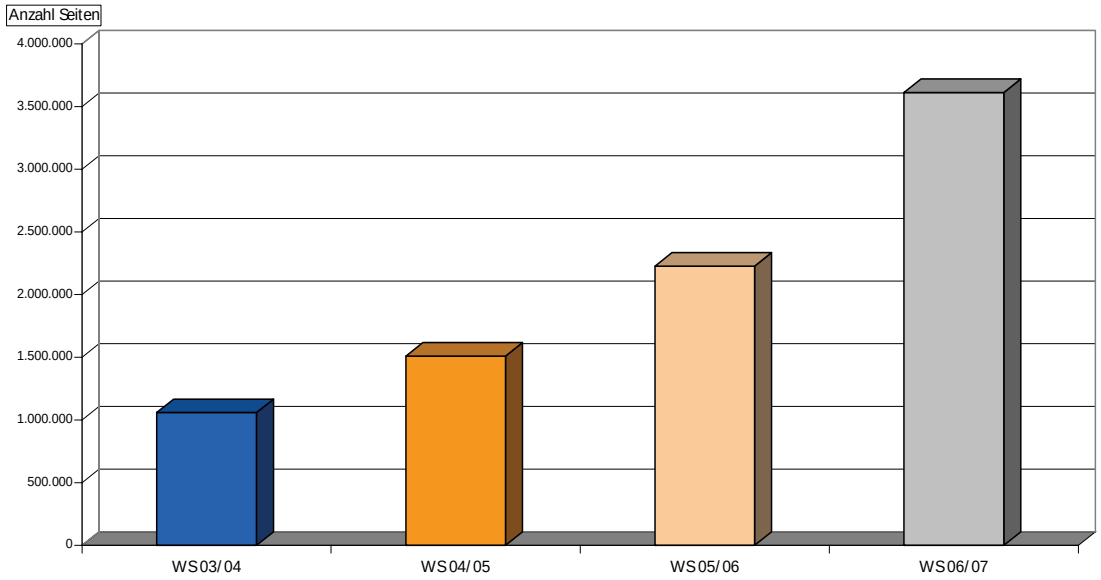


Abb. 2: Entwicklung der Seitenabrufe in der jeweils ersten Vorlesungswoche seit 2003

Das CAMPUS-Informationssystem nutzt selbst grundlegende Dienste wie das Identity Management TIM der RWTH. Es enthält elektronische Kennungen für alle Studierenden und wird genutzt, um zahlreiche Dienste für Studierende im CAMPUS-Informationssystem und von anderen Dienstleistern freizuschalten (E-Mail-Accounts, Netzzugänge wie VPN und WLAN, Softwarelizenzen im Rahmen der MSDN Academic Alliance, UMS, privater Webspace etc.)

3 Das integrierte Lehr- und Lernportal L²P

Bei der Entwicklung des Lehr- und Lernportals L²P wird von Anfang an auf die Integration mit der bestehenden und bewährten IT-Infrastruktur gesetzt. Abbildung 3 zeigt die Verzahnung der Abläufe und Systeme. Um Lehrveranstaltungen einzurichten, legen die Dozenten vor Beginn

des Semesters einen entsprechenden Eintrag in CAMPUS an. Dabei werden die Termine und Räume der Lehrveranstaltung verbindlich gebucht und weitere Details zur Lehrveranstaltung wie zugehörige Studiengänge und Hörerkreise, Dozenten und Veranstalter, Umfang, Credits, Voraussetzungen, Prüfungsleistungen, Kurzbeschreibung zum Inhalt und Literatur etc. angegeben. Außerdem kann für die Lehrveranstaltung eines von mehreren alternativen Online-Anmeldeverfahren bestimmt werden, anhand dessen sich Studierende in ihrem persönlichen Studienplaner CAMPUS-Office zu der Veranstaltung anmelden können.

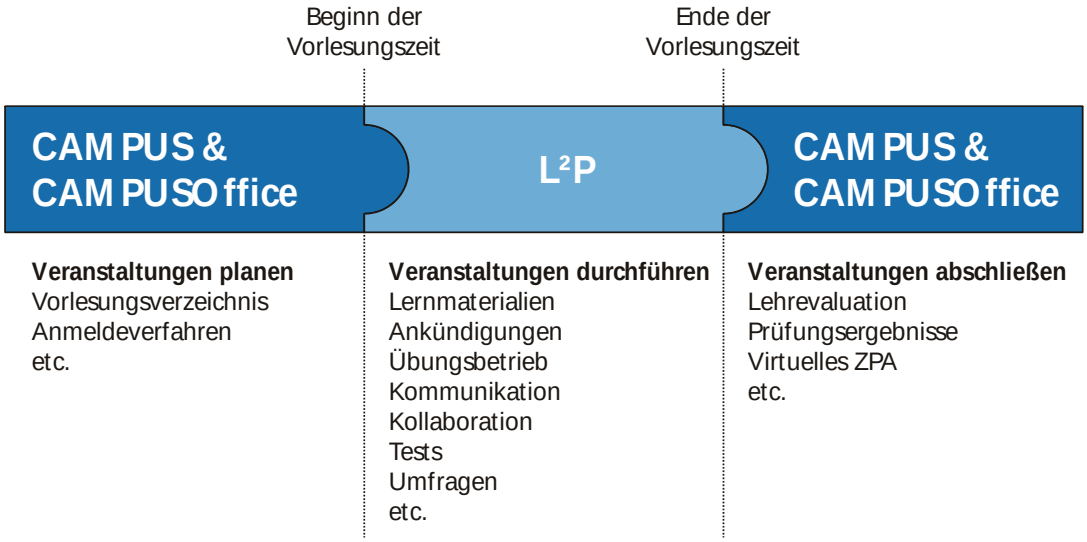


Abb. 3: Verzahnung von CAMPUS und L²P

Die Daten aus CAMPUS zu einer Lehrveranstaltung werden dann genutzt, um einen virtuellen Lernraum in L²P zu generieren, der zu der entsprechenden Lehrveranstaltung zugeordnet ist. Relevante Daten werden dabei direkt aus CAMPUS bezogen, so dass Dopplungen und Redundanzen strikt vermieden werden und für die jeweiligen Informationen tatsächlich nur ein Dienst zuständig ist. Innerhalb der virtuellen Lernräume können während des Semesters die elektronischen Lernmaterialien verteilt werden, es können Ankündigungen eingestellt und abgerufen und entsprechende Kommunikations- und Kollaborations-Elemente genutzt werden. Ferner können Dozenten elektronische Tests oder Umfragen einrichten, die Veranstaltungsteilnehmer online nutzen können. Im Rahmen eines von Tutoren betreuten Übungsbetriebs können Aufgabenblätter verteilt, Bearbeitungen eingereicht und Korrekturen abgerufen werden. Am Ende des Semesters erfolgt dann wieder die Übergabe zu CAMPUS, um die zentrale Lehrevaluation zu den Veranstaltungen durchzuführen und um gegebenenfalls Prüfungsergebnisse und -leistungen an das Virtuelle Zentrale Prüfungsamt zu übermitteln. Da

die Lernräume mit den Veranstaltungen im Vorlesungsverzeichnis und insbesondere die Teilnehmer mit denen im Prüfungsamt gemeldeten Teilnehmern stets übereinstimmen, ist der nahtloser Übergang sichergestellt.

Die Strategie zur Integration eines Lehr- und Lernportals mit der bestehenden IT-Infrastruktur macht deutlich, dass ein Learning-Management-System „von der Stange“ den Anforderungen nicht gerecht werden kann. Nutzer beider Ebenen, der administrativen und der des Lehr- und Lernportals, sind die gleichen Personengruppen, in beiden Ebenen müssen nicht-disjunkte Daten vorgehalten und Prozesse aufeinander abgestimmt werden. Die vorgesehene Integration erfordert insbesondere mehr als ein reines „Single-Sign-On“ in verschiedenen Systemen. Alle Personen- und Lehrveranstaltungsdaten sollen in den beteiligten Komponenten abgeglichen sein, um das sonst zu erwartende Chaos bei inkonsistenten Daten wie z.B. Veranstaltungsnamen oder E-Mail-Adressen, der zu erwartende Unmut der Nutzer bei unklaren Zuständigkeiten der Systeme und die zu erwartenden Widersprüche bei nicht abgestimmten Prozesse zu vermeiden. Insbesondere betrifft die genannte Integration nicht nur die technische Verbindung verschiedener Softwaresysteme, sondern gerade auch die Integration von Daten und administrativen Prozessen. Entsprechend müssen die Benutzerdaten von L²P nicht neu eingerichtet werden, sondern werden aus den beiden bestehenden Quellen bezogen: die Benutzerdaten der Studierenden aus dem Identity Management TIM und die der Mitarbeiter aus dem CAMPUS-Organisationsverzeichnis.

Bei der Evaluierung geeigneter Lösungen kam weiterhin die allgemeine Strategie des Rechen- und Kommunikationszentrums der RWTH zum tragen, dass – wenn möglich und angebracht – kommerzielle Software gegenüber Eigenentwicklungen oder OpenSource-Lösungen zu bevorzugen ist. Der Einsatz kommerzieller Lösungen garantiert die notwendige Professionalität und Skalierbarkeit der Systeme, ermöglicht den Rückgriff auf einen entsprechenden Support und erlaubt dauerhaft an der Produktweiterentwicklung zu partizipieren. Weiterhin musste die Tatsache berücksichtigt werden, dass der Markt der Learning-Management-Systeme ein hochfluider Markt ist, dessen Bereinigung noch aussteht. Vor diesem Hintergrund entstand der Wunsch der RWTH, zusammen mit kommerziellen Partnern eine nachhaltige Lösung zu entwickeln, die die oben genannte Integration der bestehenden IT-Infrastruktur realisiert und durch den Einsatz kommerzieller Software eine höhere Zukunftssicherheit verspricht, die aber durch die Möglichkeit flexibler Anpassungen und definierter Schnittstellen gewährleistet, dass

auch zukünftige Entwicklungen aufgenommen und weitere Prozesse und Systeme der RWTH oder Lösungen von Drittanbietern bei Bedarf integriert werden können.

3.1 Die Realisierung

Für die Umsetzung der im vorigen Abschnitt skizzierten strategischen Vorgaben wurde Microsofts SharePoint®-Technologie identifiziert. Als komponentenbasierte Portaltechnologie bietet SharePoint die geeigneten Mittel wie beispielsweise Single-Sign-On-Verfahren, um die gewünschte Integration für das Lehr- und Lernportal L²P zu realisieren. Die SharePoint-Technologie bietet selbst schon viele einfach zu bedienende Kommunikation- und Kollaborationselemente, die zur Realisierung von eLearning-Grundfunktionen genutzt werden können. Die Online-Befragung von HISBUS zur Nutzung und Akzeptanz internetgestützter Lernangebote für Studierende im Jahr 2005 [KlWW05] zeigt, dass Studierende mit derartigen Basisdiensten bereits zufrieden sind, diese Dienste aber auch in einer Lehrveranstaltung erwarten. Über Webservices können außerdem relativ leicht Schnittstellen zum CAMPUS-Informationssystem definiert werden, so dass bereits in CAMPUS vorhandene Daten in der SharePoint-Umgebung eingebunden werden können. Die Portal-Technologie selbst ermöglicht einen flexiblen Ausbau, Komponenten können als so genannte „Webparts“ auf der Basis moderner und nachhaltiger Programmiersprachen wie C# und ASP.NET unter Verwendung der professionellen Entwicklungsumgebung Microsoft Visual Studio® eigenständig angepasst und entwickelt werden.

Allerdings bietet SharePoint keine eigentliche eLearning-Funktionalität wie z.B. Assessments, elektronische Tests oder die Unterstützung eines tutoriellen Übungsbetriebs. Zu diesem Zweck wird als zusätzliche Komponente ein kommerzielles Learning-Management-System innerhalb von SharePoint eingebunden, nämlich CLIX Campus® der imc AG Saarbrücken. Im Rahmen eines gemeinsamen Projekts zwischen der RWTH Aachen, Microsoft Deutschland GmbH und der imc AG Saarbrücken wird seit Sommer 2006 das integrierte Lehr- und Lernportal L²P entwickelt. Ziel ist die hochschulweite Einführung von L²P zum Sommersemester 2007. Im Sommer 2006 wurde in Zusammenarbeit der Projektpartner ein Konzept für die Integration von CLIX in SharePoint entwickelt. Für das Release CLIX 7.0 übersetzt die imc AG Teile des Systems CLIX in Webparts, die dann innerhalb von Microsoft Office SharePoint Server® 2007 (MOSS 2007) direkt genutzt werden können. Auf der anderen Seite unterstützt Microsoft Deutschland GmbH die RWTH bei der Anbindung des CAMPUS-Informationssystems an

MOSS 2007, so dass beide Entwicklungsschienen zum Sommersemester 2007 zusammenlaufen, um insgesamt das Lehr- und Lernportal L²P zu bilden.

Für den Betrieb eines Lehr- und Lernportals wurde bereits Ende 2005 eine skalierbare Server-Farm im Rechen- und Kommunikationszentrum in Betrieb genommen. Im Sommersemester 2006 fand eine Testphase unter Verwendung eines „halbintegrierten" Pilotsystem aus den drei Komponenten CAMPUS, CLIX 6.0 und SharePoint 2003 statt, um erste Erfahrungen zu sammeln und zusammen mit Nutzern aus drei Fachbereichen eine formative Evaluation durchzuführen. Es wurden Lernräume für vier Veranstaltungen mit ca. 120 Studierenden eingerichtet. Informationen zur Veranstaltung wie Titel, Dozenten und Lerneinheit sowie eine Darstellung der Termine und Räume anhand einer Kalender-Darstellung wurden über Webservices direkt und synchron aus CAMPUS bezogen und über entsprechende CAMPUS-Webparts in Sharepoint eingebunden. Der Lehrplan einer zugehörigen Lehrveranstaltung in CLIX 6.0 wurde als „Seitenviewer-Webpart" innerhalb einer iframe-Konstruktion eingebunden. Zusätzlich wurden weitere SharePoint-eigene Webparts wie z.B. Ankündigungen verwendet. Die Authentifizierung erfolgte über SharePoint auf Basis eines Active Directory und wurde im Rahmen eines Single-Sign-On-Verfahrens an CLIX weitergegeben. Das Active Directory selbst enthielt die Benutzerdaten aus den weiter oben beschriebenen zentralen Datenquellen. Die Teilnehmerbuchung in CLIX und SharePoint erfolgte zunächst von Hand.

Im Wintersemester 2006/07 erfolgt die eigentliche Pilotphase unter Verwendung der gleichen Software. Es wurden Piloten aus nahezu allen Fachbereichen akquiriert. Die Gesamthörerzahl der 30 durch L²P unterstützten Veranstaltungen beträgt ca. 5.000 Studierende. Die eigentlichen Lernräume in L²P wurden erweitert und in drei Bereiche unterteilt: ein *Veranstaltungsbereich*, ein *CLIX-Bereich* und ein *gemeinsamer Bereich*. Die Erläuterung der Funktionalitäten erfolgt weiter unten. Die Lernräume werden dabei einheitlich durch die Administratoren gemäß SharePoint-Templates erzeugt. Die Buchung der Dozenten und berechtigten Mitarbeiter erfolgt von Hand, während die Buchungen der Teilnehmer gemäß den CAMPUS-Anmeldeverfahren automatisch erfolgen und täglich synchronisiert werden. Zum Sommersemester 2007 soll dann der Einsatz des voll-integrierten Produktivsystems von L²P unter Verwendung von MOSS 2007 und des SharePoint-integrierten CLIX 7.0 erfolgen. Die Lernräume in L²P werden noch einmal differenziert und um neue Funktionalitäten erweitert. Jeder Dozent kann dann beim Anlegen einer Lehrveranstaltung im CAMPUS-Informationssystem automatisch und durch einen Klick einen korrespondierenden virtuellen Lernraum in L²P erzeugen. Die Teilnehmer in den

Lernräumen werden gemäß der CAMPUS-Anmeldeverfahren vollautomatisiert zu den virtuellen Lernräumen gebucht.

3.2 Die Funktionen des Zielsystems im Sommersemester 2007

Jeder virtuelle Lernraum zu einer Veranstaltung besteht aus mehreren Bereichen, die über eine entsprechende Navigationsleiste erreicht werden können. Die Bereiche sind in zwei Gruppen unterteilt: Bereiche, die ausschließlich von Dozenten bearbeitet werden und in denen Studierenden lediglich Informationen und Materialien abrufen können, sowie Bereiche, innerhalb derer Studierende selbst aktiv Inhalte und Materialien einstellen können, so dass die Möglichkeit der Kollaboration gegeben ist. Abb. 4 stellt einen Ausschnitt aus einem virtuellen Lernraum dar.

Abb. 4: Informationsbereich eines virtuellen Lernraums

Der Informationsbereich eines Lernraums stellt die aus dem CAMPUS-Informationssystem abgerufenen Daten wie Titel der Lehrveranstaltung, Veranstaltungsform, verantwortliche Dozenten und Lehreinheiten sowie die Termine und Räume für Präsenzveranstaltungen in Form eines Kalenders dar. Der nächste Termin und Raum wird dabei hervorgehoben. Die Dozenten haben zusätzlich die Möglichkeit, jeder Lehrveranstaltung ein Bild zuzuordnen, z.B. das Logo

der veranstaltenden Lehreinheit. Weiterhin können Dozenten und berechtigte Mitarbeiter Ankündigungen (ggf. mit Verfallsdatum) einstellen sowie Hyperlinks zur Lehrveranstaltung angeben. Organisatorische Details wie Inhalt, Literatur, Prüfungsmodalitäten etc. werden gemäß der Angaben aus dem CAMPUS-Vorlesungsverzeichnis hier ebenfalls dargestellt und können durch belieben formatierten Text von den Dozenten ergänzt werden. Schließlich haben die Dozenten die Möglichkeit, direkt aus L²P heraus eine E-Mail an alle Teilnehmer der Lehrveranstaltung zu schreiben, wobei die bei der Anmeldung in CAMPUS hinterlegten E-Mail-Adressen der Studierenden genutzt werden. In einem weiteren Bereich können Dozenten elektronische Lernmaterialien und Lernressourcen wie Folien, Dokumente, Videos etc. bereitstellen, zum einen in Form eines Dateisystems mit Ordnern, Unterordnern usw., zum anderen in Form einer strukturierten Ansicht, die eine Zuordnung zu den jeweiligen Veranstaltungsterminen gemäß den Einträgen im Vorlesungsverzeichnis erlaubt und entsprechend darstellt. Die Einsatz der SharePoint-Technologie im Umgang mit Dateien gewährleistet dabei eine einfache Bedienung, die sich stark an den vertrauten Dateioperationen in den gängigen Betriebssystemen orientiert und die daher auch von denjenigen Dozenten unmittelbar genutzt werden können, die kaum Erfahrungen im Umgang mit Learning-Management-Systemen vorweisen. SharePoint garantiert andererseits ein sicheres Dateimanagement, so dass geschützte Dateien tatsächlich auch nur von entsprechend berechtigten Personen im Rahmen einer Lehrveranstaltung abgerufen werden können.

Ein anderer Bereich ermöglicht die Erstellung von Umfragen, etwa zur Ermittlung von Wissensständen oder zur spontanen Abfrage von Meinungsbildern. Umfragen werden ebenfalls in SharePoint erstellt und verwaltet, welches sowohl eine intuitive Benutzerführung bei der Erstellung wie auch – neben dem Export in gängige Datenverarbeitungssysteme – eine graphische Auswertung der Umfrage in L²P erlaubt. Ein gemeinsamer Bereich fasst kommunikative Elemente und Arbeitsbereiche zur Kollaboration von Dozenten und Studierenden zusammen: Diskussionsforen, Chats und eine Dokumentenbibliothek, in der auch Studierende Medien untereinander und mit den Dozenten austauschen können, wobei für jeden Lernraum eingestellt werden kann, ob eine vorherige Inhaltgenehmigung von Seiten der Dozenten bzw. berechtigter Mitarbeiter notwendig ist. Zusätzlich ist ein Bereich vorhanden, in dem Wiki-Seiten von allen Teilnehmern gemeinsam erstellt werden können. Wiki-Seiten sind eine Kernfunktion der unter dem Namen *Web 2.0* bekannten, gegenwärtigen Prozesse der Internet-Gemeinschaft, bei der Nutzer in der Breite Inhalte erstellen und austauschen.

Entsprechend stellen sie eine didaktisch innovative Methode dar, bei der Dozenten *und* Studierende gemeinsam Lerninhalte und Wissenseinheiten erstellen und revidieren können.

Schließlich werden in einem so genannten CLIX-Bereich Komponenten und Funktionen des Learning-Management-Systems CLIX bereitgestellt, um die bereits skizzierten eLearning-Grundfunktionen von SharePoint um weiterführende eLearning-Elemente zu ergänzen. Insbesondere können hier elektronische Tests, adaptive Lernpfade und Lernlogiken, Lernfortschrittskontrollen für die Lehrveranstaltung realisiert sowie externe Lehreinheiten wie WBT's oder CBT's in den bekannten Standardformaten eingebunden werden. Außerdem ermöglicht CLIX die webbasierte Unterstützung eines tutorieller Übungsbetriebs. Elektronische Tests ermöglichen zum einen, dass Studierende das erlernte Wissen in Selbsttests prüfen oder anwenden und unmittelbar eine entsprechende Rückmeldung zu ihrem Lernstand erhalten. Andererseits können elektronische Testate auch zur prüfungsrelevanten Leistungsbestimmung genutzt werden, wobei durch die Möglichkeit der automatischen Korrektur von entsprechenden Aufgabentypen – gegebenenfalls gemischt mit Aufgabentypen, die einer manuellen Korrektur bedürfen – eine Arbeitsentlastung gegenüber einem rein papierbasierten Test erzielt werden kann. CLIX bietet zu allen elektronischen Tests umfangreiche statistische Auswertungen und Reports, so dass Dozenten sowohl den gesamten Lernstand aller Teilnehmer als auch den von einzelnen Studierenden abrufen und in der Lehrveranstaltung entsprechend reagieren können. Lernpfade und Lernlogiken bieten dem Dozenten die Möglichkeit, vorab den logischen Ablauf einzelner Lernkomponenten zu steuern, indem entsprechende Regeln definiert werden. Beispielsweise könnten die Folien und Dokumente des 2. Kapitels erst freigegeben werden, nachdem der elektronische Test zum 1. Kapitel vom Studierenden bestanden wurde.

Die Dozenten können zum jeweiligen Lernraum auf einer entsprechenden Administrationsseite selbständig entscheiden, welche Bereiche und Funktionen aktiviert sind und ob auch den Studierenden die Liste der Teilnehmer angezeigt wird. SharePoint bietet weiterhin die Möglichkeit, sich bei Änderungen von Inhalten wie z.B. einer neuen Ankündigung oder einem geänderten Dokument per E-Mail benachrichtigen zu lassen, wobei jeder Nutzer seine eigenen Benachrichtigungseinstellungen definieren kann. Außerdem können nahezu alle aktiven Inhalte auch als RSS-Feeds „empfangen" werden. Neben den einzelnen Lernräumen steht außerdem ein „Desktop" zur Verfügung, auf dem zum einen zusätzliche Angaben zu „meinen Veranstaltungen" auf den Nutzer abgestimmt angeboten bzw. Informationen personalisiert akkumuliert werden, wie z.B. alle Ankündigungen der Lehrveranstaltungen, zu denen der

Nutzer angemeldet ist oder die Sprechzeiten der Dozenten dieser Lehrveranstaltungen. Vom Desktop aus können die Nutzer auch nach Elementen in den Lernräumen suchen, zu denen sie eine entsprechende Berechtigung besitzen.

3.3 Die Vorteile und Mehrwerte des gewählten Ansatzes

Ein besonderes Charakteristikum des gewählten Ansatzes der RWTH ist die Einbindung der bestehenden und bewährten IT-Struktur und der administrativen Abläufe der Lehre. Durch die automatische Generierung von Lernräumen in L²P aus den Metadaten zu einer Lehrveranstaltungen im CAMPUS-Informationssystems und die automatische Buchung von Studierenden gemäß der in CAMPUS realisierten, RWTH-spezifischen Anmeldeverfahren – nach formaler Prüfung der Zulassungsvoraussetzung – ist die Einstiegshürde für die Nutzung virtueller Lernräume in L²P minimiert. Die Kombination der verschiedenen Funktionalitäten aus MOSS 2007, CAMPUS und CLIX garantiert zudem sowohl eine einfache Nutzung von intuitiven Grundfunktionen für die breite Anwendung, aber auch die Möglichkeit der Umsetzung komplexer eLearning-Szenarien für erfahrene Anwender durch Einsatz eines professionellen Learning-Management-Systems.

Die Anbindung an CAMPUS, die niedrige Einstiegshürde bei der Erzeugung von Lernräumen und die intuitiven Grundfunktionen von L²P gewährleisten mittelfristig die vollständige Abdeckung des regulären Lehrbetriebs. Der Einsatz der komponentenbasierten SharePoint-Technologie ermöglicht die Anpassung an die lokalen Gegebenheiten, insbesondere durch den Einsatz entsprechender Schnittstellen, sowie einen flexiblen Ausbau. Komponenten (Webparts) können auf Basis moderner und nachhaltiger Entwicklungsumgebungen eigenständig angepasst und entwickelt bzw. von Drittanbietern lizenziert werden. Schließlich gewährleistet der Einsatz kommerzieller Lösungen die notwendige Professionalität der Systeme in Hinblick auf Skalierbarkeit, Design, nachhaltige Pflege, Support und Weiterentwicklung der zugrunde liegenden Software.

Für Dozenten und Mitarbeiter besteht der Mehrwert bei Nutzung von L²P in erster Linie darin, dass wesentliche Grundfunktionen der Lehre wie Kommunikation und Kollaboration mit den Studierenden und die Verbreitung von Informationen und Lernmaterialien einheitlich im Rahmen einer klar strukturierten Oberfläche und ohne Einarbeitung in ein komplexes System erfolgen kann. Insbesondere können dadurch eigene administrative Aufwände wie z.B. die Einrichtung und der Betrieb diverser Server für Internetdienste (z.B. Web, Mail, Forum,

BSCW, Chat etc.) vermieden werden. Der Aufwand bei der Einrichtung der Lernräume und der Buchung der Teilnehmer ist minimal und wird automatisch durch die ohnehin obligatorischen Prozesse der RWTH bereitgestellt. Durch die Authentifizierung zu L²P ist gewährleistet, dass bereitgestellte Informationen und Materialien exakt die gewünschte Zielgruppe der Teilnehmer einer Lehrveranstaltung erreichen – ein Aspekt, der auch relevant für urheberrechtliche Fragen ist. Andererseits können innerhalb der gleichen Oberfläche weiterführende eLearning-Elemente wie elektronische Tests, Umfragen, Lernfortschrittskontrollen etc. eingebunden und die Unterstützung eines tutoriellen Übungsbetriebs genutzt werden, um die eigenen Lehrveranstaltungen didaktisch aufzuwerten.

Der Mehrwert für Studierende ist insbesondere dadurch gegeben, dass sie sich nur in *einem* System zu Lehrveranstaltungen und Prüfungen anmelden müssen (CAMPUS-Office) und alle notwendigen Informationen in *einem* System (L²P) einheitlich und personalisiert unterhalb einer entsprechen strukturierten Oberfläche erhalten. Es entfällt also die mühsame Suche von Informationen und Materialien auf schwarzen Brettern, verschiedenen Webseiten der Lehreinheiten oder in verschiedenen Learning-Management-Systemen mit unterschiedlichen Benutzeroberflächen und verschiedenen Zugangsdaten.

Literaturverzeichnis

[GeBi04] Gebhardt, Michael; Bischof, Christian: CAMPUS – das integrierte Informationssystem der RWTH Aachen. In: Praxis der Informationsverarbeitung und Kommunikation 27 (2004), S. 110-115.

[BiGS05] Bischof, Christian; Gebhardt, Michael; Steves, Peter: Bridging the Gap between Administrative and E-Learning Processes. In: Proceedings of the European University Information Systems Conference (EUNIS 2005).

[KlWa05] Kleimann, Bernd; Wannemacher, Klaus: E-Learning-Strategien deutscher Universitäten. HIS Kurzinformation B4, 2005.

[KlWW05] Kleimann, Bernd; Weber, Steffen; Willige, Janka: E-Learning aus Sicht der Studierenden. HISBUS-Kurzbericht Nr. 10, 2005.

ZePeLin Bayern – Realisierung einer modular aufgebauten, flexiblen Plattform für eLearning in Bayern

Sabine Rathmayer, Ivan Gergintchev, Steffi Lämmle

Institut für Informatik
Technische Universität München
85748 Garching b. München
{sabine.rathmayer, gergintchev, steffi.laemmle}@tum.de

Abstract

Ausgehend von den innerhalb des Projekts elecTUM an der Technischen Universität München (TUM) entwickelten Konzepten, Erfahrungen und erzielten Ergebnissen wird der Aufbau von netzbasierten Lehr- und Lernszenarien an Hochschulen und deren Umsetzung in Learning Management Systemen betrachtet. Daraus resultierend wird ein Vorschlag sowie die erste Realisierung einer modular aufgebauten, flexiblen Plattform – ZePeLin - für eLearning in Bayern beschrieben. Innerhalb von ZePeLin Bayern werden interessierten Hochschulen und Bildungseinrichtungen geschlossene Räume zur Verfügung gestellt, in denen sie die Präsenzlehre mit einfachen Lehr- und Lernszenarien unterstützen können. Durch die Anbindung der einzelnen Räume an die Benutzerverwaltung der jeweiligen Einrichtung wird den Benutzern ein Rollen basierter personalisierbarer Zugriff auf die Inhalte der Lernumgebung ermöglicht. Darüber hinaus wird die an der TUM vorhandene Kompetenz im Bereich eLearning und Infrastrukturen weiter gegeben.

1 Einführung

Im Rahmen der vom BMBF in 2005 gestarteten Förderlinie „Neue Medien in der Bildung - eLearning-Dienste für die Wissenschaft“ soll unter anderem „die Entwicklung von organisatorischer Infrastruktur und Management („change management“) zur Ausschöpfung des durch die IuK-Technologien eröffneten Innovationspotenzials im Bereich von Lehre, Lernen und Prüfungen an Hochschulen systematisch und nachhaltig“ vorangetrieben werden [Bmbf04].

elecTUM ist eines von 22 in dieser Maßnahme geförderten Projekten. Dabei wird an der TUM ein umfassendes und integriertes eLearning-Konzept umgesetzt, welches Präsenzstudium und eLearning in allen Leistungsbereichen der Universität miteinander verzahnt. Die Details dieses Konzepts können in [Bör04] nachgelesen werden. Ein wesentlicher und für den Hintergrund von ZePeLin ausschlaggebender Aspekt ist zum einen die Bereitstellung eines leistungsfähigen, flexibel einsetzbaren und anpassbaren Learning Management Systems (LMS) und dessen zentraler Betrieb. An der TUM ist seit 2005 das LMS CLIX Campus der Fa. imc AG im Einsatz. Neben den internen Nutzern aus den verschiedenen Fakultäten gibt es eine Reihe assoziierter Gruppen, denen die Dienste der zentralen Lernplattform zur Verfügung gestellt werden. Hierbei ist ein wesentliches Merkmal des Learning Management Systems CLIX - die Mandanten-Fähigkeit - von entscheidendem Vorteil. Nutzergruppen können dadurch jeweils eigene „Räume“ mit separater Benutzer- und Inhaltsverwaltung bei gleichzeitigem zentralen Support und Schulung in Anspruch nehmen.

Zweiter Hauptaspekt von elecTUM ist die Integration von CLIX in die IuK Infrastruktur der TUM. Während mancherorts Projekte laufen, in denen unterschiedliche Funktionalitäten und Dienste in einem Portal für Lehre und Studium zur Verfügung gestellt werden (z.B. [Juli06]), wird an der TUM die Strategie verfolgt, die jeweiligen Kernfunktionalitäten in bereits existierenden Systemen zu belassen und Informationen bei Bedarf auszutauschen bzw. nahtlose Übergänge zu schaffen. Hierbei werden Schnittstellen und Kopplungen zwischen den unterschiedlichen Informationssystemen der Hochschule teils gemeinsam mit der imc AG entwickelt bzw. umgesetzt (s. Abb. 1). Die möglichst nahtlose Integration der verschiedenen Systeme ist ein entscheidender Erfolgsfaktor für deren nachhaltige Etablierung [Gerg06].

Die Erfahrungen der vergangenen 1 ½ Jahren mit CLIX haben die Vorgehensweise innerhalb von elecTUM bestätigt. Mehr als 10.000 aktive Nutzer sind seither verzeichnet. Im Wintersemester 2006/2007 werden 200 Lehrveranstaltungen mit eLearning-Anteilen angeboten. Die Nachfrage bzgl. der Integration mit der Studien- und Prüfungsverwaltung (HIS-GX Systeme) ist groß. Die laufenden Schulungsmaßnahmen sowie die Rückmeldungen von Dozenten wie Studierenden zeigen jedoch eine ernstzunehmende Kritik an der Komplexität und mangelnden Flexibilität des Systems.

Parallel zu den Rückmeldungen innerhalb der Hochschule gab es zunehmend großes Interesse und Anfragen aus anderen Hochschulen, Teile der Konzepte sowie die technischen Lösungen zu übernehmen. So haben die Fachhochschulen München und Regensburg, die sich im Rahmen

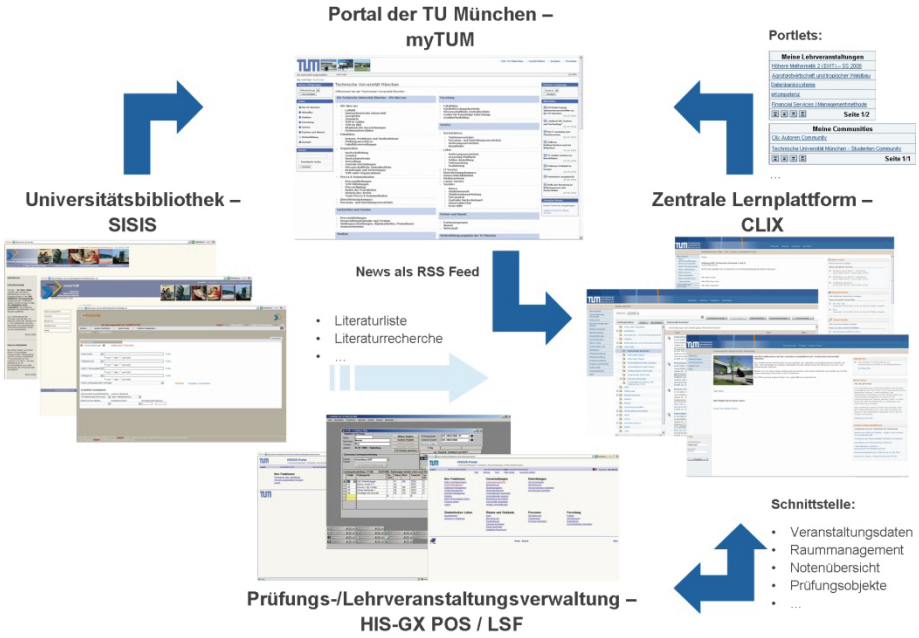


Abb. 20: Integrationsszenario an der TUM

ihrer Zielvereinbarungen mit dem bayerischen Staatsministerium für Wissenschaft, Forschung und Kunst verstärkt um den Einsatz von eLearning zur Entlastung der Lehrkapazität bemühen wollen, die Nutzung der technischen Infrastruktur der TUM angefragt.

Als Ergebnis des aufgebauten organisatorischen, fachlichen und technischen Know-Hows sowie den weiteren genannten Faktoren entstanden Überlegungen, ein hochschulübergreifendes Modell zur Unterstützung von Lehre und Forschung beim Einsatz neuer Medien zu entwickeln, welches Kosteneffektivität, Ergebnistransfer sowie die Möglichkeit zur Erbringung technologischer Dienstleistungen für Partnerhochschulen, einschließlich der Virtuellen Hochschule Bayern (vhb), bietet. Dieses Modell wird in einer ersten Version seit Oktober 2006 innerhalb des ZePeLin (Zentrales Portal für eLearning in Bayern) Portals auf Basis des Microsoft Office Sharepoint Servers 2007 (MOSS 2007) an den beiden Fachhochschulen München und Regensburg bereitgestellt.

In den folgenden Abschnitten wird ausgehend von gängigen Lehr- und Lernszenarien an Hochschulen sowie der Problematik mit existierenden Learning Management Systemen gezeigt, wie ein solches Konzept aussehen und entsprechend umgesetzt werden kann. Dabei wird neben den Funktionalitäten des Learning Managements auch die Verwaltung der Benutzer in diesem bayernweiten Szenario betrachtet.

2 Aufbau von Lehr- und Lernszenarien an Hochschulen

Nach Schulmeister [Schu01] lassen sich Lehr- und Lernszenarien durch den Einsatz verschiedener eLearning-Komponenten wie Medien, Kommunikationsmittel, eTests, etc. charakterisieren und nach dem relativen Anteil der virtuellen Komponenten skalieren. Durch den Einsatz eines LMS an Hochschulen ließen sich in der Vergangenheit diverse netzbasierte Lehr- und Lernszenarien für Dozenten und Studierende umsetzen. Dabei unterscheiden sich die Vorstellungen bzgl. der Umsetzung der Szenarien in einem LMS nicht nur von Hochschule zu Hochschule sondern auch innerhalb einer solchen sehr stark. Hersteller von LMS-Software stehen daher vor dem Problem, die Vielfalt der Anforderungen abzudecken. Der gängige Entwicklungsansatz bei kommerziellen wie Open Source Lernplattformen gleichermaßen ist dabei, bereits implementierte Lehr- und Lernszenarien bzw. Funktionalitäten sukzessive zu erweitern.

Das Ergebnis sind Systeme mit einem sehr großen Funktionsumfang, der jedoch häufig zu einer für den Benutzer schwer zu bewältigenden Komplexität führt. Um Akzeptanzprobleme, die oftmals mit der Einführung einer Lernplattform einhergehen, zu reduzieren, ist es sinnvoll Dozenten schrittweise und mit zunächst geringer Komplexität an die Benutzung einer Lernplattform heranzuführen [Müll06]. Ein LMS sollte eLearning unerfahrenen Dozenten alle grundlegenden Funktionalitäten anbieten, ohne diese technisch zu überfordern. Versierten und erfahrenen Lehrenden sollte das LMS die Auswahl aus einem breiten Funktionsumfang ermöglichen.

Bei der Gestaltung der unterschiedlichsten Lehr- und Lernszenarien sollten die individuellen Wünsche der einzelnen Dozenten erfüllt werden können. Dabei ist eine flexible und personalisierbare Gestaltung der Szenarien innerhalb der virtuellen Umgebung unter Verwendung aller benötigten eLearning-Komponenten wünschenswert.

Als weitere Anforderung innerhalb einer Hochschule zeigt sich die Experimentierfreudigkeit einzelner Dozentengruppen. Diese würden gern ihre eigens entwickelten und oft sehr ausgefeilten Szenarien in ein zentral zur Verfügung stehendes System integrieren. Ein solches System sollte daher beliebig und individuell erweiterbar sein.

Über die beschriebenen Szenarien hinaus finden sich in nahezu allen Bundesländern mittlerweile Netzwerke bzw. Verbünde (z.B. Bildungsportal Sachsen oder die Virtuelle Hochschule Bayern, vhb), die hochschulübergreifende Lehr- und Lernmodelle anbieten. Eine Plattform zur Unterstützung dieser Modelle muss die Möglichkeit bieten, Lehrveranstaltungen,

die innerhalb der einzelnen Hochschule verwaltet werden, in einem gemeinsamen Raum zur Verfügung zu stellen. Dabei müssen sämtliche Prozesse, die mit der Durchführung der Lehrveranstaltung zusammenhängen, abgewickelt werden.

3 Umsetzung der Lehr- und Lernszenarien in einer flexibel anpassbaren Lernplattform

Um die Umsetzungsmöglichkeiten der zuvor vorgestellten Idee einer flexibel anpassbaren eLearning-Umgebung zu überprüfen, wurden alle dozentenseitigen Abläufe im LMS CLIX identifiziert, dokumentiert und in einem Ablaufdiagramm dargestellt. Dabei wurde das Anlegen und Verwalten von Lehrveranstaltungen, Übungen, Communities, Medien, Kommunikationsmitteln, Ankündigungen, eTests, Evaluationen und die Benutzerverwaltung erfasst. Abb. 2 zeigt einen Ausschnitt des Ablaufdiagramms, welches das Anlegen einer Lehrveranstaltung mit verschiedenen Medien und Kommunikationsmitteln in CLIX visualisiert.

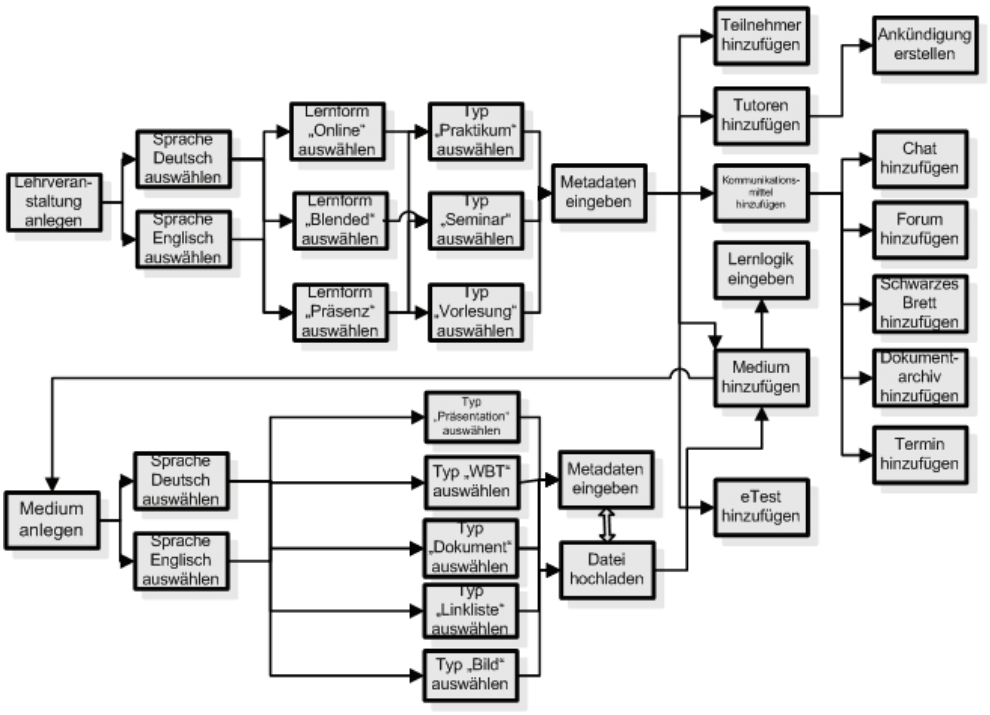


Abb. 21: Anlegen einer Lehrveranstaltung in CLIX

Für die Verkürzung und flexiblere Gestaltung der Abläufe wurde für die Dozenten an der TUM eine vereinfachte Version der Funktionalitäten in CLIX - „Clix Lite“ - bereitgestellt. „Clix Lite“ basiert auf einem Template, das Dozenten eine Lehrveranstaltung mit vordefiniertem Dokumentenarchiv zum Material-Upload sowie ein Forum anbietet und so die Erstellung und Verwaltung der Lehrveranstaltung in CLIX erleichtert. Dennoch stellte sich heraus, dass die flexible Gestaltung von Lehrszenarien in CLIX wie in anderen gängigen Learning Management Systemen stark eingeschränkt bleibt. Aus diesem Grund wurde nach einer anderen Lösung gesucht, Dozenten das Erstellen von flexiblen Kursen innerhalb eines LMS zu ermöglichen.

Im Folgenden wird eine Lösung für ein modular aufgebautes und individuell flexibel zu gestaltendes LMS auf Basis des Portalserver Microsoft Office Sharepoint Server 2007 (MOSS 2007) vorgestellt. Sharepoint wurde in den vergangenen Jahren erfolgreich in Unternehmen eingesetzt, um Mitarbeitern Zugang zu unternehmensspezifischen Informationen und Applikationen zu gewähren [Weis03]. Die neue Generation des Sharepoint Servers bietet ein verbessertes Wissensmanagement und Teamarbeitslösungen an, die durch Integration der neuen Microsoft Office Produkte ergänzt werden [Laah05]. Der Sharepoint Server 2007 wurde grundsätzlich nicht als eLearning Portal entwickelt, kann aber auf Grund seiner hohen Anpassungsfähigkeit an die Bedürfnisse der Benutzer als solches eingesetzt werden.

Ausschlaggebend für die Wahl des MOSS 2007 als Grundlage für ein flexibel konfigurierbares Portal war das Konzept der WebParts. WebParts sind kleine Programme, mit denen Benutzer relevante Informationen zusammenstellen und beliebig auf Webseiten anordnen können, ohne diese neu programmieren zu müssen. Durch das beliebige Hinzunehmen, Entfernen und Anordnen von WebParts durch Drag&Drop auf einer Webseite wird Benutzern die Möglichkeit geboten, ihre Seiten selbst zu organisieren und zu gestalten. WebParts sind ASP.NET-Steuerelemente und können auf .NET-Basis programmiert und in die Sharepoint-Umgebung eingebunden werden. Dies ermöglicht die beliebige Erweiterung und Anpassung des Sharepoint Servers an die Bedürfnisse verschiedener Dozenten bzw. Hochschulen.

Für den Aufbau des Portals wurden die Windows Sharepoint Services 3.0 (WSS 3.0) und der Microsoft Office Sharepoint Server 2007 installiert. Die WSS 3.0 sind ein kostenloser Zusatz des Windows Servers 2003 und dienen dazu, Webseiten zu erzeugen und diese für viele Benutzer aufrufbar zu machen. Sie unterstützen gängige Kollaborationsfunktionalitäten wie Dokumentenbibliotheken, Kalender, Kontaktlisten, etc…Clientseitig lassen sich mehrere Browser und verschiedene Betriebssystemen einsetzen.

Da MOSS 2007 als Portalserver keine reinen eLearning-Funktionalitäten bietet, wurde eine „eLearning-Schicht“ entwickelt, die über die normalen Portalfunktionen gelegt wurde. Ein LMS sollte nach Baumgartner, Häfele und Häfele (2002) [Baum02] nicht nur die Präsentation von Inhalten und die Bereitstellung von synchronen und asynchronen Kommunikationsmitteln, sondern auch Werkzeuge zur Erstellung von Aufgaben und Übungen, sowie Evaluations- und Bewertungshilfen zur Verfügung stellen. Zur Realisierung der eLearning-Schicht in Sharepoint wurden die in CLIX identifizierten Abläufe stark vereinfacht und alle wichtigen eLearning-Komponenten mit existierenden WebParts und dem Sharepoint Learning Kit umgesetzt. Weitere eLearning-spezifische WebParts, wie z.B. ein Modul zur Durchführung elektronischer Tests, werden momentan in einer Diplomarbeit an der TUM, aber auch an anderen Universitäten, von Microsoft sowie der Herstellerfirma von CLIX, der imc AG, entwickelt. Um den Einstieg in die Technik des Portalservers zu erleichtern, wurde eine Vorlage erstellt, die Dozenten bei dem Anlegen einer neuen Lehrveranstaltung zur Verwendung angeboten wird. Standardmäßig werden so in eine neu erzeugten Kursseite einfache eLearning-Komponenten wie Ankündigungen, Lehrmaterial, Diskussions-Forum, Bild des Dozenten, Wiki und Hyperlinks aufgenommen. Die Hinzunahme weiterer Komponenten wie Evaluation, Lernlogik, Folienbibliotheken, Online-Status, Blog, Kalender steht dem Dozenten frei. Auf diese Weise wird ein einfacher Einstieg in die Lernplattform und gleichzeitig eine flexible Anpassbarkeit und Erweiterbarkeit der Seite erzielt. Eine beispielhafte Kursseite im Sharepoint Portal der FH München ist in Abb. 3 dargestellt.

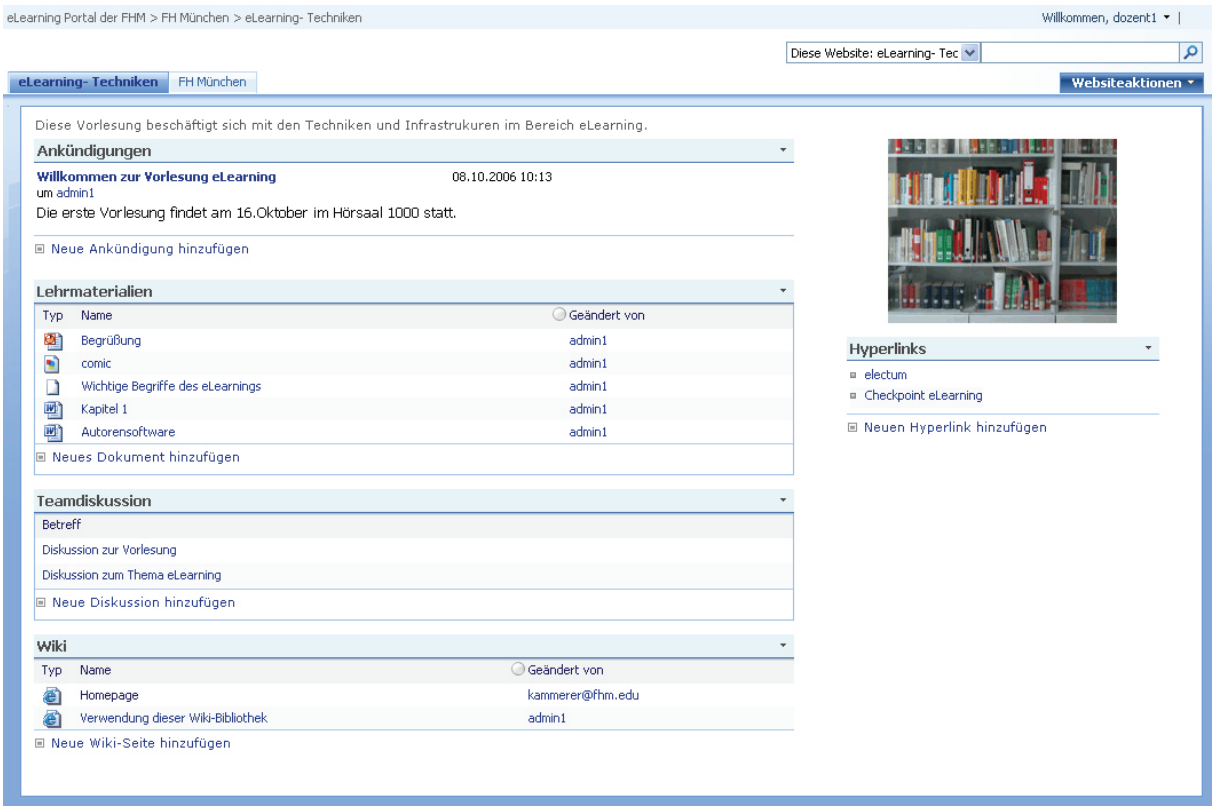


Abb. 3: Beispielhafte Kursseite der FH München

Abb. 4 zeigt das Prinzip des Anlegens einer Lehrveranstaltung in Sharepoint und stellt die starke Verkürzung der Abläufe in CLIX heraus. Alle im Kreis dargestellten Komponenten können vom Dozenten beliebig hinzugefügt oder entfernt werden.

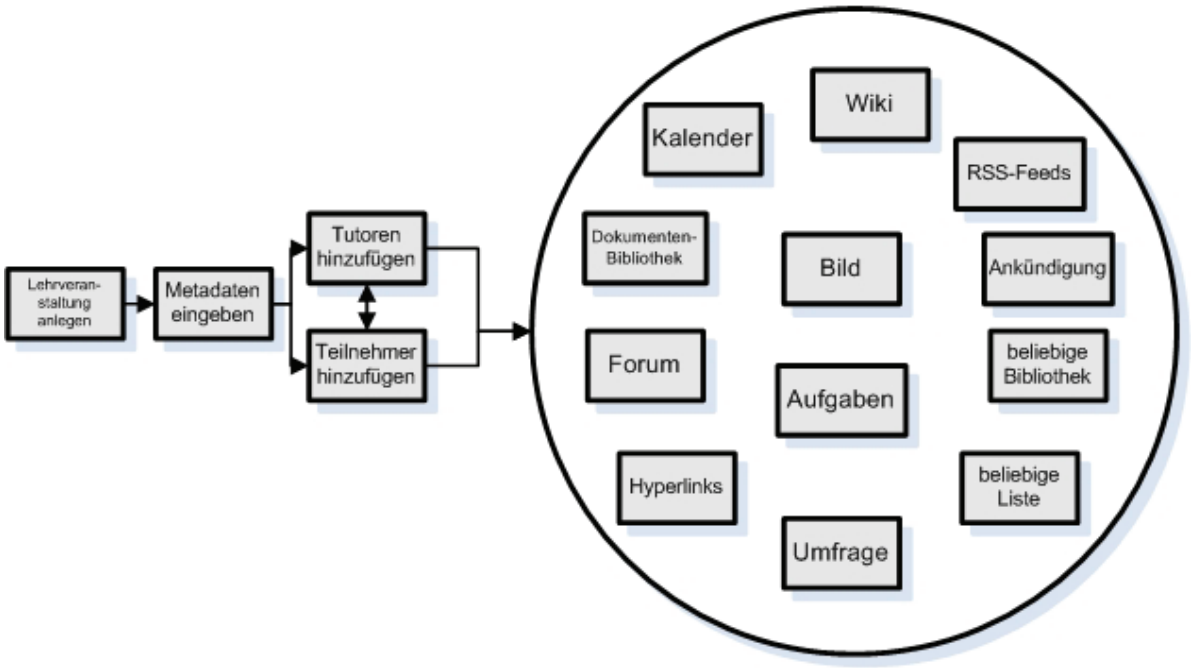


Abb. 4: Anlegen einer Lehrveranstaltung in Sharepoint

Durch den großen Vorteil der individuellen Anpassbarkeit bot sich das Sharepoint-Portal auch als Grundlage für die Konzeption eines hochschulübergreifenden LMSs (ZePeLin Bayern) an. Als Einstiegspunkt dieses Portals wurde in Sharepoint eine zentrale Website (http://www.zepelin.org) erstellt, die eine Übersicht über alle beteiligten Hochschulen ermöglicht und Neuigkeiten zum Projekt enthält. Die Einstiegsseiten der Partnerhochschulen stellen hochschulinterne, eLearning-relevante Informationen für Mitarbeiter, Dozenten und Studenten bereit (s. Abb. 5). Ein Überblick über alle angelegten eLearning-Kurse und der Zugang zu diesen werden ebenfalls auf diesen Seiten gegeben. Die Trennung der Inhalte der verschiedenen Hochschulen wird durch so genannte Sharepoint-Webapplikationen, mit WSS-Funktionalitäten erweiterte IIS-Websites, realisiert, da alle Inhalte einer Webapplikation in einer eigenen Content-Datenbank gespeichert werden. Das von ASP.NET 2.0 übernommene, neue Konzept der Seiten-Vorlage (Master Pages) gewährleistet ein einheitliches Design für alle zusammengehörenden Seiten einer Anwendung bzw. Hochschule.

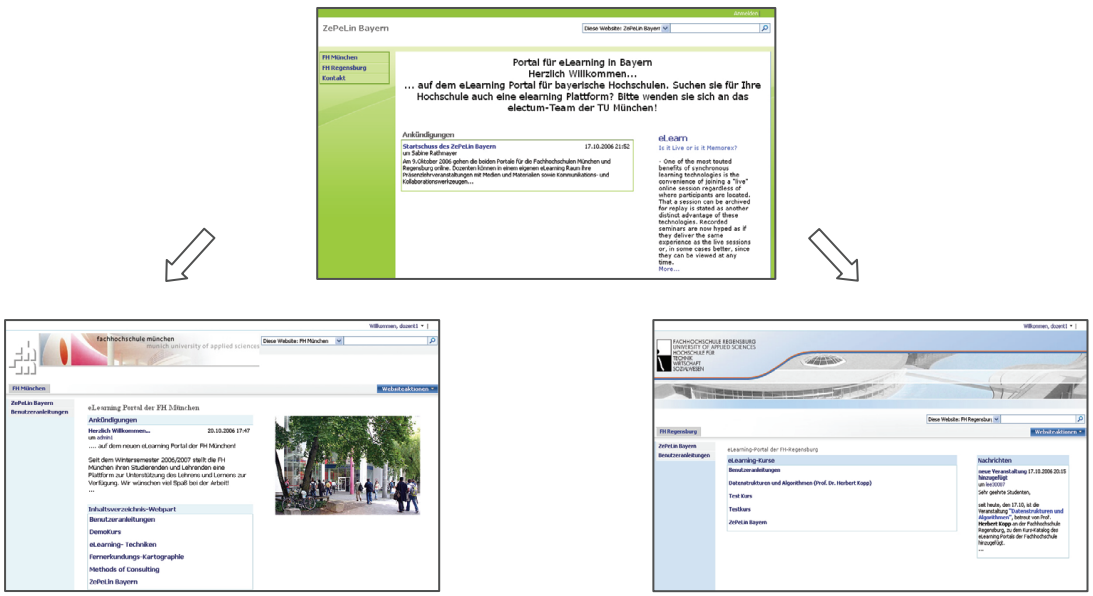


Abb. 5: Das ZePeLin Portal und Einstiegsseiten der Fachhochschulen München und Regensburg

Über die Unterstützung von eigenständigen Räumen hinaus lässt sich ZePeLin Bayern durch die Zusammenführung von Daten aus unterschiedlichen Quellen und Anwendungen unter einer einheitlichen Weboberfläche als eine Integrationsplattform einsetzen. Daher können

organisatorisch und technisch anspruchsvolle Verfahren wie die gemeinsamen Studiengänge der LMU und der TUM sowie die bayernweiten Kurse der vhb abgewickelt werden.
Bereits existierende Inhalte lassen sich in Form von SCORM-standardisierten WBTs mit Hilfe des MS Learning Kit Webparts importieren oder aus der Plattform heraus verlinken. Ergebnis einiger Förderprojekte sind jedoch Kursmodule, die in einem gängigen LMS angeboten werden. Auf solche Kurse ist eine einheitliche und integrierte Sicht zu bieten, in dem Anbindungen zur Weitergabe von Autorisierungsinformationen zwischen Sharepoint und anderen Systemen geschaffen werden. Entsprechende WebParts wurden bereits für CLIX, Blackboard, WebCT und Aspen implementiert, eine Version für Moodle wird aktuell entwickelt. Die Authentifizierung und Autorisierung auf der Plattform werden durch die Realisierung einer erweiterbaren Benutzerverwaltung, welche Gegenstand des nächsten Abschnitts ist, geregelt.

4 Identity Management

Ein zentraler Aspekt des Portals ist die Realisierung einer zukunftsorientierten, flexiblen, erweiterbaren und sicheren Benutzerverwaltung. Zu diesem Zweck werden die möglichen Profildatenquellen der beteiligten Einrichtungen und die im MOSS 2007 vorhandenen Mechanismen einander gegenüber gestellt.
In den meisten Fällen werden an Hochschulen unterschiedliche Systeme für die Studierenden-, Personal-, Gäste- und Alumniverwaltung eingesetzt. Zum einen befinden sich diese in der Regel auf Grund der Datensensibilität in geschlossenen Netzen. Zum anderen verfügen sie oft nur über schwer handhabbare Schnittstellen. Zur Schaffung einer modernen integrierten IT-Infrastruktur wird jedoch eine ganzheitliche Sicht auf personenbezogenen Daten benötigt. Daher wird heutzutage ein zentrales Identity Management bevorzugt, das durch die Verwaltungssysteme gespeist wird. So wie an der TUM und an den beiden Fachhochschulen München und Regensburg werden dabei meistens Verzeichnisdienste eingesetzt, die sich durch einen schnellen Lesezugriff auszeichnen und standardisierte Schnittstellen über LDAP anbieten. Die gespeicherten Informationen erstrecken sich von Profilstammdaten über Einrichtungen und Gruppen, bis hin zu Anmeldedaten zur Authentifizierung und ggf. Autorisierungsangaben hinsichtlich der Berechtigungen an anderen Systemen.
Da die eLearning-Dienste auf dem Portal gezielt Hochschulangehörigen anzubieten sind, lässt sich keine Selbstregistrierung durch den Benutzer und ein anonymer Zugriff nur für öffentliche

Bereiche einsetzen. Eine mögliche Selbstregistrierung mit Identitätsprüfung bei der entsprechenden Einrichtung bringt eine hohe Komplexität bei geringer Benutzerfreundlichkeit mit sich. Vielmehr bietet sich in ZePelin Bayern eine Benutzerverwaltung an, welche auf dem bereits vorhandenen Identity Management der Hochschulen aufbaut. Zu einer solchen Umsetzung stellt MOSS 2007 grundsätzlich drei Verfahren zur Verfügung:

- Provisionierte zentrale Benutzerverwaltung: Personenstammdaten werden inkrementell und taktgesteuert importiert. Die Authentifizierung kann gegen das lokale Active Directory oder ein entferntes Verzeichnis durchgeführt werden. Zwei schwerwiegende Nachteile dieses Verfahrens stellen die Datenredundanz durch die Pflege von shadow accounts und die Datenschutz dar.
- Integrierte dezentrale Benutzerverwaltung. Mit ASP.NET 2.0 liefert Microsoft eine anpassbare Standardimplementierung für ein Mitgliedschaftssystem mit Grundfunktionen wie Anmeldung oder Benutzerlisten. Das Mitgliedschaftssystem dient der Benutzerverwaltung in unterschiedlichen Datenspeichern. ASP.NET 2.0 enthält Connectoren (Provider) zu einer lokalen MSSQL-Datenbank und Active Directory Domäne (s. Abb. 6). MOSS 2007 beinhaltet des Weiteren einen Provider zu LDAP-Verzeichnisdiensten beliebiger Hersteller, der jedoch bestimmte Anforderungen an die Strukturierung der Quellsysteme, z.B. explizite LDAP-Gruppen, auferlegt. Wesentlich ist jedoch vor allem die Möglichkeit zur Implementierung eines eigenen Providers, denn dadurch können beliebige Datenquellen angeschlossen werden. Eine solche Anbindung erfolgt dynamisch zur Laufzeit ohne eine lokale Datenspeicherung. Zur Authentifizierung gegen die Datenquelle wird ein bestimmtes Web-Formular mit einem HTML-basierten Anmeldedialog verwendet. In Verbindung mit einer verschlüsselten Übertragung kritischer Angaben wie Passwörter ist diese Variante datenschutzrechtlich unbedenklich.

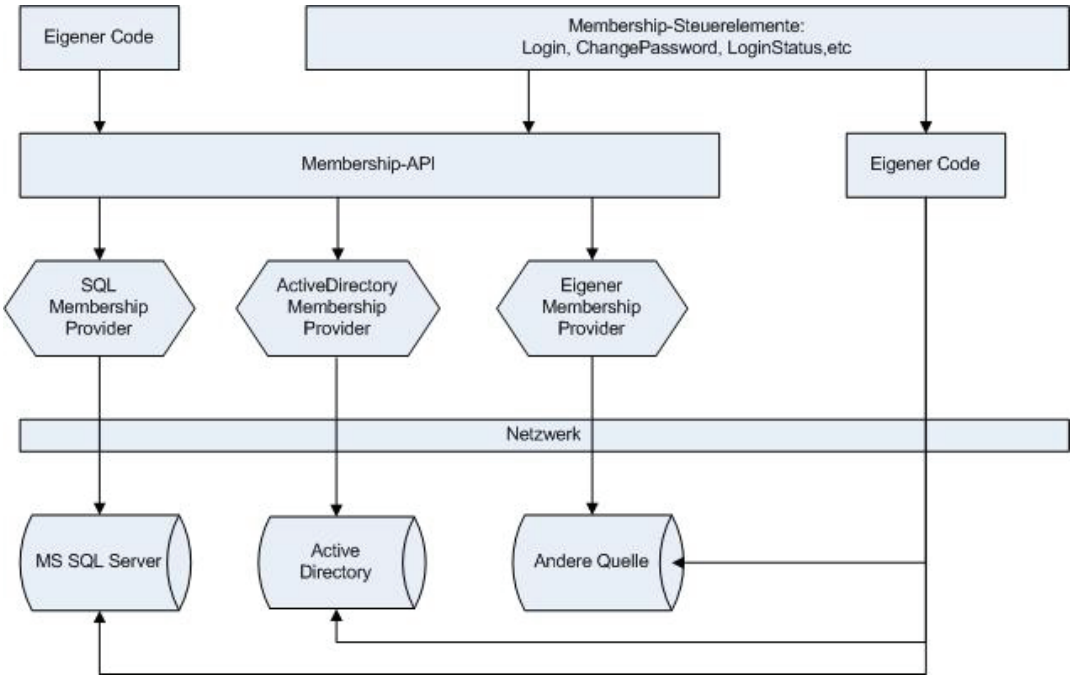


Abb. 6: Architektur des Mitgliedschaftssystems [Schw05]

- Identitätsföderation. Beim Vorhandensein einer hochschulübergreifenden Authentifizierungs- und Autorisierungsinfrastruktur (AAI) lässt sich die zweite Alternative zu einem föderativen Ansatz im Sinne eines Single-Sign On (SSO) ausbauen.

Zur Umsetzung im Portal wurde das Verfahren der integrierten dezentralen Benutzerverwaltung auf Grund der deutlichen Vorteile gegenüber dem Stammdatenimport und der noch fehlenden AAI-Infrastruktur ausgewählt. Dabei wurde ein eigenes Mitgliedschaftssystem realisiert, weil das Identity Management der TUM und der Partnerhochschulen z.Z. keine fest definierten Domänengruppen bereitstellt. Der umgesetzte Connector zeichnet sich durch die Anpassbarkeit an spezifische Anforderungen und Strukturen aus. Insbesondere werden dabei hochschulübergreifende Szenarien wie doppelte Studiengänge und die Abwicklung von Kursen der vhb mittels des gleichzeitigen Andockens mehrerer Benutzerdatenquellen ermöglicht.
Die wesentlichen Bestandteile des Mitgliedschaftssystems stellen ein Profil- und ein Rollen-Connector dar. Der Profil-Connector regelt die Authentifizierung gegen das LDAP-Verzeichnis der jeweiligen Bildungseinrichtung und den Zugriff auf Benutzerprofile und Suchlisten mit Wildcards (s. Abb. 7) nach verschiedenen Kriterien durch die Implementierung der abstrakten Klasse `System.Web.Security.MembershipProvider` aus dem ASP.NET-Framework. Von den Stammdaten werden die Kennung, ein eindeutiger fester Schlüssel und die E-Mail-Adresse

ausgelesen. Der Schlüssel dient der Zuordnung der Identität zu Inhalten auf dem Portal und wird als einziges Attribut bei Bedarf lokal gespeichert. Wichtige Attribute wie Name und Vorname können durch den Anwender im eigenen Profil auf dem Portal eingegeben werden.

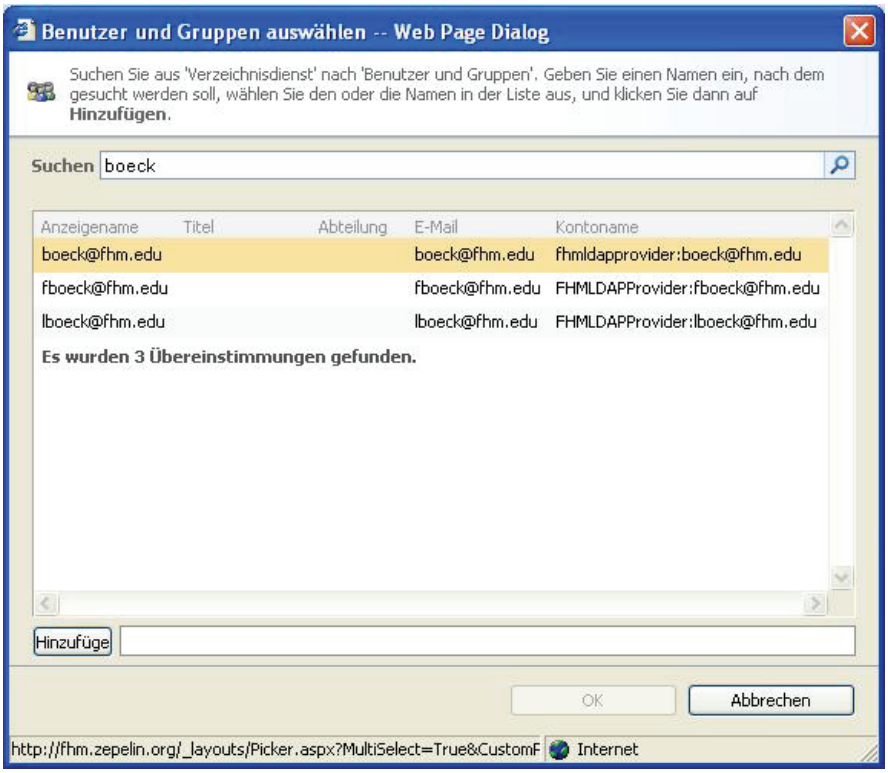


Abb.7: Mitgliedersuche in MOSS 2007

Die wichtigsten Methoden des Profil-Connectors werden im Folgenden vorgestellt:

```
// die Methode wird bei der formularbasierten Authentifizierung aufgerufen
Public Boolean ValidateUser (String username, String password)

// WSS nutzt diese Methoden bei der Suche von Benutzern
Public MembershipUserCollection FindUsersByEmail(String emailToMatch)
Public MembershipUserCollection FindUsersByName (String usernameToMatch)

// WSS ruft die Methoden bei der Auflösung von Benutzernamen auf
Public MembershipUser GetUser (Object providerUserKey)
Public MembershipUser GetUser (String username)

// WSS nutzt die Methode in Szenarien mit Benutzereinladungen
Public String GetUserNameByEmail (String email)
```

Der Rollen-Connector implementiert die Klasse `System.Web.Security.RoleProvider` und stellt die Grundlage für das Berechtigungskonzept des jeweiligen eLearning-Portals, z.B. die

Domänengruppen der Hochschulangehörigen, aller Studenten und Mitarbeiter sowie der Fachbereichsangehörigen, bereit. Die gewünschte Granularität dieser Gruppen hängt dabei hauptsächlich von der Qualität der Daten im entsprechenden Verzeichnis ab. Zur Generierung der Gruppen werden die Verzeichnisstruktur sowie Profilattribute herangezogen. Folgende Methoden sind für MOSS 2007 relevant:

```
// WSS prüft dadurch die Existenz einer Domänengruppe
Public Boolean RoleExists (String roleName)

// liefert alle Domänengruppen eines Benutzers
Public String() getRolesForUser (String username)

// liefert alle Domänengruppen
Public String() GetAllRoles ()
```

Die Datenübertragung erfolgt im Falle der FH Regensburg über einen verschlüsselten SSL-Kanal und mit der FH München über TLS. Die SSL-Kodierung beeinträchtigt unmittelbar die Performance des Connectors. So beansprucht ein SSL-Bind über 500 ms gegenüber rund 200 ms sonst. Da keine Authentifizierungs- und Profildaten lokal gespeichert werden, hängt der reibungslose Betrieb des Portals von der Verfügbarkeit der Verzeichnisse ab. Eine entsprechende Skalierung über drei Rechner wurde mit der FH Regensburg bereits umgesetzt.

5 Ausblick

Parallel zu den vom Bund - bzw. nach der Föderalismus Reform durch die Länder - geförderten eLearning Projekten stehen nahezu alle deutschen Hochschulen vor der Aufgabe, effiziente und wettbewerbsfähige Infrastrukturen zu schaffen. Vor allem die noch weiter steigenden Studierendenzahlen durch u.a. die doppelten Jahrgänge ab dem Jahr 2011 sowie die Umsetzung von eBologna verstärken diese Notwendigkeit. Somit kommt eLearning eine immer wesentlichere Rolle zu.

Aufbauend auf den fachlichen und technischen Lösungen des elecTUM Projekts leistet ZepeLin Bayern einen wichtigen Beitrag dazu, in dem es interessierten Hochschulen eine moderne integrierte Lernumgebung bei gleichzeitiger Kosteneffizienz zur Verfügung stellt, die sich durch Sicherheit, Skalierbarkeit, Flexibilität und Erweiterbarkeit auszeichnet.

Darüber hinaus bietet ZePeLin weitere Perspektiven: Durch die Integration verschiedener Produkte wird hochschulübergreifend einen zentralen Zugriffspunkt für eine Vielfalt von Diensten ermöglicht. Diese erstrecken sich von der bayernweiten Unterstützung virtueller Communities für Forschung und Lehre über die Veröffentlichung von Arbeitspapieren und Skillmanagement bis hin zu zukunftsorientierten Online-Angeboten wie „Windows Life“ und „Office Live“. Kontinuierlich wird das Portal um weitere Zielgruppen und Funktionalitäten für vernetztes Lernen und kooperatives Wissensmanagement unter Berücksichtigung der deutschlandweiten Initiativen im Bereich „Bildung und Web 2.0“ ausgebaut.

Literaturverzeichnis

[Baum02] Baumgartner, P.; Häfele, C. und Häfele, H.: e-Learning. In: CD-Austria, Sonderheft des bm:bwk; 2002

[Bmbf04] BMBF: Richtlinien über die Förderung der Entwicklung und Erprobung von Maßnahmen der Strukturentwicklung zur Etablierung von eLearning in der Hochschullehre im Rahmen des Förderschwerpunkts „Neue Medien in der Bildung“, 2004

[Bör04] Bör, A.; Borgeest, R.; Rathmayer, S.; Stross, M.: elecTUM – Integriertes eLearning an der Technischen Universität München. In (Engels, G.; Seehusen, S. Hrsg.): DeLFI 2004: Die 2. eLearning Fachtagung Informatik. Köllen Druck & Verlag GmbH, Bonn, 2004; S. 365-366.

[Gerg06] Gergintchev, I.; Graf, S.; Pongratz, H.; Rathmayer, S.: Integration von eLearning in die IuK Infrastruktur deutscher Hochschulen: Standardisierter Datenaustausch und Schnittstellen. In: Proceedings der 4. e-Learning Fachtagung Informatik der Gesellschaft für Informatik (DeLFI 2006), Darmstadt, Deutschland

[Juli06] Juling, W.; Hartenstein, H.; Maurer, A.: Karlsuher Integriertes Informations-Management KIM, DINI, September 2006

[Laah06] Laahs, K.; Mc Kenna E.; Vanamo V.: Microsoft Sharepoint-Technologien. In: Addison- Wesley; 2006.

[Müll06] Müller, A.; Lämmle, S.; Leimer, S.; Rathmayer, S.: Qualifying Lecturers: The eTeaching Qualification Matrix. In: Konferenzband M3 - Interdisciplinary Aspects on Digital Media & Education; 2006.

[Weis03] Weisbrod, M.; Ganser, R.: Microsoft Office Sharepoint Portalserver 2003; Das Handbuch. In: Microsoft Press. Deutschland; 2003.

[Schu01] Schulmeister, R.: Szenarien netzbasierten Lernens. In: Wagner, E.; Kindt, M., eds. Virtueller Campus, Szenarien - Strategien - Studium. Münster, New York, München, Berlin: Waxmann; 2001. S. 16-38.

[Schw05] Schwichtenberg, H.: Microsoft ASP.NET 2.0 mit Visual C#. In: Microsoft Press Deutschland; 2005.

Universität Karlsruhe (TH)
& TU München

Stellt integriertes Informationsmanagement an einer Hochschule zukünftig die zentrale Schlüsselfunktion dar? Die Chancen durch integriertes Informationsmanagement (IIM) und der damit verbundene Paradigmenwechsel hin zur dienstleistungsorientierten Hochschule sind in vielerlei Hinsicht bestechend. Sie versprechen insbesondere eine Steigerung der Effektivität, Effizienz und Qualität bei der Umsetzung der Ziele einer Hochschule im globalisierten Wissensmarkt.

Dieser Band enthält die Ergebnisse des ersten Workshops zum Integrierten Informationsmanagement an Hochschulen 2007 in Karlsruhe und beleuchtet in seinen Beiträgen verschiedene Aspekte der Organisation, des Identity Managements und Integration von eLearning in die Hochschullandschaft.

ISBN: 978-3-86644-112-5

www.uvka.de