



Hochschule für Angewandte Wissenschaften Hamburg  
*Hamburg University of Applied Sciences*

# **Seminarausarbeitung**

**Sven Boris Bornemann**

**Entwicklung einer Berechtigungsstruktur für Smart Homes**

*Fakultät Technik und Informatik  
Studiendepartment Informatik*

*Faculty of Engineering and Computer Science  
Department of Computer Science*

# Inhaltsverzeichnis

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Motivation</b>                      | <b>1</b>  |
| <b>2</b> | <b>Analyse</b>                         | <b>3</b>  |
| 2.1      | Berechtigungskonzepte . . . . .        | 3         |
| 2.1.1    | Mandatory Access Control . . . . .     | 3         |
| 2.1.2    | Discretionary Access Control . . . . . | 4         |
| 2.1.3    | Role Based Access Control . . . . .    | 4         |
| 2.1.4    | Bewertung . . . . .                    | 5         |
| 2.2      | Herausforderungen . . . . .            | 6         |
| <b>3</b> | <b>Masterarbeit</b>                    | <b>7</b>  |
| 3.1      | Vorarbeiten . . . . .                  | 7         |
| 3.2      | Zielsetzung . . . . .                  | 8         |
| 3.3      | Entwicklung eines Szenarios . . . . .  | 9         |
| 3.4      | Chancen und Risiken . . . . .          | 10        |
| <b>4</b> | <b>Zusammenfassung</b>                 | <b>11</b> |

# 1 Motivation

In heutigen modernen Wohnumgebungen steigt die Anzahl technischer Geräte ständig. Diese Geräte bieten immer mehr Funktionalitäten und können aufgrund ihrer Netzwerkkonnektivität zusammen mit anderen Geräten zu intelligenten Services verschmelzen. Diese zunehmende Allgegenwärtigkeit von Computern und Rechenleistung wird als Ubiquitous Computing bezeichnet. Dieser Begriff wurde von Mark Weiser in seinem Artikel *The Computer for the 20st Century* (Weiser (1991)) geprägt.

Aufgrund dieser Entwicklung und der damit einhergehenden Steigerung digitaler Services in Wohnumgebungen, ist die Entwicklung und Einführung einer Berechtigungsstruktur notwendig. Gerade im Mehrpersonenhaushalt wird eine solche Struktur benötigt, um den verschiedenen Familienmitgliedern einen differenzierten Zugriff auf Services und Ressourcen zu ermöglichen. Aber auch in den Einpersonenhaushalten, welche zukünftig noch zunehmen werden (Statistisches Bundesamt (2011)), wird eine Berechtigungsstruktur benötigt.

Eine Berechtigungsstruktur in diesen Smart Environments ist nicht nur notwendig um den Zugriff auf verschiedene Ressourcen von diversen Personen und Personengruppen zu kontrollieren, sondern auch um die Kommunikation und den Zugriff zu digitalen Services und Ressourcen untereinander zu reglementieren.

Um eine möglichst einfache Handhabung einer solchen Struktur für den Endanwender zu gewährleisten sollten diverse Abläufe automatisierbar sein. Hierzu können verschieden Technologien verwendet werden. Near Field Communication, kurz NFC, kann beispielsweise für einen automatisierten Zugriff auf Services oder die Integration von mobilen Endgeräten ins Netzwerk der Wohnumgebung genutzt werden. Verfahren der künstlichen Intelligenz können den Endanwender unterstützen und so das Einrichten von Benutzern und Berechtigungen erleichtern beziehungsweise automatisieren.

Die hier zu entwickelnde Berechtigungsstruktur wird im Rahmen des Living Place Hamburg (von Luck u. a. (2010)) eingesetzt und evaluiert. Das Living Place Hamburg ist ein Projekt der Hochschule für Angewandte Wissenschaften Hamburg, in dem unterschiedliche Ansätze des modernen urbanen Lebens erforscht und getestet werden. Trotz des Einsatzes im Living Place wird bei der Entwicklung der Berechtigungsstruktur darauf geachtet, dass diese möglichst

## *1 Motivation*

---

modular und dynamisch aufgebaut ist. Um somit den Einsatz in weiteren Smart Enviroments zu gewährleisten.

## 2 Analyse

In diesem Kapitel werden verschiedene Berechtigungsmodelle aufgezeigt und erläutert. Aufgrund der Eigenschaften wird eines dieser Modelle ausgewählt und erweitert. Dies ist notwendig um alle Anforderungen, die im Einsatzgebiet einer Wohnumgebung auftreten, realisieren zu können.

### 2.1 Berechtigungskonzepte

Berechtigungskonzepte oder -modelle dienen der Steuerung und Zugriffskontrolle auf Daten und Dienste. Je nach Einsatzgebiet gibt es verschiedenste Ansätze um den Zugriff zu regeln. Im Folgenden werden einige Konzepte vorgestellt und deren Vor- und Nachteile hinsichtlich des Einsatzes in einer Wohnumgebung aufgezeigt.

#### 2.1.1 Mandatory Access Control

Das Mandatory Access Control Modell kommt meist in Bereichen mit sensiblen Daten, wie dem Militär, Behörden oder in der Gesundheitsbranche zum Einsatz. Der Zugriff auf die Daten wird in diesem Modell nicht nur anhand der Benutzeridentität und der Ressource geregelt, sondern es werden weitere Regeln definiert die einen korrekten Zugriff auf die Daten sicherstellen sollen.

Im einfachsten Fall, den Multi-Level-Sicherheitssystemen, werden den zu schützenden Ressourcen sogenannte Schutzstufen zugeordnet. Diese unterteilen die unterschiedlichen Daten in „vertikale Schichten“. Im Militärbereich könnten solche Schichten: *Streng Geheim*, *Geheim*, *Vertraulich* oder *Öffentlich* heißen. Damit ein Benutzer Zugriff auf die Daten der Schicht *Geheim* erhält, muss dieser ebenfalls die Schutzstufe *Geheim* besitzen.

Die Multi-Level-Sicherheitssysteme beinhalten weitere Zugriffsmodelle, wie: Bell LaPadula, Biba, LoMAC. Diese Modelle regeln beispielsweise die Überführung der Daten in andere Schutzstufen oder gewährleisten die Integrität der Daten (Sandhu (1993)).

Einen komplexeren Aufbau des Mandatory Access Control Modells bieten multilaterale Sicherheitsmodelle, wie Compartment- oder Lattice-Modell oder Chinese Wall (Sandhu (1993)).

In diesen Modellen werden die Daten nicht nur vertikal mittels Schutzstufen, sondern auch horizontal über mehrere Schutzstufen und Codewörter abgesichert.

### 2.1.2 Discretionary Access Control

Das Discretionary Access Control Modell bildet das komplette Gegenteil zum Mandatory Access Control Modell. Hier wird der Zugriff einzig und allein auf Basis der Benutzeridentität realisiert. Dies bedeutet, Zugriffsrechte für Ressourcen sind im Benutzer eingetragen und müssen somit für jeden Benutzer verwaltet werden. Hierdurch entsteht ein erhöhter Aufwand bei der Erstellung neuer Benutzer oder einer dynamischen Anpassung der Berechtigung.

### 2.1.3 Role Based Access Control

Das Role Based Access Control Modell erweitert das vorher beschriebene Discretionary Access Control Modell um Benutzergruppen und -rollen. Die Gruppen dienen in diesem Fall dazu die Benutzer hinsichtlich organisatorischer Strukturen zu gruppieren. Die Rollen gruppieren hingegen Berechtigungen, welche für die Ausübung eines bestimmten Arbeitsprozesses benötigt werden. Dies erleichtert zum einen die Zuweisung von Rechten, zum anderen erlaubt es die dynamische Erweiterung aktueller Berechtigung durch Zuweisung einer Rolle.

Der RBAC Standard wurde 1996 veröffentlicht ([Sandhu u. a. \(1996\)](#)) und besteht aus insgesamt vier Versionen. Die Beziehung der verschiedenen Versionen zueinander ist in der Abbildung 2.1 dargestellt. Hierbei wird die Version 0 auch als Kernmodell bezeichnet, da in dieser Version

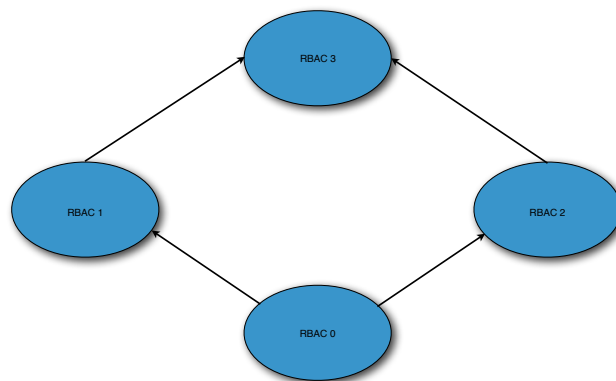


Abbildung 2.1: Beziehung zwischen den RBAC Versionen

alle grundlegenden Kernkomponenten definiert werden. Hierzu gehören Benutzer, Rollen, Rechte und Sessions. Um dem Benutzer nur die Berechtigungen zu geben die er im Moment benötigt, werden die Rollen anhand von Sessions aktiviert.

In der Version 1 wurde der RBAC Standard um eine Rollenhierarchie erweitert. Hierdurch wird es einer Rolle ermöglicht, Rechte einer darunterliegenden Rolle zu erben.

In der Version 2 wurde das Konzept zur Einschränkung von Rollen definiert. Hierdurch wird die Zuweisung konfliktbehafteter Rollen zu einem Benutzer verhindert.

Die Zusammenführung dieser beiden Konzepte wird in der Version 3 vorgenommen. Darüber hinaus stellt Version 3 keine weiteren Neuerungen bereit. Tiefer gehende Informationen zu Rollen- und Berechtigungskonzepten sind in [Tsolkas und Schmidt \(2010\)](#) zu finden.

### 2.1.4 Bewertung

Nachdem im vorherigem drei unterschiedliche Berechtigungskonzepte vorgestellt wurden, sollen diese nun hinsichtlich ihrer Vor- und Nachteile verglichen werden. Da die Berechtigungsstruktur im Living Place Hamburg eingesetzt werden soll, sind hier einige Punkte maßgeblich. Zum einen muss es mit der gewählten Struktur möglich sein nicht nur Benutzer zu verwalten, sondern auch die Services des Smart Homes. Zum anderen muss die Struktur dynamisch sein, um auf jeweilige Kontextänderung reagieren zu können. Des Weiteren sollte die Struktur möglichst editierbar und durchschaubar für den Endanwender sein.

Für den Einsatz in einem Smart Home bietet hier das Role Based Access Control (RBAC) Modell das beste Potential. Aufgrund der möglichen Benutzereinteilung in Gruppen müssen bei auftretenden Änderung nur die Eigenschaften der Gruppe angepasst werden. Im Gegensatz dazu müsste beim Discretionary Access Control Modell jeder Benutzer aktualisiert werden, welcher von der Änderung betroffen ist. Dies generiert gerade bei einer höheren Nutzeranzahl einen großen Verwaltungsaufwand. Des Weiteren können dem Benutzer dynamisch, anhand von Rollen, Berechtigungen zugewiesen werden die er zum aktuellen Zeitpunkt benötigt. Da ein Benutzer also nur die Rechte besitzt, die er zum aktuellen Zeitpunkt benötigt, erhöht sich die Sicherheit des Systems.

Weiter lehnt sich die Aufteilung in Gruppen und Rollen stark an die menschliche Denkweise an, welches dem Endanwender einen einfacheren Umgang mit dem System ermöglicht. Das Mandatory Access Control Modell bietet durch die Kategorisierung in horizontale- und vertikale Schichten zwar eine höhere Sicherheit, jedoch ist der Umgang mit dieser Verwaltungsstruktur komplexer als beim RBAC. Dies erschwert die Bedienbarkeit des Systems für

den Endanwender, wodurch unter anderem die Wahrscheinlichkeit einer Fehlkonfiguration erhöht wird.

## 2.2 Herausforderungen

In der vorhergehenden Bewertung der vorgestellten Berechtigungskonzepte stellte sich das Role Based Access Control Modell als das geeignetste Modell für den Smart Home Bereich heraus. Aufgrund dieser Wahl ergeben sich einige Herausforderungen für die Realisierung.

Eine Herausforderung stellt hierbei die Erstellung und Verwaltung von Usern, Gruppen und Rollen dar. Um das Einrichten des Systems und das Anlegen von Benutzern für den Endanwender zu erleichtern, ist die Kopplung mit anderen Systemen vorstellbar. Von diesem System können dann schon vorhandene Benutzer übernommen werden.

Des Weiteren müssen Regeln erstellt und definiert werden, welche Rollen dem User in Abhängigkeit zum aktuellen Kontext zugewiesen werden können. In diesem Zusammenhang muss auch darüber nachgedacht werden, Rollen und Gruppen von verschiedenen Personengruppen anlegen zu lassen und diese dann nach einer Prüfung durch den Wohnungsbesitzer zu aktivieren. Ein Beispiel hierfür kann sein, dass die Kinder in einer Familie eine Rolle für ihre Freunde anlegen. Diese wird dann durch die Eltern überprüft und gegebenenfalls erlaubt.

Eine weitere wichtige Frage ist auch, wie sich das Gesamtsystem verhält, wenn sich mehrere Personen mit unterschiedlichen Berechtigungen in einem Raum aufhalten, wie zum Beispiel bei einem Abendessen mit Familie und Freunden oder einer Party.

Für all diese Herausforderungen müssen noch Lösungsansätze erarbeitet werden.



## 3 Masterarbeit

Im folgenden Kapitel sollen die Vorarbeiten aufgeführt werden. Aufgrund dieser Arbeiten ergibt sich eine Zielsetzung für die Masterarbeit. Anschließend wird auf die Chancen und Risiken dieser Zielsetzung eingegangen.

### 3.1 Vorarbeiten

Aufgrund der Erkenntnisse aus der Bachelorarbeit ([Bornemann \(2011\)](#)), welche sich mit möglichen Interaktionen einer Tablet gestützten Gegensprechanlage im Smart Home Bereich beschäftigte, sind weitere Aufgabengebiete entstanden.

Die Ausarbeitung zu Anwendungen 1 ([Bornemann \(2012b\)](#)) beschäftigt sich mit der Erweiterung des Konzeptes auf ein Smartphone. Zielsetzung war hier zum einen die konventionelle Türklingel auf das Smartphone der Besucher zu portieren. Zum anderen sollte es den Bewohnern und ausgewählten Personen ermöglicht werden den Zutritt zum Smart Home über das Smartphone zu erlangen. Dafür wurden in der Ausarbeitung zu Anwendungen 1 verschiedene Szenarien vorgestellt und dessen Anforderungen identifiziert. Aufgrund dieser Anforderungen wurden Konzepte zur Kommunikation der verschiedenen Services untereinander und ein Konzept zur automatischen Integration von mobilen Endgeräten vorgestellt.

Die Ausarbeitung zu Anwendungen 2 ([Bornemann, 2012c](#)) beschäftigte sich weitergehend mit Konzepten zur Abspeicherung von Berechtigungen zu Personen und Services im Smart Home. Dafür wurde die Vision einer eigens entwickelten Infrastruktur vorgestellt, welche sich in das Living Place Hamburg integrieren lässt. Des Weiteren wurde bei der Entwicklung der Infrastruktur darauf geachtet, dass alle Teilkomponenten möglichst modular aufgebaut sind. Dies erlaubt unter anderem die Integration in andere Smart Homes. Anschließend wurden drei verschiedene Ansätze zum Thema Fernsteuerung von Smart Homes vorgestellt und dessen Vor- und Nachteile verglichen.

Aufgrund der bisher definierten Konzepte zur Realisierung einer mobilen Türklingel-Applikation

für Smart Homes, wurde in Projekt 1 und Projekt 2 damit begonnen, Teile dieser Konzepte umzusetzen. Hierbei lag der Fokus, im Projekt 1, auf der Integration mobiler Endgeräte in das Wohnungsnetz einer intelligenten Wohnung. Um eine möglichst intuitive und anwenderfreundliche Bedienung zu ermöglichen, wurde eine Datenübertragung mittels Near Field Communication (NFC) realisiert. Detailliertere Informationen sind in der Ausarbeitung zum Projekt 1 ([Bornemann \(2012a\)](#)) zu finden. Des Weiteren wurde ein Konzept zur Speicherung und Verwendung von Zugriffsberechtigungen vorgestellt.

## 3.2 Zielsetzung

Ziel der Masterarbeit soll es sein, eine robuste und langlebige Berechtigungsstruktur für Smart Homes zu entwickeln und diese in das Living Place Hamburg zu integrieren. Durch diese Struktur soll der kontrollierte Zugriff auf Ressourcen ermöglicht werden, welches zu einem erhöhtem Komfort und mehr Sicherheit führen soll. Um dies zu ermöglichen wurden in den vorhergehenden Semestern Konzepte entwickelt. Die Machbarkeit dieser Konzepte wurden evaluiert, in dem Teilsysteme dieses Vorhabens realisiert worden. Darauffolgend werden die einzelnen Teilsysteme in das bestehende System integriert und miteinander verbunden. Um die passende Strukturierung von Usern, Gruppen, Rollen und die Zuweisung der Rechte in der Berechtigungsstruktur zu finden, wird ein iterativer Entwicklungsprozess erforderlich sein. In der folgenden Abbildung 3.1 sind alle Komponenten und ihre Verbindungen dargestellt.

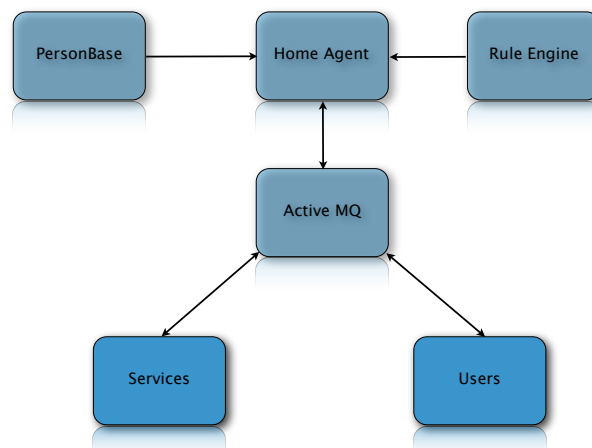


Abbildung 3.1: Aufbau des Komplettsystems

Die Kommunikation der User und Services zum Home Agent wird über den ActiveMQ ([The Apache Software Foundation](#)) ermöglicht. Hierbei bildet der Home Agent die Schnittstelle zur PersonBase ab. Möchte beispielsweise ein User eine Funktion eines Services im Smart Home nutzen, stellt dieser eine Anfrage an den Home Agent, welcher daraufhin die momentan gültigen Berechtigungen des User überprüft.

#### **Abgrenzungen**

Zur Zeit ist es nicht geplant die Zuweisung von Berechtigungen mittels Lernverfahren zu automatisieren. Dies bedeutet, dass die Berechtigungen einer Gruppe, zum Beispiel Freunde und Verwandte, oder Rollen vordefiniert werden. Demzufolge muss dem Benutzer auch die Möglichkeit gegeben werden Berechtigungen einer Person, Gruppe, Rolle oder eines Services nach seinen Präferenzen zu ändern.

Des Weiteren wird die Rule Engine nicht Bestandteil dieser Masterarbeit sein. Hierfür wird die von [Otto \(2013\)](#) im Living Place integrierte Rule Engine Drools ([JBoss Drools Team](#)) benutzt.

### **3.3 Entwicklung eines Szenarios**

Um die Funktionsweise der Berechtigungsstruktur und das Zusammenspiel der einzelnen Komponenten zu testen, wird im folgenden ein Szenario vorgestellt, welches im Living Place Hamburg realisiert werden soll.

In diesem Szenario soll es den Nachbarn ermöglicht werden die Wohnung zu betreten, um dort beispielsweise die Pflanzen gießen zu können, wenn die Eigentümer im Urlaub sind. Hierfür werden Komponenten und Services verwendet, die in vorherigen Semestern konzipiert und entwickelt wurden (siehe: [Bornemann \(2012b\)](#), [Bornemann \(2012a\)](#)). Zum Anfang des Szenarios besitzen die Nachbarn keine Möglichkeit die Wohnung zu betreten. Fahren die Bewohner in den Urlaub, erkennt das Smart Home diesen Zustand automatisch, beispielsweise anhand eines Kalendereintrages und weist dem Nachbar dynamisch das Recht zu, mit seinem Smartphone die Wohnungstür zu öffnen. Wird die Tür anschließend geöffnet, werden die Bewohner über das Betreten und Verlassen der Wohnung benachrichtigt.

Dies stellt nur eine kurze Erläuterung eines möglichen Szenarios dar. Im Zuge der Masterarbeit wird dieses Szenario noch detaillierter ausgearbeitet und erweitert.

### **3.4 Chancen und Risiken**

Die Chance in diesem Projekt besteht in der Entwicklung einer langfristig nutzbaren Berechtigungsstruktur, welche nicht nur den Einsatz im Living Place Hamburg, sondern auch in anderen Smart Homes finden soll. Eine Berechtigungsstruktur ist die Voraussetzung für die künftige Entwicklung von Multiuser Smart Homes und der damit einhergehenden Differenzierung verschiedener Endanwender und ihren Berechtigungen. Des Weiteren wird die Abbildung realer Situation und Szenarien möglich, welche den Komfort und die Sicherheit für den Endanwender steigern.

Bei der Realisierung dieses Projekts entstehenden jedoch einige Risiken. Hierzu gehört, dass bei der Entwicklung der Struktur nicht alle mögliche Eventualitäten und Szenarien abgedeckt werden können. Daher ist darauf zu achten die Berechtigungsstruktur möglichst flexibel und anpassbar zu halten. Des Weiteren können durch eine nicht optimal geplante Struktur und die Fehlkonfiguration durch den Endanwender Sicherheitslücken entstehen. Eine nicht optimale Struktur führt weiterhin zu einem erhöhten Verwaltungsaufwand für den Endanwender.

## 4 Zusammenfassung

Die Entwicklung einer Berechtigungsstruktur für Smart Homes beinhaltet einige Herausforderungen, welche von Entwicklern bewältigt werden müssen. Die wichtigste Herausforderung stellt hierbei die Organisation der Daten dar, welche möglichst flexibel ausgelegt sein muss, um den ständig wechselnden Anforderungen einer Wohnumgebung gerecht zu werden. Einige Ansätze hierzu wurden in Kapitel 2 vorgestellt.

Anschließend wurde in Kapitel 3 das weitere Vorgehen für die Masterarbeit beschrieben. Zuerst wurde darauf eingegangen welche Vorarbeiten in den vorhergehenden Projekten geleistet wurden. Darauffolgenden wurde die Zielsetzung, sowie die Chancen und Risiken dieses Themas diskutiert.

### Ausblick

Einige der benötigten Teilsysteme sind in den letzten Semestern entstanden, andere werden im kommenden Semester im Rahmen der Masterarbeit entwickelt. Neben der Vervollständigung der Berechtigungsstruktur, werden noch weitere Komponenten benötigt, welche es dem Endanwender ermöglichen die Struktur zu editieren. Des Weiteren müssen noch Regeln entwickelt werden, die das dynamische Zuweisen von Rollen in Abhängigkeit des aktuellen Kontextes ermöglichen. Zusätzlich sind noch weitere Automatisierungen möglich. Eine davon könnte die Authentifizierung eines Besuchers an der Berechtigungsstruktur sein, ohne das dieser zuvor vom Bewohner angelegt wurde. Hierfür können beispielsweise Mechanismen wie OAuth oder openID verwendet werden. Nach dieser Authentifizierung wird das Benutzerkonto, falls noch nicht vorhanden, angelegt und mit Standardrechten ausgestattet. Anschließend kann der Bewohner die Rechte dieses Benutzers nach seinen Präferenzen verändern.

Die noch zu entwickelnden Teilsysteme werden anschließend mit schon vorhandenen System kombiniert. Dies ist zum einen der in der Ausarbeitung AW 2 (Bornemann (2012c)) vorgestellte Home Agent, welcher die Schnittstelle zwischen den Services des Living Place und der Berechtigungsstruktur bildet. Zum anderen die automatisierte Integration mobiler Endgeräte mittels NFC (Bornemann (2012a)). Dieser Service ermöglicht es dem mobile Endgeräte des Besuchers eine Verbindung zum Wohnungsnetz des Smart Homes aufzunehmen.

# Literaturverzeichnis

- [Bornemann 2011] BORNEMANN, Sven B.: *Android-basierte Smart Home Interaktion am Beispiel einer Gegensprechanlage*, Hochschule für Angewandte Wissenschaften Hamburg, Bachelorarbeit, 2011
- [Bornemann 2012a] BORNEMANN, Sven B.: Integration mobiler Endgeräte in Smart Homes mittels NFC. (2012)
- [Bornemann 2012b] BORNEMANN, Sven B.: Mobile Türklingel für Smart Homes. (2012)
- [Bornemann 2012c] BORNEMANN, Sven B.: Remoteverbindungen für Smart Homes. (2012)
- [JBoss Drools Team ] JBOSS DROOLS TEAM: *JBoss Drools Fusion Documentation*. – URL <http://docs.jboss.org/drools/release/5.5.0.Final/drools-fusion-docs/pdf/drools-fusion-docs.pdf>. – letzter Zugriff: 30.01.2013
- [von Luck u. a. 2010] LUCK, Prof. Dr. K. von ; KLEMKE, Prof. Dr. G. ; GREGOR, Sebastian ; RAHIMI, Mohammad A. ; VOGT, Matthias: A place for concepts of IT based modern living / University of Applied Sciences Hamburg. URL [http://livingplace.informatik.haw-hamburg.de/content/LivingPlaceHamburg\\_en.pdf](http://livingplace.informatik.haw-hamburg.de/content/LivingPlaceHamburg_en.pdf), 2010. – Forschungsbericht. letzter Zugriff: 19.02.2013
- [OAuth ] OAUTH: *OAuth*. – URL <http://oauth.net>. – letzter Zugriff: 18.02.20.13
- [openID ] OPENID: *openID*. – URL <http://openid.net>. – letzter Zugriff: 18.02.2013
- [Otto 2013] OTTO, Kjell: *Aktuelle Entwicklungskonzepte zur Projektintegration in einem Smart Home anhand von Maven, OSGi und Drools Fusion*, Hochschule für Angewandte Wissenschaften Hamburg, Masterarbeit, 2013. – Noch nicht veröffentlicht
- [Sandhu u. a. 1996] SANDHU, Ravi S. ; COYNE, Edward J. ; FEINSTEIN, Hal L. ; YOUMAN, Charles E.: Role-Based Access Control Models. In: *Computer* 29 (1996), Februar, Nr. 2, S. 38–47. – URL <http://dx.doi.org/10.1109/2.485845>. – ISSN 0018-9162

- [Sandhu 1993] SANDHU, R.S.: Lattice-based access control models. In: *Computer* 26 (1993), nov., Nr. 11, S. 9 –19. – ISSN 0018-9162
- [Statistisches Bundesamt 2011] STATISTISCHES BUNDESAMT: *Demografischer Wandel in Deutschland*. 2011. – URL [https://www.destatis.de/DE/Publikationen/Thematisch/Bevoelkerung/VorausberechnungBevoelkerung/BevoelkerungsHaushaltsentwicklung5871101119004.pdf?\\_\\_blob=publicationFile](https://www.destatis.de/DE/Publikationen/Thematisch/Bevoelkerung/VorausberechnungBevoelkerung/BevoelkerungsHaushaltsentwicklung5871101119004.pdf?__blob=publicationFile). – letzter Zugriff: 14.02.2013
- [The Apache Software Foundation ] THE APACHE SOFTWARE FOUNDATION: *ActiveMQ*. – URL <http://activemq.apache.org>. – letzter Zugriff: 19.02.2013
- [Tsolkas und Schmidt 2010] TSOLKAS, Alexander ; SCHMIDT, Klaus: *Rollen und Berechtigungskonzepte - Ansätze für das Identity- und Access Management im Unternehmen*. 2010. Aufl. Wiesbaden : Vieweg+Teubner Verlag, 2010. – ISBN 978-3-834-81243-8
- [Weiser 1991] WEISER, Mark: The Computer for the 21st Century. In: *Scientific American* 265 (1991), September, Nr. 3, S. 94–?? (Intl. ed. 66–75). – ISSN 0036-8733 (print), 1946-7087 (electronic)