Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

Bachelorarbeit (Informatikingenieurwesen)

Individuell Konfigurierbarer Authentifizierungs-service für Votings und Wettbewerbe

Autor	Christian Bachmann
Betreuung	Jaime Oberle
Auftraggeber	inaffect AG
Datum	23.12.2015

Inhaltsverzeichnis

1 Einführung

1.1 Motivation

Die Digitalisierung fordert die Schweizer Wirtschaft heraus. Ob Banken, Pharma, Detailhandel oder Medienhäuser – es gibt keine Branche, die nicht vor fundamentalen Veränderungen steht.[1] Da verwundert es nicht, dass Wettbewerbe oder Kreuzworträtsel nicht nur auf den letzten Seiten des Klatschhafte oder Zeitungen abgedruckt werden sondern vermehrt online publiziert und durchgeführt werden. Dass bei meinungsbildenden Umfragen oder Abstimmungen weniger auf Telefonumfragen zurückgegriffen wird sondern diese immer mehr im Internet durchgeführt werden.

In der Schweiz konnten die grossen Medienhäuser ihre Zugriffszahlen auch 2015 steigern und ihre Toprangierungen beibehalten.[2] Um Ihren Werbegewinn und Resonanz zu bewahren oder sogar auszubauen sind Medien angewiesen, dass Ihre Stories/Content auf den Social Media Kanälen verlinkt und so viral verbreitet werden. Neben altbekannten plakativen Titeln und interessanten Bildern beleben die Medienhäuser immer mehr ihren Content mit so genannten Playfull Content integriert durch Social Module. Dabei handelt sich um Abstimmungen, Wettbewerbe und Umfragen oder anderen Interaktivitäten im Zusammenhang mit dem verfassten Inhalt. Diese Social-Module werden gerne verlinkt und fördern so die Verbreitung des Contents und dadurch einen Anstieg der Besucherzahlen.

Bei den meisten angebotenen Umfragen, Abstimmungen und Wettbewerbe ist es relativ simpel (gewisses Know-How vorausgesetzt) mehrfach teilzunehmen oder gefälschte Daten zu übermitteln. Dies ist auf zu einfach realisierte Programmierungen zurückzuführen, was der Glaubwürdigkeit solcher Angebote schadet. Social-Module wie Umfragen, Abstimmungen oder Wettbewerbe bedürfen somit einer Authentifizierung, um Betrug oder falschen Stimmabgaben vorzubeugen. Die Eigenentwicklung der gewünschten Authentifizierung für ein Modul übersteigt meist die kleinen Budgets für diese Angebote.

Die Glaubwürdigkeit der Umfragen, Abstimmungen und Wettbewerbe ist durch die aktuelle Situation gefährdet und soll wiederhregestellt werden. Deshalb soll diese Bachlorarbeit die Möglichkeit eines Authentifizierungsservice erörtern. Mit dieser sollen Programmierer über eine visuelle Oberfläche die Bedürfnisse eines Angebots konfigurieren und in ihren jeweiliges Modulen einbinden können.

[1] (Millischer 2015)
[2] ("NET-Metrix-Audit" 2015)

1.2 Aufgabenstellung

1.2.1 Ausgangslage

Bei populären Medienhäusern und grösseren Unternehmen werden häufig Umfragen, Abstimmungen oder Gewinnspiele im Internet durchgeführt. Bei den meisten angebotenen Programmen ist es relativ simpel (gewisses Know-How vorausgesetzt) mehrfach teilzunehmen oder gefälschte Daten zu übermitteln. Dies ist auf zu einfach realisierte Programmierungen zurückzuführen, was der Glaubwürdigkeit solcher Angebote schadet. Social-Media Module wie Umfragen, Abstimmungen oder Wettbewerbe bedürfen somit einer Authentifizierung, um Betrug oder falschen Stimmabgaben vorzubeugen. Die Eigenentwicklung der gewünschten Authentifizierung für ein Modul übersteigt meist die kleinen Budgets für diese Angebote. Die Firma inaffect AG erstellt Individuallösungen und Webapplikationen im Bereich neuer Medien. Sie ist auf der Suche nach einem Authentifizierungsservice, welche ihre Programmierer mit einer visuellen Oberfläche den Bedürfnissen eines Angebots konfigurieren und in ihr jeweiliges Modul einbinden können.

1.2.2 Ziel der Arbeit

Es soll ein Konzept für eine Authentifizierungsschnittstelle erstellt werden. Dieser Service wird über mehrere Sicherheitsstufen verfügen, die sich in der Menge und Art der zu übermittelnden User-Informationen unterscheiden. Diese Stufen sollen für den Programmierer eines Angebots über eine grafische Oberfläche individuell konfigurierbar sein. Das Konzept soll in Form eines Prototypen umgesetzt werden. Weiter soll mit mehreren Usern eine Studie zur Akzeptanz und Geschwindigkeit der verschiedenen Sicherheitsstufen durchgeführt werden. Die Ergebnisse der Studie werden im Prototyp integriert sein und sollen den Programmierer bei der Auswahl der Sicherheitsstufe unterstützen.

1.2.3 Aufgabenstellung

Im Rahmen der Bachelorarbeit werden vom Studenten folgende Aufgaben durchgeführt:

Recherche

- Research und Marktanalyse bestehender Produkte
- Arten und Methoden der Sicherheits- und Identitätsüberprüfung
- Durchführung einer Anforderungsanalyse für eine Authentifizierungsschnittstelle

Konzept

- Evaluation von geeigneten Authentifizierungsmethoden für verschiedene Stufen
- Spezifikation einer Prototypenapplikation für die Authentifizierungsschnittstelle
- Spezifikation einer Prototypenapplikation für das Verwalten der Authentifizierungsschnittstelle
- Erstellen einer Software-Architektur für die Authentifizierungsschnittstelle und dessen Verwaltung
- Ausarbeiten einer Studie über Akzeptanz und Geschwindigkeit von Authentifizierungsmethoden

Studie

- Durchführen der ausgearbeiteten Studie
- Auswertung der Studie

Proof of Concept

- Entwicklung eines Prototypen der Authtenifizierungsschnittstelle und der Verwaltung, basierend auf den erarbeiteten Spezifikationen und Architektur
- Integration der Studienresultate im Prototypen

Fazit

1.2.4 Erwartete Resultate

Im Rahmen dieser Bachelorarbeit werden vom Studenten folgende Resultate erwartet:

Recherche

- Dokumentation des Research und Marktanalyse bestehender Produkte
- Dokumentation der Arten und Methoden der Sicherheits- und Identitätsüberprüfung

Analyse

- Dokumentierte Anforderungsanalyse für eine Authentifizierungsschnittstelle

Konzept

- Dokumentation der Evaluation von geeigneten Authentifizierungsmethoden für verschiedene Stufen
- Dokumentierte Spezifikation einer Prototypenapplikation für die Authentifizierungsschnittstelle
- Dokumentierte Spezifikation einer Prototypenapplikation für das Verwalten der Authentifizierungsschnittstelle
- Dokumentation der Software-Architektur für die Authentifizierungsschnittstelle und dessen Verwaltung
- Dokumentation des Ausarbeitens einer Studie über Akzeptanz und Geschwindigkeit von Authentifizierungsmethoden

Studie

- Dokumentation der Studien-Durchführung
- Dokumentation der Auswertung der Studie

Proof of Concept

- Dokumentierte Entwicklung eines Prototypen der Authentifizierungsschnittstelle und der Verwaltung, basierend auf den erarbeiteten Spezifikationen und Architektur
- Dokumentierte Integration der Studienresultate im Prototypen
- Dokumentiertes Fazit

1.3 Rahmenbedingungen Bachelorarbeit

Die vorliegende Bachelorarbeit umfasst gemäss Regelment unter anderem folgende Punkte:

- Eine Bachelorarbeit besteht aus einer konzeptionellen Arbeit und deren Umsetzung. Der Schwerpunkt liegt auf dem konzeptionellen Teil, in dem die theoretischen und methodischen Grundlagen einer Entwicklung oder eines Konzeptes ausgearbeitet und dargelegt werden. Im Umsetzungsteil erfolgt anschliessend die Beschreibung der Implementierung bzw. der Anwendung. Die Umsetzung besteht zumindest aus einem „Proof of Concept“, um die prinzipielle Realisierbarkeit darzulegen. Die Bachelorarbeit ist als praxisnahes Projekt durchzuführen.
- Der Aufwand für die Fertigstellung einer Bachelorarbeit beträgt insgesamt mindestens 360 Stunden.
- Die Bachelorarbeit hat die Form eines technischen Berichtes.[3]

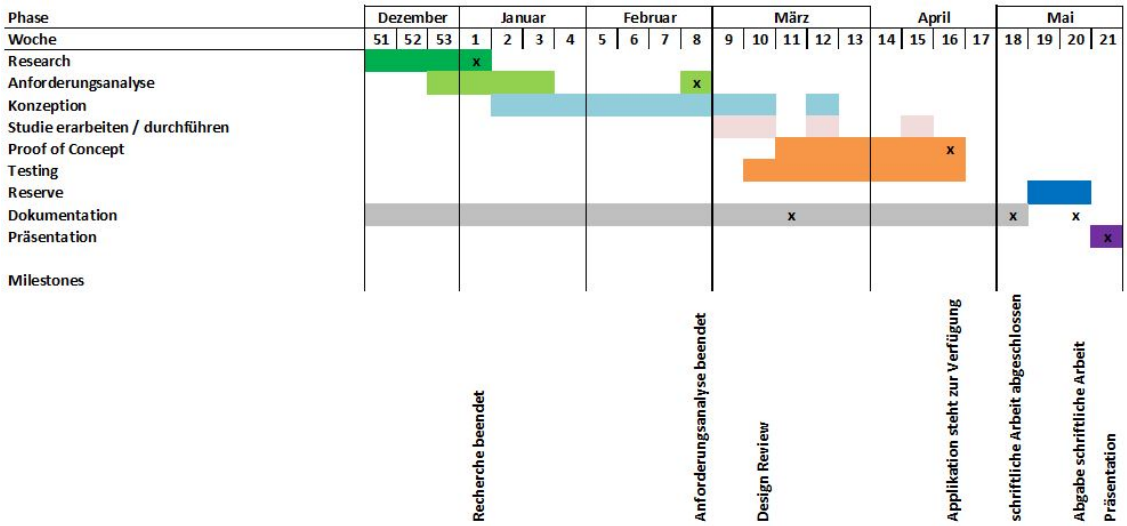
[3] (Stern 2012)

2 Projektmanagement

In diesem Kapitel wird die Planung der Bachelorarbeit ausgeführt. Weiter wird die verwendete Infrastruktur erläutert.

2.1 Grobe Projektplanung

Der grobe Projektplan illustriert die Strukturierung der Bachelorarbeit über die knapp sechs Monate lange Projektzeit. Der Projektplan liefert einen generellen Überblick über den zeitlichen Ablauf der Bachelorarbeit und legt die Milestons fest. Als Soll Aufwand der Bachelorarbeit wurden 375 Stunden veranschlagt. Der effektive aufgelaufene Aufwand betrug xx Stunden.



2.2 Aufwand

Im Unterkapitel Rahmenbedingungen Bachelorarbeit wurde bereits ausgeführt, dass eine Bachelorarbeit laut Regelement mindestens 360 Stunden betragen soll. Diese Rahmenbedingung wurde bei Aufgabenstellung und Aufwandschätzung der Bachelorarbeit berücksichtigt.

Tabelle 2.1: Soll/Ist Analyse

Arbeitsschritt	**Soll**	**Ist**
Initialisierung	10	
Recherche	45	
Analyse	20	
Konzeption	80	
Prototyp	60	
Dokumentation	140	
Abgabe	20	
Total	**375**	**xx**

2.3 Meilensteine

Meilensteine sind zum einen sehr wichtig für das Projektmanagement, da sie den gesamten Ablauf der Bachelorarbeit in mehrere kleine und überschaubarere Etappen und Zwischenziele einteilen. Dadurch kann auf dem Weg die Bachelorarbeit erfolgreich umzusetzten immer wieder Inne gehalten und kontrolliert werden, wie der Stand der Dinge ist, ob die Richtung geändert werden muss. So bleibt stets der Überblick gewahrt und das Projekt Bachelorarbeit gerät nicht ausser Kontrolle.[1]

Tabelle 2.2: Meilensteine

Ende Meilstein	**Meilenstein**
bis 10. Januar 2016	Recherche beendet
bis 28. Februar 2016	Anforderungsanalyse beendet
bis 20. März 2016	Design Review
bis 24. April 2016	Applikation steht zur Verfügung
bis 8. Mai 2016	schriftliche Arbeit abgeschlossen
bis 22. Mai 2016	Abgabe schriftliche Arbeit
bis 29. Mai 2016	Präsentation

[1] ("Projektmanagement: Definitionen, Einführungen Und Vorlagen" 2015)

2.4 Termine

Tabelle 2.3: Termine der Bachelorarbeit

Datum	**Termin**
28.10.2015	Besprechung Aufgabenstellung mit Betreuer
18.11.2015	Freigabe der Aufgabenstellung
9.12.2015	Kichkoff
6.01.2016	Statusmeeting mit Betreuer
	Statusmeeting mit Betreuer
	Statusmeeting mit Betreuer
	Statusmeeting mit Betreuer
	Designreview
	Statusmeeting mit Betreuer
	Abgabe schriftliche Arbeit
	Präsentation

2.5 Infrastruktur

Im Unterkapitel Infrastruktur sollen die verwendeten Tools erläutert werden.

2.5.1 Quellcode-Verwaltung

Um einerseits eine Datensicherung zu gewährleisten und anderseits die Änderungen nachvollziehbar abzulegen, wird die Bachelorarbeit mittels Git und GitHub versioniert. Das Repository[2] ist für den Betreuer, Experten und Auftrageber jederzeit einsehbar.

2.5.2 Zeitmanagement

Beim Arbeiten an der Bachelorarbeit kann man sich schnell in details verlieren. Das Zeitmanagement Tool toggl[3] gibt einem schnell ein Feedback zu aktuell verbrauchten Zeit und einen Überblick um das geplante mit der realen Zeit zu vergleichen.Die Software ist besonders unter Kreativagenturen und Freelancern beliebt. Sie präsentiert sich als eine besonders simple Lösung, die die flexible Zeiterfassung in den Fokus stellt. Der User kann neue Aufgaben mit nur einem Klick anlegen und die Stoppuhr starten, um Arbeitszeiten automatisch zu erfassen.

[2] https://github.com/coffeefan/bachelorarbeit
[3] https://toggl.com

2.5.3 yUML

Um Abläufe, Use Case und andere Uml-Diagramme zu visualisieren bedarf es ein Tool dass die Diagramm sowohl optisch ansprechend wie aber auch einfach und schnell anpassbar umsetzt. yUML ist ein gratis online service über welchen Code und dadurch ziemlich strukturiert ein UML-Diagramm kreiert werden kann. Der Code welche zum Diagramm führt kann so einfach als Textdatei abgespeichert werden und wird in dieser Bachelorarbeit im Github-Repository hinterlegt.

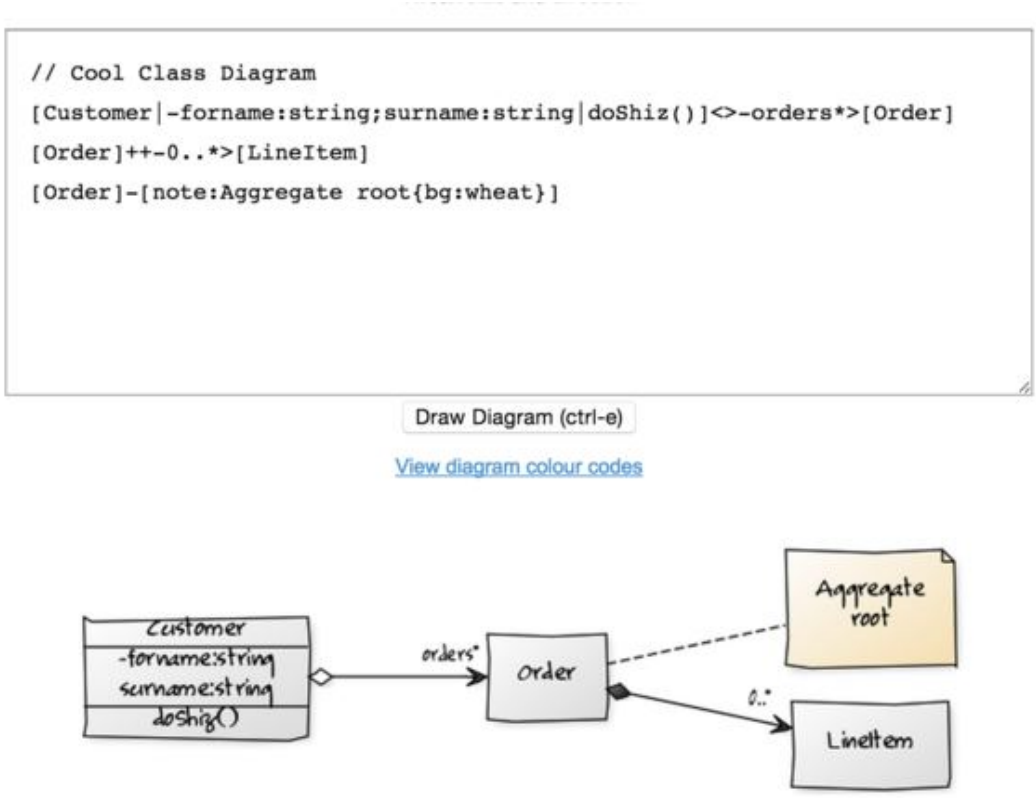


Abbildung 2.1: Screenshot yUML Beispiel Klassendiagramm

3 Recherche

3.1 Fachbegriffe

Eine ausführliche Erklärung der Fachbegriffe befindet sich im Anhang unter dem Kapitel "Glossar".

3.2 Erläuterung der Grundlagen

In diesem Kapitel werden Funktionsweisen und Grundlage ausgeführt, die als für die Bearbeitung dieser Bachelorthesis herangezogen wurden.

3.2.1 Authentifizierung

Authentifizierung - beglaubigen, die Echtheit von etwas bezeugen[1]

Eine Person oder Objekt eindeutig zu **authentifizieren** bedeute zu ermitteln ob die oder derjenige auch der ist als welcher er sich ausgibt.[2] Dies unterstreicht auch die Ableitung des Wortes vom Englischen Verb *authenicate*, was auf Deutsch sich als *echt erweisen, sich verbürgen, glaubwürdig sein* bedeutet. Das bekannteste Verfahren der Authenfizierung ist die Eingabe von Benutzernamen und Passwort. Weiter ist die PIN-Eingabe bei Bankautomaten oder Mobiletelefon häufig verbreitet. Die Möglichkeiten der Authentifizierung nahe zu grenzenlos.[3]

3.2.2 Autorisierung

Autorisierung - Befugnis, Berechtigung, Erlaubnis, Genehmigung[4]

Wenn die AuthenfizierungAuthentifizierung erfolgreich war erteilt das System die Autorisierung. Dabei wird der Person oder Objekt erlaubt bestimmte Aktionen/Zugriffe durchzuführen. Meist verfügen unterschiedliche Benutzer eines Systems über verschiedene Zugriffsrechte. Die korrekte Zuweisung der individuellen Rechte ist ebenfalls Bestandteil der Autorisierung.

Der Begriff Authentifizierung wird vielfach mit dem Begriff Autorisierung verwechselt. Die Authentifizierung wird vom Benutzer initiiert. Sie dient dem Nachweis, zur Ausübung bestimmter Rechte befugt zu sein. Die anschließende Autorisierung erfolgt automatisch durch das System selbst. Im Zuge der Autorisierung werden dem Benutzer seine Zugriffsrechte zugewiesen. ("Http://authentifizierung.org" 2015)

[1] (*Duden* 2014)
[2] (Rouse 2015)
[3] ("Http://authentifizierung.org" 2015)
[4] (*Duden* 2014)

3.2.3 OAuth

OAuth ist ein Protokoll. Es erlaubt sichere API-Autorisierungen.

Das Bedürfnis nach OAuth

2006 implementiere Blaine Cook OpenID für Twitter. Ma.gnolia erhielt dabei ein Dashboard welches sich durch OpenID autorisieren lies. Deshalb suchten die Entwickler von Ma.gnolia und Blaine Cook eine Möglichkeit OpenID auch für die Verwendung von APIs zu gebrauchen. Sie diskutierten Implementierungen und stellten fest, dass es keinen offenen Standart für API-Access Delegation gab. So fingen sie an den Standard zu entwickeln. 2007 entstand daraus eine Google Group. Am 3. October 2007 war dann der OAuth Core 1.0 bereits released worden.

Funktionalität von OAuth

Ein Programm/API (Consumer) stellt über das OAuth-Protokoll einem Endbenutzer(User) Zugriff (Autorisierung) auf seine Daten/Funktionalitäten zur Verfügung. Dieser Zugriff wird von einem anderen Programm (Service) gemanagt. Das Konzept ist nicht generell neu. OAuth ist ähnlich zu Google AuthSub, aol OpenAuth, Yahoo BBAuth, Upcoming api, Flickr api, Amazon Web Services api. OAuth studierte die existierenden Protokolle und standardisiert und kombinierte die existierende industriellen Protokolle. Der wichtigste Unterschied zu den existierenden Protokollen ist, das OAuth sowohl offen ist und es geschafft hat genügend Einsatzgebiete zu finden um als Standard zu gelten. Jeden Tag entstehen neue Webseite welche neue Funktionalitäten und Services offerieren und dabei Funktionalitäten von anderen Webseiten brauchen. OAuth stellt dem Programmierer einerseits eine standardisierte Implementierung zur Verfügung. Anderseites erhält der Endbenutzer dank dieses Protokolls die Möglichkeit Teile seiner Funktionalität/Daten bei einem anderen Anbieter zur Verfügung zu stellen. Zum Beispiel bei Facebook OAuth kann der Endbenutzer seine Posts zur Verfügung stellen nicht aber seine Freunde bekannt geben.

Dank der weiten Verbreitung gibt es nun in allen bekannten Programmiersprachen eine Implementierung sowohl von Client wie auch vom Server. Weitere Infos dazu unter oauth.net1

3.3 Ähnliche Produkte auf dem Markt

Dieses Unterkapitel erläutert existierenden Produkte auf dem Markt.

3.3.1 OAuth-Provider

Die grössten OAuth-Provider wie Google, Facebook und Twitter erziehlen eine weiter Verbreitung weltweit:

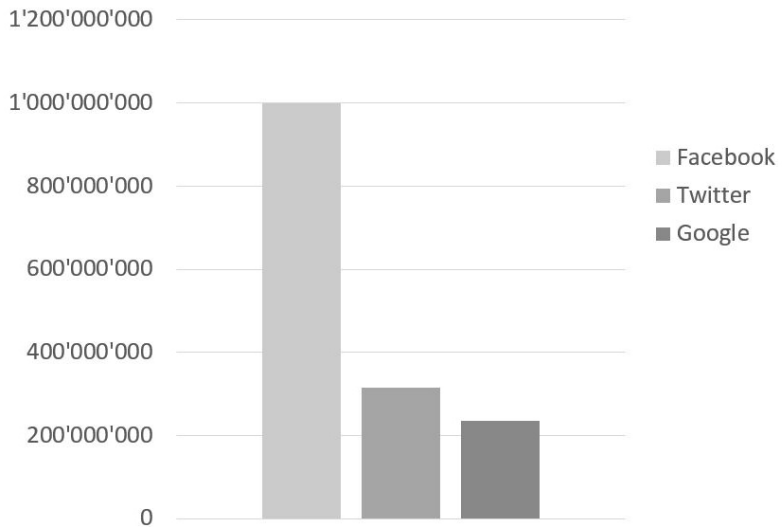


Abbildung 3.1: Aktive Nutzer Weltweit[5]

Ganze *78%* (Interactive 2015) der Schweizer Bevölkerung nutzten SocialMedia und besitzen dadurch einen OAuth-Account:

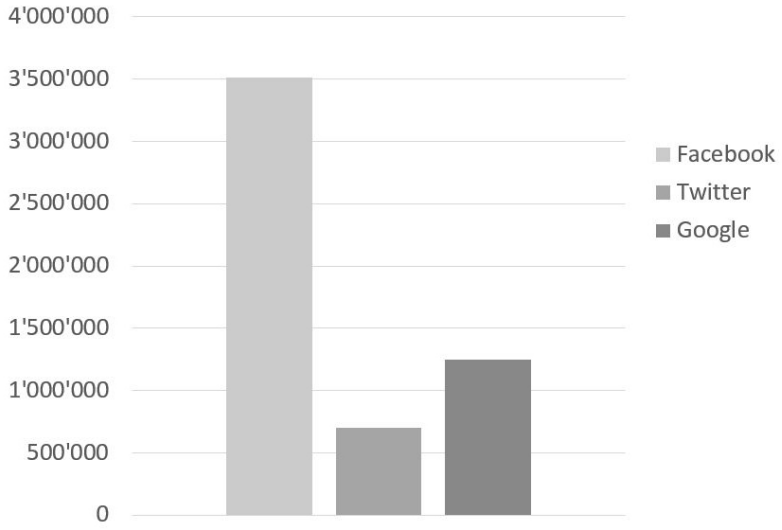


Abbildung 3.2: Anzahl Schweizer Nutzer[6]

[5] Das Statistik wurde basierend auf den Daten von socialmedia-institute ("SMI (SocialMedia Institute)" 2015)erstellt. Facebook und Twitter Daten sind am 5. November 2015 und die Google Daten sind im 2014 erhoben worden.

Vorteile

Mindestes 78% der Schweizer Bevölkerung besitzt bereits einen OAuth Account. Das Protokoll ist ein etablierter Standard.

Nachteile

Mehrfachregistrierungen sind möglich. Jenach OAuth-Provider werden verschiedene Daten zur Verfügung gestellt. Pro OAuth Provider kann man sich registrieren einen Abgleich der verschiedenen OAuth Provider wird vom OAuth-Protokoll nicht zur Verfügung gestellt. Ein Teil der Bevölkerung müsste sich vor Nutzung noch registrieren. Die Implementierung ist trotz vielen Libaries nicht ohne tiefere Programmierkenntnisse möglich.

[6] Das Statistik wurde basierend auf den Daten von Goldbach Interactive (Interactive 2015) generiert. Die Daten sind im März 2015 erhoben.

3.3.2 playbuzz.com

Youtube von Google ist im Jahr 2015 mit Abstand die meist verbreiteste Videopublishing-Plattform[7]. Medienhäuser nutzen Youtube um einfach Ihren Artikel mit einem Video zu ergänzen. Neben der einfachen Integration profitieren die Medienhäuser von der zusätzlichen Verbreitung über youtube.com und der einfachen viralen Verbreitungsmöglichkeiten von youtube. PlayBuzz möchte das Youtube für Votings, Quiz und ähnlicher Embeded Content zu werden. Neben MTV, Focus, Time oder Bild verwendet seit Herbst 2015 auch ein grosses Medienhaus der Schweiz die Plattform. Tamedia erfasst neu auf 20minuten Votings und Umfragen mit PlayBuzz.

2012 wurde Playbuzz von Shaul Olmert (Sohn des Premie Minster von Israel Ehuad Olmert) und Tom Pachys ins Leben gerufen. Der offizielle Launch war im Dezember 2013. Im Juni 2014 wurde Playbuzz bereits das 1. Mal unter den Top 10 Facebook Shared Publishers aufgelistet. Im Juni 2014 konnte Playbuzz bereits 70 millionen unique views aufweisen. Im September 2014 kamen 7 von den 10 Top Shares auf Facebook laut forbes.com von Playbuzz. Playbuzz setzt nach eigenen Angaben auf Content wie Votes und Quizes welcher gerne Viral geteilt wird und ermöglicht Endnutzer und Redaketeueren einfache Verwendung.[8][9]

Vorteile

Playbuzz ist kostenlos und lässt sich einfach integrieren. Durch Verwendung von Playbuzz kann die Verbreitung des eigenen Inhalts gesteigert werden. Die Verwaltungsoberfläche und Reports sind übersichtlich und einfach zu bedienen.

Nachteile

Der Verweis auf Playbuzz ist ersichtlich. Auch beim Posten auf den SocialMedia-Kanälen ist die Herkunft von Playbuzz offensichtlich. Die Möglichkeiten in Funktionalität und Design haben Grenzen. Individuelle Erweiterungen sind nicht einfach möglich.

[7] ("Statistik Plattform" 2015)
[8] ("Interview Mit Shaul Olmert" 2015)
[9] ("PlayBuzz" 2015)

3.3.3 WebSMS.com Zwei-Faktor-Authentifizierung

WebSMS.com bittet eine Zwei-Faktor-Authentifizierung über SMS an. Der User gibt seine Mobilnummer in der Webmaske der Schnittstelle ein und erhält einen Code welcher der User danach in der Webschnittstelle eingibt. Dadurch kann sichergestellt werden dass der User zur eingegebenen Mobilenummer passt. Der Service kostet monatlich 20 CHF und weitere 0.08 CHF pro SMS[10]

Die Stärke und Sicherheit dieses Service ist direkt mit mit dem Umgang von Mobilenummern/SIM-Karten und dessen Authentifizierung verbunden.

Seit 1. Juli 2004 müssen auch bei Prepaid-Karten in der Schweiz Personalien hinterlegt werden.[11] Dadurch ist eine eindeutige Authentifizierung über Mobilennummer gewährleistet. Die Mobilefunkanbieter schrenken die Anzahl SIM-Karten auf maximal 5 pro Person ein. Dieses Maximum konnte aber auf den Webseiten der Anbieter nicht direkt gefunden werden. Daher galt es den Wert zu untersuchen und mögliche abweichungen ausfindig zu machen.

Swisscom

Die Swisscom hat kein öffentlich zugängigliches Dokument welches die maximale Anzahl SIM-Karten pro Person beschreibt. Mündlich durch das Verkaufspersonal des Swisscom-Shops Zürich HB Dezember 2015 und im Chatprotokoll[12] wurde der Wert bestätigt. Es hingewiesen, dass nicht ein Dokument mit dieser Zahl vorhanden ist.

Selbstversuch Es wurde versucht bei zwei unabhängigen Handyanbieter mehr als 5 Swisscom-Perpaid-Abos abzuschliessen. Dabei wurden von Thomas Bachmann über 4 Wochen verteilt bei dem Anbieter Interdiscount im Manor Winterthur bei verschiedenem Kaufspersonal ein Prepaidhandy eingekauft. Beim Einkauf des 6. Handys wurde der Verkauf von der Kasse abgelehnt. Die Fehlermeldung der Kasse beinhaltete den Hinweis, dass sich die Nummer nicht erneut auf den Kunden registrieren lassen kann, da er schon 5 SIM Karten bei der Swisscom besitzt. Christian Bachmann kaufte über 2 Wochen verteilt bei dem Anbieter Migros Electronics in der Migros Limmat, Interdiscount im Manor Winterthur, Interdiscount im Zürich HB bei verschiedenem Kaufspersonal ein Swisscom Prepaidhandy. Beim Einkauf des 6. Handys wurde der Verkauf von der Kasse abgelehnt. Die Nummer liess sich nicht erneut auf den Kunden registrieren, da er schon 5 SIM Karten bei der Swisscom besitzt.

Sunrise

Die Sunrise hat nach Rücksprache ein PDF mit Ihren Bestell- und Lieferbedingunge zugesendet.[13] Die maximale Anzahl SIM-Karten ist in diesen Bestell- und Lieferbedingungen festgelegt. Auch die Sunrise hat das Maximum auf 5 pro Person festgelegt.

[10] Die Kosten sind am 28. Dezember 2015 unter folgendem Link abgerufen worden: https://websms.ch/preise#at-preisuebersicht

[11] Meldung des UVEKS über Gesetzesänderung: ("NET-Metrix-Audit" 2004)

[12] Chat-Protokoll Swisscom 12.Februar 2016 http://bit.ly/swisscom-chat

[13] Kopie Bestell- und Lieferbedingungen http://bit.ly/sunrise-bedienungen

SALT

Bei der Die Firma SALT konnte mir ebenfalls kein Dokument mit der Kennzahl gegeben werden. SALT stellt vergibt ihrer schriftlichen Auskunft[14] pro Person maximum 3 SIM Karten.

Vorteile

Die mehrfache Registrierung ist auf maximal 5 beschränkt. Durch die Kosten für eine SIM-Karte/Mobilenummer wird der Wert zusätzlich gemindert. Bei Missbrauch kann der User eindeutig identifiziert werden. Eine Automatisierung ist nahe zu unmöglich.

Nachteile

Der Versand von SMS verursacht Kosten. Die Implementation bedarf hohes technisches Know-How.

[14] E-Mail von Salt 13.Februar 2016 http://bit.ly/salt-email

3.4 Grundlegende Sicherheitsprinzipien

In diesem Unterkapitel werden die Grundlagen der Sicherheitsprinzipien vermittelt auf denen eine Authentifizierungssoftware aufgebaut werden kann.

3.4.1 KISS

Keep **I**t **S**tupid *and* **S**imple

Ein verbreitetes Problem unter Software Engineers und Programmier heute ist, dass sie dazu tendiert wird, Probleme zu kompliziert und verschachtelt zu lösen. 8-9 von 10 Entwickeln machen den Fehler, Probleme zu wenig auseinander zu brechen und alles in einem grossen Programm zu lösen. Anstatt es in kleinen Paketen verständlich zu programmieren.[^apachekiss]

Die folgenden Punkte listen die Vorteile für Software Entwickler bei verwenden von Kiss auf:

- Mehr Probleme sollen schneller gelöst werden
- Der Entwickler kann komplexe Probleme in wenigen Zeilen Code lösen
- Die Codequalität steigt
- Der Entwickler kann grössere System erstellen und unterhalten
- Der Code wird flexibler werden, einfach wieder zu verwenden und zu modifizieren
- Die Zusammenarbeit in grösseren Entwicklerteams und Projekten wird vereinfacht da der Code bei allen "stupid simple" ist

KISS fördert die Sicherheit

Die Begründung warum KISS die Sicherheit fördert, liefert Saltzer und Schroeder: Ungewollte Zugriffspfade können nur durch zeilenweise Codeinspektion entdeckt werden und die wiederum setzt voraus, dass Designs einfach und klein sein sind. Designs müssen so beschaffen sein, dass sie abgeschlossene Bereiche enthalten, über die konkrete und sichere Aussagen über Zugriffsmöglichkeiten und Effekte getroffen werden können. [^sicheresysteme_93]

3.4.2 Default-is-deny

Ob eine Person oder Programm Zugriff auf Daten/Funktionen haben, sollte nicht durch Verbote sondern durch explizite Erlaubnis geregelt werden. Dies bedeutet solange keine explizite Erlaubnis gesetzt ist, kann das Programm oder die Person nicht auf die Daten oder Funktionen zugreifen. You *deny* it. So simpel und logisch diese Idee klingt, umso verwunderlich ist wie viele Organisationen und Entwicklungsfirma nicht dieses vorgehen verwenden. z.B. Filesysteme setzten auf Verbote anstatt auf explizite Erlaubnise.[^sicheresysteme_94] [^defaultdeny]

3.4.3 Open Design

Abgeleitet von der Kryprotografie: Nicht das Design der Software sollte die Sicherheit sein, sondern der verwendete Schlüssel. Dieses Konzept gilt es in der Softwareentwicklung und Systemtechnik nur bedingt einzuhalten. Die Software soll nach dem Ansatz entworfen werden. Mindestens intern soll das Software-Design durch einen Design-Review Prozess analysiert werden. In manchen Fällen macht es jedoch das Softwaredesign geheimzuhalten um einem Angreifer nicht zu viele Informationen zur Verfügung zu stellen. [^sicheresysteme_95]

3.4.4 Zusammenfassung der Sicherheitsprinzipien

Die wichtigsten Sicherheitsprinzipien zusammengefasst:

- Software muss aus kleinen, isolierten Einheiten aufgebaut werden, deren externe Beziehungen am Interface deutlich werden. Damit wird sowohl praktische Schadensreduzierung durch Isolation als auch eine schnelle und einfache Sicherheitsanalyse möglich.
- Zugriffsentscheidungen dürfen nur auf der Basis expliziter, minimaler und keinesfalls durch immer und global verfügbare Permissions fallen.
- Das Softwaredesign von Applikationen sollte wenn möglich öffentlich sein. Zumindest sollte ein interner Review-Prozess stattfinden, in dessen Verlauf eine Sicherheitsanalyse durch nicht an der Entwicklung Beteiligte erstellt wird.

[^sicheresysteme_93] : (Kriha and Schmitz 2009, 93) [^sicheresysteme_94] :(Kriha and Schmitz 2009, 94) [^sicheresysteme_95] :(Kriha and Schmitz 2009, 95) [^apachekiss]: (Hanik 2015) [^defaultdeny]: (Rothman 2015)

3.5 Authetentifizierungskomponenten

Die Authentifizierung kann mit verschiedenen Komponenten durchgeführt werden. Folgend gilt es die Komponenten zu erklären.

3.5.1 Captcha

Captcha - Test, mit dem festgestellt werden kann, ob sich ein Mensch oder ein Computer eines Programms bedient[15]

Im Jahre 2000 wurde das Captcha an der Carnegie Mellon University erfunden. Captcha steht für **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. Luis von Ahn, Professor der Entwickler-Gruppe, erklärte die Dringlichkeit von Captcha damals so: "Anybody can write a program to sign up for millions of accounts, and the idea was to prevent that". ****[16]

Captcha Zahlen

In 2014 wurden 200 Million Captchas pro Tag eingegeben. Dabei braucht ein User durchschnittlich 10 Sekunden das entspricht 500'000 Stunden.[17]

3.5.2 Zweiweg Authentifizierung

Die Zwei-Faktor-Authentifizierung wird häufig 2FA genannt. Der User wird mittels zweier unabhängigen Faktoren identifiziert. Der Begriff Faktor umschreibt dabei eine Komponente oder Authentifizierungsmethode. [^cnet-2fa]

[15] (*Duden* 2014)
[16] (Burling 2012)
[17] Die statistischen Daten wurden von Google 2014 in ihrem Blog publiziert ("ReCAPTCHA Digitization Accuracy" 2014)

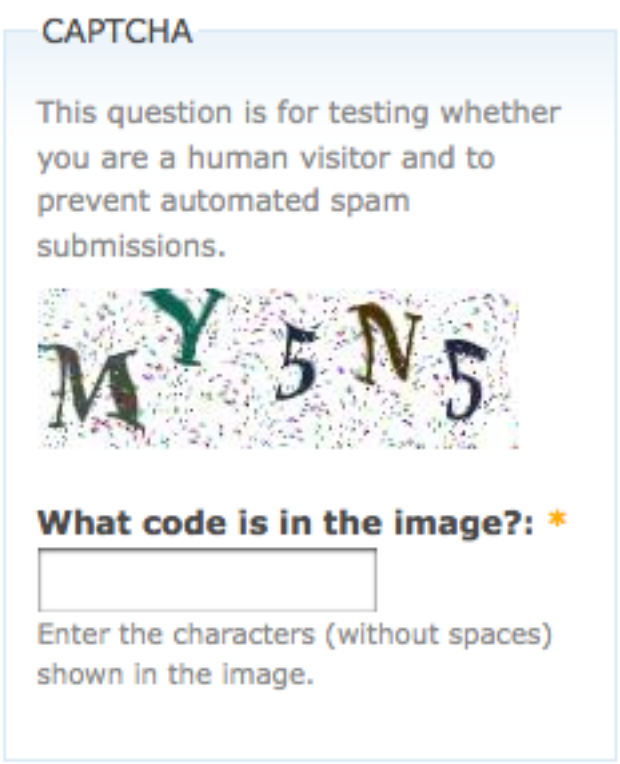


Abbildung 3.3: Beispiele von Captchas *Quelle:drupal.org*

Die Zwei-Faktor-Authentifizierung ist in der Schweiz durch das E-Banking bekannt geworden. Der User gibt als 1. Faktor Username/Vertragnummer und Passwort ein. In einem 2. Schritt gibt er vom System gewünschten Code aus der Codekarte oder des elektirschen Rechners als 2. Faktor ein. Im Alltag bei einem Einkauf im Detailhandel authentifiziert sich der EC-Karten Chip als 1. Faktor. Als 2. Faktor hat sich der Kunde ein Passwort auswendig gemerkt welches er eingibt.

Diese 2 Faktor Authentifizierung hatte die Entwicklung und Förderung der Vielfalt von Faktoren/Komponenten zu folge von welchen wir nun für unsere Authentifizierung profitieren können:

3.5.3 E-Mail Bestätigungs-Code

Im Registrationsprozess ist das Erhalten eines E-Mails mit Bestätigungs-Code zum quasi Standart geworden. Durch diese Methodik kann man garantieren, dass die angegebene E-Mail Adresse auch tatsächlich existiert und der User darauf Zugriff hat. Der User soll also auch bei der Authentifizierungsschnittstelle seine E-Mail eintragen und erhält dann umgehend den Bestätigungslink an seine E-Mail Adresse zugesandt.

Automatisierungsmöglichkeit

Das automatische Auslesen von E-Mails ist möglich. Jedoch ist der Aufwand dafür sehr hoch.

Mehrfach Teilnahme

Ein User kann verschiedene E-Mail Adressen besitzen. Dass Erstellen von neuen E-Mail Adressen ist mit Aufwand verbunden. Aber einfach möglich.

Anbieter wie 10-Minutes Mail[18] stellen auf Knopfdruck für einige Minuten eine temporäre E-Mail Adresse zur Verfügung. Dadurch können schnell einige E-Mail Adressen erstellt werden. Diese Domains müssen über eine aufwendige Blacklist gefiltert werden oder durch zeitversetztes Bestätigungsmail ausgehebelt werden.

Kosten

Das Versenden von E-Mails über einen SMTP Server ist generell kostenlos. Bei hohem Gebrauch dieser Komponente lohnt es sich die E-Mails über eine professionelle Inrastruktur für Massenversendung zu versenden und analysieren. Beispiele dafür sind Mailchimp[19] oder Sendgrid[20]

3.5.4 SMS Bestätigungs-Code

Das Konzept des im einem vorherigen Kapitel Anbieters WebSMS soll von der Authentifizierungsschnittstelle ebenfalls implementiert werden. Der User gibt im 1. Schritt seine Mobilenummer ein. Er hält dann einen Code per SMS zu gesandt. Im 2. Schritt gibt der User der erhaltene Mobilecode im Webform ein und bestätigt so, dass ihm die Mobilenummer gehört. Zum Versenden der SMS ist ein SMS-Gateway nötig.

Automatisierungsmöglichkeit

Die Automatisierung kann als nicht möglich eingestuft werden

Mehrfach Teilnahme

Die mehrfache Teilnahme wurde bereits im Kapitel zum Anbieter WebSMS eingehenden behandelt. Daraus resultierte, dass in der Schweiz maximal 5 Mobilenummern pro Anbieter und Person bezogen werden können.

Kosten

Je nach SMS-Gateway, Mobileanbieter des Empfängers und Verwendungsintensität belaufen sich der Versand eines SMS zwischen 0.04 CHF und 0.15 CHF[21]

[18] 10-Minute Mail ("10minutemail.com" 2016)
[19] www.mailchimp.com
[20] sendgrid.com
[21] Die Preise wurden am 1. März 2016 auf aspsms.ch/instruction/prices.asp, tropo.com/pricing und twilio.com/sms/pricing abgefragt

3.5.5 Telefonanruf mit Bestätigungscode

Nacheingabe der Telefonnummer oder Mobilenummer erhält der User einen digitalen Anruf. Die Computerstimme liest dem User einen Code vor, welcher er danach in der Webpage einggibt.

Automatisierungsmöglichkeit

Die Automatisierung kann als nicht möglich eingestuft werden

Mehrfach Teilnahme

Die Teilnahmeanzahl ist von den vorhandenen Telefonanschlüssen abhängig und daher nur eingschrenkt möglich.

Kosten

Die Kosten berechnen sich bei den analysierten Anbietern basierend auf einer geringen Monatspauschle zwischen CHF 1.00 und CHF 2.00 und Kosten pro Minute je nach Telefonanbieter des Empfängers und Voicegateway zwischen CHF 0.10 und CHF 0.65.[22]

[ˆcnet-2fa] [ˆcnet-2fa]: (“Two-Factor Authentication: FAQ” 2016)

[22] Die Preise wurden am 1. März 2016 auf nexmo.com/products/voice/, tropo.com/pricing und twilio.com/voice/pricing abgefragt

4 Anforderungen

Dieses Kapitel beschreibt das Durchführen einer Anforderungsanalyse festgehalten. Anhand der Anforderungsanalyse sollen die Anforderungen für die entwickelnden Software ermittelt werden. Die Anforderungen bilden die Basis für die Architektur, das Softwaredesign, die Implementationund die Testfälle. Ihnen ist dem entsprechend ein sehr grosser Stellenwert zuzuschreiben.

4.1 Use-Cases

Im Nachfolgenden werden alle UseCases aufgelistet die im Rahmen dieser Thesis gefunden wurden.

4.2 Akteure

Akteure	
Developer	Der Developer ist der Entwickler der Webseite. Er möchte sein programmiertes oder sein verwendetes Social-Media Modul mit dem Authentifizierungsschnittstellen-Service schützen.
User	Der User ist der Endkunde. Er nimmt am Social-Media Modul teil und authentifiziert sich über den Authentifizierungsschnittstellen-Service

4.2.1 Diagramm

Das Use-Case Diagramm illustriert die nachfolgenden Use Cases. Dadurch kann rasch ein Überblick über die zu entwickelnde Lösung geschaffen werden.

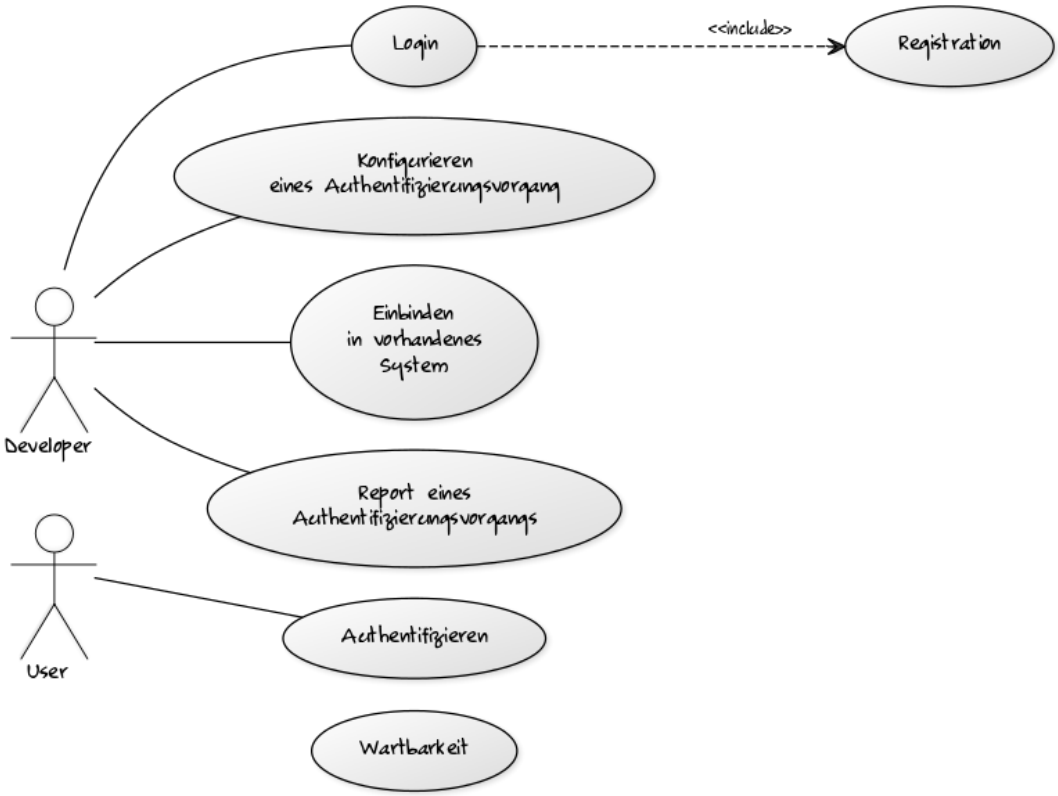


Abbildung 4.1: Use-Case Diagram

UC-11 Registration

UseCase	
Ziel	Ein Developer ist am Authentifizierungsschnittstellen-Service registrieren
Beschreibung	Ein Developer muss sich am Authentifizierungsschnittstellen-Service registrieren können
Akteure	Developer
Vorbedingung	Keine
Ergebnis	Registrierter Developer
Hauptszenario	Der Developer füllt ein Registrationsformular aus und bestätigt seine E-Mail Adresse
Alternativszenario	-

UC-12 Login

UseCase	
Ziel	Ein Developer kann sich beim Authentifizierungsschnittstellen-Service
Beschreibung	Ein Developer muss sich am Authentifizierungsschnittstellen-Service authentifizieren können
Akteure	Developer
Vorbedingung	Der Developer ist registriert.
Ergebnis	Authentifizierter und eigeloggter Developer
Hauptszenario	Der Developer loggt sich mit E-Mail und Passwort am Authentifizierungsschnittstellen-Service ein.
Alternativszenario	Der Developer sendet sich das verpasste Passwort per E-Mail zu. Erstellt über den im erhaltenden E-Mail enthaltenen Link ein neues Passwort und loggt sich mit E-mail und dem neuen Passwort am Authentifizierungsschnittstellen-Service ein.

UC-21 Konfigurieren eines Authentifizierungsvorgang

UseCase	
Ziel	Es ist eine neuer Authentifizierungsvorgang für ein neus Social Media-Modul konfiguriert
Beschreibung	Der Developer kann ein neuer Authentifizierungsvorgang eröffnen
Akteure	Developer
Vorbedingung	Der Developer hat sich am System angemeldet
Ergebnis	Neuer Authentifizierungsvorgang

UseCase	
Hauptszenario	Der Developer eröffnet einen neuen Authentifizierungsvorgang. Er benennt ihn sinnig. Die zu verwende(n) Authentifizierungskomponennten werden ausgewählt. Bei der Konfiguration unterstützen die Resultate die Studie den Developer für die optimalte Konfiguration. Am Ende der Konfiguration werden die Akzeptanzkritieren für eine erfolgreiche Authtentifizierung festgelegt.
Alternativszenario	Ein bestehender Authentifizierungsvorgang wird dupliziert

UC-25 Einbinden in vorhandenes System

UseCase	
Ziel	Die Authentifizierungsschnittstelle kann in ein (bestehendes) System eingebunden werden
Beschreibung	Der Developer kann die Authentifizierungsschnittstelle in seinem System integrieren
Akteure	Developer
Vorbedingung	Der Developer hat sich am System angemeldet. Der Developer hat ein neues Authentifizierungsvorgang konfiguriert
Ergebnis	Der Developer hat eine Möglichkeit die Authentifizierungsschnittstelle mit seinem konfigurierten Authentifizierungsvorgangs in seiner Software einzubinden
Hauptszenario	Der Developer öffnet die Einbindeseite. Es werden ihm alle Schritte zur Erfolgreichen Einbindung aufgelistet. Der Code liegt individualisiert vor. Der Developer kopiert den Code in sein Programm
Alternativszenario	-

UC-31 Authentifizieren

UseCase	
Ziel	Der User ist authtentifiziert oder der User abgelehnt
Beschreibung	Der User probiert sich über den Authentifizierungsschnittstellen-Service zu authentifizieren um an einem Social-Media Modul teilzunehmen
Akteure	User
Vorbedingung	Der Developer hat den Authentifizierungsvorgang konfiguriert und in seinem System eingebunden.
Ergebnis	Der Authentifizierungsschnittstellen-Service authentifiziert den User oder lehnt ihn ab.

UseCase	
Hauptszenario	Der User wird vom Social Media Modul an den Authentifizierungsschnittstellen-Service weitergeleitet. Der User authentifziert sich. Der User kann die Eingabe des Social Media Modul erfolgreich abschliessen
Alternativszenario	Der User wird vom Social Media Modul an den Authentifizierungsschnittstellen-Service weitergeleitet. Der User wird vom System abgelehnt. Der User kann die Eingabe des Social-Media Modul nicht erfolgreich abschliessen.

UC-41 Report eines Authentifizierungsvorgangs

UseCase	
Ziel	Die Verwendung des Authentifizierungsvorgangs ist übersichtlich dargestellt
Beschreibung	Um den Verwendung des Authentifizierungsvorgangs auszuwerten soll ein Report erstellt werden
Akteure	Developer
Vorbedingung	Der Developer hat sich am System angemeldet. Der Developer hat ein neues Authentifizierungsvorgang konfiguriert. (Der Authentifizerungsvorgang ist eingebunden und verwendet worden)
Ergebnis	Report eines Authentifizierungsvorgangs
Hauptszenario	Nach Beenden eines Quizes, Votings, Wettbewerbs logt sich der Developer im System ein und generiert einen automatisierten Report um die Verwendung des Authentifizierungsvorgangs auszuwerten.
Alternativszenario	Um den Zwischenstand deines Quizes, Votings, Wettbewerbs auszuwerten logt sich der Developer im System ein und generiert einen automatisierten Report um die Verwendung des Authentifizierungsvorgangs auszuwerten.

UC-51 Wartbarkeit

UseCase	
Ziel	Der Authentifizierungsschnittstellen-Service soll mit geringen Aufwand angepasst werden können.
Beschreibung	
Akteure	Entwicklungsteam-Mitglied
Vorbedingung	Das Entwicklungsteam-Mitglied hat Zugriff auf das Entwicklungs-Repository, Testsystem und Livesystem
Ergebnis	Die Anpassung ist integriert
Hauptszenario	Dank eingehaltenen Coderichtlinien ist es einfach möglich die Anpassung einzupflegen

UseCase	
Alternativszenario	-

4.3 Anforderungen

Die Anforderungen sollen basierend auf der Satzschablone erstellt werden. Ziel ist sprachliche Missverständnisse dadurch zu vermeiden. Die Schablone fördert eine syntaktische Eindeutigkeit der Anforderungen und eine optimalen Zeit- und Kostenrahmen für die Verfassung.

4.3.1 Aufbau

Die folgenden Abbildungen zeigen den Aufbau der Satzschablonen. Es wird zwischen der grundlegenden Version ohne zeitlichem oder Bedienungsorientiertem Aspekt und der Schablone mit diesen Eigenschaften unterschieden.

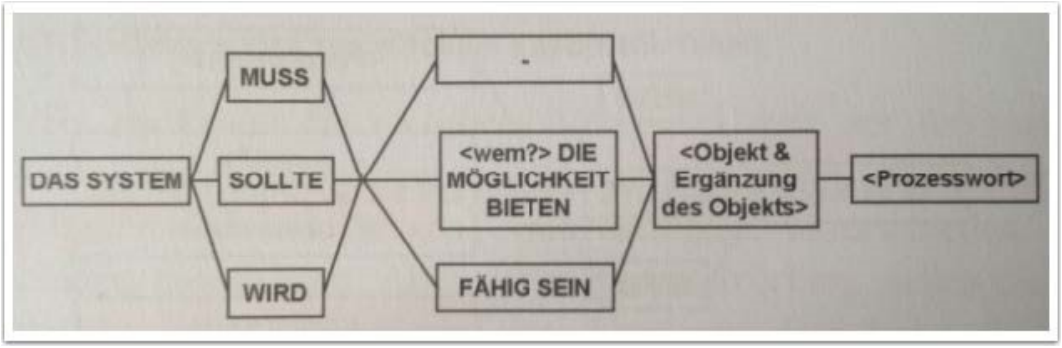


Abbildung 4.2: Basis Schablone *Quelle Rupp*[1]

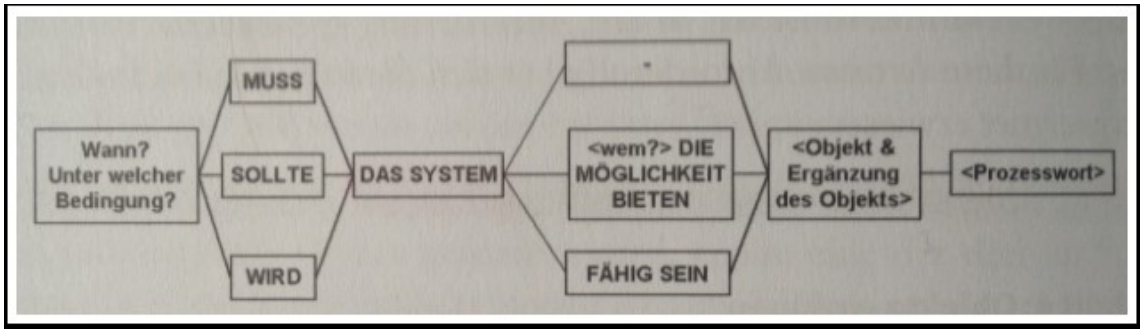


Abbildung 4.3: Erweiterte Schablone *Quelle Rupp*[2]

[1] Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering (Rupp 2011)
[2] Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering (Rupp 2011)

4.4 Funktionale Anforderungen

Die funktionalen Anforderungen legen die Funktionen des Authentifizierungsschnittstellen-Service fest. Die Wünsche des Arbeitgebers aus sind als Anforderungen umformuliert. Die funktionalen Anforderungen dienen als Grundlage für die Testfälle. Die Testfälle wiederum, bringen den Beweis dar, dass alle gewünschten Funktionen implementiert wurden.

Funktionale Anforderungen werden als FREQ-*Identifikation* bezeichnet

4.4.1 FREQ-111 Developer Registration

UC-Referenz	UC-11
Beschreibung	Ein Developer kann sich an der Authentifizierungsschnittstellen-Service registrieren.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.2 FREQ-112 Developer Login

UC-Referenz	UC-12
Beschreibung	Ein Developer muss sich an der Authentifizierungsschnittstellen-Service mittels E-Mail und Passwort anmelden.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.3 FREQ-113 Developer Passwort vergessen

UC-Referenz	UC-11, UC-12
Beschreibung	Ein Developer kann ein Passwort per E-Mail anfordern.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.4 FREQ-114 Developer Passwort ändern

UC-Referenz	UC-11, UC-12
Beschreibung	Ein Developer kann sein Passwort ändern. Dafür muss der Developer das alte und neue Passwort angeben.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.5 FREQ-211 Konfigurieren einer neuen Social-Media Modul Authentifizierungsvorgang

UC-Referenz	UC-21
Beschreibung	Ein Developer kann ein neuer Authentifizierungsvoragn für sein neus Social-Media Modul erfassen.
Techn. Risiko	Niedrig
Business Value	Sehr Hoch

4.4.6 FREQ-214 Studien Ergebnis zur Konfiguration nutzten

UC-Referenz	UC-21
Beschreibung	Ein Developer kann zur Konfiguration des Authentifizierungsvorangs die Studien-Ergebnisse visualisiert nutzen
Techn. Risiko	Niedrig
Business Value	Mittel

4.4.7 FREQ-214 Anpassen eines Authentifizierungsvorgangs

UC-Referenz	UC-21
Beschreibung	Ein Developer kann ein neues Social-Media Modul erfassen
Techn. Risiko	Hoch
Business Value	Mittel

4.4.8 FREQ-215 Authentifizerungs-Stufe auswählen

UC-Referenz	UC-21
Beschreibung	Ein Developer muss eine Authentifizerungs-Stufe für den Authentifizierungsvorgangs auswählen
Techn. Risiko	Niederig
Business Value	Hoch

4.4.9 FREQ-251 Generierung von Code für einbinden in vorhandenes System

UC-Referenz	UC-25
Beschreibung	Ein Developer kann einen Code generieren lassen. Dieser Code soll ihm die Integration in sein System vereinfachen
Techn. Risiko	Sehr Hoch
Business Value	Hoch

4.4.10 FREQ-311 Authentifizieren

UC-Referenz	UC-31

Beschreibung	Ein User kann isch über den Authentifizierungsschnittstellen-Service authentifizieren um am Social-Media Modul teilzunehmen. Der Authentifizierungsschnittstellen-Service authentifiziert oder lehnt den User ab.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.4.11 FREQ-411 Report generieren

UC-Referenz	UC-41
Beschreibung	Der Developer kann ein Report generieren. Der Report soll die Verwendung übersichtlich darstellen.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.5 Nicht Funktionale Anforderungen

Nicht Funktionale Anforderungen werden als FREQ-*Identifikation* bezeichnet.

4.5.1 NFREQ-110 Betriebsystemunabhängigkeit

UC-Referenz	Alle
Beschreibung	Der Authentifizierungsschnittstellen-Service muss auf allen bekannten Betriebsystemen mit HTML5 und javascritfähigen Browser vewerdent werden können.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.5.2 NFREQ-115 Wartbarkeit

UC-Referenz	UC-51
Beschreibung	Die Wartbarkeit des sSystems soll sichergestellt werden
Techn. Risiko	Mittel
Business Value	Mittel

4.5.3 NFREQ-120 Einfache Integration

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Der Authentifizierungsschnittstellen-Service soll einfach im vorhandenen System eingebunden werden können.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.4 NFREQ-120 Performance

UC-Referenz	UC-31
Beschreibung	Das System soll insbesondere an der Stelle der Authentifzierung Performant sein.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.6 Risiken

Nachfolgend sind die im Gespräch mit dem Auftraggeber gefundenen Riskiken bezüglich der Bachelorarbeit, sowie deren Auswirkungen, aufgeführt.

4.6.1 R-01 Akzeptanz

Developer und insbesondere auch User, welche den Authentifizierungsschnittstellen-Service verwenden soll, sind völlig unterschiedlich. Deren unterschiedliche Ansprüche machen es schwierig, eine Lösung zu entwickeln welchen Akteuren gerecht wird.

Da der Auftraggeber sowohl die Zielgruppe Developer wie auch User kenn, kann er hier gezielt Feedback geben.

Die Auswirkung bei Eintritt dieses Risikos ist im Rahmen der Bachelorarbeit gering, da der Erfolg der Arbeit nicht von der tatsächlichen Verwendung im produktiven Umfeld abhängt.

4.6.2 R-02 Kosten

Da es sich bei diesem Projekt um eine Bachelorarbeit handelt, besteht kein Personalkostenrisiko. Kostenpflichtige Produkte Dritter werden nicht verwendet. Einzig der Betrieb/Hosting der Bachelorarbeit verursacht Kosten. Das Kostenrisiko kann dank fixen Leistungsparameter auf ein Minimum reduziert werden.

4.6.3 R-03 Überkomplexität

Es besteht die Möglichkeit, dass die Komplexität des zu entwickelnden Systems viel höher ist, als angenommen. Da die Komplexität nur zu einem gewissen Grad durch Architekturentscheide beeinflusst werden kann, muss besonderes Augenmerk auf dieses Risiko gelegt werden.

Dieses Risiko wird mit hoher Wahrscheinlichkeit eintreten.

Die Auswirkung bei Eintritt dieses Risikos ist, dass nicht der gesamte Umfang der Bachelorarbeit erarbeitet werden kann, weil zur Lösung der Komplexitätsprobleme zusätzliche Zeit benötigt wird.

4.6.4 R-04 Systemumfeldänderungen

Umsysteme könnten während der Projektphase dieser Bachelorarbeit massgeblich verändert werden.

Dieses Risiko wird mit sehr geringer Wahrscheinlichkeit eintreten.

Die Auswirkung bei Eintritt dieses Risikos kann nicht abgeschätzt werden. Situativ muss dieses Risiko behandelt werden.

4.6.5 R-05 Schlechte/Unzureichende Framework

Die Bachelorarbeit wird basierend auf verschiedenen Frameworks umgesetzt. Das Risiko, dass Frameworks nicht wie beschrieben funktionieren, schlecht dokumtiert oder instabil sind besteht.

Dieses Risiko wird mit mittlerer Wahrscheinlichkeit eintreten Als Auswirkungen dieses Risikos sind Wechsel des Frameworks oder gar manuelle Entwicklungen und daraus zusätzliche nicht einschätzbare Aufwendungen nötig.

4.6.6 R-06 Termineinhaltung

Der fixe Abgabetermin der Semesterarbeit gilt es einzuhalten. Das Risiko das die Arbeit verspätet abgegeben wird besteht.

Dieses Risiko wird mit geringer Wahrscheinlichkeit eintreten. Die Auswirkung bei Eintritt dieses Risikos ist das nicht Bestehen der Arbeit.

4.6.7 R-07 Auslastung

Das Projekt wird durch einen Mitarbeiter getragen. Dieser ist sowohl im Beruf wie auch privat stark ausgelastet. Der hohe schulische Aufwand kann beeinflusst werden. Mit zusätzliche Ausfälle durch Krankheit oder nicht vorhersehbaren Vorfällen muss gerechnet werden.

Das Risiko wird mit mittlerer Wahrscheinlichkeit eintreten. Die Auswirkungen bei Eintritt dieses Risikos werden sich in der Qualität und Quantität der Arbeit wiederspiegeln.

4.6.8 Risikomatrix

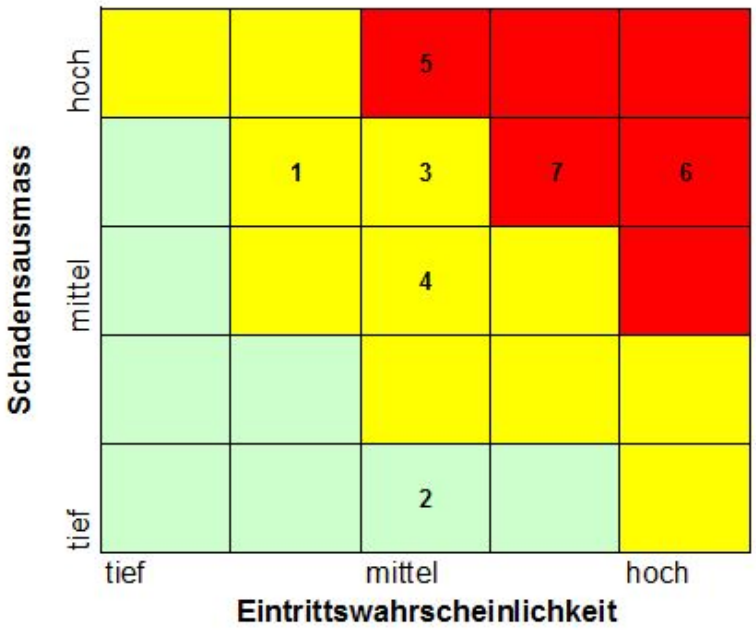


Abbildung 4.4: Risikomatrix[3]

Rot: Massnahmen erforderlich

Gelb: Risiken beobachten

Grün: Keine Massnahmen erforderlich

1 Akzeptanz

2 Kosten

3 Überkomplexität

4 Systemumfeldänderungen

5 Schlechte/Unzureichende Frameworks

6 Termineinhaltung

7 Auslastung

4.6.9 Massnahmen

Um das Zusammenspiel der verschiedenen Technologien und die daraus resultierende Komplexität einschätzen zu können wird vor Projektbeginn ein Prototyp mittels Durchstich durch alle Technologien erstellt. Danach kann die Komplexität im Zusammenspiel der Technologie eingeschätzt und bei Bedarf eine Technologie durch eine andere Ersetzt werden. So kann das Risiko 3 Überkomplexität und Risiko 5 Schlechte/Unzureichende Frameworks minimiert werden.

[3] Die Risikomatrix wurde basierend auf der Excel-Vorlage der Stadtpolizei Zürich Abteilung Informatik entworfen

Das Projekt ist über eine Anzahl von Feiertagen gelegt, welche gebraucht werden könnten. Zusätzlich wurden vom Studenten eine Arbeitswoche Ferien genommen, welche im Notfall auch für die Arbeit verwendet werden könnte. Durch diese Massnahmen sollte das Risiko 6 Termineinhaltung minimal bleiben. Das Risiko 7 Auslastung kann nicht direkt vermindert werden. Die Aktivitäten im Bereich der freiwilligen Arbeit wurde auf ein Minimum reduziert. Für die restliche freiwilige Arbeit wurde mit Freunden ein Nofallszenario entwickelt, so kann der Student bei Bedarf seine freiwillige Arbeit durch andere Personen übernehmen lassen. Der Kontakt mit dem mit Arbeitgeber wird intensiv gepflegt um, so bei Bedarf die Arbeitsbelastung zu vermindern. Die Massnahmen welche für Risiko 6 ergriffen wurden entschärfen auch Risiko 7.

5 Design der Software

In diesem Kapitel soll ein System entworfen werden. Das System soll den Anforderungen, welche im vorherigen Kapitel definiert wurden, entsprechen.

5.1 Authentifizierungsmöglichkeiten

5.2 Integration der Schnittstelle

Wie in der Anforderungsanalyse und Aufgabenstellung geschrieben, soll die Schnittstelle möglichst einfach in Bestehende Systeme integriert werden können. Bevor wir untersuchen wie wir die Integration umsetzten können, bedarf es die wichtigsten bestehenden Systeme zu kennen um evtl für diese Systeme eine spezifisch einfach Integration zu entwickeln.

5.2.1 Bestehende Systeme für Votings, Wettbewerbe und Quizes

Das bestehende Social-Media Modul wird als Teil einer Webseite in einer Webapplikation geführt. Webapplikation, welche Inhalte verwalten, werden sinngemäss Content Management Systeme genannt. Die Abkürzung CMS hat sich im IT-Fachjargon etabliert. Statista.com wertetet mehrmals im Jahr die Verbreitung der verschiedenen CMS aus.[1] Folgend ist die Erhebung aus dem November 2015 abgebildet:

Die von statista.com veröffentlichten Zahlen wurden mit Werten von W3techs.com verglichen[2]. Die Unterschiede sind für unsere Verwendung minimal und liegen im 10tels Prozentbereich. Da beide bekannten Statistik unternehmen auf die selben Werte gekommen sind, kann von einem hohen Warheitsgrad ausgegangen werden. Beim Betrachten der Statistik fällt auf das Wordpress mit 25,2 mit Abstand am meisten genutzt wird. Alle dynamischen Webseiten unter den Top 10 basieren auf Systemen in PHP[3]. Adobe Dreamviewer und FrontPage sind keine Systeme welche auf dem Server betrieben werden. Sie sind Editoren welche auf dem jeweiligen Computer ausgeführt werden und danach mehrheitlich HTML, CSS und Javascript Code an den Server ausliefern. Funktionalitäten werden mit den beiden Editoren manuell geschrieben.

Basierend auf diesen statistischen Erkenntnissen lohnt es sich die Wordpress Welt kennen zu lernen und recherchieren wie dort eine Authentifizierungsschnittstelle eingebunden werden könnte.

5.2.2 Wordpress PlugIn Hook

Erweiterungen im Wordpress nennen sich Plugins. Die Plugins können direkt über das CMS-Backend eingespielt werden. Alternativ können Sie natürlich manuell installiert werden. Zum

[1] CMS Nutzungsstatistik von statista.com ("Top 10 CMS November 2015" 2015)
[2] CMS Nutzungsstatistik von w3techs.com ("Usage of Content Management Systems for Websites" 2015)
[3] Die Information wurde von den jeweiligen Hersteller- bzw. Communitywebseiten bezogen.

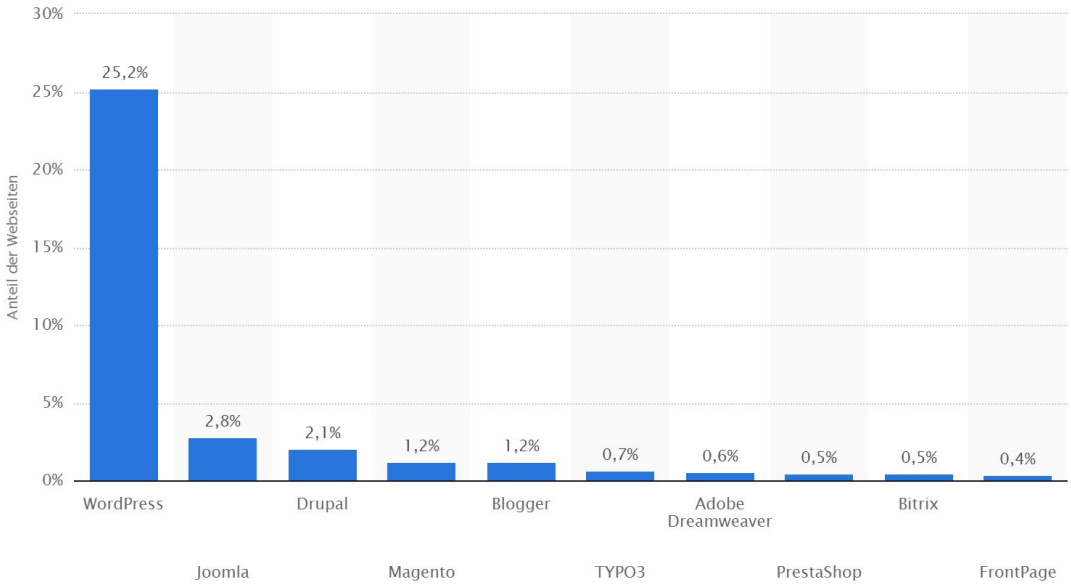


Abbildung 5.1: Nutzungsanteil CMS weltweit *Quelle:de.statista.com*

Beispiel in dem man ein Plugin selber Programmiert oder beim Hersteller oder über das Plugin-Verzeichnis von Wordpress[ˆplugin-verzeichnis] downloadedt. Wordpress sammelt zugleich die aktiven Installationen der PlugIns (sofern man als Entwickler den Informationsaustausch nicht unterbindet). Die Gesamtzahl wird im CMS-Backend Wordpress und auf Ihrer Plugin-Verzeichnis Webseite[ˆplugin-verzeichnis] veröffentlicht. Dank dieser Kennzahl kann nun die meist verbreiteten Plugins herrausgefunden werden.

Wordpress basiert auf einem sogennanten Hook-System. "Hook" eins zu eins übersetzt bedeutet "Haken", "Aufhänger" oder "Greifer". Ein Hook ist im Wordpress eine definierte Codestelle bei der man seinen eigenen Code einhaken kann. Der PlugIn Entwickler definiert diese Hooks um anderen PlugIns oder Funktionalitäten zu erlauben sein PlugIn zu erweitern. Auch der Core vom Wordpress enthält solche Hooks. Dadurch soll verhindert werden, dass PlugIn's oder der Core von Wordpress direkt umgeschrieben werden muss und dann nicht mehr einfach so unabhängig upgedatet werden kann. Um unsere Schnittstelle einzubinden, könnten wir evtuell also solche Hooks verwenden. Dieser "Hook"/Haken hat lustigerweise auch einen Haken: Der PlugIn-Entwickler kann selbständig bestimmen ob und wo er solche Hooks einsetzen will und welche Möglichkeiten dann zur Verfügung stehen. Kommerzielle PlugIn's verfolgen vielfach den Weg möglichst verschlossen zu agieren um mögliche Erweiterungen monetär umzusetzen und so eine Abhängigkeit zu erzeugen. Diese These gilt es nun zu untersuchen. Dafür wurden verschiedene Social Plugin's ausgewählt. Die Top 1000 installierten Wordpress PlugIns welche von der Art Social-Media Modul waren, ein paar Stichproben von kommerziellen Plugins und Stichproben aus in Beiträgen empfohlenen PlugIns:,[4][5]

[4]Das Pluginverzeichnis befindet sich unter http://de.wordpress.org/plugins
[5]Envato bietet eine Plattform für den Verkauf von Wordpress-Plugin's an http://market.envato.com

Tabelle 5.1: Recherche PlugIn's

PlugIn			
WP-Polls	kostenlos	100000+	Über "wp_polls_add_poll" könnte man den erstellten Poll authentfizieren und bei fehlerhafter Authentifizierung löschen
__Polldaddy Polls & Ratings_	_ Freemium	20000+	-
Wp-Pro-Quiz	kostenlos	20000+	Hooks vorhanden. Nicht für eine Authentifizierungsschnittstelle zu gebrauchen.
Responsive Poll	15$	-	Keine Hooks. Laut Hersteller sind welche geplant (Zeitpunkt ungewiss)
TotalPoll Pro	18$	-	Hooks vorhanden. Ähnlich wie bei WP-Polls könnte man evtl. den erstellten Datensatz löschen. Jedoch ist dies ohne Kauf nicht ersichtlich.
Easy Polling	15$	-	-
Opinion Stage	kostenlos	10000+	-
Wedgies	Freemium	800+	-

Wir haben nun verschiedene Wordpress-Plugin's für Umfragen, Wettbewerbe & Abstimmungen auf Hooks untersucht. Alle PlugIn's bieten gar keinen Hook an oder keinen Hook, welcher unseren Anforderungen einer einfachen Integration genügt. Die aufgelisteten Plugins bilden eine wesentliche Verbreitung ab. Selbst wenn wieder erwartet alle nicht untersuchten Plugin's eine perfekte Hookanbindung liefern würden, hätten wir, mit den nicht getesteten Plugin's eine zu geringe Verbreitung. Der Ansatz die Integration per Hooks zu machen muss also fallen gelassen werden.

5.2.3 Parallellen im ähnliches Anwendungsfeld

Der vertieften Research der letzten Kapitel wird verlassen und es wird probiert einen anderen Herangehensweise zur Findung der Lösung zu nehmen: Forscher adaptieren immer wieder erfolgreiche Modelle aus anderen Bereich in ihr Gebiet. Vielfach wird die Natur als erfolgreiches Vorlagemodell genommen. Ganz soweit wird hier nicht gegangen. Payment-Gateways wie der Schweizer Anbieter Datatrans müssen Webshop-Entwicklern auch eine Möglichkeit bieten das Gateway einfach in Ihren Webshop einbinden zu können. Auch bei Ihnen steht die Sicherheit auf der obersten Stufe und eine einfache Integration ist für den Erfolg trotz internationalem Druck von nöten. Dabei fährt Datatrans eine Zweiwegstrategie. Sie stellen für bekannte Shopsysteme gleich ganze PlugIns zur Verfügung[6]. Auf der anderen Seite bieten Sie ausführliche beschriebene und einfache Schnittstellen an.

Datatrans Zahlungsablauf

Um die Gateway-Implementation der Datatrans als Ganzes zu verstehen, führen wir uns der generellen Ablauf eines Payment Gateways eines Webshopeinkaufs bei Datatrans vor Augen. Der Ablauf:

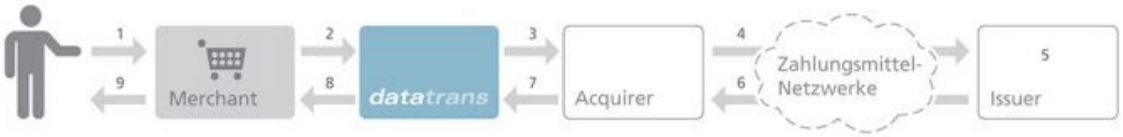


Abbildung 5.2: Nutzungsanteil Zahlungsablauf Webshop mit Datatrans *Quelle:datatrans*

1. Der Endkunde wählt Produkt aus und schliesst die Bestellung ab
2. Der Webshop/Merchant zeigt Zahlungsseite von Datatrans, Karteninhaber gibt seine Kartendaten ein. 3.-7.Datatrans autorisiert und verarbeitet wennmöglich die Transaktion zum Acquirer.
3. Datatrans zeigt den Status dem Kunden an und sendet Status dem Merchant zurück.
4. Merchant zeigt dem Karteninhaber die Antwortseite (erfolgreich oder abgelehnt)[7]

[6] Übersicht der Web-Shop PlugIn's ("Webshop" 2016)

[7] Für die Bachelorarbeit wurde die V 9.1.13 verwendet ("Datatrans ECom - Technical Implementation Guide" 2016)

Datatrans XML/SOAP API Lightbox Mode

Bei Schritt 2 des Zahlungsablaufs ruft der Webshop das Datatransgateway auf. Beim "Lightbox Mode" wird dabei ein iframe in einem Overlay über die Webseite gelegt und der Webshop ansich verdunkelt dargestellt.

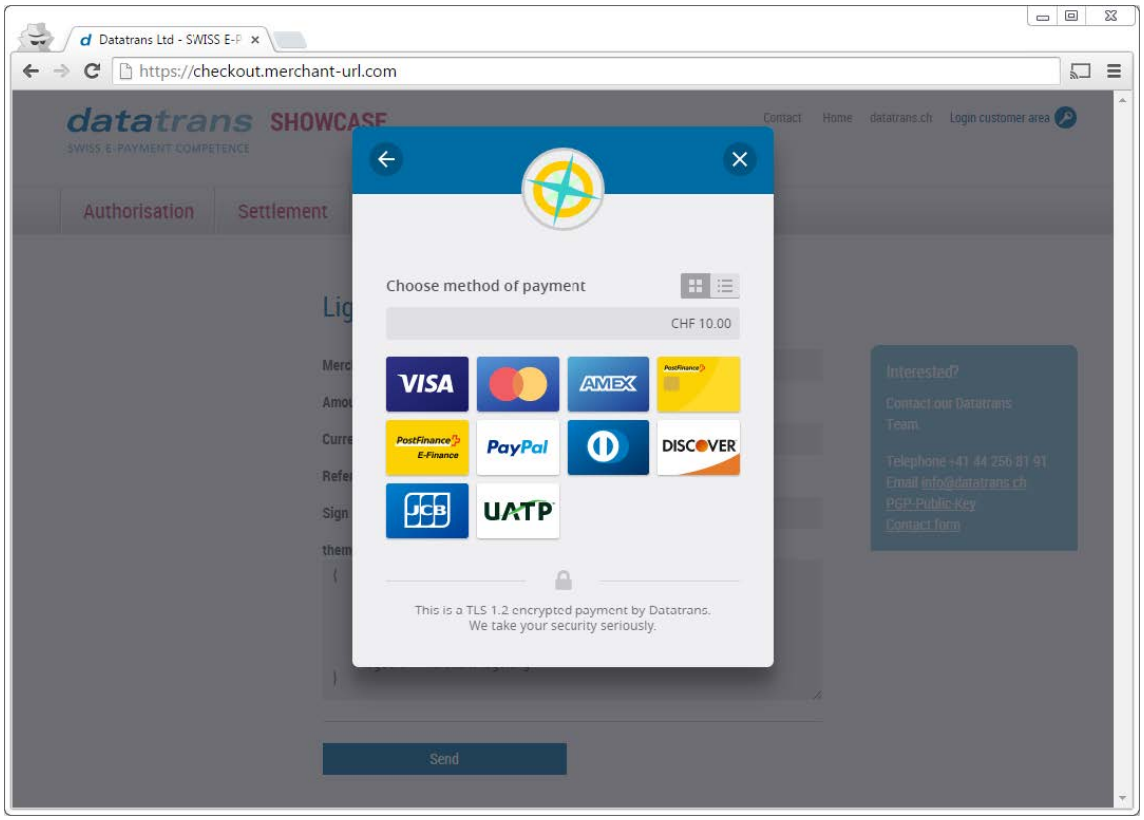


Abbildung 5.3: Datatrans Lightbox Integration *Quelle:datatrans*

Das Gateway muss eine minimum an Informationen erhalten, um den Zahlungsvorgang überhaupt starten zu können. So muss es wissen, wer der Verchäufer ist. Datatrans regelt dies über eine Merchan-ID. Wie viel Geld in welcher Währung verkauft werden sollte, muss Datatrans über amount und currceny mitgeteilt werden. Um dem Shop später mitteilen zu können, welche Bestellung erfolgreich verarbeitet wurde, braucht es eine Referenznummer. Die Referenznummer nennt Datatrans singemäss refno. Die Ganzen Parameter werden optional mit einem sign-Parameter gesichert und mittels Html-Form dem Javascript übergeben:[8]

[8]Für die Bachelorarbeit wurde die V 9.1.13 verwendet ("Datatrans ECom - Technical Implementation Guide" 2016)

```
<script src="https://code.jquery.com/jquery-1.11.2.min.js"></script>
<script src="https://pilot.datatrans.biz/upp/payment/js/datatrans-1.0.2.js"></script>

    <form id="paymentForm"
         data-merchant-id="1100004624"
         data-amount="1000"
         data-currency="CHF"
         data-refno="123456789"
         data-sign="30916165706580013">
         <button id="paymentButton">Pay</button>
    </form>

<script type="text/javascript">
     $("#paymentButton").click(function () {
        Datatrans.startPayment({'form': '#paymentForm'});
     });
</script>
```

6 Studie

6.1 Art der Studie

Wie die Aufgabenstellung und der Auftraggeber fordert, wird eine Studie in Form einer Umfrage mit Hilfe eines digitalen Fragebogens durchgeführt. Bevor die Studie aufgebaut wird gilt es sich Vor- und Nachteile einer schriftlichen Befragungen bewusst zu machen und basierend auf diesem Wissen die Studie zu planen.

6.1.1 Vor - und Nachteile schriftlicher Fragebogen

Schriftliche Befragungen mit Fragebogen können in verschiedenen Varianten durchgeführt werden. Deshalb unterscheiden sich zwischen den Varianten gewisse Vor- und Nachteile zu persönlich-mündlichen oder telefonischen Studie. Es wird versucht, die Möglichkeiten und Grenzen mit dem grössten gemeinsamen Nenner aufzuführen. Folgende Punkte ergeben die wichtigsten Vorteile:

- Die Kosten sind geringer. Hippler[1] definiert den Richtwert von einem Viertel der Kosten zu einer persönlich-mündlichen oder telfonischen Studie.
- Schriftliche Befragungen mit Fragebogen kann in einem relativ kurzen Zeitrum realisiert werden
- Dem zu Befragenden kann eine grössere Anonymität gegeben werden
- Verteilung in verschiedene Regionen einfach und zeitnah möglich. Insbesondere bei Online Umfrage.
- Einfluss von aussen gering. Zahlreiche Studien[2] belegen, dass Personen welche eine Studie im Interview die Beantwortung beeinflussen
- Die Antworten der befragten sind durch die Abwesenheit des Interviewers und durch die Anonymität ehrlicher. Dieser Punkt ist wissenschaftlich jedoch noch ziemlich umstritten. Schnell bezweifelen verschiedene Psychologen und Soziologen diesen Umstand. So auch Dr. Reuband in seinem Paper “Möglichkeiten und Probleme des Einsatzes postalischer Befragungen”[3]

Diesen Vorteilen stehen auch gewisse Nachteile gegenüber. Die folgenden Punkte erläutern die wichtigsten Nachteile die verschiedene Varianten von Fragebögen gemeinsam haben:

- Wenn eine Studie eine zu grosse Nonresponse-Rate hat, ist eine Verallgemeinerung der Resultate unzulässig. Kurz die Bachelorarbeit würde mit der Studie das Ziel verfehlen. Bei einer schriftlichen Studie kann die Ausfallquote aber nicht im Vornherein eingeschätzt werden.

[1] (Hippler 1988)
[2] Studien und Erklärungen zu Fremdbestimmung durch François Höpflinger(Höpflinger 2011)
[3] (Reuband 2001)

- Die Datenerhebungssituation kann nicht kontrolliert oder bestimmt werden. Wo und unter welchen Umständen der Fragebogen beantwortet wird kann nicht bestimmt und höchstens erfragt werden.
- Nachfragen basierend auf Antworten können nicht spontan gestellt werden, sondern müssen im Vornherein geplant werden.
- Bestimmte Bevölkerungsteile werden durch diese Art der Studie ausgeschlossen. Zum Beispiel Analphabeten oder bei Onlineumfragen Personen mit zu wenig technischem Know-How oder Hardware.

6.1.2 Fazit

Es gilt also die Vorteile der schriftlichen Fragebogen bei der Gestaltung der Studie zu nutzen. Das bestimme Bevölkerungsteile ausgeschlossen werden, verfältscht das Ergebniss nicht, da die Anforderung für die Umfrage geringer oder gleich hoch ist wie die der nutzung eines Social-Media Moduls. Die Nonresponse-Rate ist ein Risiko, dass unbedingt Rechnung getragen werden muss um nicht eine ungültige Studie zu erhalten. Damit die Problematik Nonresponse-Rate, der Umgang mit der Datenerhubbssituation und eine geplante vorhersehbare Fragestellung ausgefürt werdne kann gilt es sich weiter den korrekten Aufbau einer Studie zu recherchieren.

6.2 Hauptziel der Studie

In den vergangenen Kapiteln wurden immer wieder verschiedene Authentzifizierungsarten erwähnt und beschrieben. Diese verschiedenen Möglichkeiten gilt es mit einander zu vergleichen.

6.3 Aufbau Gesamtkonzept

"Ein Fragebogen soll als Gesamtkomzept (Einleitung, Hauptteil, Endteil, Design, Aufmachung) betrachtet werden, in dem die Reihenfolge und die Struktur der Frage wichtige Einflussfaktoren zur Erlangung korrekter Daten sind"[4]

In den folgenden Abschnitten wird die Theorie für die Entwicklung dieses Gesamtkonzept abgebildet.

6.3.1 Einleitung

Die Einleitung soll die Befragten motivieren an der Studie teilzunehmen und allgemeine Hinweise zur Studie geben. Die folgenden Fragen wurden Batinic (WWW-Fragebogengenerator) und dem Institut für webbasierte Kommunikation und E-Learning zusammen getragen und und für die Studie der Bachelorarbeit beantwortet:

Wer wird befragt?

Die Hauptzielgruppe sind Schweizer welche Deutsch sprechen. Die Nebenzielgruppe sind Personen die Deutsch sprechen aus anderen Nationen. Die Telnehmer sollen die technische Know-How besitzen an einem Social-Media Modul teilzunehmen und den Internetzugriff haben.

Was ist der Zweck bzw. das Ziel der Untersuchung?

Die Studie dient dem Programmierer zur richtigen Konfiugration der Authentifizierungsmethode für seinen aktuellen Verwendungszweck.

Was passiert mit den Ergebnissen?

Die Ergebnisse werden Programmierer zum Konfigurieren der Authentifizierungsmethode zur Verfügung gestellt und in der Bachelorarbeit veröffentlicht.

Können die Ergebnisse eingesehen werden?

Durch diesen Punkt kann besonders Vertrauen und Wohlwollen gewonnen werden.[5] Deshalb soll das Kapitel Studie der Bachelorarbeit auf Wunsch den Befragten per E-Mail zugesendet werden.

[4] Zitat vom Institut für webbasierte Kommunikation und E-Learning und Gräf et al. 2001 (Pratzner 2001)
[5] (Pratzner 2001)

Wer führt die Befragung durch?

ZHAW Student Christian Bachmann im Auftrag der inaffect AG

Kontakt für Support und Fragen

Christian Bachmann, bachmch3@students.zhaw.ch

Wie viel Zeit muss der Befragte Investieren?

Eine Einschätzung der durchschnittlich benötigen Zeit und Anzahl der Fragen sollte genannt werden. Folgend ist das Diagramm aus der Studie von Bosnjak und Batini abgebildet. Die Erkenntnis aus der Studie zeigt, dass nicht nur unter dem Motto je kürzer desto besser gehandelt werden sollte. Die Studie ist jedoch schon 15 Jahren alt und ist deshalb differenzierter zu sehen. Die Studie der Bachelorarbeit streben einen Aufwand von 8-12 Minuten an.

6.3.2 Hauptteil/Fragen

Offensichtlich stellt der Hauptteil den Löwenanteil des Aufwands dar.

Erste Frage

Die erste Frage ist nach Dillman[6] von grosser Bedeutung. Mit ihr wird Motivation und Einsatz für den ganzen Fragebogen gesetzt. Diese Frage soll als Interesse und Neugier der Befragten bewirken.

Das Institut für webbasierte Kommunikation und E-Learning hat dafür aus verschiedenen Studien die wichtigsten Kriterien für eine erfolgreiche erste Frage zusammen getragen[7]: - **Einfache Formulierung** Der Befragte versteht sofort um was es geht und glaubt daran dass er die Fragen meistern kann - **Kurze Beantwortungszeit, keine offenen Fragen** Ein schnelles überwinden der ersten "Hürde" motiviert den Teilnehmer - **Angstabbauend** Ängste wie z.b. die des nicht Beantworten können soll abgebaut werden. - **Inhaltlich einführen** Die Frage soll in das Thema einführen und im Idealfall Interesse und Neugier wecken - **Keine Fragen zur Person oder zur Ihrem demographischen Eigenschaften**

Es kann Sinn machen eine "perfekte" Einstiegsfrage zu erstellen, die in der Auswertung der Ergebnisse nicht berücksichtigt wird. Sie dient lediglich die Anforderungen einzuhalten und en Teilnehmer einen positives Einstiegserlebnis zu vermitteln.

Die 1. Frage der Studie dieser Bachelorarbeit: Hatten Sie schon einmal das Gefühl, dass an einem Onlinewettbewerb gemogelt werden kann? 0 Ja 0 Nein

Funktion der fragebogen

Fragen sollen eine Funktion übernehmen. Dabei schlägt Kleber[8] folgende Klassifizierung vor: - Übergangs- und Vorbereitungsfragen für Themenwechsel, - Ablenkungs- und Pufferfragen zur Minderung von Ausstrahlungseffekten, - Filterfragen zum Übergehen von eventuell irrelevanten Fragen, - Rangier- und Konzentrationsfragen zum Auflockern langer Darstellungen, - Motivationsfragen zur Stärkung des Selbstvertrauens und Verminderung von Hemmungen, - Kontrollfragen als Wahrheitskontrolle der Antworten bzw. Sichtbarmachen von Widersprüchen.

Diese Klassifizierung soll helfen den Fragebogen zu gestalten.

Frageart

Bei der Stellung der Frage sollte festgestellt werden welche Art von Frage gestellt wird. Da sich dadurch die Antwort markantlich unterscheidet. Folgende 3 Hauptgruppen gibt es - **Einstellungsfragen** Dieser Fragestellung bezieht sich auf "Wunschbarkeit oder negativen bzw. Beurteilung , den Befragte mit bestimmten Statements verbinden. - **Verhaltensfragen** Dabei wird direkt auf das Verhalten des Befragten bezug genommen. Dabei muss beachtet werden, dass der Befragte sein Verhalten selbst beschreibt. Einerseits entspricht die Selbstwahrnehmung der Teilnehmer teilweise nicht der Realität anderseits kann die Antwort auch dem Wunschdenken des Befragten zugrunde liegen - **Eigenschftsfragen** Diese Fragestellung fragt nach den Eigenschaften von Personen. Vielfach sind es persönliche und demographische Daten.

[6](Dillman 1978)
[7](Pratzner 2001)
[8](Hippler 1992)

Fragetypen

Die Fragen können generell in zwei Typen unterteilt werden

Tabelle 6.1: Fragetypen

Form	Eigenschaften
Offene Frage	Der Aufwand bei der Auswertung ist sehr hoch. Ungeübte Teilnehmer können unverwertbare Antworten niederschreiben. Antworten sind schwer vergleichbar Dafür Teilnehmer kann sich so ausdrücken wie er möchte. Er wird nicht durch vorgegebene Antworten beeinflusst.
Geschlossene Frage	Leichte Auswertung. Gefahr besteht, dass der Teilnehmer ratet und durch die Antworten beeinflusst wird. Der Vorbereitungsaufwand für die Frage ist hoch. Auswahlmöglichkeiten für die Antwort könnten irelevant sein.

6.3.3 Abschluss

Der Abschluss des Fragebogens kann sehr kurz gehalten werden. Folgende Elemente sollten enthalten sein:

Dankensformel

Eine kurze Dankensformel gehört zum guten Ton und motiviert den Teilnehmer die Umfrage korrekt abzuschliessen.

Einladung zur Kommentierung

Durch Kommentare am Schluss können Befrate dem Untersucher Hinweise zukommenlassen die für die Auswertung und weitere Untersuchungen dienlich sind. Dieser Möglichkeit wird nach der Erfahrung von Reuband[9] gewürdigt.

6.4 Umsetzung Gesamtkonzept

Basierend auf der Erarbeitung der Theoretischen Umsetzung eines Gesamtkonzepts einer wissenschaftlichen Studie, gilt es nun dieses Umzusetzen.

[9](Reuband 2001)

7 ProofOfConcept

7.1 Techologien

Der Auftraggeber möchte dass die aktuell in seinem Betrieb eingesetzten Technologien für die Implementation der Arbeit verwendet werden. Die Technologien wurden abgesprochen und im folgenden Kapitel erklärt.

7.1.1 C-Sharp

Im Rahmen der Einführung von .net veröffentlichte Microsoft 2002 die Programmiersprache C-Sharp oder verkürzt C#. C# orientiert sich stark an Java, C++, Haskell und Delphi. Daher liegt es Nahe das C# eine objektorientierte Programmiersprache ist und der Wechsel von den zu vorgenannten Programmiersprachen auf C# einfach fällt.

Neben Grundprinzipen der objektorientierten Programmierung resultiert aus folgende innovativen Sprach-Konstrukte eine vereinfachte Programmierung:

- Gekapselte Methodensignaturen, Delegaten genannt, die typsichere Ereignisbenachrichtigungen ermöglichen
- Eigenschaften, die als Accessoren für private Membervariablen dienen
- Attribute, die zur Laufzeit deklarative Metadaten zu Typen bereitstellen
- Inline-XML-Dokumentationskommentare
- Sprachintegrierte Abfrage (Language-Integrated Query, LINQ), die integrierte Abfragefunktionen für eine Vielzahl von Datenquellen bereitstellt

Der C#-Erstellungsprozess ist im Vergleich zu C und C++ einfach und flexibler als in Java. Es gibt keine separaten Headerdateien und es ist nicht erforderlich, Methoden und Typen in einer bestimmten Reihenfolge zu deklarieren. Eine C#-Quelldatei kann eine beliebige Anzahl von Klassen, Strukturen, Schnittstellen und Ereignissen definieren.[1]

7.1.2 ASP.net Web API 2 / ASP.net MVC Framework

Microsoft entwickelte mit dem ASP.net MVC Framework ein schlankes und einfach zu testendes Präsentationsframework. Wie im Namen enthalten basiert das Framework auf dem MVC-Pattern. Die klare Trennung von Eingabelogik, Geschftslogik und Präsentationslogik wird durch die vom Framework bereitgestellten Komponenten unterstützt. Um RESTful-Webservices einfach entwickeln zu können stellt Microsoft mit ASP.net Web API 2 eine einfache zu verwendendes und starkes Software Paket zur Verfügung. ASP.net Web API 2 basiert auf dem ASP.net MVC Framework.[2]

[1] Quelle:(MSDN 2015a)
[2] Quelle:(MSDN 2015a)

7.1.3 Entity Framework

Entity Framework (EF) ist eine objektrelationale Zuordnung, die .NET-Entwicklern über domänenspezifische Objekte die Nutzung relationaler Daten ermöglicht. Ein Grossteil des Datenzugriffscodes, den Entwickler normalerweise programmieren, muss folglich nicht geschrieben werden. [^efbasic]

7.1.4 AngularJS

Mittels AngularJS wird die Client-Browser App entwickelt. AngularJS ist ein Javascript Framework, welches OpenSource von Google Inc. veröffentlicht wurde. AngularJS macht einen Grossteil des Codes, den man normalerweise schreibt, überflüssig. Die Reduktion des Codes begründet sich durch die Automatisierung von Standardaufgaben. Die manuelle DOM-Selektion, DOM-Manipulation und Event-Behandlung werden durch AngularJS überflüssig. Durch Einsatz von Direktiven und Modulen wird die Wiederverwendbarkeit von Code ermöglicht.

Die normalen Datentypen von JavaScript können verwendet werden. Dadurch ist es sehr einfach möglich, fremde Bibliotheken einzubinden, ohne eine weitere Zwischenschicht (Glue Code) zu implementieren. Die Methode, die AngularJS dazu verwendet nennt sich Dirty-Checking und wird im Vertiefungskapitel näher erklärt.[^angularjsbasic]

7.1.5 JSON

Zwischen der AngularJS WebApp und dem Webservice dient JSON(JavaScript Object Notation) als Datenübertragungsformat. JSON zeichnet sich durch seine schlanke Notation und der objektnahen Darstellung aus [^efbasic]: Quelle (MSDN 2015b) [^angularjsbasic]: Quelle (Sandeep 2014)

8 Fazit

A Glossar

2FA 2FA bedeutet Zwei-Faktor-Authentifizierung. Weitere Infos im Kapitel Authentifizierungs Komponenten

Github Github ist ein Cloud basierter SourceCode Verwaltungsdienst für Git. `https://github.com`

Non-Response Nichtbeantwortung einer oder mehrerer einzelner Fragen. Die Repräsentativität einer Befragung hängt stark ab von der Rücklaufquote, auch Response-Rate genannt.

ORM ORM steht für object-relational mapping und ist eine Technik mit der Objekte einer Anwendung in einem relationalen Datenbanksystem abgelegt werden kann.

REST / Restfull REST steht für Representational State Transfer. REST ist eine Software Architektur des Webs. System welche die REST Architektur einhalten nennt man RESTful. REST System kommunizieren allgemein über das HTTP-Protokoll und nutzen die gleichen HTTP verbs wie ein Browser der eine Webseite abfragt. Neben GET und POST werden die weniger bekannten Verben PUT und Delete verwendet. Die URI beschreibt die zu beziehende oder verändernde Webressource.

B Verzeichnisse

Neues Verzeichnisse

B.1 Abbildungsverzeichnis

B.2 Quellenverzeichnis

B.3 Tabellenverzeichnis

"10minutemail.com." 2016. http://www.10minutemail.com.

Burling, Stacey. 2012. "CAPTCHA: The Story Behind Those Squiggly Computer Letters." http://phys.org/news/2012-06-captcha-story-squiggly-letters.html.

"Datatrans ECom - Technical Implementation Guide." 2016. https://pilot.datatrans.biz/showcase/doc/Technical_Implementation_Guide.pdf.

Dillman, Don A. 1978. *Mail and Telephone Surveys.The Total Design Method*. New York: John Wiley & Sons Inc.

Duden. 2014. Vol. 26. Dudenredaktion.

Hanik, Filip. 2015. "Kiss." https://people.apache.org/~fhanik/kiss.html.

Hippler, Hans-Jürgen. 1988. *Methodische Aspekte Schriftlicher Befragungen: Probleme Und Forschungsperspektiven*.

———. 1992. *Diagnostik in Pädagogischen Handlungsfeldern*. Weinheim, München: Juventa Verlag.

Höpflinger, François. 2011. "Standardisierte Erhebungen - Methodische Hinweise Zu Umfragen." http://www.hoepflinger.com/fhtop/Umfragemethodik.pdf.

"Http://authentifizierung.org." 2015. http://authentifizierung.org/.

Interactive, Goldbach. 2015. "Nutzerzahlen Der Wichtigsten Plattformen." https://twitter.com/revogt/.

"Interview Mit Shaul Olmert." 2015. https://www.youtube.com/watch?v=X_fQ1uG9rFY.

Kriha, Walter, and Roland Schmitz. 2009. *Sichere Systeme*. Xpert.press. Berlin, Heidelberg: Springer Berlin Heidelberg.

Millischer, Sven. 2015. "Die Digitale Revolution." handelszeitung.ch/digitalisierung/hz-sonderausgabe-die-digitale-revolution-874557.

MSDN. 2015a. "Einführung in Die Programmiersprache C# Und in .NET Framework." https://msdn.microsoft.com/de-de/library/z1zx9t92.aspx.

———. 2015b. "Entity Framework." https://msdn.microsoft.com/de-ch/data/ef.

aspx.

"NET-Metrix-Audit." 2004. news.admin.ch/message/index.html?lang=de&msg-id=13600.

"NET-Metrix-Audit." 2015. http://netreport.net-metrix.ch/audit/.

"PlayBuzz." 2015. http://www.playbuzz.com.

Pratzner, Axel. 2001. *Wissenschaftlich Fundierter Aufbau von Fragebogen*. Institut für webbasierte Kommunikation und E-Learning.

"Projektmanagement: Definitionen, Einführungen Und Vorlagen." 2015. http://projektmanagement-definiti
de/glossar/meilenstein/.

"ReCAPTCHA Digitization Accuracy." 2014. http://www.google.com/recaptcha/digitizing.

Reuband, Prof. Dr. Karl-Heinz. 2001. "Möglichkeiten Und Probleme Des Einsatzes Postalischer Befragungen."

Rothman, Mike. 2015. "Default Deny." https://securosis.com/blog/network-security-fundamentals-de

Rouse, Margaret. 2015. "Authentifizierung - Definition." http://www.searchsecurity.de/definition/Authentifizierung.

Rupp, K. P. 2011. *Basiswissen Requirements Engineering*. dpunkt.verlag.

Sandeep, Panda. 2014. *AngularJS Novice to Ninja*. Sitepoint Pty. Ltd.

"SMI (SocialMedia Institute)." 2015. http://socialmedia-institute.com/.

"Statistik Plattform." 2015. http://de.statista.com/.

Stern, Olaf. 2012. *Reglement Bachelorarbeit*. Zürcher Hochschule für Angewandte Wissenschaften.

"Top 10 CMS November 2015." 2015. http://de.statista.com/statistik/daten/studie/320685/umfrage/nutzungsanteil-der-content-management-systeme-cms-weltweit/.

"Two-Factor Authentication: FAQ." 2016. http://www.cnet.com/news/two-factor-authentication-what-

"Usage of Content Management Systems for Websites." 2015. http://w3techs.com/technologies/overview/content_management/all.

"Webshop." 2016. https://www.datatrans.ch/de/e-payment/shop-schnittstellen.