Abbildung von Zugriffskontrollaussagen in Geschäftsprozessmodellen

Heiko Klarl[1, 2], Christian Wolff[1], Christian Emig[3]

[1]Institut für Medien-, Informations- und Kulturwissenschaft, Universität Regensburg
[2]iC Consult GmbH, Keltenring 14, 82041 Oberhaching
[3]Cooperation Management, Universität Karlsruhe (TH)

h.klarl[at]klarl.eu, christian.wolff[at]sprachlit.uni-regensburg.de, emig[at]cm-tm.uka.de

Abstract: Die Modellierung von Geschäftsprozessen ist weit verbreitet. Bisher werden aber Anforderungen des Identitätsmanagements, insbesondere Anforderungen an die Zugriffskontrolle, nur separat in Spezifikationsdokumenten oder erst auf technologischer Ebene erfasst. Die fachlichen Hintergründe der Zugriffskontrollanforderungen legen eine Erfassung dieser bereits im Modell des Geschäftsprozesses durch die Fachabteilung nahe. Diese Arbeit stellt ein UML2-Profil für die Erweiterung des Aktivitätsdiagramms zur Erfassung von Zugriffskontrollaussagen vor. Auf Basis eines Metamodells kann die Fachabteilung sämtliche Zugriffskontrollanforderungen abbilden und dadurch die Konsistenz zwischen Geschäftsprozess und dessen Sicherheitsanforderungen auch über Änderungen hinweg erhalten.

1 Identitätsmanagement und Geschäftsprozessmodellierung

Obwohl die Modellierung von Geschäftsprozessen durch eine Vielzahl ausgereifter Notationen [OMG06a, OMG07a, KNS92] und eine gute Werkzeugunterstützung bereits gelebte Praxis ist, ist die Abbildung von Anforderungen, die deutlich über den Prozessablauf hinausgehen, nicht weit verbreitet. Im Rahmen des Identitätsmanagements (*Identity Management*, IdM), zu dessen Bestandteilen die Zugriffskontrolle gehört, fallen eine Vielzahl von Anforderungen an, die den Zugriff auf einzelne Schritte des Geschäftsprozesses beschreiben. Diese Anforderungen werden oftmals von der Fachabteilung als nicht formalisierte Aussagen in Spezifikationsdokumenten gesammelt und existieren losgelöst vom abzusichernden Geschäftsprozess. Liegen diese Dokumente nur lückenhaft vor, beginnt ein 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. Zu diesem Zeitpunkt stellt nicht mehr der Eigentümer des Prozesses alle Anforderungen an die Zugriffskontrolle zur Verfügung, er verlässt sich vielmehr auf die Unterstützung seitens der „fachfremden“ IT-Spezialisten. Die Trennung von Geschäftsprozessmodell und dessen Anforderungen an das Identitätsmanagement führt leicht zu Inkonsistenzen, wenn Änderungen nicht unmittelbar in beiden Anforderungsbeschreibungen nachgezogen werden. Die vorliegende Arbeit löst diese Problematik durch

Integration der IdM-Anforderungen in das Modell des Geschäftsprozesses und liefert damit auch einen Beitrag für einen durchgängig modellgetriebenen Softwareentwicklungsprozess im Sinne der *Model Driven Architecture* (MDA) [OMG01].

Die Arbeit gliedert sich wie folgt: Abschnitt 1.1 gibt einen kurzen Abriss über das Identitätsmanagement und seine Elemente. Daran anschließend wird in Abschnitt 1.2 der Zusammenhang zwischen Identitätsmanagement und der Geschäftsprozessmodellierung aufgezeigt. Der aktuelle Forschungsstand und verwandte Arbeiten werden in Abschnitt 1.3 vorgestellt. Das als Lösungsansatz entwickelte UML2-Profil für das Identitätsmanagement wird in Abschnitt 2 erklärt, auf Anwendungsbeispiele geht Abschnitt 3 ein. Der Beitrag schließt mit einer Zusammenfassung der vorgestellten Ergebnisse und einen Ausblick auf zukünftige Forschungsarbeiten in Abschnitt 4.

1.1 Identitätsmanagement und seine Elemente

Aufgrund der Komplexität der IT-Landschaft größerer Unternehmen, der z. Z. kurzen Lebenszyklen eingesetzter Software und der immer umfassenderen Unterstützung und Abwicklung unternehmenskritischer Prozesse durch Informationstechnologie ist das Identitätsmanagement zu einem Schlüsselfaktor der IT-Sicherheit geworden [Gö07]. Das Identitätsmanagement gehört zu den Hauptbestandteilen in der Sicherheitsarchitektur einer Organisation. Es umfasst dabei unter anderem die Bereiche Authentisierung von Identitäten, die Autorisierung 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 Lebenszeit und endend mit dem Entfernen der Identität aus den Systemen beim Austritt aus dem Unternehmen. Die Verwaltung und Vergabe von Berechtigungen wird durch Beantragungs-, Freigabe- und wiederum Provisionierungsprozesse gestützt. In [Blu05] wird eine beispielhafte Referenzarchitektur für das Identitätsmanagement, in [Hom07] eine Architektur für föderiertes Identitätsmanagement vorgestellt. Berechtigungen, eine der sichtbarsten Auswirkungen des IdM für den Endbenutzer, bilden die Grundlage für Zugriffskontrollentscheidungen. Sie autorisieren einen Zugriff auf ein Objekt auf Basis einer vorangegangen Authentisierung eines Subjekts und legen dadurch fest, wer oder was im Softwaresystem in welcher Weise agieren kann. Im Rahmen von gesetzlichen Regelungen, wie zum Beispiel dem Sarbanes-Oxley-Act für in den USA börsennotierte Unternehmen, steigen die Anforderungen an die Verwaltung und Dokumentation von Zugriffsberechtigung im Rahmen des IdM, was die Notwendigkeit eines professionellen und umfassenden IdM-Betriebs erhöht.

1.2 Identitätsmanagement in der Geschäftsprozessmodellierung

Mit den Ansätzen zur Geschäftsprozessneugestaltung [Ham90] in den 1990er Jahren und dem Paradigma der serviceorientierten Architekturen [RHS05] ist die Bedeutung modellierter Geschäftsprozesse stark gestiegen. Die nahezu beliebige Kombination einzelner Subprozesse oder Dienste im Sinne einer serviceorientierten Architektur zu neuen Geschäftsprozessen kann nur auf Basis aussagekräftiger und möglichst ausführbarer Modelle geschehen. Dies versetzt Unternehmen in die Lage, flexibel und agil auf Herausforderungen des Marktes oder Änderungen gesetzlicher Rahmenbedingungen zu reagieren [Kla07]. Ziel ist dabei immer die optimale Unterstützung des Geschäftsnutzens, die IT ist dabei in der Rolle des „Erfüllungsgehilfens“. Zur Modellierung von Geschäftsprozessen haben sich verschiedene Notationen etabliert, unter anderem die ereignisgesteuerten Prozessketten (EPK) [KNS92], die *Business Process Modelling Notation* (BPMN) [OMG06a] und die Verhaltensdiagramme der *Unified Modeling Language* (UML) [OMG07a].

Der kurze Lebenszyklus von Geschäftsprozessen sowie deren Öffnung nach Außen, beispielsweise in B2B-Szenarien, erfordert neben der fachlichen Anpassung an diese neuen Szenarien eine ständige Aktualisierung der Anforderungen an die Zugriffskontrolle [KP06]. Einerseits ändern sich fachliche Vorgaben in Bezug auf Identitäten, Rollen und Zugriffsberechtigung. Auf der anderen Seite fließen immer mehr sich ändernde Vorgaben aus organisatorischen Richtlinien des Unternehmens, wie Mechanismen zur Korruptionsbekämpfung, oder gesetzlicher Regelungen, wie zum Beispiel auf dem Gebiet des Datenschutzes, mit ein.Um diesen Anforderungen gerecht zu werden, ersetzen dynamisch änderbare Sicherheitsrichtlinien (*Policies*) hart verdrahtete Sicherheitsmechanismen in den Applikationen.

Der Lückenschluss zwischen Spezifikation der Anforderungen an das Identitätsmanagement in Dokumenten oder Werkzeugen zur Anforderungserfassung und dem Modell des abzusichernden Geschäftsprozesses hat bis dato nicht stattgefunden, was zu verschiedenen sich ergänzenden Teilspezifikationen führt. Eine wünschenswerte enge Kopplung zwischen Modell des Geschäftsprozesses und dessen Sicherheitsanforderungen gewährleistet einen konsistenten Zustand auch über Prozessänderungen – und daraus entstehenden Änderungen der Sicherheitsanforderungen – hinweg: Das Management sicherheitsrelevanter Aspekte kann dadurch enger an den Entwicklungsprozess der Geschäftsprozesse gebunden werden und Inkonsistenzen bei der Absicherung sind leichter zu vermeiden. Zusätzlich lassen sich für die Fachabteilung Werkzeuge entwickeln, mit denen nicht nur in bekannter Weise der Geschäftsprozess modelliert werden kann, sondern zusätzlich auch die Sicherheitsanforderungen, die vor allem durch die Fachabteilung entstehen, integriert werden können.

1.3 Forschungsstand und verwandte Arbeiten

Eine Vielzahl von Arbeiten beschäftigt sich mit der Integration von Anforderungen in Modellen. Ein Teil der Arbeiten beschäftigt sich mit Geschäftsprozessmodellen, die bereits

auf der Seite der Fachabteilungen akzeptiert sind und verwendet werden. Ein anderer Teil modelliert die Anforderungen vor allem in IT-zentrischen Modellen wie beispielsweise UML-Klassendiagrammen, die fast ausschließlich von IT-Fachleuten erstellt, verwendet und verstanden werden.

In [KL06a] wird das UML2-Aktivitätsdiagramm zur Darstellung von Geschäftsprozessen um Artefakte zur Modellierung von Geschäfts- und Leistungszielen angereichert. Diese betriebswirtschaftlichen Anforderungen sind ein wichtiger Bestandteil in der Verwaltung von Geschäftsprozessen und werden in Konzepten wie der *Balanced Scorecard* eingesetzt. Zur Modellierung ereignisgesteuerte Prozessketten (EPK) [KNS92], einem wesentlichen Bestandteil des ARIS Konzepts [SN00], wird in [KL06b] das UML2-Aktivitätsdiagramm erweitert. Elemente der EPK wie beispielsweise Ereignis, Funktion und Informationsobjekt werden in einem UML2-Profil abgebildet und können anschließend zu semantisch korrekten Geschäftsprozessmodellen mit Unterstützung gängiger UML-Werkzeuge modelliert werden.

Im Bereich der Informationssicherheit stellt [RFMP06] ein UML2-Profil zur deskriptiven Erfassung der Anforderungen vor. In [RFMP07] wird der gleiche Ansatz als Erweiterung für die BPMN vorgestellt. Im Geschäftsprozessmodell des Aktivitätsdiagramm werden dabei verschiedene Stereotypen wie „SecurityAuditing“ oder „SecurityRequirement“ eingeführt, um Anforderungen zur Auditierung oder die klassischen Sicherheitsanforderungen wie Zugriffskontrolle, Nichtveränderbarkeit sowie Integrität von Daten, Software und Personen feststellen zu können. Dabei verbleibt die Arbeit allerdings bei reinen Anmerkungen, hinter den Stereotypen verbirgt sich kein weiterer Informationsgehalt, sie stellen daher lediglich einen verbesserten, weil klassifizierten Kommentar dar. In der Zukunft sollen diese Anmerkungen mit konkreten Anforderungen oder einer Logik hinterlegt werden können.

Bei den IT-zentrischen Ansätzen zur Modellierung von Anforderungen wird in [Jue05] ein UML-Profil namens UMLsec zur Modellierung sicherheitskritischer Systeme vorgestellt. UML-Modelle können damit um Informationen zu sicherheitsrelevanten Anforderungen angereichert werden. Die Zielgruppe dieser Erweiterung liegt bei Entwicklern mit dedizierten Kenntnissen im Gebiet der IT-Sicherheit. Die Abbildung von Zugriffskontrollaussagen, im Speziellen bereits auf der Ebene der Fachabteilung, wird nicht berücksichtigt. Lodderstedt stellt in [LBD02] eine UML-basierte Modellierungssprache kombiniert mit einer Sprache zur Spezifikation von Zugriffskontrollmodellen vor. Dieser Ansatz greift allerdings ebenfalls relativ spät im Rahmen des Softwareentwicklungsprozesses, da die Anforderungen erst im Klassendiagramm eingefügt werden. Zielgruppe ist auch hier der Entwickler mit Kenntnissen im Gebiet der IT-Sicherheit. Muster zur Absicherung von Webservices werden in [IT03] vorgestellt. Diese sog. Idiome, die auf die orchestrierten Dienst angewandt werden, enthalten zu vorab definierten Bedrohungsszenarien technische Lösungsvorschläge und Schablonen, um diese zu konkretisieren. Sie kapseln somit nichtfunktionale Anforderungen an das Softwaresystem, berücksichtigen diese allerdings erst zum Zeitpunkt der Orchestrierung der einzelnen Services. Eine explizite Abbildung von IdM-Anforderungen ist nicht vorgesehen.

Mit dem Thema der sicheren Geschäftsprozessverwaltung setzten sich Neubauer et al. [NKB06] auseinander. Der Lebenszyklus eines Geschäftsprozesses wird in seinen ver-

schiedenen Phasen betrachtet und existierende Ansätze zur Integration von Sicherheitsaspekten vorgestellt. Sie entwickeln eine Methodologie, die mit dem Durchlaufen der vorgestellten Phasen die Integration von Sicherheitsaspekten in Geschäftsprozesse erheblich verbessern soll. In der zweiten Phase wird dabei der mit Sicherheitsaspekten angereicherte Geschäftsprozess angesiedelt, der die Grundlage für die Ausführung in Workflowsystemen darstellt. In diese Phase lässt sich das hier vorgestellte UML2-Profil einordnen.

Weitere Ansätze zur Integration von Zugriffskontrollinformationen in Notation wie BPMN und EPK sind – außer den vorgestellten – nicht bekannt.

Dieser Ausschnitt aus verwandten Forschungsarbeiten lässt erkennen, dass die Modellierung von Geschäftsprozessen aus nahe liegenden Gründen stark auf klassische betriebswirtschaftliche Aspekte hin ausgelegt ist. Konkrete Möglichkeiten, sicherheitsrelevante Anforderungen, die über reine Anmerkungen hinausgehen, in die Modelle zu integrieren, finden sich erst auf einer tieferen, technischen Ebene. Für diese sind allerdings sowohl Kenntnisse der Modellierung und Architektur von Softwaresystemen als auch ein ausgeprägtes Wissen über deren Sicherheitslösungen erforderlich. Insgesamt ergibt sich die erwähnte Zweiteilung in auf der Ebene der Fachabteilung modellierte Geschäftsprozesse einerseits, und in Dokumenten oder Werkzeugen zur Anforderungserfassung hinterlegte Sicherheitsspezifikationen andererseits. Das Modell ist damit von seinen Sicherheitsanforderungen vollständig losgelöst. Erst auf technischer Ebene gibt es Ansätze, diese Anforderungen in Modellen zu hinterlegen, eine Abbildung von Zugriffskontrollaussagen ist aber auch in diesem Bereich nicht verfügbar.

2 Das UML2-Profil für das Identitätsmanagement

Damit IdM-Anforderungen konsistent mit den sich schnell ändernden Geschäftsprozessen bleiben, sollten diese Anforderungen im selben Modell wie der Geschäftsprozess definiert werden. Der Fachabteilung muss die Möglichkeit gegeben werden, die von ihr oder von Compliance-Regeln getriebenen Anforderungen an die Zugriffskontrolle größtenteils selbst umzusetzen, da in der Fachabteilung auch das entsprechende Domänenwissen vorhanden ist. Mit der Abkehr von separat erfassten und oftmals nur in natürlicher Sprache vorliegenden Sicherheitsspezifikationen im Bereich der Zugriffskontrolle wird die Konsistenz zwischen Geschäftsprozess und dessen IdM-Anforderungen erhöht und der Weg für einen vollständigen modellgetriebenen Softwareentwicklungsprozess geebnet, der mit der Modellierung der Zugriffskontrollanforderungen in der Fachabteilung beginnt und mit der technologiespezifischen Ausprägung konkreter Zugriffskontrollrichtlinien für das Softwaresystem endet.

Dieser Abschnitt stellt daher ein UML2-Profil für die Erfassung von Anforderungen an das Identitätsmanagement in Geschäftsprozessmodellen vor. Die Wahl fiel aus verschiedenen Gründen auf die Erweiterung der UML. Das Ziel dieser und verwandter Arbeiten (vgl. [EKA+08]) ist eine modellgetriebene Erzeugung von konkreten Zugriffskontrollaussagen ausgehend von der fachlichen Ebene des Geschäftsprozesses. Da Standardsoftwarewerkzeuge einen UML-gestützten modellgetriebenen Ansatz mittlerweile gut beherrschen

[Sto06], kann die konzeptuelle Idee ohne zusätzliche Hürden im Bereich der Werkzeugunterstützung aufgezeigt werden. An eine kurze Einführung zu den Grundlagen der UML2-Profile schließt sich eine Beschreibung des Modells, der Bestandteile sowie der nötigen *Constraints* des UML2-Profils für IdM an.

2.1 Erweiterbarkeit der *Unified Modeling Language* durch Profile

Die UML kann für ihren Einsatz in bestimmten Domänen angepasst werden. Um keine nur eingeschränkt nutzbaren Erweiterungen zu schaffen, werden dabei mittels eines „leichtgewichtigen“ Ansatzes Metaklassen auf Ebene des Metamodells erweitert (vgl. [OMG07a, OMG07b]). Die Grundlagen für diese Erweiterungen stellt das UML-Package *profile* zur Verfügung. Mit sog. Stereotypen wird nicht das Metamodell verändert, sondern bestehende Metaklassen für einen bestimmten Einsatzzweck erweitert und genauer spezifiziert. Sie erhalten dabei einen eigenen Namen und können fortan als Element des UML-Profils verwendet werden. Mittels *Constraints* können Stereotypen in Prosa, (Pseudo-)Programmiersprachen oder dedizierten Sprachen wie der OCL (*Object Constraint Language*) [OMG06b] mit Einschränkungen belegt werden. *Constraints* dürfen dabei nicht im Widerspruch zu Einschränkungen der erweiterten Metaklasse stehen. *Tagged Values*, mit Werten vorbelegte Attribute, reichern Stereotypen mit zusätzlichen Informationen an. Syntax und Semantik der UML bleiben von den Erweiterung mittels eines UML-Profils unberührt.

Das Aktivitätsdiagramm ist eines der Verhaltensdiagramme der UML und stellt elementare Bestandteile zur Beschreibung des Verhaltens von Kontroll- und Datenflüssen wie zum Beispiel Geschäftsprozessen zur Verfügung [OMG07b, BHK04]. Hauptbestandteile einer Aktivität sind Aktionen und Objekte, die als Knoten visualisiert und mit Kanten zur Darstellung des Kontroll- bzw. Objektflusses verbunden werden. Reichen die im Aktivitätsdiagramm vorhandenen Elemente zur Abbildung der Anforderungen der jeweiligen Domäne nicht aus, so stellen UML-Profile die benötigten Erweiterungen zur Verfügung. So ermöglicht [KL06a] Elemente zur Abbildung von Geschäftsprozesszielen sowie die Angabe von Kenngrößen zur Verwendung als *Key-Performance*-Indikatoren und [KL06b] passt das Aktivitätsdiagramm an, um ereignisgesteuerte Prozessketten (EPK) [KNS92] modellieren zu können.

2.2 Modell des UML2-Profils für das Identitätsmanagement

Das hier eingeführte UML2-Profil für das IdM ermöglicht es, Zugriffskontrollaussagen bereits im Aktivitätsdiagramm zu modellieren. Im konkreten Fall eines Geschäftsprozesses entsteht somit die Möglichkeit, einerseits das konkrete Verhalten und andererseits zugleich Einschränkungen für den Zugriff abbilden zu können.

Das Metamodell des Profils basiert auf dem in [EBA+07] vorgestellten Metamodell zur Zugriffskontrolle in web-serviceorientierten Architekturen (WSOA). Im Fokus des WSOA-

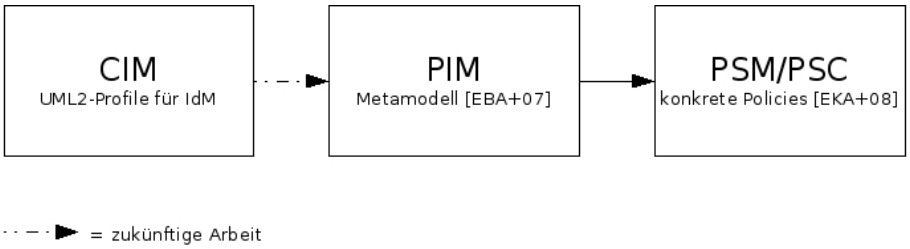

Abbildung 1: Einordnung der Arbeit in die Schichten der OMG MDA

Metamodells liegt dabei die Modellierung der Zugriffskontrolle für einzelne Webservices und die daraus modellgetrieben Erzeugung konkreter Zugriffsrichtlinien. Anlehnend an die verschiedenen Modelleebenen der MDA [OMG01] entspricht das in diesem Beitrag vorgestellte Metamodell dem *Computational Independent Model* (CIM), wohingegen das in [EBA$^+$07] vorgestellte Metamodell dem *Platform Independent Model* (PIM) entspricht, das bereits über das *Platform Specific Model* (PSM) zu *Platform Specific Code* (PSC) im Sinne von konkreten produktspezifischen Zugriffskontrollrichtlinien transformiert werden kann (vgl. Abb. 1).

WSOA-spezifische Elemente wurden dabei nicht übernommen und Ergänzungen für eine konkrete Abbildung von Zugriffskontrollaussagen sowie für das Aktivitätsdiagramm relevante Elemente wurden ergänzt. Abbildung 2 zeigt das Metamodell für das UML2-Profil für IdM. Innerhalb des gestrichelten Kastens befindet sich exemplarisch das in [EBA$^+$07] dargestellte Policy-Modell, das im Weiteren aber nicht näher behandelt wird.

Die Elemente ≪Policy≫ und ≪Permission≫ werden bereits in [EBA$^+$07] eingehend beschrieben und sind in ihrer Bedeutung nicht verändert worden. Das Element ≪Policy≫ dient zur disjunkten Verknüpfung einzelner ≪Permission≫-Elemente. Dieses Konstrukt ermöglicht als Container die Wiederverwendung einzelner ≪Permission≫-Objekte, da diese in verschiedenen ≪Policy≫-Elementen Verwendung finden können. Die Attribute *complianceClassifier* und *securityClassifier* ermöglichen eine Einordnung der ≪Policy≫ in die Compliance- und Sicherheitsvorgaben der jeweiligen Organisation. Um Konflikte durch widersprüchliche Aussagen zu vermeiden, kann ein Element immer nur eine ≪Policy≫ zugewiesen haben. Das Element ≪Permission≫ beinhaltet die eigentliche Zugriffskontrollaussage, die als positive Aussage ausschließlich Zugriff gewährt. Dadurch muss jede Zugriffserlaubnis dediziert formuliert werden. Eine grundsätzliche Zugriffsfreigabe mit Negation einzelner unerwünschter Zugriffe ist in diesem Modell nicht vorgesehen. In einer ≪Permission≫ können ≪SubjectAttribute≫, ≪ObjectAttribute≫, ≪EnvironmentAttribute≫, ≪InputParameter≫ und ≪Constant≫ zu einer Zugriffskontrollaussage *und*-verknüpft werden. In Erweiterung zum in [EBA$^+$07] vorgestellten Modell wird das Objekt, auf welches der Zugriff erlaubt werden soll, als Menge seiner Attribute abgebildet. In der Unternehmensarchitektur definierte Geschäftsobjekte erleichtern die Auswahl der relevanten Objektattribute erheblich. Informationen zum aktuellen Systemzustand wie Datum, Uhrzeit und ähnlichen Parametern sind im Attribut ≪EnvironmentAttribute≫ enthalten, während ≪InputPara-

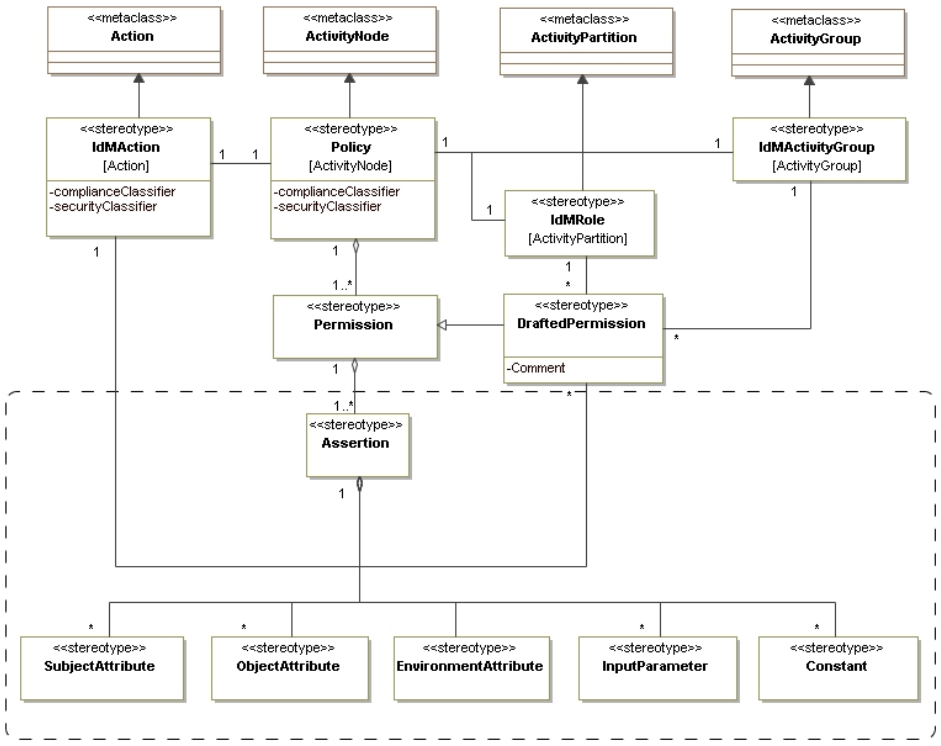

Abbildung 2: Metamodell des UML2-Profils für das Identitätsmanagement

meter≫ Eingabedaten genauer spezifiziert. Für Vergleiche mit einem festen Wert steht ≪Constant≫ zur Verfügung. Das Element ≪DraftedPermission≫ beinhaltet Zugriffskontrollaussagen, die nicht formalisiert bzw. noch nicht vollständig ausgearbeitet sind. Mit der ≪DraftedPermission≫ erhält die Fachabteilung die Möglichkeit, vorhandenes Wissen abzubilden, das im Anschluss durch einen Geschäfts- oder Sicherheitsanalysten überarbeitet und in eine ≪Permission≫ überführt werden kann. Mit dem Element ≪IdMAction≫ wird das *Action*-Element des Aktivitätsdiagramms erweitert. Wie bereits ≪Policy≫ enthält es die Attribute *complianceClassifier* und *securityClassifier* zur genaueren Klassifikation. ≪IdMRole≫ erweitert das Konzept der Aktivitätspartitionen (*Swimlanes*), um fachliche Rollen zur Zugriffskontrolle auf die darin enthaltenen Objekte abbilden zu können. Rollen werden wie in [EBA$^+$07] nicht im klassischen RBAC-Verständnis (*Role Based Access Control*, [FSG$^+$01]), sondern als eine Menge von Rollen-Attributen nach dem Konzept der attributbasierten Zugriffskontrolle [YT05] angesehen. Die ≪IdMActivityGroup≫ kann eine Gruppierung mehrerer Elemente vornehmen, mit dem Ziel einmalig der Gruppe und nicht jedem einzelnen Gruppenmitglied eine ≪Policy≫ zuzuweisen. Tabelle 1 gibt einen Überblick über die wichtigsten Elemente und deren Einschränkungen.

Name	≪**IdMAction**≫
Metaklasse	Action
Beschreibung	Für diese Aktion ist eine Zugriffskontrolle nötig. Die Sicherheitsklassifizierung ist in den Attributen *complianceClassifier* und *securityClassifier* beschrieben.

Einschränkung Prosa bzw. Object Constraint Language	Eine ≪IdMAction≫ darf maximal eine ≪Policy≫ oder null oder mehrere ≪DraftedPermission≫-Elemente besitzen.
	
	`context IdMAction`
	`inv: self.policy->size <= 1 or`
	`self.draftedPermission->size() >= 0`
	
	Ist eine ≪IdMAction≫ in einer ≪IdMActivityGroup≫, so darf nur entweder der ≪IdMAction≫ oder der ≪IdMActivityGroup≫ eine ≪Policy≫ zugewiesen sein.

Name	≪**Policy**≫
Metaklasse	ActivityNode
Beschreibung	Eine ≪Policy≫ beinhaltet ein oder mehrere disjunkt verknüpfte ≪Permission≫-Elemente. Sie dient somit als Container für diese Elemente.
Einschränkung	keine
Name	≪**Permission**≫
Metaklasse	Class
Beschreibung	UND-Verknüpfung der Elemente ≪SubjectAttribute≫, ≪ObjectAttribute≫, ≪EnvironmentAttribute≫, ≪InputParameter≫ und ≪Constant≫ zu einer positiven Zugriffskontrollaussage. Im Attribut *Comment* kann ein erklärender Kommentar beigefügt werden.
Einschränkung	keine
Name	≪**DraftedPermission**≫
Metaklasse	≪Permission≫
Beschreibung	Der Zugriffskontrollausdruck einer ≪DraftedPermission≫ ist nicht formalisiert und bedarf immer einer Überarbeitung mit dem Ziel der Überführung in eine ≪Permission≫. Im Attribut *Comment* kann ein erklärender Kommentar beigefügt werden.
Einschränkung	keine

Tabelle 1: Hauptelemente des Metamodells

Name	≪**IdMRole**≫
Metaklasse	ActivityPartition
Beschreibung	Dient zur Abbildung des organisatorischen Rollenmodells (fachliche Rolle). Für den Zugriff auf Aktivitäten innerhalb der Partition muss das zugreifende Subjekt Inhaber der jeweiligen fachlichen Rolle sein.
Einschränkung	Befinden sich mit ≪Policy≫ versehene ≪IdMAction≫- oder ≪IdMActivityGroup≫-Elemente in der ≪IdMRole≫-Partition, so müssen die Subjektattribute der jeweiligen Rolle mit den Subjektattributen der entsprechenden ≪Policy≫ übereinstimmen.
Name	≪**IdMActivityGroup**≫
Metaklasse	ActivityPartition
Beschreibung	Dient zur Gruppierung mehrerer ≪IdMAction≫-Elemente, um nur einmalig der ≪IdMActivityGroup≫ eine ≪Policy≫ oder ≪DraftedPermission≫ zuweisen zu müssen.

Einschränkung Prosa bzw. Object Constraint Language	Eine ≪IdMActivityGroup≫ darf maximal eine ≪Policy≫ oder null oder mehrere ≪DraftedPermission≫-Elemente besitzen.
	
	`context IdMActivityGroup`
	`inv: self.policy->size <= 1 or`
	`self.draftedPermission->size() >= 0`
	
	Enthält eine ≪IdMActivityGroup≫ eine ≪IdMAction≫, so darf entweder der ≪IdMActivityGroup≫ oder der ≪IdMAction≫ eine ≪Policy≫ zugewiesen sein.

Tabelle 1: Hauptelemente des Metamodells

Im Abschnitt 1.1 werden Authentisierung/Authentifizierung, Autorisierung und Auditierung als drei Bestandteile einer Architektur für das Identitätsmanagement aufgeführt. Im UML2-Profil für IdM ist mit den Stereotypen nur die Autorisierung mittels ≪Policy≫- und ≪Permission≫-Elementen zur Zugriffskontrolle direkt abgebildet. Anforderungen für die Art und Stärke der Authentisierung des zugreifenden Subjekts können indirekt durch Verwendung des ≪SubjectAttribute≫ innerhalb einer ≪Permission≫ formuliert werden. Informationen zur Auditierung der getroffenen Entscheidungen können nicht im vorgestellten UML2-Profil modelliert werden. Die Protokollierung ist vollständig den betreffenden Bestandteilen der IdM-Architektur überlassen.

3 Anwendungsbeispiel

Als Beispiel zur Anwendung des UML2-Profils für IdM wird exemplarisch ein vereinfachter Begutachtungsprozess für Konferenzbeiträge dargestellt (vgl. Abb. 3). Ein bereits zur Konferenz angemeldeter Teilnehmer reicht als Autor einen Beitrag ein, der im Anschluss vom Programmkomitee einem Gutachter zugewiesen wird. Dieser kann die Zuweisung annehmen oder ablehnen. Mit Annahme der Zuweisung kann der Gutachter den eingereichten Beitrag einsehen und die Bewertung vornehmen. Das abgeschlossene Gutachten wird im Anschluss vom Programmkomitee ausgewertet und führt zu einer Annahme- oder Ablehnungsbenachrichtigung an den Autor. Im Falle einer Annahme kann der Autor die überarbeitete und druckreife Fassung seines Beitrages in das System stellen.

Mit dem Stereotyp ≪IdMRole≫ werden die fachlichen Rollen in den einzelnen Aktivitätspartitionen festgelegt. Am Geschäftsprozess sind die Rollen „Teilnehmer“ als Autor, „Organisator“ und „Gutachter“ beteiligt. Die Einreichung eines Beitrages steht jedem Teilnehmer offen, der die Bedingungen der ≪DraftedPermission≫ „Teilnehmer-Bedingung“ erfüllt. Diese legt fest, dass nur Teilnehmer, die bereits die Konferenzgebühr bezahlt haben einen Beitrag einreichen dürfen und muss überarbeitet und anschließend in eine ≪Permission≫ in einer ≪Policy≫ überführt werden. Exemplarisch könnte die von der Fachabteilung formulierte ≪DraftedPermission≫ in Pseudocode so dargestellt werden:

```
teilnehmer.istGebuehr == teilnehmer.sollGebuehr
```

Die Einreichung der Druckfassung ist allen Teilnehmern erlaubt, deren Beitrag angenommen wurden, was in einer ≪Permission≫ innerhalb der ≪Policy≫ „ED-Policy“ als

```
teilnehmer.ID == beitrag.AutorID
&& beitrag.status == "angenommen"
```

abgebildet werden kann. Sämtliche Aktionen in der Partition des Gutachters unterliegen einer weiteren ≪Policy≫ „Gutachten-Policy“. Diese schränkt den Zugriff auf die eigenen Anfragen für ein Gutachten ein und unterbindet den Zugriff auf bereits bewertete Gutachten. Als ≪Policy≫ kann dies mittels drei ≪Permission≫-Elementen abgebildet werden:

```
1) gutachter.ID  == beitrag.GutachterID
2) beitrag.status == "zugeteilt"
3) beitrag.status == "inArbeit"
```

Mit 1) wird nur den Zugriff auf zugeteilte Beiträge erlaubt, 2) und 3) schränken den Zugriff auf noch zu begutachtende Beiträge ein.

Das für das Beispiel verwendete Vokabular zur Beschreibung der Zugriffskontrollaussagen setzt das Wissen über die betreffenden Geschäftsobjekte der Unternehmensarchitektur, deren Attribute und deren mögliche Werte in der Fachabteilung voraus.

Im Rahmen der Modellierung eines *Single Sign-On*-Zugangs für Administratoren und Workgroup-Manager einer Universität wird das UML2-Profil in den kommenden Monaten einem weiteren Praxistest unterworfen.

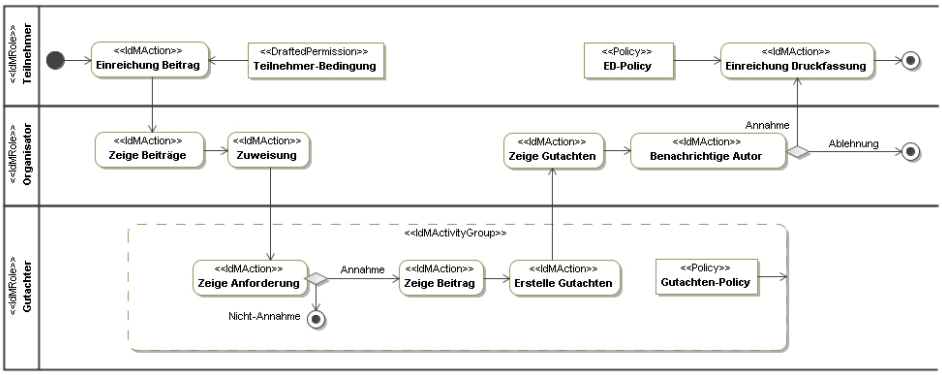

Abbildung 3: Anwendung des UML2-Profils für das Identitätsmanagement

4 Zusammenfassung

Das UML2-Profil für das Identitätsmanagement erweitert das UML-Aktivitätsdiagramm um Methoden zur Modellierung von Zugriffskontrollinformationen. Der Anwender wird dadurch in die Lage versetzt, bereits zum Zeitpunkt der Modellierung eines Geschäftsprozesses Aussagen über die Zugriffskontrolle anzufügen. Dies führt zu einer engen Verzahnung (fach-)funktionaler und nichtfunktionaler Anforderungen des Identitätsmanagements für einen Geschäftsprozess. Einseitige Änderungen von Zugriffsspezifikationen ohne Beachtung des betreffenden Geschäftsprozesses und umgekehrt sind dann nicht mehr möglich. Der formalisierte und modellbasierte Ansatz zum Erfassen der sicherheitsrelevanten Informationen bildet zudem die Grundlage für einen modellgetriebenen Softwareentwicklungsprozess, dessen Beginn in der Fachabteilung, den Wissensträgern der geschäftlichen Anforderungen liegt und an dessen Ende konkret ausgeprägte Sicherheitsrichtlinien zum Import in IdM-Werkzeuge stehen (vgl. Abb. 1).

Zukünftige Arbeiten umfassen die Schließung der Lücke zwischen dem vorgestellten UML2-Profil für IdM und den in [EKA+08] beschriebenen Ansatz zur modellgetriebenen Erzeugung von Zugriffskontrollaussagen. Hierzu müssen Modelltransformationen entwickelt werden, mit denen die im vorgestellten UML2-Profil abgebildeten Anforderungen auf das Zielmodell übertragen werden können. In Ergänzung zu den fachlichen Sicherheitsanforderungen rückt die Abbildung unternehmensweiter, organisatorischer Sicherheits-Meta-Policies in den Fokus [Kla07]. Mit voranschreitender Ausdifferenzierung der Unternehmensarchitektur werden automatische Überprüfungen der Geschäftsprozessmodelle auf ihre Übereinstimmung mit gesetzlichen und organisatorischen Sicherheitsvorgaben erforderlich. Die Rolle des IdM sowie der dazugehörigen Sicherheitsrichtlinien in der Unternehmensarchitektur und die damit verbundenen Notwendigkeiten hinsichtlich Lebenszyklus und der organisatorischen Aufstellung bilden weitere Aspekte kommender Forschungsarbeit.

Literatur

[BHK04] Marc Born, Eckhardt Holz und Olaf Kath. *Softwareentwicklung mit UML 2*. Addison-Wesley, München, 2004.

[Blu05] Dan Blum. Identity Management. Bericht, Burton Group, November 2005.

[EBA+07] Christian Emig, Frank Brand, Sebastian Abeck, Jürgen Biermann und Heiko Klarl. An Access Control Metamodel for Web Service-Oriented Architecture. In *Proceedings of the International Conference on Software Engineering Advances*. IEEE Computer Society, August 2007.

[EKA+08] Christian Emig, Sebastian Kreuzer, Sebastian Abeck, Jürgen Biermann und Heiko Klarl. Model-Driven Development of Access Control Polcies for Web Services. 2008. Submitted for publication.

[FSG+01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn und Ramaswamy Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, August 2001.

[Gö07] Stefanie Götzfried. Identity Management. Untersuchungen zum Einsatz von Identity Management-Systemen in Unternehmen und Organisationen. Diplomarbeit, Universität Regensburg, Institut für Medien-, Informations- und Kulturwisssenschaft (Informationswissenschaft), 2007.

[Ham90] Michael Hammer. Reengineering work: don't automate, obliterate. *Harvard Business Review*, 68(4):104–112, 1990.

[Hom07] Wolfgang Hommel. *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management*. Dissertation, Fakultät für Mathematik, Informatik und Statistik der Ludwig-Maximilians-Universität München, 2007.

[IT03] Takeshi Imamura und Michiaki Tatsubori. Patterns for Securing Web Services Messaging. In *OPSLA Workshop on Web Services and Service Oriented Architecture Best Practice and Patterns*, 2003.

[Jue05] Jan Juerjens. *Secure Systems Development with UML*. Springer, 2005.

[KL06a] Birgit Korherr und Beate List. Extending the UML 2 Activity Diagram with Business Process Goals and Performance Measures and the Mapping to BPEL. In *Advances in Conceptual Modeling - Theory and Practice*, Jgg. 4231 of *Lecture Notes in Computer Science*, Seiten 7–18. Springer, 2006.

[KL06b] Birgit Korherr und Beate List. A UML 2 Profile for Event Driven Process Chains. In *Research and Practical Issues of Enterprise Information Systems*, Jgg. 205 of *IFIP International Federation for Information Processing*, Seiten 161–172. Springer, 2006.

[Kla07] Heiko Klarl. Modellgetriebene, mustergestützte Sicherheit in serviceorientierten Architekturen. *Informatik-Spektrum*, 30(3):175–177, Juni 2007.

[KNS92] G. Keller, M. Nüttgens und A.-W. Scheer. *Semantische Prozessmodellierung auf der Grundlage Ereignisgesteuerter Prozessketten (EPK)*, Jgg. 89. Universität des Saarlandes, Januar 1992.

[KP06] Heiko Klarl und Markus Preitsameter. Securing Service-Oriented and Event-Driven Architectures – Results of an Evaluation of Enterprise Security Frameworks. In *Proceedings of the IEEE Services Computing Workshops*, Seite 89. IEEE Computer Society, 2006.

[LBD02] Torsten Lodderstedt, David A. Basin und Jürgen Doser. SecureUML: A UML-Based Modeling Language for Model-Driven Security. In *Proceedings of the 5th International Conference on The Unified Modeling Language*, Jgg. 2460 of *Lecture Notes In Computer Science*, Seiten 426–441. Springer, 2002.

[NKB06] Thomas Neubauer, Markus Klemen und Stefan Biffl. Secure Business Process Management: A Roadmap. In *Proceedings of the First International Conference on Availability, Reliability and Security*, Seiten 457 – 464. IEEE Computer Society, April 2006.

[OMG01] Object Management Group, Inc. Model Driven Architecture (MDA). `http://www.omg.org/cgi-bin/apps/doc?ormsc/01-07-01.pdf`, Juli 2001.

[OMG06a] Object Management Group, Inc. Business Process Modeling Notation (BPMN) Specification. `http://www.bpmn.org/Documents/OMGFinalAdoptedBPMN1-0Spec06-02-01.pdf`, Februar 2006.

[OMG06b] Object Management Group, Inc. Object Constraint Language – Version 2.0. `http://www.omg.org/technology/documents/formal/ocl.htm`, Mai 2006.

[OMG07a] Object Management Group, Inc. Unified Modeling Language: Infrastructure – Version 2.1.1. `http://www.omg.org/docs/formal/07-02-06.pdf`, Februar 2007.

[OMG07b] Object Management Group, Inc. Unified Modeling Language: Superstructure – Version 2.1.1. `http://www.omg.org/docs/formal/07-02-05.pdf`, Februar 2007.

[RFMP06] Alfonso Rodriguez, Eduardo Fernandez-Medina und Mario Piattini. Security Requirement with a UML 2.0 Profile. In *Proceedings of the First International Conference on Availability, Reliability and Security*, Seiten 670–677. IEEE Computer Society, 2006.

[RFMP07] Alfonso Rodriguez, Eduardo Fernandez-Medina und Mario Piattini. A BPMN Extension for the Modeling of Security Requirements in Business Processes. *IEICE-Transactions on Info and Systems*, E90-D(4):745–752, 2007.

[RHS05] Jan-Peter Richter, Harald Haller und Peter Schrey. Serviceorientierte Architektur. *Informatik-Spektrum*, 28(5):413–416, Oktober 2005.

[SN00] August-Wilhelm Scheer und Markus Nüttgens. ARIS Architecture and Reference Models for Business Process Management. In *Business Process Management, Models, Techniques, and Empirical Studies*, Jgg. 1806 of *Lecture Notes In Computer Science*, Seiten 376 – 389. Springer, 2000.

[Sto06] Harald Stoerrle. A Comparison of (e)EPCs and UML 2 Activity Diagrams. In Markus Nüttgens, Frank J. Rump und Jan Mendling, Hrsg., *EPK 2006 – Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten*, Seiten 177–188, Vienna, 2006. CEUR Workshop Proceedings.

[YT05] Eric Yuan und Jin Tong. Attributed based access control (ABAC) for Web services. In *Proceedings of the IEEE International Conference on Web Services*. IEEE Computer Society, Juli 2005.

Alle Web-Referenzen (URLs) wurden zuletzt am 22.02.2008 überprüft.