Rollenbasierte Identitäts- und Autorisierungsverwaltung an der TU Berlin

Christopher Ritter, Odej Kao, Thomas Hildmann

tubIT – IT Dienstleistungszentrum, TU Berlin
Einsteinufer 17, 10587 Berlin
christopher.ritter@tu-berlin.de, odej.kao@tu-berlin.de
thomas.hildmann@tu-berlin.de

Abstract: Studierende und Mitarbeiter erreichen die Universitäten mit gestiegener Erwartungshaltung bezüglich der Verfügbarkeit von und des Zugangs zu universitären Diensten. Analog zum Alltagsleben sollen möglichst alle Vorgänge auf Onlinedienste abgebildet werden. Eine solche Dienstintegration stellt die Universitäten vor organisatorische und technische Herausforderungen. In diesem Beitrag wird das personalisierte Dienstportal der TU Berlin vorgestellt, das auf dem Identity Management System TUBIS basiert und den Ansatz einer rollen-basierten Zugangsregelung verfolgt. Jedes Mitglied der TU Berlin wird automatisch erfasst und mit Standardrollen ausgestattet, die durch Delegation, Stellvertretung oder Übertragung von Funktionen durch weitere Rollen ergänzt werden. Die Rollenzuordnung und –verwaltung erfolgt vollständig dezentral und bildet das tägliche Arbeitsleben nach. Eine Rolle dient als Ausgangspunkt für die Darstellung von Anwendungen im personalisiertem Portal, für die Bildung von Teams, zur Bestimmung der Art und des Umfangs der zugelassenen Berichte usw. Das System befindet sich seit einem Jahr im produktiven Betrieb und regelt den Zugang zu mehreren Anwendungen aus der Universitätsverwaltung- und dem Rechenzentrum für mehr als 37000 Mitglieder der TU Berlin.

1 Einleitung

Die Veränderungen der IT-Hochschullandschaft in den letzten Jahren spiegelt der Trend zur Integration vielfältiger Universitätsbereiche wider, die vorher weitgehend unabhängig voneinander gearbeitet haben. Der Bedarf für eine solche Integration entsteht durch die Erwartungen von Studierenden und Mitarbeitern, zahlreiche Dienste durch Selbstbedienungsfunktionen zu nutzen und somit Zeit für Studium und Forschung zu gewinnen. Sie sind offensichtlich nicht mehr bereit, Papierformulare auszufüllen oder bei Routinevorgängen irgendwo anzurufen und einen Wunsch vorzutragen. Warum sollten sie das auch, wenn sie im Alltagsleben einen direkten Zugang zu Informationen und Aktivitäten gewohnt sind.

Die Umsetzung eines integrierten Dienstangebots stellt die Hochschulen vor signifikante technische und organisatorische Herausforderungen. Geschäftsprozesse und Verantwortlichkeiten sind selten umfassend dokumentiert, wodurch eine übergreifende Planung, Steuerung und Operationalisierung erschwert wird. Die TU Berlin hat sich diesen Prob-

lemen vor drei Jahren gestellt und eine neue Planungs- und Leitungsstruktur für den Bereich IuK umgesetzt. Dazu gehört die Verankerung von CIO in den Leitungsgremien der Universität, die Zusammenführung der Dienstleistungseinrichtungen im IT Bereich und die konsequente Umsetzung des Kooperationsmodells. Parallel dazu wird auf technischer Seite ein Dienstleistungsportal aufgebaut, das in Verbindung mit dem Identity Managementsystem TUBIS den direkten Zugang zu den IT-gestützten Diensten des Rechenzentrums und der Verwaltung bietet. TUBIS koppelt primäre Datenquellen mit einer dezentralen Rollenverwaltung und bildet die Befugnisse und Arbeitsvorgänge des täglichen Lebens ab. Jedes Mitglied wird eindeutig erkannt und seinem aktuellen Kontext wie Status (Studierender, Mitarbeiter), Rolle (Dekan, FG-Leiter, Abteilungsleiter usw.) oder Studiengang zugeordnet, um die passenden Dienste herauszusuchen und anzubieten. Alle Mitarbeiter und Studierende werden bei der Einstellung bzw. Immatrikulation erfasst. Mitarbeiter werden entsprechend der Kostenstellen den Fachgebieten zugeordnet und mit den zugehörigen Rollen ausgestattet. Der Rollenansatz ist eine gute Metapher, die auf den verschiedenen Ebenen der Universität verstanden wird. Die Herausforderung besteht darin, jedem Benutzerkreis eine eigene Sicht auf das Modell zu ermöglichen. Eine dezentrale Vergabe und Pflege der Rollen und Rechte erhöht die Akzeptanz des Systems.

Als Kristallisationspunkt dient ein personalisiertes Portal, in dem nach und nach alle Anwendungen integriert werden, die für die tägliche Arbeit notwendig sind. Der Integrationsprozess ist aufwendig, weil jede Anwendung an das Autorisierungs- und Authentisierungssystem angepasst werden muss. Die ersten Beispiele waren die HIS Systeme zur Studierenden- und Prüfungsverwaltung. Mittlerweile sind eine Reihe weiterer Anwendungen – von persönlichen Daten über Einkaufsportalen bis hin zu Systemen für Leistungserfassung – eingebettet und im produktiven Betrieb etabliert.

Im weiteren Verlauf werden die TUBIS-Architektur und die Rollenabbildung vorgestellt. Ferner wird die Integration von Beispielanwendungen erläutert.

2 TUBIS

TUBIS (*TU Berlin Integrationsservice für Campusmanagement*) ist ein an der TU Berlin entwickeltes rollen-basiertes Identitätsmanagement System [Fe03] mit Metadirectory-Funktionalität. Ziel ist es, verschiedene Datenquellen zusammenzufassen und die Daten 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 dem Benutzer ein möglichst hohes Maß an informationeller Selbstbestimmung zu gewährleisten. Dies geschieht zum einen durch den Rollenansatz, durch die konsequente Umsetzung der Datensparsamkeit und durch Transparenz.

2.1 Datenquellen

Personenbezogene Daten werden von mehreren unterschiedlichen Dienstanbietern an vielen Stellen benötigt. Zur Vermeidung redundanter und ggf. inkonsistenter Datenbestände sowie vieler unterschiedlicher, fehleranfälliger Zugriffswege auf primäre Daten-

quellen[1] dient TUBIS als zentrale Datenvermittlung für Anwendungen als Metadirectory. Die Daten werden nicht im TUBIS vorgehalten, sondern erst zum Zeitpunkt des Zugriffs von den jeweiligen datenhaltenden Stellen abgerufen. Das TUBIS Modell hält stattdessen Referenzen zu flexiblen Adapterklassen, die den Datenbankenzugriff realisieren. Auf diese Weise werden u.a. Personendaten aus dem Personalmanagementsystem Loga oder der Studierendenverwaltung SOSPOS bezogen. Abhängig davon, ob es sich bei der 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.

2.2 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 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.

2.3 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

[1] Datenhaltende Stellen die als hauptverantwortliche für ein bestimmtes Datum gelten.

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 abzubildend in einem unwartbaren und dennoch unvollständigen Modell endet. Die Ziel muss irgendwo in der Mitte liegen. Das TUBIS Modell der TU Berlin unterteilt sich in drei Abschnitte: Identitätssicht, Organisationssicht und Anwendungssicht.

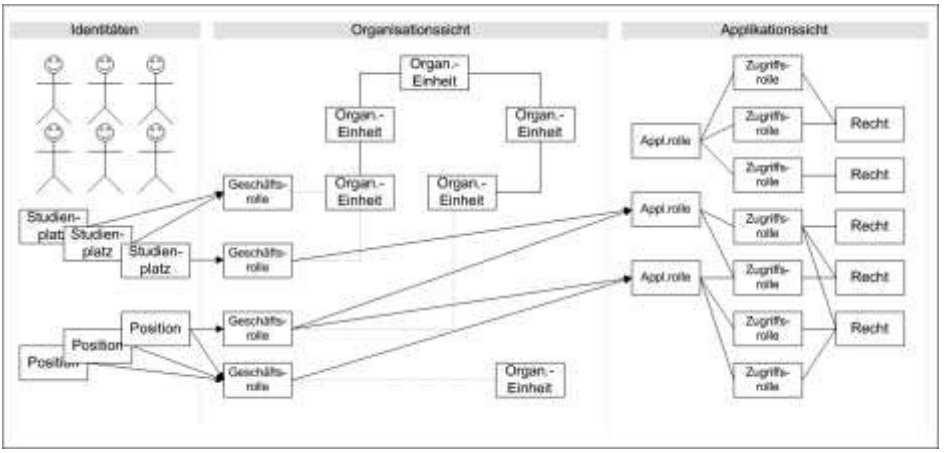

Abbildung 1: Vereinfachte Darstellung des Modells der TU Berlin

Im Bereich der Identitäten werden die Personen der TU-Berlin abgebildet. 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 der studentische Mitarbeiter, der sowohl einen Matrikeleintrag als auch einen Vertrag besitzt. Die organisatorische Sicht beinhaltet die hierarchische Organisationsstruktur und die Vererbungshierarchie der organisatorischen Geschäftsrollen. Innerhalb der Anwendungssicht werden sowohl die Anwendungen selbst als auch deren Anwendugsrollen und Zugriffsrechte abgebildet. Eine Anwendung kann dabei beliebig viele Anwendungsrollen besitzen. Anwendungsrollen enthalten eine Menge von Zugriffsrollen die wiederum eine Menge von Zugriffsrechten bündeln.

3 Integration in die IT-Infrastruktur und Arbeitsprozesse

Um Mitgliedern der TU Berlin Zugriff auf die Anwendungen zu ermöglichen, die für ihre Arbeitsprozesse benötigt werden, muss zunächst die Identität im System erfasst werden, müssen entsprechende Benutzerkonten angelegt werden und benötigte Rechte vergeben werden. Bei Austritt einer Person aus dem Kontext der TU Berlin müssen existierende Rechte und Konten wieder entzogen werden.
Die folgenden Abschnitte beschreiben den Lebenszyklus einer Identität in der IDM Infrastruktur der TU Berlin.

3.1 Provisionierung

In der Kartenausgabestelle (KAS) werden neue Mitarbeiter und Studierende im System aufgenommen. Die persönlichen Daten für das vorliegende Ordnungsmerkmal werden über ein Web-Service Schnittstellenmodul des TUBIS abgefragt. Das Schnittstellenmodul leitet diese Anwendung an das Modellverwaltungsmodul des TUBIS-Kernsystems weiter. In diesem Fall das Identitätenmodul. Dort wird zunächst überprüft, ob für das übermittelte Ordnungsmerkmal bereits ein Objekt im Modell existiert. Dies sei nun nicht der Fall. Anhand des Ordnungsmerkmales wird entschieden, ob es sich um einen Mitarbeiter oder Studierenden handelt und ein Objekt angelegt. Die Daten für das neue Objekt werden direkt aus der Primärdatenquelle bezogen. Da es sich hier um einen Mitarbeiter handelt verweisen die Referenzen der Daten auf das Datenbankmodul der Personalabteilung. Das Datenbankmodul sorgt nun für eine Verbindung zu der gewünschten Datenquelle und liefert die entsprechenden Daten. Das Modellverwaltungsmodul wertet die empfangenen Daten aus und kann das neuen Identitätsobjekt so im Organigramm der TU-Berlin positionieren und mit den entsprechenden Rollen ausstatten. In diesem Fall bekommt die neue Position mindestens die Rolle „TU-Mitarbeiter“ sowie eine Tätigkeitsbezogene Rollen (z.B. Professor).

3.2 Benutzerverwaltung

Die zentrale Benutzerverwaltung wurde in die Infrastruktur des TUBIS integriert. Schließt ein Nutzer das Provisioning erfolgreich ab, so erhält er vom System ein initiales Passwort. Dieses ermöglicht ihm die Anmeldung bei der Anwendung zur Generierung eines neuen Nutzerkontos. Die Anwendung bezieht die benötigten Personendaten ebenfalls aus TUBIS. Der Benutzer muss lediglich den gewünschten Benutzernamen und das Passwort eingeben. Das neue Nutzerkonto wird automatisch der entsprechenden Person zugewiesen. Die unterschiedlichen Agenten der Benutzerverwaltung sorgen für die Benachrichtigung der Hintergrundsysteme. So wird u.a. ein Kerberos-Principal und ein ActiveDirectory Nutzer angelegt, ein Bereich im AFS angelegt und die entsprechenden E-Mailkonten und Alias im Mailserver konfiguriert.Die Kontodaten werden zur besseren Performance zusätzlich in einem LDAP abgelegt, der über die entsprechenden Schnittstellen bei Änderungen im TUBIS aktualisiert wird.

3.4 Rollen- und Autorisierungsverwaltung

Rollenbasierte Autorisierungssysteme werden in der Regel im Bezug auf ihre Modelleigenschaften, ihre Reichwerte, ihre Granularität, der Schicht, auf der sie ansetzen und ihrem Distributionsmodell charakterisiert. Eine andere entscheidende Charakterisierung hängt direkt mit dem verwendeten Modell zusammen. Es ist die Frage nach der Administration der Rollen oder konkret die Beantwortung der Fragen: „Wer kann wem Rollen zuweisen?“ oder „Wie kommen die Benutzer zu ihren Rollen“ [Dr03]?. Das abstrakte Zugriffsmodell von TUBIS ist dreigeteilt:

1. **Identitäten**: Im ersten Teil wird die Identität (genauer Teilidentität [Kö01]) eines Benutzers abgebildet. Hierzu gehören die beschriebenen Prozesse „Provisioning“ und

„Benutzerverwaltung“. Einer Person in der physischen Welt werden Attribute zugeordnet, sie bekommt eine eindeutige Kennung und Werkzeuge zur Authentisierung (Chipkarte, Benutzername, Passwort, TAN-Liste).

2. **Anwendungen**: Am anderen Ende der Zugriffskette stehen die Anwendungen mit ihren konkreten Rechten, die an sog. Anwendungsrollen gebunden sind. Dieser Teil des Modells wird von den Anwendungsverwaltern (in der Regel ein Team aus Administratoren und für den Betrieb verantwortlichen) definiert. Die Anwendungsverwalter können modellieren, wer auf welchem Weg die Anwendungsrollen den Benutzern zugänglich machen kann.

3. **Organisationsmodell**: Der organisatorische Teil des Modells stellt den Klebstoff zwischen den beiden erst genannten Teilen dar. Die Struktur der Universität ist hier abgebildet. Innerhalb der Struktur können nun sog. Geschäftsrollen definiert werden, die Identitäten mit Anwendungsrollen zusammenbringen.

TUBIS implementiert zur Zeit vier Varianten der Rollenzuweisung. Welche Rechte über welche der genannten Varianten zur Verfügung gestellt werden können, kann von den Anwendungsverwaltern definiert werden. So ist eine Gewaltenteilung (Seperation-of-Duty) auf der Modelebene implementiert, die die Gefahr reduziert, dass auf Grund der Komplexität des Modells grobe Fehler bei der Rechtevergabe gemacht werden.

- **Standardrollen:** Über Standardrollen können Rechte an Anwendungen automatisch vergeben werden. Die Vergabe ist nicht fein granular, bedeutet jedoch den geringsten Administrationsaufwand. Jedem Benutzer werden automatisch Standardrollen zugewiesen, die aus den Primärdatenquellen abgeleitet werden können. Vergebene Standardrollen sind z.B.: „TU-Mitglied“, „Studierender“, „Mitarbeiter/in“, „Professor“, ... Rechte können unmittelbar an diese Standardrollen vergeben werden. So kann beispielsweise jeder Studierender der TU Berlin Software beim Softwareportal zu besonderen Konditionen erwerben.

- **Strukturverwaltung:** Oft sind Zugriffe an eine Struktureinheit innerhalb der TU gebunden. So gibt es beispielsweise einen oder mehrere Bestellbefugte, die für eine Struktureinheit (z.B. ein Institut) Software beziehen darf. Der Anwendungsverwalter kann in diesem Fall die „Besteller/in“-Rolle den jeweiligen Struktureinheiten („Fakultät“, „Institut“, „SFB“, ...) zur Verfügung stellen. In jeder Einheit ist ferner ein „Strukturverwalter“ definiert, der nun wiederum in der Lage ist, dieser der Einheit zur Verfügung gestellten Rolle der richtigen Person zuzuweisen. Das Ergebnis dieses Vorgehens ist eine verteilte Administration, die administrative Engpässe bei der Vergabe der Rechte verhindert. Dabei muss die Verwaltung der Struktureinheit natürlich nicht auf den Schultern einer einzigen Person lasten.

- **Delegation:** Im Universitätsalltag ist es üblich, Vorgänge zu delegieren (Rollendelegation siehe [Ba00]). So liegt eine Bestellbefugnis für Hardware beispielsweise für Person A vor, Person B ist jedoch mit der Materie sehr vertraut und führt daher die Beschaffung faktisch im Auftrag und selbstverständlich auch unter der Verantwortung von Person A durch. Die Möglichkeit zur Delegation von Rechten ist an der TU

eines der Killerapplikationen im Bezug auf die Einführung von TUBIS. Natürlich kann die Delegation nur auf Grundlage von arbeitsorganisatorischen und rechtlichen Grundlagen erfolgen. Auch wurden von uns Mechanismen zur Kontrolle für den Delegierenden implementiert. So bekommt der Bestellbefugte z.B. eine Kopie jeder Bestellung zugestellt, die vom Delegierten durchgeführt wurden.

- **Teambildung:** Mit den sog. Teams bietet TUBIS den Mitarbeitern die Möglichkeit, selbst verwaltete Struktureinheiten zu bilden, sie mit Mitgliedern zu versehen und darin Rollen zu verteilen. Der Unterschied zu den Struktureinheiten besteht darin, dass Teams nicht aus Primärdaten abgeleitet, sondern von Benutzern selbst angelegt werden. Das ermöglicht im Gegensatz zur „nominalen Struktur" der Organisation auch eine „realere Struktur" abzubilden. Für bestimmte Aufgaben oder Gebiete werden Teams gebildet, wieder aufgelöst, eine Person ist Mitglied in unterschiedlichen Teams (auch Bereichsübergreifens), in der sie mitarbeitet. Auch werden Teamzusammenstellungen evtl. kurzfristig geändert, um auf neue Aufgaben zur reagieren oder die Arbeit anders zu verteilen. Dies ist über die Teamfunktion in TUBIS jeder Zeit möglich. Teams können mit unterschiedlichen Applikationen verknüpft werden und ermöglichen z.B. auch die Verwaltung von Mailinglisten oder Funktionsmailboxen, SVN Festplattenplatz usw.

4 Beispielanwendungen

Die wichtigste Anwendung von TUBIS ist das personalisierte Portal der TU Berlin, das im aktuellen Webauftritt integriert ist und den Zugang zu allen Anwendungen bietet, die für die tägliche Arbeit erforderlich sind. Derzeit sind einige Anwendungen aus dem Berichtswesen (SuperX), Prüfungswesen (Prüfungsverwaltung HIS SOSPOS, Modulverwaltung), Eintragung und Einsicht der persönlichen Daten und Gehaltsinformationen (Loga HCM). Als zweiter großer Block sind die IT Anwendungen zu nennen, mit denen Hardware und Software beschafft werden können (Portal der Firma asknet), Gästeeintragung, DNS- und Account-Verwaltung, Gästeeintragung. Auch der Zugang zum Content Management System Typo3 wird über das Portal realisiert. Somit findet ein Benutzer alle benötigten Anwendungen an einem Ort.

Der Portalausbau schreitet durch die Einbettung weiterer Anwendungen fort. Bei jeder neuen Anwendung werden zwei große Aufgaben gelöst: Anpassung der Anwendungsoberfläche an das Corporate Design der TU Berlin, Einbindung in die TUBIS-Infrastruktur und das Portal und somit die Aktivierung des Zugangs mit der Campuskarte bzw. mit PIN/TAN. Zur Veranschaulichung des Integrationsprozesses werden im Folgenden zwei Anwendungen näher beschrieben.

4.1 CMS über Typo3

TU-Berlin nutzt als Content Management System Typo3, dessen interne Benutzer- und Rechteverwaltung auf einem LDAP System basiert. Um die Befugnisse innerhalb von Typo3 rollenbasiert, dezentral und dynamisch anpassen zu können, müssen die Daten

aus TUBIS in ein passendes LDAP-Schema gewandelt werden. Hierzu wird das Open-Source Produkt Penrose – ein Java-basierter virtueller Verzeichnisserver – eingesetzt. Dieser hält keine Daten vor, sondern bezieht alle für die Bearbeitung einer Anfrage benötigten Daten aus den primären Datenbanken. Dabei kann es sich sowohl um Verzeichnisserver wie LDAP als auch um relationale Datenbanken oder Dateisysteme handeln [PENR]. Im Fall der Typo3-TUBIS-Anbindung wurde mit Penrose ein virtueller Verzeichnisserver entwickelt, der die notwendigen Daten aus TUBIS und dem LDAP der TU-weiten Benutzerverwaltung kombiniert. Bei einer Frontend-Anmeldung (geschützte Seiten) oder einer Backend-Anmeldungen (Administrationsoberfläche) werden die benötigten Attribute durch unterschiedliche Adapter aus den Daten von TUBIS und weiteren Primärdaten „on-the-fly“ zusammengestellt.

Besitzt ein Benutzer mindestens eine Rolle für das Typo3 Backend, so wird ihm ein Link „TYPO3 Backend“ in dem TU Portal angezeigt. In das persönliche Portal gelangt ein Benutzer durch Anmeldung auf der TU Webseite mittels Campuskarte [Hi01] oder Benutzername und Passwort. In die jeweiligen Anwendungen gelangt der Benutzer durch Auswahl der Links, die ihm im persönlichen Portal zur Verfügung gestellt werden.

Abbildung 2: Rollenauswahl für "TYPO3 Backend"

Dabei muss ein Link nicht zwingend einer Anwendung entsprechen. Links können auch direkt ein Modul oder eine spezielle Funktion einer Anwendung repräsentieren. Stehen dem Benutzer für eine Anwendung mehrere Rollen zur Verfügung, so gelangt er nach Anwahl der Anwendung in eine „Rollenauswahl“ und muss sich für eine Rolle entscheiden. Es ist auch möglich Superrollen zu modellieren, die mehrere Rollen in sich vereinen, um ein Wechseln der Rollen unnötig zu machen. In vielen Fällen (z.B. Administrator und Benutzer) ist es jedoch sinnvoll eine Auswahl zu erzwingen.

Technisch ist die Anmeldung über einen WWW-Proxy realisiert, der die Autorisierung mittels TUBIS und bei Typo3 die Anmeldung über die Typo3-Login-Maske vornimmt. Dabei greifen Proxy und Typo3 auf die gleiche Datenbasis zu. Nachdem der Proxy den Benutzer beim Typo3 angemeldet hat, leitet er den Datenverkehr zum Benutzer durch.

4.2 Loga HCM

Die Human Capital Management-Software (HCM) der Firma P&I ist ein webbasiertes Mitarbeiterportal, das die Optimierung der personalwirtschaftlichen Prozesse unterstützt. Die Weboberfläche wurde im ersten Schritt der Integration in die TUBIS Infrastruktur zunächst übernommen und deren Stylesheets an das Corporate Design der TU-Berlin angepasst. In einem weiteren Schritt sollen Teile der HCM Oberfläche direkt in das Portal der TU-Berlin integriert werden. Die Integration der HCM Anwendung in IDM-Infrastruktur gestaltet sich unkompliziert, da HCM auf dem Datenmodell der von der TU eingesetzten Personalmanagementsoftware Loga basiert. Loga dient TUBIS als Primärquelle für alle Mitarbeiter, so dass der Anwendung alle benötigten Personen bezogenen Daten vorliegen. Die Verwaltung der Identitäten ist implizit gegeben. Von TUBIS werden in diesem Fall lediglich die Autorisierungsinformationen benötigt.

Es musste ein Weg gefunden werden, der es ermöglicht die Zugriffskontrolle des HCM mit dem Rollenmodell der TU zu vereinen. Die Rechteverwaltung von HCM folgt bereits dem Konzept einer rollenbasierten Zugriffskontrolle, wodurch lediglich eine Spezifikation der Rollen notwendig war.

4.3 Weitere Integrationen

Die meisten Anwendungen werden auf Ebene der Anwendungsrollen in die TUBIS Infrastruktur integriert. Dabei definiert die Anwendung einen Satz an Rollen, die den einzelnen Organisationseinheiten zur Verfügung gestellt werden, oder direkt existierenden Geschäftsrollen zugewiesen werden. Die Verwaltung der Rechte, die mit einer bestimmten Rolle verknüpft werden, bleibt vollständig innerhalb der Anwendung. Diese Variante hat sich in der Praxis als praktikabelstes und effizientestes Verfahren herausgestellt. Die eher statische Definition von Rechten bleibt bei der Anwendung, während die stark dynamische Vergabe der Rollen dezentral durch die Verantwortlichen der Organisationseinheiten vorgenommen wird. Die im Produktivbetrieb gesammelten Erfahrungen haben auch gezeigt, dass die Nutzung eines pull Verfahrens zum holen der Nutzerdaten effizienter ist, als die Übergabe aller benötigten Daten während der Autorisierung im Rahmen eines push Verfahrens. Bei der Anmeldung werden zunächst die Personen ID und die entsprechende Rolle übermittelt. Alle weiteren Daten besorgt sich die jeweilige Anwendung erst bei entsprechendem Bedarf.

5 Zusammenfassung

Studierende und Mitarbeiter erreichen die Universitäten mit einem breiten IT Nutzerwissen

und mit gestiegener Erwartungshaltung bezüglich der Verfügbarkeit von und des Zugangs zu universitären Diensten. Analog zum Alltagsleben sollen möglichst alle Vorgänge auf Onlinedienste abgebildet werden. Eine solche Dienstintegration stellt die Universitäten vor organisatorischen und technischen Herausforderungen: Grenzen zwischen Universitätsbereichen müssen verschwinden, Leitungs- und Arbeitskulturen verändert sowie zentrale Verwaltungssysteme entwickelt und umgesetzt werden, die der großen Strukturkomplexität einer Universität gerecht werden. Der wichtigste Baustein ist das Identity Management System TUBIS, das neben der automatisierten Benutzererfassung und –verwaltung ein fein granulares, dezentrales Rollenmanagement ermöglicht. Jedes Mitglied der TU Berlin hat einen Satz von Standardrollen, die durch Delegation, Stellvertretung oder Übertragung von Funktionen durch weitere Rollen ergänzt werden. Ein wesentlicher Punkt ist dabei, dass die Rollenzuordnung und –verwaltung vollständig dezentral erfolgt und somit das tägliche Arbeitsleben nachbildet. Eine Rolle dient als Ausgangspunkt für die Darstellung von Anwendungen im personalisiertem Portal, für die Bildung von Teams, zur Bestimmung der Art und des Umfangs der zugelassenen Berichte usw.

TUBIS ist bereits seit einem Jahr im produktiven Betrieb. Derzeit werden weitere Anwendungen mit dem Rollenmanagement verbunden und im Portal integriert. Zukünftige Arbeiten umfassen ferner die Kopplung mit übergreifenden Systemen wie Shibboleth und die Entwicklung von Methoden für konfliktfreie Rollendefinition und –vergabe [Hi08]. Ein weiterer großer Schritt wird die Integration eines Workflow Management Systems sein. Weitere Informationen zu TUBIS finden sich unter www.tubit.tu-berlin.de/menue/dienste/internet/tuportal_tubis/.

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

[Dr03] Dridi, F.; Muschall, B. & Pernul, G. Administration of an RBAC system Proc. of the 18th IFIP International Information Security Conference (SEC 2003), 2003

[Hi01] Hildmann, T. Vermeidung von Datenspuren bei smartcard- basierten Authentisierungssystemen Verlässliche IT-Systeme 2001, Sicherheit in komplexen IT-Infrastrukturen, Vieweg Wiesbaden, 2001

[Kö01] Köhntopp, M. Pfitzmann, A. "Wie war noch gleich Ihr Name?" --Schritte zu einem umfassenden Identitätsmanagement Verlässliche IT-Systeme, Vieweg, 2001, S. 77-85

[Fe03] Ferraiolo, D. F.; Kuhn, D. R. & Chandramouli, R. Role-Based Access Control Artec House, 2003

[Hi08] Hildmann, T.; Kao, O.; Ritter, C. eXtreme Role Engineering: Ein neuer Ansatz zur Rechtedefinition und –vergabe In: Proceedings der GI Tagung Sicherheit 2008, 2008