Hochschulübergreifend integriertes Identitäts-Management am Beispiel des Münchner Wissenschaftsnetzes

Latifa Boursas, Silvia Knittl, Daniel Pluta
Technische Universität München
Ralf Ebner, Wolfgang Hommel
Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
E-Mail: boursas,knittl,pluta@tum.de; ebner,hommel@lrz.de

Abstract: Die prozessorientierte IT-Unterstützung für hochschulübergreifende Studiengänge, den Bolognaprozess und reisende Wissenschaftler stellt Anforderungen, die ohne eine reibungslos funktionierende und im Massenbetrieb gut skalierende Identitäts-Management-Infrastruktur nicht erfüllt werden können. In diesem Beitrag zeigen wir anhand des Münchner Wissenschaftsnetzes, wie verschiedene Ansätze für hochschulinternes und -übergreifendes Identitäts-Management gewinnbringend miteinander kombiniert werden können: Die Verzeichnisdienste der beiden Münchner Universitäten und des Leibniz-Rechenzentrums werden miteinander verknüpft und bilden die Grundlage für die Shibboleth-basierte Nutzung deutschland- und europaweiter IT-Dienste anderer Hochschuleinrichtungen sowie ein campusweites Single Sign-On.

1 Hochschulübergreifende IT-Dienste als Herausforderung für Verwaltung und Rechenzentren

Spätestens seit WLAN-fähige Notebooks zum Alltagsgegenstand geworden sind, möchte kaum ein Hochschulangehöriger darauf verzichten. Auch beispielsweise beim Besuch an anderen Hochschulen im Rahmen einer Fachtagung soll der Zugriff auf E-Mails, Online-Bibliotheksressourcen und viele andere Dienste der Heimathochschule möglich sein. Der hohe Bedarf spiegelt sich in der Geschwindigkeit und dem Abdeckungsgrad wider, mit dem sich Dienste wie das DFN-Roaming[1] und eduRoam[2] durchgesetzt haben.

Die WLAN-Nutzung ist an den meisten Einrichtungen einer der wenigen Dienste, die sich mit Benutzername- und Passwortüberprüfung begnügen. Viele andere Dienste, etwa das E-Learning, benötigen jedoch zur Personalisierung und fein granulierten Autorisierung zusätzliche Informationen über ihre Benutzer. Hierbei sind Qualität und Zuverlässigkeit der Benutzerdaten essentiell, deshalb sollen sie aus geeigneter, zuverlässiger Benutzerdatenbasis entnommen werden. Eine Selbstregistrierung durch den Benutzer wird deshalb bei Hochschuldiensten, abgesehen von Online-Bewerbungen, immer seltener gewünscht, um Missbrauch durch Identitätsdiebstahl oder Eintragung fiktiver Personen vorzubeugen.

Hochschulintern kann dieser gesteigerte Bedarf an benutzerspezifischen Daten erfolgreich

[1] `http://www.dfn.de/index.php?id=43036`
[2] `http://www.eduroam.org/`

durch Identitäts-Management-Systeme (IMS) abgedeckt werden: Sie entnehmen Verwaltungssystemen relevante Teile der Personendatensätze, reichern diese um Informationen wie Benutzerkennung und Passwort an, und verteilen die resultierenden digitalen Identitäten wiederum selektiv an die IT-Systeme der Hochschule. Die Kanalisierung über ein zentrales IMS stellt dabei sicher, dass alle IT-Dienste auf demselben, konsistenten Datenbestand operieren, und bietet aus Benutzerperspektive u. a. den Mehrwert eines einheitlichen Passworts für alle Hochschuldienste [Gie04].

Mit dem Aufkommen hochschulübergreifend angebotener Studiengänge, dem Bologna-Ziel des mobilen Studenten, verteilten Ressourcen wie den DFG-Nationallizenzen, virtuellen Hochschulen, Grid-Projekten und Download-Portalen für lizenzierte Software namhafter Hersteller ergibt sich jedoch der dringende Bedarf, elektronische Benutzerprofile unter Berücksichtigung des Datenschutzes auch IT-Dienstleistern außerhalb der eigenen Hochschule zugänglich zu machen. Neben der Technik zum Austausch von Benutzerprofilen spielt die Datenqualität eine zentrale Rolle, um zu vermeiden, dass beispielsweise ausgeschiedene Studenten noch Zugriff auf extern erbrachte Dienste haben.

In diesem Beitrag präsentieren wir den im Münchner Wissenschaftsnetz (MWN) erarbeiteten und weitgehend implementierten Lösungsansatz für diese Herausforderungen: Die Münchner Universitäten haben innerhalb von CampusLMU bzw. des DFG-geförderten Projekts IntegraTUM zentrale Verzeichnisdienste aufgebaut; in Abschnitt 2 stellen wir vor, wie diese nun über das IMS des Leibniz-Rechenzentrums (LRZ), das der gemeinsame IT-Dienstleister der Münchner Hochschuleinrichtungen ist, selektiv miteinander gekoppelt werden sollen. Dadurch wird eine MWN-weit einheitliche Dienstnutzung für Studenten gemeinsamer Studiengänge wie Medizin und Bioinformatik möglich. Das LRZ betreibt auch für beide Universitäten die technischen Komponenten zur Teilnahme an der Authentifizierungs- und Autorisierungsinfrastruktur des DFN-Vereins (DFN-AAI), die als Basis für die hochschulübergreifende Dienstnutzung fungiert; unsere Anwendungsfälle und Beiträge zur Weiterentwicklung werden in Abschnitt 3 diskutiert. Um die Synergien durch hochschulinterne und -übergreifende Technologien zu nutzen, hat die Hochschulleitung der Technischen Universität München (TUM) beschlossen, die DFN-AAI-Softwarebasis Shibboleth auch als TUM-internes Single Sign-On System zu nutzen; die resultierende Steigerung der Integration und Benutzerfreundlichkeit der IT-Systeme der TUM und die Eckpunkte unserer in Arbeit befindlichen Realisierung stellen wir in Abschnitt 4 vor.

2 Kopplung der Hochschul-Identitäts-Management-Systeme

Die Rolle von IMSen als Schlüsseltechnologie zur Integration von IT-Diensten wurde an den Münchner Hochschulen früh erkannt und gefördert: Der Aufbau und die breite Nutzung hochschulweiter Verzeichnisdienste bilden an beiden Universitäten in München das technische Rückgrat der zentralen IT-Dienste [BH06]. Wie Abbildung 1 zeigt, aggregieren beide Universitäten Benutzerdaten aus den Verwaltungssystemen in einem Verzeichnisdienst. Der zentrale Datenbestand wird gezielt den hochschulweiten Diensten zur Verfügung gestellt. Am LRZ wird ein dediziertes IMS betrieben, das auf einem zentralen

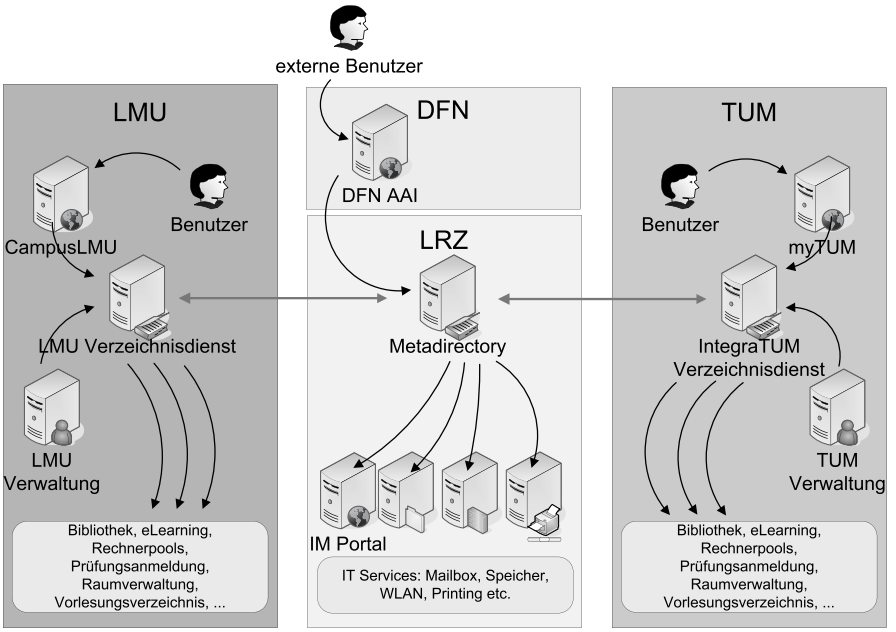

Abbildung 1: Angestrebte hochschulübergreifende Kopplung der Identitäts-Management-Systeme

Meta-Directory basiert und es uns ermöglicht, auch die Benutzer der weiteren Münchner Hochschulen sowie die deutschland- und europaweiten Benutzer des Höchstleistungsrechner und die Teilnehmer an den verschiedenen Grid-Projekten effizient zu verwalten.

Während früher eine Mehrfacherfassung von Benutzern sowohl an der jeweiligen Hochschule als auch am LRZ erforderlich war, arbeiten wir nun verstärkt an einer einrichtungsübergreifenden Kopplung der IMSe. Leider eignen sich Föderationsansätze wie Shibboleth (vgl. Abschnitt 3) nur für web-basierte Anwendungen und somit nicht für herkömmliche Dienste mit dedizierten Protokollen wie beispielsweise File-Server und die eingesetzte Groupware. Da an LMU, TUM und LRZ auf Basis dasselbe IMS-Produkt verwendet wird, lassen sich jedoch mit relativ geringem Aufwand IMS-Konnektoren entwickeln, die die benötigten Daten über Hochschulangehörige an das LRZ übermitteln. Die resultierende Kopplung an einen Meta-Verzeichnisdienst werden in [HKP08] betrachtet.

So können sich etwa LMU-Studenten über das LMU-Webportal ihren E-Mail-Account freischalten; hierbei wird auch die Synchronisation ausgewählter Daten mit dem LRZ angestoßen. Innerhalb weniger Sekunden wird dadurch ein neues Benutzerkonto im LRZ-Datenbestand eingerichtet und für den E-Mail-Dienst konfiguriert. Dieses Verfahren bewirkt einige Mehrwerte; so können etwa Selbstbedienfunktionen zum Ändern von Weiterleitungsadressen in das jeweilige Hochschulportal integriert werden, so dass den Anwendern eine einheitliche Bedienoberfläche und Supportinfrastruktur zur Verfügung steht.

Da sich diese Kopplung der IMSe bewährt hat, planen wir nun eine Erweiterung, so dass

auch ganze Studentendatensätze zwischen LMU und TUM ausgetauscht werden können. Die Motivation hierfür liefern die von LMU und TUM gemeinsam angebotenen Studiengänge, deren Studenten im Laufe ihres Curriculums an Veranstaltungen und Prüfungen an beiden Universitäten teilnehmen. Durch den IMS-basierten Datenaustausch sollen der Aufwand zur Erfassung und Pflege der Daten reduziert und in der Praxis damit bislang unvermeidlich verbundene Probleme wie Dateninkonsistenzen gelöst werden. Die datenschutzrechtlich relevanten Aspekte in diesem Umfeld werden in [BH06] behandelt.

3 Föderationen als Basis für die internationale Dienstnutzung

Die vom DFN-Verein koordinierte deutschlandweite Shibboleth-Föderation DFN-AAI ermöglicht ein organisationsübergreifendes Single Sign-On (SSO) sowie den Transfer von Benutzerprofilen auch an außerhalb der eigenen Hochschuleinrichtung betriebene Web-Anwendungen. Diese Technik wurde bereits von wissenschaftlichen Verlagen zum Zugang zu elektronischen Dokumenten, Softwareherstellern zum partiell kostenlosen Download lizenzierter Software sowie regionalen bzw. fachspezifischen E-Learning-Anbietern aufgegriffen und wird von Münchner Hochschulangehörigen bereits aktiv genutzt.

Die zur Nutzung externer Dienste notwendige Software, der so genannte „Shibboleth Identity Provider“, wird für die Münchner Universitäten vom LRZ betrieben; sie greift im Hintergrund auf die Datenbestände von CampusLMU bzw. IntegraTUM zu. Seitens LMU und TUM sind somit keine zusätzlichen technischen Maßnahmen erforderlich; die Nutzung einiger der externen Dienste setzt jedoch bilaterale Verträge zwischen dem Anbieter und der Heimathochschule der Nutzer voraus, die unabhängig vom LRZ geschlossen werden und typischerweise Datenschutzvereinbarungen enthalten, die wiederum auf die Shibboleth-Konfiguration abgebildet werden müssen.

Bei der Möglichkeit, auch eigene webbasierte IT-Dienste zur Nutzung durch Angehörige anderer Hochschulen freizugeben, hat an den Münchner Universitäten das E-Learning eine Vorreiterrolle: Die LMU-Kontaktstelle für Forschungs- und Technologietransfer und das BMBF-geförderte E-Learning-Projekt elecTUM arbeiten gemeinsam mit dem LRZ an einer raschen Umsetzung des Föderationsansatzes, der auch die strategische Basis für Angebote im Rahmen der virtuellen Hochschule Bayern (vhb) darstellt.

Durch den Einsatz von Shibboleth kann dabei nicht nur der Benutzerkomfort gesteigert werden, da dank SSO ein zusätzliches Passwort pro Hochschule bzw. Learning Management System (LMS) entfallen kann; vielmehr wird auch der administrative Aufwand zum Einspielen der Studentendatensätze in das jeweilige LMS und bei Supportanfragen rund um den Zugang zu den entsprechenden Diensten minimiert.

Um die Möglichkeiten eines LMS zur Personalisierung und im Hinblick auf Leistungsnachweise voll ausschöpfen zu können, sind eine Reihe von Datenfeldern notwendig, die vom ursprünglichen Datenmodell der DFN-AAI nicht abgedeckt wurden – beispielsweise Angaben zur Studienrichtung. Aus diesem Grund beteiligen sich LMU, TUM und LRZ intensiv an den aktuellen DFN-geleiteten Gremien zur Definition domänenspezifischer Schemaergänzungen wie dem DFN-AAI E-Learning-Profil.

Ein wichtiger Schwerpunkt ist dabei die Berücksichtigung der Interoperabilität mit Föderationen aus anderen Ländern wie etwa Finnland und der Schweiz [Kie06], mit denen die gemeinsame Nutzung von LMS bereits bei europäischen Forschungsprojekten wie EUREA pilotiert wurde. Durch einen sukzessiven Ausbau und die zu erwartende Integration der Shibboleth-Funktionalität in Campus Management Systeme wird sich auch die im Bologna-Kontext erwünschte Studentenmobilität gezielt technisch unterstützen lassen.

Shibboleth spielt ferner eine wichtige Rolle für die Arbeit von Wissenschaftlern im Rahmen von Grid-Projekten. Durch Middleware-Erweiterungen wie GridShib[3] werden herkömmliche Grid-Basistechnologien wie das Globus Toolkit um Shibboleth-basierte Autorisierungsmöglichkeiten erweitert, die eine deutlich verbesserte Skalierbarkeit und einen höheren Automatisierungsgrad erzielen sollen. Im Rahmen des D-Grid-Projekts, an dem die Münchner Universitäten und das LRZ beteiligt sind, wird deshalb im Teilprojekt zum integrierten Management virtueller Organisationen (IVOM) konzipiert, wie die Infrastrukturen von D-Grid und DFN-AAI nachhaltig miteinander kombiniert werden können [HS08].

4 Synergien durch hochschulinterne Shibboleth-Nutzung

Die Shibboleth-basierte Öffnung web-basierter Anwendungen für externe Benutzer hat das Interesse an einer SSO-Lösung, die auch hochschulintern genutzt werden kann, verstärkt. Die Hochschulleitung der TUM beschloss deshalb, Shibboleth auch als campusweites SSO-System einzusetzen. Viele Hersteller der im universitären Umfeld eingesetzten webbasierten Software reagieren hier bereits mit der Integration der Shibboleth-Unterstützung in ihre Produkte, was wiederum den Implementierungs-, Konfigurations- und Administrationsaufwand für die Universitäten reduziert.

Herausforderungen stellen jedoch solche Web-Anwendungen dar, die Passworteingaben nicht nur zur Benutzerauthentifizierung, sondern darüber hinaus zur Weitergabe an nachgelagerte Dienste verwenden, wie z.B. der in beiden Hochschulportalen integrierten Webmail-Dienst zur Anmeldung am IMAP-Mail-Server. SSO-Systeme zielen aber genau darauf ab, das Passwort nur noch an einer zentralen Stelle und nicht mehr bei jedem einzelnen Dienst eingegeben zu müssen. Zur Lösung evaluieren wir derzeit verschiedene Ansätze im Zusammenspiel mit Shibboleth inVersion 2.0. Ein aussichtsreicher Ansatz ist dabei die Übertragung von Kerberos-Tickets als Shibbleth-Benutzerattribute, wie sie bereits in mehreren sächsischen Hochschulen im Zusammenspiel mit dem verteilten Dateisystem AFS erfolgreich eingesetzt wird. Im MWN hätte dies den Vorteil, dass ein zentrales, MWN-weit positioniertes Microsoft Active Directory in seiner Rolle als Kerberos Key Distribution Center Desktop- und Web-SSO miteinander kombinieren könnte.

[3] `http://gridshib.globus.org/`

5 Zusammenfassung

IMSe haben sich sowohl auf der Ebene der Hochschulprozesse als auch bei der technischen Integration von IT-Diensten als Schlüsselkomponente erwiesen. In diesem Beitrag haben wir vorgestellt, wie die beiden Münchner Universitäten und das LRZ im Bereich der IMSe sehr eng kooperieren: Wir arbeiten an einer sehr engen Kopplung der geschaffenen Verzeichnisdienste, um eine Mehrfacherfassung sowohl bei gemeinsamen Studiengängen als auch für die Nutzung der LRZ-Dienste zu vermeiden; die Benutzerfreundlichkeit wird dabei durch einheitliche Benutzerkennungen und ein durchgängiges Supportkonzept erhöht. Das LRZ betreibt für die beiden Universitäten darüber hinaus den zur Teilnahme an der DFN-AAI notwendigen Shibboleth Identity Provider, der auch im Bereich des Höchstleitungsrechnen im Rahmen von Grid-Projekten zunehmend an Bedeutung gewinnt. Schließlich haben wir vorgestellt, dass Shibboleth auch TUM-intern als campusweites Single Sign-On zum Einsatz kommt, wobei noch geeignete Strategien für die Anbindung von Legacy-Anwendungen umzusetzen sind.

Danksagung

Die Autoren danken der IntegraTUM-Projektgruppe und dem Munich Network Management (MNM) Team für fruchtbare Diskussionen und Anregungen zu diesem Beitrag. IntegraTUM ist das Projekt der TUM zur Schaffung einer nahtlosen und benutzerfreundlichen IuK-Infrastruktur, das von der DFG unter Vertragsnummer WGI 554 975 gefördert und vom Vizepräsidenten und CIO der TUM, Prof. Dr. Arndt Bode, geleitet wird. Das MNM-Team ist eine Forschungsgruppe mit Mitgliedern an der LMU, der TUM, der Universität der Bundeswehr München und dem Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften unter Leitung von Prof. Dr. Heinz-Gerd Hegering.

Literatur

[BH06] L. Boursas und W. Hommel. Efficient Technical and Organizational Measures for Privacy-aware Campus Identity Management and Service Integration. In *12th International Conference of European University Information Systems (EUNIS 2006)*, Tartu, Estland, Juni 2006.

[Gie04] P. Gietz. Chancen und Risiken LDAP-basierter zentraler Authentifizierungssysteme. In *11. Workshop Sicherheit in vernetzten Systemen*. Marco Thorbrügge, 2004.

[HKP08] W. Hommel, S. Knittl und D. Pluta. Strategy and Tools for Identity Management and its Process Integration in the Munich Scientific Network. In *14th Int. Conference of European University Information Systems (EUNIS 2008)*, Aarhus, Denmark, Juni 2008.

[HS08] W. Hommel und M. Schiffers. Benutzergesteuerter Datenschutz in Grids. In *Erstes DFN-Forum Kommunikationstechnologien - Verteilte Systeme im Wissenschaftsbereich*. GI-Verlag, Mai 2008.

[Kie06] U. Kienholz. Shibboleth-based, Federated Identity Management in Swiss Higher Education. In *EUNIS 2006 Conference Proceedings*, Tartu, University of Tartu, 2006.