Heiko Klarl

Zugriffskontrolle in Geschäftsprozessen

Ein modellgetriebener Ansatz

WISSENSCHAFT

VIEWEG+
TEUBNER

Heiko Klarl

Zugriffskontrolle in Geschäftsprozessen

VIEWEG+TEUBNER RESEARCH

Heiko Klarl

Zugriffskontrolle in Geschäftsprozessen

Ein modellgetriebener Ansatz

Mit einem Geleitwort von Prof. Dr. Christian Wolff

VIEWEG+TEUBNER RESEARCH

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dissertation Universität Regensburg, 2010

D 355

1. Auflage 2011

Lektorat: Ute Wrasmann | Sabine Schöller

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8348-1465-4

Meinen Eltern

Geleitwort

Die Frage, wie Zugriffskontrollen für Geschäftsprozesse systematisch modelliert und verwaltet werden können, bildet den Kern der Dissertation von Heiko Klarl. Das Thema steht in unmittelbarer Verbindung mit der Problematik der Kommunikation zwischen fachlicher Spezifikations- und technischer Umsetzungsebene – ein wesentliches Ziel ist es, den Zugriff auf unternehmenskritische Prozesse so zu modellieren und abzusichern, dass sowohl aus fachlicher wie aus technischer Sicht ein leichtes Verständnis der inhaltlichen Anforderungen und eine eindeutige technische Operationalisierung möglich sind. Dabei ist das Thema im Bereich *Identity Management* anzusiedeln, einem Gebiet, das aufgrund der wachsenden Heterogenität und Komplexität der Softwarelandschaften in großen Unternehmen in den letzten Jahren zu einem wichtigen Forschungsfeld in der angewandten Informatik geworden ist.

Gerade die neuen Architekturprinzipien lose gekoppelter Dienste stellen dabei erhöhte Anforderungen an die systematische Steuerung der Zugriffskontrolle, da wesentliche Architekturteile grundsätzlich dynamisch angelegt sind. Die Arbeit von Heiko Klarl bietet hier Lösungsansätze auf unterschiedlichen Ebenen an: Neben Entwurfsmitteln zur Spezifikation von Rollen sollen auch geeignete Modellierungswerkzeuge und Entwicklungsmethoden herausgearbeitet werden. Der Autor stellt das von ihm neu entwickelte Metamodell *Business & System Role-Based Access Control (B&S-RBAC)* vor, das für die fachliche wie die technische Sicht eine Zusammenschau bietet. Aufbauend auf diesem Zugriffskonzept geht der Autor an die für seine Arbeit zentrale Frage der Modellierung sicherer Geschäftsprozesse und stellt sein Vorhaben dabei methodisch in den Kontext der modellgetriebenen Softwareentwicklung.

Durch weitestgehende Verwendung existierender Standards ist die Kompatibilität mit etablierten Modellierungsverfahren gesichert: Heiko Klarl stellt ein Profil IdM-BPMN als Erweiterung der *Business Process Modeling Notation (BPMN)* vor und zeigt auch auf, wie für eine web service-basierte Softwareumgebung die mit IdM-BPMN spezifizierten Policies auf die *Web Service Access Control Markup Language (WSACML)* abgebildet werden können.

Ausgehend von den wesentlichen Transformationsschritten der modellgetriebenen Softwareentwicklung ordnet der Autor diesen Artefakte, Ressourcen und Transformationswerkzeuge seines Modells zu und arbeitet für die einzelnen Pha-

sen des Softwareentwicklungsprozesses heraus, welche Verantwortlichkeiten, Artefakte und Werkzeuge jeweils benötigt werden. Damit zeigt sich, dass Heiko Klarls Ansatz sehr gut auf die Kernphasen der Softwareentwicklung abbildbar ist. Eine Fallstudie verdeutlicht die Anwendbarkeit des von Heiko Klarl entwickelten Modells: Mit der (vereinfachten) Modellierung des Geschäftsprozesses einer Kreditvergabe wählt der Autor bewusst einen „Klassiker“ aus, der bereits unter unterschiedlichsten Perspektiven Forschungsgegenstand in der (Wirtschafts-) Informatik gewesen ist, und der daher besonders gut geeignet ist, die hier neu vorgestellten Konzepte zu illustrieren.

Heiko Klarl ist eine Arbeit gelungen, die durch ihren systematischen und klaren Aufbau besticht: Für ein klar umrissenes Forschungsdesiderat auf einem aktuellen Feld der Geschäftsprozessmodellierung wird nicht nur eine überzeugende Lösung entworfen, diese Lösung wird auch in den Kontext aktueller Standards eingeordnet, mit einer passenden Werkzeugumgebung unterfüttert und durch eine Fallstudie abgesichert. Dabei ist die Darstellung von vorbildhafter Klarheit, sodass auch die teilweise sehr technische Materie leicht nachzuvollziehen ist. Gerade der integrative Ansatz, der Fach- und Systemperspektive verbindet und explizit zueinander in Verbindung setzt, überzeugt und kann hoffentlich für die Praxis weite Verbreitung finden. Durch die systematische Entwicklung auf der Basis einschlägiger internationaler Standards hat der Autor hierfür selbst beste Voraussetzungen geschaffen.

Regensburg im März 2011

Prof. Dr. Christian Wolff

Danksagung

Die Arbeit, die tüchtige, intensive Arbeit, die einen ganz in Anspruch nimmt mit Hirn und Nerven, ist doch der größte Genuss im Leben.

Rosa Luxemburg

Zum Abschluss dieser Arbeit, die manche Mühe, aber noch viel mehr Freude bereitet hat, möchte ich meinem Dank Ausdruck verleihen.

Allen voran geht mein großer Dank an Prof. Dr. Christian Wolff, der diese Arbeit wissenschaftlich betreut hat. Seine immerwährende Verfügbarkeit für interessante Gespräche und Diskussionen, seine wertvollen Anregungen und seine stete Unterstützung dieses externen Promotionsverfahrens prägten die Zusammenarbeit in den letzten Jahren. Für die wissenschaftliche Begleitung der Arbeit, für hilfreiche Anregungen und der Übernahme des Koreferats sei Prof. Dr. Rainer Hammwöhner herzlich gedankt; sowie auch dem Doktorandenseminar für den gegenseitigen Gedankenaustausch und die dadurch erzeugten positiven Impulse für diese Arbeit.

Neben der wissenschaftlichen Arbeit war ich hauptberuflich als *Security Consultant* im Bereich des Identitätsmanagements bei der Firma *iC Consult GmbH* tätig. Große Unterstützung habe ich dabei vom Inhaber und Geschäftsführer Jürgen Biermann erfahren, der von Beginn an dem Vorhaben gegenüber positiv gestimmt war und die Integration von Beruf und wissenschaftlicher Arbeit wo immer es ging förderte. Dafür meinen herzlichen Dank! Mein Dank geht auch an Prof. Dr. Sebastian Abeck, an seinen ehemaligen Mitarbeiter und meinen jetzigen Kollegen Dr. Christian Emig, dessen Vorarbeiten in dieser Arbeit aufgegriffen wurden sowie an die ehemaligen Diplomanden Florian Marmé und Korbinian Molitorisz.

Für die Unterstützung im privaten Bereich möchte ich mich allen voran bei Annette bedanken, insbesondere für ihre große Unterstützung in der Endphase der Dissertation und die gründliche Durchsicht der Arbeit. Dank auch meinen Freunden Monika und Markus, die als frühe Leser dieser Arbeit hilfreiche Anregungen lieferten. Aber auch all denjenigen sei gedankt, die nicht explizit erwähnt sind, jedoch durch Gespräche, Diskussionen und Anregungen zum Gelingen dieser Arbeit beigetragen haben.

Nicht zuletzt geht mein aufrichtiger Dank an meine Eltern, die mich und meine Ausbildung von frühster Kindheit an im größten Maße förderten und unterstützten.

Regensburg im April 2010

Heiko Klarl

Zusammenfassung

Zugriffskontrollanforderungen von Geschäftsprozessen werden von der Fachseite oftmals nachrangig behandelt und zudem losgelöst und kaum formalisiert vom Modell des fachlichen Geschäftsprozesses erfasst. Bei der Implementierung von Zugriffskontrollpolicies kommt es daher zu einem fehleranfälligem und kompliziertem Abstimmungsprozess zwischen Fach- und IT-Abteilung oder es entstehen Inkonsistenzen zwischen den spezifizierten Zugriffskontrollanforderungen und den implementierten Zugriffskontrollpolicies. Ziel dieser Arbeit ist es, Fach- und IT-Seite bei der Absicherung von Geschäftsprozessen näher zusammen zu bringen und einen modellgetriebenen Softwareentwicklungsprozess für Zugriffskontrollpolicies zu ermöglichen. Zugriffskontrollanforderungen sollen dabei durchgängig von den Domänenmodellen der Fachabteilung bis zu plattformspezifischen Zugriffskontrollpolicies abgebildet werden.

In dieser Arbeit wird daher als Grundlage ein unternehmensweites Rollenkonzept entworfen, das die Schwächen bisheriger Rollenkonzepte umgeht. Es definiert die Begriffe „Geschäftsrolle“ und „Systemrolle“ und beschreibt in einem Metamodell deren Bezug zueinander sowie zu den Geschäftsprozessen, den Anwendern und den Anwendungssystemen des Unternehmens. Daran schließt sich ein Ansatz zur formalisierten Erfassung von Zugriffskontrollanforderungen in Geschäftsprozessmodellen auf Basis des entwickelten Metamodells für Zugriffskontrollinformationen. Die Fachabteilung wird in die Lage versetzt, mit einem Editor Zugriffskontrollinformationen visuell zu modellieren und diese, sowie Geschäftsrollen, in Geschäftsprozessmodelle einzubetten. Dafür wird die BPMN zur IdM-BPMN erweitert. Aus den abgesicherten Geschäftsprozessmodellen in IdM-BPMN können modellgetrieben plattformunabhängige und letztlich plattformspezifische Zugriffskontrollpolicies erzeugt werden. Diese Konzepte werden in einen modellgetriebenen Softwareentwicklungsprozess eingebettet, dessen Phasen im Zusammenhang mit den beteiligten Akteuren und deren Aufgaben, den erzeugten und verwendeten Artefakten sowie den Werkzeugen und Verzeichnissen aufgezeigt werden. Die Arbeit schließt mit einer Fallstudie in der gezeigt wird, wie ein Geschäftsprozess zur Kreditvergabe mit den beschriebenen Konzepten abgesichert wird und daraus modellgetrieben Zugriffskontrollpolicies erzeugt werden.

Schlagwörter: Zugriffskontrolle, Zugriffskontrollanforderungen, Zugriffskontrollpolicies, Identitätsmanagement, Geschäftsprozess, Geschäftsprozessmodellierung, Modellierung, Modellgetriebene Sicherheit, Rollenmodell
CCS: D.2.0, D.2.1, D.2.2, K.6.3, K.6.5

Abstract

Requirements regarding access control within business processes are often considered a low priority in the software development process by the business department. Furthermore, they are collected in a non-formalised manner and separated from the business processes model. At the time of the implementation of access control policies, this either results in an error-prone and complicated communication process between business and IT department or in inconsistencies between specified access control requirements and implemented access control policies. The aim of this work is to align the business site with the IT site while securing business process models and establishing a model-driven software development process. During the software development process, access control policies should be continuously considered, starting with the domain models of the business process and ending with platform-specific access control policies.

In this thesis, an enterprise-wide role model is designed as a basis, avoiding the weaknesses of existing concepts. It defines the terms “business role” and “system role” and their relation to each other in a meta-model which also covers the relation between the enterprises business processes, users, and IT systems. Subsequently, the formalised collection of access control requirements within business process models is supported by the meta-model for access control information. The business department is thus enabled to visually model access control information in a developed editor and can also attach them and business roles to business process models. The concept shows platform-independent and finally platform-specific access control policies created in a model-driven way. The phases of the model-driven development process are described in relation to the participating actors and their responsibilities, the created and used artefacts and the used tools and directories. A case study shows how a business process for credit applications is secured by the presented concepts and how platform-specific access control policies are generated using model-driven techniques.

Keywords: Access Control, Access Control Requirements, Access Control Policies, Identity Management, Business Process, Business Process Modeling, Modeling, Model-Driven Security, Role-Model

CCS: D.2.0, D.2.1, D.2.2, K.6.3, K.6.5

Inhaltsverzeichnis

1 Einleitung

Im vorliegenden Kapitel wird in den Themenbereich dieser Arbeit eingeführt. Beginnend mit der Darstellung des Szenarios werden im Anschluss die damit verbundenen Probleme konkretisiert und dadurch die Motivation dieser Arbeit dargelegt. Darauf aufbauend wird die Zielsetzung der Arbeit innerhalb vorgegebener Prämissen erarbeitet.

1.1 Einführung in das Szenario

Mit der rasanten Verbreitung des Internets und der immer stärkeren Durchdringung der Unternehmen mit Informationstechnik hat sich das geschäftliche Umfeld seit den 1990er Jahren stark verändert. Die ständige Verfügbarkeit der „Ware" Information definiert den Wettbewerb vor allem von global agierenden Unternehmen kontinuierlich neu. Auf Änderungen im Geschäftsmodell von Mitbewerbern muss genauso flexibel reagiert werden, wie neue, im Unternehmen ersonnene Verbesserungen und Geschäftsmodelle innerhalb der Anwendungssysteme umgesetzt werden müssen (vgl. Laudon et al., 2006, S. 31 f.). Das Paradigma der agilen Entwicklung ist nicht nur auf den reinen Softwareentwicklungsprozess gemünzt, sondern gilt gleichermaßen als Maxime für das gesamte Unternehmen (vgl. Perlitz et al., 1997).

Aber nicht nur der Wettbewerb zwischen den Unternehmen erfordert agiles Handeln, auch die zunehmenden Vorgaben und Regulierungen, sowie unternehmenseigene Regelungen – zusammengefasst unter dem Schlagwort *Compliance* – tragen dazu bei (vgl. Burling, 2005). Die Spannweite der Vorschriften reicht dabei von der Sicherstellung der Kreditwürdigkeit im Sinne von Basel II (vgl. Basel II, 2006), der Korrektheit der regelmäßig abzugebenden Finanzberichte im Rahmen des *Sarbanes-Oxley-Act (SOX)* (vgl. SOX, 2002), bis hin zum *Bundesdatenschutzgesetz (BDSG)* (vgl. BDSG, 2009). Zur Erfüllung dieser Vorgaben und um Missbrauch zu verhindern, ist eine schnelle und vollständige Umsetzung in den Anwendungssystemen erforderlich.

Bei der Umsetzung dieser fachlichen Vorgaben in den technischen Anwendungssystemen werden die zugrunde liegenden Geschäftsprozesse, die im Rahmen des Geschäftsprozessmanagements (*Business Process Management (BPM)*) möglichst

H. Klarl, *Zugriffskontrolle in Geschäftsprozessen,* DOI 10.1007/978-3-8348-9913-2_1,

vollständig erfasst werden, genutzt (vgl. Weske, 2007). Sie geben einem im Anwendungssystem umgesetzten Ablauf eine konkrete Repräsentation im Sinne eines Geschäftsprozessmodells, das von den Fachabteilungen des Unternehmens analysiert werden kann. Eine solche Analyse kann *Compliance*-relevante Stellen aufzeigen und im Anschluss daran den Handlungsbedarf für notwendige Anpassungen an den Anwendungssystemen definieren. Auch zur Verbesserung der Prozessabläufe, um im Sinne der Geschäftsprozessneugestaltung (*Business Process Reengineering*) Kosteneinsparungen oder Wettbewerbsvorteile zu erlangen, werden die Geschäftsprozessmodelle ausgewertet (vgl. Hammer und Champy, 1996). Zur vereinfachten technischen Umsetzung der Geschäftsprozesse in Anwendungssystemen hat sich seit Mitte der 1990er Jahre das Paradigma der *serviceorientierten Architektur (SOA)* entwickelt (vgl. Newcomer und Lomow, 2005; Richter et al., 2005). Kernfunktionalitäten des Anwendungssystems werden dabei in unabhängigen Diensten, den sogenannten Services gekapselt und innerhalb der informationstechnischen Infrastruktur des Unternehmens zur Verfügung gestellt. Grundlegende Funktionalität, zum Beispiel das Anlegen von Kundenstammdaten, wird nicht für jedes Anwendungssystem erneut – und dadurch mit zahlreichen Variationen – umgesetzt, sondern einmal entwickelte, als Dienst zur Verfügung gestellte Funktionalität wird in verschiedenen Anwendungen wiederverwendet. Dabei kann ein Dienst vollständig neu als Komponente entwickelt werden oder Funktionalität bestehender Anwendungssysteme kapseln und als definierte Schnittstelle zur Verfügung stellen. Das Anwendungssystem im Sinne einer serviceorientierten Architektur setzt sich lose gekoppelt aus verschiedenen Diensten zusammen, vergleichbar mit einem Baukasten, bei dem einzelne Bausteine zu komplexen Gebilden zusammengefügt werden können. Anpassungen des Anwendungssystems aufgrund von Änderungen der Geschäftsprozesse oder durch *Compliance*-Vorgaben können daher durch Rekombination oder Austausch einzelner Dienste effizient und mit relativ geringem Aufwand vorgenommen werden. Die engen Systemgrenzen klassischer Anwendungssysteme lösen sich dadurch auf und neue, „offene“ Anwendungssysteme entstehen.

Die Sicherheit des Anwendungssystems muss auch mit diesem neuen Architektur-Paradigma gewährleistet sein. Im Fokus dieser Arbeit steht dabei ein Teilaspekt der IT-Sicherheit, das *Identitätsmanagement (IdM)* (vgl. Mezler-Andelberg, 2008), insbesondere die Zugriffskontrolle. Im Rahmen der Zugriffskontrolle wird festgelegt, wer Zugriff auf welche Funktionalität des Anwendungssystems erhält. Beispielsweise kann für einen in den Anwendungssystemen umgesetzten Geschäftsprozess feingranular festgelegt werden, welcher Anwender auf welche Prozessschritte zugreifen darf. Mit der Abkehr von geschlossenen, monolithischen Anwendungssystemen mit engen Systemgrenzen hin zu offenen, lose gekoppelten,

serviceorientierten Anwendungssystemen haben sich die Voraussetzungen für das Identitätsmanagement grundlegend geändert (vgl. Emig, 2008, S. 3 f.). Das Identitätsmanagement muss die Zugriffskontrolle für diese lose gekoppelten Anwendungssysteme gewährleisten und deren anwendungssystemübergreifende Nutzung von Diensten unterstützen. Der Fachabteilung kommt dabei die Aufgabe zu, die nicht-funktionalen, grundsätzlich fachlich motivierten Anforderungen an die Zugriffskontrolle der Geschäftsprozesse zu spezifizieren. Diese Anforderungen werden von der Fachabteilung oftmals als nicht formalisierte Aussagen in Spezifikationsdokumenten gesammelt und existieren losgelöst vom abzusichernden Geschäftsprozess (vgl. Pohl, 2008, S. 229 ff.). Daraufhin beginnt ein Kommunikationsprozess zwischen der Fachabteilung und der IT-Abteilung mit dem Ziel, die Zugriffskontrollanforderungen vollständig zu spezifizieren und sie im Anschluss durch die IT-Abteilung in Zugriffskontrollpolicies zu überführen. Diese können in *Standardprodukten (Commercial off-the-shelf (COTS))* in einer IdM-Infrastruktur (vgl. Blum, 2005b) verwendet werden. Die zeitgleiche Implementierung, beziehungsweise Adaptierung, der Zugriffskontrollpolicies mit der fachlichen Anpassung des Geschäftsprozesses im Anwendungssystem muss dabei sicher gestellt sein, da andernfalls Inkonsistenzen zwischen der Anwendung und den Zugriffskontrollpolicies auftreten können.

Abbildung 1.1 zeigt das erläuterte Szenario. Auf der obersten Ebene befindet sich der fachliche Geschäftsprozess, der auf Seite der Informationstechnik als sogenannte Dienstkomposition (mittlere Ebene) von Basisdiensten umgesetzt ist. Diese Dienste (unterste Ebene) sind entweder eigens entwickelte Komponenten oder sie stellen lediglich gekapselte Funktionalität bereits bestehender Anwendungssysteme zur Verfügung und sind die elementaren Elemente der serviceorientierten Architektur. Das Identitätsmanagement ist als Querschnittseigenschaft auf den verschiedenen Ebenen zugegen. Auf der Ebene des Geschäftsprozesses beziehen sich Zugriffskontrollpolicies auf einzelne Prozessschritte, wohingegen auf Ebene der Dienstkomposition Zugriffskontrollpolicies die verknüpften Dienstschnittstellen der Basisdienste absichern.

1.2 Problemstellung und Zielsetzung

Im vorhergehenden Abschnitt wurde in das Szenario dieser Arbeit eingeführt, allerdings noch ohne explizit dessen Probleme in Bezug auf die Zugriffskontrolle hervorzuheben. Dieser Abschnitt konkretisiert die Probleme und damit die Motivation der vorliegenden Arbeit, um darauf aufbauend die Zielsetzung zu erarbeiten.

Der immer kürzer werdende Lebenszyklus von Geschäftsprozessen verursacht

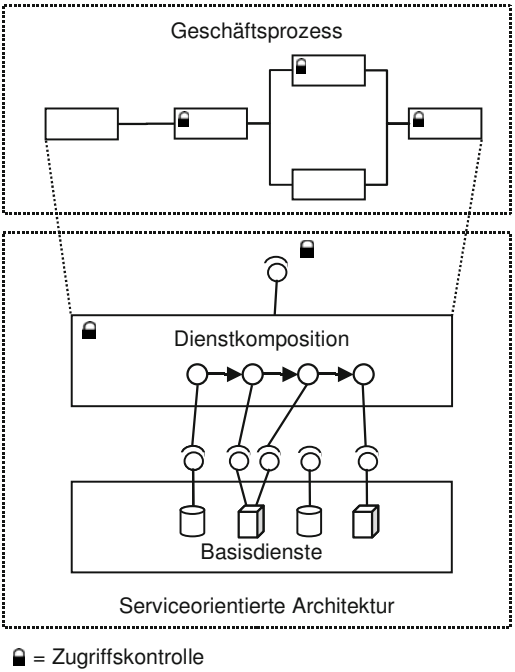

Abbildung 1.1: Abgesicherter Geschäftsprozess in einer serviceorientierten Architektur

eine immer schnellere Anpassung der zugrunde liegenden Anwendungssysteme, um den Herausforderungen des globalen Wettbewerbs gerecht zu werden. Änderungen von gesetzlichen Vorgaben und Regularien sowie von internen Regeln und Vorschriften erhöhen den Anpassungsdruck, vor allem da die Änderungen in der Regel innerhalb vorgegebener Fristen in den Anwendungssystemen umgesetzt werden müssen. Mit den Änderungen an den Geschäftsprozessen geht jedoch auch ein Anpassungsbedarf bei den Zugriffskontrollanforderungen und den darauf aufbauenden Zugriffskontrollpolicies einher. Zugriffskontrolle als ein Aspekt der Sicherheit von Informationssystemen gerät als klassische Querschnittseigenschaft während des Softwareentwicklungsprozesses sehr leicht in den Hintergrund (vgl. Lodderstedt, 2003, S. 11 f.). Für die Fachabteilung besitzt die Umsetzung der fachlichen Änderung höchste Priorität. Daher steht die Entwicklung der fachlichen Komponenten im Vordergrund. Die Absicherung des Geschäftsprozesses, also die Spezifizierung von Zugriffskontrollanforderungen und die Erzeugung, be-

ziehungsweise Erweiterung von Zugriffskontrollpolicies, wird oftmals erst zum Ende der Implementierungsphase oder im Nachhinein vorgenommen und nicht schon in den wichtigen Phasen der Analyse und des Entwurfs berücksichtigt. Dabei spezifiziert die Fachabteilung die Zugriffskontrollanforderungen oft wenig formalisiert in verschiedenen Dokumenten, die losgelöst vom abzusichernden Geschäftsprozess existieren. Liegen diese Dokumente nur lückenhaft und im Jargon der Fachdomäne vor, beginnt ein komplizierter und fehleranfälliger Abstimmungsprozess zwischen der Fach- und der IT-Abteilung mit dem Ziel, der IT-Abteilung Wissen über die fachlichen Anforderungen zu vermitteln und so Lücken in den Spezifikationen zu schließen (vgl. Cormack et al., 2001). Am Beispiel des unterschiedlichen Verständnisses für den Begriff „Rolle“ innerhalb eines Anwendungssystems ist dies gut zu erkennen. Während auf der Fachseite „Rolle“ einen fachlichen Ursprung, oftmals angelehnt an die Aufgaben des Mitarbeiters hat, so ist in den technischen Anwendungssystemen eine Rolle oftmals an die technische Funktionalität ohne Bezug zur Fachlichkeit gebunden. Nimmt die IT-Abteilung selbst die Spezifikation der Anforderungen vor, so besteht die Gefahr, wichtige Aspekte der Zugriffskontrolle aufgrund des anderen Blickwinkels der Fachabteilung zu übersehen, zumindest aber verliert die Fachabteilung die Hoheit über die Zugriffskontrollanforderungen. Diese sollten aber – aufgrund ihrer fachlichen Motivation – zur Gänze bei ihr liegen. Im ungünstigsten Fall werden die beabsichtigten, aber nicht ausreichend spezifizierten Zugriffskontrollanforderungen nicht ordnungsgemäß im Anwendungssystem zu Zugriffskontrollpolicies umgesetzt, was eine mangelhafte Absicherung desselben zur Folge hat. Diese nachrangige Behandlung der Sicherheitsaspekte ist fehleranfällig und entspricht nicht den Prinzipien einer ingenieurmäßigen Konzeption von Anwendungssystemen, bei der das gesamte System die Phasen Analyse, Entwurf und Implementierung durchläuft (vgl. Frick, 1995, S. 34 ff.). Etablierte Verfahren des Anforderungsmanagements (vgl. Schienmann, 2002; Hull et al., 2002) tragen zwar dazu bei, die Kommunkationslücke zwischen Fach- und IT-Seite zu schließen, können aber die Komplexität der Querschnittsfunktionalität der Zugriffskontrolle nicht gleichermaßen gut abbilden, wie beispielsweise Anforderungen an den rein fachlichen Teil eines Anwendungssystems. Ursächlich hierfür ist neben dem unterschiedlichen, domänenspezifischen Vokabular der Beteiligten unter anderem die Trennung zwischen der Spezifikation der fachlichen Anforderungen, beispielsweise in Geschäftsprozessmodellen und die davon losgelöste Spezifikation von Zugriffskontrollanforderungen in separaten Spezifikationsdokumenten. Diese Trennung des Geschäftsprozessmodells auf der einen und den dazugehörigen Zugriffskontrollanforderungen auf der anderen Seite kann sehr leicht zu Inkonsistenzen führen, wenn Änderungen nicht unmittelbar und vollständig in allen Spezifikationsdokumenten vorgenommen werden.

In eigenen Vorarbeiten (vgl. Klarl, 2007) wurden idealtypische Ziele formuliert, die erst umgesetzt werden können, wenn die Ziele dieser Arbeit erreicht und somit die Grundlagen dafür geschaffen wurden. Zu den Zielen mit Vorbedingung zählt die Beschreibung von organisatorischen Meta-Zugriffskontrollpolicies, die globale Sicherheitsvorgaben des Unternehmens definieren und die für konkrete Geschäftsprozesse „instanziert" werden oder die Beschreibung von Sicherheitsmustern in einem Musterkatalog zur mustergestützten Wiederverwendung von Zugriffskontrollanforderungen.

Die benötigte Grundlagen und die in diesem Abschnitt aufgezeigte Problematik motivieren verschiedene Maßnahmen zur Verbesserung der derzeitigen Situation, die im Rahmen dieser Arbeit erreicht werden sollen und nachfolgend als Ziele vorgestellt werden.

Ziel Z 1: Entwurf eines unternehmensweiten Rollenkonzepts

In existierenden Anwendungssystemen kommt zur Autorisierung von Zugriffen oftmals das Konzept der *rollenbasierten Zugriffskontrolle (RBAC)* zum Einsatz (vgl. Ferraiolo et al., 2001). Der Zugriff wird dann gewährt, wenn der handelnde Akteur beim Zugriff auf eine bestimmte Funktionalität des Anwendungssystems einer bestimmten Rolle angehört. Die traditionelle rollenbasierte Zugriffskontrolle ist dabei auf ein Anwendungssystem beschränkt. Die zu entwickelnde rollenbasierte Zugriffskontrolle soll weiterhin die Abbildung von anwendungsspezifischen Rollen ermöglichen, aber zugleich auch anwendungsübergreifende Rollenbezeichnungen aus der Fachdomäne einbinden und verknüpfen, die beispielsweise Tätigkeitsprofile der Mitarbeiter genauer definieren. Die beiden verschiedenen, das heißt aus der technischen sowie der fachlichen Domäne kommenden Rollenbegriffe werden dabei miteinander in Beziehung gesetzt. Zum einem erhöht dies die Verständlichkeit zwischen Fach- und IT-Seite, da die unterschiedlichen Rollenbezeichnungen in die „eigene" Sprache aufgelöst werden können, zum anderen wird im Rahmen eines modellgetriebenen Entwicklungsprozesses die automatische Auflösung fachlicher in technische Rollen ermöglicht.

Ziel Z 2: Verknüpfung von Zugriffskontrollanforderungen und Geschäftsprozessmodellen

Zugriffskontrollanforderungen existieren oftmals losgelöst von den Geschäftsprozessmodellen in Spezifikationsdokumenten, was zu erhöhtem Pflegeaufwand sowie zu Inkonsistenzen zwischen Modellen und Dokumenten führen kann. Der fachliche Hintergrund der Zugriffskontrollanforderungen legt die Erfassung durch

die Fachseite in den Geschäftsprozessmodellen bereits mit Beginn des Softwareentwicklungsprozesses nahe. Die Erfassung der Zugriffskontrollanforderungen muss für die Fachabteilung zu bewerkstelligen sein. Die leichtgewichtige Erweiterung (vgl. OMG, 2009d, S. 653 ff.) bestehender und bewährter Notationen für die Geschäftsprozessmodellierung ist dabei zu bevorzugen, da dies einerseits die Kompatibilität zu bestehenden Modellen und Werkzeugen gewährleistet und andererseits die Anwender die ihnen bereits bekannten Notationen weiterhin verwenden können. Die Abbildung von Zugriffskontrollanforderungen im Geschäftsprozessmodell soll einen modellgetriebenen Entwicklungsprozess von Zugriffskontrollpolicies ermöglichen.

Zielerweiterung ZE 2.1: Modellierungswerkzeuge für Zugriffskontrollanforderungen und Zugriffskontrollpolicies und deren Verknüpfung mit Geschäftsprozessmodellen

Das Ziel Z 2 umfasst die Verknüpfung von Zugriffskontrollanforderungen und Zugriffskontrollpolicies mit Geschäftsprozessmodellen und bildet damit die Grundlage für eine Umsetzung in einem Modellierungswerkzeug. Dieses Werkzeug soll die Fachabteilung in die Lage versetzen, Zugriffskontrollanforderungen und Zugriffskontrollpolicies visuell zu formulieren und somit zugleich bei einer formalisierten Erfassung unterstützen. Das Modellierungswerkzeug soll ferner die Modellierung von Geschäftsprozessen ermöglichen, damit die Fachabteilung ihre Zugriffskontrollanforderungen und Zugriffskontrollpolicies mit den Geschäftsprozessmodellen innerhalb desselben Werkzeugs verknüpfen kann.

Zielerweiterung ZE 2.2: Modellgetriebener Softwareentwicklungsprozess von Zugriffskontrollpolicies

Im Ziel Z 2 werden durch die Verknüpfung von Zugriffskontrollanforderungen und Geschäftsprozessmodellen die Grundlagen für einen modellgetriebenen Softwareentwicklungsprozess (vgl. OMG, 2001, 2003) für Zugriffskontrollpolicies bereitet. Die modellgetriebene Verarbeitung von Zugriffskontrollanforderungen und Zugriffskontrollpolicies reduziert manuelle Arbeiten und trägt damit sowohl zur Vermeidung von Inkonsistenzen, aber auch zu einer kürzeren Entwicklungszeit bei (vgl. Hitz et al., 2005, S. 345; Pietrek und Trompeter, 2007, S. 16 f.). Eine Transformation soll aus Zugriffskontrollpolicies im Domänenmodell des Geschäftsprozesses plattformunabhängige Zugriffskontrollpolicies erzeugen, die zwar eine manuelle Anreicherung mit weiteren Informationen benötigen, aber ansonsten – wie

in (Emig, 2008, S. 165 ff.) beschrieben – automatisch in plattformspezifische Zugriffskontrollpolicies für Standardprodukte für die Zugriffskontrolle transformiert werden können.

1.3 Prämissen der Arbeit

Sicherheit in der Informationstechnologie, im konkreten Fall die Zugriffskontrolle, ist eine Querschnittsfunktionalität (vgl. Moreira et al., 2002). Bei Bearbeitung dieses Themenkomplexes werden daher verschiedene Themengebiete berührt, ohne jedoch selbst im Fokus zu sein. Dieser Abschnitt gibt daher Einschränkungen und Vorbedingungen wieder, die zur Eingrenzung des Themas getroffen wurden.

Prämisse P 1: Unternehmensweites Identitätsmanagement

Das Identitätsmanagement gehört zu den Hauptbestandteilen in der Sicherheitsarchitektur einer Organisation (vgl. Götzfried, 2007). Es umfasst dabei unter anderem die Bereiche Authentifizierung von Identitäten, die Autorisierung und Autorisierungsprüfung von Zugriffen sowie die Protokollierung relevanter Ereignisse zu Auditierungszwecken. Diese drei Säulen sind in verschiedene Prozesse eingebettet, um die Komplexität des IdM verwalten zu können. Die Provisionierung von Identitäten und Identitätsattributen begleitet den gesamten Lebenszyklus einer Identität, beginnend bei der Kontoanlage in verschiedenen Systemen beim Eintritt eines Mitarbeiters in ein Unternehmen über die Aktualisierung von Attributen während der Anstellung und endend mit dem Entfernen der Identität aus den Systemen beim Austritt des Mitarbeiters aus dem Unternehmen. Die Verwaltung und Vergabe von Berechtigungen wird durch Beantragungs-, Freigabe- und wiederum Provisionierungsprozesse gestützt. Die vorliegende Arbeit beschränkt sich dabei auf den Bereich der Autorisierung. Andere Bereiche des Identitätsmanagements werden nur berührt, falls dies für die Umsetzung der in Abschnitt 1.2 definierten Ziele erforderlich ist.

Die modellgetriebene Erzeugung von plattformunabhängigen Zugriffskontrollpolicies bildet einen wesentlichen Teil dieser Arbeit. Zur Abbildung dieser Policies wird die Policy-Sprache *Web Services Access Control Markup Language (WSACML)* (vgl. Emig, 2008, S. 156 ff.) verwendet.