Verzeichnisstrukturen im Rechenzentrum einer Hochschule

Jörg Deutschmann

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

Kurzfassung. Das Lightweight Directory Access Protocol (LDAP) entwickelt sich ähnlich dem Hypertext Transfer Protocol (HTTP) zu einem Basisprotokoll für Internetanwendungen mit breiter Unterstützung durch die Anbieter und Hersteller. Inspiriert durch dieses Integrationspotential entwickeln sich Verzeichnisdienste immer mehr zu Kernkomponenten für internetbasierte Informations- und Kommunikationsinfrastrukturen. Detaillierte Analysen und erste Erfahrungen bei der Bereitstellung einer solchen Infrastruktur lassen konkrete Rückschlüsse auf den Entwurf von integrierenden Verzeichnisstrukturen im Umfeld einer Hochschule zu.

1 Motivation und Einführung

Das Studium an den Hochschulen wird zunehmend durch die Möglichkeiten ihrer vernetzten Rechnerumgebungen geprägt. Applikationen auf Basis der Internet-Technologie beeinflussen dabei nicht nur das Lehren und Lernen, sondern auch die Prozesse der Organisation sowie der Verwaltung. Es entstehen komplexe Systeme, welche die Akteure, also die Studenten, die Lehrenden und andere Angestellte in zentralen und dezentralen Bereichen, bei ihren Tätigkeiten, wie zum Beispiel dem Wissenserwerb, der Wissensvermittlung, der Bereitstellung von Literatur sowie der Prüfungsverwaltung, unterstützen. Die Aufgabe des Rechenzentrums einer Hochschule besteht nun darin, hierfür eine geeignete rechnergestützte Infrastruktur zu konzipieren und schließlich auch bereitzustellen. Im Rahmen des Projekts „E-Campus an der Technischen Universität Ilmenau“ entsteht unter der Federführung des Universitätsrechenzentrums ein Konzept für eine integrierte, multimedial orientierte Informations- und Kommunikationsinfrastruktur. Dieses Konzept beschreibt einen in sich geschlossenen Ansatz ausgehend von den netztechnischen Grundlagen über notwendige Basisdienste bis hin zur Unterstützung von Lehre, Forschung und Entwicklung. Ein wichtiges Ergebnis der konzeptionellen und praktischen Tätigkeit ist die zunehmende Bedeutung eines elektronischen Verzeichnisses als ein grundlegender Basisdienst und integrierendes Element innerhalb der sich entwickelnden Infrastruktur. Ausgehend von diesem Integrationspotential entwickelt sich der Prototyp eines Corporate Directory an der Technischen Universität Ilmenau [6], auch inspiriert durch Lösungen an anderen Einrichtungen, zu einer Verallgemeinerung für Verzeichnisstrukturen im Rechenzentrum einer Hochschule.

2 Szenario für den Einsatz eines integrierenden Verzeichnisses

Für die Einführung eines integrierenden Verzeichnisses an einer Hochschule wurde ausgehend von den Anforderungen ein komplexes Szenario entwickelt. Die Abbildung 1 gibt einen vereinfachten Überblick über das Vorhaben mit Anwendungen in den Aufgabenbereichen des IT-Managements, der Verwaltungsdatenverarbeitung und der Bibliotheksverwaltung.

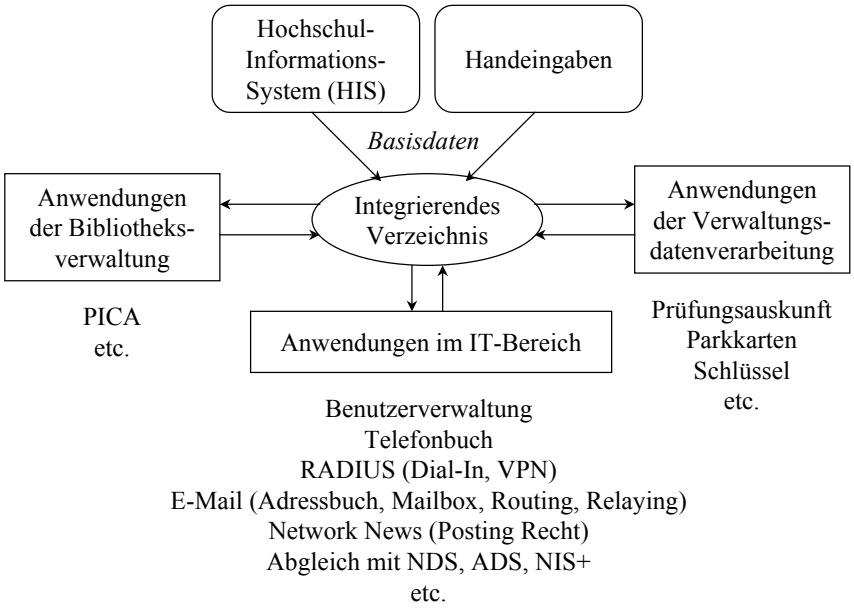


Abb. 1. Szenario für die Einführung eines integrierenden Verzeichnisses.

In einer ersten Phase geht es innerhalb des Projekts um die Gewinnung der Basisdaten für Mitarbeiter und Studenten aus den operationellen Datenbanken der Verwaltungsdatenverarbeitung. Hier muss ein Konnektor zu dem an vielen Hochschulen im Einsatz befindlichen Hochschul-Informations-System (HIS) entwickelt werden. Die Aufnahme von Basisdaten, wie zum Beispiel Namen und Adressen, sollte aber auch über eine spezielle Verzeichnisapplikation in Form von sogenannten Handeingaben möglich sein. Den Schwerpunkt der zweiten Phase bilden die Anwendungen im IT-Bereich. Ein wirklich aktuelles elektronisches Telefonbuch setzt einen Konnektor zur Verwaltungs-Software der TK-Anlage voraus. Die Benutzerverwaltung für entfernte Einwahl (Dial-In), Virtual Private Network (VPN), E-Mail und Network News ist bereits über ein elektronisches Verzeichnis sichergestellt. Dieses aktualisiert seine Daten zukünftig mit Hilfe des angestrebten integrierenden Verzeichnisdienstes, wobei für den Konnektor umfangreiche Workflows zur Lösung der Managementaufgaben in einem Rechenzentrum umzusetzen sind. Für den Abgleich mit den betriebssystemorientierten Verzeichnissen, NDS, ADS und NIS+, existieren bereits Lösungen im Rahmen

kommerzieller Produkte, wie zum Beispiel Siemens DirX Metahub oder Novells DirXML. Die dritte Phase des Projekts zielt auf die Verwirklichung von Anwendungen der Verwaltungsdatenverarbeitung und der Bibliotheksverwaltung ab. In der Diskussion befinden sich hier die Autorisierung von Studenten zur Rückmeldung und Prüfungsauskunft, die Parkkarten- und Schlüsselausgabe an Mitarbeiter sowie ein Abgleich mit dem Bibliotheksverwaltungssystem PICA.
Das Projekt orientiert sich an der in [6] vorgestellten Vorgehensweise und befindet sich derzeit in der ersten Phase. Hier stehen unter anderem grundsätzliche Entscheidungen zur Struktur des Verzeichnisses im Mittelpunkt der Betrachtungen, von denen ausgewählte Ergebnisse im folgenden diskutiert werden.

3 Verzeichnisbaum und Datenstrukturen

Die Entwicklung der Verzeichnisstruktur und des Namensmodells stellt den wichtigsten Entwurfsschritt für ein elektronisches Verzeichnis dar. Ausgangspunkt sind die im Rahmen des Projekts formulierten Entwurfsziele. Hierzu zählen die gute Unterstützung der Datenpflege, flexible Möglichkeiten der Anbindung von Verzeichnisapplikationen, die einfache Administrierbarkeit und vor allem die hohe Robustheit gegenüber Veränderungen im Umfeld des integrierenden Verzeichnisses. Für den Entwurf des Verzeichnisses müssen die Struktur des Verzeichnisbaums, Festlegungen für Distinguished Names, Namenskonventionen sowie Entscheidungen für Objektklassen und ihre Attribute betrachtet werden. Die folgenden Abschnitte setzen sich mit diesen vier Aspekten auseinander.

3.1 Struktur des Verzeichnisbaums

Die für den Aufbau des Verzeichnisbaums verwendeten Container orientieren sich an den Standards für LDAP und X.500. Für die obersten zwei Hierarchiestufen kommt das LDAP-konforme `dcObject` (Domain Component) zum Einsatz, so dass sich zum Beispiel `dc=TU-Ilmenau, dc=de` ergibt. Dieser LDAP-Style unterstützt eine spätere Suche und eventuell diverse E-Mail-Applikationen [3]. Eine Fortsetzung findet die Hierarchie durch den X.500-konformen Container `ou` (Organizational Unit). Die weitere Strukturierung geht in Anlehnung an RFC 2377 [2] von einem möglichst flachen, funktionell orientierten Ansatz aus. Diese Vorgehensweise verspricht eine hohe Robustheit gegenüber organisatorischen Veränderungen innerhalb einer Hochschule. Alle an der TU Ilmenau verzeichneten Personen sind dann zum Beispiel unter der Basis `ou=Mitglieder, dc=TU-Ilmenau, dc=de` zu finden. Wichtige Informationen bezüglich der Hochschulstruktur lassen sich in speziell dafür vorgesehenen Attributen (siehe 3.3) verankern.

3.2 Distinguished Names

Distinguished Names erlauben die eindeutige Identifikation von Einträgen innerhalb eines Verzeichnisses, in diesem betrachteten Anwendungsfall von Personeneinträgen. Es existieren verschiedene Attribute, die zur eindeutigen Identifikation von Einträgen in Frage kommen [4]. Weit verbreitet ist die Verwendung von `cn` (Common Name), `uid` (User Identifier) und `mail` (E-Mail-Adresse). Jedes dieser Attribute eignet sich für bestimmte Anwendungsfälle und besitzt bestimmte Eigenschaften bezogen auf Lesbarkeit, Wertebereich, Eindeutigkeit usw. Für ein Verzeichnis mit stark integrierendem Charakter sowie zahlreichen Anwendungen empfiehlt sich ein Namensattribut, das von den angeschlossenen Applikationen abstrahiert und bei der angestrebten flachen Strukturierung eine geringe Wahrscheinlichkeit für Namenskollisionen bietet. Im Rahmen dieses Projekts soll deshalb ein abstrakter Identifikator in Form eines möglichst zufällig erzeugten Universal Unique Identifier (UUID) zum Einsatz kommen. Als Attribut bietet sich entweder eine eigene Erweiterung oder das zu diesem Zweck von der Arbeitsgruppe ldap-bis bei der Internet Engineering Task Force (IETF) vorgeschlagene `dnComp` bzw. `dnComponent` an. Mit der Syntax eines Directory-String verspricht es eine hohe Flexibilität. Unter diesen Umständen wäre dann zum Beispiel `dnComponent=3D76E207B6D511D2B16900105A397F67, ou=Mitglieder, dc=TU-Ilmenau, dc=de` ein gültiger Distinguished Name mit dem Wert einer 128 Bit großen Zufallszahl im Namensattribut einer Person.

3.3 Objektklassen und Attribute

Für die Verzeichnisstrukturen an einer Hochschule sollen zunächst die von X.500 bzw. LDAP vorgegebenen Standards herangezogen werden. Die hier spezifizierten Schemata enthalten Objektklassen und Attribute, die schon einen großen Teil der Anforderungen einer Benutzerverwaltung abdecken. Insbesondere handelt es sich um die Objektklassen `person` (X.521), `organizationalPerson` (X.521) und `inetOrgPerson` (RFC 2256). Es können dabei Ergänzungen für Attributsemantiken und Verwendungen in Abhängigkeit von neuen Anwendungen erfolgen. Eine Wiederverwendung der Standardattribute für völlig andere Semantiken und Verwendungen ist jedoch im Sinne bereits etablierter Verzeichnisapplikationen zu vermeiden. Die notwendigen Erweiterungen des Verzeichnisschemas betreffen hochschulspezifische und –interne Aspekte. Einen ersten Ansatz für die Spezifika der Benutzerverwaltung an einer Hochschule bietet die Objektklasse `eduPerson` [5]. Für diese Objektklasse sind Attribute definiert, welche die Beziehung einer Person zur jeweiligen Bildungseinrichtung zum Ausdruck bringen, ihre Einordnung in die Universitätsstruktur und eine hochschulspezifische Rechtevergabe ermöglichen. Alle weiterführenden Anwendungen, die nicht durch Standards oder die Objektklasse `eduPerson` zu realisieren sind, verlangen nach hochschulinternen Erweiterungen. Um einen Überblick über das aktuell in Verwendung befindliche Verzeichnisschema zu bekommen, existiert ein Repository. Es enthält strukturierte Informationen zu den einzelnen Objektklassen und Attributen, wie zum Beispiel eine Syntaxdefinition nach RFC 2252 [1], eine informale Beschreibung der Semantik, Hinweise zur Indexierung,

Beispiele und Anmerkungen. Zu dem Zweck der Einführung neuer Applikationen sind auch Vorschläge für die Erweiterung des Schemas in diesem Format zu liefern, die dann diskutiert und bestätigt werden können.

3.4 Namenskonventionen

Namenskonventionen für Verzeichnisstrukturen sind sehr vielgestaltig. Sie beziehen sich zum einen auf die Benennung der Objektklassen und Attribute. Zum anderen führen Namenskonventionen zu Festlegungen bezüglich der Werte von Attributen. Prinzipiell sollte für Namen immer ein Kompromiss zwischen Aussagekraft und Kürze gefunden werden.
Bei der Benennung von Objektklassen und Attributen bietet es sich an, hochschulinterne Erweiterungen durch einen festen Präfix gegenüber dem Standardschema zu kennzeichnen. So besitzen alle Schemaerweiterungen an der TU Ilmenau den Präfix `tui`, beispielsweise auch die Objektklasse `tuiEduPerson` für die Verwaltung der Personen an der Technischen Universität Ilmenau.
Namenskonventionen bezüglich der Werte von Attributen hängen sehr stark von den jeweiligen Anwendungen ab. Auf oberster Ebene des bereits diskutierten Verzeichnisbaums orientiert man sich am Domain Name System (siehe 3.1). Für einige Attribute ist eine Kategorisierung notwendig, woraus sich ein definiertes Vokabular bzw. feste Werte ergeben. Zum Beispiel spezifiziert das Attribut `eduPersonAffiliation` die Beziehung einer Person zur Lehreinrichtung [5], was durch die fest vorgegebenen Werte Mitarbeiter, Student, Gast, Alumni zum Ausdruck gebracht wird.
Bestimmte Anwendungen können Regeln für die Struktur der Werte von Attributen erfordern. Such– und Sortierfunktionen beziehen sich oft auf das Attribut `cn` (Common Name), für dessen Werte folgende Regeln spezifiziert werden: Der Common Name setzt sich zusammen aus dem Familiennamen und allen Vornamen einer Person getrennt durch Leerzeichen. Um eventuelle Titel und Spitznamen für eine spätere Suche mit aufzunehmen, kann `cn` mehrere Werte besitzen. Eine angenommene Person Dr. Johannes Maria Knoll, genannt Knolle, ergibt dann `cn="Knoll Johannes Maria"; cn="Dr."; cn="Knolle"`. Auch Telefonnummern tauchen immer wieder in unterschiedlichen Formaten auf, obwohl Festlegungen existieren, die nur Leerzeichen zur Abtrennung von Bereichen zulassen.
Bildungsvorschriften für Benutzerdaten, die bei der Aufnahme in das Verzeichnis generiert werden, gehören ebenfalls zu den Namenskonventionen. Zu generierende Basisdaten sind im Rahmen dieses Projekts der Login-Name, ein initiales Passwort und die E-Mail-Adresse. Während Login-Name und E-Mail-Adresse Eindeutigkeit verlangen, sollte das Passwort den Wörterbuchangriffen standhalten. Für Login-Name und E-Mail-Adresse wird Lesbarkeit angestrebt. Von Interesse ist auch die Frage, wie viel Strukturinformationen eine E-Mail-Adresse enthält. Die Lösung an der TU Ilmenau, lediglich zwischen Mitarbeitern, `@TU-Ilmenau.de`, und Studenten, `@Stud.TU-Ilmenau.de`, zu unterscheiden, hat sich als sehr robust gegenüber organisatorischen und strukturellen Veränderungen erwiesen.
Die einzelnen Regeln und Festlegungen zu Namenskonventionen werden im Repository (siehe 3.3) für die jeweiligen Attribute und Objektklassen verankert.

4 Zusammenfassung und Ausblick

Die Einführung eines integrierenden Verzeichnisdienstes als Kernkomponente einer Informations- und Kommunikationsinfrastruktur stellt einen kontinuierlichen Prozess dar. Neben der Kosteneinsparung, einer höheren Produktivität und Sicherheit verspricht der Einsatz des Verzeichnisses vor allem eine bessere Erweiterbarkeit der Infrastruktur mit Blick auf neue Applikationen sowie eine höhere Qualität der durch die Strukturierung konsolidierten Daten. Die für das Verzeichnis gewählte Struktur, das Schema und die Namenskonventionen bestimmen seine Praktikabilität als integrierendes Element in einer Infrastruktur maßgeblich. Aus diesem Grund wurde innerhalb des vorgestellten Entwurfs der Verzeichnisstrukturen, auch aus den Erfahrungen anderer Projekte heraus, vor allem auf eine hohe Robustheit gegenüber organisatorischen, strukturellen und anwendungsspezifischen Variationen geachtet. Ausgangspunkt der Entwicklung sind immer die Standards X.500 und LDAP.
Während der Verzeichnisentwurf mit Hilfe einer Open-Source-Lösung bereits umgesetzt ist, werden momentan die Konnektoren zu den Zielsystemen möglichst implementierungsneutral beschrieben. Bereits beim ersten zu spezifizierenden Konnektor zum Hochschul-Informations-System (HIS) zeigen sich Rückwirkungen auf das Schema des Verzeichnisses in Form von aufzunehmenden Schlüssellisten, zum Beispiel zur Abbildung von Studiengängen. Ebenfalls Bestandteil der Spezifikation ist ein Sicherheitskonzept, das bei jedem Konnektor überprüft werden muss. Die Festlegung von Zugriffsrechten soll zukünftig basierend auf Gruppenzuordnungen erfolgen. Derzeit befinden sich hierfür Kategorisierungen, Namenskonventionen und Erweiterungen des Verzeichnisbaums in der Diskussion.

5 Literatur

[1] M. Wahl, A. Coulbeck, T. Howes, S. Kille. *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*. Network Working Group, RFC 2252, Dezember 1997

[2] A. Grimstad, R. Huber, S. Sataluri, M. Wahl. *Naming Plan for Internet Directory-Enabled Applications*. Network Working Group, RFC 2377, September 1998

[3] Michael R Gettes. *A Recipe for Configuring and Operating LDAP Directories*. Georgetown University, Georgetown Institute for Information Assurance, Internet2 Middleware Initiative, http://middleware.internet2.edu, 07.05. 2002

[4] Richard Jones, Tom Barton u.a. *Metadirectory Practices for Enterprise Directories in Higher Education*. Released for Public Review, Internet2 Middleware Initiative http://middleware.internet2.edu, Mai 2002

[5] Keith Hazelton. *EduPerson Object Class Specification, Version 1.5*. Released for Public Review, Internet2 Middleware Initiative http://middleware.internet2.edu, Mai 2002

[6] Jörg Deutschmann. *Meta Directory – integrierendes Element in einer verteilten, heterogenen IT/TK-Landschaft*. Net.ObjectDays 2001, Tagungsband S. 321-326