2009

HOCHSCHULÜBERGREIFENDES E-LEARNING: TECHNISCHE REALISIERUNG UND DATENSCHUTZ

Stephan Graf
TU München

Wolfgang Hommel
Leibniz-Rechenzentrum

Sabine Rathmayer
TU München

HOCHSCHULÜBERGREIFENDES E-LEARNING: TECHNISCHE REALISIERUNG UND DATENSCHUTZ

Stephan Graf[1], Wolfgang Hommel[2], Sabine Rathmayer[1]

Kurzfassung
Learning Management Systeme (LMSe), die hochschulintern bereits etabliert sind, werden zunehmend aus strategischen und politischen Gründen auch hochschulübergreifend eingesetzt. Für solche Szenarien konnten sich proprietäre Ansätze in der Praxis nicht durchsetzen. Mittlerweile stehen jedoch internationale Standards zur Verfügung, die an nationale Anforderungen angepasst werden können. Im vorliegenden Artikel beschreiben wir die notwendigen Anpassungen an bereits eingesetzte LMSen und die Mehrwerte, die sich durch ein deutschlandweit erarbeitetes einheitliches Datenmodell ergeben. Darauf aufbauend diskutieren wir sowohl aus Benutzer- als auch aus Betreibersicht die neuen Herausforderungen für den Datenschutz, die sich aus der hochschulübergreifenden Nutzung von Benutzerprofilen ergeben, und stellen Lösungskonzepte vor.

1. Einleitung

Die immer stärkere Orientierung an den Hochschulprozessen und deren durchgängige IT-Unterstützung, z. B. im Rahmen des Student Lifecycles, schlägt sich technisch in einer sehr engen Integration von LMSen mit Identity Management (IM) Architekturen und Campus Management (CM) Lösungen nieder. Im Rahmen von hochschulübergreifenden Studiengängen und landesweiten virtuellen Hochschulen bzw. Bildungsportalen, aber auch zur Unterstützung der Mobilität von Lehrenden und Lernenden, die im Kontext des Bolognaprozesses eine essentielle Rolle spielt, rückt die Nutzung von LMSen über die Grenzen der Alma Mater hinweg zunehmend in den Fokus der Hochschul-IT-Strategie.

LMSe sind Kernkomponenten von pervasiven Lehr- und Lernumgebungen und begleiten die Studierenden von der Bewerbungs- und Zulassungsphase (z. B. Propädeutika) an durch ihr gesamtes Studium. Somit wird den Studierenden bereits heutzutage ein konkreter Mehrwert zur Studienorganisation geboten. Über das Curriculum hinaus werden mittlerweile auch vermehrt Weiterbildungsangebote für Alumni online zur Verfügung gestellt, um eine langfristige Bindung an die Hochschule zu erreichen. Der Wandel von dedizierten, eine einzelne Präsenzveranstaltung ergänzenden elektronischen Materialien zu komplexen, hochschulprozess- und workfloworientierten LMSen, die alle Studierenden einer Hochschule in ihrer Gesamtheit erreichen und bedienen können, setzt neben zahlreichen anderen technischen Komponenten ein hochschulweites IM voraus. Dieses versorgt die Lernplattform mit allen relevanten Personendaten

[1] TU München, Fakultät für Informatik, I10, Boltzmannstr. 3, D-85748 Garching
[2] Leibniz-Rechenzentrum, MNM-Team, Boltzmannstr. 1, D-85748 Garching

über ihre Benutzer, die beispielsweise zur Autorisierung (technische Umsetzung der Berechtigungen, die ein Benutzer innerhalb des Systems hat) erforderlich sind. Darüber hinaus werden unter anderem belegte Studiengänge oder Organisationszugehörigkeiten bereitgestellt. Abbildung 1 zeigt das Prinzip einer typischen IM Architektur für Hochschulen, bei der ein zentrales Enterprise Directory aus den autoritativen Datenquellen der Studenten- und Personalverwaltung gespeist wird und die aggregierten und ggf. mit zusätzlichen Attributen wie Loginname und Startpasswort angereicherten Benutzerprofile an verschiedene technische Systeme, darunter das LMS, ausliefert oder diesen zum Abruf über Standardschnittstellen wie LDAP, JDBC und Web Services anbietet.

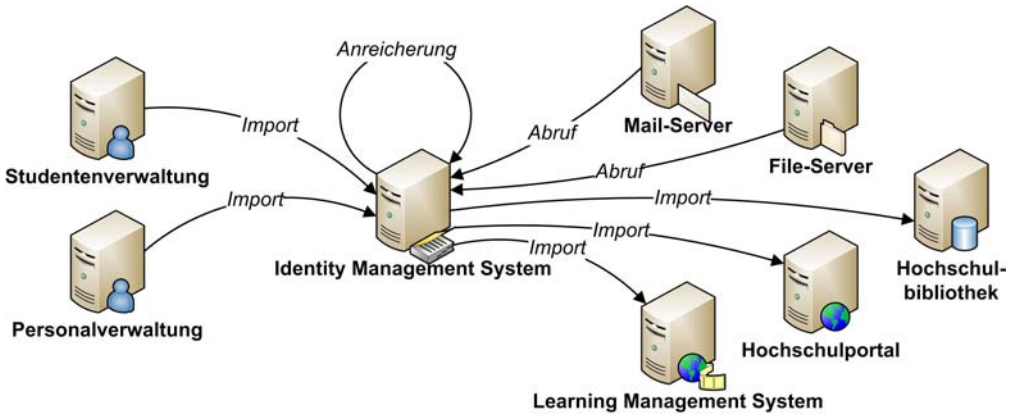

Abbildung 1: Typisches Hochschul-Identity-Management-System

Der so übermittelte Benutzerkreis deckt sich bezüglich seines Umfangs zwangsweise mit den Quellsystemen des IM Systems und ist somit in der Praxis auf die Angehörigen der eigenen Hochschule begrenzt. Wenn externe Benutzer unterstützt werden sollen, beispielsweise im Rahmen gemeinsamer Studiengänge mit anderen Hochschulen, werden neue Methoden zur Datenakquisition und -verwaltung notwendig. Dieser konkrete Bedarf ergibt sich auch über LMS-Broker wie die virtuelle Hochschule Bayern (vhb), die innerhalb Bayerns als landesweit zentrale Einrichtung den Studierenden einer Hochschule die Teilnahme an E-Learning-Kursen an anderen Hochschulen ermöglicht. Eine manuelle Erfassung größerer Mengen externer Benutzer durch die Administratoren jedes beteiligten LMS würde aufwandsbedingt nicht ausreichend skalieren. Verschiedene proprietäre Ansätze zur Übertragung von Benutzerprofilen, wie sie auch von der vhb angeboten wurden, konnten sich bei kommerziellen LMS-Lösungen jedoch nicht durchsetzen. Die alternative Selbstregistrierung durch jeden Benutzer führt in der Praxis schnell zu veralteten und mit der Heimathochschule inkonsistenten Daten; zudem müssen bestimmte Angaben wie z. B. der Studiengang geeignet nachgewiesen werden, da Lernmaterialien häufig nur einem eingeschränkten Nutzerkreis (z. B. nur Medizinstudenten) zur Verfügung gestellt werden dürfen. Somit wird deutlich, dass für das hochschulübergreifende E-Learning neue organisatorische und technische Konzepte notwendig werden.

Mit der Authentifizierungs- und Autorisierungsinfrastruktur des deutschen Forschungsnetzes (DFN-AAI) wird seit 2006 eine standardbasierte Lösung für hochschulübergreifendes IM deutschlandweit ausgerollt und seit Anfang 2008 für E-Learning-Anwendungen erweitert. Die DFN-AAI (vgl. [2]) basiert auf der Software Shibboleth (vgl. [8]), der selbst wiederum der weit verbreitete Industriestandard Security Assertion Markup Language (SAML) zugrunde liegt. Die Heimathochschule betreibt zu diesem Zweck wie in Abbildung 2 vereinfachend dargestellt einen so genannten Identity Provider (IDP), mittels dessen ausgewählte Informationen über den Benutzer vom so genannten Service Provider (SP), also z. B. einem LMS an einer anderen Hochschule, abgerufen werden können.

Ausgehend von der bisherigen E-Learning-Infrastruktur an der TUM, die wir in Abschnitt 2 vorstellen, beschreiben wir in Abschnitt 3 dieses Artikels, welche Anpassungen an einem LMS vorgenommen werden müssen, damit es als Shibboleth SP eingesetzt werden kann; als konkretes Beispiel wird das an der TUM eingesetzte Produkt CLIX des Herstellers imc AG angeführt, das im Rahmen eines Kooperationsprojekts mit dem Hersteller als eines der weltweit ersten LMSe entsprechend erweitert wurde. Die hochschulübergreifende Übermittlung von Benutzerprofilen setzt ein produktübergreifend gemeinsames Datenmodell voraus, das im Rahmen der DFN-AAI als E-Learning Profil bezeichnet wird und unter Mitwirkung der Autoren entstanden ist; seine Bedeutung wird in Abschnitt 4 diskutiert. Die Übertragung personenbezogener Daten an andere Hochschulen, welche über so genannte Privacy Policies gesteuert wird, ist datenschutzrechtlich kritisch und bildet hinsichtlich der geeigneten Unterstützung durch IT-Werkzeuge einen unserer aktuellen Forschungsschwerpunkte. In Abschnitt 5 diskutieren wir diese Problematik sowohl aus Benutzerperspektive unter dem Stichwort der informationellen Selbstbestimmung als auch aus dem Blickwinkel des Betreibers. Dabei zeigt sich insbesondere, dass die verwendete Softwarebasis beispielsweise im Bereich des automatischen Abgleichs von Privacy Policies zwischen kooperierenden Hochschulen noch verbessert werden muss. Hierfür stellen wir ein Lösungskonzept und eine web-service-basierte Realisierungsvariante vor. Ein Resümee der bisherigen Ergebnisse und ein Ausblick auf die nächsten Schritte schließen diesen Artikel ab.

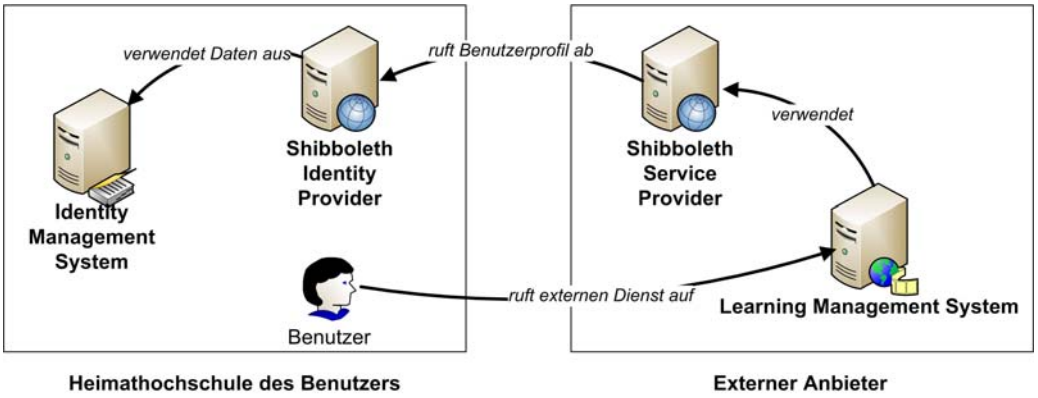

Abbildung 2: Ablauf beim Benutzerdatenabruf mit Shibboleth (vereinfachte Darstellung)

2. Ausgangssituation und Vorgehensweise an der TU München

Mit insgesamt 142 Partneruniversitäten und einer Vielzahl an Kooperationsstudiengängen bedient die IT-Infrastruktur der TUM nicht nur ihre eigenen Studenten, sondern stellt ihre Dienste auch einer breiten Masse an Gästen zur Verfügung. Externe Studierende werden nicht von der Studentenverwaltung der TUM erfasst, folglich auch nicht ins zentrale IM der TUM eingespielt und können somit die an das IM angebundenen Dienste nicht nutzen. Zur Authentifizierung vergibt die TUM aktuell an alle Personen im IM System eine zentrale Kennung, die ein so genanntes Unified Login, also die Verwendung desselben Benutzernamens/Passworts in allen an das IM angebundenen Endsystemen, ermöglicht. Ein Single Sign-On (SSO) für die zentralen Websysteme der TUM war bisher noch nicht verfügbar. Für Gastwissenschaftler, die einen den TUM-Mitarbeitern recht ähnlichen Status haben, wurde eine Lösung in Form einer dedizierten TUM-Gästeverwaltung implementiert, die vom IT-Service Desk verwendet wird. Aufgrund des mit der manuellen Erfassung verbundenen Aufwands und der Berechtigungen, die an so eingetragene Personen pauschal vergeben werden, können über diese Lösung jedoch andere Gäste, wie z. B. die Studierenden der Partneruniversitäten, nicht abgedeckt werden; zudem wäre eine explizite und aufwendige Erfassung im Prüfungsverwaltungssystem erforderlich.

Als naheliegender erster Lösungsansatz wurden - zunächst losgelöst vom zentralen IM - bei Bedarf rein LMS-interne Benutzerkonten angelegt und mit der Laufzeit eines Semesters versehen. Diese Accounts waren nicht nur aufwendig zu verwalten, sondern den zentral gepflegten Kennungen bezüglich Datenkonsistenz und Qualität weit unterlegen (z. B. Tippfehler, fehlende Nachprüfbarkeit der Angaben, seltene Aktualisierung, ...). Nachdem dieses Problem an der TUM erkannt wurde, wurde in Zusammenarbeit mit dem Leibniz-Rechenzentrum (LRZ), dem zentralen IT-Dienstleister der Müncher Hochschulen, nach einer nachhaltigen Lösung gesucht. Nach eingehender Analyse fiel die Entscheidung damals bereits - unabhängig von der späteren deutschlandweiten Einführung - für die Software Shibboleth als Lösung sowohl für SSO als auch für die Übermittlung von Benutzerprofilen. Durch die Standardkonformität zu SAML können Benutzerprofile verschlüsselt und somit auch über das Internet abhörsicher zwischen der Heimathochschule eines Nutzers und einem Diensteanbieter ausgetauscht werden. Schließen sich mehrere IDPs und SPs zusammen, so wird dies als Föderation oder Circle of Trust bezeichnet. Technisch basiert eine solche Föderation auf einer sog. Authentifizierungs- und Autorisierungsinfrastruktur, wie sie inzwischen in Deutschland vom Deutschen Forschungsnetz koordiniert aufgebaut wurde und allen Forschungseinrichtungen zur kostenfreien Nutzung zur Verfügung steht.

Alle Lehrveranstaltungen (inkl. Raummanagement, Zeitplanung, …) werden zukünftig im zentralen CM der TUM, TUMonline (siehe [10]), gepflegt. CLIX wird in der Folge primär für die Inhalte der Lehrveranstaltungen verwendet. Somit werden die in TUMonline erfassten Lehrveranstaltungsdaten über eine Schnittstelle an CLIX übertragen. Innerhalb von CLIX gibt es einen Unterschied zwischen internen (also im IM der TUM vorhandenen) und externen (nicht im IM der TUM vorhandenen und auch nicht über die Gästeverwaltung eingepflegten) Nutzern. Externe Nutzer sind bei einem Shibboleth-Szenario erst dann in der Lernplattform verfügbar, wenn sie sich das erste Mal über ihre Heimathochschule an CLIX anmelden. Für interne Nutzer wird durch einen nächtlichen Import aus dem zentralen IM in CLIX ein vollständig befüllter Account angelegt (siehe [6]) – unabhängig davon ob Shibboleth im Einsatz ist oder nicht. Die Datenschutzaspekte richten sich hierbei nach den vom Datenschutzbeauftragten der TUM freigegebenen Prozessabläufen. So werden für die internen Benutzer (d. h. die offiziellen Angehörigen der TUM) im Vergleich zu den externen Nutzern zusätzliche Informationen durch das zentrale IM der TUM zur Verfügung gestellt und in der Lernplattform verwendet (z. B. zur Bildung von dedizierten Gruppen, Communities, virtuellen Klassen, …). Weiter ermöglicht der regelmäßige Import eine automatische Anmeldung der Studierenden für Lehrveranstaltungen im CM der TUM, die wiederum an CLIX über eine Schnittstelle übertragen wird.

Websysteme unterstützen die Software Shibboleth im Normalfall erst nach entsprechenden Anpassungen, die im Jargon als „Shibbolisierung“ bezeichnet werden. Als formale Grundlage u. a. zur Durchführung der notwendigen Modifikationen für eine „Shibbolisierung“ der zentralen Systeme war es zur Sicherstellung der Nachhaltigkeit strategisch erforderlich, dass die TUM einen offiziellen Beschluss zur Nutzung von AAI-Technologien fasst. In Kooperation mit dem LRZ wurden die Überlegungen zu SSO und AAI im Rahmen des IT-Fachausschusses der TUM vorgestellt. Ferner wurde als Grundlage für einen Beschluss vom elecTUM Team (siehe [11]) ein Positionspapier erarbeitet. Darin werden die campusinternen AAI-Anwendungsszenarien beschrieben, die notwendigen Prozessanpassungen definiert und die entsprechenden Modifikationen der zentralen Systeme konkretisiert. Die Präsentation im IT-Fachausschuss und das Positionspapier führten letztendlich zur Entscheidung der TUM für den Einsatz von Shibboleth als campusinternes und hochschulübergreifendes SSO-System für alle zentralen Websysteme der TUM. Welche Konsequenzen dies auf bestehende Systeme hat, wird im nächsten Kapitel exemplarisch für das zentrale LMS diskutiert.

3. Anpassung von Learning Management Systemen an Shibboleth

Hochintegrierte LMSe wie CLIX vereinigen eine Vielzahl von Diensten rund um die Themen Lernprozesse, Lernmanagement und Organisation der Lehre in einer zentral zugänglichen (Web-) Applikation. Für die Anpassung eines solchen LMS an AAI-Technologien stehen zwei Alternativen zur Auswahl: entweder das Verschmelzen von fremdem Code mit der bisherigen Applikation oder aber die direkte Verwendung von bestehenden Komponenten im Wechselspiel mit der Applikation selbst. Beide Varianten haben charakteristische Vor- und Nachteile, die bei der konkreten Realisierung durch den Hersteller imc sorgfältig abgewogen wurden. Würde man die frei verfügbare Implementierung direkt verwenden, so müsste auf die Kompatibilität zur bisherigen produktspezifischen Freigabeliste für die Webapplikation geachtet (Apache, IIS, Tomcat, Websphere, ...) sowie die Unterstützung der diversen Betriebssysteme weiter gewährleistet werden. Zudem werden umfangreiche Tests notwendig, die aus betriebswirtschaftlicher Sicht nicht zu rechtfertigen sind. Darüber hinaus hätte das Wechselspiel zwischen der verfügbaren Implementierung von Shibboleth und CLIX eine Vielzahl an Modifikationen notwendig gemacht: CLIX basiert auf der Technologie JSP (Java Server Pages) und Java; die aktuell verfügbare Shibboleth-Implemetierung liegt hingegen in der Programmiersprache C++ vor. Die Überlegungen des Herstellers zu Aufwand und Geschäftsnutzen lassen somit nur noch die Möglichkeit zu, den Prozessablauf von Shibboleth in CLIX zu integrieren.

Basierend auf der TUM-Entscheidung konnten die Gespräche mit dem Hersteller imc intensiviert und durch eine Kooperationsvereinbarung auch die Umsetzung beschlossen werden. Insgesamt waren nach der vorangegangenen Analyse die folgenden Modifikationen am System erforderlich, um die ermittelten Anforderungen zu erfüllen; diese treffen größtenteils auch auf die LMSe anderer Hersteller zu (nach absteigendem Implementierungsaufwand sortiert):

- Integration eines dedizierten und autarken Authentifizierungsmoduls, das es ermöglicht, den Authentifizierungsvorgang wie von Shibboleth vorgesehen an ein externes System, in diesem Fall die Heimathochschule des Benutzers, zu delegieren.
- Aufbereitung der vom IDP gelieferten Attribute mittels Regeln und Filtern. Diese Verarbeitungsschritte sind notwendig, um die Benutzerprofildaten in das lokal benötigte Format umzuwandeln und die resultierenden Berechtigungen setzen zu können.
- Intervallgesteuerte Aktualisierung der Föderationsmetadaten, d. h. eines zentral verwalteten XML-Dokuments, das die technisch relevanten Daten wie Servernamen und Serverzertifikate aller IDPs und SPs einer Föderation enthält.
- Unterstützung der parallelen Teilnahme an mehreren Föderationen und Unterstützung der Authentifizierung gegen föderationsexterne IDPs (z. B. bei Gaststudierenden aus dem Ausland, deren Heimateinrichtungen meist nicht in der DFN-AAI vertreten sind).
- Integration der „Where are you from" (WAYF) - Auswahlmaske: Der WAYF ist ein Dienst, der dem Nutzer anhand der Föderationsmetadaten eine Liste aller IDPs zur Auswahl stellt; der Nutzer wählt aus dieser Liste seine Heimathochschule aus und wird von dieser z. B. anhand von Benutzername und Passwort authentifiziert.
- Berücksichtigung der informationellen Selbstbestimmung, konkret durch eine Einstiegsseite, auf der dem Nutzer alle von ihm übertragenen Attribute sowie die Nutzungsbedingungen präsentiert werden. Lehnt der Nutzer diese ab, so ist eine Nutzung des Systems nicht möglich und seine Informationen werden nicht gespeichert.
- Optionale Aktualisierung der Benutzerdaten beim Login: Loggt sich ein Nutzer das erste Mal bei einem SP an, so werden die entsprechenden Nutzerattribute – je nach Regelwerk beim IDP – an den SP übertragen. Dieser speichert die Attribute in einem lokalen

Benutzerprofil und kann sie immer dann automatisch aktualisieren, wenn der Nutzer sich das nächste Mal anmeldet.

- Möglichkeit zur Übersteuerung der Authentifizierungsart: Würde nur die Authentifizierungsvariante „Shibboleth“ zur Verfügung stehen, so könnten sich lokale Nutzer mit Spezialrechten und Testnutzer nicht anmelden. Es ist also möglich, je nach Benutzeraccount eine passende Authentifizierungsart zu wählen.

Der Datenschutzaspekt ist von besonderer Bedeutung und wird daher in Kapitel 5 im Detail aufgegriffen. Aktuell ist die Shibboleth-Integration in CLIX abgeschlossen und wird mit dem kommenden Release 8.0 vom Hersteller ausgeliefert. An der TUM wird die Integration bereits vorab getestet und der Produktiveinsatz entsprechend frühzeitig geplant. Eine Migration der bestehenden Lernplattform (Release 7.0) auf das neue Release ist für September 2008 geplant. Von der in Relation zu anderen LMSen durchaus sehr zügigen Anpassung von CLIX werden dann insbesondere die externen Benutzer der TUM profitieren; aber auch campusintern ergibt sich der Mehrwert des SSO zwischen allen bereits Shibboleth-fähigen IT-Diensten der TUM.

4. Das DFN-AAI E-Learning-Profil als föderationsweites Datenmodell

Eine der grundlegenden Voraussetzungen für jeglichen Austausch von Identitätsinformationen ist ein gemeinsames Datenmodell, das von Absender (IDP) und Empfänger (SP) syntaktisch wie auch semantisch gleich interpretiert wird. IM-Projekte an deutschen Hochschulen entwickeln jedoch meist ein stark an den lokalen Bedürfnissen orientiertes LDAP-Datenmodell, sodass häufig der gemeinsame Nenner für einen Benutzerdatenaustausch fehlt. In anderen Ländern wie beispielsweise den USA wird diesbezüglich integrierter vorgegangen - dort haben sich De-facto-Standards wie eduPerson (vgl. [7]) als gemeinsames Datenmodell etabliert.

Der DFN-Verein hat die hierzulande inhärente Problematik bei der Initiierung der DFN-AAI erkannt und ein Basisdatenmodell für die Verwendung zur Datenübertragung im Rahmen der DFN-AAI spezifiziert (siehe [5]). Da sich dieses bewusst auf grundlegende Authentifizierungs- und Autorisierungsinformationen beschränkt, wie sie beispielsweise im Umfeld von Online-Bibliotheksdiensten oder bei der Verteilung lizenzierter Software an Studenten verwendet werden, ist keine unmittelbare Anwendbarkeit auf LMSe, die z. B. Informationen über Studiengänge benötigen, gegeben. Eine im Jahr 2007 von der vhb unter ihren 36 Trägerhochschulen durchgeführte Umfrage zeigt, dass im aktuellen Schema für den Betrieb von LMSen notwendige Informationen wie Geburtsdatum, Studiengang, Abschlussart, Matrikelnummer und Fachsemester fehlen und auch die Lieferung von zur Personalisierung von Webanwendungen benötigten Daten wie dem Geschlecht und dem Titel des Benutzers nicht vorgesehen ist. Nachdem diese Thematik auch von anderen Arbeitskreisen an den DFN-Verein herangetragen wurde, hat dieser eine Arbeitsgruppe ins Leben gerufen, die mit der Erarbeitung des sogenannten DFN-AAI E-Learning Profils, d. h. einer für E-Learning-Anwendungen spezifischen Erweiterung des Basisdatenmodells (an der auch die Autoren beteiligt sind) beauftragt wurde. Nach einer deutschlandweiten Bedarfsanalyse, die unter Mitarbeit von Hochschulvertretern aus fast allen Bundesländern durchgeführt wurde, begann eine mehrere Monate dauernde Spezifikationsphase. Hierbei wurde insbesondere das Ziel verfolgt, die neuen Datenfelder so zu spezifizieren, dass sie von den an den Hochschulen bereits vorhandenen IM-Systemen möglichst einfach, d. h. mit nur einem Minimum an Konvertierungsoperationen, bereitgestellt werden können.

Die erste Version des E-Learning Profils wird im Herbst 2008 veröffentlicht werden. Es enthält alle E-Learning-spezifischen Datenfelder, die von einer Mindestanzahl der an der Bedarfsermittlung beteiligten Hochschulen als notwendig gemeldet wurden. Darüber hinaus dokumentiert es, wie bei

Bedarf weitere benötigte Benutzerattribute, die noch nicht bekannt waren oder bewusst nicht ins E-Learning-Profil aufgenommen wurden, auf einer bilateralen Basis zwischen IDPs und SPs definiert werden können,. Die TUM ist dabei eine der ersten Hochschulen in Deutschland, die das erweiterte Datenmodell sowohl in der Rolle als IDP als auch in CLIX, das als SP in der DFN-AAI fungiert, unterstützt. Dieser Pilotcharakter gilt auch für die Umsetzung der Datenschutzaspekte, die im folgenden Abschnitt diskutiert werden.

5. Anforderungen an den Datenschutz und policy-basierter Lösungsansatz

Einige Anwendungen, die in Authentifizierungs- und Autorisierungsinfrastrukturen angeboten werden, können anonym genutzt werden, sofern eine grundlegende Autorisierung zur Dienstnutzung sichergestellt ist. Beispielsweise können viele Bibliotheks- und Verlagsangebote in Anspruch genommen werden, wenn gewährleistet ist, dass der Benutzer aktuell Student oder Mitarbeiter einer Hochschule ist; eine persönliche Registrierung oder anderweitige Erfassung des Benutzers ist dabei nicht notwendig.

E-Learning-Anwendungen setzen hingegen verstärkt auf Personalisierung: Den Lernenden sollen Kurse angeboten werden, die möglichst gut in ihr Curriculum passen bzw. Dozierende lassen für manche Kurse nur Personen aus einem bestimmten Teilnehmerkreis zu. Weiter besteht die Möglichkeit zur Teilnahme an Prüfungen, die von der jeweiligen Heimathochschule anerkannt werden. Hierfür werden die allgemein üblichen Daten für Leistungsnachweise („Scheine“) vorausgesetzt, die zudem je nach Hochschule auch eine Reihe sensibler Daten wie Matrikelnummer und Geburtsdatum enthalten müssen. Somit werden im Vergleich zu den bisherigen Diensten innerhalb der DFN-AAI eine Vielzahl an datenschutztechnisch sensiblen Informationen benötigt, die besonders schützenswert sind.

Aus Datenschutzperspektive ist es offensichtlich, dass ein IDP diese stark personenbezogenen Daten nicht jedem beliebigen Dienstleister übermitteln darf, nur weil dieser eine entsprechende Anfrage stellt. Dafür würde jegliche rechtliche Grundlage fehlen: Die Personendaten wurden von der Hochschule ursprünglich zu einem völlig anderen Zweck erhoben als zur Weitergabe an externe Dienstleister im Rahmen einer AAI. Als Konsequenz muss präzise darauf geachtet werden, das Recht der Benutzer auf ihre informationelle Selbstbestimmung zu wahren. Jeder Benutzer muss folglich sein explizites Einverständnis dazugeben, dass personenbezogene Informationen, deren Inhalte dem Betroffenen offenzulegen sind, an einen Dritten übermittelt werden. Die TUM setzt hierfür ein Open Source Werkzeug ein, das mit jedem SP funktioniert und dem Benutzer beim jeweils ersten Dienstaufruf anzeigt, welche Daten an dessen Betreiber übermittelt werden würden. Der Nutzer hat dadurch die Möglichkeit, den Vorgang abzubrechen. Visuell wird hierzu auf die bekannte Visitenkarten-Metapher zurückgegriffen, bei der die personenbezogenen Daten wie auf einer Visitenkarte angeordnet werden (vgl. Microsoft CardSpace [1]). Untersuchungen zur Benutzerfreundlichkeit dieser Ansätze finden sich beispielsweise in [9].

Aus Betreibersicht ergibt sich darüber hinaus die Schwierigkeit, dass jedes Verfahren, bei dem personenbezogene Daten verarbeitet werden, zu dokumentieren ist. Dabei muss vom zuständigen Datenschutzbeauftragten eine Genehmigung vorliegen und eine Aufnahme in die offizielle Verfahrensliste stattfinden. Die hierfür im IM-Umfeld bislang übliche Dokumentation der Datenflüsse pro Datenabnehmer ist in dynamischen AAI-Umgebungen jedoch kaum noch möglich, da die Anzahl von Dienstanbietern beliebig groß werden kann und ein Benutzer auch einen Dienstleister auswählen kann, der der Heimathochschule potenziell sogar noch unbekannt ist.

Bei der technischen Umsetzung tritt in der Praxis das Problem auf, dass bei der derzeit überwiegend eingesetzten Version 1.3 des Shibboleth IDP jede Dateifreigaberegel separat für jeden einzelnen SP wiederholt werden muss. Diese Redundanz ist mit einem sehr hohen Administrationsaufwand verbunden und erschwert das Change Management drastisch, da z. B. ein neu freizugebendes Benutzerattribut an vielen statt nur an einer Stelle des Regelwerks ergänzt werden muss. Insbesondere ist es für die Benutzer nicht möglich, einen neu in der Föderation vertretenen LMS-Dienstleister zu nutzen, bis der IDP-Administrator der Heimathochschule die entsprechenden Freigaberegeln definiert hat. Das eigentliche Ziel der dynamischen Nutzung beliebiger Dienste wird dadurch verfehlt.

Auch die neue und bisher in der DFN-AAI noch nicht weit verbreitete Version 2.0 löst dieses Problem nur ansatzweise: Sie bietet die Möglichkeit, in den Föderationsmetadaten Gruppen von SPs zu hinterlegen. Datenfreigaberegeln können sich dann auf Gruppen statt auf einzelne SPs beziehen. Problematisch dabei ist, dass die Föderationsmetadaten zentral und für *alle* Föderationsteilnehmer gepflegt werden müssen. Eine dezentrale Pflege von Gruppen, beispielsweise aller bayerischen LMS durch die vhb, ist somit nicht möglich. Insbesondere kommt aus Sicherheitsgründen auch keine Selbstregistrierung von SPs für Gruppen in Frage, da sich bösartige SPs über gefälschte Gruppenzugehörigkeiten Informationen über Benutzer, die sie eigentlich nicht erhalten dürften, verschaffen könnten. Andererseits wäre auch eine Pflege sämtlicher Gruppierungswünsche durch eine zentrale Instanz wie den DFN-Verein als Koordinator der DFN-AAI unverhältnismäßig aufwendig.

Aus diesem Grund wird zunächst eine in der Praxis einfach umzusetzende, aber zur Sicherstellung ihrer Nachhaltigkeit auch flexible Lösung benötigt, mit der dezentral verwaltete Datenfreigaberegeln zwischen mehreren IDPs konsistent gehalten werden können. Im Folgenden stellen wir einen Lösungsansatz vor, der sowohl für Shibboleth 1.x als auch 2.0 geeignet ist. Exemplarisch sollen Freigaben für alle an der vhb beteiligten LMSe zwischen allen Trägerhochschulen der vhb konsistent gehalten werden. Der gewählte Ansatz verfolgt das Ziel, dass ausgewählte Freigaberegeln - wie unten beschrieben - zwischen den beteiligten Hochschulen in einem automatisierten Verfahren ausgetauscht werden. Bei den somit hochschulübergreifend synchronisierten Daten handelt sich deshalb um Fragmente der Shibboleth-Konfigurationsdateien, mit denen die Freigabe von Benutzerattributen an Dienstleister gesteuert wird (sog. Site Attribute Release Policy bzw. Attribute Filter Policies). Diese Freigaberegeln können bei jedem IDP individuell mit weiteren Regeln kombiniert werden, sodass auch mehrere voneinander unabhängige Gruppen von SPs und bilaterale Verträge zwischen IDP und SP unterstützt werden. Diese Vorgehensweise hat ferner den Vorteil, dass kein neues Datenformat eingeführt bzw. ausgewertet werden muss, und somit der Deploymentaufwand minimiert wie auch die bereits bei allen IDPs vorhandene Funktionalität ohne weiteren Eingriff in die Software angewendet werden kann.

Die gruppenspezifischen Freigaberegeln werden von einer zentralen Instanz, die allgemein als Trusted Third Party bezeichnet wird, verwaltet; im Beispiel ist es naheliegend, dass die vhb selbst die Gruppe der an der vhb beteiligten LMSe pflegt. Da es sich um vergleichsweise einfach strukturierte XML-Dokumente handelt, sind keine spezialisierten Verwaltungswerkzeuge erforderlich. Analog zu den Föderationsmetadaten müssen die Datenfreigaberegeln gegen unberechtigte Manipulation geschützt werden; zu diesem Zweck werden sie vom Verwalter entsprechend dem XMLDsig-Standard (siehe [4]) elektronisch signiert. Das resultierende Dokument muss an die beteiligten IDPs verteilt werden. Als einfache Lösung bietet sich wie in Abbildung 3 links dargestellt ein regelmäßiger Download von einem zentralen Webserver an; ein solches Verfahren hat sich im Bereich der Föderationsmetadaten bereits erfolgreich etabliert. Diese Variante hat jedoch den Nachteil, dass Änderungen am zentralen Dokument nur mit Verzögerungen

föderationsweit wirksam werden, da abgewartet werden muss, bis es vom jeweiligen IDP abgerufen worden ist. Temporäre Inkonsistenzen würden dazu führen, dass die Benutzer betroffener Heimateinrichtungen diejenigen Dienste, an denen sich Änderungen ergeben haben, nicht oder nur eingeschränkt nutzen könnten. Zudem stellt die Download-Site einen Single Point of Failure dar, dessen Hochverfügbarkeit z. B. auch unter Berücksichtigung möglicher Denial-of-Service-Angriffe sichergestellt werden muss.

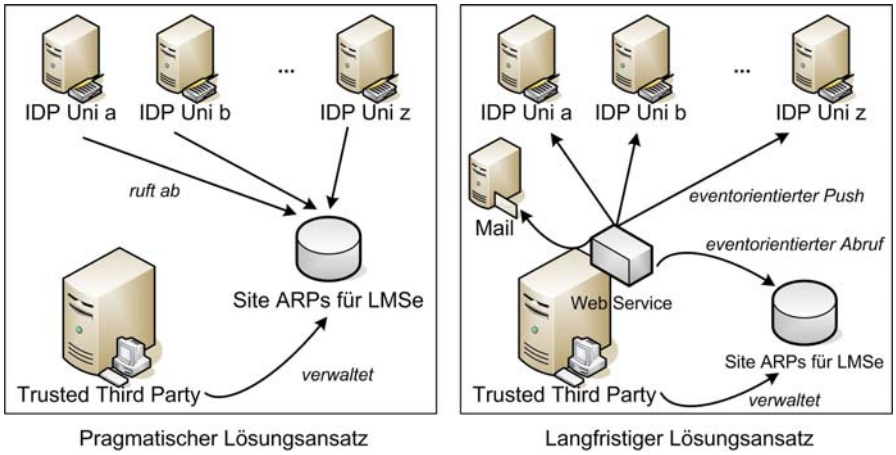

Abbildung 3: Gegenüberstellung der Lösungsansätze

Als langfristige Lösung, die diese Problembereiche vermeidet und kosteneffizient betrieben werden kann, arbeiten wir deshalb an einem push-basierten Verteilmechanismus, der technisch über Web Services umgesetzt wird und sich bezüglich der Kommunikationsprozesse am standardisierten Protokoll COPS (vgl. [3]) orientiert – auf der rechten Seite in Abbildung 3 dargestellt. Änderungen am Regelwerk werden den davon betroffenen IDPs eventorientiert mitgeteilt. Sofern ein IDP nicht temporär unerreichbar ist, werden alle Änderungen sofort wirksam. Zudem kann das zu übertragende Datenvolumen durch eine Beschränkung im Regelbetrieb auf die jeweiligen Differenzen zum vorherigen Stand minimiert werden; nur nach längeren Ausfällen ist eine erneute Übertragung des gesamten Regelwerks erforderlich. IDP-seitig können sich die Administratoren zudem automatisch per E-Mail über Änderungen am Regelbestand informieren lassen, und so als Kontrollinstanz fungieren.

Wir planen, diesen Ansatz nach Abschluss der Implementierungsarbeiten zunächst im Umfeld der vhb zu evaluieren und anschließend in die DFN-AAI einzubringen.

6. Zusammenfassung und Ausblick

In diesem Artikel haben wir zunächst skizziert, wie lokale IM Systeme und hochschulübergreifende Authentifizierungs- und Autorisierungsinfrastrukturen zusammenspielen, um externe Benutzer beispielsweise in LMSe aufnehmen zu können. Am Beispiel des an der TUM eingesetzten LMS CLIX haben wir erläutert, welche Anpassungen notwendig waren, um eine Integration in eine Shibboleth-basierte Föderation zu realisieren, wie sie in Deutschland im Rahmen der DFN-AAI betrieben wird. Zur Unterstützung LMS-spezifischer Benutzerdaten wurde eine Erweiterung des eingesetzten Datenmodells notwendig. Aufgrund der sensiblen und stark personenbezogenen Informationen müssen zahlreiche Datenschutzaspekte berücksichtigt werden. Die damit verbundenen Herausforderungen sowie einen von uns erarbeiteten Lösungsansatz, der Metadatenfragmente über Web Services verteilt und konsistent hält, haben wir in Abschnitt 5 vorgestellt.

Die nächsten Schritte bestehen darin, die praktische Umsetzung der beschriebenen Konzepte weiter voranzutreiben, wobei die gemeinsamen Studiengänge der beiden Münchner Universitäten und die bayernweite LMS-Integration im Rahmen der vhb im Vordergrund stehen. Parallel dazu sind Shibboleth-Anpassungen weiterer Dienste neben CLIX in Arbeit, durch die einerseits weitere Anforderungen an das Policy Management gestellt werden, die aber andererseits auch Synergieeffekte mit den bereits implementierten Lösungen bieten und somit unmittelbare Mehrwerte für die internen und externen Benutzer darstellen. Dabei soll auch die enge und seither sehr erfolgreiche Zusammenarbeit mit den Herstellern eingesetzter Softwareprodukte und dem DFN-Verein fortgeführt werden.

Danksagung

Die Autoren danken der IntegraTUM- sowie der elecTUM-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. elecTUM ist ein vom BMBF im Bereich „Neue Medien in der Bildung 2“ gefördertes Projekt zum Aufbau und zur Integration einer zentralen Lernplattform in die IT-Infrastruktur der TUM unter der Leitung von Dr. Sabine Rathmayer. 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.

7. Literaturangaben

[1] Chappell, David, *Introducing Windows CardSpace*. 2006. Microsoft Developer Network MSDN, http://msdn.microsoft.com/winfx/reference/infocard.

[2] DFN. *DFN-AAI - Authentifikation Autorisierungs Infrastruktur*. 2007. [abgerufen am 24.01.2008]; verfügbar unter: https://www.aai.dfn.de/.

[3] Durham, D., et al., *The Common Open Policy Service Protocol*. 2000. IETF Proposed Standard, RFC 2748.

[4] Eastlake, D., et al., *W3C XML-Signature Syntax and Processing*. 2002. W3C Recommendation.

[5] Gietz, P., et al. *DFN-AAI Technische und organisatorische Voraussetzungen - Attribute*. 2006. [abgerufen am 11.02.2008]; verfügbar unter: https://www.aai.dfn.de/fileadmin/documents/vertraege/attribute.20061130.pdf.

[6] Graf, S., Gergintchev, I. und Rathmayer, S. *Identity Management Solutions in Heterogenous Learning Environments*. in Proceedings *iLearning Forum*. 2008. Paris.

[7] Internet2, Educause. *eduPerson Object Class*. 2001. [abgerufen am 24.01.2008]; verfügbar unter: http://www.educause.edu/eduperson/.

[8] Internet2, Middleware Initiative. *Shibboleth Project - Internet2 Middleware*. 2000. [abgerufen am 06.02.2008]; verfügbar unter: http://shibboleth.internet2.edu/.

[9] Pettersson, J.S., et al. *Making PRIME Usable*. in Proceedings *Symposium on usable privacy and security (SOUPS)*. 2005: ACM Press.

[10] Technische Universität Graz. *CAMPUSonline*. 2008. [abgerufen am 24.07.2008]; verfügbar unter: https://online.tu-graz.ac.at.

[11] Technische Universität München. *Projekt elecTUM*. [abgerufen am 06.07.2008]; verfügbar unter: http://www.tum.de/electum.