# eXtreme Role Engineering: Ein neuer Ansatz zur Rechtedefinition und -vergabe

Thomas Hildmann
thomas.hildmann@tu-berlin.de

Odej Kao
odej.kao@tu-berlin.de

Christopher Ritter
christopher.ritter@tu-berlin.de

**Abstract:**
Die Technische Universität Berlin begegnet den aktuellen Anforderungen von Onlineangeboten sowie der IT-Infrastruktur mit dem Aufbau eines umfassenden rollenbasierten Identitätsmanagements. Eine verteilte Administration bis hin zur Selbstadministration der Endnutzer ermöglicht eine schnelle Reaktion auf Änderungen und entlastet zentrale Dienstleister. Die klassischen RBAC-Modelle und bekannten Role Engineering-Verfahren stoßen jedoch in der Praxis an ihre Grenzen. Aus diesem Grund wird nun an einer Workflow-Integration für Methoden auf Rollenobjekten und an einem agilen Ansatz zur Rollenverwaltung gearbeitet.

## 1 Einleitung

Bücherbestellungen, Bankgeschäfte, aber auch Gebrauchtwaren Ver- und Ankäufe werden heute selbstverständlich von überall aus im Internet getätigt. Auch an eine Universität wird die Anforderung gestellt, dass sowohl inhaltliche, wie auch organisatorische Arbeiten von überall auf dem Campus oder von zu Hause getätigt werden können. Grundlage für solche verteilten Anwendungen ist ein Identitätsmanagement (IDM). Insbesondere bei sensiblen Diensten muss besonderer Wert auf die Qualität des IDM gelegt werden. Und hierzu gehören sowohl Anwendungen, die personenbezogene Daten verarbeiten, aber auch Aufgaben aus der Verwaltung und ggf. der Zugriff auf urheberrechtlich geschütztes Material usw. Hochwertige IDM-Verfahren bedeuten immer einen hohen personellen und finanziellen Aufwand. Um diesen Aufwand rechtfertigen zu können, müssen Synergien gefördert werden. So werden heute viele Dienste in Portalen zusammengefasst, die auf Basis eines gemeinsamen IDMs arbeiten, Föderationen schaffen Vertrauensnetzwerke. Das IDM vertrauenswürdiger Partner wird gegenseitig genutzt.

Digitale Teilidentitäten [Kö01] sind nur der erste Schritt zur Nutzung von verteilten Anwendungen. Sie bieten in der Regel lediglich Möglichkeiten zur Authentisierung von Personen. Die Anwendung muss auch die Frage nach der Autorisierung beantworten. Dies geschieht heute entweder implizit z.B. durch Zugriffslisten oder durch Attribute, die den digitalen Identitäten angehängt sind. An der TU Berlin haben wir ein zentrales rollenbasiertes Autorisierungssystem entwickelt, um somit auch Synergien bei der Rechtevergabe und bei organisatorischen Informationen zu fördern.

## 2 Vom RBAC96 zum TUBIS Rollenmodell

Praktisch jedes System, das RBAC-Funktionalität besitzt basiert auf dem RBAC96-Modell [SCFY96] (siehe Abb. 1) . Auf Grundlage dieses Modells wurde auch der NIST-Standard für RBAC-Systeme entwickelt [San01].

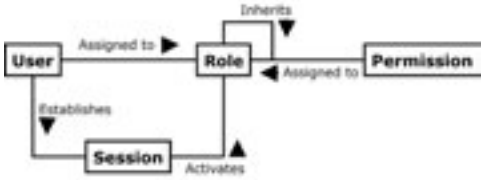


Abbildung 1: Klassisches RBAC

Das klassische RBAC-Modell wird jedoch in der Regel durch spezielle Arten von Rollen erweitert, wie bei [PM05]. Ferrariolo beschreibt in [FKC03] ein Modell, das von der Stanford University benutzt wird (siehe Abb. 2). Hier wird nicht nur zwischen Rollen und Funktionen unterschieden, sondern ein mehrstufiger Pfad von einer Person zu seinen Rechten definiert. Auch dieses Modell lässt sich auf das klassische RBAC96-Modell abbilden, wenn man davon ausgeht, dass es sich bei “Functions”, “Tasks” und “Entitlements” um spezielle Rollen handelt.

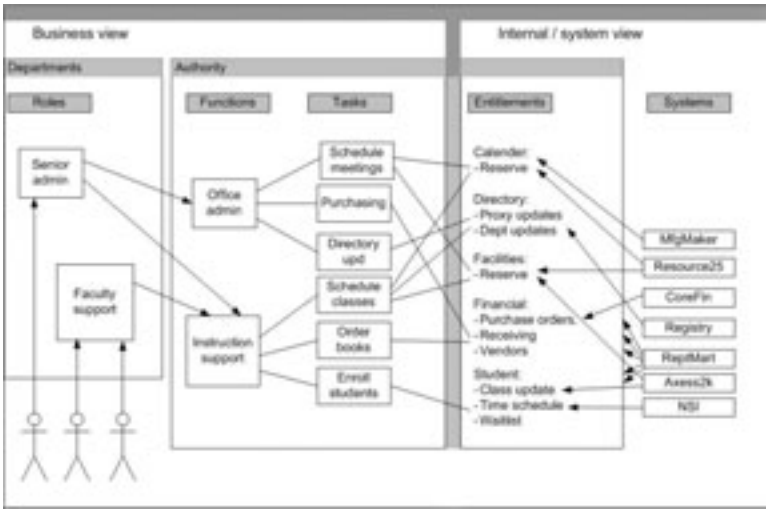


Abbildung 2: Das Stanford-Modell

Die meisten dieser Erweiterungen dienen einer strukturierten Abbildung der Organisationsstruktur und helfen den Role Engineering-Prozessen (RE). Ein Role Engineering-Prozess wird bereits 1996 in [Coy96] beschrieben und u.a. in [GDY04] oder [He03] erweitert.

## 3 Erfahrungen beim TUBIS-Einsatz

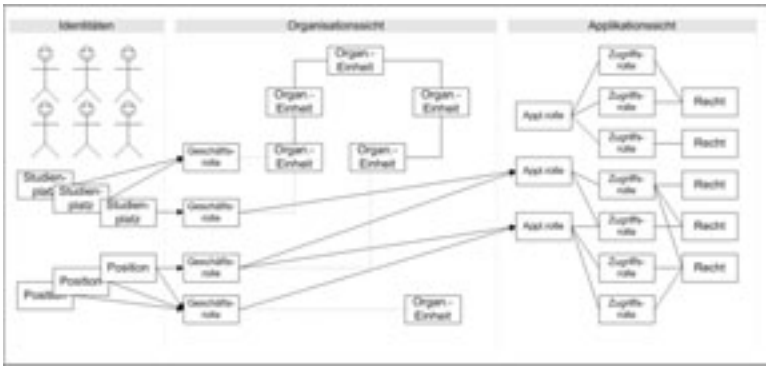


Abbildung 3: Das vereinfachte TUBIS-Modell

Das Rollenmodell, das in TUBIS, dem RBAC-System der TU Berlin eingesetzt wird, ähnelt dem Stanford-Modell (siehe Abb. 3). Es werden drei große Bereiche unterschieden: Identitäten, Organisationsschicht und Anwendungsschicht.

Der Bereich "Identitäten" wird von den datenhaltenden Stellen der Universität, also der Studierendenverwaltung, der Personalabteilung und weiteren Stellen gepflegt. Über einen Provisioning-Prozess wird die Erzeugung einer Entität im TUBIS-System initiiert. Die relevanten Attribute werden von den Primärquellen abgefragt.

Die Anwendungsschicht spiegelt den klassischen RBAC96-Teil wieder. Applikationsrollen können verschiedene Zugriffsrollen enthalten, an die Rechte gebunden sind. In der Praxis definieren Anwendungen oft nur Anwendungsrollen und verarbeiten die Zugriffslogik in der eigenen Programmlogik.

Im Organisationsteil werden Organisationsstrukturen abgebildet. Über diese Schicht findet die Zuordnung von Anwendungsrollen zu Benutzern statt. Die Verwaltung wird hier durch Hochschullehrer oder deren Mitarbeiter, von Verwaltungsangestellten o.ä. durchgeführt. Die Modellierung im Organisationsteil wirft die meisten Fragen auf und stellt die größten Herausforderungen dar, sowohl für die Anwender, als auch für die TUBIS-Entwickler.

## 4 eXtreme Role Engineering

TUBIS wurde als objektorientiertes System entwickelt, das auf einer Klassenlogik aufbaut und auf die Verarbeitung von unterschiedlichen Attributen spezialisiert ist. Es stellt sich jedoch heraus, dass es nicht ausreicht, ein statisches Modell in verschiedenen Zuständen abzubilden. Vielmehr sind die Transitionen zwischen den Zuständen relevant, also die Frage, was z.B. passiert, wenn eine Person eine Rolle zugewiesen oder entzogen bekommt. Aus diesem Grund wird ein Workflowmanagementsystem in das TUBIS integriert.

Die verschiedenen Methoden der Rollen verzweigen jeweils in einen Workflow, der im einfachsten Fall die Kontrolle an das TUBIS abgibt. Häufiger jedoch sind mit dem Hinzufügen von Rollenobjekten, der Zuweisung von Mitgliedern usw. externe Aktionen verbunden. Hierzu zählt z.B. die Benachrichtigung von Rollenmitgliedern, Administratoren oder Trusted-Third-Parties oder die Zustimmung von Beteiligten. Die Logik kann stark von den jeweiligen Rollen abhängen. Zur Zeit sind solche Bedingungen hart in das Modell kodiert. Die Praxis zeigt jedoch, dass dieser Weg in einem großen umfassenden Rollensystem hinderlich und schlecht wartbar ist.

Die klassischen RE-Ansätze gehen davon aus, dass ein Role Engineer das Design für das gesamte System durchführt. Der verteilte Ansatz widerspricht dieser Idee. Hier bieten sich verschiedene Sichten auf das Modell an. Ein Verwalter für die Geschäftssicht betreut immer nur kleine Mengen von Benutzern. Die Verwalter stammen in der Regel aus dem Verwaltungsumfeld, was ihnen einen hervorragenden Überblick über das Arbeitsumfeld liefert. Die Schulung von klassischen Role Engineering-Prozessen verursacht bei dieser Benutzergruppe jedoch Akzeptanzprobleme.

Im Rahmen von TUBIS wird daher versucht einen verteilten RE-Ansatz zu entwickeln, der den unterschiedlichen Sichten und Voraussetzungen der Benutzern Rechnung trägt. Grundsätzlich versuchen wir die Erkenntnisse aus dem Software Engineering auf das RE zu übertragen. So wurden z.B. Ansätze diskutiert, Software-Muster auf Rollenmodelle zu übertragen [TT00].

Während in der Applikationsschicht ein klassischer RE-Ansatz mit den Softwareentwicklern durchgeführt wird, ist das RE der Organisationsschicht agilem Software Engineerings angelehnt. Dabei sind zur Zeit folgende Arbeitsschritte geplant:

**Erstellung einer Story:** Der Verwalter der Organisationseinheit beschreibt anhand von Beispielen, welche Anwendung für welche Personengruppe zugänglich gemacht werden soll.

**Definition von Testfällen:** Der Verwalter wählt geeignete Testpersonen aus seiner Einheit. Über eine GUI (xreUnit) definiert er in einer Matrix, welche Personen welche Zugriffe auf die Anwendungen bekommen sollen.

**Rollenzuweisung in einer Sandbox:** In einer Sandbox kann der Verwalter ein "Was wäre wenn"-Szenario aufbauen und prüfen lassen, ob seine Zuweisungen im Organisationsteil der Testmatrix entspricht.

**Release:** Die in der Sandbox definierten Änderungen werden auf den Produktivserver kopiert. Die jeweiligen Zustände vor und nach der Änderung werden archiviert. Ein Rollback ist jederzeit möglich.

Ein wichtiger Aspekt beim XP ist die Paarprogrammierung. Hierbei bilden die Programmierer wechselnde Paare, damit der Code schon bei der Entstehung begutachtet wird und bei Ausfall eines Programmierers eine Vertretung existiert. Paare zu bilden, halten wir in unserem RE-Umfeld auf Grund organisatorischer Gegebenheiten für nicht durchsetzbar. Es gibt jedoch einige Stellen, an denen das Mehraugenprinzip wirkt. Zum einen können

Anwendungsverwalter die jeweiligen Rollen einzelnen Typen von Organisationseinheiten oder sogar einer bestimmten Entität zur Verfügung stellen. Zum anderen sollen Rollenmitglieder bei der Zuweisung der Rollen jeweils über ihre Mitgliedschaft aufgeklärt werden. Ggf. müssen diese durch Mitgliedschaften bestimmte Erklärungen unterzeichnen, Schulungen nachweisen etc. Fehlerhafte Konfigurationen können so durch verschiedene beteiligte Parteien entdeckt werden.

## 5 Zusammenfassung

Das in diesem Beitrag vorgestellte System realisiert ein zentrales rollenbasiertes Identitäts- und Autorisierungsmanagement, das dezentral administrierbar ist. Es wird an der TU Berlin täglich benutzt und verwaltet ca. 40.000 Nutzer. Da klassische Role-Engineering-Ansätze unter den Benutzern wenig Akzeptanz finden, arbeiten wir nun an Werkzeugen und Verfahren für einen agilen Ansatz; dem eXtreme Role Engineering. Dieser Ansatz nutzt Ideen aus dem eXtreme Programming für rollenbasierte Zugriffskontrollmodelle.

## Literatur

[Coy96] Edward J. Coyne. Role Engineering. In *ACM RBAC Workshop*, MD USA, 1996.

[FKC03] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli. Role-Based Access Control, 2003.

[GDY04] Shu Gao, Zhengfan Dai, and Huiqun Yu. Improving Scenario-Driven Role Engineering Process with Aspects. In *Erly Aspects Workshop in Conjunction with the OOPSLA Converence*, Vancouver, Canada, October 24-28 2004.

[He03] Qingfang He. A Goal-Driven Role Engineering Process for Privacy-Aware RBAC Systems. In *Proc. of the 11th IEEE International Requirements Engineering Conference (RE'03) Doctoral Symposium*, pages pp. 31–35, Monterey Bay, CA, September 8-12 2003.

[Kö01] Marit Köhntopp. "Wie war noch gleich Ihr Name?" – Schritte zu einem umfassenden Identitätsmanagement. In Andreas Pfitzmann, editor, *Verlässliche IT-Systeme 2001*, DuD-Fachbeitr?ge, pages S. 77–85. Vieweg, September 2001.

[PM05] Aneta Poniszewska-Maranda. Role engineering of information system using extended RBAC model. In *WETICE'05, IEEE*, 2005.

[San01] Ravi Sandhu. Future Directions in Role-Based Access Control Models. MMM-ACNS, 2001.

[SCFY96] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-Based Access Control Models. *Computer*, Volume 29(2):38–47, February 1996.

[TT00] Thomas Gebhardt and Thomas Hildmann. Rollen als Schlüssel für B2B-Anwendungen. *DuD - Datenschutz und Datensicherheit*, 24 (2000) 10, 2000.