Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Projektbericht
Wintersemester 2012 / 2013

Sven Boris Bornemann

Aufbau einer Berechtigungsstruktur für Smart Homes

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Inhaltsverzeichnis

1 Einführung **1**

2 Projektarbeit **2**

2.1 Weiterführenden Arbeiten aus Projekt 1 2

2.1.1 Datenübertragung mittels NFC 2

2.1.2 Anbindung und Steuerung des Türschlosses 2

2.2 Entwicklung der Infrastruktur 4

2.2.1 Modellierung der Berechtigungsstruktur - PersonBase 4

2.2.2 Modellierung der LDAP - Schemata 5

2.2.3 Entwicklung des Home Agent 6

2.2.4 Entwicklung der Android Applikation - Smart Home 7

3 Fazit **9**

3.1 Zusammenfassung 9

3.2 Ausblick 9

1 Einführung

Elektronische Geräte in Wohnumgebungen nehmen immer weiter zu. Die dabei fortschreitende Technologie ermöglicht eine immer weitreichendere Vernetzung dieser Geräte. Gerade die Netzwerkkonnektivät ermöglicht die Erstellung intelligenter Services, welche Smart Homes ausmachen. Diese allgegenwärtige Rechenleistung wird auch als Ubiquitous Computing bezeichnet. Dieser Begriff wurde von Mark Weiser in seinem Artikel *The Computer for the 20st Century* (Weiser (1991)) geprägt.
Durch die steigende Anzahl elektronischer Geräte und der damit verbundenen Services ist die Reglementierung des Zugriffs auf diese Dienste notwendig. Gerade in Mehrpersonenhaushalten ist dies von Interesse, um den verschiedenen Familienmitglieder einen differenzierten Zugriff auf vorhandene Ressourcen geben zu können. Hierfür ist die Einführung einer Berechtigungsstruktur notwendig. Eine Berechtigungsstruktur ist jedoch nicht nur erforderlich, um den Zugriff von Personen oder Personengruppen auf Services und Ressourcen zu reglementieren. Ebenso bedarf es bei der Kommunikation zwischen Services einer Kontrolle. Welches Berechtigungsmodell das geeignetste für den Einsatz in einer Wohnumgebung ist, wird in der Seminarausarbeitung *Entwicklung einer Berechtigungsstruktur für Smart Homes* (Bornemann (2013)) evaluiert.

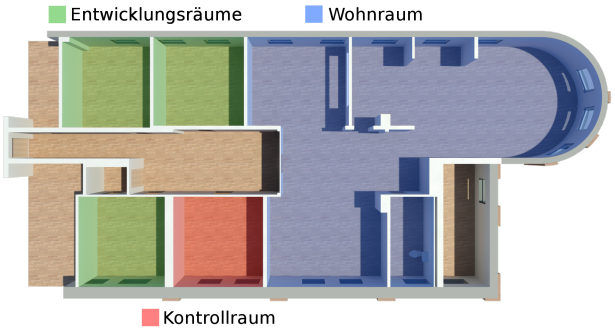

Abbildung 1.1: Grundriss des Living Place Hamburg

Der in dieser Ausarbeitung vorgestellte Aufbau einer Berechtigungsstruktur gliedert sich in den Kontext des Living Place Hamburg (von Luck u. a. (2010)) ein. Beim Living Place handelt es sich um ein Projekt der Hochschule für Angewandte Wissenschaften Hamburg, indem der Einfluss neuer Technologien im menschlichen Alltag erforscht wird.

2 Projektarbeit

2.1 Weiterführenden Arbeiten aus Projekt 1

In der Ausarbeitung zum Projekt 1 (Bornemann (2012)) wurden Lösung zur Integration mobiler Endgeräte mittels Near Field Communication (NFC) vorgestellt. Die Idee hinter diesem Konzept bestand darin, Daten auf das mobile Endgeräte zu übertragen, welche es dem Gerät ermöglichen, sich mit dem Wohnungsnetzwerk zu verbinden. Dabei sollte keine Eingabe durch den Gerätebesitzer erfolgen.

2.1.1 Datenübertragung mittels NFC

Um dies zu realisieren wurde versucht eine NFC P2P Verbindung zwischen einem Google Nexus S Smartphone mit Android 4.1 Betriebssystem und dem NFC Lesegerät ID CPR50.10-E Proximity Wandleser der Firma OBID aufzubauen. Aufgrund der fehlenden Möglichkeit das Lesegerät der Firma OBID im P2P Modus zu betreiben, wurde dieses durch einen Arduino Mega 2650 mit NFC-Shield ersetzt. Dieser beherrschte zwar den P2P Modus, jedoch nicht das Logical Link Control Protocol (LLCP), welches für die Kommunikation mit dem Android Betriebssystem Voraussetzung ist. Aufgrund der zeitlichen Begrenzung des Projekts wurde darauf verzichtet dieses Protokoll zu implementieren. Stattdessen wurden die zur Einwahl benötigten WLAN - Daten auf ein NFC - Tag geschrieben und mit einer 128 Bit AES Verschlüsselung versehen.
Dies birgt jedoch den Nachteil, dass bei einer Änderung der Zugangsdaten der NFC-Tag gegen einen neuen Tag ersetzt werden muss. Des Weiteren kann mit einem NFC - Tag keine bidirektionale Verbindung aufgebaut werden, weshalb der NFC-Tag vorerst nur zur Integration des mobilen Endgerätes in das Wohnungsnetzwerk dienen kann.

2.1.2 Anbindung und Steuerung des Türschlosses

Nachdem nun die Möglichkeit geschaffen wurde mobile Endgeräte ins Wohnungsnetz zu integrieren, fehlt jetzt noch die Ansteuerung eines elektronischen Schließsystems zum Öffnen der Tür.

In der vorangegangenen Ausarbeitung zu Projekt 1 wurden zwei verschiedene elektronische Schließsysteme vorgestellt. Zum einen das System der Firma Simonss-Voss, zum anderen das System der Firma Dorma. Vor- und Nachteile dieser System werden in der Ausarbeitung zu Projekt 1 näher erläutert. Um vorerst die Machbarkeit einer Türansteuerung mittels eines auf Android basierenden Smartphones zu evaluieren, wurde eine kostengünstigere und weniger aufwendige Variante ausgewählt.
Hierbei handelt es sich um einen Funk - Türschlossantrieb der Firma HomeMatic, welche in Abbildung 2.1 dargestellt ist. Dieses System wird außen auf das Türschloss gesetzt und kann

Abbildung 2.1: HomeMatic Funk - Türschloss

durch einen elektronischen Motor den im Schloss befindlichen Schlüssel in die gewünschte Richtung drehen. Die Steuerung dieses Antriebs wird über eine Funkfernbedienung realisiert. Um den Türschlossantrieb in das Living Place zu integrieren, müssen die Funktionalitäten der Fernbedienung nachgeahmt werden. Hierfür wurde die Fernbedienung auseinandergebaut, um nachvollziehen zu können, welche Pins auf den Platinen bei welcher Funktion geschaltet werden. Nachdem diese Befehle identifiziert waren, musste die Fernbedienung noch um Netzwerkkonnektivität erweitert werden um diese anschließend über das Netzwerk zu steuern. Das Ergebnis ist in Abbildung 2.2 zu sehen.

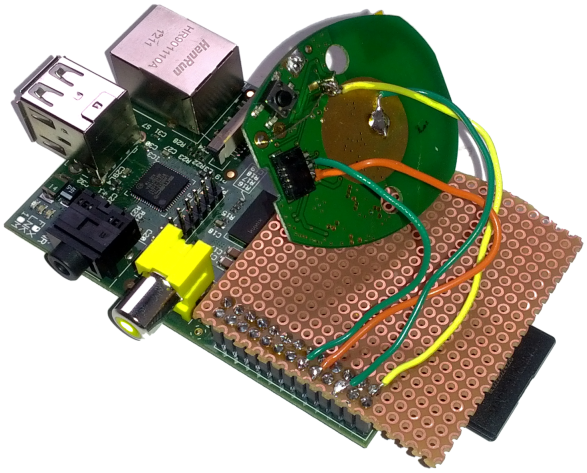

Abbildung 2.2: Raspberry Pi mit angeschlossener Fernbedienung des Funk-Türschlossantrieb

Auf dieser Abbildung wurde die Platine der Fernbedienung mit einem Raspberry Pi verbunden, welcher die Netzwerkkonnektivität herstellt.
Hierfür wurde eine Java - Applikation geschrieben, welches dem Raspberry Pi ermöglicht Befehle über den im Living Place eingesetzten ActiveMQ zu empfangen. Anschließend werden aufgrund dieser Befehle Pins auf dem Raspberry Pi geschaltet, welche die Fernbedienung zum Senden der Befehle animiert.

2.2 Entwicklung der Infrastruktur

2.2.1 Modellierung der Berechtigungsstruktur - PersonBase

Mit der Integration mobiler Endgeräte und dem elektronischen Türschlossantrieb ist das Grundgerüst zum Öffnen einer Tür geschaffen. Neben der dazugehörigen Android Applikation, welche das Öffnen der Tür ermöglichen soll, fehlt noch die Berechtigungsstruktur. Für die Modellierung dieser Struktur wird das Role Based Access Control Modell (Sandhu (1993)) verwenden. Die Entscheidung dieses Modell zu verwenden und auf die gegebene Umgebung zu adaptieren, wurde in der Seminarausarbeitung (Bornemann (2013)) getroffen. Dafür wurden verschiedene Berechtigungsstrukturen miteinander verglichen.
Um die spezifischen Daten von Personen und Ressourcen in einem Verzeichnisdienst verwalten zu können, müssen neue LDAP - Schemata erstellt werden. Die Modellierung dieser Schemata wird in 2.2.2 beschrieben. Die Abbildung 2.3 zeigt die Baumstruktur des ApacheDS Verzeichnisdienstes. Vom Wurzelverzeichnis teilt sich der Baum in drei Teilbäume auf. Der

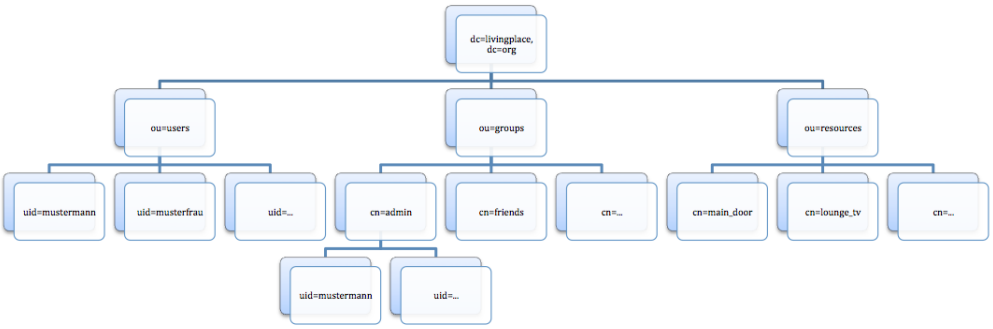

Abbildung 2.3: Baumstruktur des Verzeichnisdienstes

Teilbaum *users* dient zur Ablage der Anwenderdaten. Applikations- und Gerätedaten werden hingegen im Teilbaum *resources* abgelegt. Im dritten Teilbaum *groups* wird die Zuordnung zwischen den Anwendern und ihren Berechtigungen verwaltet.
Im folgenden wird nun näher auf die Modellierung der Struktur eingegangen.

2.2.2 Modellierung der LDAP - Schemata

Um die vorhandenen Daten in der eben vorgestellten Baumstruktur ablegen zu können, muss ein neues LDAP - Schema für das Living Place modelliert werden. Die Attribute und Objekte dieses Schemata müssen mit einer eindeutigen OID gekennzeichnet werden. Diese ermöglicht die eindeutige Identifizierung der Attribute und Objekte im LDAP - Baum. Damit die OIDs Global eindeutig sind, werden diese von der Organisation IANA herausgegeben und verwaltet. Hierdurch wird es möglich, die eigens definierten LDAP - Schemata auch in anderen Verzeichnisdiensten zu verwenden. Für die HAW Hamburg wurde bereits eine OID beantragt, welche für das erstellte Schema verwendet wird.
Im folgenden werden die Objekte und ihre Attribute des definierten LDAP - Schemata vorgestellt. Hierbei ist zu beachten, dass nicht alle Attribute aufgeführt sind.

LPUsers

Dieses Objekt dient zur Speicherung der Anwenderdaten. Hierfür werden die Eigenschaften des Objektes *inetOrgPerson* geerbt, welches die Speicherung von Namen, Benutzernamen, Passwort,

```
objectclass ( 1.3.6.1.4.1.21841.1.1.1
    NAME 'LPUsers'
    DESC 'User im LivingPlace'
    SUP inetOrgPerson
    STRUCTURAL
    MAY ( LPDoorBellEligibility $ LPDoorBellID $ LPAllergy $ LPCurrentPlace )
)
```

Abbildung 2.4: LDAP - Objekt: LPUsers

E-Mail, Adresse, Telefonnummern, etc. ermöglicht. Hinzu kommen eigens definierte Attribute, welche die Verwaltung zusätzlicher Daten gewährleistet. Hierzu gehören beispielsweise die aktuelle Position einer Person innerhalb der Wohnumgebung, der aktuelle Zustand, Hobbys, Musikgeschmack und weitere Vorlieben. Die Abbildung 2.4 zeigt einen Ausschnitt des eben vorgestellten *LPUsers* - Objekts.

LPGroups

Diese Objekt erbt Eigenschaften von *groupOfUniqueNames*. Hierdurch können Attribute vom Type *uniqueMember* hinzugefügt werden. Diese repräsentieren die User der Gruppe. Des Weiteren existiert ein Attribute, welches die Berechtigungen der in dieser Gruppe befindlichen User beinhaltet. Der Aufbau des *LPGroups* - Objekts ist in der Abbildung 2.5 zu sehen.

```
objectclass ( 1.3.6.1.4.1.21841.1.1.2
    NAME 'LPGroups'
    SUP groupOfUniqueNames
    STRUCTURAL
    MAY LPRight
 )
```

Abbildung 2.5: LDAP - Objekt: LPGroups

LPResources

Das aktuelle *LPResources* - Objekt beinhaltet ausschließlich Attribute zur Speicherung von Deviceinformationen. Hierzu zählen Gerätefunktionen, Standort, Gerätetyp, etc.
Die zukünftige Weiterentwicklung der Berechtigungsstruktur wird zeigen, ob diesem Objekt weitere Attribute zur Speicherung von anwendungsbezogenen Daten hinzuzufügen sind. Der bisherige Aufbau des Objekts ist in der Abbildung 2.6 zu sehen.

```
objectclass ( 1.3.6.1.4.1.21841.1.1.3
    NAME 'LPResources'
    STRUCTURAL
    MUST LPResName
    MAY ( LPResFunctions $ LPResIP $ LPResQueue $ LPResTopic $ LPResType )
 )
```

Abbildung 2.6: LDAP - Objekt: LPResources

2.2.3 Entwicklung des Home Agent

Nach der Modellierung und Erstellung des Verzeichnisdienstes PersonBase, muss es den Ressourcen des Living Place Hamburg ermöglicht werden, Information bei der PersonBase zu erfragen, beziehungsweise Informationen abzulegen.
Hierfür wurde eine Java - Applikation entwickelt, welche Nachrichten vom ActiveMQ empfangen und zum AktiveMQ senden kann. Eine Ressource kann somit eine Nachricht an den

ActiveMQ schicken, welcher diese dann an den Home Agent weiterleitet. Der Home Agent extrahiert anschließend alle notwendigen Informationen aus der Nachricht und übermittelt die gewünschte Anfrage an die PersonBase. Das Ergebnis dieser Anfrage wird anschließend an den ActiveMQ übermittelt und somit an die Ressource ausgeliefert. Der Aufbau dieser Umgebung ist in der Grafik 2.7 abgebildet. Dieser Ansatz bietet den Vorteil, dass jeder Service im Living

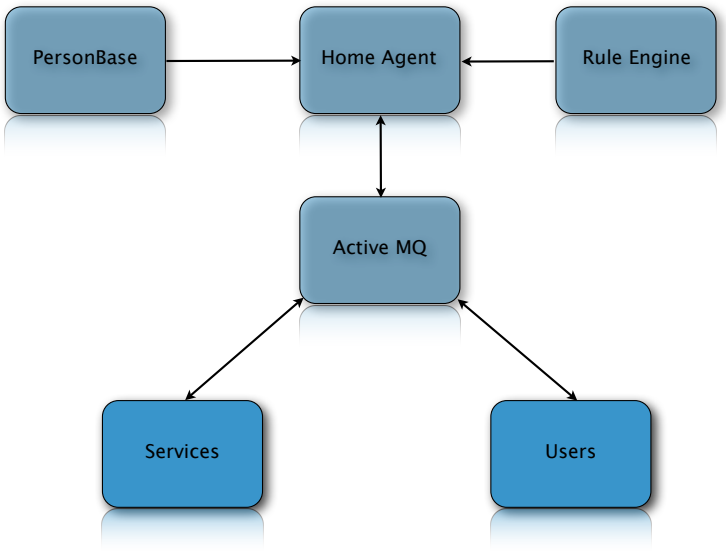

Abbildung 2.7: Aufbau des Komplettsystems

Place durch Versenden einer Nachricht mit der PersonBase kommunizieren kann. Ansonsten müsste jedem Service die Struktur des Verzeichnisdienstes bekannt sein und der Entwickler müsste die Kommunikation mit der PersonBase selber implementieren. Des Weiteren kann der Zugriff auf die PersonBase mittels Home Agent reglementiert werden.

2.2.4 Entwicklung der Android Applikation - Smart Home

Um die Funktion und das Zusammenspiel der einzelnen Komponenten zu testen, wurde eine Android Applikation namens Smart Home entwickelt. Wird das Smartphone an ein NFC - Tag gehalten, welches an der Wohnungstür angebracht ist, wird die Applikation gestartet. Durch die auf dem Tag enthaltenen WLAN - Daten wählt sich das Smartphone automatisch in das vorhandene WLAN ein.
Die linke Abbildung in 2.8 zeigt den Startbildschirm der Applikation. Hier können verschiede-

ne Funktionen ausgewählt werden. Durch einen Klick auf das Icon oben links kann geklingelt werden. Durch das daneben liegende Icon kann eine Videobotschaft für die Bewohner hinterlassen werden. Diese Funktionalitäten wurden bereits im Zuge der Bachelorarbeit (Bornemann, 2011) implementiert und auf die jetzigen Gegebenheiten angepasst.
Durch das dritte Icon können Funktionen bereitgestellt werden, welche nicht für die Öffent-

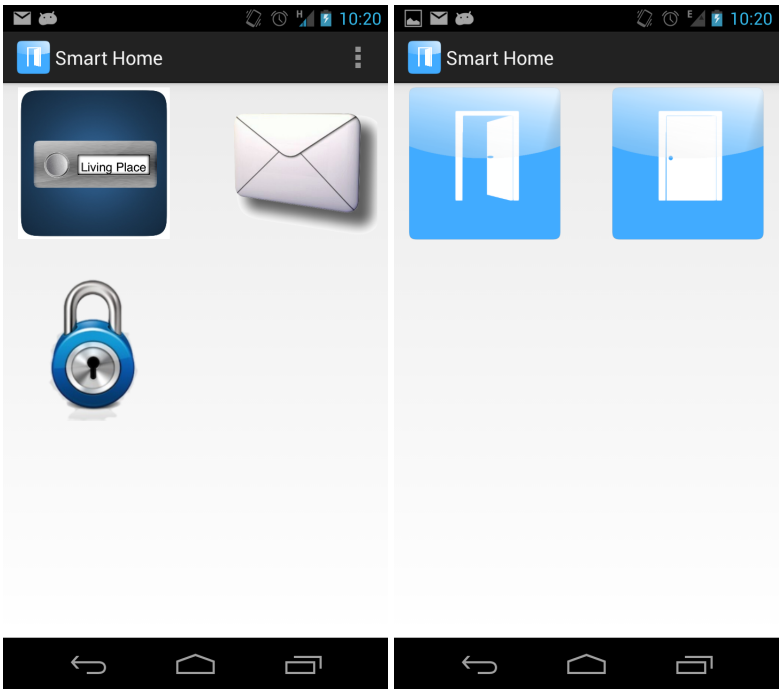

Abbildung 2.8: Android Applikation: Smart Home (links: Home Screen, rechts: Door Control Srceen

lichkeit bestimmt sind. Nach einem Klick auf das Icon mit dem Schlosssymbol werden in der Applikation gespeicherte Zugangsdaten zum Home Agent gesendet. Dieser erfragt die Richtigkeit der Zugangsdaten bei der PersonBase. Sind die Daten korrekt, werden die Berechtigungen des Nutzers erfragt und auf dem Smartphone angezeigt. Diese sind in der rechten Grafik in Abbildung 2.8 zu sehen. Der Benutzer besitzt in diesem Fall die Berechtigungen zur Öffnung, beziehungsweise Schließung, der Wohnungstür.

3 Fazit

3.1 Zusammenfassung

Am Anfang von Projekt 2 stand die Vervollständigung der Arbeiten aus Projekt 1. Diese weiterführenden Arbeiten aus Projekt 1 werden in Kapitel 2.1 beschrieben. Hierbei geht es um essentielle Funktionen, wie die Datenübermittlung durch NFC auf der einen Seite und die Ansteuerung eines elektronischen Schließsystems auf der anderen Seite.
Anschließend wird in Kapitel 2.2 auf die Entwicklung der Berechtigungsstruktur und ihrer Teilsysteme eingegangen. Das Hauptaugenmerk liegt hierbei auf der Modellierung dieser Struktur und ihrer Integration in die vorhandene Netztopologie des Living Place Hamburg. Es wurde der Aufbau der Berechtigungsstruktur mit dem Namen PersonBase vorgestellt. Darauffolgend wurde ein LDAP - Schema entwickelt und vorgestellt, welches die Speicherung von Daten ermöglichen soll, die in einer intelligenten Wohnumgebung von Relevanz sind. Im Kapitel 2.2.3 wurde die entwickelte Java - Applikation mit dem Namen Home Agent beschrieben. Anhand dieser Applikation wird es vorhandenen und zukünftigen Services ermöglicht, auf die Daten der PersonBase zuzugreifen.
In Kapitel 2.2.4 wurde die Android - Applikation mit dem Namen Smart Home vorgestellt. Anhand dieser Applikation soll die Funktionsweise der entwickelten Teilsysteme evaluiert werden. Durch diese Anwendung kann der Anwender öffentliche und private Funktionen nutzen. Bevor jedoch private Funktionen angezeigt werden können, muss sich der Benutzer an der PersonBase authentifizieren. Welche Funktionen von welchem Service der Anwender nutzen darf, ist ebenfalls in der PersonBase abgelegt.

3.2 Ausblick

Die ersten Schritte zur Realisierung einer Berechtigungsstruktur für Smart Homes sind getan. Die Authentifizierung von Personen, sowie die Speicherung und das Abfragen von Informationen sind möglich.
Im Zuge der folgenden Masterarbeit wird an der Verfeinerung der Datenhaltung der PersonBase gearbeitet. Des Weiteren muss ein Interface implementiert werden, welches dem

Bewohner eines Smart Homes die Verwaltung der PersonBase ermöglicht. Um die Steuerung und Verwaltung der PersonBase von vielen Geräten zu ermöglichen, ist die Entwicklung dieser Applikation mittels eines Web Frameworks, wie beispielsweise ASP.NET, Play oder Roo eine geeignete Option.

Des Weiteren wird noch über die Automatisierung verschiedener Prozesse nachgedacht. Hierzu gehört beispielsweise das Anlegen neuer Benutzer. Um den Bewohner bei der Verwaltung der PersonBase zu unterstützen, könnte diese zum Beispiel mit sozialen Netzen gekoppelt werden. Ebenfalls könnte die Anmeldung an die PersonBase über Dienste wie OAuth oder openID vereinfacht werden. So können sich auch Personen bei der PersonBase anmelden, ohne dass der Bewohner die Person vorher explizit anlegen musste.
Darüber hinaus werden im kommenden Semester Rollen für die Berechtigungsstruktur definiert. Diese repräsentieren verschiedene Situationen die in einer Wohnumgebung entstehen können und beinhaltet die Berechtigung welche der User in dieser Situation benötigt. Die Vergabe dieser Rollen an den User wird über die Rule Engine Drools (JBoss Drools Team) realisiert. Diese wird im Rahmen der Masterarbeit von Kjell Otto (Otto (2013)) in das Living Place integriert.

Literaturverzeichnis

[ActiveMQ] ActiveMQ: *ActiveMQ*. – URL http://activemq.apache.org. – letzter Zugriff: 07.03.2013

[ASP.NET] ASP.NET: *Microsoft ASP.net*. – URL http://www.asp.net. – letzter Zugriff: 11.03.1013

[Bornemann 2011] Bornemann, Sven B.: Android-basierte Smart Home Interaktion am Beispiel einer Gegensprechanlage. (2011)

[Bornemann 2012] Bornemann, Sven B.: Integration mobiler Endgeräte in Smart Homes mittels NFC. (2012)

[Bornemann 2013] Bornemann, Sven B.: Entwicklung einer Berechtigungsstruktur für Smart Homes. (2013)

[Google] Google: Galaxy Nexus S. . – URL http://www.google.de/nexus/#/tech-specs. – Letzter Zugriff: 11.08.2012

[IANA] IANA. – URL http://www.iana.org. – letzter Zugriff: 04.03.2013

[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

[LLCP] LLCP: Logical Link Layer Protocol. . – URL http://www.nfc-forum.org/specs/. – Letzter Zugriff: 25.06.2012

[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, 2010. – Forschungsbericht. letzter Zugriff: 19.02.2013

[OAuth] OAuth: *OAuth*. – URL http://oauth.net. – letzter Zugriff: 18.02.2013

[OBID] OBID: ID CPR50.10-E Datenblatt. . – URL http://www.feig.de/uploads/media/Datenblatt_ID_CPR50.10_01.pdf. – Letzter Zugriff: 09.08.2012

[openID] openID: *openID*. – URL http://openid.net. – letzer 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 Angewande Wissenschaften Hamburg, Masterarbeit, 2013. – Noch nicht veröffentlicht

[Play] Play: *Play Framework*. – URL http://www.playframework.com. – letzter Zugriff: 11.03.2013

[Roo] Roo, Spring: *Springsource Community*. – URL http://www.springsource.org/spring-roo. – letzter Zugriff: 11.03.2013

[Sandhu 1993] Sandhu, R.S.: Lattice-based access control models. In: *Computer* 26 (1993), nov., Nr. 11, S. 9 –19. – ISSN 0018-9162

[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)