Die Objektklasse thuEduPerson und der Meta View einer hochschulorientierten Benutzerverwaltung

Jörg Deutschmann

Technische Universität Ilmenau
Universitätsrechenzentrum
Joerg.Deutschmann@TU-Ilmenau.DE

Kurzfassung. Im Projekt „Integrierende Benutzer- und Ressourcenverwaltung an den Thüringer Hochschulen (Meta Directory)“, das durch das Thüringer Ministerium für Wissenschaft, Forschung und Kunst (TMWFK) gefördert wird, bemühen sich die Rechenzentren der Universität Erfurt, der Technischen Universität Ilmenau, der Friedrich-Schiller-Universität Jena und der Bauhaus-Universität Weimar um eine integrierende und einheitliche Sicht auf die digitale Identität der Hochschulangehörigen.

1 Motivation und Einführung

Das effiziente Management der Hochschulressourcen stellt mit der zunehmenden Eigenständigkeit der Thüringer Hochschulen eine große Herausforderung dar. Bei diesen Ressourcen handelt es sich vor allem um Personen, die an Forschung, Lehre und Verwaltung beteiligt sind, aber auch um Betriebsmittel, wie Gebäude, Räume und Geräte. Von strategischer Bedeutung ist in diesem Zusammenhang die Integration bereichsübergreifender Funktionen der zentralen Verwaltung mit den Verwaltungseinheiten der Fakultäten und Fachbereiche. An dieser Schnittstelle zwischen Hochschulverwaltung und Forschung sowie Lehre setzt das in Abbildung 1 dargestellte Projekt Meta Directory an.
Zukünftige Entwicklungen im Bereich der zentralen und akademischen Verwaltung werden auch im Hinblick auf weitere personelle Einsparungen durch zunehmende Integration erst möglich. Das Paradigma des Meta Directory besitzt das notwendige Potential, indem es mit einem integrierenden Verzeichnisdienst die hochschulweite Verwaltung der Identität von Personen, das sogenannte *Identity Management*, sicherstellt. *Synchronisation*smechanismen zwischen den operationellen Datenbanken der zentralen Verwaltung und dem Verzeichnis automatisieren Massenvorgänge, wie zum Beispiel das Einrichten neu immatrikulierter Studenten als Netzwerkbenutzer innerhalb der Hochschule. Dieser Vorgang des *Provisioning* verlangt auch wegen dem zukünftigen Einsatz von Chipkarten und einer Public Key Infrastruktur nach einem Verzeichnisdienst mit konsolidierten Benutzerdaten. Der offene Standard „Lightweight Directory Access Protocol (LDAP)“ [1] und seine breite Unterstützung durch die Hersteller ermöglichen die Bereitstellung einer integrierten Quelle zur Authentisierung der Benutzer und der gruppenbasierten Verwaltung ihrer Rechte im

Rechnernetz. Ein benutzerfreundliches *Single Sign On* für Web- und andere Applikationen basiert somit auf dem Verzeichnisdienst.

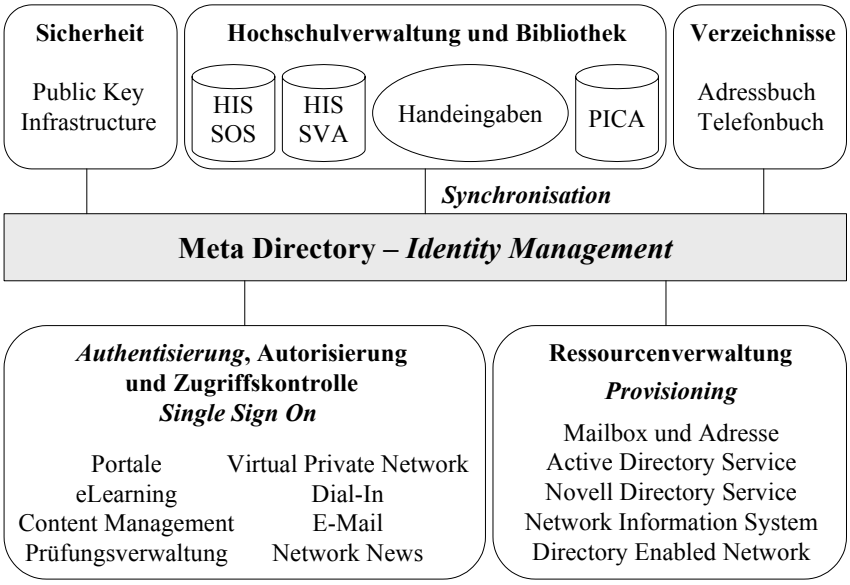


Abb. 1. Meta-Directory-Szenario an einer Hochschule.

Ausgehend von dem Ziel, einer integrierenden Benutzer- und Ressourcenverwaltung, gehen die Thüringer Hochschulen weiterhin von der These aus, dass sich LDAP und die damit verbundene Verzeichnistechnologie zum Standard für die Benutzer- und Ressourcenverwaltung entwickeln, ähnlich dem HTTP (Hypertext Transfer Protocol) zur Übertragung von Dokumenten in der Web-Technologie. Dem Paradigma des Meta Directory, dass durch Synchronisationsmechanismen die Integration unterschiedlicher Verzeichnisse und anderer Informationsressourcen innerhalb einer Organisation, eines Unternehmens oder einer Hochschule zu einem einzelnen globalen Verzeichnis gestattet und unterstützt, kommt dabei eine Schlüsselrolle zu. Die Verwirklichung dieser Integration entscheidet mit über die zukünftige Wettbewerbsfähigkeit der Hochschulen.

Die Weiterführung der Analyse- und Entwurfstätigkeit im Rahmen des Projekts führte zu der in Abbildung 1 dargestellten Konkretisierung des bereits vorgestellten Meta-Directory-Szenarios [2]. Neben den klassischen Anwendungen eines Verzeichnisses für Adress- und Telefonbuch sowie der verzeichnisbasierten Unterstützung einer Public Key Infrastruktur werden durch die Anwendungen vor allem die durch einschlägige Marktforschungsinstitute, wie zum Beispiel der Burton Group, geforderten Unterstützungen für das Identity Management, die Synchronisation, das Provisioning und die Authentisierung in Verbindung mit Single Sign On realisiert.

2 Auseinandersetzung mit Projekten im Umfeld

Die Bedeutung der Einführung eines integrierenden Verzeichnisdienstes an den Hochschulen wird deutlich in der Konstituierung einer bundesweite Arbeitsgruppe der Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre e.V. (ZKI) zum Thema Meta Directory und Identity Management. Eine erste Informationsveranstaltung zeigte zahlreiche Initiativen zur Weiterentwicklung von Verzeichnisdiensten an den deutschen Hochschulen auf. Die Ergebnisse einiger international angelegter Projekte haben den Entwurf von Verzeichnis- und Datenstrukturen beeinflusst und sollen deshalb im folgenden kurz vorgestellt und eingeschätzt werden.

2.1 DEEP

Das Projekt Definition of an European EduPerson (DEEP) der Trans-European-Research and Education Networking Association (TERENA) zielt auf die Standardisierung LDAP-konformer Verzeichnisschemata für die europäische Forschungsgemeinschaft. Es liegt der Abschlussbericht einer Bedarfsanalyse vor, in deren Ergebnis die Notwendigkeit der Definition einer Objektklasse EducationalPerson unter Beachtung europäischer Spezifika nachgewiesen wurde [3].

2.2 eduPerson

Die Objektklasse eduPerson der Internet2 Middleware Architecture Committee Directory Working Group (MACE-Dir) erweitert das Standardschema um hochschulspezifische Aspekte. Die Ergebnisse umfassen aber auch Empfehlungen zur Strukturierung des Verzeichnisbaums und zur Verwendung von Standardattributen. Leider berücksichtigen die Standardisierungsbemühungen der Arbeitsgruppe MACE-Dir im wesentlichen die Gegebenheiten an den Hochschulen der USA. So ist zum Beispiel der Spitzname einer Person als Attribut eduPersonNickName Bestandteil der Objektklasse eduPerson, wogegen für den akademischen Titel kein Attribut mit passender Semantik existiert [4].

2.2 auEduPerson

Ein Projekt australischer Bibliotheken, West Australian Libraries Authentication Project (WALAP), befasst sich mit dem Aufbau einer Infrastruktur für den autorisierten Zugriff auf elektronische akademische Ressourcen. Ein Design-Dokument [5] definiert Verzeichnisstrukturen und die Objektklasse auEduPerson mit interessanten Attributen nicht nur für die Benutzerverwaltung in Bibliotheken. Gegen eine direkte Verwendung von auEduPerson spricht die Definition als strukturelle Objektklasse. Den Standard erweiternde Objektklassen sollten als zusätzliche Objektklassen vom Typ `auxiliary` definiert sein und die Struktur des Verzeichnisbaums nicht beeinflussen.

3 Meta View und Objektklassen elektronischer Verzeichnisse

Eine der Hauptaufgaben des Meta Directory ist die Bereitstellung einer integrierten, einheitlichen Sicht auf Identitätsinformationen aus mehreren angeschlossenen Datenquellen zur Unterstützung hochschulweiter Verwaltungsprozesse. Die digitale Identität eines Hochschulangehörigen umfasst neben den anwendungsspezifischen Identifikatoren auch Funktionen und Rollen, die zunächst im Meta View integriert, später auf Rechte in den Netzwerkanwendungen abgebildet werden. Analyse und Entwurf haben gezeigt, dass Standard-Objektklassen und –Attribute für den Meta View einer hochschulorientierten Benutzerverwaltung nicht ausreichen.

3.1 Meta View

Die Abbildung 2 fasst den herstellerübergreifend anerkannten, allgemeinen Aufbau eines Meta Directory zusammen. Der Meta View entsteht im Ergebnis eines Join-Prozesses und repräsentiert eine einheitliche Sicht auf Verzeichnisobjekte, deren Daten sich durch Synchronisation mit den über Konnektoren angeschlossenen Datenbanken und Verzeichnissen ergeben. Bei dem Synchronisationsprozess fasst die Join Engine in Abhängigkeit von Arbeitsabläufen und Regeln ein bis mehrere Teilsichten auf die angeschlossenen Datenquellen zusammen. Jeder Connector prägt seine verzeichnisgetriebene Sicht, den Connector View, auf die Daten aus. Die Vereinigung aller Connector Views ergibt dann den Meta View.

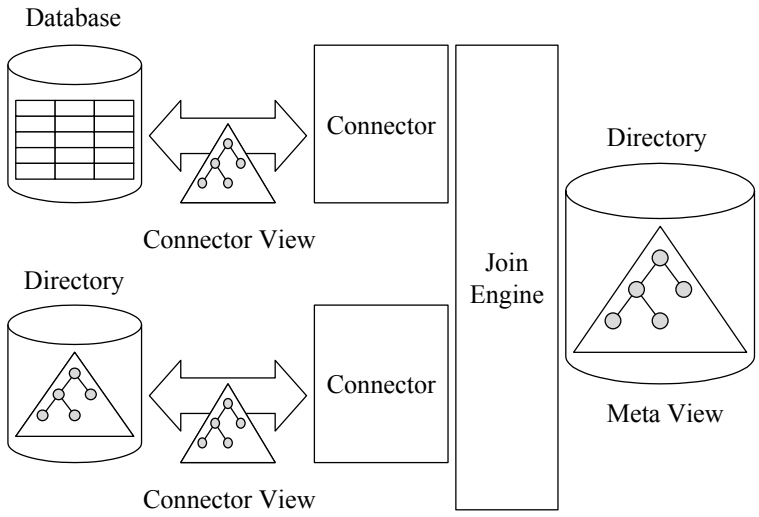


Abb. 2. Allgemeiner Aufbau eines Meta-Directory.

Verzeichnisgetriebene Sichten auf Daten lassen sich über Objektklassen und Attribute sowie über Verzeichnisstrukturen modellieren. Die Abbildung von Informationen auf die Struktur des Verzeichnisbaums ist für ein Meta Directory weniger relevant, da

Veränderungen der Baumstruktur in der Praxis sehr problematisch sind und bei der Vielzahl von zu unterstützenden Anwendungen kaum eine Struktur zu finden ist, die allen Anforderungen gerecht wird.

3.2 Verwendung und Definition von Objektklassen und Attributen

Ausgehend von einer Analyse der Datenflüsse, der Diskussion möglicher Szenarien und der Betrachtung ähnlich gelagerter Projekte in den USA, Australien und Europa wurden die Verzeichnis- und Datenstrukturen für den integrierenden Verzeichnisdienst an den Thüringer Hochschulen spezifiziert. Zunächst gingen die Bemühungen von einer Abbildung der Daten auf die Standardobjektklassen person (X.521), organizationalPerson (X.521) und inetOrgPerson (RFC 2256) aus. Ein weiteres wichtiges Ergebnis ist die Objektklasse Thuringian Educational Person, kurz thuEduPerson. Diese Objektklasse nimmt Attribute für den Meta View auf, die nicht im Standard und in der Objektklasse eduPerson (MACE-Dir) enthalten sind. In einem Prozess, der mit der Arbeit eines Standardisierungsgremiums zu vergleichen ist, einigten sich die beteiligten Einrichtungen auf relevante Attribute für die Verwaltung von Benutzern in einem Meta Directory. Die Spezifikation der Objektklasse thuEduPerson liegt in einem ersten Entwurf vor, der leider noch nicht von den zuständigen Gremien, Personalrat und Datenschutz, freigegeben wurde. Zunächst benötigt man zusätzliche Attribute zur eindeutigen Identifizierung einer Person an der Hochschule, wie zum Beispiel Familienname, Vorname, Matrikelnummer, eventuell auch Geburtsdatum, -ort und –name. Weiterhin besitzen Attribute, wie akademischer Grad, Strukturzugehörigkeit, Geschlecht oder Anrede, Kostenstelle, Befristung, Immatrikulationsdatum, Studiengang und Fachsemester eine große Relevanz für die Unterstützung hochschulinterner Prozesse.

4 Zusammenfassung und Ausblick

Die Ergebnisse der Analyse- und Entwurfsphase sind Ausgangspunkte für die Erstellung eines Pflichtenhefts für Consulting und Softwareentwicklung. Nach der unmittelbar bevorstehenden Produktauswahl erfolgt die Installation innerhalb der anvisierten Zielumgebung. Entsprechend der Prioritäten gehen als erstes die Konnektoren zu HISSOS und HISSVA in die Phase der Realisierung. Die Implementierung umfasst außerdem die Einrichtung des entworfenen Verzeichnisbaums und der Objektklassen, sowie weitere administrative Prozesse, wie zum Beispiel die produktspezifische Formulierung der Zugriffsrechte. Der Implementierungsprozess läuft innerhalb der Zielumgebung parallel zum produktiven Arbeitsbetrieb. Bis zum Beginn des Wintersemesters 2003 sollen die relevanten Daten der Studenten aus HISSOS übernommen werden können. Nach der Umsetzung des Konnektors zu HISSVA ist als nächstes der Authentisierungsserver zu installieren und die zugehörigen Synchronisationsmechanismen zu implementieren.
Der Implementierung schließt sich eine umfangreiche Testphase an. Auf Grundlage der entwickelten Workflow-Szenarien werden Testfälle generiert, um möglichst alle implementierten Funktionalitäten zu überprüfen.

Mit der Einführung in das produktive Umfeld werden alle relevanten Daten aufgenommen und die umgesetzten Funktionalitäten aktiviert. Eine Schulung der beteiligten Mitarbeiter ist für spätere einfache Änderungen und die Überwachung des produktiven Betriebs unerlässlich.
Das Projekt Meta Directory geht Anfang 2004 in die Phase der Weiterentwicklung, Anpassung und Wartung. Gemäß der gesetzten Prioritäten werden weitere Verwaltungsanwendungen integriert, was in Abstimmung mit den beteiligten Projektpartnern zum erneuten Durchlaufen der einzelnen Projektphasen führt. Wichtig ist die Integration der Bibliotheksverwaltung PICA und der dezentralen Benutzerverwaltungen in den Fakultäten. Der Einsatz eines Meta Directory lässt einen kontinuierlichen Prozess erwarten. Hierunter fällt die Anpassung an sich verändernde Bedingungen, wie zum Beispiel neue Softwareversionen der integrierten Applikationen oder sich verändernde Arbeitsprozesse.
Parallel zu allen Projektphasen müssen aktuelle Entwicklungen der Meta-Directory-Technologie verfolgt werden. Neue Standards, wie zum Beispiel das Role-based Access Control (RBAC), ermöglichen die Abbildung komplexer Regelwerke (Policies) und Rollenmodelle auf die Zielsysteme. In Verbindung mit den operationellen Datenbanken existieren hier komplexe Zusammenhänge. Ebenfalls auf der Tagesordnung steht die Gestaltung der Schnittstellen zu den anderen Projekten. Beispielgebend werden an der Technischen Universität Ilmenau im Rahmen der Initiative eCampus die Projekte Web-basierte Prüfungsverwaltung, webOffice mit Content Management System (CMS), Prozessoptimierung an Thüringer Rechenzentren und Meta Directory koordiniert. Ein Schwerpunkt ist die Gestaltung eines einheitlichen Portals für alle rechnergestützten Dienstleistungen einer Hochschule mit Single Sign On auf Basis der Verzeichnistechnologie. Aus dem Projekt Meta Directory heraus werden zukünftig Pilotapplikationen zur Demonstration der verzeichnisbasierten Authentisierung angeboten. Eine spätere Verbindung mit dem Aufbau einer Public Key Infrastruktur (PKI) ist analysiert und hängt vor allem von der Einrichtung einer Zertifizierungsinstanz ab.

5 Literatur

[1] M. Wahl, T. Howes, S. Kille. Lightweight Directory Access Protocol (v3). Network Working Group , RFC 2251, 1997

[2] Jörg Deutschmann. *Verzeichnisstrukturen im Rechenzentrum einer Hochschule*. Net.ObjectDays 2002, Tagungsband S. 637-642

[3] Peter Gietz. *Report on the Results of the DEEP questionnaire*. DAASI International Ltd. http://www.daasi.de/projects/DEEP/DEEPFinalReport, 10. Dezember 2002

[4] Internet2 Middleware Architecture Committee Directory Working Group (MACE-Dir). *EduPerson Object Class Specification (200210)*. http://www.educause.edu/eduperson/, Oktober 2002

[5] Computer Associates. *WALAP Directory Design Document Version 1.1*. http://john.curtin.edu.au/walap/docs/, 20. August 2002