T. Hildmann und C. Ritter

TUBIS – Integration von Campusdiensten an der Technischen Universität Berlin

Dipl.-Inform. *Thomas Hildmann* arbeitet im tubIT IT-Service-Center der Technischen Universität Berlin. Seit mehr als 7 Jahren ist er im Bereich IT-Sicherheit tätig. Dabei arbeitete er in mehreren internationalen und nationalen Projekten auf diesem Gebiet. In verschiedenen Projekten befasste er sich mit dem Bereich rollen-basierte Zugriffskontrolle (RBAC). Im Jahr 2000 richtete er als Local Chair den 5. ACM Workshop on Role-based access control in Berlin aus. Im Campuskartenprojekt arbeitete er an einer smartcardbasierten Infrastruktur, wobei sein Schwerpunkt auf Sicherheitskonzepten und Firewalls sowie der Integration von kontaktlosen Anwendungen (MIFARE) lag. Zur Zeit arbeitet er an seiner Promotion im Bereich RBAC und an Sicherheitsinfrastrukturkomponenten in der Arbeitsgruppe Benutzerdienste.

Dipl. Inform. *Christopher Ritter* arbeitet im tubIT IT-Service Center der Tenchnischen Universität Berlin. Seit mehr als sieben Jahren ist er im Bereich IT-Sicherheit tätig. Dabei arbeitete er in diesem Bereich zunächst bei der T-Systems International in mehreren nationalen und internationalen Projekten. Die Projekte umfassten u.a. die Themengebiete Sicherheitsplatformen, Smartcard Infrastrukturen, PKIs sowie biometrische Verfahren. 2003 wechselte er im Rahmen des Campuskarten Projektes an die Technische Universität Berlin. Nach Abschluss des Projektes beteiligte er sich an der Entwicklung eines Organisationsweiten Identitätsmanagement Systems für die TU-Berlin (TUBIS). Zur Zeit leitet er die Entwicklung des TUBIS Kernsystems und arbeitet an seiner Promotion im Bereich IDM.

tubIT ist das zentrale IT-Service-Center der Technischen Universität Berlin, das durch Zusammenschluss der Zentraleinrichtung Rechenzentrum (ZRZ) und des Fachbereichsübergreifenden Forschungsschwerpunkts (FSP-PV) Prozessrechnerverbundzentrale (PRZ) entstanden ist. tubIT bietet allen Mitarbeiterinnen und Mitarbeitern sowie allen Studierenden ein vielfältiges Informations-, Beratungs- und Dienstleistungsangebot.

ZUSAMMENFASSUNG

Die IT Landschaft der Universitäten ist historisch gewachsen. Unterschiedliche Abteilungen und Fakultäten haben jeweils für sie optimale Softwarelösungen ausgewählt und in ihre Arbeitsabläufe integriert. Die aktuellen Anforderungen an die Universitäten erfordern eine Integration der unterschiedlichen Insellösungen. Die TU-Berlin setzt hierbei auf ein eigenes Produkt, das auf Basis verschiedener Open Source-Lösungen erstellt wurde und stetig erweitert wird. Dabei werden nicht nur Daten zusammengeführt, sondern auch ein universitätsweites, rollenbasiertes Rechtesystem etabliert, das sich, wie bereits gezeigt, in unterschiedliche Anwendungen integrieren lässt.

1 EINLEITUNG

TUBIS ist ein rollen-basiertes Identitymanagement System an der TU-Berlin. Es dient der Zusammenführung verschiedener Datenquellen (Metadirectory) und hält ein rollen-basiertes Zugriffsmodell. Dieses Modell wird zum einen zum Schutz der Attribute aus dem Metadirectory, aber auch zur Verwaltung des Rollenmodells selbst genutzt. Damit ist es möglich, die Vergabe von Rollen und damit auch Rechten aufzuteilen. Die Arbeiten der jeweiligen Experten (Anwendungsbetreiber, Personalstelle und Studierendenverwaltung, Abteilungen und Arbeitsgruppen) werden konzentriert, dabei wird eine zentrale Sicherheitspolitik umgesetzt. Der Rollenansatz ist hierbei eine gute Metapher, die auf den unterschiedlichen Ebenen in Verwaltung und IT verstanden wird. Die Herausforderung besteht darin, jedem Benutzerkreis eine jeweils verständliche Sicht auf das Modell zu ermöglichen.

Die Integration unterschiedlichster Datenquellen und Anwendungen stellt die zweite große Aufgabe für das neue System dar. Es konnte jedoch an den ersten wesentlichen Beispielen, nämlich an der Integration der Daten aus Studierendenverwaltung und Personalstelle sowie der Integration in verschiedene Anwendungen gezeigt werden, dass eine solche Integration möglich ist und tatsächlich die erhofften Mehrwerte liefert.

Die Integration von immer weiteren Diensten und Datenquellen ist Mittel zur Optimierung von Prozessen an der TU-Berlin. Mit dem Abholen des Studierenden- oder Mitarbeiterausweises soll eine Person dem System bekannt sein. Anhand der bereits zur Einstellung oder Immatrikulation erfassten Daten können die ersten Rollen automatisch ermittelt werden und somit unmittelbar ein Zugriff auf Ressourcen ermöglicht. Ebenso werden Rollen mit der Exmatrikulation oder der Beendigung des Arbeitsverhältnisses angepasst und so verhindert, dass auf Grund langsamer oder unzureichender Synchronisation von Daten Sicherheitslücken entstehen.

Für den Studierenden bedeutet die Einführung von TUBIS eine zentrale Anlaufstelle für die Belange des Studiums. Denn mit TUBIS folgt auch ein Webportal, das die unterschiedlichen Dienste an der TU-Berlin bündelt. Für die Mitarbeiter bedeutet vor allem die rollen-basierte Zugriffskontrolle schnelleren und flexibleren Zugang zu nötigen Ressourcen und eine flexiblere Arbeitsverteilung. Für alle ergeben sich Arbeitserleichterungen durch geregelten Datenzugriff ohne Verzögerungen, Automatisierung von Zugriffsbelangen wo dies möglich ist und Transparenz bezüglich der Verwendung der eigenen personenbezogenen Daten.

1.1 Ist-Zustand

Mit dem Ende der Großrechner-Ära endete an der TU-Berlin, wie in fast allen größeren Organisationen, der Zeitpunkt, an dem die Entwicklung der IT-Landschaft über „einen Masterplan“ gesteuert wurde. PCs und später Client-Server-Systeme brachten viele Freiheiten und beschleunigten die Entwicklung auf diesem Sektor. Das Ergebnis waren jedoch viele unabhängige Systeme unterschiedlicher Abteilungen und Fakultäten, die einen ständigen Daten-Im- und Export, Konvertierungen und redundante Datenhaltungen erforderten. Benutzerdaten müssen auf jeder Plattforminsel doppelt gewartet werden. Viele mögliche Synergieeffekte und Potentiale der EDV gehen dabei verloren, inkonsistente Daten sind die Folge.

Für den Benutzer stellt sich die Organisation als Inselkette unterschiedlicher Staaten dar, auf der man, sinnbildlich gesprochen, jeweils ein neues Visum beantragen muss. Mitarbeiter können auf dringend benötigte Ressourcen nicht oder nicht schnell genug zugreifen.

Aber auch für Studierende ergeben sich Probleme, die durch bessere Integration mindestens in Teilen reduziert werden könnten. So sind wichtige Informationen evtl. einfach am „anderen schwarzen Brett“ zu finden oder wegen versäumter Fristen ist eine „Extrarunde“ fällig. Einige Studierende haben das Gefühl, Scheine dafür zu bekommen, dass sie Formulare von A nach B befördern. Gerade durch neue Optionen im Studium wird der Ruf nach mehr Übersicht und Automatisierung auch für den Studierenden laut. In Zukunft wird die Qualität einer Universität auch an den Laufzeiten ihrer Verwaltungsprozesse gemessen werden.

1.2 Anforderungen

Der Wunsch nach Datenkonsolidierung an der TU-Berlin entstand parallel aus sehr unterschiedlichen Interessen.

So ging es auf der einen Seite um die Erstellung eines TU Adressbuches mit aktuellen Raum- und Telefonnummern sowie E-Mailadressen. Die Rundschreiben sollten nach Möglichkeit schon aus rein ökologischen Gründen elektronisiert werden. Die Benutzerverwaltung für unterschiedliche Dienste sollte zentralisiert werden. Neben dem hohen administrativen Aufwand, der für alle Systeme parallel entsteht, stellt sich auch die Frage nach der Berechtigung der Personen. Administratoren sind gar nicht in der Lage, einen Stamm von 30.000 Studierenden auf dem aktuellen Stand zu halten und das für jede Anwendung getrennt. Ob der Anrufer, der einen Zugang zu sensiblen Daten verlangt, wirklich der Mitarbeiter ist, der er vorgibt zu sein, lässt sich ohne weiteres nicht prüfen. Hierfür müssen Werkzeuge geschaffen werden! Gefordert ist eine organisationsweite Verwaltung von Identitäten und deren Rollen bzw. Funktionen. Die Verwaltung darf nicht an einem Administrator oder einem Team hängen, sondern soll mindestens in Teilen selbst administrierbar sein. Für die Authentisierung der Benutzer sollen auch Möglichkeiten zur Verfügung stehen, die über die Sicherheit von heute üblichen Benutzernamen und Passwörtern hinausreichen. Personendaten sollen nur einmal erfasst und in das System eingepflegt werden (Provisionierung). Nach Möglichkeit sollen ihnen sofort die nötigen Dienste zur Verfügung stehen. Gleiches gilt auch für die Deprovisionierung.

2 DAS TUBIS-SYSTEM

TUBIS steht für „Technische Universität Berlin Integrationsservice für Campusmanagement und Verwaltungsprozesse“. Hierbei handelt es sich um ein an der TU Berlin entwickeltes rollenbasiertes Identitätsmanagement System mit Metadirectory-Funktionalität. Ziel ist es, die verschiedenen Datenquellen zusammenzufassen und die Daten zum einen für die Authentisierung und Autorisierung von Benutzern zu nutzen. Ein weiteres Ziel ist, die die Person betreffenden Daten für die Anwendungen zur Verfügung zu stellen und dabei dem Benutzer ein möglichst hohes Maß an informationeller Selbstbestimmung zu gewährleisten. Dies geschieht durch den Rollenansatz, durch die konsequente Umsetzung der Datensparsamkeit und durch Transparenz.

3 DAS METADIRECTORY

Insbesondere personenbezogene Daten werden von mehreren unterschiedlichen Dienstanbietern an vielen Stellen benötigt. Häufig wurden diese Daten vor der Einführung von TUBIS manuell, unter Verwendung unterschiedlicher Medien, asynchron ausgetauscht. Zur Vermeidung redundanter und ggf. inkonsistenter Datenbestände sowie vieler unterschiedlicher, fehleranfälliger Zugriffswege auf primäre Datenquellen[1] dient TUBIS als zentrale Datenvermittlung für Anwendungen als Metadirectory. Die Daten werden dabei nicht im TUBIS vorgehalten, sondern erst zum Zeitpunkt des Zugriffs von den jeweiligen datenhaltenden Stellen abgerufen. Das TUBIS Modell hält anstelle der Daten, Referenzen zu flexiblen Adapterklassen, die den eigentlichen Zugriff auf die Datenbanken realisieren. Auf diese Weise werden u.a. Personendaten aus dem Personalmanagementsystem Loga oder der Studierendenverwaltung HIS SOSPOS bezogen. Abhängig davon, ob es sich bei der entsprechenden Person um einen Mitarbeiter oder einen Studierenden handelt, wird die entsprechende Primärquelle angesprochen. Änderungen an den primären Datenquellen können so zentral in Echtzeit verteilt werden und sind für die Datennutzer transparent. Der Zugriff auf die Daten wird über die rollen-basierte Zugriffskontrolle von TUBIS geregelt. Anwendungen erhalten immer nur Zugriff auf Daten, für die sie eine Genehmigung besitzen. Um die Vertraulichkeit und Integrität der Daten zu gewährleisten, wird zudem die gesamte Kommunikation über VPN-Tunnel geleitet. Die jeweiligen Dienste authentisieren sich mittels Zertifikaten am TUBIS.

1 Datenhaltende Stellen, die als Hauptverantwortliche für ein bestimmtes Datum gelten.

4 DIE ROLLEN-BASIERTE ZUGRIFFSKONTROLLE

Die Verwendung von rollen-basierter Zugriffskontrolle für das TUBIS System hat verschiedene Vorteile. Der Grundgedanke der rollen-basierten Zugriffskontrolle (RBAC, role-based access control) ist die Einführung einer Indirektionsschicht bei der Zuweisung von Rechten zu Benutzern [Sa96]. Statt einem Benutzer direkt Zugriff auf eine Ressource zu gestatten, werden die Benutzer zunächst in Rollen gruppiert. Die Rollen erhalten dann Zugriff auf die Ressource. Dies macht die Rechteverwaltung auch bei großen Benutzerzahlen, wie an der TU Berlin, erst realistisch. Im verwendeten Modell werden verschiedene Indirektionen über Rollenhierarchien verwendet. Hauptsächlich können sog. Geschäftsrollen von Anwendungs- und Zugriffsrollen unterschieden werden.

Die Geschäftsrollen werden in der Literatur auch Funktionen (job functions) genannt [Mi05]. Sie bezeichnen die Tätigkeit der Person innerhalb des Organigramms und sind im TUBIS-Modell jeweils Organisationseinheiten zugeordnet.

Jede Anwendung hat ihre eigene Sicht auf die Organisation. So muss eine Anwendung beispielsweise nur unterscheiden, ob es sich beim Benutzer um einen Studierenden oder einen Mitarbeiter handelt, wogegen eine andere Anwendung genauere Informationen über den Status der Person benötigt, um eine Autorisierungsentscheidung treffen zu können.

Zugriffsrollen sind schließlich eine eher technische Sicht auf eine Anwendung. Hierunter fallen z.B. „Tabellenverwalter“ oder „Transaktionsbeobachter“, die zwar einen sehr engen Bezug zur Anwendung besitzen, nicht jedoch unmittelbar zur Organisation. Dieser Bezug wird vom TUBIS über die Applikationsrolle hergestellt.

4.1 Das Modell der Technischen Universität Berlin

Eine der größten Herausforderungen bei der Realisierung eines organisationsweiten, zentralen Identitätsmanagement Systems ist der Entwurf des Modells. Das Modell muss nicht nur ein Abbild der organisatorischen Struktur besitzen, sondern auch die Mitglieder der Organisation, ihre Beziehungen innerhalb der Organisation sowie die angebotenen Dienste beinhalten. Dabei muss immer beachtet werden, dass zum einen nicht alle Dienste auf das TUBIS Modell angepasst werden können, zum anderen der Versuch, alle Dienste in ihrer Form im TUBIS Modell abzubilden, in einem unwartbaren und dennoch unvollständigen Modell endet. Das Ziel muss in der Mitte liegen. Das TUBIS Modell (siehe Abb. 1) der TU Berlin unterteilt sich in drei Abschnitte: Identitätssicht, Organisationssicht und Anwendungssicht.

Im Bereich der Identitäten werden die Personen der TU-Berlin abgebildet. Dabei wird zwischen Studierenden und Mitarbeitern unterschieden. Studierende besitzen einen Matrikeleintrag mit dem ein oder mehrere Studiengänge verbunden sein können. Mitarbeiter besitzen einen oder mehrere Verträge, denen jeweils eine Position innerhalb der Organisationsstruktur zugeordnet ist. Einen Spezialfall bildet hierbei der studentische Mitarbeiter, der sowohl einen Matrikeleintrag als auch einen Vertrag besitzt.

Die organisatorische Sicht beinhaltet sowohl die hierarchische Organisationsstruktur als auch die Vererbungshierarchie der organisatorischen Geschäftsrollen.

5 DIE WEBBASIERTE ROLLEN-ADMINISTRATION

Entsprechend dem Modell kann auch die grafische Administrationsoberfläche in drei Abschnitte unterteilt werden: der Anwendungsverwaltung, der Strukturverwaltung und der Selbstverwaltung. Die Verwaltungsoberflächen stellen für das TUBIS eine Anwendung dar, wodurch alle Zugriffe auf die Verwaltungsoberflächen ebenfalls durch Anwendungsrollen geregelt werden.

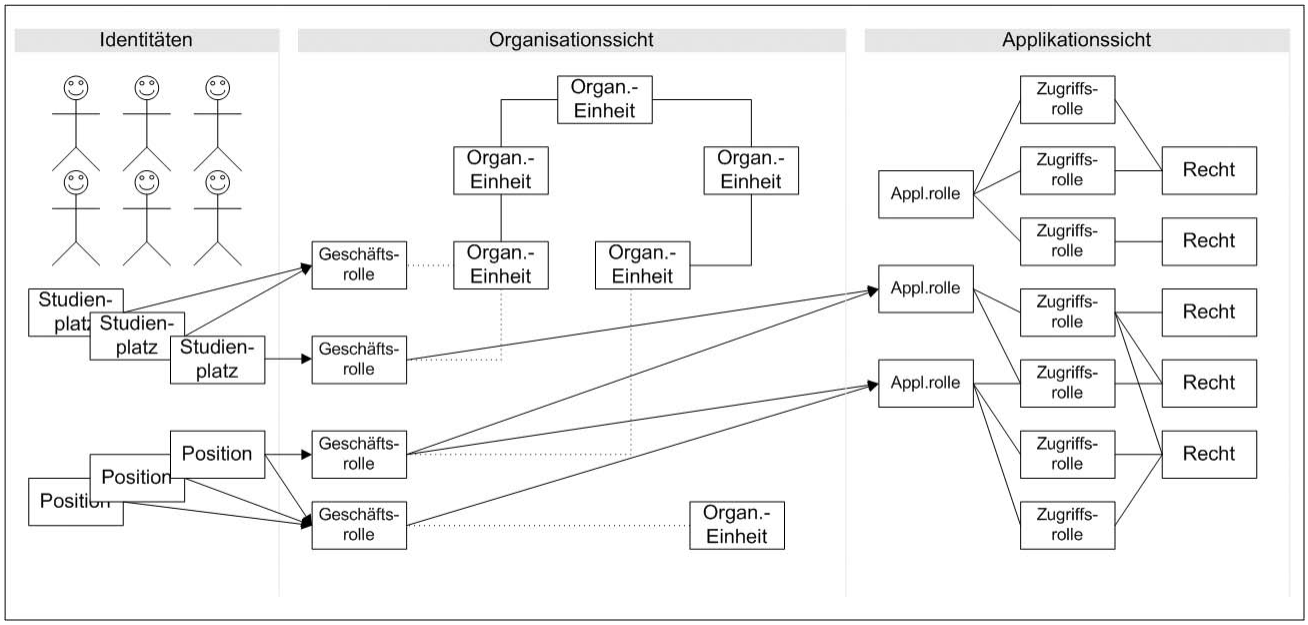

Abb. 1 Vereinfachtes TUBIS Modell

Abb. 2 Geschäftsrollenzuweisen in der Strukturverwaltung

5.1 Die Anwendungsverwaltung

Mit der Rolle des Anwendungsverwalters steht die Oberfläche der Anwendungsverwaltung zur Verfügung. Diese ermöglicht, neben dem Integrieren neuer Anwendungen in das Modell, das Definieren von Zugriffsrechten. Diese können zu Zugriffsrollen gebündelt werden, welche wiederum zu Anwendungsrollen gruppiert werden können.

Es ist der Anwendung überlassen, wie viel der Zugriffskontrolle ins TUBIS-Modell ausgelagert werden soll und wie viel Logik in der Anwendung selbst steckt. So gibt es Anwendungen, die allein die Zuordnung von Personen zu Anwendungsrollen von TUBIS verwalten lassen und andere Anwendungen, die auch die Rechteprüfungen in TUBIS durchführen lassen. Die Anwendung kann so selbst entscheiden, welcher Teil über die Benutzeroberfläche von TUBIS zentral administrierbar sein soll. So kann hier ggf. Programmieraufwand eingespart werden.

5.2 Die Strukturverwaltung

Die Rolle des Strukturverwalters ermöglicht dem Rollenmitglied den Zugriff auf die organisatorische Seite der Verwaltungsoberfläche, begrenzt auf die Organisationseinheit, für die man die entsprechende Rolle besitzt. Bezogen auf die jeweilige Organisationseinheit können hier Informationen über Mitglieder der Einheit angezeigt werden. Die in der Anwendungsverwaltung definierten Anwendungsrollen können spezifizierten, organisatorischen Geschäftsrollen zugewiesen werden. Ferner können Mitgliedern der Organisationseinheit diese Geschäftsrollen zugewiesen werden (siehe Abb. 2).

5.3 Die Selbstverwaltung

Jede Person, die im TUBIS geführt wird, besitzt die Rolle des Selbstverwalters. Diese ermöglicht den Zugriff auf die Oberfläche zur Selbstverwaltung. Hier wird dem Benutzer die Möglichkeit gegeben, eigene, persönliche Daten anzupassen und organisatorische Geschäftsrollen, in denen der Benutzer Mitglied ist, an andere Personen zu delegieren. Die Rollen-Delegation unterstützt dabei Monotonie[2], Multi-Stepping[3] und Permanenz[4] [Ba00].

5.4 Das TU-Portal

Einer der aktuellen Nutzer des TUBIS ist das TU-Portal. Dabei handelt es sich um eine personalisierte Seite innerhalb des unpersonalisierten Webauftritts der Technischen Universität Berlin. Das Portal bietet dem Nutzer persönliche Informationen, den direkten Zugang zu ihm verfügbaren (webbasierten) Anwendungen sowie die Möglichkeit der Selbstverwaltung. Um dies zu realisieren, fragt das Portal Daten über den Nutzer vom TUBIS ab, die es ermöglichen, den Nutzer persönlich anzusprechen (Anrede und Nachname) sowie eine Klassifizierung des Nutzers als Mitarbeiter oder Studierenden zu ermöglichen. Über eine spezielle Schnittstelle können vom TUBIS alle Anwendungen erfragt werden, für die ein bestimmter Nutzer eine (beliebige) Rolle besitzt. Das Portal stellt auf diese Weise nur Verweise auf Anwendungen zur Verfügung, die der Nutzer auch wirklich nutzen kann (siehe Abb. 3). Das aktuelle Portal bietet Zugriffe auf die TUBIS Oberflächen, HIS QISPOS, SuperX sowie einigen TU intern entwickelten Anwendungen zur Leistungsdatenerfassung und Kosten/Leistungs-Rechnung. Weitere Anwendungen sind bereits in Arbeit.

6 DIE SCHNITTSTELLEN

Gemäß den Anforderungen an ein Metadirectory stellt das TUBIS unterschiedliche Schnittstellen zur Datenabfrage zur Verfügung. Dabei werden zur Zeit zwei Protokolle unterstützt: LDAP- und SOAP-konforme Web-Services.

2 Bis zur Aufhebung der Delegation steht diese Rolle dem Eigentümer selbst nicht mehr zur Verfügung.
3 Die Rolle kann vom Vertretenden wiederum an eine weitere Person delegiert werden.
4 Die Delegation gilt auf unbestimmte Zeit bis zur Aufhebung durch den Eigentümer der Rolle.

Abb. 3 Ausschnitt aus der Menüleiste

6.1 LDAP

Die LDAP-Schnittstelle basiert auf dem virtuellen LDAP-Server Penrose [PENR]. Gemäß den Anforderungen der Anwendung (LDAP-Schema, Semantik, usw.) können die TUBIS Modelldaten in Echtzeit in das virtuelle LDAP eingespielt werden. Dabei wird davon Gebrauch gemacht, dass Penrose in der Lage ist, mit Hilfe von sog. Mappern, Daten zu konvertieren und mit Hilfe von Adaptern, Attribute aus Datenquellen zu beziehen. Hierbei wird TUBIS als einzige Datenquelle über den dafür entwickelten Adapter benutzt, welcher selbst wiederum über das Metadirectory auf seine verschiedenen Quellen zugreifen kann. Die Identifizierung des jeweiligen Anwendungsdienstes kann über die Autorisierungsmechanismen von LDAP vorgenommen werden. D.h. je nachdem welche Anwendung sich beim virtuellen LDAP authentisiert, wird von Mapper und Adapter das passende LDAP-Schema erzeugt.

Auch wenn zurzeit noch keine Daten vorliegen, ist davon auszugehen, dass dem Datendurchsatz Grenzen gesetzt sind. Zwar bietet Penrose Caching und andere Optimierungsoptionen, für den Einsatz z.B. im Bereich E-Mail werden jedoch auch an der TU-Berlin LDAP-Server eingesetzt, die über TUBIS gespeist werden können. D.h. bestimmte Aktionen, wie das Hinzufügen eines Benutzers, lösen auch das Einfügen von Objekten im LDAP aus. Jedoch kann so der LDAP-Server davon befreit bleiben, für viele kleine Anwendungen jeweils eigene Zweige und Schemata bereitzustellen. Der „LDAP-Wildwuchs“ mit entsprechenden „Spezialwünschen“ von Anwendungen kann über das virtuelle LDAP von TUBIS abgefangen werden.

6.2 Web-Services

Über ein Web-Service Protokoll können momentan zwei Schnittstellen angesprochen werden. Das Rollenticket Interface (RTI) kann Anfragen bzgl. der Anwendungsrollen einer bestimmten Person verarbeiten. Dabei können für eine Person entweder

- alle verfügbaren[5] Anwendungsrollen,
- nur verfügbare Anwendungsrollen einer bestimmten Anwendung oder
- alle Anwedungen, für die Rollen verfügbar sind, abgefragt werden.

Das Identitäts-Management Interface (IDMI) bietet eine Schnittstelle, um Daten über ein Pull-Verfahren vom TUBIS abzufragen. Hier können einzelne Daten zu bestimmten Personen, Organisationseinheiten oder auch Anwendungen abgerufen werden. Erfolgreiche Antworten setzten das Vorhandensein von entsprechenden Zugriffsrollen voraus.

7 ARCHITEKTUR UND TECHNOLOGIEN

Die TUBIS Architektur besteht aus mehreren Modulen, die in insgesamt drei Kategorien unterteilt werden können: Schnittstellenmodule, Modellverwaltungsmodule und Datenquellenmodule (siehe Abb. 4). Eine andere Sichtweise bietet die Unterteilung in die TUBIS-Kernmodule und die TUBIS-Erweiterungsmodule.

7.1 Die Schnittstellenmodule

Die Schnittstellenmodule dienen zur Kommunikation zwischen den jeweiligen Clients und dem TUBIS. Zurzeit existiert ein Modul zur Abfrage von Rollenzugehörigkeiten (RoleTicketInterface – RTI), zwei Module zur Abfrage von Modellinformationen und Daten (das Identity Management Interface – IDMI und der virtueller LDAP-Server – vLDAP) sowie eine grafische Oberfläsche zur Verwaltung des TUBIS-modells. Alle Module wurden in Java implementiert. Der RTI sowie der IDMI wurden als Web-Services konzipiert. Hierbei wurde auf die AXIS Bibliotheken zurückgegriffen. Als Web-Server dient ein Tomcat-Server. Die grafische Oberfläche wurde als Web-Anwendung mittels Servlets und XST Stylesheets realisiert. Sie läuft ebenfalls auf einem Tomcat Web-Server. Die LDAP-Schnittstelle wurde als virtueller LDAP-Server unter der Verwendung von Penrose aufgesetzt.

7.2 Das Modellverwaltungsmodule

Den Kern des TUBIS bilden der ModelViewController (MVC) und der MetaDataController (MDC). Der MDC enthält das komplette TUBIS-Modell in Form einer Java Klassenstruktur. Der MVC bildet das Bindeglied zwischen den Schnittstellen und dem Modell. Er enthält alle notwendigen Methoden zur Verwaltung des Modells über die grafische Oberfläche. Der TUBIS-Kern wurde vollständig in Java implementiert. Die Modellverwaltungsmodule stehen hierbei in Form einer Bibliothek zur Verfügung.

7.3 Das Datenquellenmodule

Die dritte Kategorie von Modulen dient der Kommunikation zwischen TUBIS und den primären Datenquellen. Die jeweiligen

5 Eine Person muss Mitglied einer bestimmten Rolle sein, damit sie ihr zur Verfügung steht.

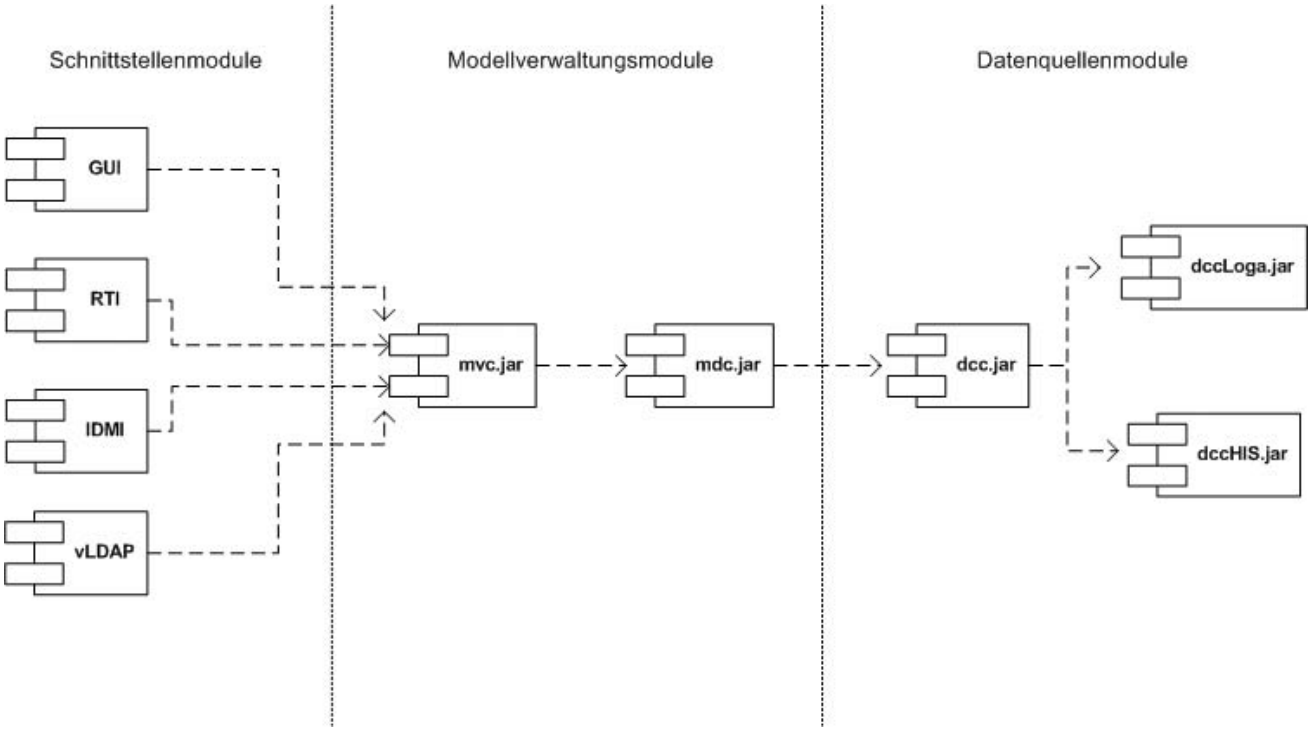

Abb. 4 Komponenten von TUBIS

Datenquellen sind in Java-Klassen gekapselt. Das Metamodell verweist auf die jeweiligen Datenquellen, in denen dann Anfragen in SQL-Befehle über JDBC oder z.B. in LDAP- oder DNS-Anfragen gewandelt werden könnten. Ferner kann das Datenquellenmodul Caches realisieren. So können bereits in einer Datenbankanfrage Attribute im Cache zur Verfügung gestellt werden, die vermutlich als nächstes über das Metamodell abgefragt werden.

Auf Datenbankseite wurden uns hierfür entsprechende Datenbank-Views zur Verfügung gestellt bzw. Zugriffsrechte für die nötigen Tabellen eingeräumt. Das Sicherheitskonzept ist hier mehrstufig. Die Primärdatenbanken stellen TUBIS nur den maximal von TUBIS benötigten Datensatz zur Verfügung. TUBIS selbst steuert dann die feineren Zugriffe an die jeweiligen Anwendungen bzw. Benutzer.

Die relationalen Datenbanksysteme sind über einen JDBC-Proxy mit dem TUBIS verbunden. Hier kommt Sequoia zum Einsatz, welches zurzeit auch dafür benutzt wird, die Primärdatenbank vor einer Überlastung zu schützen. Grundsätzlich sind hier jedoch auch noch andere Optimierungen über Datenbank-RAIDs etc. vorstellbar.

8 STAND DER ARBEIT

Die erste Version des TUBIS ist seit April 2007 im Wirkbetrieb. Der Kern verfügt über alle zur Modellverwaltung benötigten Basisfunktionen. Die Rollenverwaltung unterstützt das Erstellen von organisatorischen Rollen in Form einer Vererbungshierarchie sowie die Delegation von Rollen. Constraints werden nur in Form statischer Regeln unterstützt. Als primäre Datenquellen dienen die Oracle Datenbank der Personalverwaltung[6] und die Informix Datenbank der Studierendenverwaltung[7]. Das Metamodell ist via JDO in einer PostgreSQL-Datenbank gespeichert.

Die Benutzer können mittels Chipkarte oder PIN/TAN-Verfahren authentisiert werden und können bereits die Anwendungen SuperX, SOSPOS, die TU-eigenen Anwendungen LINF und KLR sowie einige Verwaltungsfunktionen für TUBIS selbst oder z.B. die Chipkarte nutzen.

9 AKTUELLE TÄTIGKEITEN

Die Integration sowohl von Datenquellen als auch von Diensten hat mit den o.g. Anwendungen an der TU-Berlin erst begonnen. Gerade wird eine Integration mit dem ASKnet-Portal zur Softwarebestellung getestet. Auch sind Dienste, wie Subversion und eine dezentrale Gast-Account-Verwaltung in Arbeit sowie Anbindungen an die DNS-Verwaltung, eine bessere Verknüpfung zwischen Rechnerzugängen und TUBIS, LSF, Squirrelmail und eine Anbindung an das Content Management System Typo3.

Auf der anderen Seite wird die zukünftige Authentisierung neu beleuchtet. So wird versucht, eine Token-basierte Authentisierung zu implementieren, die auf verschiedenen Plattformen lauffähig ist und zukünftig TAN-Listen weitgehend unnötig macht.

6 An der TU-Berlin verwendetes Datenbanksystem unter dem Personalverwaltungssystem Loga der Firma P&I.

7 An der TU-Berlin verwendetes Datenbanksystem unter den QIS Modulen der Firma HIS.

10 FAZIT UND AUSBLICK

Erst nachdem die ersten TUBIS-integrierten Anwendungen online waren, wurde die Phantasie der meisten Endnutzer und Dienstanbieter in Bewegung gesetzt. Es scheint, dass die Integration jeder weiteren Anwendung Ideen für weitere Synergien und Möglichkeiten eröffnet.

Wesentlicher Bestandteil des Erfolgsrezeptes TUBIS ist aus unserer Sicht die Verknüpfung von Metadirectory und rollen-basierter Zugriffskontrolle. Der Nutzen für den Endanwender wird sofort offensichtlich, wenn er selbst in der Lage ist, für seine Urlaubszeit, die ihm zugeteilten Rollen an seine Kollegen zu delegieren. Selbstverständlich müssen die Abteilungen erst langsam realisieren, dass sie nicht mehr das Rechenzentrum anrufen müssen oder gar ein Formular via Hauspost absenden müssen, um ihrem Mitarbeiter Zugriff zu Ressourcen für andere Aufgabenfelder zu ermöglichen. An den Stellen, an dem der Paradigmenwechsel zu „IT-Experten verwalten IT“ und „Team verwaltet Team“ bereits stattgefunden hat, führt er zu sehr viel reibungsloseren Abläufen und wird allgemein sehr positiv aufgefasst. Heute ist es noch so, dass Rollen übergangsweise vom Rechenzentrum gepflegt werden. Mittelfristig werden jedoch Administratoren entlastet und Mitarbeiter befähigt, selbst sinnvolle und unter anderem auch dank Delegationen sehr dynamische Arbeitsaufteilungen umzusetzen.

Sicherlich ist die Erstellung einer zentralen Sicherheitspolitik zur Vergabe von Rollen immer mit einem gewissen Risiko verbunden. Schließlich wirkt sich hier ein Fehler ggf. fatal auf die Sicherheit der gesamten IT-Struktur aus. Auf der anderen Seite ist die Zentralisierung dieser Politik ein unschätzbarer Mehrgewinn an Transparenz für die IT-Experten aber auch für die für das Personalwesen verantwortlichen Stellen.

Die Weitergabe von Passwörtern gehört der Vergangenheit an. Auch lassen sich Sicherheitslücken durch „Karteileichen“ leichter schließen. Die flächendeckende Einführung eines neuen Dienstes hat sich stark beschleunigt. Zwar muss jeder Dienst zunächst in die TUBIS Infrastruktur integriert werden, dafür entfällt jedoch das Einpflegen aller Benutzer und längerfristig natürlich auch deren Verwaltung.

Das TUBIS-Team ist an einem Austausch mit anderen Universitäten und ggf. auch anderen Einrichtungen interessiert. Gerne beraten wir im Austausch bezüglich Erfahrungen beim Einsatz ähnlicher Systeme. Längerfristig wäre auch ein Einsatz von TUBIS außerhalb der TU-Berlin denkbar.

Kontakt kann über einen der Autoren dieses Artikels hergestellt werden. Informationen zum Projekt TUBIS sind auf der tubIT-Webseite zu finden: http://www.tubit.tu-berlin.de/

LITERATURVERZEICHNIS

[Ba00] Barka, E. & Sandhu, R.: Framework for Role-Based Delegation Models Laboratory of Information Security Technology, 2000.

[Mi05] Poniszewska-Maranda, A.: Role engineering of information system using extended RBAC model WETICE '05, IEEE, 2005.

[PENR] Penrose Homepage, http://docs.safehaus.org/display/PENROSE/Home.

[Sa96] Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L. & Youman, C.E.: Role-Based Access Control Models Computer, IEEE Computer Society Press, 1996, Volume 29, 38-47.