FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Experimentelles Usability Engineering für ein NFC-Schließsystem unter Beachtung von Security- und Trustaspekten

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Software Engineering and Internet Computing

eingereicht von

Philipp Matthias Forsthuber
Matrikelnummer 0126060

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Wolfgang Kleinert

Wien, 25. August 2014

(Unterschrift Verfasser/In) (Unterschrift Betreuung)

Experimentelles Usability Engineering für ein NFC-Schließsystem unter Beachtung von Security- und Trustaspekten

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Software Engineering and Internet Computing

eingereicht von

Philipp Matthias Forsthuber
Matrikelnummer 0126060

ausgeführt am
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software
der Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Wolfgang Kleinert

Wien, 25. August 2014

Eidesstattliche Erklärung

Philipp Matthias Forsthuber
Wolfsschanzengasse 11/2/11, 1210 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

I hereby declare that I am the sole author of this thesis, that I have completely indicated all sources and help used, and that all parts of this work – including tables, maps and figures – if taken from other works or from the internet, whether copied literally or by sense, have been labelled including a citation of the source.

(Ort, Datum) (Unterschrift Verfasser/In)

Danksagung

Ich möchte mich an dieser Stelle bei einer Reihe an Personen bedanken, ohne deren Unterstützung diese Arbeit nie vollendet werden hätte können.

Zuallererst meiner liebe- und verständnisvollen Lebensgefährtin, Alexandra Tomann, die ohne Müdigkeit und immer wieder meine Entwürfe korrekturgelesen hat. Auch wenn wir uns bei Beistrichen nicht immer einig waren, vielen Dank!

Bei meinen Eltern, ohne deren moralische und finanzielle Unterstützung in meinen ersten Studienjahren wohl nie ein Akademiker aus mir geworden wäre.

Meinen Betreuer, Prof. Thomas Grechenig, ohne den das Ablegen dieser Arbeit nicht möglich gewesen wäre. Ebenso meinen Forschungskollegen am Institut, Richard Schlögl und Stefan Kuschnigg. Der Input, den ich von beiden während der Erstellung dieser Arbeit erhalten habe, war unschätzbar wertvoll und die Kommunikation immer wertschätzend und freundlich.

Meinem Arbeitgeber, der Faktor Zehn GmbH, der mir 2013 die Möglichkeit gegeben hat, 5 Monate Auszeit zu nehmen, um diese Arbeit endlich fertig zu stellen.

Allen, denen ich mit meinen Problemen in den Ohren gelegen bin, und die sich trotzdem immer positiv und unterstützend mir gegenüber verhalten haben.

Vielen Dank, ohne euch hätte das alles nicht funktioniert!

Kurzfassung

NFC-Schlösser werden in modernen Bürogebäuden und Hotels oft anstelle von herkömmlichen Schließmechanismen eingesetzt. Die Vorteile dieser Systeme liegen in der Möglichkeit der zentralen Verwaltung von Zutrittsberechtigungen, möglichen Auswertungen von Ankunfts- und Rückkehrzeiten, dem einfachen Deaktivieren und Neuausstellen von Zutrittsberechtigungen bei Verlust sowie durch elektronische Karten oder Smartcards in einer Reduktion von Hardware, die man bei sich tragen muss.

Immer öfter kommen derartige Schließmechanismen in privaten Wohngebäuden zum Einsatz. Bei der Anwendung in diesem Kontext ergeben sich grundlegend andere Überlegungen der Benutzerinnen und Benutzer in Vertrauen gegenüber dem Schloss. Liegt bei einem NFC-Schloss am Arbeitsplatz in der Regel das meiste Risiko beim Arbeitgeber, so legt man das gesamte Vertrauen in die Hände des NFC-Schlosses (bzw. des Herstellers desselben), während es um den persönlichen Besitz und die eigene Familie geht.

In dieser Arbeit soll eine Brücke geschlagen werden zwischen den Themen Usability, Trust und in weiterer Folge Security. Dazu werden zuerst die theoretischen Grundlagen erarbeitet. Es wird ein reales, elektrisches Schließsystem präsentiert und das zugehörige Verwaltungssystem einem Usability-Test unterzogen. Dabei kommen in den Grundlagen beschriebene Methoden des Usability Testing zur Verwendung.

Außerdem werden das Vertrauen von Personen in Schließmechanismen mittels einer Umfrage hinterfragt und die Ergebnisse vergleichend ausgewertet. Hier werden ebenfalls Methoden des Usability Testing verwendet.

Das Ergebnis der Arbeit ist ein Überblick über die Benutzbarkeit eines Schließsystemverwaltungsprogramms sowie eine umfassende Umfrage zur Erhebung des Grundvertrauens in drei unterschiedliche Schließmechanismen. Weiters werden Möglichkeiten aufgezeigt, wie die Messbarkeit von Trust funktionieren kann und bestehende Modelle präsentiert, die sich für eine Erweiterung um diese Dimension eignen.

Zusammenfassend wird in dieser Arbeit ein Überblick über Usability und Trust gegeben, Security behandelt und theoretische Modelle präsentiert. Danach werden zwei Studien durchgeführt und deren Ergebnisse analysiert und präsentiert.

Schlüsselwörter

Trust, Usability, Security, Schließmechanismen, Online-Umfrage, TAM, Technology Acceptance Model, System Usability Scale, Interpersonal Trust Scale, Usability Testing, Usability Engineering, Within-Subjects-Testing, Between-Subjects-Testing

Abstract

Electric locks are often used instead of common locking mechanisms in hotels and office buildings. The advantages of these systems lie in their ability to centrally manage access authorization, possibility of reporting arrival and departure times, simple deactivation and reissuing of lost access authorizations when the hardware is lost as well as a reduction of needed hardware with the end user.

More and more, such locking mechanisms are also used in residential buildings. Used in this context, there are fundamentally different priorities the user has regarding security and trust in the lock. While an electric locking mechanisms at office buildings places most, if not all of the risk in the employers responsibility, the same setup at home risks the users whole livelihood, or worse, his familiy.

This thesis is meant to build a bridge between the topics usability, trust and by extension security. For that, theoretical groundwork is laid at first. A real world example of an electric locking mechanism and the corresponding administration software is presented and put under scrutiny by a usability test. For this, previously described usability testing methods are used.

There will also be a survey with the intent of questioning a user's trust in different locking mechanisms and comparing the corresponding results. This will also be undergone by using usability testing methods.

The result of this thesis is an overview over the usability of a locking mechanisms administration software as well as a baseline depicting trust in three different locking mechanisms. There will be mentioned possibilities to measure trust and extend existing models to accommodate this new dimension.

In a nutshell, this thesis presents an overview of usability and trust, briefly describes security and presents theoretical models. Then, two studies are done and their results analysed and presented.

Keywords

Trust, Usability, Security, locking mechanisms, online survey, TAM, Technology Acceptance Model, System Usability Scale, Interpersonal Trust Scale, Usability Testing, Usability Engineering, Within-Subjects-Testing, Between-Subjects-Testing

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

ITS Interpersonal Trust Scale. 23, 70

NFC Near Field Communication. 22

PEOU Perceived Ease of Use. 26, 27

PU Perceived Usefulness. 26, 27

QSG Quick Start Guide. 56

SBI Schlüsselbundinhaber. 44, 45, 47, 48, 50, 51, 66

SBM Schlüsselbundmedium. 56, 63, 66

SSO Schließsystemoperator. 6, 44, 45, 47–51

SUS System Usability Scale. 21, 51, 72

TAM Technology Acceptance Model. 1, 2, 25–27, 29, 70–72

TRA Theory of Reasoned Action. 25

1 Einleitung

„Begin at the beginning," the King said, very gravely, „and go on till you come to the end: then stop."
Lewis Caroll, Alice in Wonderland

Die Verbreitung von Smartphones in den letzten Jahren hat die Art, in der Menschen mit ihrer Umgebung interagieren, grundlegend verändert. Alleine in den ersten drei Quartalen des Jahres 2012 wurden weltweit fast 170 Millionen Smartphones verkauft. Verglichen mit dem Vergleichszeitraum des Vorjahres bedeutet das einen Zuwachs von fast 47 Prozent. Dieses Wachstum steht einem generellen Rücklauf im Mobilfunkmarkt gegenüber, mit etwas mehr als 3 Prozent Reduktion im Verkaufsvolumen über denselben Zeitraum (Gartner Inc. 2014). Es ist davon auszugehen, dass der Markt an Smartphones noch mehr wachsen wird.

Viele Aufgaben des täglichen Lebens werden durch diese Geräte erleichtert, wie beispielsweise Bankgeschäfte (Erste Bank AG 2014), das Abrufen, Bearbeiten und Beantworten von E-Mails (Hodgekiss 2014), die Navigation im öffentlichen Raum (Apple Inc. 2014a) oder die Kommunikation mit Familie, Freunden, Freundinnen und Bekannten via verschiedener Social Networks [1]. Diese Durchdringung bewirkt weiters, dass mehr sicherheitskritische Bereiche von Smartphones durch Hard- und Software unterstützt werden. Es ist zum Beispiel möglich, eine elektronische Geldbörse auf einem Smartphone mit Guthaben aufzuladen und dann das Telefon als Zahlungsmittel zu verwenden (Google Inc. 2014b).

Aus diesem Grund ist es wichtig, dass die Applikationen, die diese Funktionen unterstützen, das Vertrauen (Den sogenannten „Trust") des Benutzers und der Benutzerin verdienen. Weiters sollen solche Anwendungen sicher („Secure") sein. Sowohl Trust als auch das subjektive Sicherheitsgefühl sind vor allem im Bereich der privaten oder finanziellen Information von Endbenutzern und Endbenutzerinnen noch nicht gegeben (Lange und Ellen 2011). Außerdem sind in diesen Bereichen Fehler in der Anwendung der unterstützenden Programme aufgrund der verwalteten Daten besonders riskant. Solche Fehler sind durch korrekten Einsatz von Usability Engineering vermeidbar (Nielsen 2001). Dabei wird durch einen wohl definierten Lebenszyklus die Usability von Software überprüft und durch Behebung der gefundenen Inkonsistenzen ständig verbessert.

In dieser Arbeit soll daher eine Usability-Studie an einem sicherheitskritischen System durchgeführt werden. Dazu wird ein laufendes Projekt zur Erstellung eines NFC-basierten Schließsystems an der Technischen Universität Wien als Fallbeispiel herangezogen, dessen Benutzerschnittstellen von Anfang an entsprechend gängigen Usability Engineering-Techniken entworfen wurden. Außerdem wird die Benutzbarkeit des sichereren Systems in Augenschein genommen und die Ergebnisse der Studie dahingehend untersucht. Dabei soll betrachtet werden, welche Auswirkungen unterschiedlich ausgereifte Usability-Entscheidungen auf die Aspekte Security und Trust des Systems haben. Gefundene Usability-Probleme werden dargestellt und nach ihrer Auswirkung auf die Sicherheit des Systems bewertet.

[1] z.B. http://facebook.com, http://twitter.com, http://plus.google.com

In weiterer Folge wird eine Möglichkeit gesucht, den empfundenen Trust mit der gemessenen Security zu verbinden. Hierzu wird das Technology Acceptance Model (TAM) als theoretisches Modell herangezogen. Dieses Modell ist leicht erweiterbar. Ein Online-Fragebogen soll eine Basis für eine Erweiterung bieten, die das TAM mit Trust verbindet. Dieser Fragebogen wird den Trust vergleichen, der den drei verschiedenen Schließmechanismen entgegengebracht wird.

Es wird erwartet, dass das System Verbesserungsmöglichkeiten in allen drei Aspekten bietet. Dazu wird im ersten Schritt ein theoretischer Überblick über Usability im Allgemeinen gegeben sowie die Sicherheiten und Unsicherheiten, die von den Usability Engineering Methoden als Ergebnis geliefert werden können, analysiert. Danach wird im zweiten Schritt der Studie in einem Snapshot das vorhandene System analysiert und eine Darstellung des Ist-Stands gegeben. In weiterer Folge werden Analysen des Systems durchgeführt und eventuelle Hürden, konkrete Sicherheitsprobleme sowie Teile mit unzureichendem Trust aufgezeigt. Abschließend wird ein Katalog an detaillierten Verbesserungsvorschlägen ausgearbeitet.

Aufbau der Arbeit:

Im zweiten Kapitel wir das getestete System beschrieben. Dadurch soll ein Überblick gegeben werden, welche Funktionen die Testpersonen im Zuge ihres Usability-Tests verwenden sollten. Es werden die verschiedenen Komponenten präsentiert, die die Funktionalität des Systems repräsentieren. Außerdem wird das Kernstück der Nutzersicht eines Schließsystems präsentiert, der Sperrvorgang.

In den nächsten beiden Kapiteln wird der theoretische Unterbau der praktischen Arbeit dargelegt. Zuerst wird der Begriff des Vertrauens beschrieben. Nach einer Literaturanalyse werden Wege vorgestellt, wie Trust messbar gemacht werden kann. Im Anschluss wird mit dem TAM ein Fragebogen-Modell vorgestellt, das um die Komponente Trust erweitert werden kann. Den Abschluss bildet ein Überblick über mögliche Symbole, die in dem Benutzer und der Benutzerin Trust erzeugen können.

Im folgenden Kapitel wird der Begriff der Verwendbarkeit beschrieben. Eine Begriffsdefinition beginnt das Kapitel. Die ISO Standards zum Thema Usability Engineering helfen dabei zu verstehen, wie gute Verwendbarkeit bei Software zu erreichen ist. Im Anschluss werden Testmöglichkeiten und -strategien erläutert, mit denen Verwendbarkeit getestet werden kann.

Das fünfte Kapitel beschäftigt sich mit dem konkreten Test des Systems. Erst wird das Testvorgehen definiert und die Fragestellung präsentiert. Eine Definition der Testfälle leitet über in die Auswertung der Egebnisse. Zuletzt werden Rückschlüsse aus den Ergebnissen gezogen und die Kommentare der Testpersonen analysiert.

Das sechste Kapitel besteht aus Vorschlägen zur Verbesserung der Verwendbarkeit des getesteten Systems. Diese werden im Detail vorgestellt und mit den gefundenen Problemen in Verbindung gebracht.

Im letzten Kapitel wird ein Ausblick auf weitere Arbeiten gegeben und die Erkenntnisse der vorliegenden Diplomarbeit zusammengefasst.

2 Systembeschreibung

Everything must be made as simple as possible. But not simpler. Albert Einstein

In diesem Kapitel wird die Funktionalität des Systems beschrieben. Dabei wird auf die einzelnen Komponenten eingegangen. Anhand von Abbildungen werden Bedienkonzepte erläutert. Zum Abschluss wird der Sperrvorgang näher beschrieben (Research Industrial Systems Engineering (RISE) GmbH 2014).

2.1 Einleitung

Bei dem getesteten System handelt es sich um das Projekt Sunrise, das an der Technischen Universität Wien mit Partnern aus der Wirtschaft durchgeführt wurde. Das Ergebnis ist mittlerweile im Handel erhältlich und firmiert unter dem Namen AirKey (EVVA Sicherheitstechnologie GmbH 2014). Getestet wurde das System unter dem Namen Sunrise, daher wird in weiterer Folge dieser Name verwendet.
Das System besteht aus den Komponenten Schließzylinder, Schließmedium (Schlüsselkarte oder Smartphone mit dazugehöriger App) sowie einem webbasierten Verwaltungssystem. Der Zylinder passt dabei in standardisierte Bohrungen von Haus- und Wohnungstüren und ist somit für den Gebrauch von Privatpersonen geeignet. Die Kommunikation zwischen Schließzylinder und Schließmedium funktioniert über den Near Field Communication (NFC)-Standard. Der Schließzylinder funktioniert offline, für die Einrichtung ist es notwendig, dass der Zylinder über einen Kartenleser oder ein Smartphone mit den relevanten Daten und Sperrberechtigungen aktualisiert wird.
Das Erteilen und Entziehen von Berechtigungen, das Erstellen von Schließbereichen (mehrere Schlösser in einer Verwaltungseinheit) sowie das Blacklisting von Medien erfolgt über die webbasierte Oberfläche. Das hat den Vorteil, dass die Verwaltung in einem sicheren Rechenzentrum liegen kann und nur über sichere Kanäle kommuniziert wird. Berechtigungen werden anhand von Credits erzeugt, die pro Synchronisierung („Anfertigen“ in der Sprache des Systems) verwendet werden müssen.

2.2 Zusammenfassung und Beschreibung der Systemkomponenten

Hier werden die verschiedenen Rollen und Komponenten im System beschrieben.

2.2.1 Administrator

Ein Administrator darf eine Schließanlage verwalten. Er kann Schlüsselbundmedien und Schließkomponenten hinzufügen, bearbeiten und löschen. Um einen Administrator anzulegen, muss der

Punkt „Administrator anlegen“ aus dem Drop-Down-Menü „Administratoren“ ausgewählt werden. Dadurch erscheint eine Eingabemaske, die der Benutzer ausfüllen muss. Wird die Eingabe gespeichert, ist der Administrator angelegt. Eine Aufforderung zur Bestätigung wird an die angegebene Email-Adresse geschickt, der nachgekommen werden muss, um den Prozess zu beenden.

Ähnlich funktioniert auch das Bearbeiten bzw. Löschen eines Administrators. Dazu muss aus demselben Drop-Down-Menü der Punkt „Administratoren“ ausgewählt werden. Dadurch erscheint eine Liste der angelegten Administratoren. Diese Liste kann durchsucht werden, und durch Klick auf einen Administrator werden die Details zu diesem Administrator angezeigt. Auf dieser Seite ist es möglich, die Daten des Administrators zu bearbeiten (das ist nach erstmaligem Einloggen nur dem jeweiligen Administrator vorbehalten) sowie den Administrator zu löschen.

2.2.2 Personen

Eine Person repräsentiert einen Benutzer oder eine Benutzerin der Schließanlage und kann Schlüsselbundmedien zugewiesen bekommen. Um eine Person anzulegen, muss der Punkt „Person anlegen“ aus dem Drop-Down-Menü „Medien & Personen“ ausgewählt werden. Beim Anlegen einer Person sind die einzigen Pflichtangaben Vor- und Nachname. Es kann ein eigener Benutzername vergeben werden. Die Kombination der drei Angaben muss innerhalb einer Schließanlage eindeutig sein. Weiters können Kontaktdaten wie Adresse oder Telefonnummer eingetragen werden. Wurde eine Person angelegt, ist es möglich wie in 2.2.4 beschrieben eine Person und ein Schließmedium zu verknüpfen.

Ähnlich funktioniert auch das Bearbeiten bzw. Löschen einer Person. Dazu muss aus demselben Drop-Down-Menü der Punkt „Personen“ ausgewählt werden. Dadurch erscheint eine Liste der angelegten Personen. Diese Liste kann durchsucht werden, und durch Klick auf eine Person werden die Details zu dieser Person angezeigt. Auf dieser Seite ist es möglich, die Daten der Person zu bearbeiten sowie die Person zu löschen.

2.2.3 Schließkomponenten

Das System unterscheidet mit Zylinder bzw. Wandleser zwei Arten von Schließkomponenten. Der einzige Unterschied zwischen den beiden besteht in der Stromversorgung des Wandlesers. Daher werden im Folgenden die beiden Komponenten synonym verwendet. Abbildung 2.1 zeigt eine Darstellung eines Zylinders ohne Stromversorgung.

Das Hinzufügen einer Schließkomponente kann entweder per Kartenleser oder per NFC-fähigem Smartphone erfolgen. Auf dem Smartphone muss dazu die App (siehe Abschnitt 2.2.6) installiert sein, es muss bei der Schließanlage registriert sein und sich im Wartungsmodus befinden. Das Smartphone wird an die Schließkomponente gehalten. Es erscheint ein Dialog am Display, der es erlaubt, eine Bezeichnung für die Schließkomponente zu vergeben und sie einer Schließanlage hinzuzufügen. Um eine Schließkomponente mittels Kartenleser einer Schließanlage hinzuzufügen muss der Punkt „Schließkomponenten“ aus dem Drop-Down-Menü „Schließanlage“ ausgewählt werden. Im folgenden Dialog erscheint eine Schaltfläche „Schließkomponente hinzufügen“. Nach Klick auf diese Schaltfläche erscheint die Aufforderung, die Schließkomponente auf den Kartenleser zu legen. Es ist wie beim Smartphone eine Bezeichnung für die Schließkomponente einzugeben, bevor sie hinzugefügt werden kann.

Ähnlich funktioniert auch das Bearbeiten bzw. Löschen einer Schließkomponente. Dazu muss

aus demselben Drop-Down-Menü der Punkt „Schließkomponenten“ ausgewählt werden. Dadurch erscheint eine Liste der angelegten Schließkomponenten. Diese Liste kann durchsucht werden, und durch Klick auf eine Schließkomponente werden die Details zu dieser Schließkomponente angezeigt. Auf dieser Seite ist es möglich, die Daten der Schließkomponente zu bearbeiten sowie die Schließkomponente zu löschen.

Abbildung 2.1: Schließzylinder ohne ständige Stromversorgung

2.2.4 Medien

In diesem Abschnitt wird beschrieben, welche verschiedenen Schlüsselbundmedien im System erkannt werden und wie diese bearbeitet werden können. Im ersten Schritt muss ein Medium angelegt werden. Um ein Medium anzulegen muss der Punkt „Medium anlegen“ aus dem Drop-Down-Menü „Medien & Personen“ ausgewählt werden. Hier gibt es nun die Möglichkeit, ein Smartphone oder eine Schlüsselkarte zu berechtigen. Für ein Smartphone muss eine Telefonnummer angegeben werden, die gültig und in der Schließanlage einzigartig sein muss. Eine Schlüsselkarte muss per Kartenleser oder einem Smartphone im Wartungsmodus hinzugefügt werden. Es kann eine Bezeichnung für die Karte vergeben werden. In Abbildung 2.2 ist eine Karte auf einem Kartenleser zu finden, in Abbildung 2.3 eine Smartphone auf einem Kartenleser.

Ähnlich funktioniert auch das Bearbeiten bzw. Löschen eines Mediums. Dazu muss aus demselben Drop-Down-Menü der Punkt „Medien“ ausgewählt werden. Dadurch erscheint eine Liste der angelegten Medien. Diese Liste kann durchsucht werden, und durch Klick auf ein Medium werden die Details zu diesem Medium angezeigt. Auf dieser Seite ist es möglich, die Daten des Mediums zu bearbeiten sowie das Medium zu löschen. Ein Smartphone kann in dieser Ansicht die Berechtigung zum Wartungsmodus erhalten.

Medien können dupliziert werden. Dazu muss das zu duplizierende Medium Berechtigungen besitzen und das Zielmedium bereits angelegt sein. Die Schaltfläche befindet sich in der Bearbeitungsübersicht. Personen und Medien können in der jeweiligen Bearbeitungsansicht auch gegenseitig

zugewiesen werden. Zuweisungen müssen vor dem Löschen aufgehoben werden.

Medien können in dieser Ansicht auch deaktiviert bzw. reaktiviert werden. Ein deaktiviertes Medium verliert nach erfolgreicher Synchronisation der Schließanlage seine Berechtigungen. Nach erfolgreicher Reaktivierung sind alle noch vorhandenen Berechtigungen wieder aktiv, sollten sie noch nicht gelöscht worden sein.

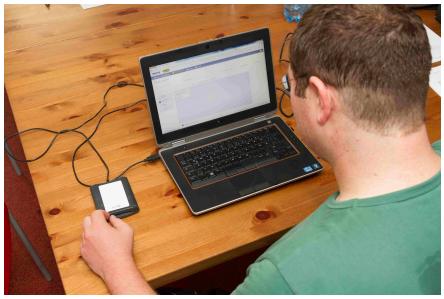


Abbildung 2.2: Synchronisieren einer Karte mittels Kartenleser

Abbildung 2.3: Synchronisieren eines Smartphone mittels Kartenleser

2.2.5 Zutrittsberechtigungen

In diesem Abschnitt wird beschrieben, welche Arten von Zutrittsberechtigungen im System erkannt werden und wie diese bearbeitet werden können. Um eine Zutrittsberechtigung anzulegen, muss entweder eine Person oder ein Medium ausgewählt werden. Auf der Medienübersicht ist es möglich, Schlüssel anzufertigen. Hier werden auch bereits erzeugte Schlüssel angezeigt, die auf diesem Medium vorhanden sind. Die Schlüssel sind farblich kodiert.

- *Grüne Farbe* bedeutet, dass die Berechtigung gültig und synchronisiert ist.
- *Blaue Farbe* bedeutet, dass die Berechtigung erstellt, aber noch nicht synchronisiert ist.
- *Gelbe Farbe* bedeutet, dass die Berechtigung geändert oder gelöscht wurde, aber noch nicht synchronisiert ist.
- *Ausgegraut* bedeutet, dass die Berechtigung nicht mehr gültig ist.

Es gibt im System mehrere Arten von Zutrittsberechtigungen, die unterschiedlich gehandhabt werden.

- *Dauerzutritt:* Hier kann eine permanente Berechtigung für eine Schließkomponente vergeben werden. Diese gilt solange sie nicht entfernt oder deaktiviert wird.
- *Periodischer Zutritt:* Hier kann ein wiederkehrender Zeitraum definiert werden, in dem die Berechtigung gilt. (Beispielsweise jeden Mittwoch von 10:00 bis 14:00h)
- *Einzelzutritt:* Hier kann der Zutritt nur für einen bestimmten Tag zu einem bestimmten Zeitpunkt definiert werden.
- *Individueller Zutritt:* Hier können die bisher beschriebenen Zutrittsarten in bis zu achtfacher Kombination vergeben werden.

Um eine Zutrittsberechtigung zu ändern oder zu löschen, ist die entsprechende Änderung aufzurufen. Auf dem folgenden Dialog finden sich die Schaltflächen „Zutritt ändern“ und „Löschen“.

2.2.6 Smartphone Applikation

Wie beschrieben kann auch ein Smartphone als Schlüsselbundmedium verwendet werden. In diesem Abschnitt wird diese Funktionalität näher beschrieben. Zu Anfang muss das Smartphone registriert werden. Dazu ist die App zu starten. Über das Kontextmenü erscheint der Menüpunkt „Schließanlage hinzufügen“. Ein Registrierungscode, der von einem Administrator oder einer Administratorin vergeben wird, muss eingegeben werden. War der Vorgang erfolgreich, ist das Smartphone für die Verwendung mit der Schließanlage registriert. Es ist auch möglich, das Smartphone als Schlüsselbund für mehrere Schließanlagen zu verwenden. Das setzt eine erfolgreiche Registrierung für jede einzelne Schließanlage voraus. Es ist auch möglich, Schließkomponenten und Schlüsselkarten mittels Smartphone zu synchronisieren. Ist das Smartphone als Wartungsgerät definiert, ist es auch möglich Schließkomponenten in einer Schließanlage zu bearbeiten.

2.2.7 Protokoll

Das System protokolliert alle Vorgänge innerhalb eines Schließsystems. Um das Protokoll einsehen zu können, muss der Punkt „Protokolle“ geöffnet werden. Es ist möglich, Protokolle über Schließkomponenten, Medien oder die Administratorentätigkeit einzusehen.

2.3 Sperrvorgang

In diesem Abschnitt wird der Sperrvorgang beschrieben, mit dem ein Schließsystemoperator (SSO) ein Schloss öffnen kann. Die Voraussetzungen dafür sind synchronisierte Schlüsselzustände auf jedem Medium, das in Verwendung ist sowie die notwendigen Berechtigungen auf dem Sperrmedium.

2.3.1 Sperrvorgang mit Karte

Die Karte wird an den Schließzylinder gehalten. Der Schließzylinder beginnt mit blauen Leuchtdioden zu blinken. Dieses Feedback bedeutet, dass ein Schlüsselmedium erkannt wurde und der Schlüssel überprüft wird. Wenn die Überprüfung positiv abgeschlossen wurde, leuchten die Dioden am Schloss grün auf, der Zylinder kuppelt ein und das Schloss kann per Drehung geöffnet

oder geschlossen werden. Wenn die Überprüfung negativ abgeschlossen wurde, leuchten die Dioden am Schloss rot auf und der Zylinder kuppelt nicht ein. Das Schloss kann nicht geöffnet werden. Die Darstellung eines erfolgreichen Sperrvorgangs mit Karte ist in Abbildung 2.4 zu finden.

Abbildung 2.4: Überprüfung des Schlüssels auf der Karte (links); Erfolgreiche Überprüfung, Tür geöffnet (rechts)

2.3.2 Sperrvorgang mit Smartphone

Der Sperrvorgang mit dem Smartphone funktioniert sehr ähnlich wie der Sperrvorgang mit der Karte. Die App, die auf dem Smartphone installiert ist und die Schlüssel verwaltet, wird geöffnet. Das Smartphone wird an den Schließzylinder gehalten. Der Schließzylinder beginnt, mit blauen Leuchtdioden zu blinken. Dieses Feedback bedeutet, dass ein Schlüsselmedium erkannt wurde und der Schlüssel überprüft wird. Wenn die Überprüfung positiv abgeschlossen wurde, leuchten die Dioden am Schloss grün auf, der Zylinder kuppelt ein und das Schloss kann per Drehung geöffnet oder geschlossen werden. Wenn die Überprüfung negativ abgeschlossen wurde, leuchten die Dioden am Schloss rot auf und der Zylinder kuppelt nicht ein. Das Schloss kann nicht geöffnet werden. Die Darstellung eines erfolgreichen Sperrvorgangs mit Smartphone ist in Abbildung 2.5 zu finden.

Abbildung 2.5: Überprüfung des Schlüssels auf dem Smartphone (links); Erfolgreiche Überprüfung, Tür geöffnet (rechts)

3 Usability

> It is impossible to design anything that is foolproof because fools are so ingenious. - *Groucho Marx*

Dieses Kapitel definiert den Begriff „Usability“. Außerdem wird beschrieben, was beim Design von Objekten oder Software beachtet werden muss, damit diese als benutzbar gelten. Es wird erläutert, wie Design, Usability und die Funktionalität eines Objekts zusammenhängen. Danach wird beschrieben, wie die Benutzbarkeit von Software im Speziellen gemessen werden kann. Zuletzt wird auf den Aspekt der Security eingegangen und wie Security und Usability zusammenhängen.

3.1 Definition

Der Begriff „Usability“ im Kontext der Software Entwicklung ist durch den ISO Standard 9241-11 ISO (1998a) folgendermaßen definiert:

> *„Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.“*

Das Wort beschreibt demnach, in welchem Ausmaß ein Objekt, egal ob es sich um einen realen, physischen Gegenstand oder um eine virtuelle Repräsentation handelt, benutzbar ist. In Erweiterung bedeutet das Wort „Usability“ , dass ein Objekt angenehm und praktisch zu verwenden ist. In diesem Kapitel wird das Hauptaugenmerk auf die Softwarebenutzbarkeit gelegt. In weiterer Folge wird Synonym für diesen Begriff das Wort „Usability“ verwendet, um die Lesbarkeit zu verbessern. Nielsen (1993) definiert fünf Qualitätsmerkmale, nach denen Usability zu bewerten ist.

- **Learnability:** Hierbei ist die Frage zu stellen, wie leicht es fällt, bei dem ersten Kontakt mit der Software ohne Hürden das Ziel zu erreichen. Als Metrik wird hier die Zeit herangezogen, die dafür notwendig ist. Je mehr Zeit notwendig ist, umso frustrierender ist es und umso weniger benutzbar ist das System.
- **Efficiency:** Hierbei ist zu hinterfragen, wie schnell und einfach wiederkehrende Aufgaben nach dem Erlernen des Systems erledigt werden können. Konkret ist hier der notwendige Aufwand, um eine Aufgabe zu erledigen, dem Nutzen dieser Aufgabe gegenüber zu stellen. Ist der Aufwand geringer als der Nutzen, ist das Merkmal der Effizienz erfüllt.
- **Memorability:** Damit dieses Merkmal erfüllt wird, ist es notwendig, dass Aufgaben auch nach langer Zeit der Nicht-Benutzung ohne signifikanten Mehraufwand weiterhin gelöst werden können. Als Metrik kann hierbei die Zeit zweier Testgruppen gemessen werden, die unterschiedlich lange Pausen zwischen Erstbenutzung und weiteren Benutzungen der Software hatten. Können beide Gruppen die Aufgabe in ähnlicher Zeit lösen, ist die Erinnerbarkeit erfüllt. Ist dies nicht der Fall, liegen Usability Probleme vor.

- **Errors:** Dieses Merkmal beschreibt die Summe aller Fehler, die bei der Verwendung einer Software begangen werden. Als Fehler ist eine Aktion zu werten, die nicht das gewünschte Ziel als Ergebnis hat. Je weniger Fehler ein System bei der Benutzung hervorruft, desto besser wird dieses Merkmal erfüllt.
- **Satisfaction:** Hierbei gilt, das subjektive Gefühl der Benutzer und Benutzerinnen nach erfolgreicher Anwendung der Software zu erfragen und zu interpretieren. Dazu ist eine Befragung, entweder mittels Interview oder eines Fragebogens anhand standardisierter Fragen hilfreich. Umso höher die Zufriedenheit, desto besser ist dieses Merkmal erfüllt.

Damit diese Merkmale erfüllt sind und dadurch gute Usablilty erreicht werden kann, wurden in ISO (1998c) Darstellungsprinzipien und Grundlagen zur Dialoggestaltung vorgegeben. Die beschriebenen Normen und Prinzipien werden hier beschrieben.

Darstellungsprinzipien

Diese Elemente sind in ISO Standard 9241-12 zu finden (ISO 1998b). Hier werden Konzepte und Ideen beschrieben, die helfen sollen, die dargestellten Informationen einfach und effektiv zu erfassen und zu verstehen.

- **Klarheit:** Informationen werden gut strukturiert sowie schnell und genau vermittelt. Die Informationen werden leicht erfasst und verstanden.
- **Unterscheidbarkeit:** Die Art der angezeigten Informationen kann genau unterschieden werden. Eine Schaltfläche kann beispielsweise leicht von normalem Text unterschieden werden.
- **Kompaktheit:** Es werden ausschließlich die Informationen angezeigt, die für das Erreichen des aktuellen Ziels notwendig sind. Weitere Informationen werden nur kontextabhängig dargestellt. Dadurch ist es nicht notwendig, hilfreiche Informationen aus unwichtigen herauszufiltern.
- **Konsistenz:** Gleichartige Informationen und Schaltflächen werden über die gesamte Software hinweg auf die gleiche Weise dargestellt. Navigationselemente befinden sich auf jedem Dialog an derselben Stelle.
- **Erkennbarkeit:** Die Aufmerksamkeit der Benutzer und Benutzerinnen wird auf die relevanten Informationen gelenkt. In Kombination mit Kompaktheit werden ausschließlich die wichtigsten Informationen an zentralen Stellen der Software angezeigt.
- **Lesbarkeit:** Information ist leicht aufzufinden und einfach zu lesen. Die Schriftgröße ist genauso zu beachten wie beispielsweise die Animationsgeschwindigkeit beweglicher Komponenten. Auf eine gute Formatierung ist zu achten, Textblöcke sind zu vermeiden.
- **Verständlichkeit:** Die Information ist eindeutig, leicht verständlich, erkennbar und interpretierbar. Beispiele dafür sind grüne Haken, die eine Eingabe bestätigen, wohingegen rote Kreuze eine Eingabe abbrechen.

Dialoggestaltung

Diese Elemente befinden sich in ISO Standard 9241-110 (ISO 2006). Hier werden Konzepte und Ideen beschrieben, die bei der Gestaltung von Dialogsystemen angewandt werden sollen.

- **Aufgabenangemessenheit:** Hierbei geht es darum, die benutzende Person zu unterstützen, ihre Aufgabe effektiv und effizient zu erledigen. Beispielsweise wird ein Textcursor direkt in das erste Eingabefeld positioniert, damit sofort mit der Eingabe gestartet werden kann.
- **Selbstbeschreibungsfähigkeit:** Ziel dieses Konzepts ist es, jeden Dialogschritt unmittelbar verständlich zu gestalten und auf Nachfrage näher zu erläutern. Ein Beispiel dafür ist ein Text, der erscheint, wenn der Mauszeiger über ein Element bewegt wird.
- **Steuerbarkeit:** Der Dialogablauf soll über die gesamte Interaktion hinweg gesteuert werden können, bis das Ziel erreicht ist. Beispielsweise kann eine Interaktion abgebrochen und nach einer Pause entschieden werden, ob die Interaktion am Punkt des Abbruchs wieder aufgenommen oder ob sie neu gestartet werden soll.
- **Erwartungskonformität:** Ein Dialog soll den Erwartungen des Benutzers und der Benutzerin entsprechen und mit den Kenntnissen, der Ausbildung und der Erfahrung korrellieren. Zum Beispiel werden Fehlermeldungen immer an derselben Stelle im Fenster angezeigt.
- **Fehlertoleranz:** Kann das Arbeitsergebnis trotz fehlerhafter Eingabe oder Bedienung mit keinem oder geringem Korrekturaufwand erreicht werden, ist ein Dialog als fehlertolerant zu bezeichnen. Beispielsweise kann bei der Eingabe einer Person das Geburtsdatum selektiv geändert werden, ohne dass alle Eingaben neu zu tätigen sind, falls das Geburtsdatum fälschlicherweise in der Zukunft liegt.
- **Individualisierbarkeit:** Individualisierbar ist ein Dialog dann, wenn Anpassungen an die Erfordernisse der Arbeitsaufgabe, der individuellen Vorlieben oder Fähigkeiten getroffen werden können. Ein Beispiel dafür sind barrierefreie Darstellungsmodi für sehbehinderte Benutzer und Benutzerinnen.
- **Lernförderlichkeit:** Um als lernförderlich zu gelten, muss ein Dialog beim Erlernen des Systems unterstützen. In Hilfe-Programmen mit den Dialogen zu experimentieren, ist eine mögliche Hilfestellung.

Die soeben beschriebenen Ideen werden von vielen Unternehmen praktisch umgesetzt. Konkrete Beispiele dafür sind Style Guides wie Apple Inc. (2014b) für das Betriebssystem OS X von Apple, oder Google Inc. (2014a) für das Betriebssystem Android für mobile Endgeräte, die viele Konventionen des Betriebssystems präsentieren und mittels Beispielen und Vorlagen das Gestalten von Software mit hoher Usability vereinfachen.

3.2 Usability Engineering

Der Prozess, der befolgt werden muss, um ein hohes Maß an Benutzbarkeit sicher zu stellen, heißt „Usability Engineering“ . Nielsen definiert diesen Prozess wie folgt:

> *„Usability Engineering is not a one-shot affair where the user interface is fixed up before the release of a product. Rather, usability engineering is a set of activities*

> *that ideally take place throughout the lifecycle of the product, with significant activities happening at the early stages before the user interface has even been designed.“*(Nielsen 1993)

Laut Nielsen ist es wichtig, Usability von Anfang an als Qualitätsmetrik zu beachten. Je später Probleme mit der Benutzbarkeit entdeckt werden, umso teurer wird die Behebung dieser Probleme, vor allem wenn diese Probleme mit fundamentalen Bedienkonzepten verbunden sind. Nielsen empfiehlt daher, bereits lange vor der Implementierungs-Phase eines Produkts mit dem Benutzbarkeits-Prozess zu beginnen. Der Lebenszyklus des Benutzbarkeits-Prozesses nach Nielsen (1992) wird im Folgenden genauer beschrieben.

Usability Lifecycle nach Nielsen

Hier wird der sogenannte „Usability Lifecycle“ beschrieben. So nennt Nielsen die Sammlung an Schritten, die durchlaufen werden müssen, um Usabiltiy Engineering bei einem Softwareentwicklungsprozess zu beachten. Bevor der Prozess durchlaufen wird, ist es notwendig, den Kontext des Produkts zu verstehen, um die fundamentalsten Entscheidungen treffen zu können. Beispielsweise ist bei Software, die über viele Jahre unterstützt und weiterentwickelt werden soll, der Aspekt Rückwärtskompatibilität zu beachten. Die Schritte im „Usability Lifecycle“ sind laut Nielsen (1992) wie folgt definiert.

- **Know the User:** In diesem Schritt werden die zukünftigen Benutzer und Benutzerinnen des Produkts studiert. Dabei werden Eigenheiten, die Arbeitsumgebung, die Aufgabe die durch das Produkt erleichtert werden soll sowie mögliche Entwicklungen der Personen berücksichtigt.
- **Competitive Analysis:** Der Hintergrund für diesen Schritt ist, dass Prototyping ein mächtiges Werkzeug innerhalb der Entwicklung ist. Nachdem am Beginn des Lebenszyklus eines Produkts noch kein Prototyp vorhanden ist, werden Produkte von Mitbewerbern als Prototypen herangezogen. Es können mehrere Produkte miteinander verglichen werden. Ziel dieses Schritts ist keinesfalls, andere Produkte zu kopieren, sondern bereits vor Erstellung eines eigenen Prototypen zu erarbeiten, welche Konzepte Sinn machen und funktionieren und welche zu verbessern sind.
- **Setting Usability Goals:** Hier werden Ziele anhand der fünf eingangs erwähnten Benutzbarkeitsmerkmale definiert. Diese Ziele sollten detaillierter definiert sein als die Merkmale. Zur Evaluierung werden bei jedem Ziel verschiedene Stufen der Erfüllung definiert. Nielsen (1992) unterscheidet dabei vier Erfüllungsstufen.
  - *„worst acceptable level“* der schlechteste noch benutzbare Zustand
  - *„planned usability level“* der geplante Zielzustand
  - *„current level“* der momentan vorhandene Zustand in anderen Produkten
  - *„best possbile level“* die beste erreichbare Stufe
- **Participatory Design:** In dieser Phase soll das Entwicklerteam mit Personen, die das Produkt zukünftig nutzen sollen, zusammenarbeiten. Das hat den Vorteil, dass aufgrund verschiedener Blickwinkel unterschiedliche Fragen gestellt werden. Obwohl von den Benutzern und Benutzerinnen laut Nielsen keine Design-Ideen zu erwarten sind, geben sie rasches Feedback, wenn etwas nicht funktioniert. Diese Phase kann bereits mit *„Mock-Ups“* auf Papier durchgeführt werden.

- **Coordinated Design:** In diesem Schritt ist wichtig, das Design des Produkts über das gesamte Entwicklerteam zu koordinieren. Das Ziel ist, durch eine zentrale Ansprechstelle, konsistentes Design an jeder Stelle des Produkts zu erreichen. Ein Prototyp, an den sich das Entwicklerteam anlehnen kann, ist hilfreich. Weitere Hilfsmittel in diesem Schritt sind, sich an zentral definierte Standards zu halten oder eine *„product identity“*, die auf einer abstrakten Ebene beschreibt, was das Produkt sein soll und welche Funktionen es bietet.
- **Guidelines and heuristic analysis:** Richtlinien helfen dem Entwicklerteam, bekannte Prinzipien zu beachten. Nielsen (1992) definiert drei Arten dieser Richtlinien.
  - *„general guidelines“* allgemeine Richtlinien die auf alle Benutzerschnittstellen zutreffen
  - *„category-specific guidelines“* Richtlinien, die speziell auf diese Kategorie an Schnittstellen zutreffen
  - *„product-specific guidelines“* Richtlinien, die nur für dieses spezielle Produkt zutreffen

  Heuristische Evaluation kann anhand dieser Richtlinien stattfinden, indem jedes Element mit jeder Richtlinie verglichen und in Einklang gebracht wird. Dieser Prozess ist zeitaufwändig, führt jedoch zu sehr konsistentem Design.
- **Prototyping:** Nielsen empfiehlt experimentelles Prototyping für den Beginn des Lebenszyklus. Ein Prototyp ist wesentlich günstiger zu verwerfen als ein fertig entwickeltes Produkt. Die Implementierung soll solange wie möglich hinausgeschoben werden, damit möglichst viele Prototypen getestet und wertvolle Erfahrungen gesammelt werden können.
- **Empirical Testing:** Hier gilt die Maxime, dass jeder Test unter Einbeziehung der Benutzergruppe besser ist als gar kein Test. Es können sich hierbei verschiedene Usability-Probleme zeigen. Diese werden priorisiert und nach Zeit und Aufwand sortiert. Auf verschiedene Testmethoden wird in 3.3 näher eingegangen.
- **Iterative Design:** Nachdem die Tests aus dem vorigen Schritt abgeschlossen sind, ist es notwendig, die durchgeführten Änderungen konsistent in das Gesamtkonzept einfließen zu lassen. Diese Lösungen können neue Probleme verursachen. Weitere Tests und das erneute Durchlaufen verschiedener Schritte im Lebenszyklus sind erforderlich.
- **Collect Feedback:** Nach Fertigstellung des Produkts bietet das Feedback der Benutzer und Benutzerinnen wertvolle Ressourcen für nächste Versionen. Um dieses Feedback zu sammeln, ist es möglich, die Benutzung zu protokollieren oder eine zentrale Anlaufstelle zur Verfügung zu stellen, bei der die Meinung publik gemacht werden kann. Hierbei werden meist Probleme bekannt. Um positive Erfahrungen zu erhalten, ist es notwendig, benutzende Personen direkt zu beobachten und mit ihnen zu sprechen.

Dieser Lebenszyklus gibt dem Entwicklerteam die Möglichkeit, vor dem Design eine genaue Analyse durchzuführen, um im Design- und Entwicklungsprozess Zeit und Geld zu sparen. In 3.1 ist der Lebenszyklus noch einmal aufbereitet.

3.3 Usability Testing

In dieser Arbeit werden die zwei Arten von Usability Testing vorgestellt, die im praktischen Teil Verwendung gefunden haben. In der ersten Variante werden Testpersonen befragt, die bislang

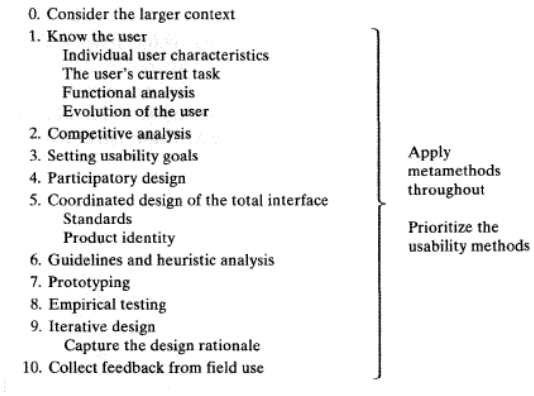


Abbildung 3.1: Usability Lifecycle nach Nielsen, (Nielsen 1992)

keine Erfahrung mit der zu testenden Software hatten. In der zweiten Variante werden Experten und Expertinnen herangezogen, die bereits mit Software in dieser Domäne Erfahrung gesammelt haben. Weitere Usability Testmethoden werden hier nicht erwähnt, um den Rahmen der Arbeit nicht zu sprengen.

3.3.1 Usability Testing mit zukünftigen Benutzern

Eine direkte Art, die Usability von Software zu testen, ist, mit Repräsentanten und Repräsentantinnen der zukünftigen Benutzergruppe Tests durchzuführen. Dabei werden Personen ausgewählt, die der durchschnittlichen Benutzung entsprechen. Die so ausgewählten Personen werden danach mit vordefinierten Arbeitsaufträgen mit der Software vertraut gemacht. Die Testpersonen haben im Idealzustand das zu testende Produkt betreffend dieselben Vorerfahrungen. Vor dem Test erhalten sie dieselben Informationen, die sachlich vorgetragen werden. Das bewirkt, dass die Voraussetzungen für jede Person möglichst gleich sind. Für erfolgreiche Tests ist eine geringe Anzahl an Testpersonen ausreichend, da die Ergebnisse redundant sind. Nach Nielsen (2000) reichen 5 Testpersonen für die Identifizierung der meisten Usability-Probleme aus.

In Rubin (1994) werden vier verschieden Arten an Usablity Tests unterschieden:

Exploratory Tests

Diese Tests werden früh im Zyklus der Produktherstellung durchgeführt. In dieser Phase existieren keine Implementierungen, sondern erste Ideen und grobe Konzepte über die Funktionalität der Software. Dementsprechend werden die Tests mit Mock-Ups, Prototypen oder handgeschriebenen Masken durchgeführt, um herauszufinden, ob die Ideen sinnvoll erscheinen. Diese Tests sind durch ihre Freiheit von technischen Beschränkungen kreativ und spontan. Es ist zum Beispiel möglich, das Interface sehr rasch umzubauen, um die Effekte von Änderungen, die die Testperson vorgeschlagen hat, direkt beobachten zu können. Die Interaktion mit dem Testmonitor - die Person, die den Test anleitet - ist bei dieser Testart stark ausgeprägt.

Assessment Tests

Dies ist die am häufigsten durchgeführte Art von Usability Tests. Sie wird früh im Lebenszyklus der Produktherstellung durchgeführt. Es werden erste Implementierungen getestet und be-

reits komplette Aufgaben durchgeführt. Ziel dieses Tests ist Detailaufgaben durch den Benutzer und die Benutzerin lösen zu lassen, um Usability-Probleme frühzeitig erkennen zu können.

Validation Tests

Das Ziel liegt darin, einen bestehenden Standard an Usability zu bestätigen. Beispielsweise wird ein vordefinierter Arbeitsablauf in einer neuen Version einer Software überprüft. Das Ziel des bestätigenden Tests ist, zu erfahren, ob der Arbeitsablauf in derselben Zeit und mit gleich vielen oder weniger Fehlern durchgeführt wird. Bei der ersten Version einer Software werden hier die Benchmarks für weitere Versionen erstellt, die später getroffen oder unterboten werden sollen. Bei dieser Testvariante interagiert die Testleitung kaum mit den Testpersonen.

Comparison Tests

Dieser Test kann jederzeit im Produktzyklus sowie in Verbindung mit den anderen drei Testvarianten angewendet werden. Mit ihm werden zwei oder mehrere Ausführungen einer Software miteinander verglichen. Mit starren, statistischen Vorgaben, etwa wenn eine Dimension des Produkts zwischen Test- und Kontrollgruppe variiert, kann diese Variante signifikante Ergebnisse liefern. Ein Beispiel dafür ist, dass ein Buchhaltungssystem in zwei Versionen getestet wird, wobei der einzige Unterschied die Sortierung der Einträge - einmal alphabetisch, einmal nach dem Datum - ist. Es ist möglich, einen vergleichenden Test weniger formal als bei bisher beschriebenen Testarten durchzuführen, indem Feedback der Testpersonen eingeholt wird. Dabei werden keine Leistungsdaten erhoben und verglichen. In Rubin (1994) wird vorgeschlagen, bei informellen Tests unterschiedliche Designs zur Verfügung zu stellen. Das Feedback der Testpersonen kann damit wertvoll ausfallen. Begründet wird dies mit der notwendigen Kreativität des Design-Teams, das mehr Ideen sammeln und umsetzen muss, um mehrere Möglichkeiten zur Auswahl zu stellen, sowie der Herausforderung für die Testperson, zu erklären, warum ihr diese Möglichkeit besser gefällt als alle anderen.

3.3.2 Expert Review

Bei dieser Technik wird die Software von Experten und Expertinnen begutachtet und überprüft. Das hat die Vorteile, dass weniger Ressourcen benötigt werden, die Tests schneller von statten gehen und früher Ergebnisse vorliegen. Dabei werden konzeptuelle Probleme gefunden. Fehler bei der Verwendung werden kaum gefunden. Es ist möglich, dass „falscher Alarm“ ausgelöst wird, weil durch den eingeschränkten Blick auf die Software, Probleme erkannt werden, die keine Relevanz haben. Aus diesen Gründen sollten Expert Reviews zusätzlich zu anderen Usability Tests durchgeführt werden.

3.3.3 Weitere Aspekte für Usability Tests

Zum Abschluss werden einige Techniken vorgestellt, die bei jedem Usability Test eingesetzt werden können.

Testmethodik - Thinking Aloud

Die Testperson wird gebeten, jede Handlung und jeden Gedanken deutlich zu verbalisieren. Dadurch erhält die Testleitung Feedback darüber, was die Testpersonen über das Design denken,

welche Missverständnisse auftreten und wie Handlungsabläufe sinnvoller gestaltet werden können. Es handelt sich um eine flexible Technik, die schnell und einfach verwertbare Ergebnisse liefert. Die Testleitung muss gute Kommunikationsskills aufweisen, nachdem diese Technik bei vielen Menschen als ungewohnt wahrgenommen wird. Außerdem ist es notwendig, die Testpersonen am Reden zu halten, damit der Output nicht durch Filter läuft, die die Testpersonen aufstellen um intelligent oder höflich zu erscheinen. Es ist notwendig, die Ergebnisse vertraulich zu behandeln und es sollte den Testpersonen erlaubt sein, den Test jederzeit zu beenden, wenn sie sich unwohl fühlen. (C. Lewis und Rieman (1994))

Studiendesign - Withing und Between Subjects Testing

Bei der Variante Within Subjects handelt es sich um einen Usability Test, bei dem jede Testperson alle Testfälle bearbeitet. Diese Testmethode hat den Vorteil, dass weniger Testpersonen benötigt werden, um alle Testfälle abzudecken. Allerdings ist zu bedenken, dass bei einander ähnelnden Testfällen Lerneffekte eintreten, denen entgegengewirkt werden muss (Jackson 2012). Wenn eine Testperson mit einem Softwaresystem noch keine Erfahrung hat, ist es wahrscheinlich, dass die erste Aufgabe, die diese Testperson lösen muss lange dauert. Das liegt daran, dass die Person sich erst an das neue System gewöhnen muss. Im Gegenzug werden weitere Aufgaben signifikant schneller erledigt. Damit diese Zeit nicht jedes Mal bei derselben Aufgabe in die Statistik einfließt, ist es möglich die Testaufgaben über diese Technik auszubalancieren. Das lässt sich beispielsweise mit einem Latin Square bewerkstelligen, in dem jede Testperson mit einem anderen Testfall beginnt und auch weitere Testfälle in unterschiedlicher Reihenfolge bearbeiten muss. Dadurch wird der Lerneffekt auf alle Testaufgaben verteilt. Ein praktisches Beispiel dazu findet sich in Abbildung 5.1.
Bei der Variante Between Subjects handelt es sich um einen Usability Test, bei dem jede Testperson nur einen einzigen Testfall bearbeitet. Hier ist Counterbalancing nicht notwendig, da keine Lerneffekte auftreten können. Ein Nachteil gegenüber Within Subjects Tests ist allerdings, dass mehr Testpersonen notwendig sind, was den Testaufwand und den notwendigen Verwaltungsaufwand erhöht.

Messskala - System Usability Scale

In Brooke (1996b) wird geschrieben, dass Usability nie absolut gemessen werden kann. Es muss der Kontext in die Skala miteingerechnet werden. Daher wird in Brooke (1996b) eine Skala vorgestellt, die diese Aufgabe lösen kann. In J. R. Lewis und Sauro (2009) wird die Skala erfolgreich auf Valididtät getestet. In dieser Skala werden Parameter, wie die Effektivität, die Effizienz und die Zufriedenheit des Benutzers und der Benutzerin beim Erledigen verschiedener Aufgaben gemessen. Die System Usability Scale (SUS) ist dazu geeignet, eine normierte Messung über Usability durchzuführen. Die klassische SUS besteht aus zehn Fragen, einige positiv, einige negativ formuliert. Die Fragen sind anhand einer Likert-Skala zu beantworten. Der in Brooke (1996b) vorgeschlagene Bewertungsmechanismus ergibt durch Gewichtung ein Gesamtergebnis von 0-100, wobei 100 das Optimum darstellt. Es handelt sich hierbei nicht um eine klassische Prozentangabe. Um repräsentative Ergebnisse zu erhalten, ist es notwendig, die Skala als Perzentil-Skala zu betrachten. Ab 68 Punkten wird von verwendbarer Software gesprochen, bis hin zu bestmöglich benutzbarer Software bei 100. Die Grafik in 3.2 veranschaulicht diesen Umstand und gibt Beispiele für verschiedene Interpretationen der SUS.

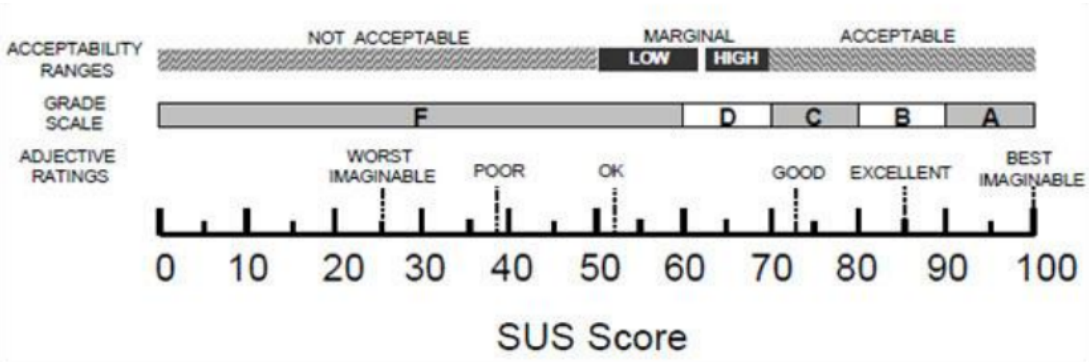


Abbildung 3.2: Scoreboard für die SUS, (Brooke 2013)

3.4 Security

In diesem Abschnitt wird kurz über das Thema Security gesprochen. Im Softwarebereich gibt es klar definierte Prozesse, die Sicherheit für die nutzenden Personen oder die benutzten Daten sicherstellen sollen. Im Zusammenhang mit dem Schließmechanismus, der in Folge analysiert wird, ist besonders der Prozess, in dem festgestellt wird, ob jemand das Recht hat, eine Ressource zu benutzen, interessant. Dieser Prozess heißt „Authentifizierung“ . Hierbei gibt es drei Möglichkeiten, um sich zu identifizieren (Renaud 2005):

- Was ein Benutzer oder eine Benutzerin ist: Hierbei handelt es sich um das Feld der Biometrik. Die Authentifzierung erfolgt per Fingerabdruck, Iris-Scan oder Stimmmodulation. Hand- und Fingergeometrie sowie Gesichtserkennung sind ebenfalls mögliche Charakteristika. Experimentellere Ansätze sind beispielsweise das Authentifizieren anhand der Verwendung der Tastatur oder auch die Art wie bestimmte Wörter getippt werden. (Coventry 2005)

- Was ein Benutzer oder eine Benutzerin kann oder erkennt: Hierbei handelt es sich um das Feld der Mnemometrik. Die Authentifizierung erfolgt mit einem klassischen Passwort. Als Passwörter werden, wenn sie beliebig gewählt werden dürfen, in den meisten Fällen unsichere Zeichenfolgen gewählt (McCue 2014). Werden kulturelle Passwörter verwendet, steigt die Sicherheit durch die erhöhte Zahl der Passwörter, die eingegeben werden müssen. Hier ist mit Designproblemen zu rechnen, wie beispielsweise der Umgang mit Groß- und Kleinschreibung, Tippfehlern etc. gehandhabt wird (Just 2005)
  Sicher und benutzbar sind sogenannte grafische Passwörter (Jermyn u. a. 1999). Es wird ein Bild präsentiert und es sind bestimmte Ausschnitte anzuklicken, die vorab vereinbart wurden.

- Was ein Benutzer oder eine Benutzerin besitzt: Zur Identifizierung wird im Regelfall ein physisches Objekt benötigt. Es kann sich um eine Schlüsselkarte oder um ein USB-Laufwerk mit kryptografischen Daten handeln.

Usability von Security Devices erhöhen

Piazzalunga, Salvaneschi und Coffetti (2005) empfehlen mehrere Maßnahmen, um mobile Security Devices benutzbarer zu machen und die Akzeptanz bei Benutzern und Benutzerinnen zu erhöhen. Ein Punkt, auf den eingegangen wird, ist, das gesamte System zu betrachten und sowohl

die technischen als auch die menschlichen Faktoren zu berücksichtigen. Wird ein eigenes Lesegerät für Security Devices benötigt, so beeinträchtigt das die Mobilität der nutzenden Personen. Dies ist, wenn möglich, zu vermeiden. Wichtig ist auch, den Devices zusätzlichen Wert zu verleihen. Beispielsweise kann das Device als Schlüsselanhänger gestaltet werden. Dadurch beginnt ein Prozess, der Security Devices an Objekte knüpft, die jemand bereits bei sich trägt. Ein Beispiel dafür ist die Implementierung von NFC auf aktuellen Smartphones. Diese Technologie kann auch zum Sperren von Schlössern verwendet werden.

4 Trust

Trust me. I know what I'm doing.
Sledge Hammer

In diesem Kapitel wird das Thema Trust behandelt. Folgende Themen werden bearbeitet:

- Trust wird definiert.
- Es wird auf den Zusammenhang zwischen Trust und Technologien eingegangen.
- Es werden verschiedene Möglichkeiten vorgestellt, um Trust zu messen.
- Es wird mit der Interpersonal Trust Scale (ITS) ein Fragebogen vorgestellt, der das Vertrauen der Befragten zu einem bestimmten Thema messen soll.
- Abschließend wird ein Experiment präsentiert, mit dem Vertrauen von Personen in verschiedene Schließmechanismen erhoben wird.

4.1 Begriffsdefinition

Das *Merriam-Webster's English Dictionary Trust* (2014) definiert das Wort „Trust"als:

> *assured reliance on the character, ability, strength, or truth of someone or something*

Es handelt sich demnach um das Vertrauen in das Verhalten von etwas oder jemandem. Es gibt drei Kerncharakteristiken von Trust, die in Wade und Robinson (2012) beschrieben werden.

- Trust auf Basis von Fähigkeiten: Bei dieser Art des Trust geht die vertrauende Person davon aus, dass eine vertraute Person Fähigkeiten besitzt, ein Verhalten so auszuführen, wie die vertrauende Person es sich erwartet. Ein Beispiel dafür ist das Vertrauen in eine Polizistin, die, unabhängig davon, ob sie ein bekannter oder ein unbekannter Mensch ist, gewisse Fähigkeiten besitzen muss, um die soziale Ordnung aufrecht zu erhalten.
- Trust auf Basis von Wohlwollen: Bei dieser Art des Trust geht die vertrauende Person anhand einer emotionalen Bindung zu der vertrauten Person davon aus, dass diese sich gemäß ihrer Erwartungen verhalten wird. Ein Beispiel dafür ist das Vertrauen eines Kindes in seine Eltern, dass sie es nicht hilflos zurücklassen werden.
- Trust auf Basis von Integrität: Diese Art des Trust wird durch das Verhalten einer vertrauten Person anhand sozialer Normen sowie ethischer und moralischer Prinzipien gebildet. Ein Beispiel dafür ist Ehrlichkeit in der Kommunikation.

Trust ist immer mit Risiko verbunden. Ohne Risiko kann es keinen Trust geben, da Vertrauen ohne die Gefahr von Verlust keinen Wert besitzt (Luhmann 1979). In Sasse (2005) wird geschrieben, dass es früher selten war, einen Menschen zu treffen, den man noch nie gesehen hatte. Heutzutage passiert das häufiger und es wird einfacher. Multiplayer Spiele im Internet, elektronische Marktplätze wie eBay oder auch in Chat Foren, der Kontakt zu fremden Menschen gestaltet sich einfacher als früher.

Die einfachste Situation in der Trust greift, beinhält zwei Aktoren, den Trustor (der oder die Vertrauende) und den Trustee (der oder die Vertraute). Im Folgenden werden im Sinne der Lesbarkeit die englischen Begriffe verwendet. Beide haben etwas aus dem gemeinsamen Kontakt zu gewinnen, entweder Geld, Information oder Güter. Online haben die Aktoren übereinander weniger Informationen, weil sie sich nicht am selben Ort befinden und einander nicht sehen können. Daher sind Online-Interaktionen riskanter einzustufen als Interaktionen in der realen Welt. Damit diese Kontakte funktionieren können, ist es notwendig, dass der Trustor sowohl dem Trustee vertraut als auch der Technologie, die zwischen den beiden vermittelt. Diese Tatsache, in Verbindung mit den Kerncharakteristiken von Trust, die nur von einem Menschen mit freiem Willen wahrgenommen werden können, ergibt eine dritte Partei, der in einer Online-Interaktion vertraut werden muss: dem Erstellerteam der Technologie, die zur Kommunikation genutzt wird. Da eine Maschine oder Technologie keinen freien Willen besitzt, sondern nur den Willen des Erstellerteams implementiert, ist dieses als dritte Partei zu beachten. Daraus ergeben sich zwei weitere Szenarien:

1. Die dritte Partei ist von einem oder beiden Aktoren als prinzipiell nicht vertrauenswürdig einzustufen. In diesem Fall wird sie in die gegenseitige Trustbewertung der Aktoren mit einbezogen.
2. Die dritte Partei ist von beiden Aktoren als vertrauenswürdig einzustufen. In diesem Fall kann sie ignoriert werden.

In Sasse (2005) werden mehrere Faktoren identifiziert, die bei Trustor und Trustee Trust erzeugen:

- Die Anzahl bereits durchgeführten Transaktionen mit diesem Trustee: Haben bereits viele andere Aktoren in einer ähnlichen Transaktion vertraut und wurde dieses Vertrauen nicht missbraucht, baut das Trust auf.
- Die Art der Aktoren und ihre Reputation: Handelt es sich um Aktoren der Regierung, um Händler oder Händlerinnen in einem Online-Shop oder um einzelne, unbekannte Individuen? Die Reputation kann auch abhängig vom Trustor variieren, ein Trustor vertraut der Regierung sehr stark, während ein anderer möglicherweise keinerlei Vetrauen zur Regierung hegt.
- Ob die Kommunikation zwischen den Parteien synchron, also mit sofortiger Antwort des Trustees oder asynchron, mit Wartezeit zwischen Abfrage und Antwort, abläuft: Synchrone Kommunikation erzeugt eher Trust als asynchrone.
- Kann der Trustor vertrauenswürdige Eigenschaften identifizieren?
- Die verschiedenen Signale und Kommunikationskanäle, die der Trustee verwendet, um Vertrauenswürdigkeit zu kommunizieren: Hierbei kann es sich um Verschlüsselungen bei Online-Interaktionen oder ein Treuhandservice bei der Bezahlung handeln. Außerdem ist eine Unterscheidung der Trust-Bewertung zwischen den Signalen einer Person und eines Unternehmens möglich.

- Empfehlungen (Recommendations) von Bekannten, Freunden oder Freundinnen des Trustors beeinflussen den Trust. Zertifikate und Beurteilungen von neutralen Dritten helfen ebenfalls beim Aufbau von Glaubwürdigkeit (Credibility) des Trustees.
- Die generelle Disposition des Trustor zu vertrauen.
- Das Wissen des Trustor über die Situation, in der Vertrauen notwendig ist.
- Die vorangegangene Erfahrung des Trustor: Wurde diesem Trustee bereits erfolgreich vertraut, oder wurde in ähnlichen Situationen bereits erfolgreich vertraut führt das zu hohem Trust.
- Die möglichen Vorteile, die der Trustor aus der Interaktion zu erwarten hat.
- Das eigentliche Risiko, dass der Trustor trägt.

4.2 Trust messbar machen

In diesem Abschnitt sollen mit der ITS und dem TAM Metriken vorgestellt werden, die Trust messbar und vergleichbar machen.

4.2.1 ITS

In Rotter (1967) findet sich der erste Vorschlag für die Messung von Trust. Hier wird das Augenmerk sehr auf die Trust Propensity, die prinzipielle Bereitschaft einem Menschen zu vertrauen gelegt. Als Beispiel nennt Rotter das Vertrauen in Respektpersonen, wie Lehrer und Lehrerinnen, Bürgermeister und Bürgermeisterinnen oder Geistliche, das aufgrund von Verhalten in der Familie automatisch entsteht. Ein Entwurf für eine Skala wird wie folgt vorgeschlagen:

- Die ITS ist eine Likert-Skala. Die Fragen sind mit Werten von 1-5 zu beantworten. 1 steht dabei für starke Zustimmung, 5 für starke Ablehnung.
- Sie ist als additive Skala konzipiert, ein hoher Gesamtwert als Ergebnis bedeutet viel Trust.
- Sie besteht aus spezifischen Fragen, generellen Fragen die die Disposition der befragten Person zur Gesellschaft allgemein hinterfragen sowie einigen Füllfragen. Letztere haben den Sinn, die Absichten der Skala zu verschleiern und somit ehrlichere Antworten zu bewirken.
- Die Fragen sind so konzipiert, dass etwa die Hälfte aller Antworten bei Zustimmung, die andere Hälfte bei Nichtzustimmung Trust bedeuten.

Fragen der ITS sind beispielsweise „Sind Sie der Meinung, dass Sie [Software] ohne Unterstützung durch eine technisch versierte Person benutzen könnten?“ oder „Haben Sie sich während der Benutzung von [Software] sicher und souverän gefühlt?“

4.2.2 Trust im TAM

Eine weitere Möglichkeit, Trust zu messen, findet sich im TAM. Dieses Modell wurde in F. D. Davis (1989) erstmals vorgestellt und seitdem weiter verfeinert und angepasst. Mittels dieses Modells lassen sich Voraussagen über das Verhalten von Benutzern und Benutzerinnen treffen, die mit neuen Technologien konfrontiert werden. Es basiert auf der Theory of Reasoned Action (TRA),

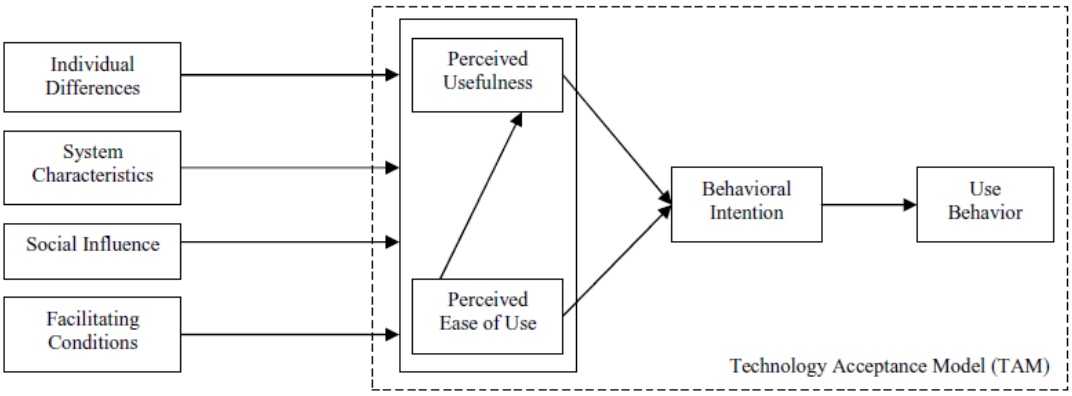


Abbildung 4.1: Technology Acceptance Model, (Venkatesh, G. Davis und F. Davis 2003)

die in Fishbein und Ajzen (1975) publiziert ist. Bei der TRA wird ein Modell vorgestellt, in der die persönlichen Einstellungen einer Testperson und das von der Allgemeinheit erwartete Verhalten verknüpft werden, um so das erwartete Verhalten der Testperson vorherzusagen. Eine Übersichtsgrafik zum TAM findet sich in Abb. 4.1. In TAM sind folgende Faktoren für die Akzeptanz einer Technologie verantwortlich:

- Externe Variablen
- Die wahrgenommene Nutzbarkeit Perceived Usefulness (PU)
- Die wahrgenommene Einfachheit der Benutzung Perceived Ease of Use (PEOU)

Zu diesen Faktoren werden bei der Anwendung des TAM jeweils Hypothesen aufgestellt, die mittels eines Fragebogens und einer Likert-Skala überprüft bzw. widerlegt werden sollen. Diese Hypothesen werden mittels des Cronbach-Alpha-Tests auf ihre Stabilität und Konsistenz überprüft. Hier ist wieder auf unterschiedliche (positive und negative) Formulierung der Fragen zu achten. Das Ergebnis der Befragung lässt auf die Intention des Benutzers oder der Benutzerin ein System zu benutzen sowie die wirkliche Benutzung schließen. Bis zu 40% der Varianz zwischen Intention und Benutzung lassen sich durch dieses Modell erklären (F. D. Davis 1989).

Erweiterungen zum TAM

Seit der Entwicklung der ersten Version des TAM wurde dieses Modell auf mehrere Arten weiterentwickelt.

TAM2

Hierbei wird das TAM um die folgenden fünf Konstrukte erweitert, die Einfluss auf die Kenngröße PU haben.

- Die Relevanz für die Arbeit: Wie verwendbar das getestete System für die tägliche Arbeit der Testperson erscheint. (Venkatesh und F. D. Davis 2000)
- Die Qualität des Ergebnisses: Wie korrekt das Ergebnis des Systems für die Testperson erscheint. (Venkatesh und F. D. Davis 2000)

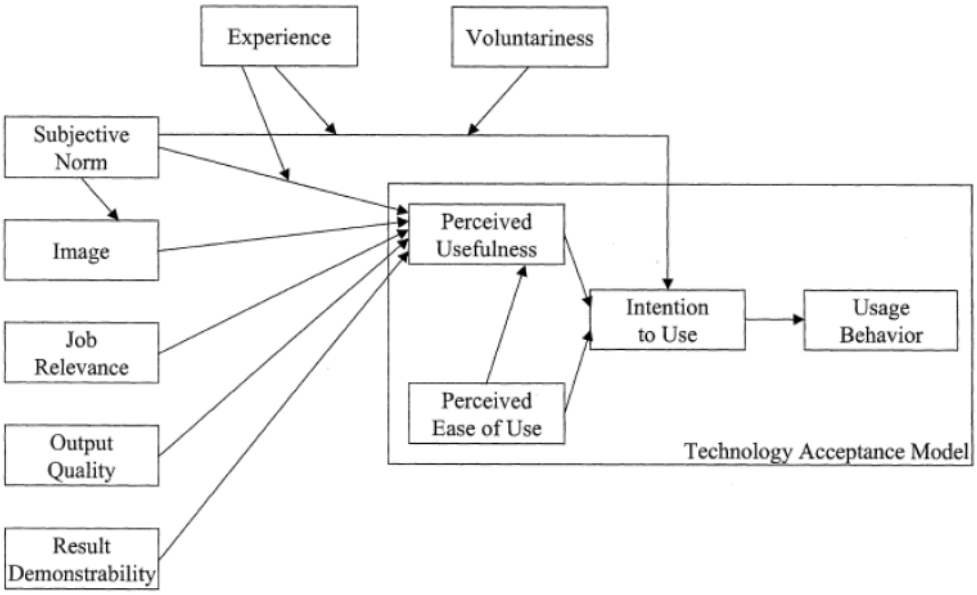


Abbildung 4.2: TAM2, (Venkatesh, G. Davis und F. Davis 2003)

- Die Demonstrierbarkeit des Ergebnisses: Wie greifbar und beobachtbar das Ergebnis für die Testperson erscheint. (Moore und Benbasat 1991)
- Das Ansehen der Technologie: Welche Statusveränderungen im sozialen System der Testperson durch die Verwendung des Systems erwartet werden. (Moore und Benbasat 1991)
- Die Subjektive Norm: Wie stark fühlt sich die Testperson dazu veranlasst, das System zu verwenden, weil Leute die ihr wichtig sind das von ihr erwarten. (Fishbein und Ajzen 1975), (Venkatesh und F. D. Davis 2000)

Zusätzlich wird noch die Freiwilligkeit der Verwendung und die Erfahrung als „moderierend“ angenommen. Die Erfahrung wird als unterstützender Faktor für die beeinflussten Messgrößen in das Ergebnis mit einberechnet, die Freiwilligkeit als nicht unterstützender Faktor. Ein konkretes Beispiel dafür lautet: Je mehr Erfahrung die Testperson mit dem getesteten System (oder ähnlichen Systemen) hat, umso weniger Gewicht wird die Testperson auf die PU legen. Dieses Modell (visualisiert in Abb. 4.2) ist durch die verfeinerte Auflösung der abgefragten Faktoren in der Lage, die angenommene Akzeptanz noch genauer vorherzusagen als das bisherige Modell (Venkatesh und F. D. Davis 2000),(Venkatesh, G. Davis und F. Davis 2003).

TAM3

Venkatesh und Bala (2008) stellt eine erneute Erweiterung des TAM vor (siehe Abb. 4.3). Es werden sechs neue Einflussgrößen auf die PEOU eingeführt. Anders als beim Vorgänger TAM2 wird hier angenommen, dass die Erfahrung der Testperson wesentlich stärkeren Einfluss auf das Gesamtergebnis hat. Konkret handelt es sich hierbei um die Achsen **Computerfurcht - PEOU**, **PEOU - PU** und **PEOU - Verhaltenspsychologische Intention**, die durch die Erfahrung beeinflusst werden. Bei den neuen Einflussgrößen handelt es sich um:

- Die Selbstwirksamkeit der Testpersonen in Bezug auf Computer: Wie gut schätzt der Befragte seine Fähigkeiten ein, eine bestimmte Aufgabe an einem Computer durchzuführen. (Compeau und Higgins 1995).

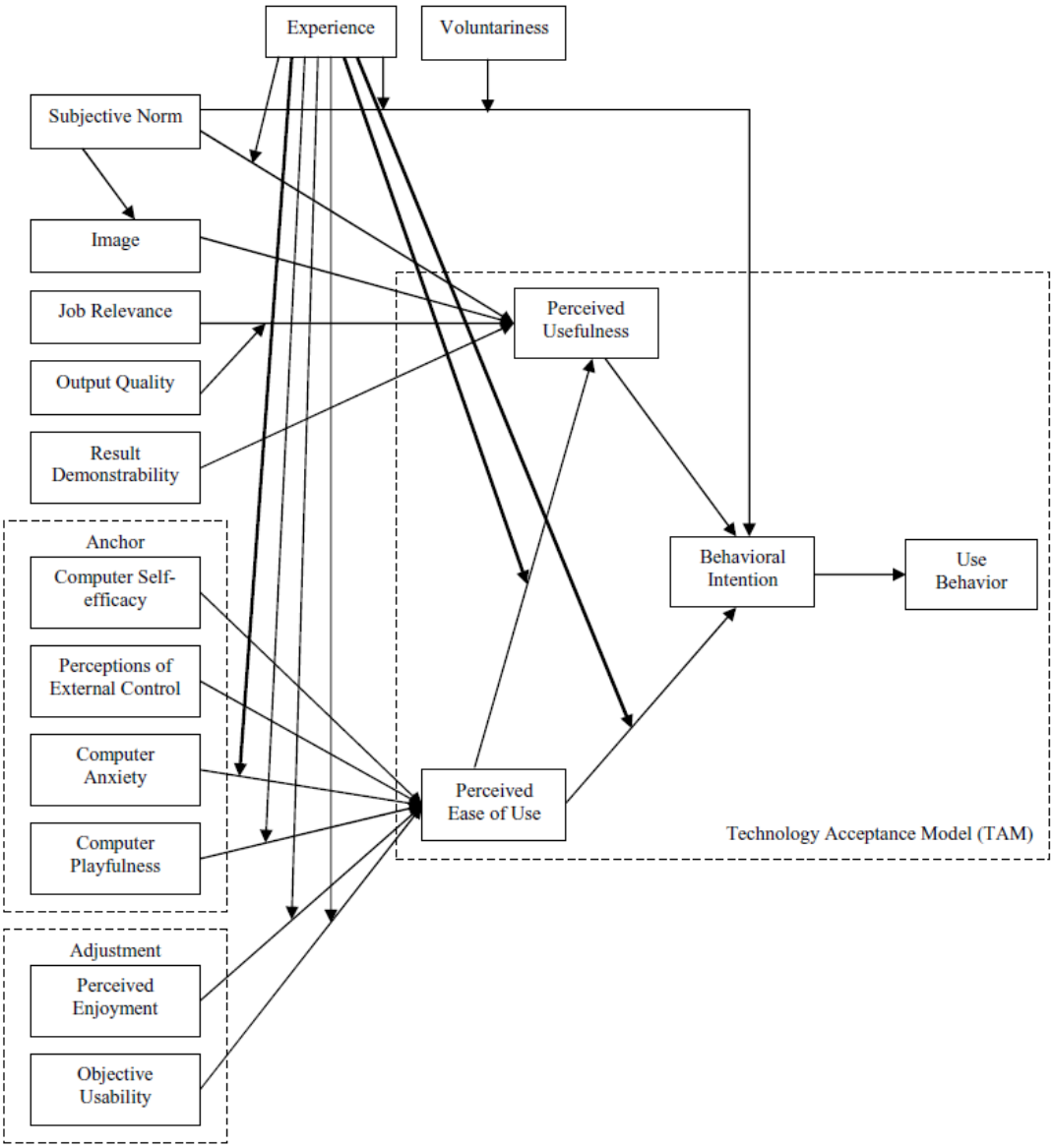


Abbildung 4.3: TAM3, (Venkatesh und Bala 2008)

- Der Spieltrieb in Bezug auf Computer: Wie spontan ist die Testperson in der Interaktion mit Computern. (Webster und Martocchio 1992)
- Die objektive Verwendbarkeit: Wie verhält sich der Aufwand im neuen System zu dem Aufwand in bisherigen Systemen. (Venkatesh und F. D. Davis 2000)
- Die Furcht vor Computern: Wie stark ist die Furchtreaktion der Testperson, wenn er Computer benutzen muss. (Venkatesh und F. D. Davis 2000)
- Die Wahrnehmung von externer Kontrolle: Wie sehr glaubt die Testperson daran, dass externe Ressourcen existieren, um die Benutzung des Systems zu unterstützen, beispielsweise Schulungen die vom Arbeitgeber organisiert und vom Systemersteller gehalten werden. (Venkatesh, G. Davis und F. Davis 2003)
- Die wahrgenommene Unterhaltung: Wie sehr wird die Aktivität an sich als unterhaltsam wahrgenommen, ungeachtet des Nutzens. (Venkatesh und F. D. Davis 2000)

Mittels der neuen Parameter ist das TAM3 in der Lage zwischen 31% und 36% der Varianz in der Benutzung zu erklären.

Kontextabhängige Erweiterungen

In Mohamed u. a. (2011) wird eine Erweiterung des TAM für die Domäne e-Health vorgeschlagen (siehe 4.4). Es handelt sich hierbei um eine Studie, die im Vereinigten Königreich und den Vereinigten arabischen Emiraten durchgeführt wurde. Aus diesem Grund wurden Untersuchungen aus Hofstede (1984) und Hofstede (2001) berücksichtigt, die vorschlagen, sozio-kulturelle Dimensionen bei der Untersuchung der Akzeptanz von e-Health Diensten zu berücksichtigen. Es wird das TAM um kontextabhängige Determinanten erweitert. In diesem konkreten Fall handelt es sich um die PC Kenntnisse der Testpersonen, die Konkretheit der verwendeten Begriffe und Symbole, der Trust, die Vermeidung von Unklarheiten und die Männlichkeit. Die Verlässlichkeit dieser Studie ist mittels Cronbach Alpha auf einen Koeffizienten von 0.651 getestet worden und ist somit akzeptabel.

Eine ähnliche Erweiterung des TAM findet sich in Kaasinen (2007). Hier wird das TAM for Mobile Services (TAMM) vorgestellt (siehe 4.5. In diesem Modell werden die Beziehungen **Trust - Nutzungsintention** und **Wahrgenommene Einfachheit der Technologie - eigentliche Benutzung** zum TAM hinzugefügt. Kaasinen (2007) defniert die zwei Faktoren wie folgt:

> **Trust**: *„The User should be able to rely on the overall service - The accuracy of information provided such as location or other context data should be sufficient for the kinds of tasks for which the user will be using the service - The privacy of the user must be protected - The user needs to feel and really be in control“*
> **Wahrgenommene Einfachheit der Technologie**: *„Actual values of the service need to be emphasized - Disposable Services for occasional needs - The service has to support evolving usage cultures“*

Das TAM ist ein flexibles Werkzeug, das um viele Faktoren erweitert werden kann. Es ist denkbar, das TAM um die Dimension des Trust zu erweitern. Eine derartige Erweiterung ist nicht Teil dieser Arbeit.

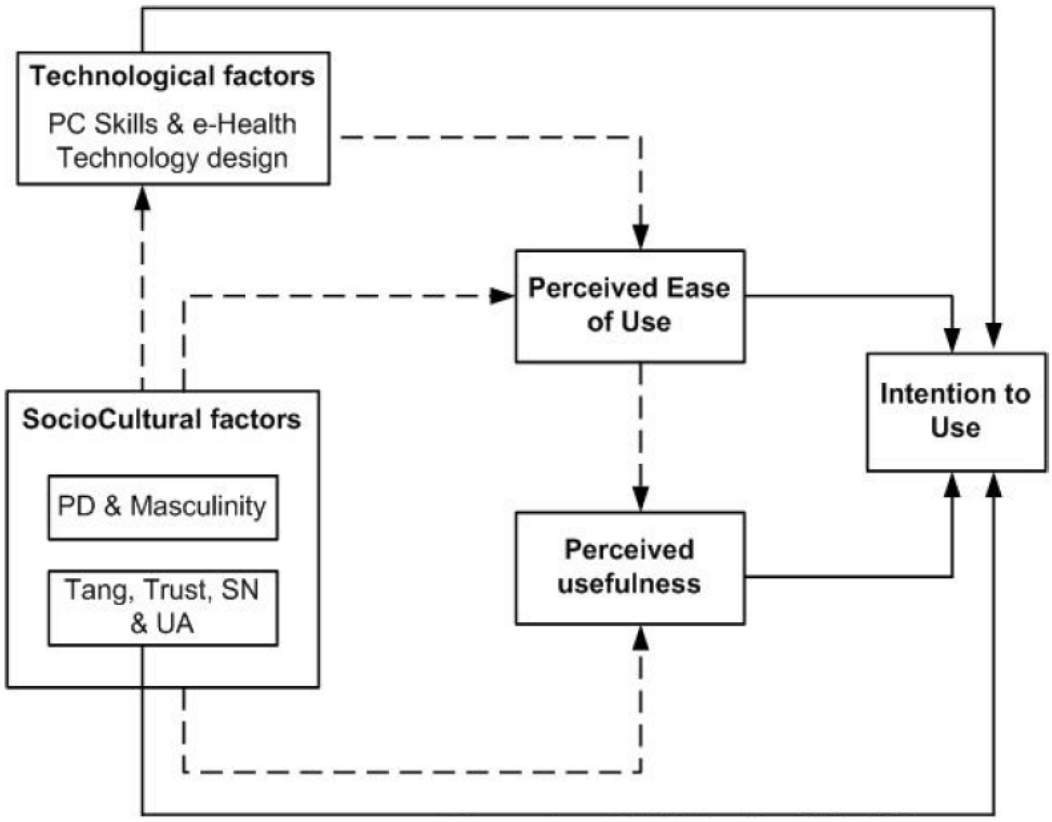


Abbildung 4.4: TAM adaptiert für die Domäne e-Health, (Mohamed u. a. 2011)

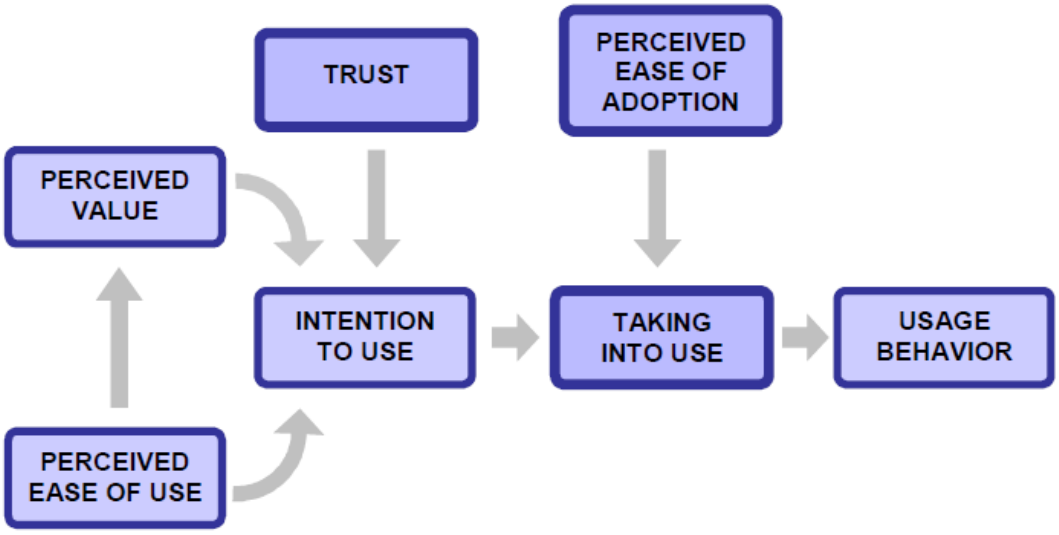


Abbildung 4.5: TAM for Mobile Services, (Kaasinen 2007)

Abbildung 4.6: Bild Bristol Lokativ (Kindberg u. a. 2008)

4.2.3 Symbole, die Trust erzeugen

Vertrauen ist ein subjektiver Faktor (Sasse 2005). In Sasse (2005) wird ebenfalls beschrieben, dass frühere Erfahrungen und identifizierbare Symbole zum generellen Vertrauen beitragen können. In Kindberg u. a. (2008) wird demonstriert, wie Symbolik das Vertrauen von Benutzern und Benutzerinnen beeinflussen kann. Der Versuchsaufbau besteht aus einem WiFi Hotspot an zwei Orten (in Bristol respektive London), der schnellen, kabellosen Zugang zum Internet zur Verfügung stellt. Dieser Hotspot ist mit einem Server verbunden, der jeder Testperson, der die Verbindung nutzen möchte, einen Startbildschirm präsentiert. Auf diesem Startbildschirm wird die Testperson gebeten, seine Mobiltelefonnummer einzugeben. Daraufhin wird von einem Telefon, das mit dem Server verbunden ist, eine PIN an die eben eingegebene Nummer gesendet, der wiederum einzugeben ist. Weiters wird das Bild, das auf dem Startbildschirm zu sehen ist, aus verschiedenen möglichen Bildern ausgewählt. Die möglichen Kombinationen sind dabei „*London - Bild aus Bristol* (anti-lokativ)“, „*London - neutrales Bild* (a-lokativ)“, „*Bristol - neutrales Bild* (a-lokativ, Abb. 4.7)“ und „*Bristol - Bild aus Bristol* (lokativ, Abb. 4.6)“. Das Ziel des Experiments ist, herauszufinden, ob die Lokativität des Bildes einen Einfluss auf das Vertrauen der Testpersonen hat.

Die Ergebnisse des Experiments lassen darauf schließen, dass anti-lokative Hinweise eher dazu führen, dass Testpersonen weniger vertrauen. A-lokative und lokative Hinweise weisen keine signifkanten Unterschiede in dem Vertrauen der Testpersonen auf. Die Autoren der Studie sind sich der Tatsache bewusst, dass es für weitere Studien notwendig ist dass die Testpersonen zielgerichteter ausgewählt werden sollen, weitere Studien zu den Unterschieden zwischen lokativem, anti-lokativem und a-lokativem Inhalt angestellt werden müssen und Bilder ausgewählt werden müssen, die auf wissenschaftlich akzeptierte Art und Weise besser getestet und verglichen werden können (Kindberg u. a. 2008).

Eine weitere Studie zu diesem Thema findet sich in Silver (2013). Hier wurden im September 2013 mehr als 5000 Personen aus den USA und Kanada befragt, ob und auf welche Symbole sie bei einem Einkauf im Internet achten. Dabei haben 91% angegeben, auf irgendeine Art nach Symbolen zu suchen, die bei ihnen Vertrauen auslösen. Ein Beispiel für solche Symbole ist die *Verified by Visa* Eingabemaske. Hierbei handelt es sich um eine Maske, die von VISA bereitgestellt wird. Dabei ist die Zahlungsmaske immer in einem einheitlichen Design, es verändern sich nur die Informationen in Bezug auf den Online-Shop, den Betrag und den Preis. Weiters ist eine Nachricht abgebildet, die nur der Benutzer oder die Benutzerin und VISA kennen kann, um Phishing Angriffe zu verhindern.

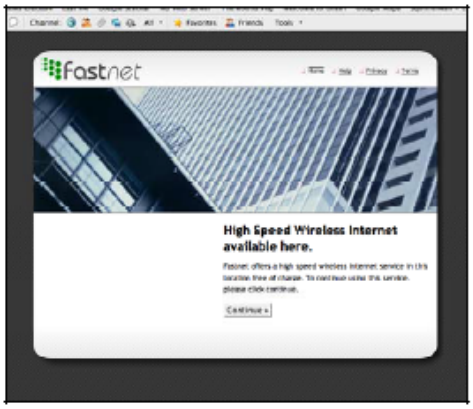


Abbildung 4.7: Bild Bristol A-Lokativ (Kindberg u. a. 2008)

> *„Verified by Visa not only protects your card against unauthorised use, it also means you can have confidence that the online retailer you're buying from has made your security a priority.“* (Visa Europe 2014)

Es lässt sich also Einfluss von Symbolen auf das Vertrauen aus diesen Arbeiten ableiten. Es ist hierbei aber anzumerken, dass der Kontext in diesem Fall die Kreditkartenzahlung bei einem Bestellvorgang im Internet ist, es kann also auch möglich sein, dass bereits vorher Symbole oder andere Faktoren Trust ausgelöst haben, und dieses Symbol den Trust nur noch verstärkt.

Herauszufinden, wie sehr Personen den angezeigten Symbolen bzw. Signalen wirklich vertrauen ist eines der Ziele des folgenden Experiments.

4.3 Experimentelles Messen von Trust

Ein erster Versuch, das Vertrauen von Menschen in einen Sicherheitsmechanismus messbar zu machen, wird in diesem Abschnitt präsentiert. Außerdem werden die Ergebnisse des Versuchs dargelegt und interpretiert.

4.3.1 Versuchssetup

Erfasst wurde das Vertrauen einer Gruppe von Menschen in drei verschiedene Schließzylinder. Der Test wurde **Between Subjects** durchgeführt. Die Präsentation der Schließzylinder wurde in Form eines Videos durchgeführt.
Jeder Schließzylinder wurde einmal bei einem Entsperrvorgang auf Video aufgezeichnet. Um Faktoren abseits der Schließzylinder möglichst auszuschließen, wurde in jedem Video dieselbe Tür zur selben Tageszeit gezeigt, und es führte jedesmal dieselbe Person den Entsperrvorgang durch. Außerdem waren alle Videos gleich lang. Dieses Vorgehen hilft dabei, die Aufmerksamkeit der Testpersonen auf die wesentlichen Teile des Versuchs zu lenken. Für den elektrischen Zylinder stand das Original nicht zur Verfügung, daher wurde eine Attrappe aus verfügbaren Teilen improvisiert und das Video im Nachhinein bearbeitet, um einen authentischeren Effekt zu erzeugen. Konkret wurden blinkende Lichter während des Entsperrvorgangs und ein akustisches Signal nach erfolgreichem Entsperren hinzugefügt.
Der Versuch wurde als Umfrage gestaltet, die mit Hilfe des Tools „Surveymonkey“ (SurveyMonkey 2014) erzeugt wurde. In den Abbildungen 4.9, 4.10 und 4.11 sind Screenshots der jeweiligen

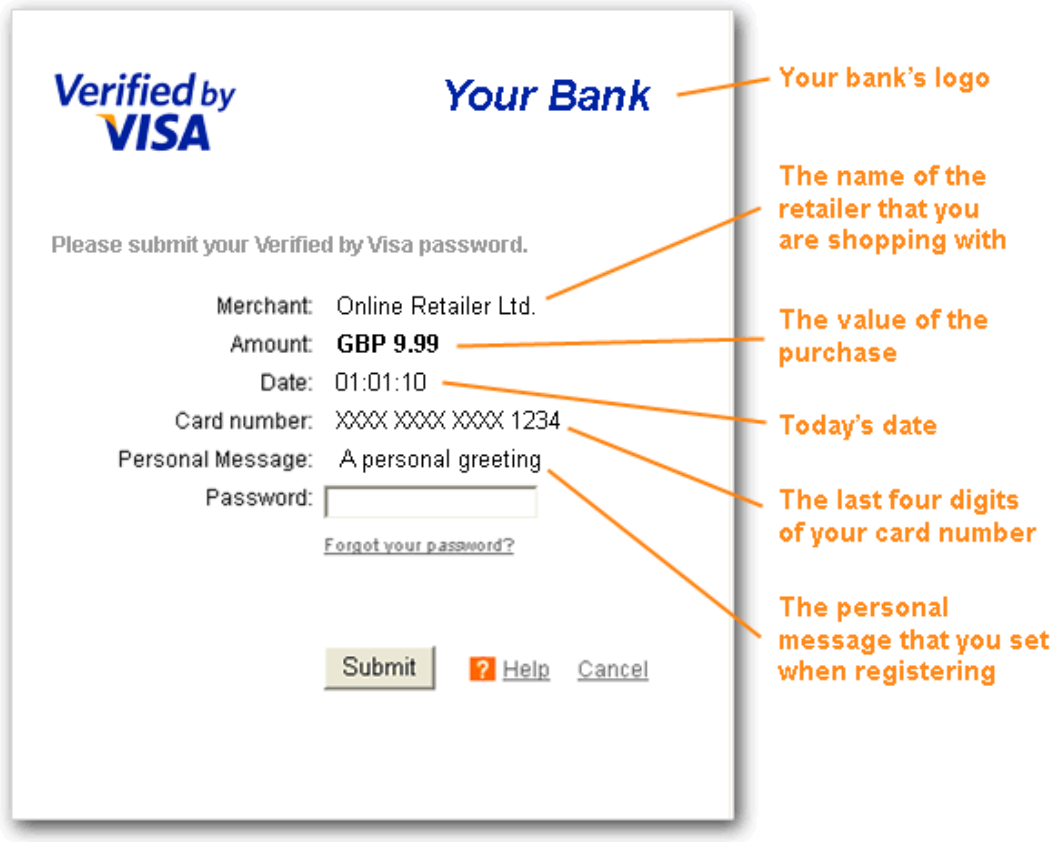


Abbildung 4.8: Verified by VISA Sample Image, (Visa Europe 2014)

Abbildung 4.9: Screenshot des Videos des alten Zylinders

Videos zu sehen, um eine Vorstellung über die Videos zu geben.
Die Personen wurden nach Betrachtung des jeweiligen Videos darum gebeten, folgende Frage zu beantworten: *Sie haben nun einen Schließmechanismus bei einem Aufsperrvorgang beobachtet. Bitte beantworten Sie die folgende Frage mit einem Wert von 1 bis 4, wobei 1 komplette Ablehnung und 4 komplette Zustimmung bedeutet: „Ich vertraue diesem Schloss“*. Es wurde eine Likert Skala mit 4 Werten verwendet (-2,-1,1,2), um neutrale Angaben (den mittleren Wert) auszuschließen. Weiters wurden die Testpersonen gebeten, einige demographische Daten anzugeben (Alter, Geschlecht). Außerdem wurde den Testpersonen die Möglichkeit gegeben, ihre Entscheidung zu begründen, falls gewünscht.

Abbildung 4.10: Screenshot des Videos des neuen Zylinders

Abbildung 4.11: Screenshot des Videos des elektrischen Zylinders

Statistische Größen Alter Zylinder	
n	93
Varianz	1,53
Mittelwert	-0,87
Median	-1
Standardabweichung	1,24
Konfidenzintervall (95%)	[-0,8790;-0,8628]

Tabelle 4.1: Statistische Auswertung alter Zylinder

4.3.2 Ergebnisse

Insgesamt haben sich 317 Personen an der Umfrage beteiligt. Die demographischen Aufteilungen sind in den Abbildungen 4.12 bis inklusive 4.19 zu finden, jeweils aufgeteilt nach den verschiedenen Zylindern und auch in der Gesamtabbildung. Aufgrund der sehr niedrigen Beteiligung von Personen jünger als 20 sowie älter als 60 Jahren (jeweils eine Person) wurden diese Antworten bei den vergleichenden Analysen jeweils ausgenommen.

In Tabelle 4.4 ist aufgrund des P-Werts zu erkennen, dass die unterschliedlichen Mittelwerte der Zustimmung nicht zufällig aufgetreten sind und das Vertrauen in die verschiedenen Zylinder unterschiedlich ist. Weiters lässt sich aus dem F-Wert ablesen, dass die Gruppen wirklich unterschiedliche Werte hervorgebracht haben. Der Mittelwert ist bei dem alten Zylinder -0,87, bei dem neuen Zylinder 0,5 und bei dem elektrischen Zylinder 0,31. Genaue Auswertungen der Testdaten befinden sich in den Tabellen 4.1, 4.2 bzw. 4.3.

Statistische Größen NFC Zylinder	
n	111
Varianz	1,91
Mittelwert	0,5
Median	1
Standardabweichung	1,32
Konfidenzintervall (95%)	[0,4965;0,5123]

Tabelle 4.2: Statistische Auswertung NFC Zylinder

Statistische Größen neuer Zylinder	
n	113
Varianz	1,74
Mittelwert	0,31
Median	1
Standardabweichung	1,38
Konfidenzintervall (95%)	[0,2981;0,3144]

Tabelle 4.3: Statistische Auswertung neuer Zylinder

Streuungsursache	*Quadratsummen (SS)*	*Freiheitsgrade (df)*	*Mittl. Quadratsumme*
Untersch. zw. d. Gruppen	109,3995	2	54,6997
Innerhalb der Gruppen	552,28	314	1,76
Prüfgröße (F)	31,0993975950985		
P-Wert	4,7579830713697 * E-13		
kritischer F-Wert	3,02449585867811		
Gesamt	661,68	316	

Tabelle 4.4: ANOVA der drei Gruppen

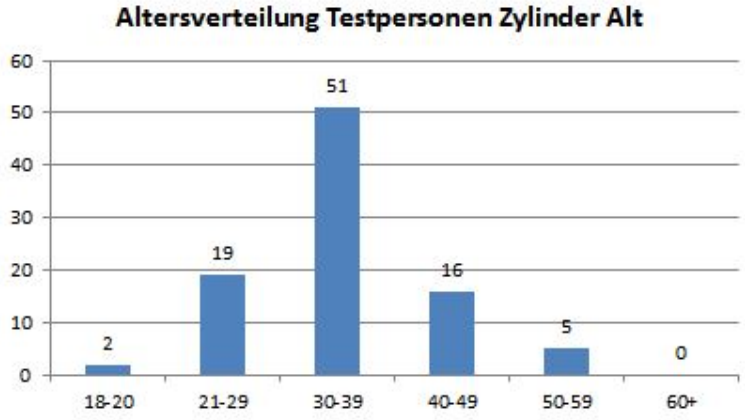


Abbildung 4.12: Altersverteilung Testpersonen, alter Zylinder

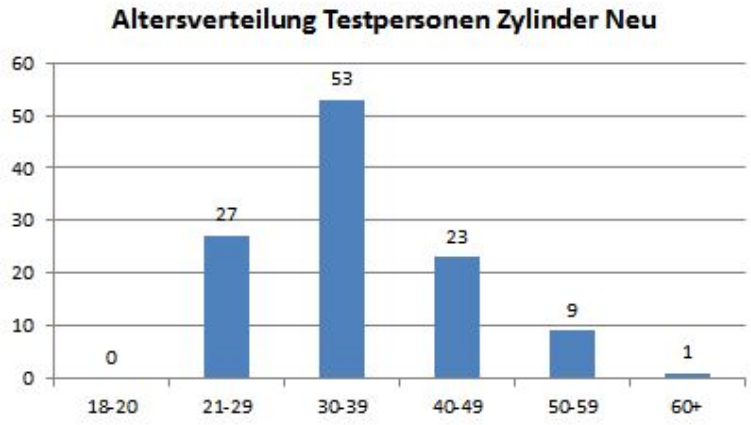


Abbildung 4.13: Altersverteilung Testpersonen, neuer Zylinder

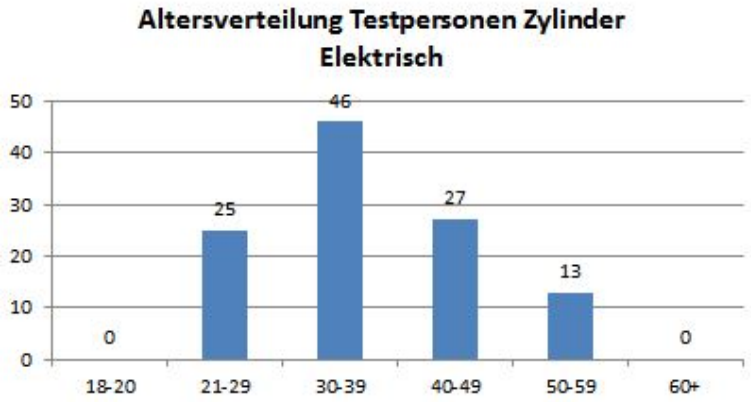


Abbildung 4.14: Altersverteilung Testpersonen, elektrischer Zylinder

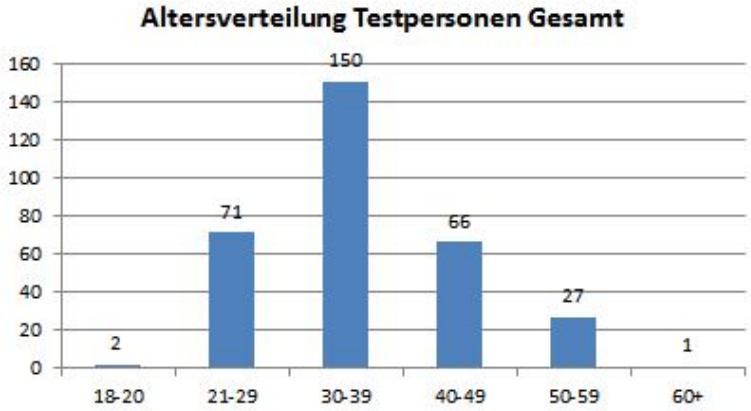


Abbildung 4.15: Altersverteilung Testpersonen, gesamt

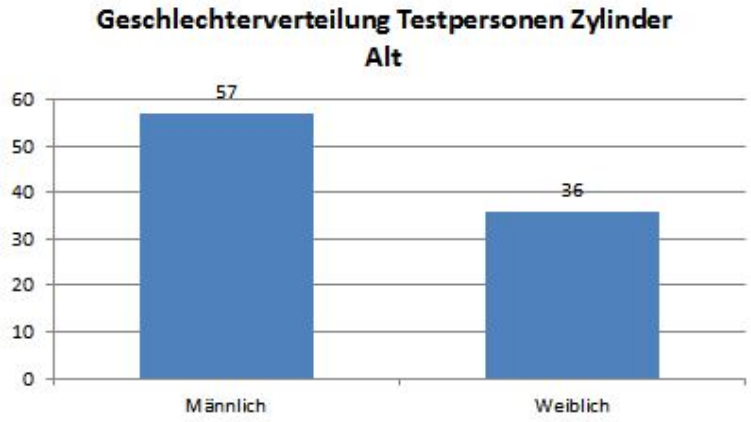


Abbildung 4.16: Geschlechterverteilung Testpersonen, alter Zylinder

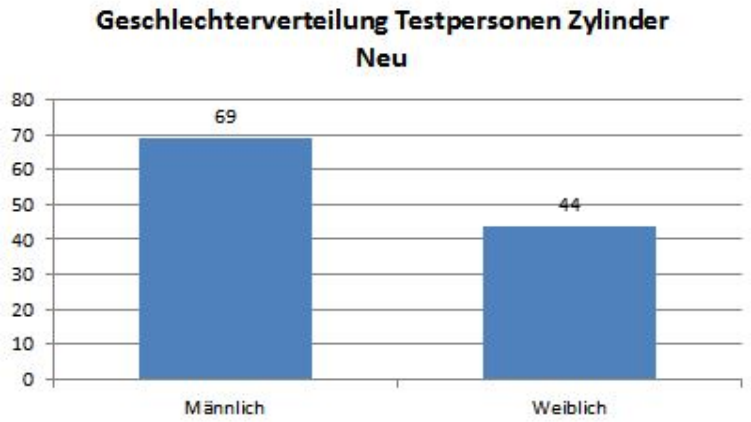


Abbildung 4.17: Geschlechterverteilung Testpersonen, neuer Zylinder

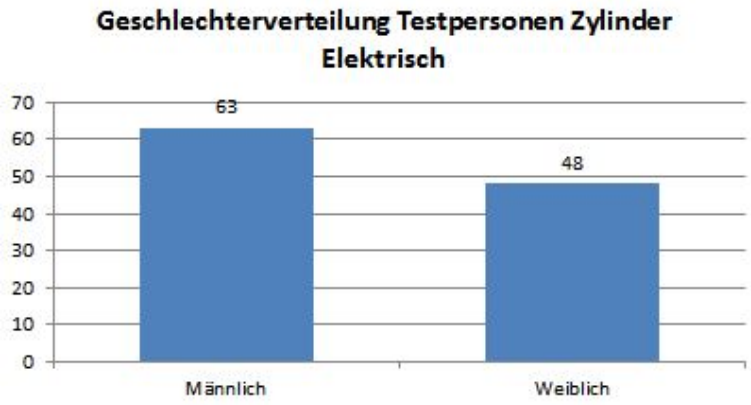


Abbildung 4.18: Geschlechterverteilung Testpersonen, elektrischer Zylinder

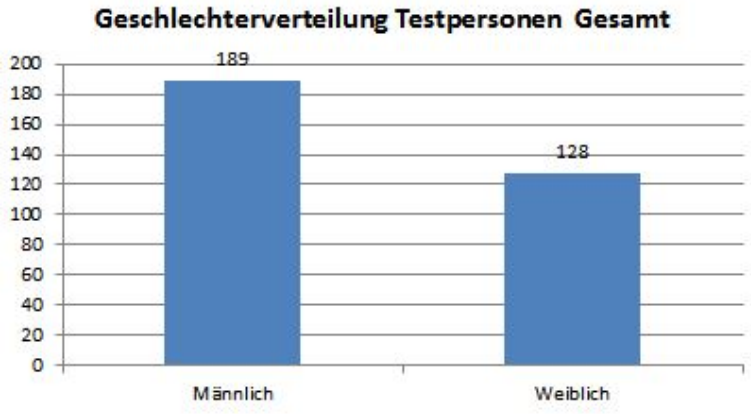


Abbildung 4.19: Geschlechterverteilung Testpersonen, gesamt

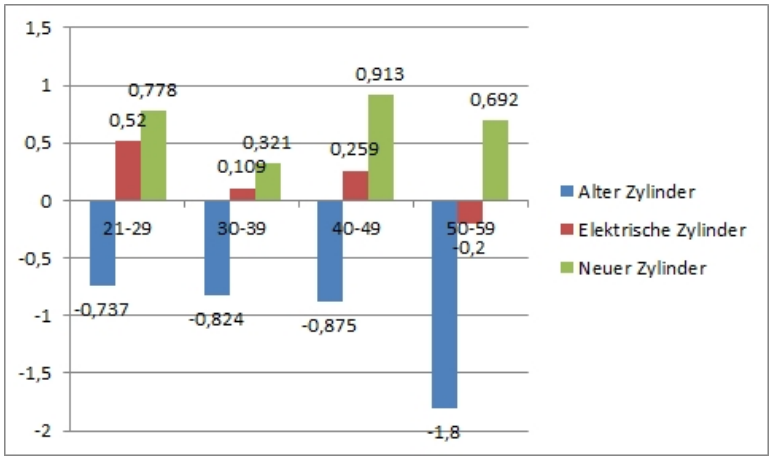


Abbildung 4.20: Mittelwerte des gemessen Vertrauens gesamt, nach Alter

4.3.3 Interpretation

Die bisher präsentierten Daten werden in diesem Teil zueinander in Kontext gestellt und es werden Interpretationen vorgeschlagen. Danach werden noch die textuellen Bemerkungen der Testpersonen präsentiert und auf einige davon eingegangen.

Dateninterpretation

Die Interpretation der Daten in diesem Abschnitt wird sich auf die Dimension der Korrelationen *Mittelwert - Alter* und *Mittelwert - Geschlecht* beziehen. Als erstes wird die Korrelation *Mittelwert - Alter* betrachtet. Als Übersicht für diese Korrelation eignet sich am besten Diagramm 4.20. Folgende Ausreißer sind hier zu beobachten:

- **Mittelwert des gemessen Vertrauens - alter Zylinder, Gruppe 50-59 Jahre:** In dieser Gruppe ist der Mittelwert für den alten Zylinder mehr als doppelt so hoch wie der nächsthöhere Mittelwert (der aus der Gruppe 40-49 Jahre). Daraus könnte geschlossen werden, dass Menschen in dieser Altersklasse herkömmlichen Schlössern wesentlich weniger vertrauen. In dieser Studie wird dieses Ergebnis aber aufgrund der niedrigen Auswertungsmenge (in dieser Altersklasse bei diesem Zylinder: n=5) als Ausreißer beachtet.

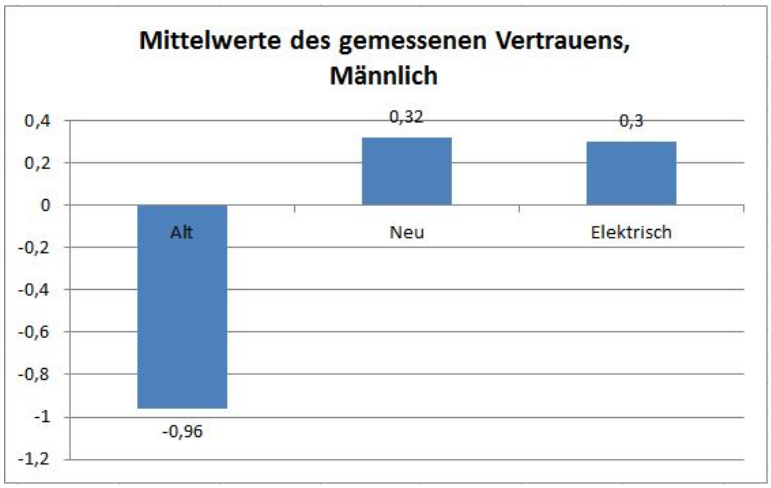


Abbildung 4.21: Mittelwerte des gemessen Vertrauens nach Zylinder, männlich

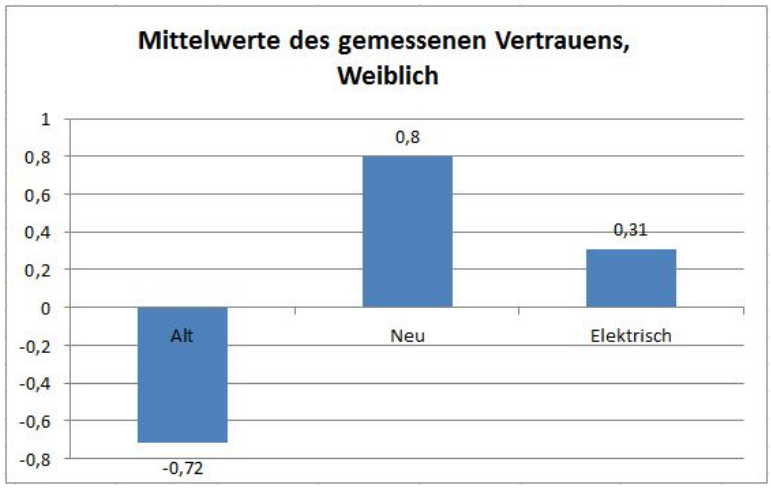


Abbildung 4.22: Mittelwerte des gemessen Vertrauens nach Zylinder, weiblich

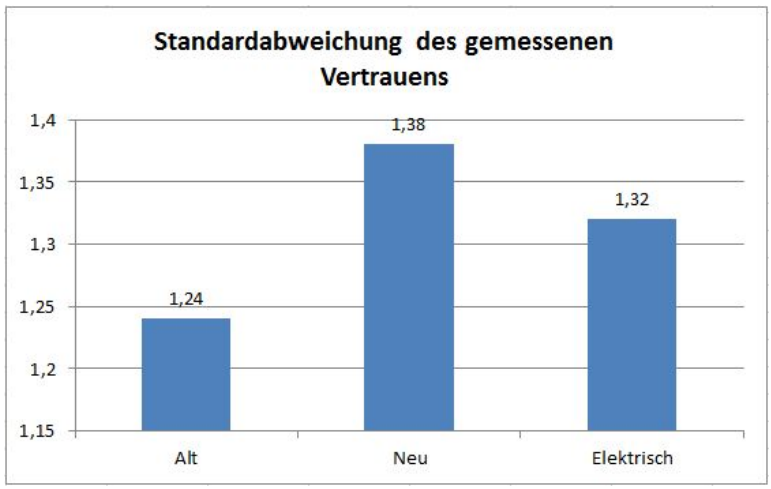


Abbildung 4.23: Standardabweichung des gemessen Vertrauens, nach Zylinder

- **Mittelwert des gemessen Vertrauens - neuer Zylinder, Gruppe 30-39:** Hier ist zu beobachten, dass der Mittelwert dieser Gruppe ebenfalls stark vom Erwartungswert und den Vergleichswerten abweicht. Von etwa der Hälfte bis hin zu einem Drittel der anderen Mittelwerte des gemessen Vertrauens ist dieser Wert als signifikant kleiner zu bewerten. Daraus lässt sich der Schluss ziehen, dass Personen im Alter von 30-39 Jahren handelsüblichen Sicherheitsschlössern am wenigsten vertrauen.
- **Mittelwert des gemessen Vertrauens - elektrischer Zylinder, Gruppe 21-29:** Der Mittelwert dieser Gruppe ist zweimal bis fünfmal so hoch wie die anderen zustimmenden Mittelwerte des gemessen Vertrauens für diesen Zylinder. Daraus ist zu schließen, dass junge Menschen diesem Mechanismus grundsätzlich mehr vertrauen als Menschen über 29 Jahre.
- **Mittelwert des gemessen Vertrauens - elektrischer Zylinder, Gruppe 50-59:** Der einzige negative Mittelwert abseits des alten Zylinders ist hier zu finden. Daraus lässt sich schließen, dass Menschen der Gruppe 50-59 sehr wenig Vertrauen in die neue Technologie der elektronischen Türverriegelung empfinden.

Der Grund für die beschriebenen Ausreißer könnte sein, dass junge Menschen (jünger als 30 Jahre) bereits in einer Mentalität groß geworden sind, die eine Grundakzeptanz für neue Technologien erlaubt. Dieser Erklärungsversuch passt auf die absteigende Akzeptanz des elektrischen Zylinders sowie die stabil bleibende Akzeptanz des neuen Zylinders. Einzig den Einbruch der Akzeptanzwerte für beide Zylinder in der Gruppe der 30-39 Jährigen ist mit dieser These nicht zu erklären. Die niedrigen Werte können damit erklärt werden, dass für 30-39 Jahre alte Menschen andere Werte wichtig und schützenswert sind als für Menschen anderen Alters.
Beide dieser Theorien müssen bei weiterer Forschung und weiteren Umfragen berücksichtigt und validiert werden.

Bemerkungen der Testpersonen

Zuletzt wird in diesem Abschnitt noch den Bemerkungen der Testpersonen und möglichen Interpretationen dazu Platz gegeben. Es werden diejenigen Bemerkungen präsentiert, die den meisten Bezug zu dem getesteten System aufweisen, in Kombination mit dem von den Testpersonen vergebenen Vertrauenswert. Weiters ist anzumerken, dass die Auswahl der Kommentare zeigen soll, welche Art von Bemerkungen am häufigsten vorgekommen sind. Die Bemerkungen werden auch kommentiert und in Bezug zu dem getesten System gesetzt.

- **Kommentare zum alten Zylinder:**
  - *(-1) Für ein Haustürschloss völlig ungeeignet:* Dieser Kommentar bezieht sich auf die Art der Tür, in der das Schloß eingesetzt wird.
  - *(-2) Mit einem simpel gebauten Dietrich zu knacken. Je nach Sicherheitsanspruch ist das Schloss vertrauensvoll/nicht vertrauensvoll:* Dieser Kommentar bezieht sich auf die Möglichkeit, das Schloss mit technischen Mitteln zu umgehen.
  - *(-1) Sieht nicht massiv genug aus, um einen Einbruch standzuhalten:* Dieser Kommentar bezieht sich auf die Brachialkraft, die notwendig ist um dieses Schloss zu umgehen bzw. zu zerstören.
  - *(-1) Schlüssel leicht nachmachbar; Dietrich nutzbar:* Auch hier wird festgehalten, wie einfach das Schloss mit technischen Mitteln umgangen werden kann.
  - *(-2) Depends on purpose: The mechanism is not safe enough if someone really desires to enter (thiefs, etc.), yet safe enough to prevent that anybody enters äccidentally":*Ein

weiteres Mal wird herausgestrichen, dass es für eine Person mit den richtigen technischen Mitteln einfach ist, den Sicherheitsmechanismus zu umgehen.

- **Kommentare zum neuen Zylinder:**
  - *(-1) Solche Schlösser sind relativ leicht zu knacken:* In diesem Kommentar wird darauf eingegangen, wie der Sicherheitsmechanismus umgangen werden kann.
  - *(1) Es scheint ein ganz normales Türschloss zu sein:* Dieser Kommentar weist darauf hin, dass das Schloss nach einem gewohnten Mechanismus aussieht.
  - *(-2) nur 1 fach Verriegelung:* In diesem Kommentar bezieht sich die Testperson auf die Methodik der Verriegelung. Das unterscheidet sich von vielen anderen Kommentaren, indem es von der Präposition ausgeht, dass das Schloss sicher wäre, wäre es denn ein zweites Mal zugesperrt.
  - *(2) hört sich sicher an:* Hier bezieht sich die Testperson auf nicht visuelle Sinneseindrücke.
  - *(2) sieht wie ein normales Schloss aus:* Ein weiteres Mal wird das Schloss mit einem gewohnten Mechanismus verglichen.
- **Kommentare zum elektrischen Zylinder:**
  - *(-1) Ein Schlüssel ist aus Eisen, auf der Karte sind „nur" Daten:* In diesem Kommentar findet sich der häufige Vergleich mit sogenannten „herkömmlichen" Schlössern. Neu im Vergleich zu den vorigen Kommentaren ist, dass hier der Vergleich negativ ausfällt.
  - *(1) System ist bekannt. Mit einem zweiten Sicherheitsmechanismus (keine zusätzliche Hardware aus Keycard; bspw. Nummereingabe auf Schloss) würde ich dem System voll vertrauen:* Dieser Kommentar zeigt zum einen generelles Grundvertrauen, demonstriert aber auch, dass die Wahrnehmung von Schlüsselkarten immer noch „unsicherer" ist als die Wahrnehmung von Sicherheitsschlüsseln.
  - *(-2) The are not enough information to trust the particular mechanism. Can you pull the mechanism off, for example? It is outside of the body of the door, this means that it is less protected at least. Where the power cord is? Or the power supply is embedded? If it not, the cord must come from inside of the door so installation problems can appear:* Ein Beispiel für einen Kommentar der demonstriert, dass die Kenntniss um die Funktionsweise von elektrischen Schlössern noch nicht weit verbreitet ist.
  - *(2) kenn ich so aus Hotels –> gewohnt:* Dieser Kommentar vergleicht das Schloss mit bereits bekannten und vertrauten Schlössern.
  - *(2) gleiche Funktion wie „normaler" Schlüssel:* Dieser Kommentar vergleicht das Schloss ebenfalls mit bereits bekannten und vertrauten Schlössern, allerdings der nicht elektrischen Variante.

Beispielhaft anhand von jeweils fünf Bemerkungen lassen sich Muster in der verbalen Bewertung des Vertrauens erkennen.

Beim alten Zylinder wird hauptsächlich danach beurteilt, wie leicht Schloss und Tür zu knacken oder aufzubrechen sind. Obwohl jedesmal dieselbe Tür verwendet wurde, finden sich bei diesem gehäuft Kommentare in denen es um Gewalteinwirkung geht. „Trust auf Basis von Fähigkeiten" vorrangig beachtet wurde.

Zweifel beim neuen Zylinder sind im Vergleich dazu in der Art, wie die Tür versperrt war und wie das Schloss und die Tür aussehen und klingen.

Beim elektrischen Zylinder finden sich zwei Themenkreise immer wieder. Einerseits der Vergleich mit ähnlichen Schlössern in Hotels oder Büros, der meist positiv besetzt ist und andererseits die Sorge, die Technik dahinter sei nicht sicher oder die Testperson verstehe einfach zu wenig davon, was die Karte und das Schloss sicher oder unsicher macht.

Korrelation zur Theorie

Zuletzt werden die Korrelationen zu den Trust-Grundlagen präsentiert, die sich nach Befragung der Testpersonen ergeben haben.

Charakteristika

Die grundlegenden Charakteristika von Trust werden von folgenden Phänomenen abgedeckt:

- *Trust auf Basis von Fähigkeiten*: Der alte Zylinder wird danach beurteilt, wie leicht er aufzubrechen ist, respektive wie gut er einem Einbruchsversuch standhalten kann.
- *Trust auf Basis von Wohlwollen*: In einem Hotel, in dem die Testperson für den Raum bezahlt, geht er davon aus, dass die Tür sicher ist.
- *Trust auf Basis von Integrität*: Die Sicherheit der Technik ist nicht für jede Testperson endgültig ersichtlich.

Faktoren, die Trust erzeugen

Faktoren, die Trust erzeugen oder durch ihre Abwesenheit verhindern, sind von folgenden Aussagen gedeckt:

- *Die Anzahl bereits durchgeführter Transaktionen mit diesem Trustee*: Testpersonen, die bereits mehrfach mit ähnlichen Schlössern zu tun hatten, vertrauen mehr als solche die derartige Schlösser nicht kennen. Dieses Phänomen lässt sich auf alle drei getesten Schlossarten auslegen. Dem alten Zylinder wird nicht vertraut, weil jede Testperson weiß, wie schlecht er schützt. Dem neuen Zylinder wird vertraut, weil jeder weiß, wie gut er schützt. Dem elektrischen Zylinder wird nur vertraut, wenn bereits bekannt ist, dass er gut schützt.
- *Die Art der Aktoren und ihre Reputation*: Hier wird ebenfalls die Art der Zylinder und Schlüssel beurteilt, allerdings in Verbindung mit Geschichten, die der Testperson gehört hat. Beispiel: „System ist bekannt, daher +1 Trust“
- *Kann der Trustor vertrauenswürdige Eigenschaften identifizieren?*: Dieser Punkt ist belegbar durch Aussagen wie „Hört sich sicher an!“ Testpersonen suchen Eigenschaften, die sie bereits als vertrauenswürdig kennengelernt haben.
- *Die vorangegangene Erfahrung des Trustor*: Hier ist der mehrfach gefallene Vergleich mit Hotel- oder Büroschlössern auffällig. Testpersonen, die bereits Erfahrung mit ähnlichen Schlössern gemacht haben, nutzen ihre Erfahrungen um die Vertrauenswürdigkeit zu bewerten.
- *Das eigentliche Risiko, dass der Trustor trägt*: Ein sehr plakatives Beispiel dafür ist „Für ein Haustürschloss völlig ungeeignet“ . Hier erwähnt eine Testperson, dass das Risiko, ein derartiges Schloss an einer Außentür anzubringen, für ihn viel zu hoch ist.

5 Usability-Test

I didn't fail the test, I just found 100 ways to do it wrong. Benjamin Franklin

In diesem Kapitel wird beschrieben, wie beim Testen der Usability von Sunrise vorgegangen wurde. Das Setting, die Aufgaben und die verwendeten Geräte werden aufgelistet. Danach werden die Resultate der Testpersonen tabellarisch aufbereitet. Für eine verlässliche statistische Auswertung ist die Anzahl an Testpersonen zu gering. Der Grund dafür ist, dass das Ziel des Tests das Herausarbeiten von Usability-Problemen ist. Dafür ist wie im 3 beschrieben eine geringe Anzahl an Testpersonen ausreichend. Dennoch sollen die gemessenen Metriken in Relation gestellt und interpretiert werden. Außerdem wird die Standardabweichung für jeden einzelnen Testfall angegeben. Die Formel dazu lautet:

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \overline{x})^2} \tag{5.1}$$

Danach werden Rückschlüsse aus den Testergebnissen gezogen. Zuletzt werden die Ergebnisse der Interviews aufgelistet und interpretiert.

5.1 Überblick über das Testvorgehen

Der Usability-Test für das Projekt Sunrise wurde in zwei Teile geteilt. Für den ersten Teil sollten vier Testpersonen jeweils vier Problemstellungen aus dem Aufgabenbereich des SSO lösen. Im zweiten Teil sollten vier andere Testpersonen jeweils 4 Problemstellungen aus dem Aufgabenbereich des Schlüsselbundinhaber (SBI) lösen. Die Zeit, die für das erfolgreiche Absolvieren der Aufgaben benötigt wurde sowie die aufgetretenen Fehler und die Anzahl der notwendigen Hilfestellungen beim Lösen der Tests wurden gemessen beziehungsweise aufgezeichnet. Als Fehler wird hier jede Aktion gezählt, die ein anderes Ergebnis als das gewünschte zur Folge hat.

Für die Durchführung der Studie wurde ein entspannter Rahmen gewählt. Die Testpersonen wurden gebeten, sich ausreichend Zeit für die Usability-Tests zu nehmen um Stressbildung bei Testpersonen und den beiden Testleitern zu vermeiden. Der Ort, an dem die Tests durchgeführt wurden, war die Institutsbibliothek der Forschungsgruppe für Industrielle Software (INSO). Durch die Wahl dieses Ortes konnte ein ruhiges und ungestörtes Umfeld für die Durchführung der Tests sichergestellt werden.

In Dumas und Redish (1993) wird festgestellt, dass es hilfreich ist, wenn möglichst wenige Personen um die Testperson platziert sind. Das senkt das subjektive Beobachtungsgefühl und die Testpersonen entspannen sich. Dadurch lassen sich Fehlbedienungen, die in einem realen Setting nicht auftreten würden, reduzieren und die Genauigkeit des Tests steigern. Aus diesem Grund wurde als Testgerät ein Laptop verwendet, der mittels Bildschirmspiegelung an einen externen Flachbildschirm angeschlossen wurde. Das erlaubte es dem Testbeobachter, von Testleiter und der

Testperson mehrere Meter entfernt zu sitzen und trotzdem jeden Klick und jeden Bedienungsfehler der Testperson zu beobachten und zu protokollieren.

Zusätzlich wurde ein USB-Kartenleser sowie mehrere Schlüsselbundmedien für die Tests zur Verfügung gestellt.

Bei der Selektion der Testpersonen wurde keine besondere Vorauswahl getroffen. Die einzige Anforderung an die Testpersonen war, ein beliebiges Smartphone zu besitzen, um etwaige Fehlbenutzungen auszuschließen, die bei Erstbenutzern von Smartphones womöglich aufgetreten wären.

Als Testmethode wurde **Thinking Aloud** verwendet. Daher lief auf dem Testlaptop während der Tests ein Diktiergerät, das die gesprochenen Gedanken der Testpersonen aufzeichnete. Diese Aufzeichnungen wurden nach den Tests mit den handgeschriebenen Protokollen abgeglichen. Das erlaubte es, ein noch detaillierteres Bild über den Eindruck der Sunrise-Webapplikation auf ihre Benutzer und Benutzerinnen zu bekommen.

Vor der Durchführung der eigentlichen Tests wurde für jede Testgruppe ein Pilottest durchgeführt. Bei einem derartigen Test werden die Tests mit Personen, die nicht aus der Gruppe der Haupttestpersonen stammen, durchgeführt. Dabei handelt es sich um eine Verifikation des Testvorgehens. Es wird nach methodischen und praktischen Fehlern im Testsetup gesucht. Außerdem werden dabei Benchmarkzeiten erstellt, um eine Terminplanung für den Haupttest zu erleichtern.

Jeder einzelne Test wurde in drei Phasen gegliedert

- Pre-Test Interview
- Testcases
- Post-Test Interview

5.1.1 Pre-Test Interview

Beim Pre-Test Interview werden die Vorkenntnisse der Testpersonen dokumentiert. Es wird in Erfahrung gebracht, wieviel Kontakt die Testperson mit ähnlichen Systemen wie dem Getesteten hatten. Des weiteren wird die Testperson auf die kommenden Aufgaben vorbereitet, indem durch die Fragestellung der Rahmen des Tests festgelegt wird. Die Daten aus diesem Interview dienen der Interpretation der Ergebnisse.

5.1.2 Testcases

In den Testcases werden die eigentlichen Tests festgehalten. Es handelt sich hier um Aufgaben, die einen breites Spektrum an Funktionaltät des Systems widerspiegeln sollen.

Die Kurzform der getesten Aufgaben für den Bereich SSO lauten:

- SSO1: Erstellen eines Dauerzutritts und Synchronisieren auf die Karte
- SSO2: Erstellen eines periodischen Zutritts und Synchronisieren auf die Karte
- SSO3: Synchronisieren eines Mobiltelefons per SMS
- SSO4: Deaktivieren eines Mediums

Sowie für den Bereich SBI:

Testperson	Testcase #1	Testcase #2	Testcase #3	Testcase #4	Testcase #5
1	SSO1	SSO2	SSO3	SSO4	U1
2	SSO2	SSO3	SSO4	SSO1	U1
3	SSO3	SSO4	SSO1	SSO2	U1
4	SSO4	SSO1	SSO2	SSO3	U1
5	SBI1	SBI2	SBI3	SBI4	U1
6	SBI2	SBI3	SBI4	SBI1	U1
7	SBI3	SBI4	SBI1	SBI2	U1
8	SBI4	SBI1	SBI2	SBI3	U1

Tabelle 5.1: Latin Square der Testcases

- SBI1: Aktualisieren der Sperrberechtigungen
- SBI2: Aufsperren eines Schlosses mit dem Mobiltelefon
- SBI3: Aussagen über die Öffnungszeiten eines bestimmten Schlosses treffen
- SBI4: Aussage über Zutritt mittels Protokoll treffen

Weiters sollten alle Testpersonen unabhängig von ihrer Testgruppe den Testfall U1 durchführen, bei dem es sich um einen einzelnen Sperrvorgang mit einer Schlüsselkarte handelte. Die Kurzbeschreibung dazu lautet: „Aufsperren eines Schlosses mit Karte - Sperrberechtigung vorhanden“.

Um der Testperson Kontext für die Ausführung der Aufgaben zu bieten, werden diese in kurze Geschichten, sogenannte **User Stories** verpackt. Ein Beispiel für eine solche **User Story** anhand des Testfalls SSO3 lautet: „Sie möchten Ihrem Freund, Stefan Test, ermöglichen, Sie jederzeit in Ihrer Wohnung zu besuchen. Allerdings ist Stefan gerade im Ausland. Verwenden Sie Sunrise, um ihm trotzdem den Zutritt mithilfe seines Handys zu ermöglichen.“

Als Counterbalancing Methode wurde hier ein Latin Square gewählt. Die Verteilung der Aufgaben auf die Testpersonen ist in Tabelle 5.1 zu sehen. Der Testfall U1 hat keine besonderen Auswirkungen auf den Lerneffekt der anderen Testfälle und muss daher nicht ausbalanciert werden.

5.1.3 Post-Test Interview

Nachdem eine Testperson alle gestellten Aufgaben durchgearbeitet hat, wird ein Post-Test Fragebogen ausgefüllt. Dieser bestand in diesem Fall zum Teil aus offenen Fragen und zum Teil aus einer angepassten Version der System Usability Scale. Die Antwortmöglichkeit „keine Angabe“ wurde gestrichen, um die Testpersonen zu einer eindeutigen Stellungnahme zu bringen. Diese **forced-choice scale** wird in Brooke (1996a) vorgestellt. Weiters werden die Fragen nur auf Verlangen eingegrenzt, um genauere Informationen und Einblicke bezüglich der Akzeptanz der Software zu finden.

Eine detaillierte Version des verwendeten Testplans ist im Appendix A zu finden.

5.2 Tabellarische Auswertung der Ergebnisse

In weiterer Folge werden die Messergebnisse der Testmetriken statistisch aufbereitet und kommentiert. Für jede Testgruppe und Metrik werden die Ergebnisse aller Testpersonen, der Durchschnitt und der Median der Ergebnisse aufgezeigt.

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SSO 1	20:20	01:10	00:39	01:15	*05:51*	*01:13*	*09:40*
SSO 2	04:28	07:17	05:45	04:01	*05:23*	*05:07*	*01:28*
SSO 3	01:27	05:27	00:49	01:53	*02:24*	*01:40*	*02:05*
SSO 4	01:10	01:39	00:46	03:16	*01:43*	*01:25*	*01:06*
Ø	*06:51*	*03:53*	*02:00*	*02:36*			
Median	*02:58*	*03:33*	*00:48*	*02:35*			

Tabelle 5.2: Benötigte Zeit in Minuten für die SSO Tests

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SSO 1	9	0	0	1	*2,50*	*0,5*	*4,25*
SSO 2	2	4	5	4	*3,75*	*4*	*1,26*
SSO 3	1	3	0	3	*1,75*	*2*	*1,5*
SSO 4	0	0	0	1	*0,25*	*0*	*0,5*
Ø	*3,00*	*1,75*	*1,25*	*2,25*			
Median	*1,50*	*1,50*	*0,00*	*2,00*			

Tabelle 5.3: Begangene Fehler bei den SSO Tests

5.2.1 SSO-Tests

In diesem Abschnitt werden die Zeiten, Fehler und benötigten Hilfeleistungen für die SSO-Tests aufgezeigt und analysiert. Bereits in den Pilottests wurde erkannt, dass diese Tests länger dauern als die der SBI Tests.

Benötigte Zeit

Beim Vergleichen der Kennziffern Mittelwert und Median ist ersichtlich, dass es bei SSO1 einen starken Ausreißer gibt. Es ist symptomatisch, dass der jeweils erste Test, den eine Testperson ausgeführt hat, signifikant länger gedauert hat als die folgenden Tests. Eine Ausnahme zu dieser Beobachtung bildet SSO2, der bei jeder Testperson ungeachtet der Position, an der er ausgeführt wurde, etwa vier bis fünf Minuten gedauert hat.

Begangene Fehler

Die Metriken der begangenen Fehler verhalten sich ähnlich wie die der benötigten Zeit. Ein sehr steiles Gefälle ist nach dem ersten oder spätestens dem zweiten Test zu erkennen. Ebenfalls finden sich hier signifikante Ausreißer bei Testcase SSO2. Hier wurden ungeachtet der Position die meisten Fehler bei der Bedienung notiert.

Benötigte Hilfestellungen

Die Auflistung der benötigten Hilfestellungen ist wenig aussagekräftig. Es haben nur zwei Testpersonen bei je einem Test Hilfestellung benötigt. Die anderen Aufgaben wurden ohne Hilfe zur Vollendung gebracht. Erwähnenswert ist noch, dass Testperson 4 die Hilfestellungen bei dem letzten Test benötigte.

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SSO 1	4	0	0	0	*1,00*	*0*	*2*
SSO 2	0	0	0	0	*0,00*	*0*	*0*
SSO 3	0	0	0	2	*0,50*	*0*	*1*
SSO 4	0	0	0	0	*0,00*	*0*	*0*
Ø	*1,00*	*0,00*	*0,00*	*0,50*			
Median	*0,00*	*0,00*	*0,00*	*0,00*			

Tabelle 5.4: Benötigte Hilfestellungen bei den SSO Tests

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SBI 1	00:33	00:58	00:38	00:42	*00:43*	*00:40*	*00:11*
SBI 2	01:09	04:20	00:39	01:58	*02:02*	*01:34*	*01:38*
SBI 3	00:47	01:11	01:12	00:37	*00:57*	*00:59*	*00:18*
SBI 4	01:06	00:38	01:44	00:12	*00:55*	*00:52*	*00:39*
Ø	*00:54*	*01:47*	*01:03*	*00:52*			
Median	*00:57*	*01:05*	*00:56*	*00:40*			

Tabelle 5.5: Benötigte Zeit in Minuten für die SBI Tests

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SBI 1	0	2	1	1	*1,00*	*1*	*0,82*
SBI 2	2	6	1	3	*3,00*	*2,5*	*2,16*
SBI 3	0	1	1	0	*0,50*	*0,5*	*0,58*
SBI 4	1	0	2	2	*1,25*	*1,5*	*0,96*
Ø	*0,75*	*2,25*	*1,25*	*1,50*			
Median	*0,50*	*1,50*	*1,00*	*1,50*			

Tabelle 5.6: Begangene Fehler bei den SBI Tests

5.2.2 SBI-Tests

Für die SBI-Tests wurden kürzere Durchlaufzeiten erwartet als für die SSO-Tests.

Benötigte Zeit

Bei der Analyse der Zeiten für den SBI-Test sind wenige Ausreißer zu erkennen. Ebenso fehlt das Muster, das bei den SSO-Tests zu erkennen war, bei dem die späteren Tests stark durch den Lerneffekt der ersten Tests beeinflusst wurden. Dadurch liegen auch Median und Durchschnitt sehr nahe beieinander.

Begangene Fehler

Werden die begangenen Fehler analysiert, bietet sich ein Bild, das mit den gemessenen Zeiten nicht konsistent ist. Obwohl sehr kurze Zeiten gemessen wurden, wurden von den Testpersonen zum Teil viele Fehler gemacht (Median zwischen 0,5 und 2,5).

	TP 1	TP 2	TP 3	TP 4	*Ø*	*Median*	*Standardabweichung*
SBI 1	0	0	0	0	*0,00*	*0*	*0*
SBI 2	0	2	0	1	*0,75*	*0,5*	*0,96*
SBI 3	0	0	0	0	*0,00*	*0*	*0*
SBI 4	0	0	0	0	*0,00*	*0*	*0*
Ø	*0,00*	*0,50*	*0,00*	*0,25*			
Median	*0,00*	*0,00*	*0,00*	*0,00*			

Tabelle 5.7: Benötigte Hilfestellungen bei den SBI Test

Testperson	Zeit	Fehler	Hilfestellungen
TP 1	02:16	3	2
TP 2	01:00	0	0
TP 3	00:51	1	0
TP 4	00:36	1	0
TP 5	03:44	5	1
TP 6	02:43	4	1
TP 7	02:57	7	2
TP 8	02:24	4	2
Ø	*02:04*	*3,13*	*1*
Median	*02:20*	*3,5*	*1*

Tabelle 5.8: Ergebnisse Testcase U1, Zeit in Minuten

Notwendige Hilfestellungen

Interessant ist, dass im Vergleich zu den SSO Tests mehr Fehler begangen wurden, die geforderten Hilfeleistugnen allerdings vergleichbar wenige sind.

5.3 Rückschlüsse aus den Ergebnissen

Allgemeine Rückschlüsse auf die Benutzbarkeit des Systems lassen sich durch den Testcase U1 ziehen, der von beiden Testgruppen durchgeführt wurde. In Tabelle 5.8 ist ersichtlich, dass der Durchschnitt und der Median der gemessenen Metriken sehr nahe beieinander liegen. Es ist daher anzunehmen, dass für ungeschulte Erstbenutzer und Erstbenutzerinnen des Systems eine Zeit von etwas mehr als zwei Minuten zu erwarten ist, bis dieser das Schloss das erste Mal erfolgreich geöffnet hat. Diese Zeit ist im akzeptablen Bereich. Es war bei den Tests, die deutlich länger als zwei Minuten gedauert haben, deutliche Frustration bei den Testpersonen bemerkbar. Sehr deutlich ist auch die Korrelation der erhöhten Testzeit und der geforderten Hilfestellungen zu beobachten.

5.3.1 SSO

Aus den gewonnenen Daten lässt sich der Schluss ziehen, dass die Lernkurve für die gestellten Aufgaben sehr steil nach unten geht. Der jeweils erste Testcase dauerte bei den meisten Testpersonen am längsten, jeder weitere wesentlich kürzer. Die Ausreißer bei Testperson 1 lassen sich dadurch erklären, dass diese Person mit den Techniken des „Web 2.0“ nicht vertraut war. Dadurch war eine Eingewöhnungszeit auf diese Technologie notwendig, die auf die Lernzeit für die Webapplikation aufgeschlagen wurde. Beispielsweise war der Testperson nicht klar, dass es sich

um eine Webapplikation und nicht um eine Desktopapplikation gehandelt hat. Daher hat die Testperson Hilfestellungen wie Kontextmenüs gesucht, die in der Applikation aber nicht vorhanden waren. Einige Minuten später hat der Kontext der Webseite verhindert, dass die Testperson die Technik Drag & Drop für das Erstellen und Zuteilen von Berechtigungen verwendet. Diese und ähnliche Fehler erklären die etwas mehr als 20 Minuten, die die Testperson für die erste Aufgabe gebraucht hat.

Die Tabelle der begangenen Fehler lässt den Schluss zu, dass nicht alle Funktionen der Applikation selbsterklärend sind. Viele Testcases wurden nur mit Fehlern zum Abschluss gebracht. Im Kontext mit den benötigten Hilfestellungen lässt sich schließen, dass Benutzer und Benutzerinnen trotzdem in der Lage sind, die an sie gestellten Aufgaben zu erfüllen.

5.3.2 SBI

Die Daten, die aus den Aufzeichnungen der SBI-Tests gewonnen wurden, lassen den Schluss zu, dass die Aufgaben der Testcases für die SBI-Tests alle gleich herausfordernd waren. Es wurden wesentlich mehr Fehler als bei den SSO-Tests begangen. Bemerkenswert ist, dass dennoch ähnlich oft um Hilfe gebeten wurde. Daraus lässt sich schließen, dass bei der Smartphone App leichter Fehler gemacht werden, respektive mehr Potential zur Verbesserung liegt als bei der Webapplikation.

Die Korrelation zwischen den Testcases U1 und SBI2 ist interessant. Es lässt sich beobachten, dass das Aufsperren mit einer Schlüsselkarte sowie mit einem Smartphone sehr ähnliche Zeiten und Fehleranfälligkeiten haben. Für einen weiteren Usability-Test wäre es interessant, den Lerneffekt beim Aufsperren mit dem Smartphone zu beobachten und zu testen. Dadurch würde die Frage beantwortet, ob das Aufsperren mit dem Smartphone nach mehreren Verwendungen schneller bewerkstelligt werden kann.

5.4 Resultate der Interviews

Die Interviews wurden vor und nach dem Testvorgehen von derselben Person durchgeführt, die die Testpersonen auch durch die Tests begleitet hat. Die Fragen wurden in einem neutralen Tonfall gestellt und für jede Testperson von einem Blatt abgelesen, um unbewusste Beeinflussung der Testpersonen zu vermeiden.

5.4.1 Pre-Test Interview

Das Pre-Test Interview wurde dazu verwendet, um die Erfahrung der Testpersonen mit den verwendeten Technologien zu kalibrieren.

Bei den Pre-Test Interviews zeigt sich, dass viele der Testpersonen bereits mit elektronischen Schlössern Erfahrung gemacht haben. Diese Erfahrung lässt nicht darauf schließen, dass diese Personen in weiterer Folge ein Sunrise-Schloss ohne Probleme bedienen können. Außerdem ist zu beobachten, dass die Technologie NFC bei Besitzern von Smartphones bekannt ist, auch wenn diese nicht verwendet wird.

5.4.2 Post-Test Interview

Das Post-Test Interview bestand aus 13 Fragen, von denen zehn analog zur SUS gestellt wurden. Die letzten drei Fragen zielten darauf ab, ein Stimmungsbild der Testpersonen zu erhalten.

	TP 1	TP 2	TP 3	TP 4
Geschlecht	männlich	männlich	männlich	männlich
Alter	51-70	20-30	20-30	31-50
Mobiltelefon	Samsung Galaxy, iPhone 4S	iPhone	HTC Sensation	Samsung Galaxy Nexus
NFC bekannt	Ja	Ja	Ja	Ja
NFC verwendet	Nein	Nein	Nein	Ja
Erfahrung mit elektr. Schlössern	Ja, Code Eingabe, Fingerprint	Ja, Chipschloss	Ja, Chipschloss	Ja, verwenden und entwickeln

Tabelle 5.9: Ergebnisse des Pre-Test Interviews der SSO Tests

	TP 5	TP 6	TP 7	TP 8
Geschlecht	männlich	männlich	weiblich	weiblich
Alter	31-50	20-30	31-50	31-50
Mobiltelefon	iPhone	HTC	Blackberry Bold	HTC Desire
NFC bekannt	Ja	Ja	Ja	Ja
NFC verwendet	Ja	Ja	Ja	Ja
Erfahrung mit elektr. Schlössern	Nein	Nein	Ja, im Hotel	Ja, im Hotel

Tabelle 5.10: Ergebnisse des Pre-Test Interviews der SBI Tests

	TP 1	TP 2	TP 3	TP 4
Frage 1	2	2	2	2
Frage 2	1	-1	-1	-2
Frage 3	1	1	1	1
Frage 4	-1	2	2	2
Frage 5	2	1	1	1
Frage 6	-2	2	-2	1
Frage 7	1	2	-1	2
Frage 8	-2	-1	-1	-2
Frage 9	1	1	2	1
Frage 10	1	-2	-2	-2

Tabelle 5.11: Ergebnisse der Post-Test Interviews der SSO Gruppe

Es wurde gefragt, ob sich die Testpersonen vorstellen könnten, das Schloss bei sich zuhause zu installieren, ob sie es für sicherer oder unsicherer halten als ein herkömmliches Schloss und sie wurden darum gebeten, generelles Feedback und Anmerkungen abzugeben. Aufgrund der unterschiedlichen Beantwortungsweise dieser Fragen werden die SUS Fragen gesondert ausgewertet und danach wird auf die textuellen Fragen und Antworten eingegangen. Der komplette Fragenkatalog findet sich in Appendix A.7.4

Auswertung der SUS Fragen

Die Fragen werden in diesem Abschnitt getrennt nach der Gruppe der Testpersonen ausgewertet. Die Auswertung der Antworten in Tabelle 5.11 ergibt für die Testpersonengruppe SSO die vier Usability Scores von **75, 67.5, 72.5** sowie **75** und somit einen Mittelwert von **71.25** Punkten.

	TP 5	TP 6	TP 7	TP 8
Frage 1	2	1	2	2
Frage 2	-2	-2	-2	-1
Frage 3	2	-1	1	1
Frage 4	2	1	-2	2
Frage 5	2	2	-1	2
Frage 6	-2	1	-2	-2
Frage 7	2	2	2	2
Frage 8	-2	-2	-2	-2
Frage 9	2	1	2	1
Frage 10	-2	1	-2	-2

Tabelle 5.12: Ergebnisse der Post-Test Interviews der SBI Gruppe

Die Auswertung der Antworten in Tabelle 5.12 ergibt für die Testpersonengruppe SBI die vier Usability Scores von **90, 65, 90** sowie **82.5** und somit einen Mittelwert von **81.875** Punkten.

Aus diesen Auswertungen lässt sich schließen, dass Benutzer und Benutzerinnen, die nur mit den Schließkomponenten in Kontakt kommen, dem System eine bessere Usability bescheinigen als Benutzer und Benutzerinnen, die auch mit der Schlüsselerstellung und Verwaltung beauftragt wurden. Insgesamt ergibt sich für das gesamte System ein Mittelwert von **76,5625** Punkten. Die Usability des Gesamtsystems ist damit nach Brooke 1996b überdurchschnittlich zu bewerten.

Auswertung der textuellen Fragen

Die letzten drei Fragen des Post-Test Interviews lauteten:

- Würden Sie Sunrise in Ihrer Wohnung verwenden?
- Glauben Sie, dass Sunrise sicherer als ein herkömmliches Schloss ist?
- Zusätzliche Anmerkungen, Vorschläge, Kritikpunkte?

Die Antworten auf die erste Frage waren bis auf einmal einstimmig Ja, mit Begründungen wie: *„Ich bin an der Technik interessiert.“*, *„Das System ist sehr flexibel.“*, *„Mit einem physischen Schlüssel herumgehen ist mir unangenehm.“*, aber auch kritischen Punkten wie: *„Ich habe Bedenken, nicht mehr in die Wohnung zu kommen, wenn die Batterie leer ist.“* oder *„Gerne im Büro installieren, für meine Wohnung warte ich, bis die Sicherheitsaspekte geklärt sind.“*. Die Begründung für die einzelne Gegenstimme lautete: *„Ich habe datenschutzrechtliche Bedenken wegen des Zutrittsprotokolls“*. Aus diesen Antworten lässt sich eine prinzipiell positive Disposition neuen Technologien gegenüber bei den Testpersonen ableiten, allerdings sind auch Bedenken zu bemerken.

Die Antworten auf die zweite Frage waren differenzierter als bei der ersten Frage. Hier finden sich fünf Antworten mit Ja, die begründet werden beispielsweise mit: *„Alte Schlösser sind leicht zu knacken, elektronische Schlüssel schwer zu reproduzieren.“*, *„Ich vertraue der Kryptographie.“* oder *„Ich kann verlorene Schlüssel leicht deaktivieren.“*. Nur einmal wurde diese Frage mit Nein beantwortet, die Begründung hierfür war *„Warum sollte es sicherer sein, wenn es gleich sicher ist, ist das doch gut genug“*. Sehr interessant sind die zwei unentschlossenen Antworten, die begründet wurden mit *„Ich weiß, wie leicht normale Schlösser geknackt werden können, ich weiß aber*

nicht wie leicht diese Schlösser getäuscht werden können“ und *„Weder sicherer noch unsicherer, der Schließmechanismus ist ja derselbe wie bei anderen Schlössern, nur der Sperrmechanismus ist ein anderer“*. Aus diesen Antworten lässt sich ableiten, dass Vertrauen in die Technologie davon abhängt, wie sehr sich die Testperson bereits mit NFC, Kryptographie oder ähnlichen Technologien auseinandergesetzt hat.

Die Anmerkungen, die bei der dritten Fragen genannt wurden sind: *„Die Protokollierung ist ein tolles Feature.“*, *„Die UI ist sehr gut, Texthilfen wären aber hilfreich.“*, *„Es dauert zu lange bis die Authentifizierung am Schloss erfolgt.“*, *„Das blaue, schnell blinkende Licht am Zylinder ist verwirrend und hindert mich daran, ohne Anleitung eine Tür zu sperren.“*, *„Die Schlüssel per SMS zu verschicken ist ein tolles Feature.“* und *„Das Test-Smartphone war umständlich zu bedienen, die Applikation sollte auf jedem NFC fähigen Gerät laufen.“*. Auch hier lässt sich ein Trend erkennen, dass technik-affine Testpersonen leicht mit der Technologie zurecht kommen, während andere Testpersonen auf Hilfestellung angewiesen sind, um nicht verwirrt zu sein.

6 Testresultate

You may never know what results come of your actions, but if you do nothing, there will be no results.
Mahatma Ghandi

In diesem Kapitel werden die gefundenen Inkonsistenzen der Usability Tests beschrieben. Für jedes Problem, das in den Tests entdeckt wurde, wird ein eigener Eintrag erstellt, der nach folgenden Gesichtspunkten analysiert und beschrieben wird.

- **Problembeschreibung**
  Hier wird eine textuelle Beschreibung der gefundenen Inkonsistenz gegeben. In einigen Fällen wird das Verständnis durch Screenshots unterstützt.
- **Häufigkeit des Auftretens**
  Hier wird angegeben, wie viele Testpersonen auf diese Inkonsistenz gestoßen sind. Jede Session wurde mit jeweils vier Testpersonen durchgeführt. Die einzige Ausnahme stellt der Test zum Öffnen der Tür mittels Schlüsselkarte dar. Dieser wurde mit allen acht Testpersonen durchgeführt.
- **Klassifizierung**
  Die Klassifizierung gibt an, wie schwerwiegend die Inkonsistenz einzustufen ist. Die möglichen Stufen sind in aufsteigender Reihenfolge: Gering, Bedenklich und Kritisch.
- **Mögliche Ursachen**
  Es werden Theorien postuliert und gegebenenfalls Beispiele aus anderen Applikationen gegeben, um die möglichen Ursachen der Inkosistenz zu finden. Wurde während des Testens ein Bug entdeckt, wird dieser ebenfalls hier festgehalten.
- **Vorschläge zur Behebung**
  Es werden Vorschläge gebracht, wie die Inkonsistenzen zu beheben sind. Wenn Testpersonen Aussagen getroffen haben, wie die Software zu verbessern ist, werden diese hier festgehalten. Wurde während des Testens ein Bug entdeckt, wird hier nur die Meldung „Bugfix“ festgehalten.

Danach werden Probleme, die ein Sicherheitsrisiko darstellen, separat besprochen. Zuletzt werden die Verbesserungsvorschläge zusammengefasst.

6.1 Gefundene Inkonsistenzen

Die Inkonsistenzen werden hier durchnummeriert aufgeführt.

- **Problembeschreibung — IK1**
  Beim Erstellen eines ganztägigen Schlüssels ist die Testperson verwirrt, weil die Maske zur manuellen Zeiteingabe angezeigt bleibt.
- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Wenn ein ganztägiger Schlüssel erstellt wird, erwartet die Testperson, dass keine weiteren Einstellungen notwendig sind.
- **Vorschläge zur Behebung**
  Die Textfelder zur Zeiteingabe bei der Erstellung von ganztägigen Schlüsseln werden ausgeblendet.

- **Problembeschreibung — IK2**
  Wenn ein neuer Schlüssel generiert wurde, erscheint im Schlüsselicon der Text „Schlüssel – wird erstellt“. Dieses Verhalten suggeriert der Testperson, dass im Hintergrund etwas passiert und er auf das Ergebnis warten muss.
- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Die Meldung ist für einen Erstbenutzer oder eine Erstbenutzerin undeutlich formuliert.
- **Vorschläge zur Behebung**
  Die einfachste Lösung ist, die Meldung anzupassen – beispielsweise: „Der Schlüssel wurde erstellt – Bitte synchronisieren Sie das Medium!“

- **Problembeschreibung — IK3**
  Wenn das Schloss eingekuppelt ist und diesen Zustand durch das grüne Licht signalisiert hat, erkennt die Testperson nicht, dass es ein mechanisches Schloss ist, das per Hand geöffnet und geschlossen werden muss.
- **Häufigkeit des Auftretens**
  5 von 8 Testpersonen

- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Die Testperson hat aufgrund vorgegangener Erfahrungen mit elektronischen Schlössern die Erwartungshaltung, dass das Schloss automatisch öffnet und schließt.
- **Vorschläge zur Behebung**
  Ein Quick Start Guide (QSG), der ähnlich wie bei heutigen Druckern oder Kopierern auf wenigen Seiten illustriert die wichtigsten Schritte anzeigt, die zur Bedienung des Schlosses notwendig sind. Diese Methode wurde von mehreren Testpersonen (5 von 8) als bevorzugte Lösung genannt.

- **Problembeschreibung — IK4**
  Beim Öffnen der Tür mittels der Schlüsselkarte zieht die Testperson die Karte zu schnell wieder vom Schloss weg, was in einem fehlerhaften Sperrvorgang resultiert.
- **Häufigkeit des Auftretens**
  7 von 8 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Das sofortige Feedback mit dem blau blinkenden Licht verwirrt die Testperson. Sie denkt, die Authentifizierung ist erledigt und die Karte wird nicht mehr benötigt. Dass die Authorisierung noch läuft, ist nicht klar.
- **Vorschläge zur Behebung**
  Ebenfalls per QSG. Das blinkende Licht zu entfernen ist nicht empfehlenswert. Das Feedback ist notwendig, um Aktivität zu signalisieren.

- **Problembeschreibung — IK5**
  Die Aufgabe, die Karte zu deaktivieren, löst die Testperson dadurch, dass sie alle auf der Karte vorhandenen Schlüssel löscht, anstatt das gesamte Medium zu deaktivieren.
- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Der Button, der das Schlüsselbundmedium (SBM) deaktiviert, ist sehr weit am unteren Bildschirmrand angeordnet. Dadurch ist er von der Testperson schwierig zu finden. Wird eine niedrige Bildschirmauflösung verwendet verschwindet der Button komplett aus dem Sichtfeld und ist nur durch Scrollen zu finden.

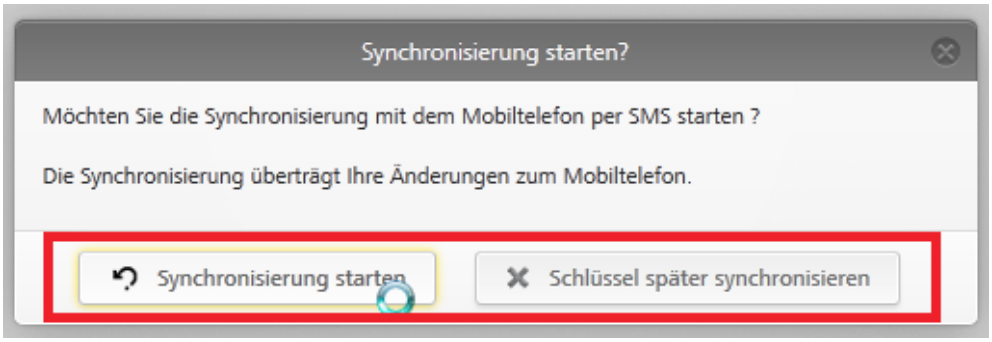


Abbildung 6.1: Problem IK6

- **Vorschläge zur Behebung**
  Den Button am oberen Ende des Schlüsselfensters plazieren. Den Button mit Metaphern aus dem realen Leben zu designen, beispielsweise eine rote Färbung, oder eine gelb-schwarze Ummantelung, um den Effekt klarer zu gestalten.

- **Problembeschreibung — IK6**
  Bei der Funktion, ein Mobiltelefon per SMS zu synchronisieren, sind die Buttons wie in Abbildung 6.1 zu sehen, mit der semantischen Bedeutung „OK“ und „Abbrechen“ relativ zu allgemeinen Betriebssystem Metaphern verkehrt angeordnet. „OK“ ist klassischerweise rechts und „Abbrechen“ klassischerweise links.

- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Manche Testpersonen sind die Anordnung von „OK“ und „Abbrechen“ sehr stark gewohnt und werden durch diese Anordnung verwirrt.
- **Vorschläge zur Behebung**
  Die beiden Buttons werden vertauscht.

- **Problembeschreibung — IK7**
  Die Testperson erstellt einen neuen Schlüssel und klickt auf den Text „Ändern“ um die Art des Zutritts zu ändern. Daraufhin verschwindet das Fenster ohne weitere Meldung. Siehe Abbildung 6.2.

- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen

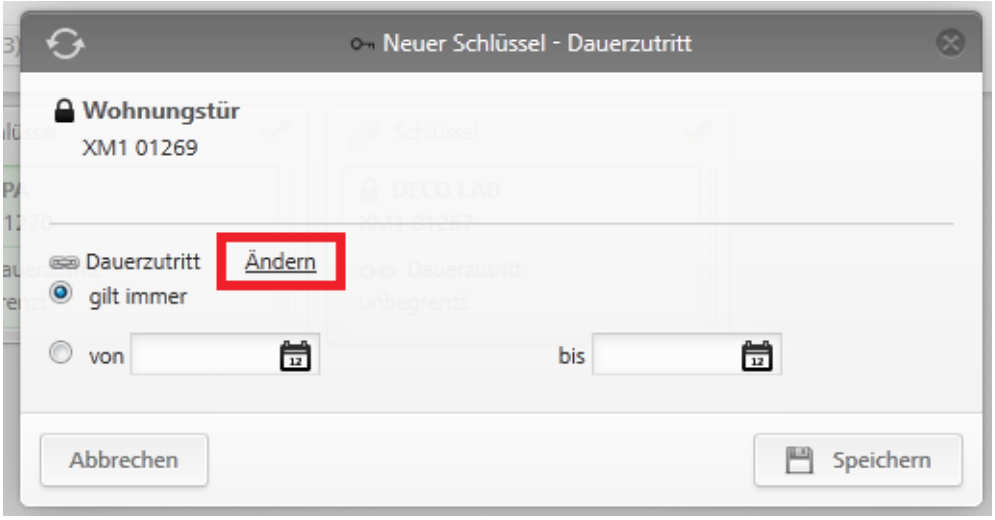


Abbildung 6.2: Problem IK7

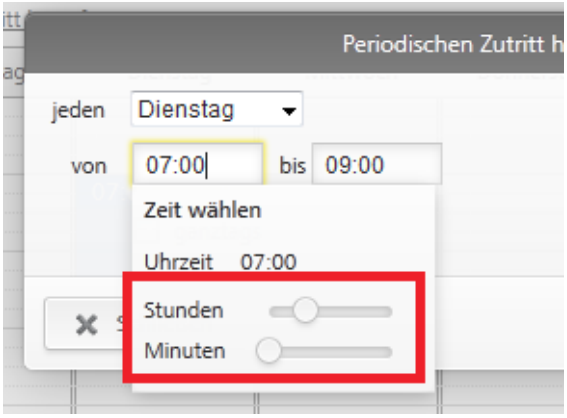


Abbildung 6.3: Problem IK8

- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Bug
- **Vorschläge zur Behebung**
  Bugfix

- **Problembeschreibung — IK8**
  Wenn die Testperson einen periodischen Zutritt mit beschränkten Tageszeiten eingibt, dann ist sie verwirrt wenn sie die Slider sieht, die die Stunden und Minuten angeben sollen. Zu sehen sind diese Slider in Abbildung 6.3.

- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Hier wird ein im Kontext „Zeiteingabe“ unklarer Skeuomorphismus verwendet, der für manche Testpersonen nicht von vornherein klar ist.
- **Vorschläge zur Behebung**
  Entweder werden die Slider komplett entfernt und nur die Möglichkeit einer textuellen Eingabe geboten, oder es werden leichter verständliche Eingabemethoden zur Verfügung gestellt. Hier bieten sich Ziffernblätter oder ein Pulldown Menü wie bei den meisten elektronischen Terminkalendern an.

- **Problembeschreibung — IK9**
  Die Testperson filtert auf der Seite der Schlüsselbundmedien nach Kriterien, die nur einen einzelnen Eintrag übrig lassen. Ein Klick auf diesen Eintrag bewirkt nichts.
- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Das ist ein schwierig reproduzierbarer Bug. Es wird nach dem gesamten Text des Feldes „Notiz“ gefiltert bis nur mehr ein Eintrag vorhanden ist. In einigen Fällen bewirkt dann ein Klick auf diesen Eintrag nichts.
- **Vorschläge zur Behebung**
  Bugfix

- **Problembeschreibung — IK10**
  Die Testperson sucht für die Lösung seiner Aufgaben in der Übersichtsliste der Schlüsselbundmedien nach dem gewünschten Medium, anstatt die Karte auf den Kartenleser aufzulegen und somit in die Kartendetails zu gelangen.
- **Häufigkeit des Auftretens**
  3 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Erstbenutzerinnen und Erstbenutzer schließen nicht automatisch darauf, dass das Legen der Karte auf den Kartenleser der schnellste Weg in die Kartendetails ist.

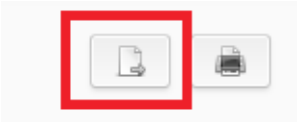


Abbildung 6.4: Problem IK11

- **Vorschläge zur Behebung**
  Wir haben während der Tests das Feedback bekommen, dass ein Quick Start Guide oder ein kleines Tutorial für einee unerfahrene Testperson sehr viel bringen würde.

- **Problembeschreibung — IK11**
  Die Testperson klickt auf ein Symbol und landet nach einem vermeintlichen Crash wieder auf der Startseite. Zu sehen ist dieses Verhalten in Abbildung 6.4.

- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Bug
- **Vorschläge zur Behebung**
  Bugfix

- **Problembeschreibung — IK12**
  Bei vielen Funktionen erwartet sich die Testperson Tooltips beim Hovern der Maus über den Funktionen, wartet aber vergeblich auf diese.
- **Häufigkeit des Auftretens**
  2 von 4 Testern
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Viele Testpersonen sind intuitiv gewohnt, dass ein Hovertext erscheint, wenn sie mit der Maus über eine Funktion fahren.
- **Vorschläge zur Behebung**
  Sinnvolle Hilfetexte in Tooltipform.

- **Problembeschreibung — IK13**
  Die Testperson doppelklickt einen Schlüssel in der Übersichtsliste des Schlüsselbundmediums und setzt damit einen Filter, ohne es zu merken. Danach wundert sich die Testperson, dass sie die restlichen Schlüssel nicht mehr sehen kann.
- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Die Tatsache, dass ein Schlüsselfilter gesetzt wurde, wird der Testperson nicht ausreichend kommuniziert.
- **Vorschläge zur Behebung**
  Ein Filtersymbol sollte angezeigt werden, wenn ein Filter gesetzt wurde.

- **Problembeschreibung — IK14**
  Die Testperson entfernt die Karte und legt sie erneut auf das Lesegerät um an das Popup-Menü zu gelangen
- **Häufigkeit des Auftretens**
  3 von 4 Testpersonen
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Die Testperson erkennt den Button zum Öffnen des Popup-Menüs nicht.
- **Vorschläge zur Behebung**
  Den Pfeil für das Aufklappen besser hervorheben. Anstatt des „eingedrückten“ Reliefdesigns ein „herrausstehendes“ Design verwenden. Die Menüpunkte entweder auslagern und das Popup-Menü komplett zu entfernen oder die Funktionalität duplizieren.

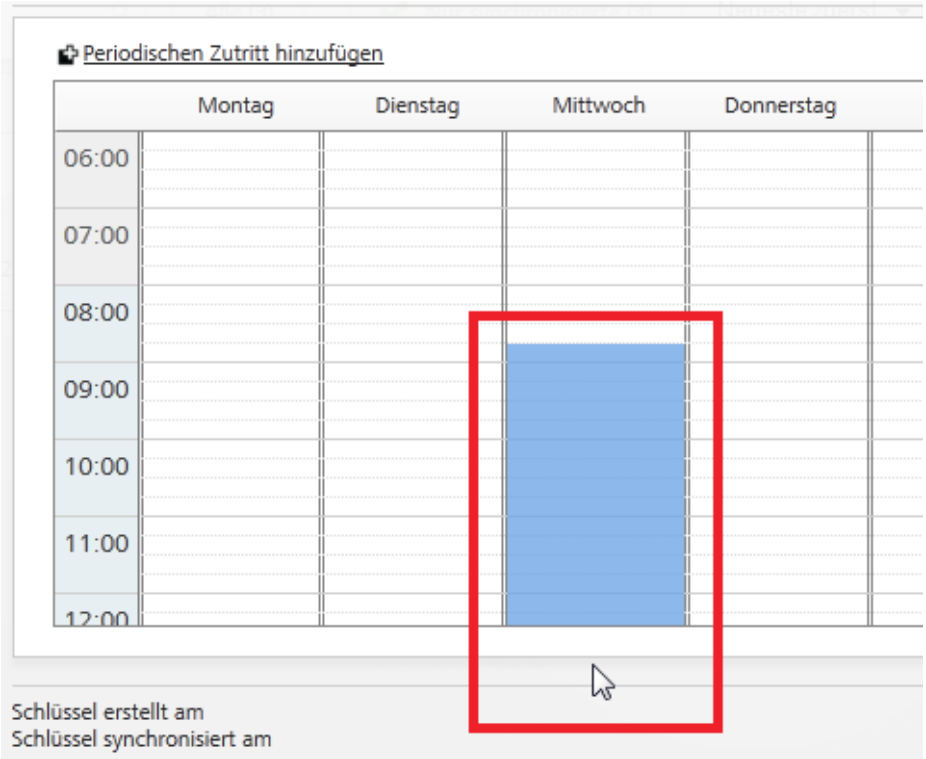


Abbildung 6.5: Problem IK15

- **Problembeschreibung — IK15**
  Die Testperson hat Probleme beim Scrollen in der Kalenderansicht beim Erstellen eines periodischen Zutritts, weil die Zeitansicht nicht mitscrollt. Problemansicht zu sehen in Abbildung 6.5.

- **Häufigkeit des Auftretens**
  4 von 4 Testpersonen
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Hier liegt vorraussichtlich eine Limitierung der Technologie (JavaScript) vor, die diese Funktionalität nicht „Out-of-the-Box“ anbietet.
- **Vorschläge zur Behebung**
  Die Tage komplett anzeigen, um das Ziehen der Zutrittszeiten zu vereinfachen. Außerdem eine Scrollfunktion implementieren.

- **Problembeschreibung — IK16**
  Bei der Suche nach einem bestimmten Schlüsselbundmedium erkennt die Testperson nicht, dass sie die Liste filtern kann.

- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Es finden sich Inkonsistenzen bei der Darstellung von Filterungsmöglichkeiten durch die Applikation. Die Filterung der SBM sieht anders aus als die Filterung der Schlüssel eines bestimmten SBMs.
- **Vorschläge zur Behebung**
  Die Darstellung der Filter über die gesamte Applikation konsistent halten.

- **Problembeschreibung — IK17**
  Die Testperson klickt auf Haupt-Menüeintrag und es passiert nichts. Beispiel: SBM
- **Häufigkeit des Auftretens**
  3 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Die Einträge sind nicht klickbar, eine Ausnahme bildet Home.
- **Vorschläge zur Behebung**
  Die Einträge gesamt klickbar oder nicht klickbar machen.

- **Problembeschreibung — IK18**
  In der Ansicht der Schlüssel eines bestimmten SBMs versucht die Testperson mittels eines Rechtsklicks zum gewünschten Ziel zu kommen.
- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Die Applikation ist leicht zu verwechseln mit einer Desktop-Applikation, nachdem viele Paradigmen und Metaphern vom Desktop ihren Weg in die Webapplikation gefunden haben.
- **Vorschläge zur Behebung**
  Es gibt hier zwei Möglichkeiten. Entweder wird das Kontextmenü komplett deaktiviert, und die Testperson realisiert mit ihrem ersten oder zweiten Klick, das ein Rechtsklick sie nicht weiterbringen wird, oder das Kontextmenü wird genutzt und mit hilfreichen Einträgen bevölkert.

Abbildung 6.6: Problem IK19

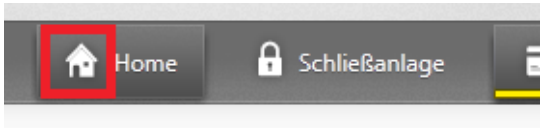


Abbildung 6.7: Problem IK20

- **Problembeschreibung — IK19**
  Die Testperson realisiert nicht, dass das Popup-Menü, mit dem die Kartendetails erreichbar sind, per Hand, oder überhaupt aufklappbar ist. Problem zu sehen in Abbildung 6.6.

- **Häufigkeit des Auftretens**
  4 von 4 Testpersonen

- **Klassifizierung**
  Kritisch

- **Mögliche Ursachen**
  Wenn noch kein einziges Medium auf den Leser gelegt wurde, ist nicht erkennbar, dass hier Funktionalität dahinter liegt.

- **Vorschläge zur Behebung**
  Entweder wird der Pfeil deutlicher hervorgehoben oder sogar bei längerer Inaktivität das Menü von selbst aufgeklappt, mit dem Hinweis „Bitte Medium auf das Lesegerät legen“ falls eine Synchronisation ausständig ist.

- **Problembeschreibung — IK20**
  Die Testperson klickt auf den obersten Menüeintrag und nichts geschieht. Nur ein Klick auf einen untergeordneten Menüeintrag bringt Erfolg.
  Beispiel: Auf das Schloss oder den Text Schließanlage zu klicken, bringt keine Reaktion. Nur wenn auf den Text „Schließzylinder“ in dem Menü, das bei einem Mouseover aufklappt, geklickt wird, passiert etwas. Besonders problematisch wird dieses Thema, da bei „Home“ dieses Verhalten inkonsistent ist. Hier ist das Symbol klickbar und bringt auch das erwünschte Resultat. Siehe dazu den Screenshot in Abbildung 6.7.

- **Häufigkeit des Auftretens**
  3 von 4 Testpersonen

- **Klassifizierung**
  Gering

Abbildung 6.8: Problem IK21.11

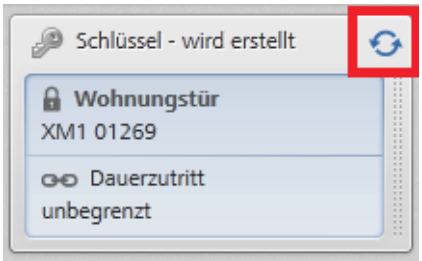


Abbildung 6.9: Problem IK21.12

- **Mögliche Ursachen**
  Wie bereits beschrieben wird von der Testperson erwartet, dass die Titelleisten klickbar sind und eine Art „Hauptmenü“ zu diesem Thema erscheint.
- **Vorschläge zur Behebung**
  Hier ist Konsistenz von höchster Priorität. Entweder werden alle Titelleisten klickbar gemacht oder alle werden unklickbar, aber mit Mouseover Menü hinterlegt.

- **Problembeschreibung — IK21**
  Die Testperson sieht das Symbol mit den zwei Pfeilen und assoziiert dieses mit „Synchronisation“. Ein Klick auf diese Symbole bringt jedoch nicht den gewünschten Erfolg. Siehe dazu die Abbildungsfolge 6.8 und 6.9.

- **Häufigkeit des Auftretens**
  4 von 4 Testpersonen
- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Das Symbol impliziert Synchronisationsaktivität, nicht die Notwendigkeit einer Synchronisation. Besonders problematisch war diese Situation bei den Testpersonen, die vor den Tests mit der Schlüsselkarte ein Mobiltelefon synchronisiert haben. Bei diesem Use Case ist das obere Symbol ein Button und bewirkt eine Synchronisation. Hier war es unumgänglich, den Testpersonen zu helfen, um den Testfall zu einem Abschluss zu bringen.
- **Vorschläge zur Behebung**
  Entweder muss hier ein anderes Symbol verwendet werden, das weniger mit Synchronisation assoziiert wird, oder die Symbole werden mit der Synchronisationsfunktionalität hinterlegt.

- **Problembeschreibung — IK22**
  Nachdem ein neuer Schlüssel erstellt wurde, erkennt die Testperson nicht, dass die Karte noch nicht synchronisiert wurde und ist der Meinung, der Schlüssel ist bereits aktiv.
- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Kritisch
- **Mögliche Ursachen**
  Es ist möglich, dass der Farbunterschied zwischen synchronisiert und nicht synchronisiert zu gering ist. Außerdem sind die verwendeten Symbole und der angezeigte Text sehr verwirrend.
- **Vorschläge zur Behebung**
  Noch deutlichere Hinweise geben, dass eine Synchronisation unbedingt notwendig ist.

- **Problembeschreibung — IK23**
  Die Testperson erkennt nicht, dass die Felder bei der Schlüsselerstellung (Dauerzutritt, periodischer Zutritt) dazu gedacht sind, Schlüssel darauf zu „droppen“.
- **Häufigkeit des Auftretens**
  1 von 4 Testern
- **Klassifizierung**
  Bedenklich
- **Mögliche Ursachen**
  Die Felder sind nicht auffällig genug gestaltet, um zu signalisieren, dass etwas auf Ihnen abgelegt werden soll.
- **Vorschläge zur Behebung**
  Bei einem begonnenen Drag eines Schlüssels könnte die restliche UI ausgegraut werden, um die Aufmerksamkeit noch mehr auf das Drop-Feld zu lenken. Weiters ist es denkbar, Pfeile anzuzeigen sobald ein Schlüssel gezogen wird, um die Richtung anzuzeigen in der der Schlüssel wandern soll.

- **Problembeschreibung — IK24**
  Die Testperson erkennt nicht, dass die Schlüssel Drag&Drop Funktionalität besitzen und verwendet diese daher nicht. Das behindert sie im Vorankommen mit der Aufgabe.
- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen
- **Klassifizierung**
  Gering

- **Mögliche Ursachen**
  Vorraussichtlich ist hier die Erfahrung der Testperson mit Web 2.0 Technologien noch nicht stark genug. Allerdings gab es auch das Feedback, dass es nicht deutlich genug angezeigt wurde, dass Drag&Drop funktioniert.

- **Vorschläge zur Behebung**
  Eine mögliche Lösung wäre, dass das Maussymbol sich beim Hovern über den Schlüsseln von dem klassischen „Klickfinger“ in ein Symbol verwandelt, dass „Greifen“ symbolisiert.

- **Problembeschreibung — IK25**
  Die Testperson hat Schwierigkeiten, mit den Begriffen SBM und SBI umzugehen. Das verwirrt sie bei der Lösung seiner Aufgaben.

- **Häufigkeit des Auftretens**
  1 von 4 Testpersonen

- **Klassifizierung**
  Gering

- **Mögliche Ursachen**
  Die Benennungen der verschiedenen Objekte und Subjekte im System sind verwirrend.

- **Vorschläge zur Behebung**
  Entweder werden die Benennungen klarer formuliert, oder ein Quick Start Guide vermittelt das notwendige Basiswissen.

- **Problembeschreibung — IK26**
  Auf der Seite der Schlüsselbundmedien erkennt die Testperson nicht, dass hier Paging Navigation verwendet wird und erwartet sich statt dessen einen Scrollbalken.

- **Häufigkeit des Auftretens**
  3 von 4 Testpersonen

- **Klassifizierung**
  Bedenklich

- **Mögliche Ursachen**
  Möglicherweise sind die Pfeile für das Paging nicht prominent genug angeordnet. Es kann auch sein, dass die Tatsache, dass die Pfeile nur am unteren Ende der Liste platziert sind, der Grund für die Verwirrung ist.

- **Vorschläge zur Behebung**
  Entweder werden die Pfeile unterhalb und oberhalb der Liste platziert, oder sie werden größer und prominenter gestaltet.

- **Problembeschreibung — IK27**
  Bei der Aufgabe, das Schließprotokoll auf einem Mobiltelefon zu interpretieren, gibt sich die Testperson mit dem Protokoll auf der „Startseite“ zufrieden. Das bedeutet, dass sie sich die Schlüssel-ID merken muss und diese dann im Protokoll sucht. Dass der Schlüssel ein separates Protokoll hat, bemerkt die Testperson erst, wenn sie aus einem anderen Grund auf den Schlüssel geklickt hat.
- **Häufigkeit des Auftretens**
  4 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Es ist nicht von vornherein klar, dass der Schlüssel ein separates Protokoll hat, das wesentlich lesbarer gestaltet ist.
- **Vorschläge zur Behebung**
  Es wäre denkbar, das Protokoll, das von der Startseite aus zugänglich ist, filterbar zu machen. Dadurch kann die Testperson, wenn sie dieses Protokoll betrachtet, nach den für sie interessanten Einträgen filtern. Weiters könnte eine Verknüpfung zum Schlüsselprotokoll implementiert werden. Wird auf einen Eintrag geklickt, stellt die App direkt das separate Protokoll dieses Schlüssels dar.

- **Problembeschreibung — IK28**
  Die Testperson realisiert nicht, dass der Schlüssel auf der Startseite der Smartphone App klickbar ist.
- **Häufigkeit des Auftretens**
  2 von 4 Testpersonen
- **Klassifizierung**
  Gering
- **Mögliche Ursachen**
  Die Testperson hat wenig Erfahrungen oder Forschungsdrang. Alternativ kann es auch sein, dass der Schlüssel nicht als „klickbar“ wahrgenommen wird.
- **Vorschläge zur Behebung**
  Eine reliefartige Darstellung des Schlüssels könnte den Drang, ihn „einzudrücken“ größer gestalten.

6.2 Bewertung der gefundenen Probleme hinsichtlich Security

In diesem Abschnitt werden die Probleme erläutert, die ein Sicherheitsrisiko darstellen können, indem sie Fehlbenutzungen der Software hervorrufen.

6.2.1 Konsistenter/Inkonsistenter Stand

Eine negative Eigenschaft des getesteten Systems ist die Art und Weise, wie Synchronisationen für Benutzer und Benutzerinnen angezeigt werden. Beispielsweise wird nicht klar genug signalisiert, dass ein erstellter Schlüssel erst mit der Karte synchronisiert werden muss. Das kann dazu führen, dass der Benutzer oder die Benutzerin Schlüssel bereits vermeintlich erstellt hat, diese aber nicht auf der Karte vorhanden sind. Wesentlich weitreichender sind die negativen Konsequenzen, wenn Berechtigungen, die seiner oder ihrer Meinung nach gelöscht wurden, nicht mehr synchronisiert werden, und auf einer Karte mehr Zutrittsberechtigungen zu belassen als er oder sie eigentlich möchte. Hierbei wird der Stand des Systems inkonsistent. Es bietet sich an, expliziter auf die notwendige Synchronisation hinzuweisen.

6.2.2 Schlüssel werden ungewollt ausgestellt

Es ist möglich, durch verschiedene Tätigkeiten Filter auf die angezeigten Schlüssel zu setzen. Somit nicht mehr alle Schlüssel sichtbar, die bereits vorhanden sind. Das kann dazu führen, dass mehr Zutrittsberechtigungen ausgestellt werden als eigentlich gewünscht. Des Weiteren wird der Benutzer oder die Benutzerin glauben, dass Berechtigungen gelöscht sind, weil sie nicht mehr in der Maske aufscheinen, dabei ist nur ein Filter gesetzt, der diese ausblendet. Hier bietet es sich an, expliziter auf die gesetzten Filter hinzuweisen.

Allgemein ist zu sagen, dass das getestete System in mehreren Punkten des UI Designs Verbesserungsmöglichkeiten birgt, die stärker präsentieren können, dass es sich hier um ein System handelt, dass hohen Sicherheitsstandards entspricht.

7 Fazit

I may not have gone where I intended to go, but I think I have ended up where I needed to be.
Douglas Adams, The Long Dark Tea-Time of the Soul

7.1 Zusammenfassung

In dieser Arbeit wurden zu Beginn das zu testende System Sunrise (heute AirKey) vorgestellt und die grundlegenden Funktionen erläutert. Danach wurden die methodischen und theoretischen Grundlagen für die folgenden Studien erläutert. Das Thema Usability wurde präsentiert, der Begriff definiert. Usability Engineering wurde anhand von ISO Standards definiert und eine Auswahl an verschiedenen Methoden für Usability Engineering und Usability Testing vorgestellt (*Thinking Aloud*, *Between/Within Subjects Testing*, *System Usability Scale*).
Das Thema Trust wurde präsentiert. Die Hauptcharakteristika von Trust wurden vorgestellt (Fähigkeit, Wohlwollen, Integrität). Es wurden Faktoren, die Trust erzeugen und verstärken (Erfahrungen des Trustor, Reputation des Trustee, Umstände der Situation, in der Trust erforderlich ist, usw.) aufgezeigt und analysiert. Techniken, mit denen es möglich ist, Trust zu messen, wurden vorgestellt (ITS, TAM).
Die praktischen Arbeiten bestanden aus einem Experiment, das eine Baseline für Trust - verschiedenen Schliesszylinderarten gegenüber - etablieren sollte, sowie einer Usability Studie. Die Ergebnise und Findings der Usability Studie wurden präsentiert, die Usabilityprobleme aufgezeigt und - wo notwendig - Lösungsvorschlägen vorgestellt.

7.2 Forschungsfragen

In dieser Arbeit wurden die zwei folgenden Forschungsfragen gestellt.

1. Existiert eine Verbindung zwischen Trust und Security?
2. Ist es möglich, ein System gleichzeitig sicher und benutzbar zu designen?

Um diese Fragen zu beantworten, wurden Theorieforschung betrieben und zwei Experimente durchgeführt.

7.2.1 Trust und Security

Die Definition von Trust ist auch nach der Analyse in dieser Arbeit weiterhin als sehr subjektiv einzustufen. Menschen reagieren auf verschiedene Signale und Symbole, die Trust hervorrufen

können, sehr unterschiedlich. Aus diesem Grund wurde für den Kontext von Schließmechanismen eine Studie entworfen, die eine Basis für weitere Forschungen bieten soll.

Eine Online Umfrage *Between Subjects* mit n=317 Teilnehmern hat grundlegende Vertrauenswerte bei zufällig ausgewählten Testpersonen abgefragt. Die Bewertungen und auch Kommentare der Testpersonen geben Aufschluss über die Einschätzung der drei getestete Sperrmechanismen. So ist zu sehen, dass ältere Menschen eher dazu neigen, elektrischen Schließmechanismen wesentlich weniger zu vertrauen als junge Menschen. Hohe Security korreliert nur dann mit hohem Vertrauen, wenn der Benutzer oder die Benutzerin bereits Erfahrungen mit den zu vertrauenden Systemen haben. In einigen Fällen reicht auch der Vergleich mit ähnlichen Systemen. Als Beispiel sei hier der Vergleich zwischen elektrischen Schlössern in Hotels und dem elektrischen Zylinder aus dem Test genannt.

Für eine Erweiterung des TAM bedeutet das, dass es eine Korrelation zwischen Trust und Security gibt, auf die aufgebaut werden kann.

Die erste Forschungsfrage ist daher mit „Ja“ zu beantworten. Anhand der Ergebnisse der Online Umfrage lässt sich erkennen, dass schwache Security mit niedrigem Trust korreliert. Der Umkehrschluss ist nicht im selben Maß ausgeprägt zu beobachten. Es wird angenommen, dass weitere Forschung in diese Richtung die angesprochene Korrelation weiter belegen kann.

Die Ergebnisse der Studie wurden nicht nur numerisch ausgewertet, sondern auch die zusätzlichen Kommentare der Testpersonen ausgewertet und analysiert. Dabei haben sich Korrelationen zu den theoretischen Definitionen von Trust gezeigt. Beispielsweise wurden die Signale, die ein Schließzylinder von sich gibt (sowohl akustisch als auch visuell) von den Testpersonen dazu verwendet, ihren Trust dem Zylinder gegenüber einzustufen. Daher ist ein Vorschlag, den die Ergebnisse dieser Arbeit nahelegen, die Signale des elektrischen Zylinders dahingehend zu bearbeiten, dass sie näher an modernen Sicherheitszylindern angelehnt sind als dies aktuell der Fall ist.

Die Ergebnisse legen weiterhin nahe, dass die Mehrheit der Testpersonen, die einem neuartigen Schloss vertrauen, bereits Erfahrungen mit einem solchen oder ähnlichen Schloss gemacht haben. Das legt den Schluss nahe, dass eine größere Durchdringung mit elektrischen Schlössern mehr Trust in der Bevölkerung bedingen wird. Mehr Durchdringung bedeutet, dass mehr Erfahrungen gemacht werden, was wiederum bedeutet, dass Menschen den Schlössern mehr vertrauen. Über den Zeitraum dieser Annahme wird in dieser Arbeit keine Aussage getroffen, hier bietet sich eine erweiterte Variante des TAM an, um nähere Informationen zu erhalten.

7.2.2 Usability

Anhand von ISO-Standards wurden Kriterien vorgestellt, die zur Bewertung von Softwareverwendbarkeit herangezogen werden können. Weiters wurde der theoretische Unterbau für den praktischen Usabilitytest erarbeitet.

Der Usabilitytest wurde *Within Subjects* mit freiwilligen Teilnehmern und Teilnehmerinnen an der Technischen Universität Wien durchgeführt. Hier haben sich in den Ergebnissen große Variationen zwischen der technischen Vorbildung der Testpersonen gezeigt. Allerdings konnte bereits nach dem ersten erfolgreich durchgeführten Test eine Nivellierung dieser Ungleichheit beobachtet werden. Diese Beobachtung lässt den Schluss zu, dass die Bedienung des Systems mit wenig Einarbeitungsaufwand zu erlernen ist.

Die SUS wird percentil-basiert anhand einer Kurve bewertet. Für eine Bewertung „A“ ist ein Score von mindestens 80,6 notwendig. Ein SUS Score von 77 Punkten, der im Test erreicht wurde, ist ein deutlich überdurchschnittliches Ergebnis, das schon sehr nahe an die Bestnote reicht. Das System ist damit als benutzbar einzustufen.

Es wurden aber sehr wohl auch sicherheitskritische Probleme während des Tests identifiziert, die inkonsistente Systemzustände zur Folge haben. Für jedes dieser Probleme wurde eine Lösung vorgeschlagen, die die Verwendbarkeit des Systems nicht einschränkt. Die zweite Forschungsfrage ist daher mit „Ja“ zu beantworten.

In Verknüpfung mit 7.2.1 ist zu erwähnen, dass *Thinking Aloud* sehr ähnliche Ansätze verfolgt, wie das freie Kommentarfeld in einer Umfrage. Es war auch bei dieser Befragung sehr wertvoll, die Gedankengänge der Befragten verfolgen zu können.

7.3 Ausblick

Für weitere Forschung bietet sich ein Fragebogen anhand eines um die Dimension Trust erweiterten TAM an. Diese Fragebögen haben das Potential, sehr präzise vorherzusagen, ob die Zielgruppe eines neuen Produkts dieses auch wirklich verwenden wird. Es ist ebenfalls denkbar, dass TAM um eine Zeitkomponente zu erweitern und abzufragen, wie lange befragte Personen die Dauer einschätzen, bis sie der abgefragten Technologie hinreichend vertrauen. Außerdem hat die durchgeführte Umfrage gezeigt, dass in Bereichen, die stark mit der psychologischen Struktur des Menschen zu tun haben, ein Kommentarfeld für freie Assoziationen ohne jegliche Richtungsvorgabe der Fragenden äußerst wertvolle Einblicke in die Gedankenprozesse der Befragten liefert. Es wird an dieser Stelle empfohlen, bei weiteren Forschungen nach Maßgabe der Umstände diese Tatsache zu beachten und die Gedanken der Teilnehmerinnen und Teilnehmer abzufragen. Eine weitere Idee für zukünftige Arbeit ist, das Experiment zu wiederholen und andere Faktoren gleich zu belassen bzw. zu ändern. War bei diesem Experiment die einzige Konstante die Tür, so lässt sich leicht ein Versuchsaufbau vorstellen, bei dem der Schliessmechanismus gleich bleibt, aber drei verschieden stabil wirkende Türen verwendet werden. Auf dieselbe Geräuschkulisse zu achten ist ebenfalls ein Vorschlag für Future Work.

Die Ergebnisse legen für den Kontext von elektrischen Schließzylindern folgenden Schluss nahe: Gute Benutzbarkeit der Verwaltungssoftware gemeinsam mit Schließzylinderdesign, das dem Benutzer vertraut erscheint, können ein starkes Gefühl des Vertrauens hervorrufen. Dieses Gefühl exisitiert ungeachtet dessen, ob der Zylinder wesentlich sicherer oder weniger sicher ist als ein herkömmliches Sicherheitsschloss.

Literatur

Referenzen

Apple Inc. (2014a). *Apple Maps*. URL: https://www..apple.com/ios/maps/ (besucht am 14. 07. 2014).

— (2014b). *OS X Human Interface Guidelines*. URL: https://developer.apple.com/library/mac/documentation/UserExperience/Conceptual/AppleHIGuidelines/Intro/Intro.html#//apple_ref/doc/uid/20000957 (besucht am 14. 07. 2014).

Brooke, John (1996a). "SUS: A quick and dirty usability scale". In: *Usability evaluation in industry*. Hrsg. von P. W. Jordan u. a. London: Taylor und Francis.

— (1996b). "SUS-A quick and dirty usability scale". In: *Usability evaluation in industry* 189, S. 194.

— (2013). "SUS: A Retrospective". In: *Journal of Usability Studies* 8.2, S. 29–40. URL: http://www.upassoc.org/upa_publications/jus/2013february/brooke2.html (besucht am 14. 07. 2014).

Compeau, Deborah R. und Christopher A. Higgins (1995). "Computer self-efficacy: development of a measure and initial test". In: *MIS Q.* 19.2, S. 189–211. ISSN: 0276-7783. DOI: 10.2307/249688. URL: http://dx.doi.org/10.2307/249688.

Coventry, Lynne (2005). "Usable Biometrics". In: *Security and Usability. Designing Secure Systems that People Can Use*.

Davis, Fred D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology". In: *MIS Q.* 13.3, S. 319–340. ISSN: 0276-7783. DOI: 10.2307/249008. URL: http://dx.doi.org/10.2307/249008.

Dumas, Joseph F. und Janice C. Redish (1993). *A Practical Guide to Usability Testing*. Westport, CT, USA: Greenwood Publishing Group Inc. ISBN: 089391990X.

Erste Bank AG (2014). *Erste Bank mobiles Netbanking*. URL: http://www.gartner.com/newsroom/id/2237315 (besucht am 14. 07. 2014).

EVVA Sicherheitstechnologie GmbH (2014). *AirKey Systemüberblick*. URL: http://www.evva.at/produkte/elektronische-schliesssysteme-zutrittskontrolle/airkey/systemueberblick/de/ (besucht am 14. 07. 2014).

Fishbein, M. und I. Ajzen (1975). *Belief, attitude, intention, and behavior: an introduction to theory and research*. Addison-Wesley series in social psychology. Addison-Wesley Pub. Co. ISBN: 9780201020892. URL: http://books.google.com/books?id=8o0QAQAAIAAJ.

Gartner Inc. (2014). *Market Share: Mobile Phones by Region and Country, 3Q12, Press Release*. URL: https://developer.apple.com/library/mac/documentation/UserExperience/Conceptual/AppleHIGuidelines/Intro/Intro.html#//apple_ref/doc/uid/20000957 (besucht am 14. 07. 2014).

Google Inc. (2014a). *Android Design Guidelines*. URL: http://developer.android.com/design/index.html (besucht am 14. 07. 2014).

— (2014b). *Elektronisches bezahlen mit Google Wallet*. URL: https://wallet.google.com (besucht am 14. 07. 2014).

Hodgekiss, Ros (2014). *Marktanteile an gesendeten E-Mails iOS vs. Android*. URL: http://www.campaignmonitor.com/blog/post/3843/apple-leads-email-client-market-share-but-android-gains-ground (besucht am 14. 07. 2014).

Hofstede, Geert (1984). *Culture's Consequences: International Differences in Work-Related Values*. en. SAGE. ISBN: 9780803913066.

Hofstede, Geert (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*. en. SAGE. ISBN: 9780803973244.

ISO (1998a). *ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability*. Englisch. URL: http://www.it.uu.se/edu/course/homepage/acsd/vt09/ISO9241part11.pdf.

— (1998b). *ISO 9241-12:1998, Ergonomic requirements for office work with visual display terminals (VDTs) – Part 12: Presentation of information.* Englisch. ISO.

— (1998c). *ISO 9241:1998, Ergonomic requirements for office work with visual display terminals (VDTs)*. Englisch. ISO.

— (2006). *ISO 9241-110:2006, Ergonomic requirements for office work with visual display terminals (VDTs) – Part 10: Dialogue principles.* Englisch. ISO.

Jackson, Sherri (2012). *Research Methods and Statistics: A Critical Thinking Approach*. Wadsworth CENGAGE Learning. ISBN: 1111346550.

Jermyn, Ian u. a. (1999). "The design and analysis of graphical passwords". In: *Proceedings of the 8th USENIX Security Symposium*, S. 1–14. URL: http://www.usenix.org/events/sec99/full_papers/jermyn/jermyn.pdf (besucht am 14. 07. 2014).

Just, Mike (2005). "Usable Biometrics". In: *Security and Usability. Designing Secure Systems that People Can Use*.

Kaasinen, Eija (2007). "User acceptance of mobile Internet services". In: *Proceedings of the Workshop on Mobile Internet User Experience*. URL: http://research.nokia.com/files/Kaasinen-Acceptance.pdf.

Kindberg, Tim u. a. (2008). "Measuring Trust in Wi-Fi Hotspots". In: *CHI 2008 Proceedings · Trust and Security*. URL: http://dl.acm.org/ft_gateway.cfm?id=1357084&ftid=498844&dwn=1&CFID=236572544&CFTOKEN=22876761.

Lange, Martin und Gareth Ellen (2011). "From armed to charmed". In: *Preparing and profiting from the new mobile-enabled point of sale*.

Lewis, Clayton und John Rieman (1994). *Task-Centered User Interface Design:A Practical Introduction*. URL: http://hcibib.org/tcuid/.

Lewis, James R. und Jeff Sauro (2009). "The factor structure of the system usability scale". In: *Human Centered Design*. Springer, S. 94–103. URL: http://link.springer.com/chapter/10.1007/978-3-642-02806-9_12.

Luhmann, Niklas (1979). *Trust and Power*. John Wiley und Sons Ltd. ISBN: 0471997587.

McCue, Andy (2014). *Is your cat a target for password-stealing hackers?* URL: http://www.zdnet.com/is-your-cat-a-target-for-password-stealing-hackers-3040145995/ (besucht am 14. 07. 2014).

Merriam-Webster's English Dictionary Trust (2014). URL: http://www.merriam-webster.com/dictionary/trust (besucht am 14. 07. 2014).

Mohamed, Abdul Hakim HM u. a. (2011). "e-HTAM: A Technology Acceptance Model for electronic health". In: *Innovations in Information Technology (IIT), 2011 International Conference on*, S. 134–138. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5893804.

Moore, Gary und Izak Benbasat (1991). *Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation*.

Nielsen, Jakob (1992). "The usability engineering life cycle". In: *Computer* 25.3, S. 12–22. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=121503.

— (1993). *Usability Engineering*. en. Morgan Kaufmann. ISBN: 9780125184069.

— (2000). *Why you only need to test with 5 users*. URL: http://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/ (besucht am 14. 07. 2014).

— (2001). *Ten Usability Heuristics – Heuristic Number 5: Error prevention*. URL: http://www.nngroup.com/articles/ten-usability-heuristics/ (besucht am 14. 07. 2014).

Piazzalunga, Ugo, Paolo Salvaneschi und Paolo Coffetti (2005). "The Usability of Security Devices". In: *Security and Usability. Designing Secure Systems that People Can Use*.

Renaud, Karen (2005). "Evaluating Authentication Mechanisms". In: *Security and Usability. Designing Secure Systems that People Can Use*.

Research Industrial Systems Engineering (RISE) GmbH (2014). *Benutzerhandbuch Administrator Working Draft MS5*.

Rotter, Julian B. (1967). "A new scale for the measurement of interpersonal trust1". In: *Journal of personality* 35.4, S. 651–665. URL: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6494.1967.tb01454.x/abstract.

Rubin, Jeffrey (1994). *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. Hrsg. von Theresa Hudson. New York, NY, USA: John Wiley & Sons, Inc. ISBN: 0471594032.

Sasse, Martina Angela (2005). "Usability and trust in information systems". In: URL: http://discovery.ucl.ac.uk/20346/.

Silver, Hayley (2013). *Trust symbols are a key factor driving a customer's willingness to purchase*. URL: http://www.bizrateinsights.com/blog/2013/09/23/trust-symbols-are-a-key-factor-driving-a-customers-willingness-to-purchase/ (besucht am 14. 07. 2014).

SurveyMonkey (2014). *SurveyMonkey*. URL: https://www.surveymonkey.com/ (besucht am 14. 07. 2014).

Venkatesh, Viswanath und Hillol Bala (2008). "Technology acceptance model 3 and a research agenda on interventions". In: *Decision sciences* 39.2, S. 273–315. URL: http://onlinelibrary.wiley.com/doi/10.1111/j.1540-5915.2008.00192.x/full.

Venkatesh, Viswanath und Fred D. Davis (2000). "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies". In: *Manage. Sci.* 46.2, S. 186–204. ISSN: 0025-1909. DOI: 10.1287/mnsc.46.2.186.11926. URL: http://dx.doi.org/10.1287/mnsc.46.2.186.11926.

Venkatesh, Viswanath, Gordon Davis und Fred Davis (2003). *User Acceptance of Information Technology*.

Visa Europe (2014). *Verified by VISA Sample Image*. URL: http://www.visaeurope.com/en/cardholders/verified_by_visa.aspx (besucht am 14. 07. 2014).

Wade, Lydia und Rosie Robinson (2012). "The Psychology of Trust and its relation to sustainability". In: *Global Sustainability Institute Briefing Note*.

Webster, Jane und Joseph J. Martocchio (1992). "Microcomputer playfulness: development of a measure with workplace implications". In: *MIS Q.* 16.2, S. 201–226. ISSN: 0276-7783. DOI: 10.2307/249576. URL: http://dx.doi.org/10.2307/249576.

A Testplan

An dieser Stelle wird der verwendete Testplan in unveränderter Form wiedergegeben.

A.1 Testziel

A.1.1 Allgemeines

Sunrise ist ein Schlüsselverwaltungssystem, welches sowohl aus einem Webinterface, als auch aus Schlössern besteht. Die Schlösser können entweder mit speziellen Karten als auch mit NFC Mobiltelefonen gesperrt werden. Die Komponenten von Sunrise sind:

- Webinterface mit einer Administrationsrolle (SUA) welche die Mandanten verwaltet
- Webinterface des Mandanten (SSO) selbst in welcher Personen, Schlösser und Sperrberechtigungen verwaltet werden
- Sunrise Zylinderschloss
- NFC fähiges Mobiltelefon mit Sunrise App
- Schlüsselkarte

Sunrise bietet eine Vielzahl an Rollen und Funktionalitäten. Da allerdings viele dieser Operationen Verwaltungsoperationen sind, ist es sinnvoll, sich für einen Usabilitytest auf die Kernfunktionalitäten zu beschränken:

- Verwaltung von Sperrberechtigungen des SSOs
- Verwendung der App auf dem Mobiltelefon
- Interaktion mit dem Schloss mittels Karte und Mobiltelefon

Ziel des Tests ist es eventuelle Usabilityprobleme des Systems aufzudecken und – soweit innerhalb des Tests möglich – Lösungen zu erarbeiten.

A.1.2 Einschränkungen

Da es sich um einen Usabilitytest handelt, werden vor allem Usabilityprobleme erkannt werden. Laut wissenschaftlichen Erkenntnissen ist dafür nur eine geringe Anzahl von Testpersonen (maximal 5) notwendig.

Daher liefert der Usabilitytest:

- keine quantitativen Werte über Kaufwilligkeit, mögliche Preisgestaltung oder andere Marketingdaten

- keine absoluten Aussagen über die Performance (benötigte Zeit) für die Erfüllung bestimmter Aufgaben
- keine Aussagen über die Performance oder Stabilität des Systems

A.2 Testzeitraum

Der Zeitaufwand für einen Test wird mit etwa 45 Minuten pro Testperson veranschlagt. Um genügend Spielraum für die Vor- bzw. Nachbereitung zu lassen, beträgt ein Zeitslot eine Stunde.

A.3 Testort

Als Testort dient die Bibliothek der Forschungsgruppe für Industrielle Software (INSO) in der Wiedner Hauptstraße 76/2, 2. Stock, 1040 Wien. Dieser Raum ist ca. 30 qm groß und bietet ein akustisch ungestörtes Umfeld.

A.4 Ressourcen

Die Interviews und Testcases vor Ort werden von 2 Testleitern durchgeführt.

Zusätzlich werden folgende Ressourcen benötigt:

- 1 Laptop mit externer Maus und Verbindung zum Sunrise Produktivsystem
- 1 USB Kartenleser, der sowohl mit Schlüsselkarten als auch Mobiltelefonen arbeiten kann
- 2 personalisierte Sunrise Schlüsselkarten (1 als Reserve)
- 2 Android Smartphones mit vorinstallierter App sowie einbuchbaren SIM Karten mit ausreichendem Datenvolumen. Zusätzlich müssen die SIM Karten personalisiert und wie die Schlüsselkarte einem Mandanten zugewiesen sein (1 als Reserve)
- Diktiergerät
- Stoppuhr

A.5 Zielgruppe

Da Sunrise voraussichtlich sowohl für Privatnutzer als auch für KMUs eingesetzt werden soll, ist keine besondere Selektion für die Zielgruppe erforderlich. Um Verfälschungen durch eventuelle Erstbenutzer von Smartphones zu vermeiden, werden für die Tests der Mobiltelefone nur Testpersonen, welche ein Smartphone besitzen (Marke gleichgültig) rekrutiert.

A.6 Methodik

Der Test besteht aus folgenden drei Phasen:

- Pre-Test Interview
- Testcases
- Post-Test Interview

A.6.1 Pilottest

Zusätzlich wird vor Beginn der Tests ein so genannter Pilottest durchgeführt. Dabei wird mit einer Testperson, die **nicht** dem Testsample entnommen wurde, der gesamte Testablauf vor Ort einmal durchgeführt. Der Pilottest dient der formalen Verifikation sowie der Ermittlung so genannter Benchmarkzeiten. Dabei handelt es sich um Richtwerte über ungefähr zu erwartende Zeiten für die Absolvierung einzelnen Testcases. Die Ergebnisse des Pilottests fließen nicht in die Evaluierungsergebnisse ein, werden aber gesondert ausgewiesen. Für jede Testgruppe (SSO, SBI) wird ein gesonderter Pilottest mit jeweils einer anderen Testperson durchgeführt.

A.6.2 Pre-Test Interview

Da sich zur Beantwortung offener Fragestellungen ein persönliches Interview besser als ein Fragebogen eignet, wird vor der eigentlichen Ausführung der Testcases ein Pre-Test Interview durchgeführt.

Zusammenfassend sind die Ziele des Pre-Test Interviews die Feststellung der Ausgangssituation und die Vorbereitung auf die Ausführung der Testcases. Vorkenntnisse und Erfahrungen rund um die Technologien werden festgehalten. Bei der Auswertung und Interpretation der Ergebnisse spielen diese Daten eine wichtige Rolle.

A.6.3 Testcases

Die eigentlichen Benutzertests erfolgen mittels Testcases. Dabei handelt es sich um atomare Aufgaben, die die Funktionen des Systems möglichst weit abdecken sollen. Die Testpersonen werden vor Absolvierung der Testcases dazu aufgefordert, ihre Gedanken während der Tests fortlaufend laut zu äußern. Bei dieser so genannten **„Thinking Aloud“** Methode können tiefere Einblicke in Abläufe und eventuelle Probleme gewonnen werden als dies alleine durch Post-Test Interviews möglich ist. Als Endgeräte verwenden die Testpersonen ein von der Testleitung zur Verfügung gestelltes Mobiltelefon. Im Testlabor liegen außerdem Ersatzgeräte und -SIMs für allfällige Störungen bereit. Für den Webteil wird ein handelsüblicher Laptop mit externer Maus und Verbindung zum Testsystem verwendet.

A.6.4 Detailbeschreibung der Testcases

Nachfolgend werden die Testcases mit allen Eckdaten beschrieben, wie Sie während der Benutzertests Anwendung finden und den Testpersonen vorgelegt werden. Generell wird den Testpersonen bei den Testcases keine bestimmte Vorgehensweise vorgegeben. Die Entscheidung, auf welche Art eine Aufgabe gelöst wird, liegt bei den Teilnehmern der Studie. Bei allen SSO Testcases sind die Teilnehmer bereits eingeloggt und befinden sich auf der Startseite des Systems.

A.6.5 Counterbalancing

Um den Einfluss von Lerneffekten auf die Ergebnisse der Evaluierung zu vermeiden, wird die Reihenfolge der Testcases mit der Latin Square Methode ausbalanciert (sog. Counterbalancing). Jede Testperson führt die Aufgaben in einer anderen Reihenfolge aus, somit werden eventuell auftretende Lerneffekte gleichmäßig verteilt.

- **Testcase U1**
  - **Aufgabe:** Aufsperren eines Schlosses mit Karte – Sperrberechtigung vorhanden
  - **Vorbedingung:** Testkarte enthält enthält gültige Zutrittsberechtigung, Schloss geschlossen
  - **Aufgabe Endzustand:** Testkarte enthält enthält gültige Zutrittsberechtigung, Schloss geöffnet
  - **Formulierung für die Testperson:** „Stellen Sie sich vor, dass es sich bei diesem Schloss um Ihre Wohnungstüre handelt. Versuchen Sie, das Schloss mit ihrer Karte zu öffnen.“
- **Testcase SSO1**
  - **Aufgabe:** Erstellen eines Dauerzutritts & Synchronisieren auf Karte
  - **Vorbedingung:** Person Hans Test ist im System vorhanden, hat keinen Zutritt für den Testzylinder, Testzylinder „Wohnungstür“ vorhanden.
  - **Aufgabe Endzustand:** Person Hans Test hat einen unbegrenzten Dauerzutritt für den Testzylinder
  - **Formulierung für die Testperson:** „Sie entschließen sich, einen Mitbewohner (Herrn Hans Test) auf unbestimmte Zeit bei sich aufzunehmen. Verwenden Sie Sunrise, damit Herr Test die Wohnungstür mit seiner Karte aufsperren kann.“
- **Testcase SSO2**
  - **Aufgabe:** Erstellen eines periodischen Zutritts & Synchronisieren auf Karte
  - **Vorbedingung:** Person Ida Test ist im System vorhanden, hat keine Zutritte für den Testzylinder, Testzylinder “Wohnungstür” vorhanden
  - **Aufgabe Endzustand:** Person Ida Test hat einen periodischen Zutritt für den Testzylinder (1.10-15.10. jeden Montag ganztags, Mittwochs 10:00-12:00, Freitags 08:00-17:00).
  - **Formulierung für die Testperson:** „Sie möchten auf Urlaub fahren. Ihre Freundin Ida Test erklärt sich dazu bereit, Ihre Pflanzen zu gießen und ihre Fische zu füttern. Dazu benötigt Sie einen Zutritt zu folgenden Zeiten zu Ihrer Wohnung:
- Montags ganztags
- Mittwochs zwischen 10:00 und 12:00
- Freitags zwischen 08:00 und 17:00
Verwenden Sie Sunrise, damit Ida die Wohnungstür mit Ihrer Karte aufsperren kann.“
- **Testcase SSO3**
  - **Aufgabe:** Synchronisieren eines Mobiltelefons per SMS
  - **Vorbedingung:** Person Stefan Test ist im System vorhanden aber nicht auf dem Mobiltelefon synchronisiert

  - **Aufgabe Endzustand:** Person Stefan Test hat einen synchronisierten Dauerzutritt auf dem Mobiltelefon
  - **Formulierung für die Testperson:** „Sie möchten ihrem Freund, Stefan Test ermöglichen, sie jederzeit in Ihrer Wohnung zu besuchen. Allerdings ist Stefan gerade im Ausland. Verwenden Sie Sunrise, um ihm trotzdem den Zutritt mithilfe seines Handys zu ermöglichen.“

- **Testcase SSO4**
  - **Aufgabe:** Deaktivieren eines Mediums
  - **Vorbedingung:** Karte Richard Test ist nicht deaktiviert, hat gültigen Dauerzutritt für Testzylinder
  - **Aufgabe Endzustand:** Karte von Richard Test ist im System deaktiviert
  - **Formulierung für die Testperson:** „Ihr Mitbewohner Richard Test hat seine Karte verloren! Verwenden Sie Sunrise, um sicherzustellen dass niemand diese Karte mehr verwenden kann.“

- **Testcase SBI1**
  - **Aufgabe:** Aktualisieren der Sperrberechtigungen
  - **Vorbedingung:** Mobiltelefon hat keinen gültigen Zutritt für Testzylinder, Sperrberechtigung ist im Backend vorhanden aber nicht auf dem Mobiltelefon synchronisiert
  - **Aufgabe Endzustand:** Mobiltelefon hat gültigen Zutritt für Testzylinder
  - **Formulierung für die Testperson:** „“Sie möchten Ihre Bekannte, Julia Test besuchen. Allerdings sind sie zu früh bei Julia und sie ist noch nicht zuhause. Sie hat Ihnen allerdings einen Schlüssel ausgestellt. Überprüfen Sie, ob Sie den Schlüssel bereits auf Ihrem Mobiltelefon haben und holen Sie Ihn sich wenn nötig ab.“

- **Testcase SBI2**
  - **Aufgabe:** Aufsperren eines Schlosses mit dem Mobiltelefon
  - **Vorbedingung:** Mobiltelefon hat gültigen Zutritt für Testzylinder
  - **Aufgabe Endzustand:** Testzylinder geöffnet
  - **Formulierung für die Testperson:** „Versuchen Sie, das Schloss mit Hilfe des Mobiltelefons zu öffnen.“

- **Testcase SBI3**
  - **Aufgabe:** Aussage über Öffnungszeiten eines bestimmten Schlosses treffen
  - **Vorbedingung:** Mobiltelefon hat gültigen periodischen Zutritt für Testzylinder
  - **Aufgabe Endzustand:** Testperson trifft korrekte Aussage
  - **Formulierung für die Testperson:** „“Ihre Bekannte Julia Test hat Ihnen einen Schlüssel zu ihrer Wohnung geschickt, damit Sie in Julias Abwesenheit die Blumen gießen können. Bringen Sie mittels Sunrise in Erfahrung, wann bzw. wie lange Sie Zutritt zu Julias Wohnung haben.“

- **Testcase SBI4**
  - **Aufgabe:** Aussage über Zutritt mittels Protokoll treffen

- **Vorbedingung:** Mobiltelefon hat mindestens einen Protokolleintrag über Zutritt zu Testzylinder
- **Aufgabe Endzustand:** Testperson trifft korrekte Aussage
- **Formulierung für die Testperson:** „In die Wohnung Ihrer Freundin Julia Test wurde während ihres Urlaubs eingebrochen! Sie können sich erinnern, dass bei Ihrem letzten Besuch noch alles in Ordnung war. Versuchen Sie den genauen Zeitpunkt Ihres letzten Besuches zu nennen um der Polizei die Ermittlungen zu erleichtern."

A.6.6 Post-Test Interview

Nach dem Durchlauf aller Testcases wird ein Post-Test Interview (siehe Anhang 7.5 Post-Test Interview) durchgeführt. Ziel des Interviews ist es, möglichst viele subjektive Meinungen der Testpersonen zu erheben. Das Post-Test Interview besteht teilweise aus einer angepassten Version der System Usability Scale1 (SUS) und teilweise aus offenen Fragen. Die SUS ermöglicht es, einen Usability Index zum Vergleich verschiedener Systeme zu erstellen. Um präzisere Antworten zu erhalten, wird eine so genannte forced-choice scale verwendet, d.h. zu jeder Frage muss eindeutig Stellung bezogen werden. Dadurch werden zusätzlich ausführlichere Antworten der Testpersonen provoziert die tiefere Einblicke in eventuelle Probleme ermöglichen. Wie auch beim Pre-Test Interview werden alle Fragen (auch die der SUS) offen gestellt und nur bei Unklarheiten eingegrenzt. Dies führt ebenfalls zu besseren Ergebnissen und zusätzlichen Informationen.

A.7 Appendix

A.7.1 Begrüßungstext (mündlich)

Sehr geehrte/r Frau/Herr .....

wir sind ein Team von der Forschungsgruppe Industrial Software der Technischen Universität Wien und führen eine Untersuchung eines neuartigen Systems namens Sunrise durch. Bei Sunrise handelt es sich um ein System, welches es erlaubt Türschlösser sowohl mittels elektronischer Karten als auch mittels Mobiltelefonen aufzuschließen. Das System erlaubt auch eine Vielzahl von Konfigurationsmöglichkeiten durch den Benutzer. Ziel unserer Untersuchung ist es, herauszufinden inwieweit Benutzer einige Funktionalitäten von Sunrise bedienen können und wo es noch Verbesserungspotential gibt.

Bitte seien Sie sich darüber im Klaren, dass bei diesem Test nicht Ihre Fähigkeiten getestet werden sondern Sunrise überprüft wird. Sie können dabei keine Fehler machen. Falls Probleme auftreten, liegt es an Mängeln des Systems.

Der Test besteht aus drei Teilen:

- Wir beginnen mit einem Interview, indem wir Ihre Bedürfnisse, Vorlieben und Vorkenntnisse rund um das zu testende Produkt erheben möchten.

- Im zweiten Teil werden Sie ein paar praktische Aufgaben durchführen. Wir bitten Sie während der Ausführung der Aufgaben laut zu denken. Erzählen Sie einfach, wie Sie vorgehen und was Sie sich dabei denken. Anfangs ist es etwas ungewohnt, aber bitte versuchen Sie es trotzdem,

da diese Methode besonders gute Hinweise auf die Qualität der Services liefert. Von uns werden Notizen gemacht und die Zeit gestoppt. Lassen Sie sich davon nicht irritieren oder unter Druck setzen, denn getestet wird wie gesagt das Produkt und nicht Sie.

- Im Abschlussgespräch möchten wir Sie zu Ihrer Meinung und Ihren Erfahrungen befragen, nachdem Sie das Produkt getestet haben.

Haben Sie Fragen zum Testablauf? Sie können auch während dem Test Fragen stellen oder unterbrechen, wenn Sie eine Pause machen möchten.

Die Ergebnisse werden selbstverständlich vollkommen anonym ausgewertet. Für uns spielt es keine Rolle WER einen Mangel entdeckt hat oder eine bestimmte Aussage trifft, sondern WELCHE Bereiche optimiert werden können und WIE eine Verbesserung aussehen kann.

Zur Dokumentation und Auswertung möchten wir ein Diktiergerät verwenden. Das erleichtert uns einerseits die Aufzeichnung und außerdem verbessern sie die Qualität der Dokumentation. Die Aufnahmen werden ausschließlich von uns ausgewertet und nach Fertigstellung des Berichts gelöscht.

Vielen Dank im Vorhinein für Ihre Unterstützung!

A.7.2 Pre-Test Interview

Im Pre-Test Interview wird nach dem Alter und dem Geschlecht der Testpersonen gefragt. Weiters werden ihnen folgende Fragen gestellt.

- Welches Mobiltelefon besitzen Sie (Marke, Type)?
- Ist Ihnen die Technologie NFC bekannt? Haben Sie sie schon einmal verwendet?
- Haben Sie Erfahrung mit elektronischen Schlössern? Wenn ja, welche?

A.7.3 Einleitungstext Testcases (mündlich)

„Wir werden nun Sunrise System in der Praxis testen und ihnen einige kleinere Aufgaben stellen. Wenn Ihnen eine Aufgabenstellung unklar sein sollte, fragen Sie bitte lieber noch mal nach. Bitte versuchen Sie, diese möglichst selbstständig zu lösen. Wenn Sie eine Aufgabe nicht lösen können, werden wir Ihnen gerne dabei helfen. Es gibt keine Zeitbeschränkung zum Lösen der Aufgaben. Sollten Sie eine Pause machen wollen oder sich unwohl fühlen, teilen Sie uns das bitte mit. Wir möchten Sie bitten während der Aufgaben „laut nach zu denken“. Äußeren Sie ruhig Unklarheiten oder wenn Ihnen etwas „komisch“ vorkommt. Auch wenn es sich hierbei um einen Prototyp handelt, können Sie ungezwungen damit umgehen. Es ist nicht möglich, etwas zu beschädigen.“

A.7.4 Post-Test Interview

Fragen werden zuerst offen gestellt und nur bei Unklarheiten/undefinierter Meinung auf die vorgegebenen Antwortmöglichkeiten eingegrenzt. Antwortmöglichkeiten sind Stimme voll zu, Stimme zu, Stimme kaum zu und Stimme nicht zu. Die letzten drei Fragen werden frei beantwortet,

- Denken Sie, dass Sie Sunrise in Zukunft verwenden werden?

- Finden Sie, dass Sunrise unnötig kompliziert ist?
- Dachten Sie während des Tests, dass Sunrise einfach zu verwenden ist?
- Sind Sie der Meinung, dass Sie Sunrise ohne Unterstützung durch eine technisch versierte Person benutzen könnten?
- Sind die verschiedenen Funktionen Ihrer Ansicht nach gut in das Gesamtkonzept von Sunrise integriert?
- Nachdem Sie Sunrise getestet haben, finden Sie, dass es zu viele Inkonsistenzen im Gesamtkonzept gegeben hat?
- Können Sie sich vorstellen, dass die meisten Personen die Benutzung von Sunrise sehr schnell erlernen können?
- Denken Sie, Sunrise ist sehr mühsam bzw. umständlich zu verwenden?
- Haben Sie sich während der Benutzung von Sunrise sicher und souverän gefühlt?
- Finden Sie, es waren eine Menge Dinge zu lernen, bevor Sie mit Sunrise umgehen konnten?
- Würden Sie Sunrise in Ihrer Wohnung verwenden? Wieso/wieso nicht?
- Glauben Sie, dass Sunrise sicherer als ein herkömmliches Schloss ist? Wieso/wieso nicht?
- Haben Sie noch zusätzliche Anregungen, Vorschläge oder Kritikpunkte?

B Test-Protokolle

B.1 Test-Protokolle

In diesem Abschnitt finden sich die rohen Daten, die während der Usability Tests aufgezeichnet wurden. Die Audiodateien wurden wie von uns angekündigt verarbeitet und danach gelöscht, um die Privatsphäre der Testpersonen zu schützen.

SUNRISE USEABILITY TEST

Testperson **TP1**

Testreihenfolge SSO1 SSO2 SSO3 SSO4 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SSO1

Erfolg	X
Zeit	23:24
Fehler	~~IIII~~ IIII
Hilfe	1

SSO2

Erfolg	✓
Zeit	4:23
Fehler	11
Hilfe	—

SSO3

Erfolg	✓
Zeit	1:27
Fehler	~~nn~~ 1
Hilfe	—

SSO4

Erfolg	✓
Zeit	1:14
Fehler	—
Hilfe	—

- ✓ Post-Test Interview

U1

ERFOLG	✓
ZEIT	2:16
FEHLER	3
HILFE	11

Abbildung B.1: Testprotokoll Testperson 1

SUNRISE USEABILITY TEST

Testperson **TP2**

Testreihenfolge SSO2 (3) SSO3 (4) SSO4 (2) SSO1 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SSO2 (3)

Erfolg	✓
Zeit	5:27
Fehler	III
Hilfe	—

SSO3 (4)

Erfolg	✓
Zeit	1:39
Fehler	—
Hilfe	—

SSO4 (2)

Erfolg	✓
Zeit	7:17
Fehler	III
Hilfe	—

SSO1

Erfolg	✓
Zeit	1:10
Fehler	—
Hilfe	—

U1

ERFOLG	✓
ZEIT	1:00
FEHLER	—
HILFE	—

- ✓ Post-Test Interview

Abbildung B.2: Testprotokoll Testperson 2

SUNRISE USEABILITY TEST

Testperson **TP3**

Testreihenfolge SSO3 SSO4 SSO1 SSO2 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SSO3 4

Erfolg	✓
Zeit	0:46
Fehler	—
Hilfe	—

SSO4 3

Erfolg	✓
Zeit	0:49
Fehler	—
Hilfe	—

SSO1 2

Erfolg	✓
Zeit	5:45
Fehler	IIII
Hilfe	—

SSO2 1

Erfolg	✓
Zeit	0:39
Fehler	—
Hilfe	—

U1

ERFOLG	✓
ZEIT	0:51
FEHLER	1
HILFE	—

- ✓ Post-Test Interview

Abbildung B.3: Testprotokoll Testperson 3

SUNRISE USEABILITY TEST

Testperson **TP4**

Testreihenfolge SSO4 (2) SSO1 SSO2 (4) SSO3 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SSO4 (2)

Erfolg	✓
Zeit	4:01
Fehler	IIII
Hilfe	—

SSO1

Erfolg	✓
Zeit	1:15
Fehler	I
Hilfe	—

SSO2 (4)

Erfolg	✓
Zeit	3:16
Fehler	II
Hilfe	—

SSO3

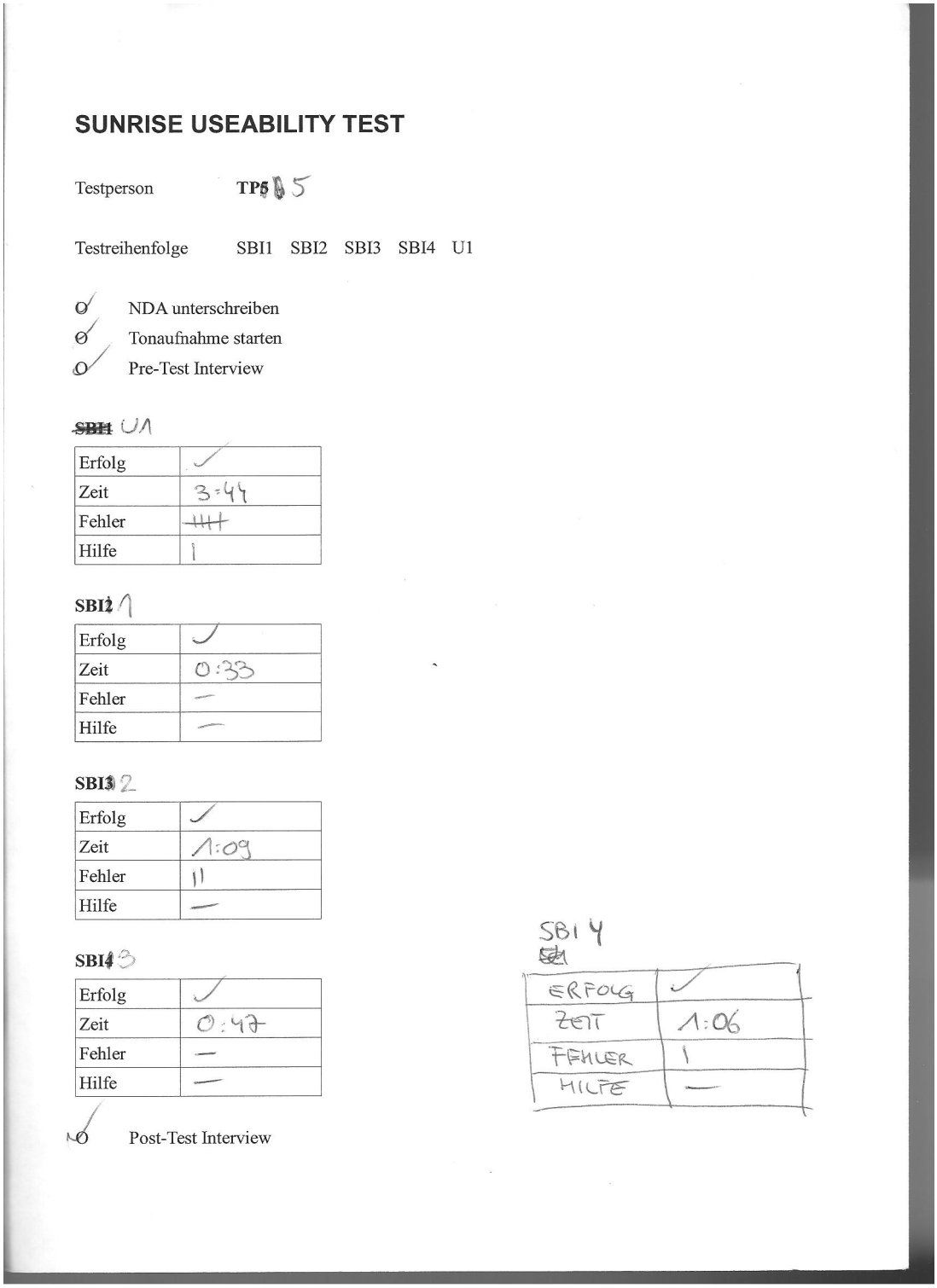
Erfolg	✓
Zeit	1:53
Fehler	III
Hilfe	II

U1

ERFOLG	✓
ZEIT	0:36
FEHLER	I
HILFE	—

- ✓ Post-Test Interview

Abbildung B.4: Testprotokoll Testperson 4



SUNRISE USEABILITY TEST

Testperson TP5 5

Testreihenfolge SBI1 SBI2 SBI3 SBI4 U1

✓ NDA unterschreiben
✓ Tonaufnahme starten
✓ Pre-Test Interview

~~SBI1~~ U1

Erfolg	✓
Zeit	3:44
Fehler	HH
Hilfe	1

SBI2 1

Erfolg	✓
Zeit	0:33
Fehler	—
Hilfe	—

SBI3 2

Erfolg	✓
Zeit	1:09
Fehler	11
Hilfe	—

SBI4 3

Erfolg	✓
Zeit	0:47
Fehler	—
Hilfe	—

✓ Post-Test Interview

SBI 4

ERFOLG	✓
ZEIT	1:06
FEHLER	1
HILFE	—

Abbildung B.5: Testprotokoll Testperson 5

SUNRISE USEABILITY TEST

Testperson TP6 6

Testreihenfolge SBI3 SBI4 SBI1 SBI2 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SBI3

Erfolg	✓
Zeit	1:11
Fehler	1
Hilfe	—

SBI4

Erfolg	✓
Zeit	0:38
Fehler	—
Hilfe	—

SBI1

Erfolg	✓
Zeit	0:58
Fehler	11
Hilfe	—

SBI2

Erfolg	✓
Zeit	4:20
Fehler	||| 1
Hilfe	11

- ✓ Post-Test Interview

U1

ERFOLG	✓
ZEIT	2:43
FEHLER	1111
HILFE	1

Abbildung B.6: Testprotokoll Testperson 6

SUNRISE USEABILITY TEST

Testperson TP7

Testreihenfolge SBI4 SBI3 SBI2 SBI1 U1

- ✓ NDA unterschreiben
- ✓ Tonaufnahme starten
- ✓ Pre-Test Interview

SBI4

Erfolg	✓
Zeit	1:44
Fehler	II
Hilfe	—

SBI3

Erfolg	✓
Zeit	1:12
Fehler	I
Hilfe	—

SBI2

Erfolg	✓
Zeit	0:39
Fehler	I
Hilfe	—

SBI1

Erfolg	✓
Zeit	0:38
Fehler	I
Hilfe	—

U1

ERFOLG	✓
ZEIT	2:57
FEHLER	HHII
HILFE	II

- ✓ Post-Test Interview

Abbildung B.7: Testprotokoll Testperson 7

SUNRISE USEABILITY TEST

Testperson TP4 8

Testreihenfolge SBI2 SBI1 SBI4 SBI3 U1

✓ NDA unterschreiben
✓ Tonaufnahme starten
✓ Pre-Test Interview

SBI2

Erfolg	✓
Zeit	1:58
Fehler	III
Hilfe	I

SBI1

Erfolg	✓
Zeit	0:42
Fehler	I
Hilfe	—

SBI4

Erfolg	✓
Zeit	0:12
Fehler	II
Hilfe	—

SBI3

Erfolg	✓
Zeit	0:37
Fehler	—
Hilfe	—

U1

ERFOLG	✓
ZEIT	2:24
FEHLER	IIII
HILFE	II

O Post-Test Interview

Abbildung B.8: Testprotokoll Testperson 8