Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Projektbericht Sommersemester 2012

Sven Boris Bornemann

Integration mobiler Endgeräte in Smart Homes mittels NFC

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Inhaltsverzeichnis

1 Einführung **3**

2 Projektarbeit **5**
2.1 Integration der Endgeräte in das Netzwerk des Smart Homes 5
2.1.1 Anforderungen 5
2.1.2 Eingesetzte Hardware 6
2.2 Ablage der Authentifizierungsdaten 8
2.3 Umsetzbarkeit 9

3 Fazit **11**
3.1 Zusammenfassung 11
3.2 Ausblick 11

Literaturverzeichnis **13**

1 Einführung

Der Trend in der Informatik geht zu immer kleineren Geräten, mit wachsender Funktionsvielfalt. Near Field Communication (NFC) ist hierbei eine Schwellentechnologie, die eine Kommunikation zwischen verschiedensten Geräten ermöglicht. Die Kommunikation findet statt, sobald sich die Geräte auf wenige Zentimeter nähern, somit bietet NFC eine einfache und intuitive Möglichkeit der Interaktion. Durch die Verwendung verschiedener NFC-Tags, besitzt NFC das Potential zu einer ausgereiften physikalischen Benutzerschnittstelle (Broll und Hausen (2010)).
Gerade in Wohnumgebungen bietet NFC ein enormes Potential. Durch eine simple Berührungsgeste können einzelne Funktionen verschiedener Geräte kombiniert oder es kann ein Datenaustausch dieser Geräte initiiert werden. In Chen u. a. (2012) werden einige Beispiele diesbezüglich aufgeführt. Dies ermöglicht dem Anwender eine einfache und intuitive Interaktionsmöglichkeit. Zusätzlich bietet NFC momentan noch eine höhere Robustheit und Stabilität gegenüber anderen Technologie wie beispielsweise Sprach- oder Gestenerkennung.

Das Projekt gliedert sich im Kontext des Living Place Hamburg ein. Hierbei handelt es sich um ein interdisziplinäres Projekt der Hochschule für Angewandte Wissenschaften (HAW) Hamburg. Dies ermöglicht nicht nur Informatikern, sondern auch Künstlern, Designern, Städteplanern und partizipierenden weiterer Fachrichtungen an dem Projekten teilzunehmen (Rahimi und Vogt (2009/2010)).

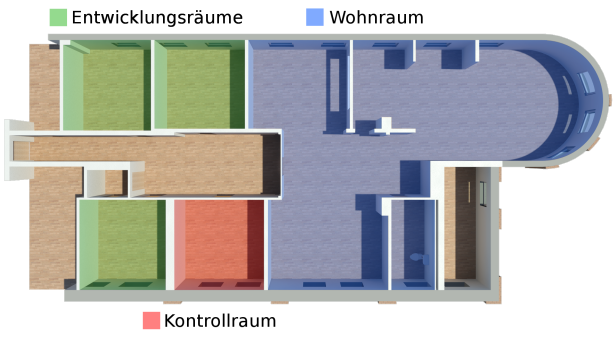

Abbildung 1.1: Grundriss des Living Place Hamburg

Der Aufbau des Living Place begann 2009 und entwickelt sich seitdem ständig weiter. Das Living Place befindet sich in einem Bestandsgebäude der HAW Hamburg (Abb. 1) und bietet eine Fläche von 130m^2. Dies ermöglicht es, den Einfluss neuer Technologien im alltäglichen Leben der Menschen durch Realexperimente zu erforschen.

Ziel

In der Ausarbeitung zu Anwendungen 1 (Bornemann (2012a)) wurde die Vision einer mobilen Türklingel Applikation vorgestellt. Darin soll es Personen ermöglicht werden, mittels eines Smartphones vor einer Wohnungstür zu klingeln, Nachrichten zu hinterlassen oder sogar die Tür zu öffnen. Letzteres darf natürlich nur bestimmten Personen vorbehalten sein und muss dementsprechend abgesichert werden. Dem Bewohner hingegen sollen weitere Funktionen zur Verfügung stehen, wie beispielsweise: Von unterwegs aus sehen, wer vor der Tür steht oder Personen für einen bestimmten Zeitraum das Öffnen der Wohnungstür ermöglichen.

In dieser Ausarbeitung werden einige relevante Teilaspekte dieser Vision evaluiert, um die Machbarkeit der Vision zu gewährleisten. Dies ist zum einen die Integration mobiler Endgeräte in die Wohnumgebung. Hierfür werden in Kapitel 2.1.2 verschiedene Ansätze aufgezeigt und beschrieben. Dies ist notwendig um die eben genannten Funktionalitäten auf den Geräten der Personen zur Verfügung zu stellen.
Zum anderen muss sichergestellt werden, dass die Privatsphäre der Bewohner gewahrt bleibt und die Personen nach der Integration in das Netzwerk der Wohnung keinen Zugriff auf Daten und Services erhalten. Dies wiederum erfordert eine Authentifizierungsmöglichkeit, um gewissen Personen private Funktionalitäten, wie das Öffnen der Tür, zu ermöglichen. Die dafür erforderlichen Komponenten wurden in der Vision der Ausarbeitung Anwendungen 2 (Bornemann (2012b)) angerissen. Die Realisierung dieser Komponenten wird in Kapitel 2.2 näher erläutert.

2 Projektarbeit

In diesem Kapitel sollen die Ergebnisse des Projekts vorgestellt werden. Dabei wird im ersten Teil 2.1 des Kapitels auf die Kommunikation zwischen Smartphone und Smart Home eingegangen. Der zweite Teil 2.2 beschäftigt sich mit der Ablage von Authentifizierungsdaten und Berechtigungen einer Person.

2.1 Integration der Endgeräte in das Netzwerk des Smart Homes

Die Integration mobiler Endgeräte in das Netzwerk einer intelligenten Wohnung ist ein essentieller Bestandteil, des in Kapitel 1, vorgestellten Projekts. Da ohne diese Integration, die unterschiedlichen Dienste des Smart Homes nicht in Anspruch genommen werden können. Zu diesen Diensten gehört beispielsweise die Authentifizierung für die hier vorgestellte Zutrittskontrolle. Einige weitere Funktionalitäten werden in der Vision zur Ausarbeitung Anwendungen 1 Bornemann (2012a) vorgestellt.
Die Eingliederung der mobilen Endgeräte in das Netzwerk, findet über ein sogenanntes „Gast WLAN“ statt. In diesem Netzwerk hat der Anwender nur Zugang zum Internet und ist physikalisch vom Wohnungsnetzwerk getrennt. Dies ist notwendig um die Privatsphäre und die persönlichen Daten der Bewohner zu schützen. Mittels einer Authentifizierung können dem Anwender in diesem Netz nun weitere Berechtigungen, wie beispielsweise das Öffnen der Wohnungstür, gewährt werden. Die Authentifizierung und die Ablage der Daten werden in 2.2 näher erläutert. Damit sich das mobile Endgerät mit dem „Gast WLAN“ verbinden kann muss dies die Einwahldaten erhalten. Im Folgenden werden dafür Anforderungen definiert und eine mögliche Realisierung präsentiert.

2.1.1 Anforderungen

Im Folgenden werden die Anforderungen für die Zusammenführung des mobilen Endgerätes mit dem „Gast WLAN“ vorgestellt.

Bedienbarkeit: Das System soll so einfach wie möglich für den Anwender sein. Dabei soll sich das Gerät möglichst automatisch, also ohne Zutun des Anwenders mit dem „Gast WLAN“ verbinden.

Konfigurationszeit: Die Integration und das Bereitstellen der Funktionalitäten auf dem mobilen Endgerät darf nur einen gewissen Zeitraum in Anspruch nehmen, da ansonsten die Bereitschaft zur Nutzung des Systems sinkt.

Plattformunabhängig: Der Zugang zum „Gast WLAN“ soll verschiedensten Geräten ermöglicht werden.

Stabilität und Zuverlässigkeit: Dies ist eine essentielle Anforderung, da sich ein Endgerät ansonsten nicht mit dem Netzwerk des Smart Homes verbinden kann. Somit können Services, wie beispielsweise das Öffnen der Tür nicht in Anspruch genommen werden.

Sicherheit: Hierbei handelt es sich ebenfalls um eine essentielle Anforderung. Ohne eine Authentifizierung darf kein Zugriff auf private Daten oder Services ermöglicht werden.

Erweiterbarkeit: Es muss gewährleistet werden, dass veränderte Bedingungen der Wohnumgebung, sowie Erweiterungen in das System integriert werden können.

2.1.2 Eingesetzte Hardware

Um die Einwahldaten des „Gast WLAN“ für das mobile Endgerät bekannt zu machen, können verschiedene Übertragungstechnologien verwendet werden. Die simpelste Möglichkeit ist die manuelle Eingabe der Daten durch den Anwender. Gegen diesen Ansatz spricht zum einen die Anforderung der Bedienbarkeit, da hier der Anwender selbst die Daten eingeben muss. Zum anderen sind dem Anwender die Zugangsdaten danach bekannt. Dies stellt ein erhöhtes Sicherheitsrisiko dar.
Eine weitere Möglichkeit besteht darin, die Einwahldaten über einen QR-Code bekannt zu geben. Nachteil dieses Ansatzes ist jedoch, dass bei einer Änderung der Daten, der Code neu generiert werden muss.
Daher wurde für dieses Projekt die Übertragung mittels NFC gewählt. Diese ermöglicht eine automatische Übertragung der Daten, sowie eine anschließende Einwahl, sobald sich die Geräte berühren.

Im Projektverlauf kamen zwei NFC-Lesegeräte zum Einsatz. Beim ersten handelt es sich um den ID CPR50.10-E Proximity-Wandleser (Abb. 2.1) der Firma OBID. Das Lesegerät arbeitet mit den Standards: ISO14443-A, ISO14443-B, ISO15693 und kann somit zur Kommunikation mit RFID-Tags, sowie NFC-Anwendungen verwendet werden. Das Lesegerät wird mittels Power over Ethernet (PoE) mit Spannung versorgt. Über diese Schnittstelle findet ebenfalls der Datentransfer statt, welches eine dezentrale Steuerung des Lesegerätes ermöglicht. Der

Hersteller bietet verschiedene Wrapper an, wodurch das NFC-Lesegerät über .Net oder Java programmiert werden kann. Weitere Spezifikationen sind im Datenblatt (OBID (2012)) des Lesegeräts enthalten.

Da der ID CPR50.10-E in Verbindung mit dem aktuellem Java-Wrapper keine Möglichkeiten zur Nutzung des NFC-P2P Modus bot, kam ein zweites NFC-Lesegerät zum Einsatz. Hierbei handelt es sich um einen Arduino Mega 2650 mit einem NFC-Shield (Abb. 2.2). Einen guten Überblick über die Bedienung und Funktionen des Arduino bietet der Artikel von Mellis u. a. (2007). Der Arduino kann über ein angeschlossenes USB-Kabel oder einem Externen Netzteil mit Spannung versorgt werden. Der Datenaustausch mit dem Arduino findet über das angeschlossene USB-Kabel statt. Für die Möglichkeit einer dezentralen Steuerung, muss der Arduino um ein Ethernet-Shield erweitert werden. Die Programmierung des Arduino erfolgt über C, sowie C++ in der Open-Source Arduino Software (ArduinoSoftware). Durch die eingesetzte Bibliothek PN532 (siehe Seeedstudio (2012)), ist es möglich das NFC-Shield im P2P-Modus zu betreiben, jedoch ist das Logical Link Control Protocol (LLCP) nicht in dieser Bibliothek implementiert. Um eine NFC-P2P Kommunikation zwischen dem NFC-Shield und dem für das Projekt gewählten Smartphone, Google Galaxy Nexus S (Google) zu ermöglichen, wird dieses Protokoll benötigt. Grund hierfür ist das auf dem Smartphone befindliche Android Betriebssystem, welches das Protokoll bei einer P2P Kommunikation voraussetzt. Standardisiert wurde das Logical Link Control Protocol vom NFC-Forum, welches auch für die Weiterentwicklung verantwortlich ist.

Abbildung 2.1: ID CPR50.10-E Proximity-Wandleser (Quelle: OBID (2012))

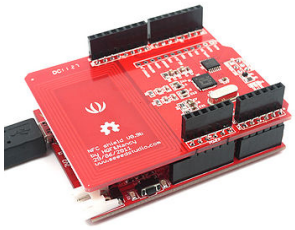

Abbildung 2.2: Arduino mit NFC-Shield (Quelle: Seeedstudio (2012))

Des Weiteren wird ein elektronisches Schließsystem benötigt, welches zum Öffnen der Tür angesteuert werden muss. Mittels Recherchen wurden hier zwei mögliche Schließsysteme identifiziert.
Zum einen ein elektronisches Schließsystem der Firma Siemons-Voss, welches durch drücken eines Funktransponders das Schloss freigibt und dann per Hand geöffnet werden kann. Vorteil bei diesem System ist, das nur das Schloss und ein Transponder benötigt werden. Somit ist ein einfacher Einbau des Systems gewährleistet. Der Transponder kann in der

Nähe der Tür angebracht werden und in Verbindung mit dem schon eingesetzten Arduino angesteuert werden. Nachteilig bei diesem System ist, dass sich das Schloss nur entriegeln lässt. Das Drehen des Zylinders zum Öffnen der Tür erfolgt weiterhin von Hand. Detaillierte Spezifikationen sind unter (Siemons-Voss (b), Siemons-Voss (a)) zu finden.
Zum anderen handelt es sich um ein selbstverriegelndes Panikschloss der der Firma Dorma (Dorma). Das Schloss der Baureihe SVP besitzt ein Motorschloss, welches über eine spezielle Steuereinheit angesteuert wird. Vorteil dieses Systems ist es, dass Aufgrund des verwendeten Motorschlosses, die Tür nach Wunsch verschlossen oder offen gehalten werden kann. Bedingt durch den höheren Funktionsumfang, ist dieses System jedoch aufwendiger und teurer im Einbau.

Die Entscheidung, welches System eingebaut werden soll, viel zu Gunsten eines SVP Schlosses der Firma Dorma aus. Ausschlaggebend hierfür war der höhere Funktionsumfang dieses Systems, welches eine bessere Abbildung verschiedener alltäglicher Situationen einer Wohnumgebung ermöglicht.

2.2 Ablage der Authentifizierungsdaten

Nachdem die Einwahldaten des „Gast WLAN“ auf das Smartphone Galaxy Nexus S übertragen wurden, fehlt nun noch eine Komponente, an der sich die Anwender authentifizieren können und auf der eventuelle Berechtigungen abgelegt sind. Die Wahl viel hier auf einen Verzeichnisdienst, welcher das LDAP-Protokoll verwendet. Dieser bringt aufgrund seiner Performance und Erweiterbarkeit alle notwendigen Voraussetzungen mit sich.
Zum Einsatz kommt der Apache Directory Service (Apache Software Foundation), da dieser noch einige Erweiterungen gegenüber einem Standard LDAP-Verzeichnisdienst mit sich bringt. Hierzu gehört beispielsweise die Integration von Kerberos 5, welches eine einheitliche und sichere Authentifizierung ermöglicht.
Um den ApacheDS in das LivingPlace zu integrieren, wurde dieser in die PersonBase eingebettet. Der architektonische Aufbau sowie einzelne Komponenten sind in der Abbildung 2.3 dargestellt. Der Zugriff auf die Daten des ApacheDS wird über eine Kommunikationsschnittstelle realisiert, die in den Home Agent integriert ist. Diese nimmt fest definierte JSON-Nachrichten über den ActiveMQ entgegen und bearbeitet diese entsprechend. Dies bietet den Vorteil, dass diverse Applikation des Living Place Zugriff auf den Verzeichnisdienst erhalten, ohne dessen interne Struktur kennen zu müssen. Des Weiteren kann so der Zugriff auf die Daten begrenzt und gesteuert werden, da kein direkte Verbindung zur PersonBase hergestellt werden kann. Für den Zugriff auf die Daten des Verzeichnisdienstes kommt das LDAP-Framework von Springsource zum Einsatz. Dieses bietet im Gegensatz zum JNDI-Framework von Java (Oracle) eine geringe Einarbeitungszeit, sowie eine höhere Performance.

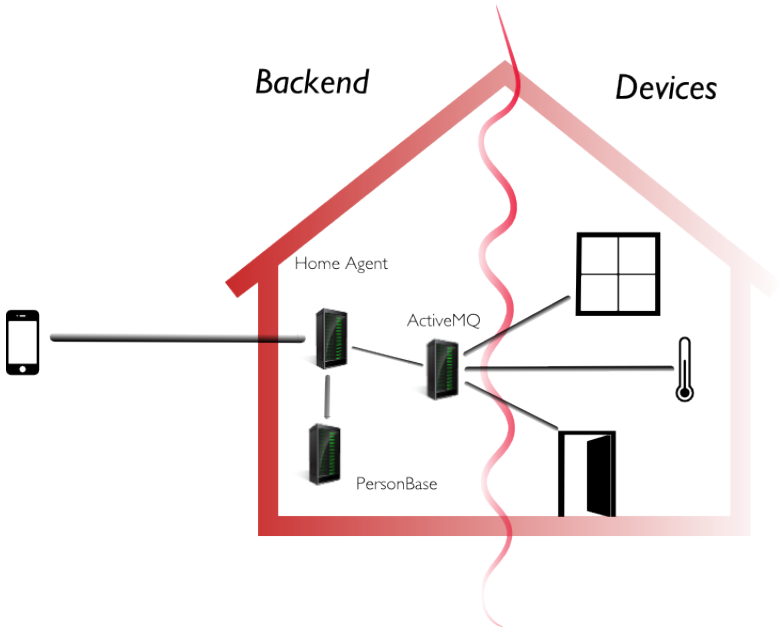

Abbildung 2.3: Architektur

Des Weiteren, sind speziell für das LivingPlace notwindige LDAP-Schemas entwickelt worden, welche die Ablage spezieller Daten ermöglichen. Hierzu gehört zum Beispiel ein „Device-Schema“, welches es ermöglicht den Standort, Namen, Funktionen, etc. zu einem Gerät abzulegen. Ebenfalls wurde ein „Personen-Schema“ erstellt, welches das Speichern relevanter Daten zu einer Person ermöglicht, die einer intelligenten Wohnung von nutzen sein können. Ein konkreter Fall ist das Öffnen der Wohnungstür. Hierfür werden die Daten zur Authentifizierung der Personen, sowie zur Identifizierung des Gerätes in dem Schema abgelegt. Sobald sich eine Person erfolgreich authentifizieren konnte, liest der der Home Agent diese Berechtigungen aus und die zusätzlichen Funktionen werden auf dem mobilen Endgerät eingeblendet.

2.3 Umsetzbarkeit

Die Übertragung der Einwahldaten und die Verbindung zum „Gast WLAN“ stellen einen essentiellen Schritt in diesem Projekt dar. Ohne diese Verbindung kann keine weitere Authentifizierung oder die Inanspruchnahme von Services gewährleistet werden. Mit der verwendeten Technologie NFC, zur Übertragung der Daten, konnte bisher noch keine erfolgreiche Datenübertragung gewährleistet werden. Die Gründe hierfür wurden im Abschnitt 2.1.2 erläutert. Für die Realisierung der Datenübertragung stehen nun drei mögliche Lösungswege zur Verfügung.

Ein Lösungsweg ist die Implementierung des Protokolls LLCP auf dem Arduino. Hierdurch wird eine NFC-P2P Kommunikation zwischen dem Arduino und dem Smartphone ermöglicht. Jedoch benötigt die Implementierung des Protokolls einen erheblichen Zeitaufwand.
Eine zweite Lösung besteht in der Emulationen eines NFC-Tags. Hierbei emuliert das NFC-Lesegerät einen NFC-Tag, der dann vom Smartphone gelesen, beziehungsweise beschrieben werden kann. Bei dieser Kommunikation wird das Protokoll nicht verwendet und erleichtert somit die Kommunikation.
Die dritte Möglichkeit besteht darin, das NFC-Lesegerät durch ein weiteres Smartphone auszutauschen. Dieses arbeitet ebenfalls mit dem Android Betriebssystem, welches das LLCP Protokoll implementiert hat. Somit kann eine P2P Kommunikation ermöglicht werden.
Sollte wiedererwartend keiner dieser Lösungsansätze eine erfolgreiche Datenübertragung ermöglichen, können aufgrund der gewählten Architektur auch andere Technologien zur Integration mobiler Endgeräte in Betracht gezogen werden. Einige dieser Möglichkeiten wurden am Anfang des Kapitels 2.1.2 bereits erwähnt.

Die Realisierung der Datenübertragung wird in Projekt 2 weiter verfolgt. Aufgrund des zeitlich begrenzten Rahmens, kann die Realisierung durch den ersten vorgestellten Lösungsweg vernachlässigt werden. Eine prototypische Realisierung durch den zuletzt vorgestellten Lösungsweg, bei dem ein zweites Smartphone als Lesegerät verwendet wird, verspricht die besten Erfolgschancen, da auf dem Android Betriebssystem alle Voraussetzungen für eine auf NFC-basierende Kommunikation vorhanden sind.

Die Realisierung der PersonBase zur Authentifizierung von Personen und Speicherung personenspezifischer Informationen stellte keinerlei Probleme dar. Die entwickelte Lösung kann somit für die Anforderungen weiterer Applikationen des LivingPlace erweitert werden.

3 Fazit

3.1 Zusammenfassung

Zu Beginn von Projekt 1 stand die Integration der mobilen Endgeräte im Vordergrund. Es wurden Recherchen durchgeführt, um das passende NFC-Lesegerät für dieser Projekt zu finden. Aufgrund der beherrschenden Standards und der vorhandenen Ethernet-Schittstelle fiel die Wahl auf den ID CPR50.10-E Proximity-Wandleser der Firma OBID (OBID (2012)). Während der Verwendung des Lesegerätes fiel jedoch auf, das dieser den NFC-P2P Kommunikationsmodus noch nicht unterstützte.
Aufgrund der zeitlichen Beschränkung in Projekt 1, wurde ein weiteres NFC-Lesegeräte angeschafft, welches den NFC-P2P Kommunikationsmodus beherrscht. Hierbei handelte es sich um den Arduino Mega 2650, der um ein NFC-Shield (Seeedstudio (2012)) erweitert wurde. Durch dieses Lesegerät konnte eine P2P Verbindung zum Galaxy Nexus S Smartphone hergestellt werden. Eine funktionierende Datenübertragung konnte aber über dieses Lesegerät nicht etabliert werden. Die Ursache hierfür bestand darin, dass die verwendete Bibliothek nicht das Logical Link Control Protocol (LLCP) implementierte. Diese ist aber für eine funktionierende Datenübertragung erforderlich. In Kapitel 2.3 wurden verschiedene Lösungswege aufgezeigt, mittels derer eine funktionierende Datenübertragung aufgebaut werden kann.
Des Weiteren wurde eine Realisierung zur Authentifizierung und der Ablage von Berechtigungen zu einer Person vorgestellt. Die gewählte Struktur basiert auf einem LDAP-Verzeichnisdienst. Dieser wurde mittels LDAP-Schemata um die benötigten Attribute erweitert und an die Umgebung des Living Place angepasst. Zusätzlich wurde eine Kommunikationsschnittstelle entwickelt, die den Verzeichnisdienst in die Kommunikationsstruktur des Living Place einbettet. Somit haben auch anderen Services Daten im Verzeichnisdienst ablegen oder Informationen erfragen.

3.2 Ausblick

Aufgrund der Ergebnisse aus Projekt 1 wird in den folgenden Semestern die Kombination der hier vorgestellten Services vorangetrieben. Bevor dies jedoch geschehen kann, wird

eine funktionierende Datenübertragung zwischen dem verwendeten Smartphone und dem NFC-Lesegerät benötigt. Hierfür wird der in Kapitel 2.3 vorgestellte Lösungsansatz realisiert. Anschließend werden das elektronische Schließsystem, die Integration der mobilen Endgeräte und der Verzeichnisdienst zu einem System verbunden.
Des Weiteren soll die Entwicklung der PersonBase vorangetrieben werden. Da hier die Speicherung verschiedenster Informationen ermöglicht wird. Dies können personenbezogene Informationen, wie Musikgeschmack oder Lebensmittelallergien sein. Hierdurch können Services zur Verfügung gestellt werden, die zum Beispiel ein Rezept für eine Mahlzeit erstellen, in der keine Zutat enthalten ist, durch die eine Allergie hervorgerufen werden kann. Aber auch die Speicherung gerätespezifischer Informationen, wie Standort oder Funktionsumfang eines Gerätes könnten abgelegt werden. Somit könnte ein Service Discovery Dienst etabliert werden, der eine einfache Integration neuer Geräte ermöglicht. Auf Basis dieser Informationen können weitere vielfältige Services entstehen, die das alltägliche Leben des Bewohners bereichern und vereinfachen.
Nachdem die verschiedenen Service zu einem System zusammengeführt wurden, soll die Akzeptanz des Systems mittels einer Usability-Untersuchung evaluiert werden.

Literaturverzeichnis

[ArduinoSoftware] *Arduino Software*. – URL http://arduino.cc/en/Main/Software. – Letzter Zugriff: 13.08.2012

[Apache Software Foundation] APACHE SOFTWARE FOUNDATION, Apache: ApacheDS. . – URL www.apacheds.org. – Letzter Zugriff: 15.08.2012

[Bornemann 2012a] BORNEMANN, Sven B.: Mobile Türklingel für Smart Homes. (2012)

[Bornemann 2012b] BORNEMANN, Sven B.: Remoteverbindungen für Smart Homes. (2012)

[Broll und Hausen 2010] BROLL, Gregor ; HAUSEN, Doris: Mobile and physical user interfaces for NFC-based mobile interaction with multiple tags. In: *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services*. New York, NY, USA : ACM, 2010 (MobileHCI '10), S. 133–142. – URL http://doi.acm.org/10.1145/1851600.1851624. – ISBN 978-1-60558-835-3

[Chen u. a. 2012] CHEN, Longbiao ; PAN, Gang ; LI, Shijian: Touch-driven interaction via an NFC-enabled smartphone. In: *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, march 2012, S. 504 – 506

[Dorma] DORMA: Selbstverriegelnde Schlösser. . – URL http://www.dorma.de/prod/content/download/40000/544149/version/2/file/052442-SVP_SVZ-D.pdf/f965d660d8bd19c568a86b9c8032e908.pdf. – Letzter Zugriff: 14.08.2012

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

[Mellis u. a. 2007] MELLIS, David A. ; BANZI, Massimo ; CUARTIELLES, David ; IGOE, Tom: Arduino: An Open Electronics Prototyping Platform. (2007). – URL http://web.media.mit.edu/~mellis/arduino-chi2007-mellis-banzi-cuartielles-igoe.pdf

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

[OBID 2012] OBID: ID CPR50.10-E Datenblatt. (2012). – URL http://www.feig.de/uploads/media/Datenblatt_ID_CPR50.10_01.pdf. – Letzter Zugriff: 09.08.2012

[Oracle] ORACLE: JNDI Overview. . – URL http://www.oracle.com/technetwork/java/overview-142035.html. – Letzter Zugriff: 14.08.2012

[Rahimi und Vogt 2009/2010] RAHIMI, Mohammadali ; VOGT, Matthias: Aufbau des Living Place Hamburg. (2009/2010). – URL http://users.informatik.haw-hamburg.de/~ubicomp/projekte/master09-10-proj/rahimi-vogt.pdf

[Seeedstudio 2012] SEEEDSTUDIO: NFC Shield. (2012), Mai. – URL http://www.seeedstudio.com/wiki/NFC_Shield. – Letzter Zugriff: 09.08.2012

[Siemons-Voss a] SIEMONS-VOSS: Digitale Schließsysteme. . – URL http://www.simons-voss.de/fileadmin/media/Produktkatalog_2012/Bereiche_Auzuege/04_Schliesszylinder/04_DE_Produktkatalog_2012_Schliesszylinder.pdf. – Letzter Zugriff: 14.08.2012

[Siemons-Voss b] SIEMONS-VOSS: Transpondermedien. . – URL http://www.simons-voss.de/fileadmin/media/Produktkatalog_2012/Bereiche_Auzuege/03_Transpondermedien/03_DE_Produktkatalog_2012_Transpondermedien.pdf. – Letzter Zugiff: 14.08.2012

[Springsource] SPRINGSOURCE: Spring-Framework. . – URL http://www.springsource.org/. – Letzter Zugriff: 14.08.2012