

Bachelorarbeit (Informatik)

Individuell konfigurierbarer Authentifizierungsservice für Votings und Wettbewerbe

Autor	Christian Bachmann
Betreuung	Jaime Oberle
Auftraggeber	inaffect AG
Datum	09.05.2016

S

Inhaltsverzeichnis

1 Einführung	2
1.1 Motivation	2
1.2 Aufgabenstellung	3
1.3 Rahmenbedingungen der Bachelorarbeit	5
2 Projektmanagement	6
2.1 Projektplan	6
2.2 Soll - Ist Analyse/Vergleich	7
2.3 Meilensteine	7
2.4 Termine	8
2.5 Infrastruktur	9
3 Recherche	11
3.1 Fachbegriffe	11
3.2 Erläuterung der Grundlagen	11
3.3 Sicherheitsprinzipien	12
3.4 Marktanalyse	14
3.5 Findings	18
3.6 Authentifizierungs-Komponenten	19
4 Anforderungen	31
4.1 Akteure	31
4.2 Use-Cases	32
4.3 Anforderungen	37
4.4 Funktionale Anforderungen	38
4.5 Nicht Funktionale Anforderungen	41
4.6 Risiken	44
5 Konzept	48
5.1 Systemarchitektur	48
5.2 Architekturübersicht	49
5.3 Genereller Ablauf der Authentifizierung	50
5.4 differenziertes Domänenmodell	51
5.5 Datenbankdesign	52
5.6 Integration der Schnittstelle	53
5.7 Sicherheitsstufen integrieren	60
5.8 Modularität und Erweiterbarkeit	63
5.9 Mockup	67
5.10 "Du" oder "Sie" – Ansprache	71
5.11 Wahl des Applikation Hosters	73
5.12 Validierung von Benutzereingaben	73
5.13 Testing	74

6 Proof of Concept	75
6.1 Technologien	75
6.2 Umsetzung Sicherheitsstufe	78
6.3 Finale Screens	81
6.4 Implementation Authentifizierung	88
6.5 Testing	91
7 Studie	92
7.1 Definition der Begriffe aus der Aufgabenstellung	92
7.2 Ziel der Studie	92
7.3 Art der Studie	92
7.4 Aufbau Gesamtkonzept	94
7.5 Hauptteil/Fragen	96
7.6 Erste Frage	96
7.7 Theorie Fragen	97
7.8 Fragen über Akzeptanz	98
7.9 Frage Anstrengung	99
7.10 "Bonus Frage"	99
7.11 Weitere Fragen	99
7.12 Abschluss	100
7.13 Verständlichkeit	100
7.14 Auswertung	100
7.15 Anstrengung	102
7.16 Akzeptanz	103
8 Fazit	104
8.1 Ausblick	104
8.2 Offene Fragen	104
8.3 Limitationen	104
8.4 Validation	105
8.5 Schlusswort	107
A Anhang	108
A.1 Glossar	108
A.2 Verzeichnisse	110
A.3 Arbeitsergebnisse	113
A.4 Danksagung	113
A.5 Bestätigung	114
A.6 Umfrage	115

1 Einführung

1.1 Motivation

Die Digitalisierung fordert die Schweizer Wirtschaft heraus. Ob Banken, Pharmaindustrie, Detailhandel oder Medienhäuser – es gibt keine Branche, die nicht vor fundamentalen Veränderungen steht.¹ Da verwundert es nicht, dass Wettbewerbe oder Kreuzwörter nicht nur auf den letzten Seiten der Magazinen oder Zeitungen abgedruckt werden, sondern vermehrt online publiziert und durchgeführt werden und dass bei meinungsbildenden Umfragen oder Abstimmungen weniger auf Telefonumfragen zurückgegriffen wird, sondern immer mehr Umfragen 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 ihre Resonanz zu bewahren oder sogar auszubauen, sind Medien darauf angewiesen, dass ihre Stories bzw. Inhalte auf den Social Media Kanälen verlinkt und so viral verbreitet werden. Neben altbekannten plakativen Titeln und interessanten Bildern beleben die Medienhäuser immer mehr ihren Inhalt mit so genannten “Playful Content” oder auf Deutsch: Mit Interaktivitäten. Dabei handelt es sich um Abstimmungen, Wettbewerbe und Umfragen oder andere 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 Wettbewerben ist es mit geringem technischen Verständnis möglich mehrfach teilzunehmen oder gefälschte Daten zu übermitteln. Dies ist auf zu einfach realisierte Programmierungen zurückzuführen, was der Glaubwürdigkeit solcher Angebote schadet. Interaktivitäten bedürfen somit einer Authentifizierung, um Betrug oder falschen Stimmabgaben vorzubeugen. Die Eigenentwicklung einer angemessenen Authentifizierung für eine Interaktivität übersteigt meist die kleinen Budgets für diese Angebote.

Die Glaubwürdigkeit der Umfragen, Abstimmungen und Wettbewerbe ist durch die aktuelle Situation gefährdet und soll wiederhergestellt werden. Deshalb soll diese Bachelorarbeit die Möglichkeiten eines Authentifizierungsservices erörtern. Mit dieser sollen Programmierer über eine visuelle Oberfläche die Bedürfnisse eines Angebots konfigurieren und in ihren jeweiligen 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 Authentifizierungsschnittstelle 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 der Bachelorarbeit

Die vorliegende Bachelorarbeit umfasst gemäss Regelment unter anderem folgende Punkte:

- Der offizielle Projektstart ist der 18. November 2015. Das Projekt muss bis spätestens 18.05.2016 abgegeben werden.
- Die Bachelorarbeit muss zwei Wochen vor der Präsentation abgegeben werden
- 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 durchgeführt. Weiter wird die verwendete Infrastruktur erläutert.

2.1 Projektplan

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 Milestones fest. Als Soll-Aufwand der Bachelorarbeit wurden 374 Stunden veranschlagt. Der effektive Aufwand betrug 412 Stunden.

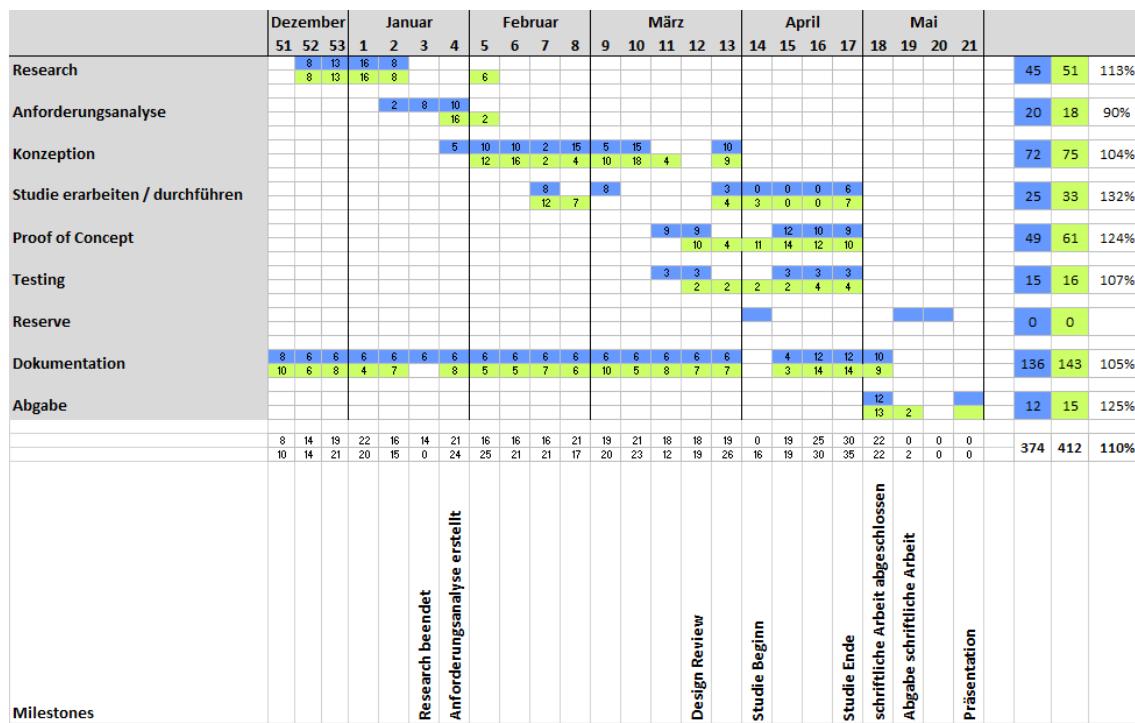


Abbildung 2.1: Projektplan der Bachelorarbeit

2.2 Soll - Ist Analyse/Vergleich

Im Unterkapitel [Rahmenbedingungen der Bachelorarbeit](#) wurde bereits aufgeführt, dass eine Bachelorarbeit laut Regelement mindestens 360 Stunden betragen soll. Diese Rahmenbedingung wurde bei der Aufgabenstellung und Aufwandschätzung der Bachelorarbeit berücksichtigt.

Tabelle 2.1: Soll - Ist Analyse/Vergleich

Arbeitsschritt	Soll	Ist
Recherche	45	51
Anforderungsanalyse	20	18
Konzeption	72	75
Studie erarbeiten / durchführen	25	33
Proof of Concept	49	61
Testing	15	16
Dokumentation	136	143
Abgabe	12	15
Total	376	412

2.3 Meilensteine

Meilensteine sind 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 zur erfolgreichen Umsetzung der Bachelorarbeit immer wieder innegehalten und kontrolliert werden, wie der Stand der Dinge ist und ob die Richtung geändert werden muss. So bleibt stets der Überblick gewahrt und das Projekt "Bachelorarbeit" gerät nicht ausser Kontrolle.⁴

Tabelle 2.2: Meilensteine

Datum	Meilenstein
24. Januar 2016	Recherche beendet
31. Januar 2016	Anforderungsanalyse erstellt
30. März 2016	Design Review
10. April 2016	Studie Beginn
24. April 2016	Studie Ende
8. Mai 2016	schriftliche Arbeit abgeschlossen
11. Mai 2016	Abgabe schriftliche Arbeit
25. Mai 2016	Präsentation

⁴(*Projektmanagement: Definitionen, Einführungen und Vorlagen* 2015)

2.4 Termine

Folgend sind die wichtigsten Termine dieser Bachelorarbeit aufgelistet.

Tabelle 2.3: Termine der Bachelorarbeit

Datum	Termin
28.10.2015	Besprechung Aufgabenstellung mit Betreuer
18.11.2015	Freigabe der Aufgabenstellung
9.12.2015	Kick Off
11.05.2016	Abgabe schriftliche Arbeit
25.05.2016	Präsentation

2.5 Infrastruktur

Im Unterkapitel Infrastruktur sollen die verwendeten Werkzeuge erläutert werden.

2.5.1 Quellcode-Verwaltung mit GitHub

Um einerseits eine Datensicherung zu gewährleisten und anderseits die Änderungen nachvollziehbar abzulegen, wird die Bachelorarbeit mittels Git versioniert. Der Quellcode wird auf github.com verwaltet. Das Repository⁵ ist öffentlich jederzeit einsehbar.

2.5.2 Zeiterfassung mit toggl

Das Zeitmanagement-Tool toggl⁶ gibt schnell ein Feedback zur aktuell gebrauchten Zeit und einen Überblick, um die geplante mit der real verwendeten 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.

2.5.3 Dokumentieren mit Pandoc und LaTex

Die Thesis dieser Bachelorarbeit soll basierend auf anerkannten, wissenschaftlichen Formaten erzeugt werden. Im Intranet der ZHAW wird die Erstellung von wissenschaftlichen Arbeiten mit LaTex empfohlen. LaTex Templates der einzelnen Abteilungen können erworben werden. Die Effizienz bei der Erstellung von LaTex Arbeiten ist umstritten. Diese Arbeit wurde zuerst im Markdown Syntax geschrieben und mittels Pandoc in LaTex umgewandelt. Basierend auf den Templates und Einstellungen in reinem LaTex wurde dann das endgültige PDF-Dokument generiert.

2.5.4 Tools für Grafik

Design Mockup Balsamiq

Der Auftraggeber wünscht, dass eine strukturelle Vorlage des Designs vor der Umsetzung illustriert wird. Dafür stellt der Auftraggeber eine Lizenz des Tools Balsamiq zur Verfügung. Mit dem Wireframing-Tool Balsamiq kann, dank den vielen konfigurierbaren Elementen, rasch ein Design-Mockup von Webseiten oder Applikationen erstellt werden.

⁵<https://github.com/coffefan/bachelorarbeit>

⁶<https://toggl.com>

yUML

Um Ablaufe-Diagramm, Use Case-Diagramme und andere UML-Diagramme zu visualisieren, bedarf es eines Tools, dass die Diagramme sowohl optisch ansprechend, wie aber auch einfach und schnell anpassbar umsetzt. yUML ist ein gratis Online-Service, über welchen mittels Code ein UML-Diagramm kreiert werden kann. Diese Art von UML-Gestaltung ist daher sehr strukturiert und nachvollziehbar. Der Code, welcher zum Diagramm führt, kann so einfach als Textdatei abgespeichert werden und wird in dieser Bachelorarbeit im Github-Repository hinterlegt.

Draw.io

Alle Diagramme, welche nicht via [yUML](#) designed werden können, werden mit dem Online Tool Draw.io erstellt. Draw.io wird in Entwicklerkreisen als webbasiertes Visio gehandelt. Seit dem letzten Release ist Draw.io ohne Einschränkung gratis verwendbar. Die gezeichneten Diagramme können direkt im Daten-Cloud Dienst Google Drive gespeichert werden.

2.5.5 Infrastruktur Entwicklung

Die Infrastruktur, welche zur Entwicklung verwendet wird, kann je nach Anforderung und Konzeption variieren. Die verwendete Infrastruktur wird deshalb nach der Definition und Konzeption im Kapitel [Entwicklungswerkzeuge](#) aufgelistet.

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 Grundlagen ausgeführt, welche für die Bearbeitung dieser Bachelorthesis herangezogen wurden.

3.2.1 Authentifizierung

Authentifizieren - beglaubigen, die Echtheit von etwas bezeugen ⁷

Eine Person oder ein Objekt eindeutig zu **authentifizieren** bedeutet zu ermitteln, ob die- oder derjenige auch die Person ist, als welche sie oder er sich ausgibt.⁸ Dies unterstreicht auch die Ableitung des Wortes vom Englischen Verb *authenticate*, was auf Deutsch "sich als *echt erweisen, sich verbürgen, glaubwürdig sein*" bedeutet. Das bekannteste Verfahren der Authentifizierung ist die Eingabe von Benutzernamen und Passwort. Weiter ist die PIN-Eingabe bei Bankautomaten oder Mobiltelefonen häufig verbreitet. Die Möglichkeiten von verschiedenen Authentifizierungen ist nahezu grenzenlos.⁹

3.2.2 Autorisierung

Autorisierung - Befugnis, Berechtigung, Erlaubnis, Genehmigung ¹⁰

Wenn die **Authentifizierung** erfolgreich war, erteilt ein System die Autorisierung. Dabei wird der Person oder dem Objekt erlaubt, bestimmte Aktionen oder 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)

⁷(Duden 2014)

⁸(Rouse 2015)

⁹(<http://authentifizierung.org> 2015)

¹⁰(Duden 2014)

3.3 Sicherheitsprinzipien

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

3.3.1 KISS

KISS steht für **K**eep **I**t **S**tupid *and* **S**imple

Ein verbreitetes Problem unter Softwareentwicklern und Programmieren heute ist, dass dazu tendiert wird, Probleme zu kompliziert und verschachtelt zu lösen. Acht bis neun von zehn Entwickeln machen den Fehler, Probleme zu wenig auseinanderzubrechen und alles in einem grossen Programm zu lösen, anstatt es in kleinen Paketen verständlich zu programmieren.¹¹

Die folgenden Punkte listet die Vorteile für Softwareentwickler beim Verwenden von Kiss auf:

- Mehr Probleme sollen schneller gelöst werden
- Der Entwickler kann komplexe Probleme mit wenigen Zeilencodes lösen
- Die Codequalität steigt
- Der Entwickler kann grössere Systeme 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 and simple" ist

Die Begründung, warum KISS die Sicherheit fördert, liefert Saltzer und Schroeder: "*Unge-wollte Zugriffspfade können nur durch zeilenweise Codeinspektion entdeckt werden und dies wiederum setzt voraus, dass Designs einfach und klein sind. Designs müssen so beschaffen sein, dass sie abgeschlossene Bereiche enthalten, über die konkrete und sichere Aussagen über Zugriffsmöglichkeiten und Effekte getroffen werden können.*"¹²

3.3.2 Default-is-deny

Ob eine Person oder ein Programm Zugriff auf Daten und Funktionen hat, sollte nicht durch Verbote, sondern durch eine explizite Erlaubnis geregelt werden. Dies bedeutet, dass 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 verwunderlicher ist es, dass viele Organisationen und Entwickler dieses Vorgehen nicht anwenden. Zum Beispiel Filesysteme setzen auf Verbote anstatt auf explizite Erlaubnisse.^{13 14}

¹¹(Hanik 2015)

¹²(Kriha and Schmitz 2009, pp.93)

¹³(Kriha and Schmitz 2009, pp.94)

¹⁴(Rothman 2015)

3.3.3 Open Design

Abgeleitet von der Theorie der Kryptografie gilt Folgendes: 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 eher nach dem Ansatz entworfen werden: Mindestens intern soll das Software-Design durch einen Design-Review Prozess analysiert werden. In manchen Fällen macht es jedoch Sinn, das Softwaredesign geheimzuhalten, um einem Angreifer nicht zu viele Informationen zur Verfügung zu stellen.¹⁵

3.3.4 Zusammenfassung der Sicherheitsprinzipien

Die Sicherheitsprinzipien sind folgend gekürzt zusammen gefasst:

- Die Software muss aus kleinen, isolierten Einheiten aufgebaut werden, deren externe Beziehungen am Interface deutlich werden. Damit werden 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.

¹⁵(Kriha and Schmitz 2009, pp.95)

3.4 Marktanalyse

Dieses Unterkapitel erläutert existierenden Produkte auf dem Markt.

3.4.1 OAuth-Provider

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

Das Bedürfnis nach OAuth

2006 implementierte Blaine Cook OpenID für Twitter. Ma.gnolia¹⁶ erhielt dabei ein Dashboard, welches sich durch OpenID autorisieren ließ. Deshalb suchten die Entwickler von Ma.gnolia und Blaine Cook eine Möglichkeit, OpenID auch für die Verwendung von APIs zu gebrauchen. Sie diskutierten verschiedene Implementierungen und stellten fest, dass es keinen offenen Standard für API-Access Delegation gab. So fingen sie an, einen Standard zu entwickeln. 2007 entstand daraus eine Google Group. Am 3. October 2007 war dann der OAuth Core 1.0 bereits veröffentlicht 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 standardisierte und kombinierte die existierenden industriellen Protokolle. Der wichtigste Unterschied zu den existierenden Protokollen ist, dass OAuth sowohl offen ist als es auch geschafft hat, genügend Einsatzgebiete zu finden, um als Standard zu gelten. Jeden Tag entstehen neue Webseiten, welche neue Funktionalitäten und Services offerieren und dabei Funktionalitäten von anderen Webseiten brauchen. OAuth stellt dem Programmierer einerseits eine standardisierte Implementierung zur Verfügung. Andererseits erhält der Endbenutzer dank dieses Protokolls die Möglichkeit, Teile seiner Funktionalität oder Daten bei einem anderen Anbieter zur Verfügung zu stellen. Bei Facebook OAuth kann der Endbenutzer zum Beispiel 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

¹⁶Ma.gnolia ist eine Lesezeichen-Webseite auf der User Lesezeichen bis 2009 bewerten und auch privat verwalten konnten.

Die grössten OAuth-Provider wie Google, Facebook und Twitter erziehlen eine weite Verbreitung weltweit. Ganze 78% (Interactive 2015) der Schweizer Bevölkerung nutzten SocialMedia und besitzen dadurch einen OAuth-Account.

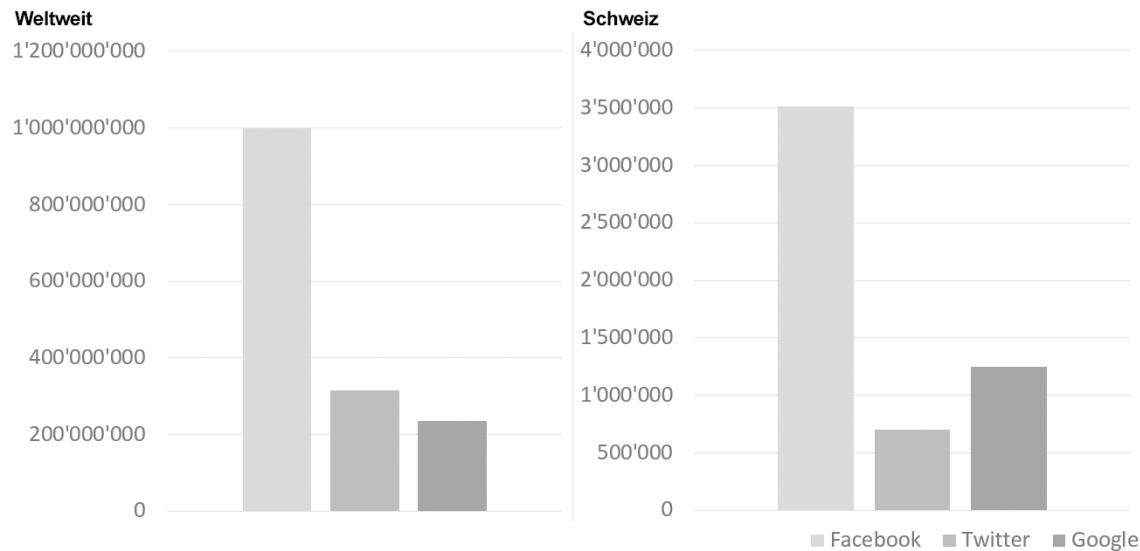


Abbildung 3.1: Aktive Nutzer weltweit und in der Schweiz ¹⁷

Vorteil

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

Nachteil

Mehrfachregistrierungen sind möglich. Jenach OAuth-Provider werden verschiedene Daten zur Verfügung gestellt. Pro OAuth Provider kann man sich registrieren. Ein 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 Libraries nicht ohne höhere Programmierkenntnisse möglich.

¹⁷ Die Statistik der aktiven Nutzer weltweit 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 im 2014 erhoben worden. Die Statistik der aktiven Nutzer in der Schweiz wurde basierend auf den Daten von Goldbach Interactive (*Interactive 2015*) generiert. Die Daten sind im März 2015 erhoben worden.

3.4.2 playbuzz.com

Youtube von Google ist im Jahr 2015 mit Abstand die meist verbreitete Videopublishing-Plattform¹⁸. Medienhäuser nutzen Youtube, um ihren Artikel einfach 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 Embedded Content werden. Neben MTV, Focus, Time oder Bild verwendet seit Herbst 2015 auch ein grosses Medienhaus der Schweiz die Plattform. Tamedia erfasst neuerdings immer wieder auf 20minuten Votings und Umfragen mit PlayBuzz.

2012 wurde Playbuzz von Shaul Olmert (Sohn des Premier Ministers von Israel *Ehud 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 sieben von den zehn Top Shares auf Facebook laut forbes.com von Playbuzz. Playbuzz setzt nach eigenen Angaben auf Content wie Votes und Quizes, welche gerne viral geteilt werden, und ermöglicht Endnutzern und Redakteuren eine einfache Verwendung. ¹⁹ ²⁰

Vorteile

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

Nachteile

Der Verweis auf Playbuzz ist immer klar ersichtlich. Auch beim Veröffentlichen auf den SocialMedia-Kanälen ist die Herkunft von Playbuzz offensichtlich. Die Möglichkeiten in Funktionalität und Design sind eher begrenzt. Individuelle Erweiterungen sind nicht einfach möglich. Bestehende Interaktivitäten, solche die nicht von PlayBuzz erstellt werden, können nicht verwendet werden. Mehrfachteilnahmen waren ebenfalls möglich.

¹⁸(Statistik Plattform 2015)

¹⁹(Interview mit Shaul Olmert 2015)

²⁰(PlayBuzz 2015)

3.4.3 WebsMS.com Zwei-Faktor-Authentifizierung

WebsMS.com bietet 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.²¹

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

Seit 1. Juli 2004 müssen auch bei Prepaid-Karten in der Schweiz Personalien hinterlegt werden.²² Dadurch ist eine eindeutige Authentifizierung über Mobilnummern gewährleistet. Die Mobilfunkanbieter schränken die Anzahl SIM-Karten auf maximal fünf 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 zugängliches Dokument, welches die maximale Anzahl SIM-Karten pro Person beschreibt. Mündlich durch das Verkaufspersonal des Swisscom-Shops Zürich HB im Dezember 2015 und im Chatprotokoll²³ wurde der Wert bestätigt. Es wurde darauf hingewiesen, dass kein Dokument mit dieser Zahl vorhanden ist.

Selbstversuch

Es wurde versucht, bei zwei unabhängigen Handyanbietern mehr als fünf Swisscom-Prepaid-Abos abzuschliessen. Dabei wurde von Thomas Bachmann über vier Wochen verteilt bei dem Anbieter Interdiscount im Manor Winterthur bei unterschiedlichen Verkäufern ein Prepaidhandy gekauft. Beim Einkauf des sechsten Handys wurde der Verkauf durch die Kasse abgelehnt. Die Fehlermeldung der Kasse beinhaltete den Hinweis, dass die Nummer nicht erneut auf den Kunden registriert werden könne, da er schon fünf SIM Karten bei der Swisscom besitze. Christian Bachmann kaufte über zwei Wochen verteilt bei dem Anbieter Migros Electronics in der Migros Limmat, Interdiscount im Manor Winterthur, Interdiscount im Zürich HB bei unterschiedlichen Verkäufer ein Swisscom Prepaidhandy. Der Einkauf des sechsten Handys wurde ebenfalls durch die Kasse abgelehnt. Die Nummer liess sich nicht erneut auf den Kunden registrieren, da er schon fünf SIM Karten bei der Swisscom besass.

Sunrise

Die Sunrise hat nach Rücksprache ein PDF mit ihren Bestell- und Lieferbedingungen zugesendet.²⁴ Die maximale Anzahl SIM-Karten ist in diesen Bestell- und Lieferbedingungen festgelegt. Auch die Sunrise hat das Maximum auf fünf SIM-Karten pro Person festgelegt.

²¹ Die Kosten sind am 28. Dezember 2015 unter folgendem Link abgerufen worden:
<https://websms.ch/preise#at-preisuebersicht>

²² Meldung des UVEKS über Gesetzesänderung: (*NET-Metrix-Audit 2004*)

²³ Chat-Protokoll Swisscom 12.Februar 2016 <http://bit.ly/swisscom-chat>

²⁴ Kopie Bestell- und Lieferbedingungen <http://bit.ly/sunrise-bedienungen>

SALT

Bei der Firma SALT konnte mir ebenfalls kein Dokument mit einer Kennzahl gegeben werden. SALT vergibt gemäss ihrer schriftlichen Auskunft ²⁵ pro Person maxmal drei SIM Karten.

Vorteile

Die mehrfache Registrierung ist auf maximal fünf SIM-Karten/Rufnummern beschränkt. Durch die Kosten für eine SIM-Karte/Mobilenummer wird der Wert zusätzlich gemindert. Bei Missbrauch kann der User eindeutig identifiziert werden und eine Automatisierung ist nahezu unmöglich.

Nachteile

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

3.4.4 SuisseID

Die SuisseID schafft die rechtlichen und technischen Voraussetzungen für den elektronischen Geschäftsverkehr. Als digitaler Identitätsausweis im Internet bietet sie ihren Anwenderinnen und Anwendern eine sichere Authentifikation zu Web-Applikationen, eindeutige Identifikation für Internet-Dienste und digitales, rechtsgültiges Signieren von Dokumenten. Der Erwerb einer solchen SuisseID kostet den Endkunden eine beträchtliche Summe Geld. Den Anbieter der Authentifizierung erwarten keine grossen Kosten. Dadurch ist eine kleine Verbreitung für den privaten Nutzen offensichtlich. Entwickler von Integrationen erhalten eine umfangreiches SDK und Kontaktmöglichkeiten.

Vorteile

Hohe Sicherheit durch sichere und eindeutige Authentifikation ist gewährleistet. Rechtliche Voraussetzungen sind gegeben. Entwickler von Integrationen werden unterstützt.

Nachteile

Kleine Verbreitung und hohe Kosten für den Endnutzer sind die Nachteile von SuisseID.

3.5 Findings

Auf dem Markt sind verschiedene Anbieter, welche Interaktivitäten schützen können oder ganze Packages anbieten. Ein Service, welcher es erlaubt individuell konfigurierbare Sicherheitsstufen festzulegen und diese in eine bestehende Interaktivität einzubauen, wurde nicht gefunden. Einige Anbieter könnten als einzelne Sicherheitsstufe in der Umsetzung berücksichtigt werden. ²⁶

²⁵ E-Mail von Salt 13.Februar 2016 <http://bit.ly/salt-email>

²⁶ Stand 4. Januar 2016

3.6 Authentifizierungs-Komponenten

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

3.6.1 Cookie

Ein Cookie ist ein kurzes Text-Snippet, welches beim Besuch einer Webseite an den Browser gesendet wird. Dabei kann das Cookie serverseitig vom Webserver an den Browser gesendet werden oder in einem Skript wie Javascript erstellt werden. Der Browser sendet das Cookie bei jeder Aufforderung wieder der Webseite zu. Der Erfinder der Cookie-Technologie ist Vita Lou Montulli, der 1994 nach seinem Studienabbruch bei Netscape einstieg und zudem den Navigator mitentwickelte. Der Betreiber der Interaktivität speichert also im Cookie die Teilnahme. Beim erneuten Aufruf erhält er das Cookie und weiß so, dass der Teilnehmer schon einmal teilgenommen hat oder nicht. Das Absichern von Interaktivitäten durch Cookies ist weit verbreitet. Durch die browserseitige/clientseitige Speicherung kann diese Speicherung auch clientseitig relativ einfach manipuliert werden.²⁷

Automatisierungsmöglichkeit und Mehrfachteilnahme

Die Automatisierung ist ohne IT-Know-How möglich. Es stehen einige Browser Plugins zur Verfügung, welche es ermöglichen, sein Surfverhalten über einfache Record-Funktionen aufzunehmen und danach Cookies zu löschen. So kann mehrfach an einer Interaktivität wie z.B. Umfragen teilgenommen werden.

Kosten

Cookies verursachen keine direkten Kosten.

3.6.2 Flash-Cookies

Ein Flash-Cookie ist, wie es der Name bereits vermuten lässt, ein Cookie, das an den Adobe-Flash Player gebunden ist. Da der Flash-Player im Betriebssystem installiert wird, funktionieren die Flash-Cookies browserunabhängig. Die Bedienungen dieser Flash-Cookies werden von Adobe festgelegt und der Browser kann nicht direkt in das Handling eingreifen. Auch hier wird die Speicherung clientseitig durchgeführt und es kann auch diese Speicherung clientseitig manipuliert werden. Seit Steve Jobs mit Apple keinen Support für die mobilen Geräte in Aussicht stellte und auf die Probleme und Risiken hinwies, verlor die Plattform durch immer wieder auftretende Sicherheitsprobleme User. So haben am 1. Januar 2016 noch knapp 10%²⁸ aller Webseitenbesucher den Flash-Player installiert.

Mehrfachteilnahme

Flash-Cookies können je nach Betriebssystem mit verschiedenem Aufwand gelöscht werden und dadurch ist eine Mehrfach-Teilnahme möglich.

²⁷(So verwendet Google Cookies 2016)

²⁸(w3techs 2016)

Automatisierungsmöglichkeit

Die automatisierte Teilnahme und Löschung ist im Gegensatz zu klassischen Cookies aufwendiger, aber durchaus machbar.

Kosten

Flash-Cookies verursachen keine direkten Kosten.

3.6.3 IP-Adresse

Bei der Nutzung einer Interaktivität wird die IP-Adresse des Teilnehmers gespeichert. So kann bei erneutem Teilnehmen die Teilnahme verweigert werden. Das Internetprotokoll, kurz "IP", sieht für jedes Gerät, welches an einem IP-Netzwerk angeschlossen ist, eine eindeutige Adresse vor. Generell wird im Internet über den "IP Version 4 Standart" kommuniziert. Damit lassen sich aber nur 4,22 Milliarden eindeutige Adressen im World Wide Web vergeben. Deshalb mussten einige Methoden entwickelt werden um vorerst das Problem umgehen zu können. Unter anderem identifiziert sich ein Router wie ein Rechner, und nutzt intern mittels subnetting andere IP-Adressen. Gegen aussen haben also alle Nutzer des Netzwerks die selbe IP-Adresse. Dadurch entsteht die Problematik an dieser Methode, dass in einem Grossraumbüro mit einem Internetanschluss auch nur eine Person an einem Wettbewerb teilnehmen kann.²⁹

Mehrfachteilnahme

Es gibt verschiedene Möglichkeiten, die IP-Adresse zu wechseln. Eine einfache Möglichkeit ist durch Verwenden von Proxy-Servern eine andere IP-Adresse zu benutzen. Die Mehrfachteilnahme ist also einfach möglich.

Automatisierungsmöglichkeit

Das automatisierte Wechseln eines Proxys ist etwas aufwendiger und braucht technisches Know-How aber durchaus möglich.

Kosten

Das Authentifizieren via IP-Adresse verursacht keine direkten Kosten.

²⁹(Kirk 2005)]

3.6.4 Ausweisnummer: Schweizer Pass oder Identitätskarte

Die Schweiz führt für ihre Bürger zwei Ausweisarten: Den Schweizer Pass und die Identitätskarte. Diese dienen zum Nachweis der Schweizer Staatsangehörigkeit und der Identität. In der Schweiz besteht weder eine Ausweispflicht noch eine Mitführpflicht, niemand muss eine Identitätskarte oder einen Pass besitzen oder gar bei sich tragen. Auf der Rückseite der Identitätskarte oder auf der ersten Innenseite des Passes befindet sich im unteren Bereich eine maschinenlesbare Zone, welche auch von Menschen gelesen werden kann. Die verschiedenen Bereiche werden in der folgenden Abbildung beschrieben. Die orange umrandeten Zahlen sind jeweils Checksummen. Der orangefarbene Bereich ist die Gesamtchecksumme.

Identitätskarte:	ID CHE C1234567<0<<<<<<<<<	ID-/Passnummer	C1234567
	6012317M0109110CHE<<<<<<<6	Geburtsdatum	31.12.1950
	MUSTER<<WALTER<HANS<<<<<<	Ablaufdatum	11.09.2001
Pass:	PACHEMUSTER<<WALTER<HANS<<<<<<<<	Geschlecht	Männlich
	C1234567<0CHE6012317M0109110CHE<<<<<<6	Nachname	Muster
		Vorname(n)	Walter Hans

Abbildung 3.2: Beispiel der maschinenlesbaren Zone einer Identitätskarte und eines Passes

Checksummenberechnung

Die Checksummenberechnung funktioniert wie folgt:

1. Stelle wird mit 7 multipliziert,
2. Stelle wird mit 3 multipliziert,
3. Stelle wird mit 1 multipliziert,
4. Stelle wird wieder mit 7 multipliziert, usw.

Alle diese Produkte werden dann summiert und daraus Modulo 10 berechnet.

Bemerkung: Buchstaben werden in Zahlen umgewandelt. Dabei wird die Position des Alphabets beginnend ab 0 gezählt. Also A=0, B=1, C=2 und so weiter. Das Zeichen "<" wird in eine 0 umgewandelt.

Beispiel: „C1234567<“ => „212345670“

$$2 \times 7 = 14$$

$$1 \times 3 = 3$$

$$2 \times 1 = 2$$

$$3 \times 7 = 21$$

$$4 \times 3 = 12$$

$$5 \times 1 = 5$$

$$6 \times 7 = 42$$

$$7 \times 3 = 21$$

$$0 \times 1 = 0$$

$$\text{Summe} = 120$$

$$120 \bmod 10 = 0$$

Es gibt aus Datenschutzgründen keinen öffentlichen Service, über welchen man die Identität anhand der Passangaben überprüfen könnte. So besteht nur die Möglichkeit zu überprüfen, ob das eingegebene Muster anhand der Checksummen stimmt und ob bereits dieselben Informationen vorhanden sind.

Mehrfachteilnahme und Automatisierungsmöglichkeit

Der Algorithmus der Checksummen kann nachgebaut werden und so können automatisiert Identitätskarten generiert werden. Dadurch kann mehrfach und automatisiert an der Aktivität teilgenommen werden werden.

Kosten

Die Überprüfung verursacht keine direkten Kosten.³⁰ ³¹

³⁰(*Pass und Identitätskarte 2016a*)

³¹(*Pass und Identitätskarte 2016b*)

3.6.5 Captcha

Captcha ist ein Test, mit dem festgestellt werden kann, ob sich ein Mensch oder ein Computer eines Programms bedient.³²

Im Jahr 2000 wurde das Captcha an der Carnegie Mellon University erfunden. Captcha steht für Completely Automated Public Turing test to tell Computers and Humans Apart. 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".³³

Captcha Zahlen

In 2014 wurden 200 Millionen Captchas pro Tag eingegeben. Dabei braucht ein User durchschnittlich 10 Sekunden. Das entspricht 500'000 Stunden.³⁴

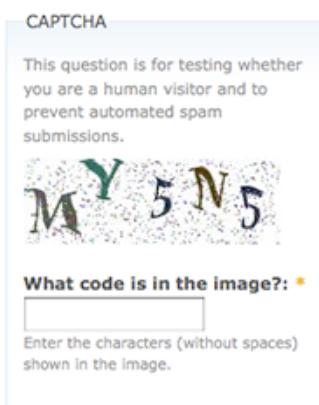


Abbildung 3.3: Beispiele von Captchas Quelle:drupal.org

Automatisierungsmöglichkeit

Die Automatisierung wird unterbunden.

Mehrfachteilnahme

Eine manuelle Mehrfachteilnahme ist möglich.

Kosten

Es entstehen keine direkten Kosten.

³²(Duden 2014)

³³(Burling 2012)

³⁴Die statistischen Daten wurden von Google 2014 in ihrem Blog publiziert (*reCAPTCHA Digitization Accuracy 2014*)

3.6.6 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung wird häufig 2FA genannt. Der User wird mittels zweier unabhängiger Faktoren identifiziert. Der Begriff "Faktor" umschreibt dabei eine Komponente oder Authentifizierungsmethode.³⁵

Die Zwei-Faktor-Authentifizierung ist in der Schweiz durch das E-Banking bekannt geworden. Der User gibt als ersten Faktor Username/Vertragsnummer und Passwort ein. In einem zweiten Schritt gibt er vom System gewünschten Code aus der Codekarte oder des elektrischen Rechners als zweiten Faktor ein. Im Alltag bei einem Einkauf im Detailhandel authentifiziert sich der EC-Kartenchip als erster Faktor. Als zweiter Faktor hat sich der Kunde einen PIN-Code auswendig gemerkt, welchen er eingibt.

Die folgenden Authentifizierungen basieren auf den Prinzip der Zwei-Faktor-Authentifizierung.

3.6.7 E-Mail-Bestätigungscode

Im Registrationsprozess ist das Erhalten eines E-Mails mit Bestätigungscode quasi zum Standard 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 Adresse eintragen und erhält dann umgehend den Bestätigungslink an diese zugesandt.

Automatisierungsmöglichkeit

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

Mehrfachteilnahme

Ein User kann verschiedene E-Mail Adressen besitzen. Das Erstellen von neuen E-Mail Adressen ist mit Aufwand verbunden, aber einfach möglich.

Anbieter wie 10-Minutes Mail³⁶ 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 ein zeitversetztes Bestätigungsmaill ausgehebelt werden.

Kosten

Bei der Annahme, dass jedes Unternehmen bereits ein E-Mail Server oder ein E-Mail Konto bei einem kostenlosen Anbieter besitzt, verursacht das Versenden von E-Mails über einen SMTP-Server ist generell keine zusätzlichen Kosten. Bei hohem Gebrauch dieser Komponente lohnt es sich, die E-Mails über eine professionelle Infrastruktur für Massenversendungen zu versenden und zu analysieren. Dadurch können weitere Kosten entstehen. Beispiele dafür sind Mailchimp³⁷ oder Sendgrid.³⁸

³⁵([Two-factor authentication: FAQ 2016](#))

³⁶10-Minute Mail (10minutemail.com 2016)

³⁷www.mailchimp.com

³⁸sendgrid.com

3.6.8 SMS- Bestätigungscode

Das Konzept des in einem vorherigen Kapitel erwähnten Anbieters WebSMS soll von der Authentifizierungsschnittstelle ebenfalls implementiert werden. Der User gibt im ersten Schritt seine Mobilenummer ein. Er erhält dann einen Code per SMS zugesandt. Im zweiten Schritt gibt der User den erhaltenen 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.

Mehrfachteilnahme

Die mehrfache Teilnahme wurde bereits im Kapitel zum Anbieter WebSMS eingehenden behandelt. Daraus resultierte, dass in der Schweiz maximal fünf 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.³⁹

3.6.9 Telefonanruf mit Bestätigungscode

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

Automatisierungsmöglichkeit

Die Automatisierung kann als nicht möglich eingestuft werden.

Mehrfach Teilnahme

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

Kosten

Die Kosten berechnen sich bei den analysierten Anbietern basierend auf einer geringen Monatspauschale zwischen CHF 1.00 und CHF 2.00 und Kosten pro Minute je nach Telefonanbietern des Empfängers und Voicegateway zwischen CHF 0.10 und CHF 0.65.⁴⁰

³⁹ Die Preise wurden am 1. März 2016 auf aspsms.ch/instruction/prices.asp, tropo.com/pricing und twilio.com/sms/pricing abgefragt

⁴⁰ Die Preise wurden am 1. März 2016 auf nexmo.com/products/voice/, tropo.com/pricing und twilio.com/voice/pricing abgefragt

3.6.10 Postversand

Im Telefonbuch digital oder analog waren früher fast alle Personen erfasst. Immer weniger Personen haben heute einen Fixanschluss und einige lassen ihr Nummern nicht mehr eintragen. Nur vereinzelte Personen tragen ihre mobile Telefonnummer und Adresse im Telefonbuch ein. Google steht vor dem gleichen Problem mit ihrem Produkt Google Maps. In Google Maps sollen schnell neue Firmendaten, Veranstaltungslocations oder andere Adresseinträge erfasst werden können. Doch sollen Betrüger oder Spassvögel daran gehindert werden, Falscheinträge zu machen. Daher versendet Google zur Verifikation einfach einen Code per Brief bzw. Postkarte an die Adresse.⁴¹ Dieses simple Konzept kann auch für die Authentifizierungsschnittstelle umgesetzt werden, um die Adresse eindeutig zu verifizieren. Einen Haken hat dieses Konzept jedoch. Jemand muss den Brief ausdrucken, in ein Couvert legen, frankieren und per Post versenden. Dies kann als Service, z.B. beim Schweizer Startup pingen.com eingekauft werden.

Automatisierungsmöglichkeit

Die Automatisierung kann als nicht möglich eingestuft werden.

Mehrfachteilnahme

Die Teilnahmeanzahl ist von den vorhandenen Adressanschriften abhängig und daher ist eine Mehrfachteilnahme nur eingeschränkt möglich.

Kosten

Die Kosten berechnen sich für den Versand in der Schweiz bei den analysierten Anbietern je nach Druck und Versandart des Empfängers zwischen CHF 1.20 und CHF 1.65.⁴²

⁴¹(*Google Business 2016*)

⁴²Die Preise wurden am 10. März 2016 auf pingen.com abgefragt

3.6.11 OAuth

Die Zwei-Faktor-Authentifizierung OAuth wurde im Kapitel [OAuth-Provider](#) ausführlich erläutert.

Automatisierungsmöglichkeit

Eine OAuth-Registrierung kann als nicht automatisierbar eingestuft werden. Automatisierbares Anmelden und Verwenden von verschiedenen Accounts ist durchaus möglich. Plattformen wie kingfluencers.ch zeigen Möglichkeiten auf, wie automatisiert auf SocialMedia Plattformen von Dritten zugegriffen werden kann und Tätigkeiten ausgeführt werden können.

Mehrfachteilnahme

Eine Mehrfachregistration ist möglich.

Kosten

OAuth bewirkt keine direkten Kosten.

3.6.12 SuisseID Integration

SuisseID wurde bereits im Kapitel [SuisseID](#) erläutert.

Automatisierungsmöglichkeit

Eine Automatisierung ist nahezu unmöglich.

Mehrfachteilnahme

Eine Mehrfachteilnahme ist nahezu unmöglich.

Kosten

Für den Betreiber fallen geringe Kosten an. Der Endnutzer zahlt aber einen relativ hohen Preis.

3.6.13 Browser Fingerprints

Der Fingerabdruck ist aus der Kriminaltechnik nicht mehr wegzudenken. Bereits vor 2000 Jahren haben Chinesen ihre Schuldscheine mit Fingerabdrücken unterzeichnet. Es sollten über 19 Jahrhunderte vergehen, bis der Fingerabdruck auch in der Kriminaltechnik eingesetzt wurde. Seit über 100 Jahren, genauer seit 1913, ist der Fingerabdruck auch im Dienst der Schweizer Eidgenossenschaft. Im Gegensatz zur DNA unterscheidet sich der Fingerabdruck bei Zwillingen klar, auch wenn ähnliche Merkmale erkennbar sind. Bereits nach nur vier Monaten Schwangerschaft sind die Muster der Papillarleisten beim Embryo festgelegt. Der einzigartige Fingerabdruck des Menschen ist bereits dann fertig gestellt. Dieses Muster ändert sich bis zur Auflösung des Körpers nach dem Tod nicht mehr. ⁴³



Abbildung 3.4: Fingerabdruck: Mit Kohlepulver werden Fingerabdrücke sichtbar gemacht und auf Klebefolie gesichert. Quelle:phi-hannover.de

Der Fingerabdruck eignet sich zur Authentifizierung einer Person durch folgende Merkmale:

- Der Fingerabdruck ist eindeutig.
- Der Fingerabdruck ist über den Tod hinaus beständig.
- Der Fingerabdruck ist von aussen einfach "abrufbar". Er ist von blossem Auge sichtbar und wir hinterlassen das Muster der Papillarleisten auf Gegenständen wie Gläsern.

Fingerabdruck des Browsers

Im Gegensatz zum Datenschutz wäre es aus Sicht der eindeutigen Identifikation wünschenswert, wenn digitale Personen oder deren Geräte auch einen Fingerabdruck von sich geben würden, der sowohl eindeutig, beständig als auch abrufbar ist. Immer wieder versuchten unter dem Thema "Hardware Fingerprint" oder "Browser Fingerprint" Personen und Organisationen ein Verfahren zu entwickeln, das genau dies ermöglicht. Microsoft führte laut eigenen Angaben ⁴⁴ mit Windows XP Produktaktivierung ein Verfahren ein, das aus Prozessor-Typ, Grafikkarteninformationen und Festplatte einen Fingerabdruck des Geräts erstellt. So konnte bei einer zweiten Aktivierung mit dem selben Registrationsschlüssel Massnahmen getroffen werden.

Auch der Browser übermittelt an den Server verschiedene Informationen:

⁴³([Sondereggerl 2013](#))

⁴⁴([Technical Details on Microsoft Product Activation for Windows XP 2001](#))

Passives Fingerprinting

Die Kommunikation zwischen Client und Browser ist paketbasiert. Es besteht keine feste Leitung zwischen Client und Server. Ausserdem ist der Kommunikationsweg nicht zwingend gleich bleibend. Jedes HTTP-Paket besitzt Header-Daten aus den verschiedenen OSI-Layern. So können aus IP-Header, TCP-Header und HTTP-Header unter anderem folgende Daten gelesen werden:

Tabelle 3.1: Übersicht möglicher passiven Daten

Bezeichnung	Schicht
Quell-IP-Adresse	IP
Quellport	TCP
Aufrufende Seite	HTTP
Bezeichnung des Browsers („User-Agent“)	HTTP
Akzeptierende Dateitypen	HTTP
Akzeptierende Zeichensätze	HTTP
Akzeptierende Kompressionsformate	HTTP
Akzeptierende Sprachen	HTTP

Diese Daten werden zwingend an den Server gesendet und könnten passiv, also ohne dass ein zusätzliches „Programm“ beim Client läuft, ausgelesen werden.

Aktives Fingerprinting

Beim aktiven Fingerprinting werden per Javascript mögliche Browserkennzahlen abgefragt. In der folgenden Tabelle sind die komplexeren Gewinnungen von Kennzahlen aufgelistet.

Tabelle 3.2: Komplexere Kennzahlen aktives Fingerprinting

Bezeichnung	Beschreibung
Browser-Plugins	Die Funktionalität der Browser wird mit Browsererweiterungen ausgebaut. Bekannte Plugins: Adobe Reader, Adobe Flash Abfrage: navigator.plugins
Unterstützte Datenarten	Internetdokument können verschiedene Datenarten so genannte MIME-Type unterstützen. Abfrage: navigator.mimeTypes
Installierte Schriften	Mittels CSS kann geprüft werden welche Schriftarten beim Client installiert sind. Dabei wird probiert einen Katalog darzustellen. Die installierten Schriften können dargestellt werden.
Performance Messung	Basierend auf Javascript Performance-Tests kann unter Berücksichtigung der Implementation von JavaScript im Browser die Performance des Rechners ermittelt werden.

Das aktive Fingerprinting kann vom Endbenutzer festgestellt werden, da Javascript-Code in seinem Browser ausgeführt werden. Noch offensichtlicher wird es, wenn nach der Analyse die Daten auch an den Server übertragen werden.

Eine Beispielimplementation von Browserfingerprints wurde umgesetzt: <http://www.christianbachmann.ch/minifingerprint/>⁴⁵

⁴⁵Die kleine Testimplementation wurde basierend auf der Vorlage von Hennig Tillmann umgesetzt: (Tillmann 2013)

4 Anforderungen

Dieses Kapitel beschreibt das Durchführen einer Anforderungsanalyse. Anhand der Anforderungsanalyse sollen die Anforderungen für die zu entwickelnden Softwares ermittelt werden. Die Anforderungen bilden die Basis für die Architektur, das Softwaredesign, die Implementation und die Testfälle. Ihnen ist dementsprechend ein sehr grosser Stellenwert zuzuschreiben.

4.1 Akteure

Programmierer Der Programmierer ist der Entwickler der Webseite. Er möchte sein programmiertes oder sein verwendetes Social-Media-Modul mit dem Authentifizierungsservice schützen.

User Der User ist der Endbenutzer. Er nimmt am Social-Media-Modul teil und authentifiziert sich über den Authentifizierungsservice.

4.2 Use-Cases

Im Nachfolgenden werden alle Use-Cases aufgelistet, die im Rahmen dieser Thesis gefunden wurden.

4.2.1 Use-Cases Diagramm

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

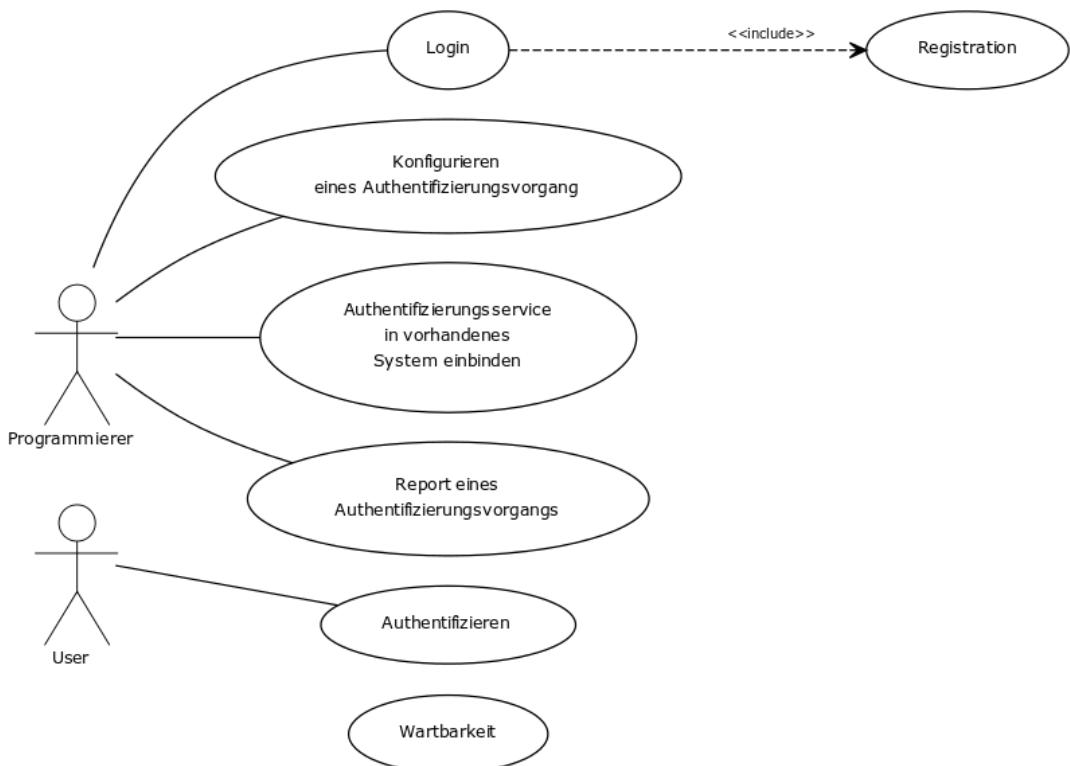


Abbildung 4.1: Use-Case Diagram

4.2.2 Use-Cases Beschreibung

Die im Diagramm dargestellten Use-Cases werden nun noch beschrieben. Die Use-Cases wurden numerisch nach Themenbereichen gruppiert.

UC-11 Registration für den Konfigurator

Use-Case	
Ziel	Ein Programmierer ist beim Authentifizierungsservice registriert.
Beschreibung	Ein Programmierer muss sich am Authentifizierungsservice registrieren können.
Akteure	Programmierer
Vorbedingung	Keine
Ergebnis	Registrierter Programmierer
Hauptszenario	Der Programmierer füllt ein Registrationsformular aus und bestätigt seine E-Mail Adresse.
Alternativszenario	-

UC-12 Login Konfigurator

Use-Case	
Ziel	Ein Programmierer kann sich beim Authentifizierungsservice registrieren.
Beschreibung	Ein Programmierer muss sich am Authentifizierungsservice authentifizieren können.
Akteure	Programmierer
Vorbedingung	Der Programmierer ist registriert.
Ergebnis	Authentifizierter und eingeloggter Programmierer
Hauptszenario	Der Programmierer loggt sich mit E-Mail und Passwort am Authentifizierungsservice ein.
Alternativszenario	Der Programmierer sendet sich das verpasste Passwort per E-Mail zu. Er erstellt über den im erhaltenen E-Mail enthaltenen Link ein neues Passwort und loggt sich mit E-mail und dem neuen Passwort am Authentifizierungsservice ein.

UC-21 Konfigurieren eines Authentifizierungsvorgang

Use-Case	
Ziel	Es ist ein neuer Authentifizierungsvorgang für ein neues Social Media-Modul konfiguriert.
Beschreibung	Der Programmierer kann ein neuer Authentifizierungsvorgang eröffnen.
Akteure	Programmierer
Vorbedingung	Der Programmierer hat sich am System angemeldet.
Ergebnis	Neuer Authentifizierungsvorgang
Hauptszenario	Der Programmierer eröffnet einen neuen Authentifizierungsvorgang. Er benennt ihn sinnig. Die zu verwerde(n) Authentifizierungskomponenten werden ausgewählt. Bei der Konfiguration unterstützen die Resultate der Studie den Programmierer für die optimale Konfiguration. Am Ende der Konfiguration werden die Akzeptanzkriterien für eine erfolgreiche Authentifizierung festgelegt.
Alternativszenario	Ein bestehender Authentifizierungsvorgang wird dupliziert.

UC-25 Authentifizierungsservice in vorhandenes System einbinden

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

UC-31 User authentifizieren

Use-Case	
Ziel	Der User ist authentifiziert oder der User abgelehnt.
Beschreibung	Der User probiert sich über den Authentifizierungsservice zu authentifizieren, um an einer Interaktivität teilzunehmen.
Akteure	User
Vorbedingung	Der Programmierer hat den Authentifizierungsvorgang konfiguriert und in seinem System eingebunden.
Ergebnis	Der Authentifizierungsservice authentifiziert den User oder lehnt ihn ab.
Hauptszenario	Der User wird von der Interaktivität an den Authentifizierungsservice weitergeleitet. Der User authentifiziert sich. Der User kann die Eingabe der Interaktivität erfolgreich abschliessen.
Alternativszenario	Der User wird von der Interaktivität an den Authentifizierungsservice weitergeleitet. Der User wird vom System abgelehnt. Der User kann die Eingabe der Interaktivität nicht erfolgreich abschliessen.

UC-41 Report eines Authentifizierungsvorgangs

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

UC-51 Wartbarkeit des Authentifizierungsservices

Use-Case	
Ziel	Der Authentifizierungsservice soll mit geringem 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.
Alternativszenario	-

4.3 Anforderungen

Die Anforderungen sollen basierend auf der Satzschablone erstellt werden. Ziel ist es, sprachliche Missverständnisse dadurch zu vermeiden. Die Schablone fördert eine syntaktische Eindeutigkeit der Anforderungen und einen 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 zeitlichen oder bedienungsorientierten Aspekt und der Schablone mit diesen Eigenschaften unterschieden.



Abbildung 4.2: Basis Schablone Quelle Rupp⁴⁶

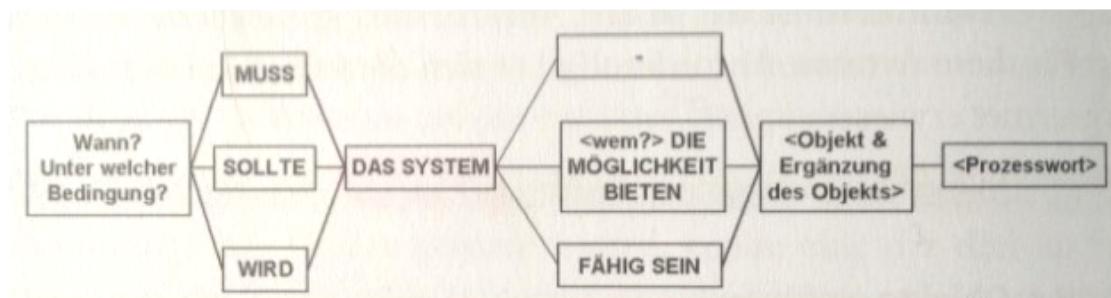


Abbildung 4.3: Erweiterte Schablone Quelle Rupp⁴⁷

⁴⁶ Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering (Rupp 2011)

⁴⁷ Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering (Rupp 2011)

4.4 Funktionale Anforderungen

Die funktionalen Anforderungen legen die Funktionen des Authentifizierungsservices fest. Die Wünsche des Arbeitgebers sind als Anforderungen umformuliert. Die funktionalen Anforderungen dienen als Grundlage für die Testfälle. Die Testfälle wiederum, zeigen dass alle gewünschten Funktionen implementiert wurden.

Funktionale Anforderungen werden als FREQ-*Identifikation* bezeichnet.

4.4.1 FREQ-111 Programmierer Registration

UC-Referenz	UC-11
Beschreibung	Ein Programmierer kann sich beim Authentifizierungsservice registrieren.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.2 FREQ-112 Programmierer Login

UC-Referenz	UC-12
Beschreibung	Ein Programmierer muss sich beim Authentifizierungsservice mittels E-Mail und Passwort anmelden.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.3 FREQ-113 Programmierer Passwort vergessen

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

4.4.4 FREQ-114 Programmierer Passwort ändern

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

4.4.5 FREQ-211 Konfigurieren eines neuen Authentifizierungsvorgangs

UC-Referenz	UC-21
Beschreibung	Ein Programmierer kann einen neuen Authentifizierungsvorgang für seine Interaktivität erfassen.
Techn. Risiko	Niedrig
Business Value	Sehr Hoch

4.4.6 FREQ-212 Antworten der Umfrage in Authentifizierungsservice importieren

UC-Referenz	UC-21
Beschreibung	Die Umfrageantworten müssen in den Authentifizierungsservice abgespeichert werden können. Der Import ist direkt über die Datenbank realisierbar.
Techn. Risiko	Niedrig
Business Value	Mittel

4.4.7 FREQ-213 Umfrageergebnisse zur Konfiguration nutzen

UC-Referenz	UC-21
Beschreibung	Ein Programmierer kann zur Konfiguration des Authentifizierungsvorangs die Umfrageergebnisse visualisiert nutzen. Dabei sollen verschiedene Auswertungsmöglichkeiten zur Anstrengung und Akzeptanz der Sicherheitsstufe möglich sein.
Techn. Risiko	Niedrig
Business Value	Mittel

4.4.8 FREQ-214 Anpassen eines Authentifizierungsvorgangs

UC-Referenz	UC-21
Beschreibung	Ein Programmierer kann den Authentifizierungsvorgang anpassen.
Techn. Risiko	Hoch
Business Value	Mittel

4.4.9 FREQ-215 Authentifizierungs-Stufe auswählen

UC-Referenz	UC-21
Beschreibung	Ein Programmierer muss eine Authentifizierungsstufe für den Authentifizierungsvorgangs auswählen.
Techn. Risiko	Niedrig
Business Value	Hoch

4.4.10 FREQ-251 Generierung von Code für Einbinden in ein vorhandenes System

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

4.4.11 FREQ-311 Authentifizieren

UC-Referenz	UC-31
Beschreibung	Ein User kann sich über den Authentifizierungsservice authentifizieren, um an der Interaktivität teilzunehmen. Der Authentifizierungsservice authentifiziert oder lehnt den User ab.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.4.12 FREQ-411 Report der Authentifizierungen generieren

UC-Referenz	UC-41
Beschreibung	Der Programmierer kann einen 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 NFREQ-*Identifikation* bezeichnet.

4.5.1 NFREQ-110 Betriebssystemunabhängigkeit

UC-Referenz	Alle
Beschreibung	Der Authentifizierungsservice muss auf allen bekannten Betriebssystemen mit HTML5 und javascriptfähigen Browser verwendet werden können.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.5.2 NFREQ-115 Wartbarkeit

UC-Referenz	UC-51
Beschreibung	Die Wartbarkeit des Systems 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 Authentifizierungsservice soll einfach im vorhandenen System eingebunden werden können.
Techn. Risiko	Mittel
Business Value	hoch

4.5.4 NFREQ-122 Einfache und verständliche visuelle Konfiguration

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Der Authentifizierungsservice soll einfach und verständlich/optisch konfiguriert werden können.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.5 NFREQ-126 Einfache und verständliche Authentifizierung

UC-Referenz	UC-31
Beschreibung	Der User soll einfach und verständlich/optisch authentifizieren können.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.6 NFREQ-127 Responsives Design für Authentifizierung

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Der User soll sich mit Desktop, Tablet und Smartphone authentifizieren können
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.7 NFREQ-130 Performance

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

4.5.8 NFREQ-132 Skalierbar

UC-Referenz	UC-31, UC-25, UC-21, UC22
Beschreibung	Das System soll eine hohe Skalierbarkeit aufweisen.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.9 NFREQ-135 Hohe Verfügbarkeit

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Der Authentifizierungsservice soll eine Verfügbarkeit von mindestens 99.9% haben.
Techn. Risiko	Hoch
Business Value	Mittel

4.5.10 NFREQ-210 Programmierer kann aus Vielzahl von verschiedenen Sicherheitsstufen auswählen

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Dem Programmierer stehen verschiedene Sicherheitsstufen zur Verfügung. Das Wort "verschieden" wurde durch folgende Aspekte mit dem Auftraggeber definiert: Abgeleitet von der Aufgabenstellung sind die Aspekte "Mehrfachteilnahme" und "Automatisierung" definiert worden. Beide Aspekte können durch eine Sicherheitsstufe mehr oder weniger verhindern werden. Abhängig von der Art der Interaktivität ist es wirtschaftlich sinnvoll, dass Kosten entstehen dürfen. Deshalb sind die Höhe der Kosten ein Aspekt. Ein weiterer Aspekt ist der Aufwand für den Benutzer.
Techn. Risiko	Niedrig
Business Value	Hoch

4.5.11 NFREQ-212 Die verwendeten Sicherheitsstufen sind in der Schweiz verbreitet

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Die eingesetzten Sicherheitsstufen sollten in der Schweiz verbreitet sein.
Techn. Risiko	Niedrig
Business Value	Hoch

4.6 Risiken

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

4.6.1 R-01 Akzeptanz

Programmierer und insbesondere auch User, welche den Authentifizierungsservice verwenden sollen, sind völlig unterschiedlich. Deren unterschiedlichen Ansprüche machen es schwierig, eine Lösung zu entwickeln, welchen den Akteuren gerecht wird.

Da der Auftraggeber sowohl die Zielgruppe Programmierer wie auch User kennt, 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/ das Hosting der Bachelorarbeit verursacht Kosten. Das Kostenrisiko kann dank fixen Leistungsparametern 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 Architekturentscheid beeinflusst werden kann, muss ein 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 dokumentiert 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 zusätzlicher, nicht einschätzbarer Aufwand nötig.

4.6.6 R-06 Termineinhaltung

Den fixen Abgabetermin der Bachelorarbeit gilt es einzuhalten. Das Risiko, dass die Arbeit verspätet abgegeben wird, besteht.

Dieses Risiko wird mit geringer Wahrscheinlichkeit eintreten. Die Auswirkung bei Eintritt dieses Risikos ist das Nichtbestehen 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 zusätzlichen Ausfällen durch Krankheit oder nicht vorhersehbare 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 widerspiegeln.

4.6.8 Risikomatrix

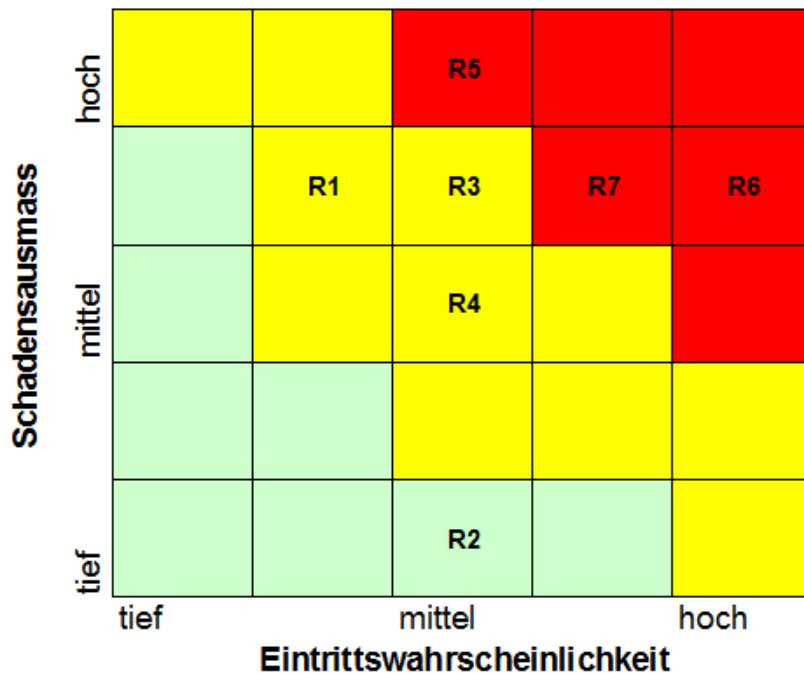


Abbildung 4.4: Risikomatrix ⁴⁸

R1 Akzeptanz

R2 Kosten

R3 Überkomplexität

R4 Systemumfeldänderungen

R5 Schlechte/Unzureichende Frameworks

R6 Termineinhaltung

R7 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.

Das Projekt ist über eine Anzahl von Feiertagen gelegt, welche gebraucht werden könnten. Zusätzlich ist vom Studenten eine Arbeitswoche Ferien eingeplant, welche im Notfall auch für

⁴⁸Die Risikomatrix wurde basierend auf der Excel-Vorlage der Stadtpolizei Zürich Abteilung Informatik entworfen. ([Vorlage Risikomatrix](#))

die Arbeit verwendet werden könnte. Durch diese Massnahmen soll das Risiko 6 "Termineinhaltung" minimal bleiben. Das Risiko 7 "Auslastung" kann nicht direkt vermindert werden. Die Aktivitäten im Bereich der freiwilligen Arbeit ist auf ein Minimum reduziert. Für die restliche freiwillige Arbeit ist mit Freunden ein Notfallszenario entwickelt worden, so kann der Student bei Bedarf seine freiwillige Arbeit durch andere Personen übernehmen lassen kann. Der Kontakt mit dem Arbeitgeber wird intensiv gepflegt, um bei Bedarf die Arbeitsbelastung zu vermindern. Die Massnahmen, welche für Risiko 6 ergriffen sind, entschärfen auch Risiko 7.

5 Konzept

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

Um die Komponenten unabhängig voneinander zu entwickeln, wird bei der Entwicklung der Architektur des Authentifizierungsservice darauf geachtet eine möglichst geringe Kopplung aufzuweisen.

5.1 Systemarchitektur

Gemäss den nichtfunktionalen Anforderungen muss die Serversoftware - unter anderem - folgende Eigenschaften erfüllen:

- Hohe Verfügbarkeit von 99.9%
- Wartbarkeit
- Performance

Die Softwarearchitektur wurde im Hinblick auf diese Anforderungen erstellt.

5.2 Architekturübersicht

Der Authentifizierungsservice besteht aus den Hauptkomponenten: Webserver mit Web-API und MVC-Webpages, Konfigurator und Autorisierung. Die folgende Abbildung zeigt die Verbindungen der drei Hauptkomponenten im Systemkontext des Authentifizierungsservice auf.

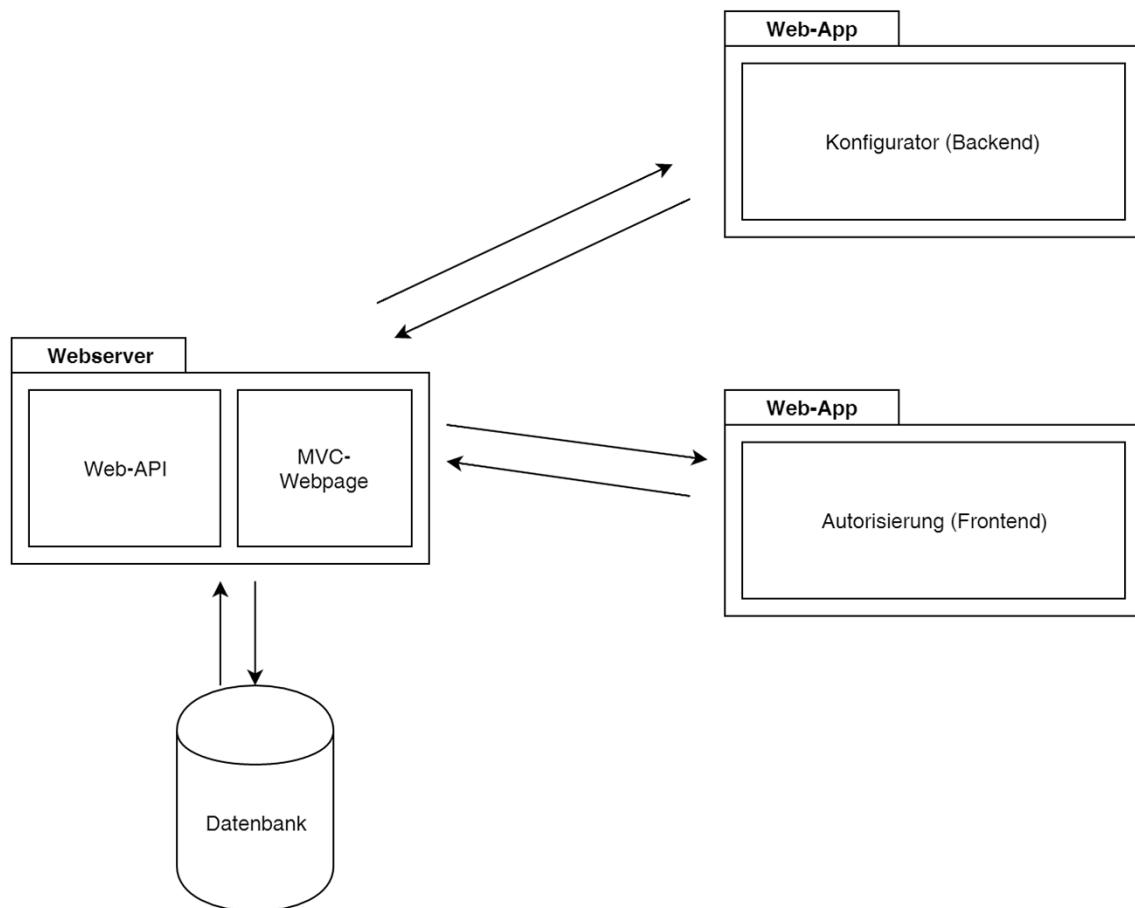


Abbildung 5.1: Übersicht der Hauptkomponenten

5.3 Genereller Ablauf der Authentifizierung

Der User nimmt an einer Interaktivität eines Anbieters teil. Dabei füllt er den Wettbewerb oder die Umfrage aus oder löst die gegebene Aufgabe und sendet einmal oder mehrmals ein Feedback an die Anbieter-Webseite zurück. Nach Abschluss der Interaktivität werden die Daten gespeichert und mit der daraus resultierenden eindeutigen Identität des Feedbacks wird die Authentifizierung gestartet. Das vom Programmierer definierte Authentifizierungsverfahren, bestehend aus ein oder mehreren Sicherheitsstufen, wird durchgeführt, um die Identität im gewünschten Maße sicherzustellen. Der User und das Anbieter-System werden über die erfolgreiche Authentifizierung informiert. Nach Möglichkeit wird auch eine fehlerhafte Authentifizierung mitgeteilt.

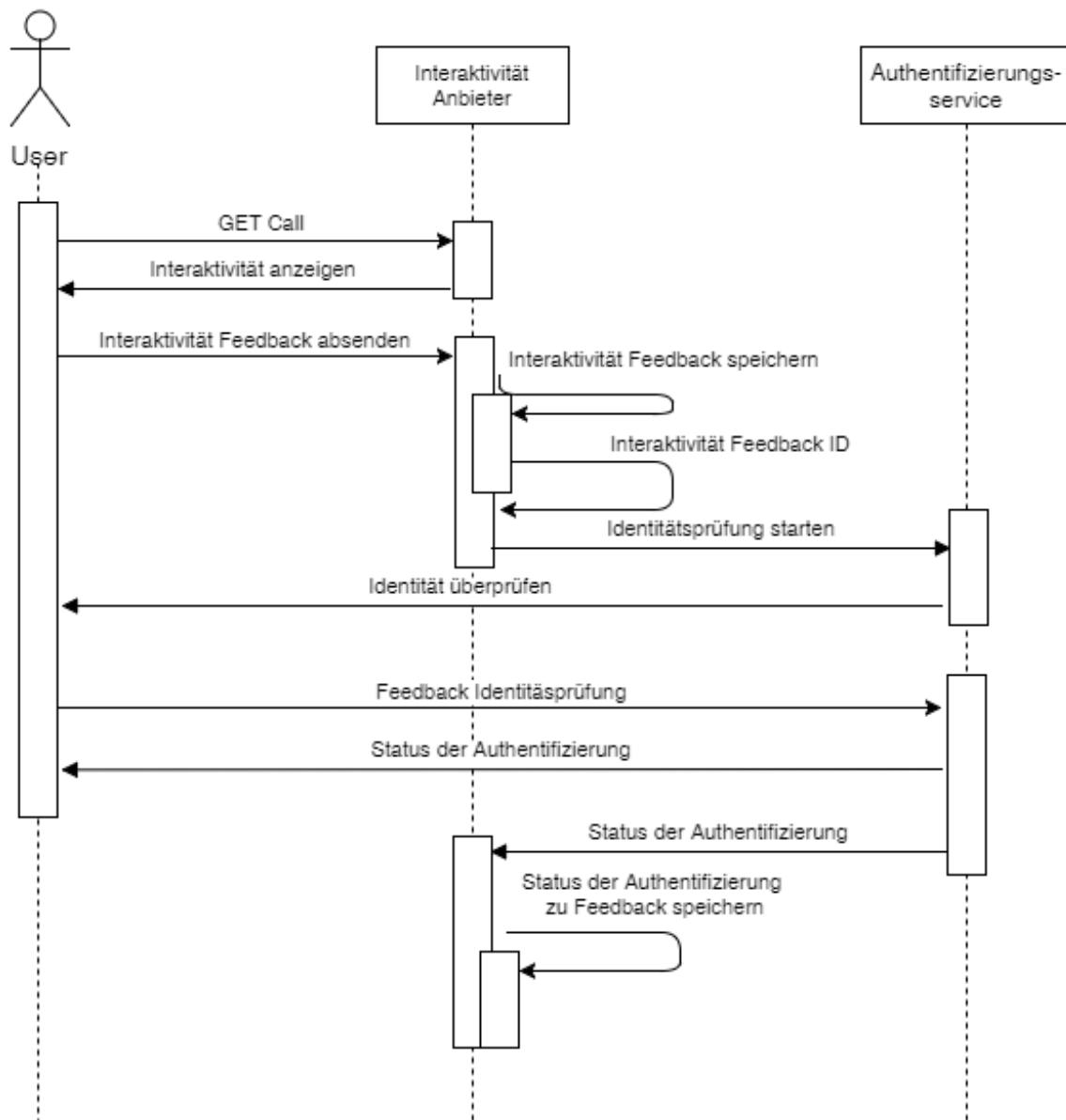


Abbildung 5.2: Sequenzdiagramm Ablauf der Authentifizierung

5.4 differenziertes Domänenmodell

Ein Domänenmodell - auch Domänenmodell Basis Level genannt - erlaubt eine vereinfachte Kommunikation zwischen Kunde/Auftraggeber und Entwicklungsteam/Entwicklungsperson. Die Denkweise im Modell erfordert keine Programmierkenntnisse und fördert die strukturierte Wiedergabe von Datengefäßen. Beim Domänenmodell werden die Begriffe aus der Domäne des Kunden verwendet und fördern so die Verständlichkeit auf beiden Seiten. Der Programmierer kann Projekte besitzen. Diese Projekte bestehen aus mehreren Sicherheitsstufen. Die Projekte haben keine oder mehrere Authentifizierungssversuche.

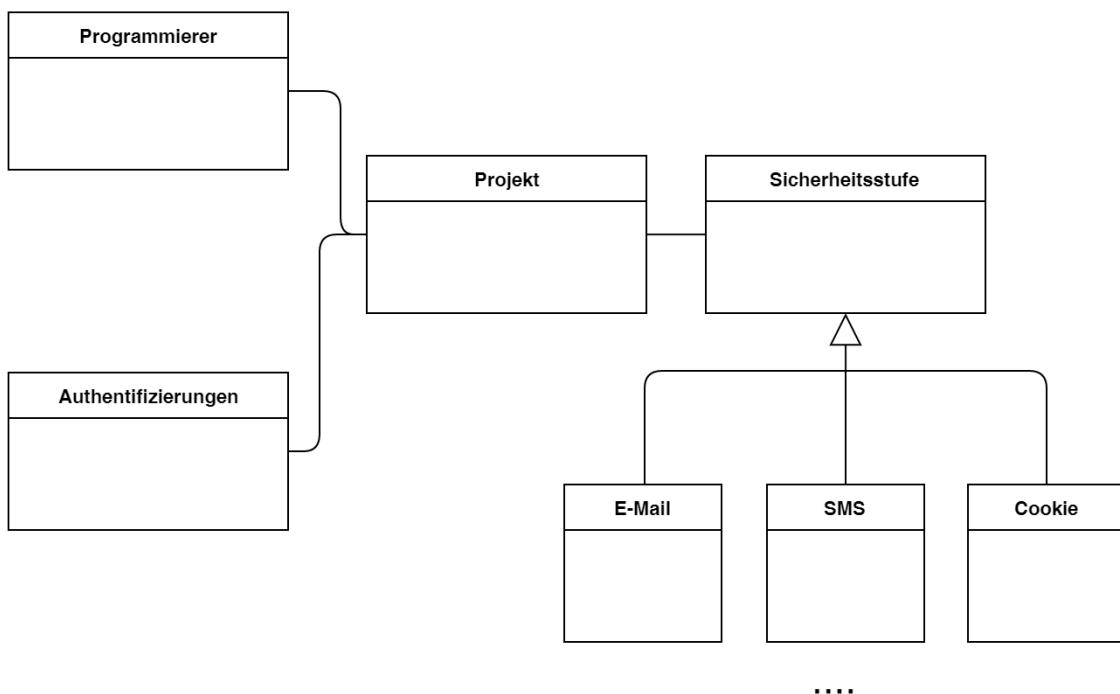


Abbildung 5.3: Differenziertes Domänenmodell des Authentifizierungsservice

5.5 Datenbankdesign

In der Systemarchitektur des Authentifizierungsservice stehen Objekte nur während der Ausführungszeit zur Verfügung. Um sie zu persistieren, werden sie in einer relationalen Datenbank gespeichert. Die Paradigmen der objektorientierten Programmiersprache und der relationalen Datenbank sind grundlegend verschieden. So kapseln Objekte ihren Zustand und ihr Verhalten hinter einer Schnittstelle und haben eine eindeutige Identität. Relationale Datenbanken basieren dagegen auf dem mathematischen Konzept der relationalen Algebra. Dieser konzeptionelle Widerspruch wurde in den 1990er Jahren als "object-relational impedance mismatch" bekannt.⁴⁹ Um diesen Widerspruch zu mindern, stellt Microsoft das Entity-Framework zur Verfügung.

5.5.1 Entity-Framework

Das Entity-Framework hat verschiedene konzeptionelle Ansätze um möglichst viele Bedürfnisse an den ORM-Mapper zu erfüllen. Es gilt nun den richtigen Ansatz für den Authentifizierungsservice zu wählen.

Database First

Beim Database First Ansatz wird zuerst die Datenbankdesign entworfen. Das Entity-Framework bildet aus der Datenbank die POCO-Klassen⁵⁰ ab. Sollten Anpassungen getätigt werden, sollen diese zuerst in der Datenbank implementiert werden und daraus werden wiederum neuen POCO-Klassen generiert.

Code First

Beim Code First Ansatz werden zuerst die POCO-Klassen erstellt. Das Entity-Framework bildet aus den POCO-Klassen die Tabellen in der Datenbank. Alle Anpassungen werden gleich in den POCO-Klassen umgesetzt und durch das Entity-Framework in der Datenbank geändert erstellt.

Entscheidung

Wenn die POCO-Klassen gleich mehrheitlich für die Schnittstellendefinition als Parameterdefinition verwendet werden könnten, fallen Mehraufwendungen für Umwandlungen im Programmcode weg. Eine Schnittstellendefinition sollte aber nicht willkürlich durch eine Datenbankänderung beeinflusst werden. Der umgekehrte Fall ist aber minder wichtig, da die Datenbank nur von der Schnittstelle verwendet wird. Deshalb wird das Konzept Code First eingesetzt.

5.5.2 ERD

Durch den Codefirst Ansatz werden die Datenbank und alle zugehörigen Tabellen durch das Entity Framework selbstständig generiert

⁴⁹(Neward 2006)

⁵⁰Eine POCO-Klasse ist ein ganz "einfaches" .NET-Objekt. Damit ist es geeignet schlank Daten zu transportieren. Weitere Informationen im [Glossar](#)

5.6 Integration der Schnittstelle

Wie in den [Anforderungen](#) und der [Aufgabenstellung](#) geschrieben, soll die Schnittstelle möglichst einfach in bestehende Systeme integriert werden können. Bevor wir untersuchen, wie wir die Integration umsetzen können, bedarf es die wichtigsten bestehenden Systeme zu kennen um eventuell für diese Systeme eine spezifisch einfache Integration zu entwickeln.

5.6.1 Bestehende Systeme für Votings, Wettbewerbe und Quizes

Das bestehende Interaktivitäts-Modul wird als Teil einer Webseite in einer Webapplikation geführt. Webapplikationen, welche Inhalte verwalten, werden sinngemäß Content-Management-Systeme genannt. Die Abkürzung CMS hat sich im IT-Fachjargon etabliert. Statista.com wertet mehrmals im Jahr die Verbreitung der verschiedenen CMS aus ⁵¹. Folgend ist die Erhebung aus dem November 2015 abgebildet:

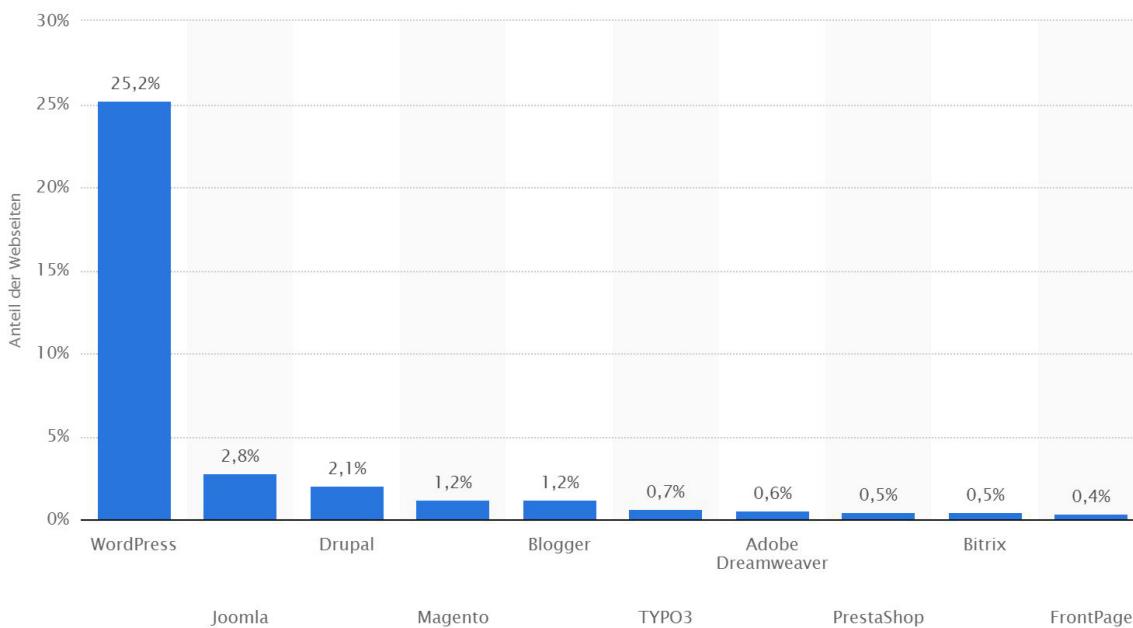


Abbildung 5.4: Nutzungsanteil CMS weltweit Quelle:de.statista.com

⁵¹CMS-Nutzungsstatistik von statista.com (*Top 10 CMS November 2015* 2015)

Die von statista.com veröffentlichten Zahlen wurden mit Werten von W3techs.com verglichen⁵². Die Unterschiede sind für unsere Verwendung minimal und liegen im Zehntelprozentbereich. Da beide bekannten Statistik Unternehmen auf die selben Werte gekommen sind, kann von einem hohen Wahrheitsgrad ausgegangen werden. Beim Betrachten der Statistik fällt auf, dass Wordpress mit 25,2% mit Abstand am meisten genutzt wird. Alle dynamischen Webseiten unter den Top 10 basieren auf Systemen in PHP⁵³. Adobe Dreamviewer und Front-Page 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 zu recherchieren, wie dort eine Authentifizierungsschnittstelle eingebunden werden könnte.

5.6.2 Wordpress-Plugin Hook

Erweiterungen im Wordpress nennen sich Plugins. Die Plugins können direkt über das CMS-Backend eingespielt werden. Alternativ können sie auch manuell installiert werden. Zum Beispiel, indem man ein Plugin selber programmiert oder beim Hersteller bzw. über das Plugin-Verzeichnis von Wordpress⁵⁴ herunterlädt. 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 Webseite⁵⁵ veröffentlicht. Dank dieser Kennzahl können nun die meistverbreiteten Plugins herausgefunden werden.

Wordpress basiert auf einem sogenannten Hook-System. "Hook" 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 von Wordpress enthält solche Hooks. Dadurch soll verhindert werden, dass Plugins 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 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 Plugins 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 Interaktivitäts-Plugins ausgewählt. Aus den Top 1000 der installierten Wordpress Plugins, welche von der Art Social-Media Modul sind werden Stichproben von kommerziellen Plugins und Stichproben aus in Beiträgen empfohlenen Plugins zur Untersuchung verwendet: ^{56 57}

⁵²CMS-Nutzungsstatistik von w3techs.com (*Usage of content management systems for websites 2015*)

⁵³Die Information wurde von den jeweiligen Hersteller- bzw. Communitywebseiten bezogen.

⁵⁴Das Pluginverzeichnis befindet sich unter <http://de.wordpress.org/Plugins>

⁵⁵Das Pluginverzeichnis befindet sich unter <http://de.wordpress.org/Plugins>

⁵⁶Das Pluginverzeichnis befindet sich unter <http://de.wordpress.org/Plugins>

⁵⁷Envato bietet eine Plattform für den Verkauf von Wordpress-Plugins an <http://market.envato.com>

Tabelle 5.1: Recherche Plugins

Plugin	Kosten	Installation	Info zu Hooks
WP-Polls	kostenlos	100000+	Über "wp_polls_add_poll" könnte man den erstellten Poll authentifizieren 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-Plugins für Interaktivitäten auf Hooks untersucht. Alle Plugins 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 wider Erwarten alle nicht untersuchten Plugins eine perfekte Hookanbindung liefern würden, hätten wir, mit den nicht untersuchten Plugins eine zu geringe Verbreitung. Der Ansatz, die Integration per Hooks zu machen, muss also fallen gelassen werden.

5.6.3 Parallelen in ähnliche Anwendungsfelder

Die vertiefte Untersuchung der letzten Kapitel wird beendet und es wird probiert eine andere Herangehensweise zur Lösungsfindung zu suchen: Forscher adaptieren immer wieder erfolgreichere Modelle aus anderen Bereichen 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 an der ersten Stelle und eine einfache Integration ist für den Erfolg - trotz internationalem Druck - notwendig. Dabei fährt Datatrans eine Zweiwegstrategie. Einerseits stellen sie für bekannte Shopsysteme gleich ganze Plugins zur Verfügung⁵⁸. Auf der anderen Seite bieten sie ausführlich beschriebene und einfache Schnittstellen an.

Datatrans Zahlungsablauf

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

1. Der Endkunde wählt ein oder mehrere Produkte aus und schliesst die Bestellung ab
2. Der Merchant (Webshop) zeigt Zahlungsseite von Datatrans, Karteninhaber gibt seine Kartendaten ein.
3. Datatrans autorisiert und verarbeitet - wenn möglich - die Transaktion zum Acquirer (akquirierende Bank).
4. Datatrans zeigt den Status dem Kunden an und sendet Status dem Merchant (Webshop) zurück.
5. Merchant (Webshop) zeigt dem Karteninhaber die Antwortseite (erfolgreich oder abgelehnt). ⁵⁹

⁵⁸Übersicht der Web-Shop Plugins ([Webshop 2016](#))

⁵⁹Für 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 selbst wird verdunkelt dargestellt.

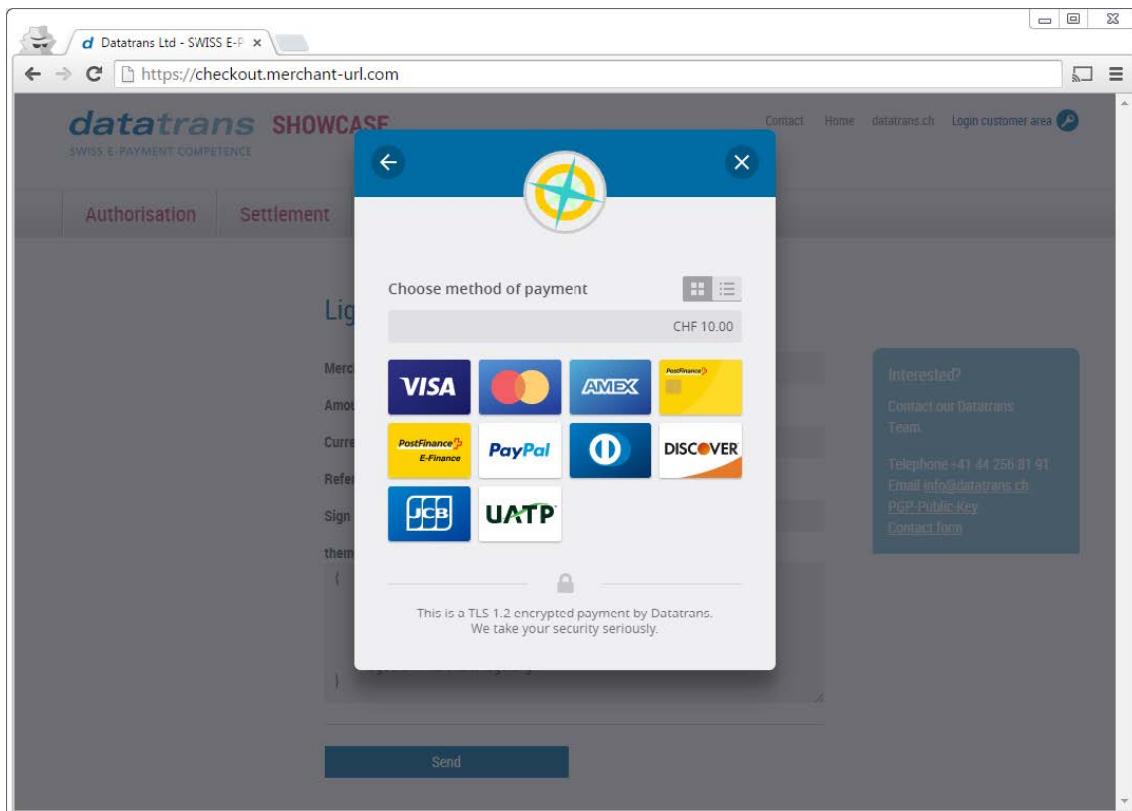


Abbildung 5.5: Datatrans Lightbox Integration Quelle:datatrans

Das Gateway muss ein Minimum an Informationen erhalten, um den Zahlungsvorgang überhaupt starten zu können. So muss es wissen, wer der Verkäufer ist. Datatrans regelt dies über eine Merchant-ID. Wieviel Geld in welcher Währung verkauft werden sollte, muss Datatrans über amount und currency mitgeteilt werden. Um dem Shop später mitteilen zu können, welche Bestellung erfolgreich verarbeitet wurde, braucht es eine Referenznummer. Die Referenznummer nennt Datatrans singgemäß refno. Die ganzen Parameter werden optional mit einem sign-Parameter gesichert und mittels Html-Form dem Javascript übergeben:⁶⁰

⁶⁰Für die Bachelorarbeit wurde die V 9.1.13 verwendet (*Datatrans eCom - Technical Implementation Guide 2016*)

Implementierungscode der Datatrans:

```

1 <script src="https://code.jquery.com/jquery-1.11.2.min.js"></
2   script>
3 <script src="https://pilot.datatrans.biz/upp/payment/js/
4   datatrans-1.0.2.js"></script>
5
6   <form id="paymentForm"
7     data-merchant-id="1100004624"
8     data-amount="1000"
9     data-currency="CHF"
10    data-refno="123456789"
11    data-sign="30916165706580013">
12      <button id="paymentButton">Pay</button>
13    </form>
14
15 <script type="text/javascript">
16   $("#paymentButton").click(function () {
17     Datatrans.startPayment({ 'form': '#paymentForm' });
18   });
19 </script>
```

5.6.4 Integrationsentscheid

Die Strategie der Paymentintegration von Datatrans soll für den Authentifizierungsservice genutzt werden.

Durch automatisches Öffnen der Lightbox erreicht der Endbenutzer mühelos den Schritt der Authentifizierung. Die Authentifizierung springt ihm nahezu entgegen. Dadurch ist eine hohe Effektivität gegeben. Der User bleibt auf derselben Seite und wird dadurch nicht aus dem Fluss der Abarbeitung der Interaktivität geworfen. Das Verfahren ist sehr effizient. Die Javascript- und CSS-Daten werden beim Laden der Interaktivität bereits mitgeladen. So entsteht eine minimale Wartezeit beim Einblenden der Lightbox. Dies ist für den User nicht spürbar oder störend.

Bei der Darstellung der Authentifizierung auf einer einzelnen Seite müsste das Web-Design des Interaktivitäts-Anbieter adaptiert werden können. Da die Authentifizierungs-Lightbox auf seiner Seite dargestellt wird, braucht der Interaktivitäts-Anbieter nicht sein Design mühsam für eine Authentifizierungsseite zu konfigurieren.

Die Lightbox des Authentifizierungsservice wird mit einer grösseren Verbreitung einen gewissen Wiedererkennungswert erhalten. So wird die Lösung als professionelles Produkt wahrgenommen werden. Das Ziel, dass Benutzer und Entwickler den Authentifizierungsservice als ein sicheres und glaubwürdiges Produkt für Interaktivitäten wahrnehmen, wird so versteckt werden.

5.6.5 Integrationskonzept

Der eingeschlagene Weg für die Integration wird nun konkret festgehalten. Die Parameter für die Schnittstelle zwischen Anbieter und Authentifizierungs-Lightbox sind eindeutig spezifiziert:

Tabelle 5.2: Parameter Authentifizierungsservice Lightbox

Feldname	Wert	Beschreibung
projectId	Integer	Project ID
providerId	String	Die ID um die Interaktivität seitens Interaktionsanbieter eindeutig zu erkennen
sign	String	Signatur, welche die Eingaben überprüft.

Einfache Signatur

Die Verwendung einer einfachen Signatur beugt Eingabefehler vor. Die Signatur, ist eine weitere Hürde den Missbrauch der Schnittstelle zu verhindern. Um eine korrekte Signatur zu erstellen werden folgende Parameter konateniert und mit einem Plus(+) separiert.

- projectId: Parameterfeld
- providerId: Parameterfeld
- validationCode: Beim Anlegen eines Projektes im Konfigurator des Authenifizierungsservice soll ein ValidationCode vom Authenifizierungsservice generiert werden und dem Programmierer zur Verfügung gestellt werden.

Beispiel: 30045+12+BUQHFMNZ4P3T8XNVNOLK

Der daraus resultierende String wird mit MD5 verschlüsselt.

Beim Beispiel gäbe es die Signatur b37b3d4cd7cd8cba3f409f07d6f6d9bd

5.6.6 Schlussspeicherung

Nach Abschluss der Authentifizierung erhält der User visualisiert ein Feedback. Sofern die Authentifizierung erfolgreich war, wird im Hintergrund die im Konfigurator angegebene URL des Anbieters aufgerufen. Über die Post-Parameter ProjectId und ProviderID erfährt die Serverapplikation um welchen Datensatz es sich handelt. Wiederum wird der sign-Parameter zum Absichern mitgegeben. Die Gefahr besteht trotzdem, dass diese Redirect-URL auch von einem anderen Programm aufgerufen werden könnte. Deshalb kann als zweite Absicherung die Serverapplikation des Anbieters die Validate WebAPI des Authenifizierungsservice aufrufen und die erhaltenen Daten gegenprüfen. Bei erfolgreicher Gegenprüfung gilt der Datensatz seitens Anbieter auch als valide und kann dann persistiert werden.

5.7 Sicherheitsstufen integrieren

Im Kapitel [Recherche](#) wurden einige Sicherheitskomponenten recherchiert und illustriert. Es gilt nun ein Setting an Komponenten zu finden, welche dem Programmierer eine breite Auswahlmöglichkeit (NFREQ-210) bietet und eine genügende Verbreitung in der Schweiz hat (NFREQ-212), ihn aber nicht durch komplexes Auswählen der Sicherheitsstufen aufhält (NFREQ-222).

Ausweisnummer

Durch Überprüfung der Checksumme und Doppelspeicherung des Ausweises soll ein Benutzer, der bereits an einer Interaktivität teilgenommen hat, identifiziert werden. Da der Checksummen-Algorithmus öffentlich ist, können diese auch vom Anwender (automatisch) generiert werden. Dadurch ist sowohl das Verhindern mehrfacher Teilnahmen, wie auch das Verhindern einer automatisierten Teilnahme an einer Interaktivität ungenügend geschützt. Vorteilhaft für die Sicherheitsstufe Ausweisnummer ist, dass es dem Anwender eine, wenn auch nicht existierende, Sicherheit vermittelt und keine Kosten verursacht.

Browser Fingerprint

Durch Generierung eines Browser Fingerprints (siehe [Recherche](#)) kann der Browser identifiziert werden. Das Verfahren kann zu 94% einen User wiedererkennen. Das Verwenden mehrerer Browser oder Geräte führt zu verschiedenen Browser Fingerprints. Das iPhone taugt nicht für diese Methode. Deshalb muss Eindeutigkeit und Verhinderung von Automatisierung als ungenügend bewertet werden. Die Methode kann als kostenlos eingestuft werden und generiert beim Endbenutzer keinen Aufwand.

Cookie

Durch Speicherung des Cookies soll ein Benutzer der bereits an einer Interaktivität teilgenommen hat, identifiziert werden. Da die Cookies clientseitig verwaltet werden, können diese auch vom Anwender manipuliert werden. Mit Browser-Makro-Tools wie iMacro kann ganz einfach ein Cookie gelöscht werden. Dadurch ist sowohl das Verhindern mehrfacher Teilnahmen, wie auch das Verhindern einer automatisierten Teilnahme an einer Interaktivität ungenügend geschützt. Vorteilhaft für die Cookiemethode ist, dass der Benutzer keinen Aufwand betreiben muss und es keine Kosten verursacht. Die Automatisierung ist bei Flash-Cookies etwas aufwendiger, da die Verbreitung kleiner ist.

E-Mail Authentifizierung

Der Benutzer gibt seine E-Mail ein. Durch Versenden eines Codes wird sichergestellt, dass dem Benutzer die E-Mail gehört. Da einfach mehrere E-Mail-Adressen registriert werden können, kann der Benutzer nicht eindeutig anhand der E-Mail-Adressen erkannt werden. Die Automatisierung ist aufwendig. Für die E-Mail Authentifizierung entstehen keine direkten Kosten.

IP-Adresse

Durch Speicherung der IP-Adresse soll ein Benutzer, der bereits an einer Interaktivität teilgenommen hat, identifiziert werden. Eine IP-Adresse vertritt gegen Aussen alle Benutzer mit dem selben "Internetanschluss". Dadurch könnte nur einmal pro "Internetanschluss" an einer Interaktivität teilgenommen werden. Dass durch Wechseln des Proxys eine andere IP-Adresse verwendet werden kann und dies auch ohne IT-Know-How durch Tools möglich ist, lässt sowohl Eindeutigkeit als auch Verhinderung von Automatisierung als ungenügend bewerten. Die Methode kann als kostenlos eingestuft werden und generiert beim Endbenutzer keinen Aufwand.

OAuth

Der Benutzer authentifiziert sich beim OAuth Anbieter. Mehrere Accounts können bei einem Anbieter erstellt werden. Die Erstellung eines Accounts ist meist nicht automatisierbar aber dafür deren Verwendung. Die Methode kann als kostenlos eingestuft werden und generiert beim Endbenutzer wenig Aufwand.

Postversand Authentifizierung

Der Benutzer gibt seine Adresse ein. Um sicherzustellen, dass die Adresse dem User gehört, wird automatisiert ein Brief an die Adresse gesendet. Da die Gefahr besteht, dass falsch adressierte Briefe den Empfänger trotzdem erreichen, wird es bei der Eindeutigkeit in der Bewertung Abzug geben. Eine Automatisierung ist praktisch unmöglich. Die Kosten pro Brief sind von allen aufgelisteten Methoden am höchsten. Der Benutzer muss bei dieser Methode den Brief nach Erhalt auf einer Webseite quittieren.

SMS Authentifizierung

Der Benutzer gibt seine Mobilenummer ein. Durch Versenden eines Codes wird sichergestellt, dass dem Benutzer die Telefonnummer gehört. In der Schweiz können maximal fünf Mobilenummern bei den Anbietern gekauft werden (Siehe Kapitel [Recherche](#)). Der Benutzer kann eindeutig anhand der Mobilenummer erkannt werden. Die möglichen Mobilenummern pro User sind beschränkt. Eine Automatisierung ist praktisch unmöglich. Die Kosten pro SMS sind tragbar. Der Benutzer muss bei dieser Methode sein Handy bei sich tragen und den Code übertragen.

SuisseID

Der Benutzer authentifiziert sich via SuisseID. SuisseID garantiert eine hohe Sicherheit und verhindert Mehrfachteilnahmen. Die Verbreitung ist jedoch ziemlich gering und die Kosten für den Endbenutzer zu hoch.

Telefon Authentifizierung

Der Benutzer gibt seine Telefonnummer ein. Der Benutzer wird automatisiert angerufen und die Computerstimme liest einen Code vor, welcher der Benutzer im Rückbestätigungsformular

einträgt. Dadurch wird sichergestellt, dass die Telefonnummer dem Benutzer gehört. Mobilenummern sind, wie vorhin erwähnt, eingeschränkt. Festnetzanschlüsse unterliegen einer finanziellen Hürde.

5.7.1 Sicherheitsstufen bewerten

Die Recherche der verschiedenen Sicherheitsstufen wurden dem Auftraggeber vorgelegt. Beim Auftraggeber wurden die verschiedenen Sicherheitsstufen intern besprochen und bewertet. Pro Sicherheitsstufen wurde den vier definierten Aspekten und dem Musskriterium Verbreitung eine Bewertung in Form einer Schweizer Schulnote vergeben.

Tabelle 5.3: Übersicht der Authentifizierungs Methoden

Sicherheitsstufen	Verhinderung Mehrfach- teilnahme	Verhinderung Automat- sierung	Kosten	Aufwand Benutzer	Verbreitung in der Schweiz
Ausweis- nummer	3.5	3.5	6	5	6
Browser	3.5	3.5	6	6	6
Fingerprint					
Cookie	2.5	2.5	6	6	6
E-Mail	4	4.5	6	4.5	6
Flash-Cookie	2.5	3	6	6	3.5
IP	3	3	6	6	6
OAuth	3.5	4.5	5.75	5.5	5.25
Postversand	5.25	5.75	5	4.5	5.75
SMS	5.5	5.75	5	4.5	5.5
SuissID	5.5	5.75	3.5	5	3
Telefonanruf	5.25	5.75	5	4.5	5.75

5.7.2 Auswahl der zu integrierenden Sicherheitsstufen

SuissID und Flash-Cookies erreichen beim Musskriterium Verbreitung in der Schweiz (nach NFREQ-212) keine genügende Note und werden daher ausgeschlossen. Um die geforderte Breite an Sicherheitsmethoden zu erlangen, wurden die folgenden Methoden mit verschiedenen Stärken in Aspekten durch den Auftraggeber ausgewählt:

- IP-Adresse
- Captcha
- E-Mail
- SMS
- Telefonanruf
- Postversand
- Ausweisnummer

5.8 Modularität und Erweiterbarkeit

Wie in der Einführung zum Konzept erwähnt, sollte eine Architektur so konstruiert werden dass Sie möglichst modular aufgebaut ist. Auch wenn wir die zu verwendenden Authentifizierungsmethoden im vorherigen Kapitel definiert haben, werden sich diese in Zukunft ändern. Anderseits können sich auch die Authentifizierungsmethoden selbst komplett verändern. Sehr realistisch ist, dass für einen Browser-Fingerprint neue Berechnungsmethodiken bekannt werden. Der Anbieter, der hinter einer Authentifizierungsmethode steht, kann sich verändern oder dessen Anbindung anpassen. Kurz gesagt, die Modularität der Authentifizierungsmethoden muss unbedingt gewährleistet sein. Eine Implementation der Sicherheitsstufe SMS wie im folgenden einfachen Beispiel, sollte nicht verwendet werden.

```
1 SMSecurityStep inst = new SMSecurityStep();
```

5.8.1 Design by Contract

Das Design Pattern “Design by Contract” soll das Zusammenspiel von Modulen durch eine Definition/Vertrag regeln. Herr Bertrand Meyer führte das Pattern bei der Entwicklung der Programmiersprache Eiffel ein.⁶¹ Die Vertragsdefinition besteht aus

- precondition: “Die Zusicherung, die der Aufrufer einzuhalten hat”
- postcondition: “Die Zusicherung, die der Aufgerufene einhalten wird”
- Invariants: “Invariants sorgen dafür, dass bei Eintritts- und Austrittspunkten des Server Codes gewisse Bedienungen erfüllt bzw. Zustände gewahrt sind. Invariants sind in gewisser Weise also Pre- und Postconditions.”

Im Grunde geht es darum, den Operator new zu eliminieren.

Der Beispielcode als Design by Contract Pattern:

```
1 ISecurityStep proxy = new SomeFactory.GetSecurityStep(...);
```

ISecurityStep-Vertrag ist im Beispielcode der Vertrag. Die Instanz “proxy” liefert ein Objekt zurück, welches nach ISecurityStep-Vertrag definiert ist. Welches Objekt (Implementierung) sich dahinter verbirgt, ist uninteressant, da diese Komponente gegen eine andere Implementierung ausgetauscht werden kann. In diesem konkreten Fall, könnten beispielsweise die Komponenten SMSecurityStep und CookieSecurityStep die Schnittstelle ISecurityStep implementieren.

SomeFactory muss für die Umsetzung jedoch implementiert werden. Dafür gibt es in der .NET-Welt einiges an Beispiel-Code und Frameworks zu finden. Ein beliebtes Framework ist die Windows Communication Foundation.⁶²

⁶¹(Hausherr 2006)

⁶²(Hausherr 2006)

5.8.2 MEF - Managed Extensibility Framework

MEF, das Managed Extensibility Framework, ist seit der Version 4.0 Bestandteil des .NET Frameworks. MEF ist eine Bibliothek und implementiert das Problem der Erweiterbarkeit sogar zur Laufzeit. Es vereinfacht die Implementierung von erweiterbaren Anwendungen und bietet Ermittlung von Typen, Erzeugung von Instanzen und Composition Fähigkeiten an.

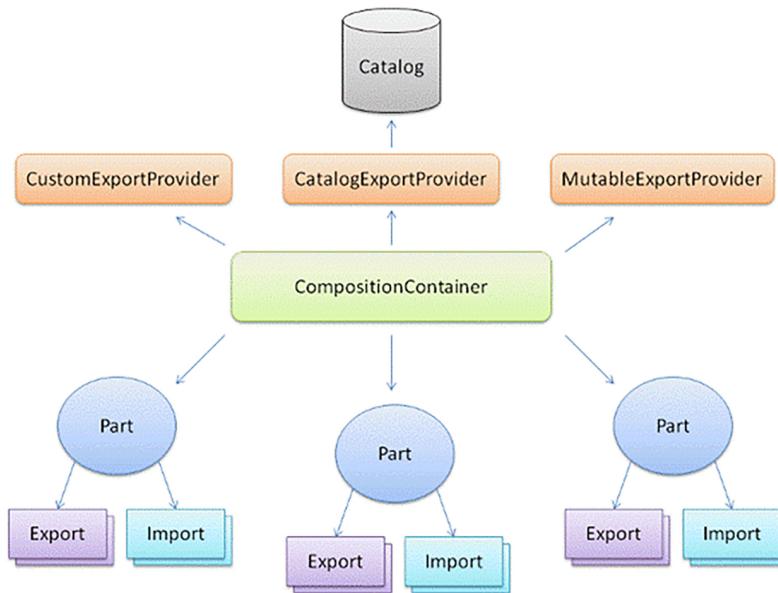


Abbildung 5.6: Vereinfachte Architektur des Managed Extensibility Framework Quelle: msdn.microsoft.com

Die Abbildung zeigt eine stark vereinfachte Architektur von MEF auf. Die Hauptmodule vom MEF-Core sind Catalog und CompositionContainer. Der Catalog kontrolliert und stellt das Laden der Komponenten sicher. Der CompositionContainer erzeugt aus den Komponenten Instanzen und bindet diese an die entsprechenden Variablen. Parts sind die Objekte die vom Type Export oder Import sein können. Die Komponenten die geladen und instanziert sind nennen sich Exports. Imports sind die Variablen, an den Exports gebunden werden sollen.

Um das Konzept besser zu verstehen, soll der Beispielcode von [Design by Contract](#) herangezogen werden: In einer MEF-Anwendung wäre die Variable proxy vom Type ISecurityStep und die Instanz dieser Komponente wäre ein „Import“. Die Objekte der SMSecurityStep oder CookieSecurityStep wären in einer MEF-Anwendung ein Export.

MEF automatisiert die Instanzierung mit Hilfe von Catalog und Container.

5.8.3 Entscheidung

Der Ansatz der Umsetzung des Design by Contract bräuchte eine geeignete Integration für die Factory, um die Modularität für NFREQ-115 sicherzustellen. MEF stellt den vollen Umfang an Funktionalität, zur Lösung der Problematik, zur Verfügung. MEF bietet des Weiteren die Möglichkeit die DLL-Daten zur Laufzeit auszutauschen und eine automatisierte Instanzierung. Deshalb sind die Sicherheitsstufen des Authentifizierungsservices basierend auf MEF zu integrieren.

5.8.4 Sicherheitsstufen Library-Übersicht anhand MEF

Basierend auf dem Managed Extensibility Framework wird der Aufbau umstrukturiert. Neu wird nicht alles in einer Library im Webservice gespeichert sondern mehrere Libraries erstellt. Die Library SecurityStepContracts beinhaltet den Contract/Vertrag der Sicherheitsstufen ISecurityStep. Es besteht keine Abhängigkeit zwischen dem Authentifizierungsservice und den Sicherheitsstufen.

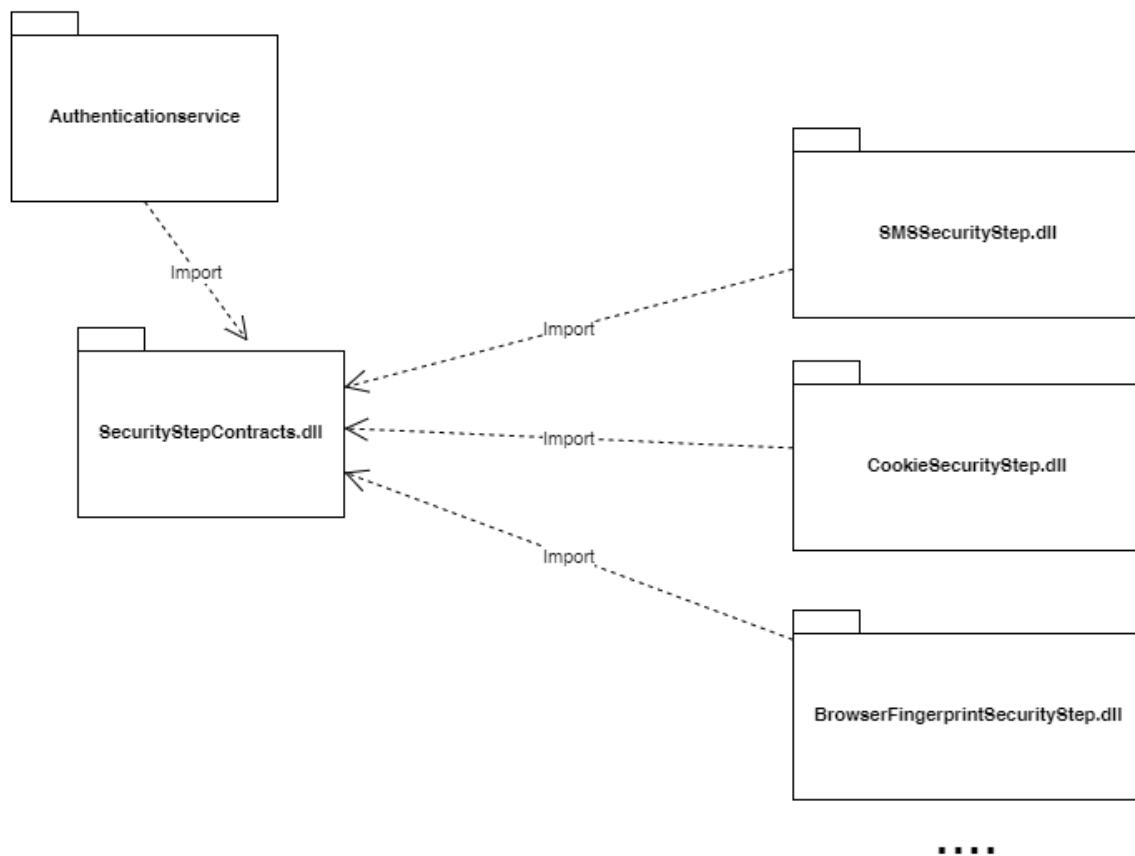


Abbildung 5.7: UML Library Overview

5.8.5 Definition der Sicherheitsstufenverträge

Verträge für das Backend

Pro Projekt des Anbieters und muss der Programmierer für jede Sicherheitsstufe verschiedene Konfigurationen tätigen können. Die Konfigurationen können da variieren. So kann bei der Sicherheitsstufe E-Mail der Absendername und Antwort-E-Mail-Adresse definiert werden, bei der Telefonvalidierung ein Grusswort. Es soll eine Abfrage der Konfigurationsparameter pro Plugin vorhanden sein. Diese soll mit allfällig bereits erfassten Werten übermittelt werden. Um die Werte zu speichern muss eine Speicherfunktionion pro Plugin aufrufbar sein. Weiter sollen statische Vergleichsparameter pro Plugin übergeben werden können. Die Vergleichsparameter entsprechen generell den Angaben aus Kapitel [Sicherheitsstufen bewerten](#). Für neuere Plugins werden diese Bewertungen vom Auftraggeberteam neu definiert. Anzumerken ist hier, dass die Studienergebnisse zentral verwaltet werden und dynamisch, sofern das Plugin in der Studie bewertet wurde, ausgelesen werden.

Verträge Frontend

Der Authentifizierungsservice soll von jedem Sicherheitsstufen-Plugin den Status über die Validierung erfragen können. Um die Validierung der einzelnen Stufe (noch einmal) zu beginnen oder als valide zu bezeichnen. Das Microsoft MVC-Framework braucht, falls nicht anders definiert, eine Index-Seite pro Controller. Diese Vorbedingung wird als Einstiegspunkt für die Validierung einer Sicherheitsstufe verwendet.

Aus den gegebenen Ansprüchen wird folgendes Interface konzeptioniert:

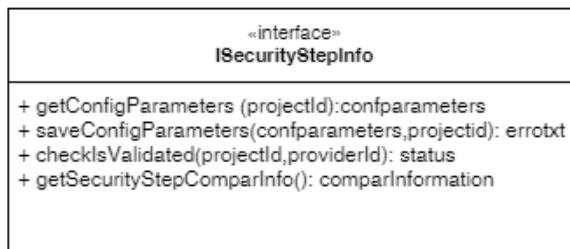


Abbildung 5.8: Interface ISecurityStepInfo

5.9 Mockup

Ein Mockup ist eine grobe Vorlage für die Design-Umsetzung. Es ist eine ideale Möglichkeit das visuelle Konzept abzubilden und mit dem Auftraggeber vorgängig anzuschauen. Die folgenden Unterkapitel bilden die Mockups der App ab.

5.9.1 Konfigurator Template

Der Konfigurator soll den Programmierer visuell beim Konfigurieren und Verwalten seiner Authentifizierungssoftware unterstützen. Bei der Zielgruppe handelt es sich um Programmierer. Es kann deshalb von einem hohen Know-How ausgegangen werden. Die Oberfläche soll möglichst effizient gestaltet sein. Die Designelemente sollen deshalb klar und einheitlich gestaltet werden. Generell ist davon auszugehen, dass der Programmierer beim Einrichten seines Projektes am Desktop-Computer arbeitet. Für Auswertungen und Präsentationen kann der Programmierer durchaus auch mobile Endgeräte verwenden. Deshalb soll die Umsetzung responsive gestaltet werden.

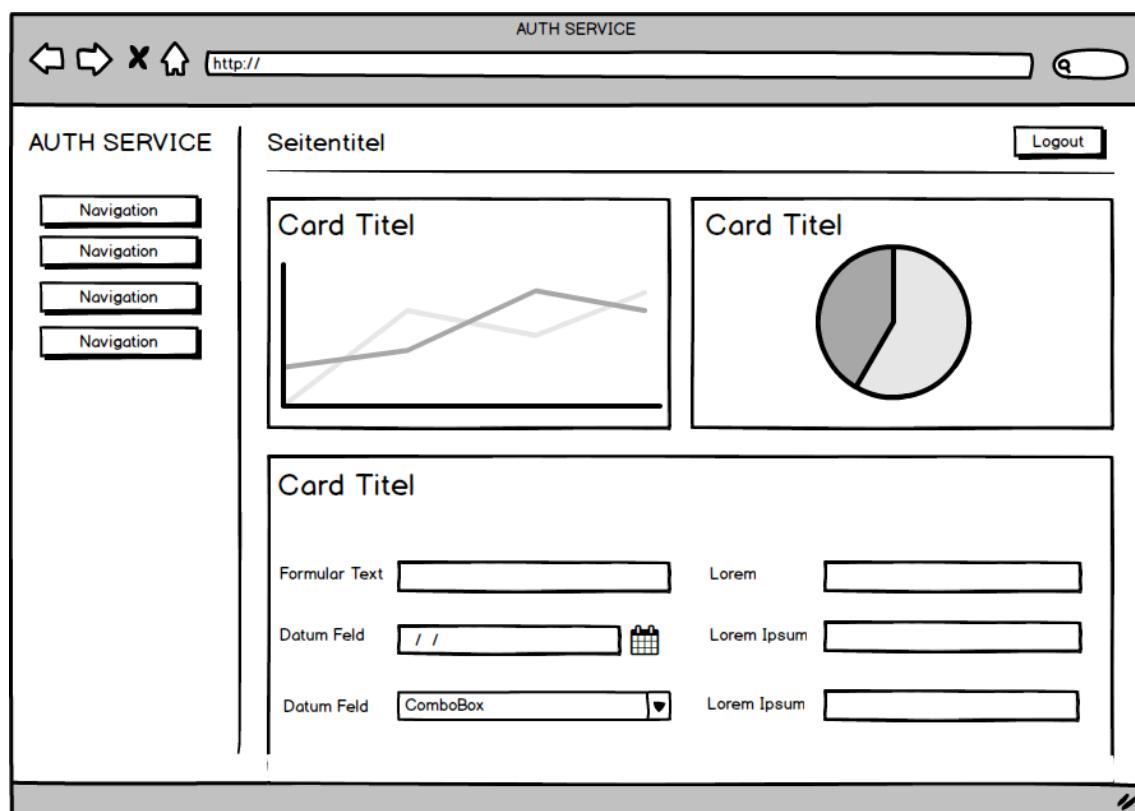


Abbildung 5.9: Mockup Konfigurator Template Desktop

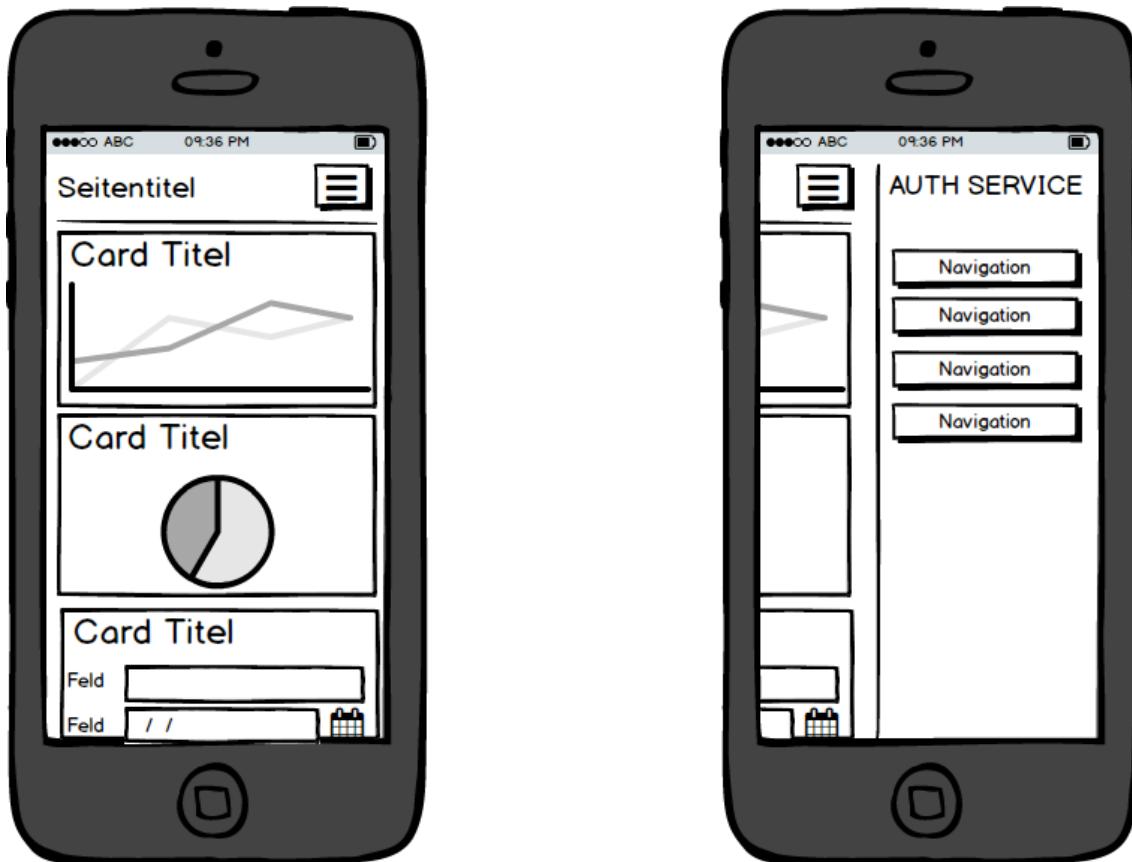


Abbildung 5.10: Mockup Konfigurator Template Mobile

Seitenaufbau

Im Header wird der Programmierer anhand des Seitentitels gleich über seinen aktuellen Standort orientiert.

Navigation

Im Designkonzept ist von einer Klappmenü oder Topnavigation abgesehen. Die Wichtigkeit, durch einen Klick alle Navigationspunkte zu erreichen, überwiegt den Platzersparnissen in der Breite. Die wenigen Navigationspunkte erlauben eine flache Navigationsstruktur. Dadurch können in der Desktopansicht links immer alle Navigationspunkte angezeigt werden. Der Programmierer kann rasch auf die gewünschte Seite wechseln. In der Mobileansicht kann durch einen einzigen Klick auf die "Burger-Navigation" das gesamte Menü eingefahren werden. Der Entscheid, für eine statische linke Navigationsstruktur in der Desktopansicht, wurde ausserdem begründet durch den Wunsch des Auftraggebers den Konfigurator gestalterisch mit Farben und Bildbereich aufzuwerten. Dies ist über die linke Spalte einheitlich und einfach umsetzbar.

Inhaltaufbau

Trotz unterschiedlichstem Inhalt (Text, Tabellen, Diagramme, Bilder und Formulare) und Grösse soll eine einheitliche Struktur geschaffen werden. Die Struktur soll es erlauben, einerseits Übersichten wie Dashboards mit verschiedenen Inhalten, auf einer Seite abzubilden. Andererseits soll die selbe Struktur aber auch für Seiten mit nur einem Inhaltselement, wie Registration oder Login-Seite verwendet werden können. Verschiedene Designe lösen diese Problematik mit einem Karten-Konzept (Card Based Design). Dabei wird jedes Inhaltselement als "Card" dargestellt. Die "Card" hat einen klar abgegrenzten Darstellungsbereich. Die Card ist in Header und Content unterteilt. Im Header wird mittels Titel dem Anwender kommuniziert, was für ein Inhalt im Bereich Content der "Card" zu erwarten ist.⁶³

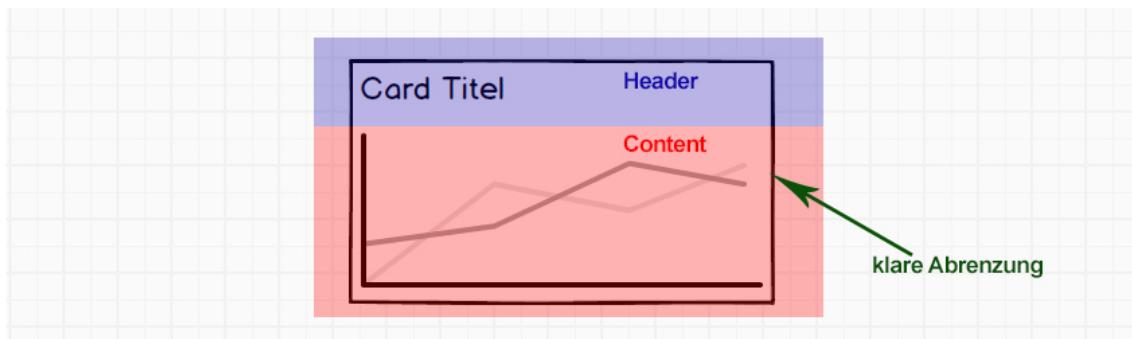


Abbildung 5.11: Aufbau Inhalt im Card-Design

⁶³Weitere Informationen und Beispiele auf webdesigner.com ([A Serious Look At Card Based Design 2014](#))

5.9.2 Authentifizierungs-Lightbox Template

Die Authentifizierungs-Lightbox wird vom Endbenutzer verwendet. Der Endbenutzer kann ein geringes technisches Know-How aufweisen. Deshalb muss das Design einen Bereich verfügbar machen, in welchem die zu tätigen Schritte erklärt werden können. Die Möglichkeiten und Anzahl der Schritte sollen auf einem Minimum gehalten werden. Im besten Fall kann der User eine Eingabe machen und dies mit einem Button bestätigen. Damit der Endbenutzer fokussiert bleibt, soll, wie bei einer Lightbox üblich, der Rest der Seite abgedunkelt werden.



Abbildung 5.12: Mockup Konfigurator Template Mobile

5.9.3 Hinweis zur Zusammenarbeit mit dem Auftraggeber

Die hier abgebildeten Mockups und weitere Ansichten sind das Ergebnis aus den Absprachen mit dem Auftraggeber. Sie sind vom Auftraggeber abgenommen und zur Implementation freigegeben.

5.10 "Du" oder "Sie" – Ansprache

Die Definition, ob der Benutzer im Userinterface mit Du oder Sie angesprochen werden soll, muss laut Jutta Beyer, vorgängig klar geregelt sein.⁶⁴ Eine einheitliche Kommunikation auf der Plattform ist unabdingbar.

5.10.1 Bestehende Vorurteile

Tabelle 5.4: Auflistung von Vorurteilen

Art	Positiv	Negativ
Du	Du steht für - Vertrautheit - Verbundenheit - Modern	Du steht aber auch für - weniger Respekt - weniger Kompetenz - "Stammtischniveau"
Sie	Sie steht für - Respekt - Kompetenz - Seriosität	Sie steht aber auch für - Distanz - Altmodische Einstellungen - Emotionslos

Diese Wahrnehmungen sind nicht stichhaltig noch weniger können die Rückschlüsse stimmen. Dennoch müssen diese Ansichten, zum Teil entstanden aus Kultur und Tradition, ernstgenommen werden, da sie in unseren Köpfen tief verankert sind. Kindern wird beigebracht, dass man Fremde mit "Sie" anspricht. In der Familie, die Geborgenheit und Vertrautheit ausstrahlt, ist das "Du" normal. Gegenüber Lehrern und anderen Autoritätspersonen sollte das Kind aber "Sie" sagen. Also spricht das Kind auch im fortgeschrittenen Alter Erwachsene, vor denen es zugleich Respekt haben sollte, mit "Sie" an.⁶⁵

Eine generelle Aussage zur Verwendung Du oder Sie auf Webseiten kann also nicht gemacht werden. Im Jahre 2011 wurden von statista Personen in Deutschland gefragt, "Wie möchten Sie in Social Media von Unternehmen angesprochen werden?". Dabei möchten 44% der befragten per Sie angesprochen. Einem grossen Teil (43%) ist die Ansprache egal und 13% würden eine Du-Ansprache bevorzugen.⁶⁶

⁶⁴(Beyer 2015)

⁶⁵(Beyer 2015)

⁶⁶(statista 2011)

Entscheidung

Die Authentifizierung, welche vom Endbenutzer durchgeführt wird, darf ruhig sprachlich distanziert und emotionslos wirken. Vielmehr sind Respekt, Kompetenz und Seriosität wichtige Eckpunkte dieses Produkts. Deshalb wird in der Authentifizierung der Endbenutzer, falls nötig, mit Sie angesprochen. Der Konfigurator wird durch den Programmierer administriert. Hier gilt es zu vermitteln, dass der Programmierer sich angenommen und unterstützt in seinem Problemen / Herausforderungen fühlt. Das Produkt soll zeitgemäß und trendig sein. Deshalb wird die Kommunikation über Du geführt. Diese Entscheidung wird durch die Annahme unterstützt, dass unter Programmierern auch in der Wirtschaft mehrheitlich geduzt wird.

5.11 Wahl des Applikation Hosters

5.11.1 Asp.net Shared Hosting

Ein ASP.NET Shared Hosting ist durchaus für komplexere Webapplikationen wie der Authentifizierungsservice ausgerichtet. Die Kosten sind jährlich fix und nicht abhängig von der eigentlichen Nutzung. Überschreitet die Applikation den Speicherbedarf, Zugriffszahlen oder Traffic kann auf ein grösseres Paket gewechselt werden. Ein Wechsel zu einem kleineren Paket ist meist nur jährlich möglich. Die Skalierbarkeit ist stark eingeschränkt. Die Daten können innerhalb der Schweiz gespeichert werden. Der zuständige Systemtechniker ist meist direkt oder indirekt kontaktierbar. Spezielle Konfigurationen am Hosting sind nicht möglich. Die Datacenter sind meist nicht redundant geführt. Fällt das Datacenter aus ist, die Applikation nicht verfügbar.

5.11.2 Cloud Hosting

Die Serverkosten sind direkt von der eigentlichen Nutzung abhängig. Das Hosting ist skalierbar und kann sich automatisiert an die aktuellen Nutzungsbedürfnissen anpassen. Die realen Kosten sind im vornherein schwerer zu definieren. Die Daten sind in der Cloud redundant gehalten. Fällt ein Datacenter aus, kann ein anderes dessen Aufgabe übernehmen. Ein schweizer Anbieter der direkt ASP.NET Webservice als Cloud-Hostingservice anbietet wurde nicht gefunden.⁶⁷ Indirekt z.b. über ein Docker Image könnte auch ein Schweizer Anbieter berücksichtigt werden. Die genutzten Serverdienste können komplett an seine eigenen Bedürfnissen angepasst werden. Beim Cloud Service von Microsoft kann direkt im VisualStudio administriert werden. Alle nötigen Ressourcen können in der Entwicklungsumgebung konfiguriert werden. Ausserdem ist das einfache Publishen (veröffentlichen) der Webanwendung praktisch über einen Knopfdruck aus Visual Studio möglich.

5.11.3 Entscheidung

Die in NFREQ-132 geforderte Skalierbarkeit, nutzungsabhängige Kosten und die Freiheit in der Serverdienst-Konfiguration überwiegen dem Speicherstandort Schweiz. Das einfache Publishen (veröffentlichen) und konfigurieren einer Web-Applikation aus Visual Studio wird bei Microsoft Azure angeboten, was den Development Workflow erheblich unterstützt. Deshalb ist der Authentifizierungsservice im Cloud Hosting zu betreiben.

5.12 Validierung von Benutzereingaben

NFREQ-126 und die Sicherheit des Authentifizierungsservice verlangen eine geeignete Validierung der Benutzereingaben. Um Fehlspeicherungen oder Fehloperationen vorzubeugen, werden alle Daten vorgängig validiert. Die Fehlermeldungen sollen - falls möglich - klar und spezifisch formuliert werden. Bei den Daten-/POCO-Klassen werden die gültigen Wertebereiche mittels Annotationen festgelegt. Microsoft MVC und Microsoft Web-API stellen eine "ModelState.IsValid()"-Methode zur Verfügung, welche das angelieferte Datenobjekt automatisch gegen die Annotationen prüft. Bei MVC-Implementierungen werden mittels Microsoft

⁶⁷Stand 18. Dezember 2015

jQuery Validate Standard Annotationen bereits in der Benutzereingabemaske überprüft. So muss der User bei Falscheingabe nicht zuerst einen manuellen Request auf den Server setzen, sondern wird gleich über die Fehleingabe aufmerksam gemacht. Im Konfigurator, eine AngularJS-App, ist die benutzerseitige Validierung mittels HTML5 Form Validation umgesetzt worden.

5.13 Testing

Die gewählte Architektur und Dependency Injection vereinfachen das Testing.

5.13.1 Wie kann getestet werden?

Der Authentifizierungsservice und die Sicherheitsstufen können wie normale Web-Applikationen in MVC oder Web-API getestet werden. Jedes Sicherheitsstufen-Plugin soll unabhängig eingesetzt getestet werden. Um in Unit-Test keine Datenbank zu nutzen, soll das Repository Pattern eingesetzt werden.

5.13.2 Was soll getestet werden?

Grundsätzlich sollte die Logik, welche im Controller ist, getestet werden. Wird eine spezielle Logik ausserhalb der Controller verwendet, so soll auch diese getestet werden.

5.13.3 Repository Pattern

Wie im Kapitel [Testing](#) beschrieben, sollte eine Möglichkeit geschafft werden, Datenbanken losgelöst zu testen. Dafür wird das Repository-Pattern eingesetzt. Das Repository-Pattern sieht vor, dass jedes POCO-Objekt genau eine Schnittstelle hat, an denen es die CRUD-Operationen ausführen kann. Im Prinzip eine Schnittstelle, die auf alle Anfragen an die Datenbank eine passende Reaktion hat. Diese Schnittstelle oder der Punkt, an welchem Anliegen bearbeitet werden, ist das Repository. Für beinahe jedes Objekt, was persistiert wird.

Definition des Repository-Patterns von Edward Hieatt and Rob Mee: "Vermittler für den Zugriff auf Domänenobjekte zwischen den Domänen- und Daten-Mapping-Schichten mit Hilfe einer Collection-artigen Schnittstelle"

Die Vorteile des Patterns sind zum einen die vereinfachten Unit-Tests. Man kann jedes Repository einfach testen und so auf seine korrekte Funktionalität überprüfen. Zum anderen bieten Repositories eine zentrale Anlaufstelle für Datenbankoperationen. Eine gemeinsame Schnittstelle gegenüber den Datenhaltungs-Schichten. Zudem bietet es einen idealen Punkt, an dem man Mechanismen, wie beispielsweise Caching, implementieren kann.⁶⁸

⁶⁸(Hieatt and Mee 2016)

6 Proof of Concept

Das Ziel der Implementation des Prototyps ist es, zu zeigen, dass das Architekturkonzept auch umsetzbar und sinnvoll ist. Des Weiteren wird dabei die Entscheidung über die Auswahl der geeigneten Technologie überprüft. Außerdem hilft der Prototyp, Probleme im Architekturkonzept zu erkennen und zu beheben.

6.1 Technologien

Der Auftraggeber möchte, dass die aktuell in seinem Betrieb eingesetzten Technologien für die Implementation der Arbeit verwendet werden. Die vorgegebenen Technologien sind im folgenden Kapitel erklärt.

6.1.1 C-Sharp

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

Neben Grundprinzipien der objektorientierten Programmierung resultiert aus folgenden innovativen Sprach-Konstrukten 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-Sharp-Erstellungsprozess ist im Vergleich zu C und C++ einfacher 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-Sharp-Quelldatei kann eine beliebige Anzahl von Klassen, Strukturen, Schnittstellen und Ereignissen definieren. ⁶⁹

⁶⁹(MSDN 2015a)

6.1.2 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, Geschäftslogik 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 ein einfach zu verwendendes und starkes Software Paket zur Verfügung. ASP.NET Web-API 2 basiert auf dem ASP.NET MVC-Framework.⁷⁰

6.1.3 Entity-Framework

Entity-Framework (EF) ist eine objektrelationale Zuordnung, die .NET-Entwicklern über domänenpezifische Objekte die Nutzung relationaler Daten ermöglicht. Ein Grossteil des Datenzugriffscodes, den Entwickler normalerweise programmieren, muss folglich nicht geschrieben werden.⁷¹

6.1.4 Grunt

Grunt.js ist ein sogenannter Taskrunner, d.h. es übernimmt Aufgaben wie das Kompilieren von CSS, überprüft JavaScript auf Fehler und optimiert alle Assets für das Web. Grunt.js zeichnet sich dadurch aus, dass, bei richtiger Konfiguration, die Daten selbst überwacht und bei Änderungen die oben genannten Tasks automatisch ausführt.

6.1.5 AngularJS

Mittels AngularJS ist 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 Programmcode einfacher 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.⁷²

⁷⁰(MSDN 2015a)

⁷¹(MSDN 2015b)

⁷²(Sandeep 2014)

6.1.6 jQuery

jQuery ist die meistverwendete Javascript-Bibliothek. jQuery wird bei 68% aller Webseiten⁷³ eingesetzt. jQuery stellt unter anderem Funktionen zur einfachen DOM-Manipulation, Event-Behandlung und Ajax-Kommunikation zur Verfügung. Entwicklungen von grösseren Javascript Projekten ist mit jQuery einfacher als mit blankem Javascript jedoch zeitintensiver als mit Javascript Frameworks wie AngularJS. Dafür hat jQuery eine höhrere Browserkompatibilität. Die Kompatibilität der Authentifizierung des Endbenutzer ist wichtig um eine grosse Verbreitung zu erreichen. Deshalb wird die Authentifizierung des Endbenutzer mit jQuery umgesetzt.

6.1.7 JSON

Zwischen der AngularJS WebApp und dem Webservice dient JSON (JavaScript Object Notation) als Datenübertragungsformat. JSON zeichnet sich durch seine schlanke Notation und die objektnahe Darstellung aus.

6.1.8 Entwicklungswerkzeuge

Da die Entwicklungssprache C# verwendet wird, liegt es nahe, das Entwicklungswerkzeug VisualStudio einzusetzen. Der Student hat während Studium die JetBrains Entwicklungsplattform PHPStorm kennen gelernt. Daher wird für die Entwicklung der JavaScript-Webapplikationen PHPStorm eingesetzt.

⁷³(*Web Technologies of the Year 2015 2016*)

6.2 Umsetzung Sicherheitsstufe

Aufgrund des eingeschränkten Zeitbudgets werden vier der acht definierten Sicherheitsstufen (Siehe Konzept Kapitel [Sicherheitsstufen integrieren](#)) umgesetzt. Dabei wurden nach Rücksprache mit dem Arbeitgeber, folgende Sicherheitsstufen ausgewählt:

- EMail
- SMS
- Ausweissnummer
- Telefon

6.2.1 Plugin Entwicklung

Die Entwicklung einer Sicherheitstufe wird wie im Konzept unter [Modularität und Erweiterbarkeit](#) vorgesehen, losgelöst und unabhängig entwickelt. Pro Sicherheitstufe werden drei VisualStudio Projekte angelegt. Im Hauptprojekt der Sicherheitstufe wird die klassische Runtime-Umgebung für Webprojekte mit den benötigten Standartreferenzen und Templates für Microsoft MVC und Microsoft Web-API aufgesetzt. Das Plugin kann in diesem Projekt ohne Authentifizierungsservice entwickelt und ausgeführt werden. Das Testprojekt stellt die Lauffähigkeit der im Hauptprojekt entwickelten Implementationen sicher. Um die Entwicklungen aus dem Hauptprojekt als DLL-Klassenbibliothek exportieren zu können, wird das ClassLibrary-Projekt angelegt. In diesem werden die entwickelten Klassen aus dem Hauptprojekt verlinkt. Bei Vorhandensein aller nötigen Referenzen und Verlinkungen erstellt die ClassLibrary bei einem Build die DLL-Klassenbibliothek.

- ▷ EMailSecurityStep
- ▷ EMailSecurityStep.Tests
- ▷ EMailSecurityStepLib

Abbildung 6.1: Screenshot VisualStudio der drei Projekte der Sicherheitsstufe E-Mail

6.2.2 Interface - Vertrag mit den Sicherheitsstufen

Für den Endbenutzer startet der Authentifizierungsprozess mit öffnen der Authentifizierung-Lightbox. Dabei wird die Action “Validate/Check” des Authentifizierungsservice aufgerufen. Diese zentrale Funktionalität überprüft den Status der Verifizierung und ruft die nötigen Sicherheitsstufen auf. Für den Endbenutzer ist der Ablauf der Authentifizierung pro Sicherheitsstufe sichtbar. Der Ablauf und Inhalt der Authentifizierung jeder Sicherheitsstufe kann individuell erstellt werden. Einzig der Startpunkt und Endpunkt wird von Authentifizierungsservice vorgegeben. So muss die Seite bzw. Action “Index” in jeder Sicherheitsstufe für den Start der Authentifizierung der Sicherheitsstufe vorhanden sein. Am Ende der Authentifizierung soll es wieder zurück zur Action “Validate/Check” des Authentifizierungsservice gehen. Damit die Action “Validate/Check” überprüfen kann, ob die Authentifizierung der Sicherheitsstufe erfolgreich war oder zum ersten oder wiederholten mal ausgeführt werden sollte, wird die Methode “checkIsValidated” pro Sicherheitsstufe implementiert. Diese Funktion teilt basierend auf den übergebenen Parameter ProjektID und ProviderID mit, ob die Validierung erfolgreich ist. Das MEF-Contracts Interface aller Sicherheitsstufen enthält ausserdem zwei Methoden zur Abfrage und Speicherung der individuellen Konfiguration der Sicherheitsstufen und die Methode zur Abfrage der Vergleichsparameter.

```
1 Programmcode des Interface ISecurityStepInfo:  
2  
3  
4 public interface ISecurityStepInfo  
5 {  
6     object getConfigParameters(int projectId);  
7     string saveConfigParameters(IDictionary<string, string>  
8         config, int projectId);  
9     bool checkIsValidated(int projectid, string providerid);  
10    SecurityStepCompareInfo getSecurityStepCompareInfo();  
11}  
12  
13 public class SecurityStepCompareInfo  
14 {  
15     public float MultipleParticipation { get; set; }  
16     public float Automation { get; set; }  
17     public float Costs { get; set; }  
18     public float ClientEffort { get; set; }  
19     public float Awareness { get; set; }  
}
```

6.2.3 Visualisierung

Auswahl des Anzeige-Frameworks

Nach Anforderung NFREQ-127 und dem Kapitel [Mockup](#) soll die Authentifizierung-Lightbox responsive umgesetzt werden. Bootstrap unterstützt den Entwickler bei der Visualisierung von Webapplikationen. AngularJS unterstützt seit Anfang an Bootstrap. Mit dem Plugin AngularJS Bootstrap UI stehen erweiterte Bootstrap Funktionalitäten wie Datetime-Picker zur Verfügung. Der Student hat bereits mehrfach Webseiten und Webapplikationen basierend auf Bootstrap umgesetzt. Deshalb fällt die Auswahl auf das mit ihm bekannte Responsive-Framework bootstrap. Neben der responsiven Unterstützung und mit Hilfe des Grid-Systems stehen dem Entwickler umgesetzte Vorlagen für die meistgenutzten Webkomponenten zur Verfügung. Diese können dank zentraler Parametrisierung rasch konfiguriert und individualisiert werden.

Visualisierung von Daten

Um die Umfrageergebnisse visualisieren zu können wird ein Charting-Framework eingesetzt. Die drei bekannten Charting-Frameworks GoogleCharts, ChartJs und D3 wurden verglichen. GoogleCharts und D3 visualisieren in SVG. ChartJs visualisiert in Canvas. Ein eindeutiger Vorteil der beiden Konzepte für den Authentifizierungskonfigurator ist nicht zu nennen. Alle drei Charting-Frameworks können mit AngularJS integriert werden. GoogleCharts und ChartJs bieten fixfertige Direktiven⁷⁴ an. Damit ist die Integration in AngularJS der beiden Frameworks im Gegensatz zu D3 direkt möglich. Alle drei Charting-Frameworks bieten die benötigten Diagramme an. ChartJs hat das kleinste Code-Paket (5KB) und wirkt in den Code deutlich einfacher und aufgeräumter. Visuell passt ChartJs mit den leichten Animationen am besten zum Authentifizierungskonfigurator. Zur Visualisierung wird ChartJs verwendet. Die AngularJS-Direktive, der einfache Code, das kleine Paket und die visuelle Umsetzung führt zu diesem Entscheid.

⁷⁴Angular ermöglicht es, benutzerdefinierte HTML-Elemente und -Attribute, so genannte Direktiven, zu erstellen

6.3 Finale Screens

6.3.1 AngularJS-Konfigurator

Dieses Kapitel zeigt die finalen Screens des Konfigurators, welcher mit AngularJS umgesetzt wurde. Diese Screens sind abgeleitet von den Mockups.⁷⁵

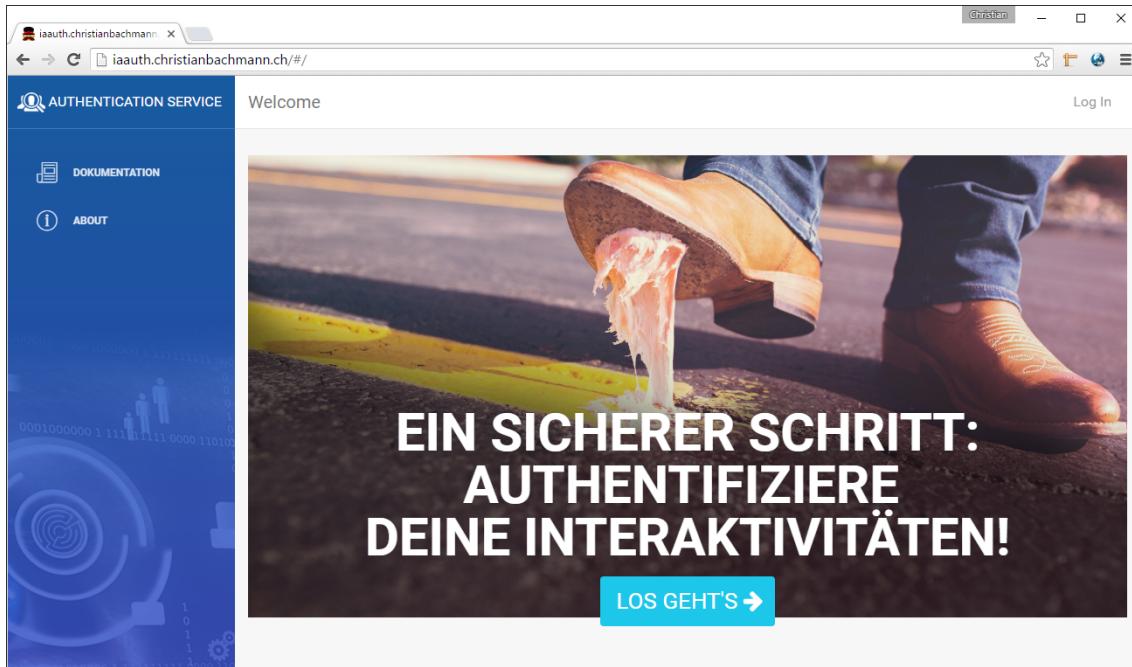


Abbildung 6.2: Startseite und Registration des Konfigurators

⁷⁵Siehe Kapitel Konfigurator Template

Dashboard

Nachdem sich der Programmierer eingeloggt hat, wird ihm das Dashboard mit der Auswahl seiner Projekte dargestellt. Falls der Programmierer noch kein Projekt erfasst hat, wird ihm erklärt, wie er nun vorgehen kann um ein Projekt im Authentifizierungsservice zu erfassen. Der 1. Schritt ist dann gleich über einen Button verlinkt. Andernfalls kann der Programmierer im Dashboard auf einen Blick die Entwicklung der Authentifizierungen pro Projekt wahrnehmen. Dabei wird ihm die verwendete Zeit für seine Authentifizierung , die Anzahl Authentifizierungen des letzten Monats und eine Übersicht über das Verhältnis valider und nicht valider Authentifizierungen dargestellt.

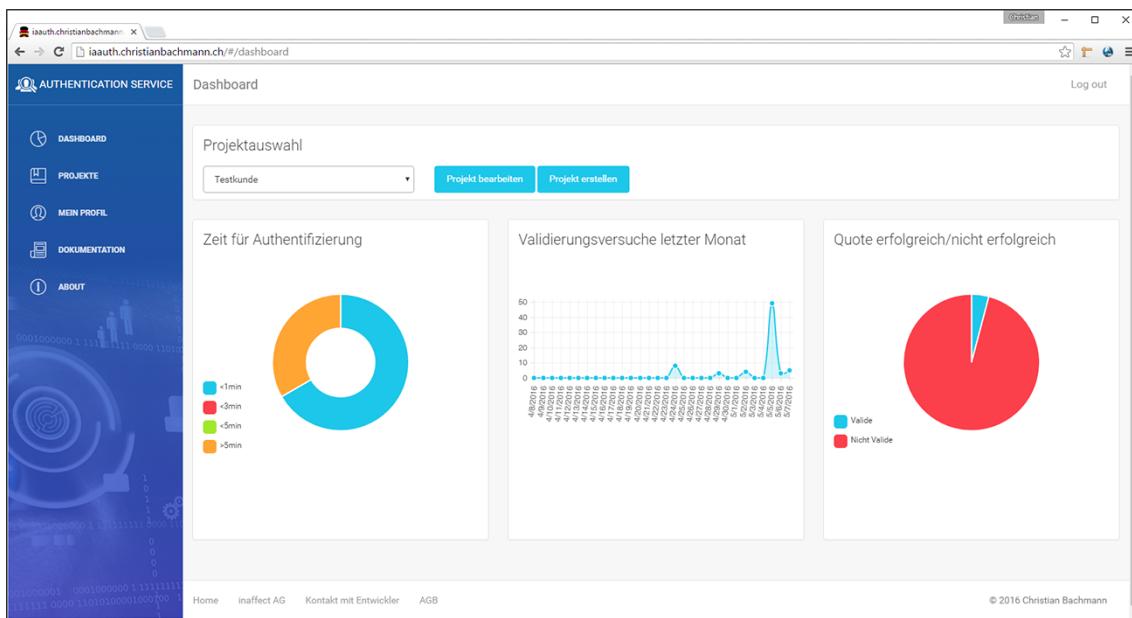


Abbildung 6.3: Dashboard mit Auswertungen der Authentifizierungen

In der Projektdetailansicht kann der Programmierer das Projekt konfigurieren.

Abbildung 6.4: Detailproduktansicht des Konfigurators

Visualisierung der Umfrageresultate

Der Programmierer kann bei der Auswahl der Sicherheitsstufe auf die Bewertungen vom Auftraggeber in affect AG aus dieser Bachelorarbeit zurückgreifen. Die Umfrageergebnisse der Studie werden übersichtlich in zwei Diagrammen zusammengefasst und pro Sicherheitsstufe dargestellt.

Spider

Erklärungen der Begriffe und weitere Informationen findest du [hier](#).



Abbildung 6.5: Screenshot Spider-Diagramm mit Bewertungen vom Auftraggeber

Prozentuelle Akzeptanz des EMailSecuritySteps nach Interaktivitätsart

Erklärungen der Begriffe und weitere Informationen findest du [hier](#).

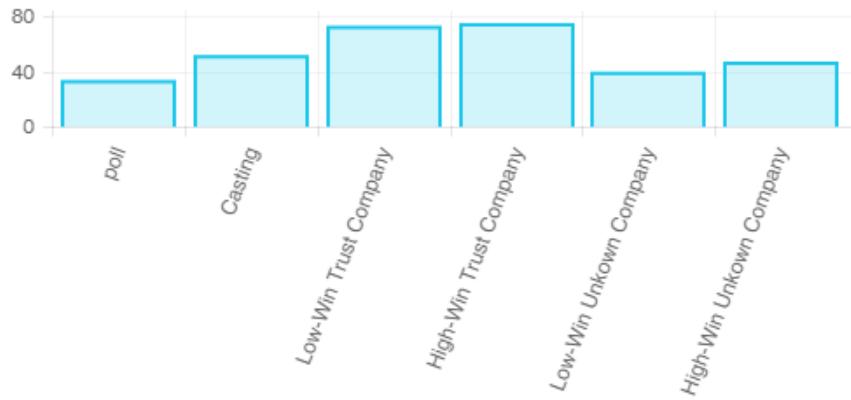


Abbildung 6.6: Screenshot Umfrageergebnisse pro Interaktivität

Prozentuelle Akzeptanz des EMailSecuritySteps nach Interaktivitätsart und Alter

Erklärungen der Begriffe und weitere Informationen findest du [hier](#).

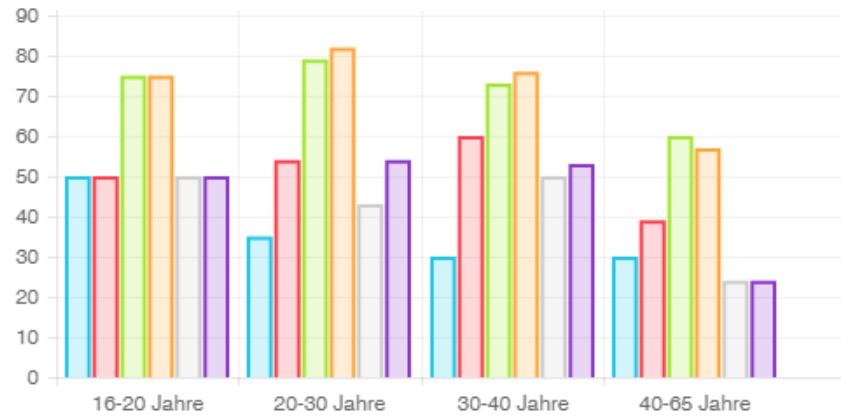


Abbildung 6.7: Screenshot Umfrageergebnisse pro Interaktivität und Alter

6.3.2 Authentifizierungs-Lightbox

Dieses Kapitel zeigt die finalen Screens der Authentifizierungs-Lightbox, welche von den Mockups⁷⁶ abgeleitet wurden. Die Authentifizierungs-Lightbox wurde für den Endbenutzer entworfen. Nach Abschluss der Interaktivität authentifiziert sich der Endbenutzer in der Lightbox. Dabei kommen die im Konfigurator definierten Sicherheitsstufen zum Einsatz.

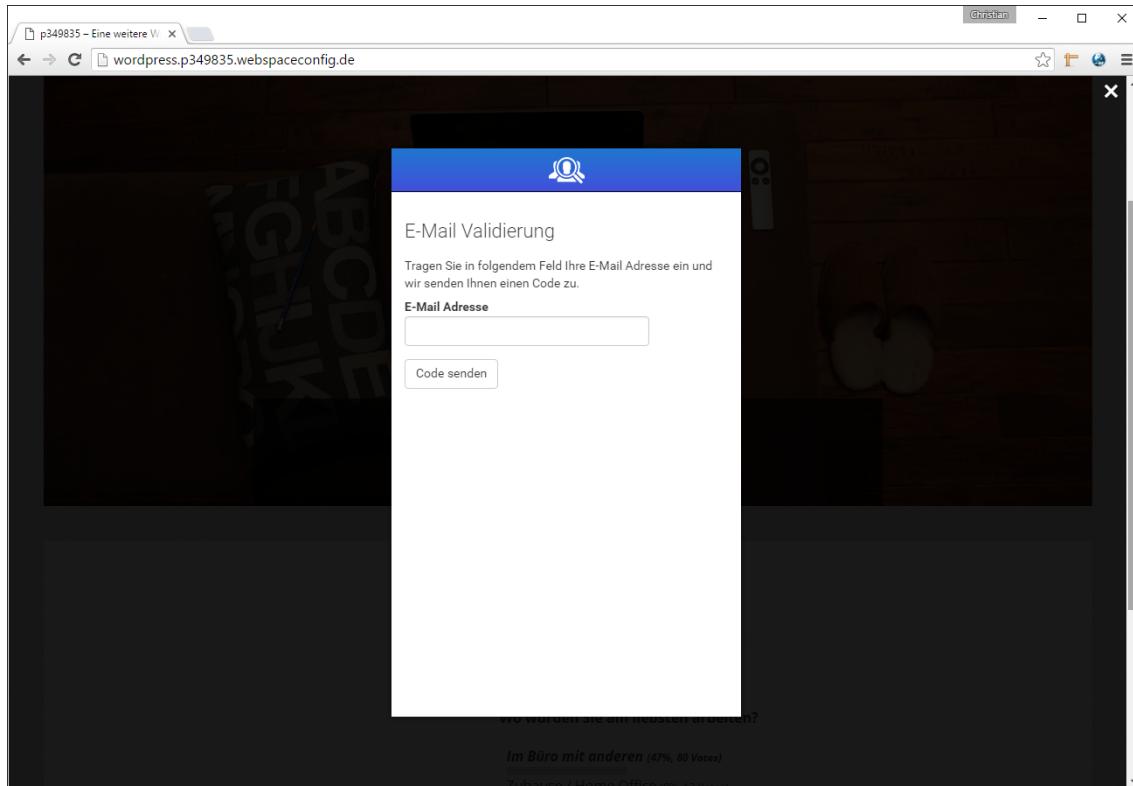


Abbildung 6.8: Desktop-Computer-Ansicht der Authentifizierungs-Lightbox

⁷⁶Siehe Kapitel [Authentifizierungs-Lightbox Template](#)

Der Endbenutzer kann mit verschiedenen Geräten die Authentifizierung durchführen. Auf der folgenden Abbildung sind Screenshots eines iPhone 6s und eines Nexus 5x mit Android 6 abgebildet.

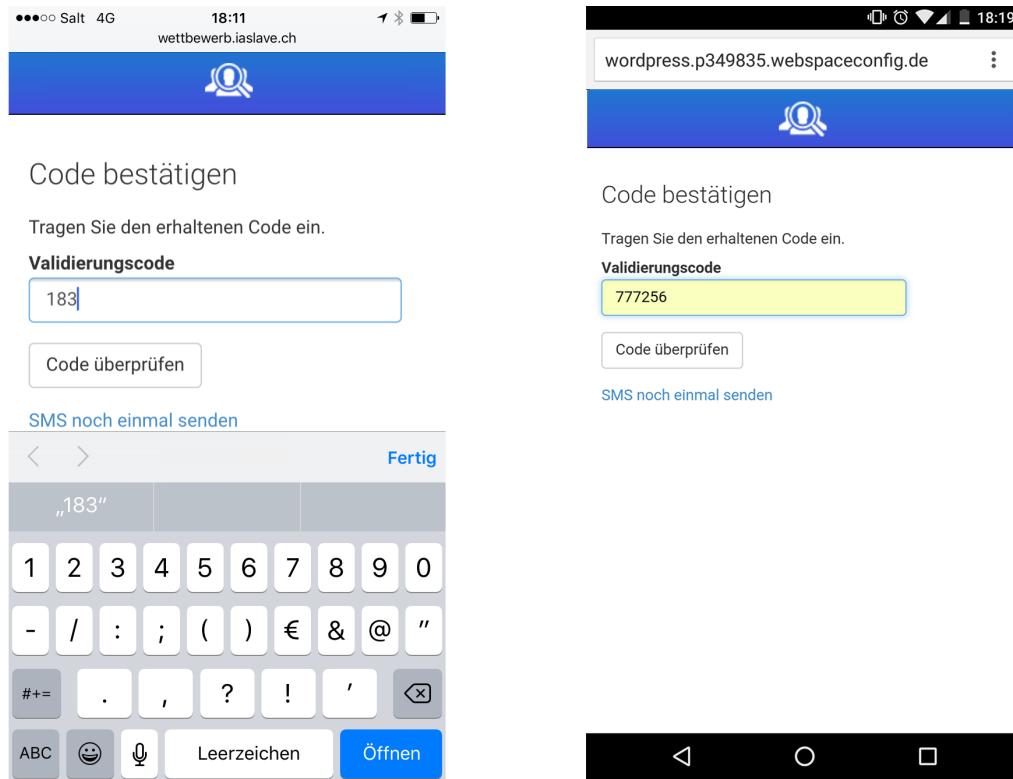


Abbildung 6.9: Mobileansicht der Authentifizierung-Lightbox

6.4 Implementation Authentifizierung

6.4.1 Aufruf der Lightbox

Die Implementation der Authentifizierung ist wie im Kapitel [Integrationskonzept](#) festgelegt, lean umgesetzt worden. Alle CSS-Befehle können von einer Datei abgerufen werden. Die Javascript-Entwicklungen sind in einem File öffentlich verfügbar. Um keine Konflikte mit bereits auf der Webseite implementierten jQuery Bibliotheken zu erhalten wird jQuery nicht im Authentifizierungs-Javascript mitgeliefert.

```
1 <script src="http://iaauth.christianbachmann.ch/include/js/
  jquery-1.12.3.min.js"></script>
2 <script src="http://iaauth.christianbachmann.ch/include/js/
  iaauthlightbox.js"></script>
3 <link type="text/css" rel="stylesheet" href="http://iaauth.
  christianbachmann.ch/include/css/iaauthlightbox.css" />
4
5 <!--OnClick Event on data-iaauthButton was handled by
  iaauthlightbox lity -->
6 <button data-iaauthButton>GO</button>
7 <div id="inline">
8   <form id="iaauthForm" action="https://iaauth.azurewebsites.
  net>Loading/Home/Validate" target="authframe">
9     <input type="hidden" name="projectId" value="30045" />
10    <input type="hidden" name="providerId" value="12" />
11    <!--Generate sign=md5(projectId+providerId+
      validationCode)-->
12    <input type="hidden" name="sign" value="
      b37b3d4cd7cd8cba3f409f07d6f6d9bd" />
13  </form>
14 </div>
```

6.4.2 Gegenprüfung der Authentifizierung

Nach Abschluss der Authentifizierung erhält der User ein Feedback visualisiert. Wie im Kapitel [Schlussspeicherung](#) im Architekturkonzept beschrieben, wird im Hintergrund ein Post auf die vom Programmierer angegebene URL ausgeführt. Als Gegenprüfung steht der Webservice Validate zur Verfügung. Der Webservice wurde implementiert ⁷⁷ und kann mit den Parametern ProjectId und ProviderId konsumiert werden.

6.4.3 Wettbewerbsplattform

Projekte sollen mit verschiedenen Abläufen und auf verschiedenen Devices und Browser getestet werden können. Dafür wurde eine einfache Wettbewerbsplattform entwickelt. Auf dieser kann ein Wettbewerb mit Titel und Text eröffnet werden. Die Wettbewerbsteilnahme soll am Schluss mit dem Authentifizierungsservice authentifiziert werden. Dafür wird im Konfigurator ein neues Projekt angelegt und konfiguriert. Die Parameter ProjectId und Validationcode aus dem Konfigurator werden zu dem erstellten Wettbewerb abgespeichert. Der von der Wettbewerbsplattform generierte Return-Link für die Gegenprüfung wird zum Projekt in der Authentifizierungsplattform eingetragen.

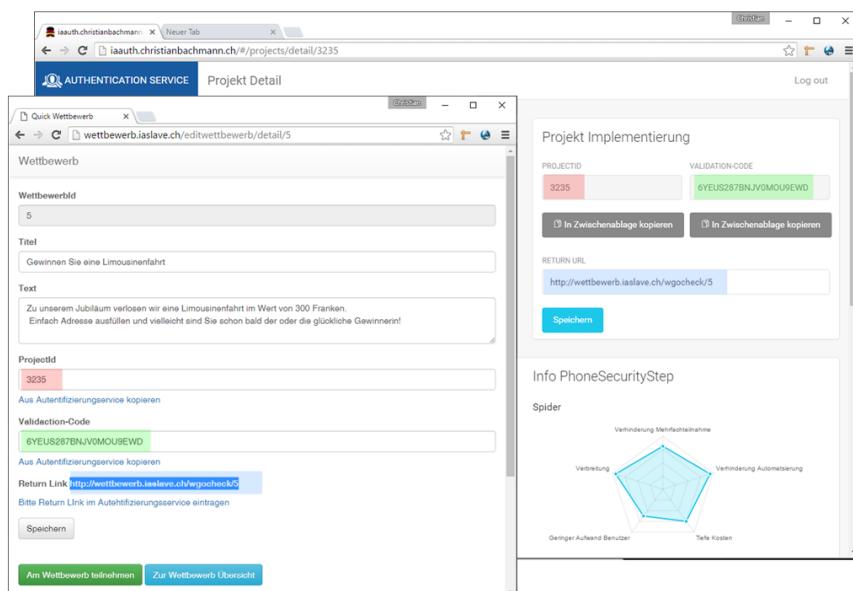


Abbildung 6.10: Screenshot Konfiguration Wettbewerb und Projekt

⁷⁷<http://iaauth.azurewebsites.net/api/Validate>

6.4.4 WordPressPlugIn / Erweiterung WP-Poll

Die Implementation in einem neu erstellten Testprojekt ist erfolgreich. Das umgesetzte Implementationskonzept soll nun auch in einer bestehenden Webapplikation integriert werden. Daher soll das verbreitete Umfrage-Modul WP_Poll aus dem Kapitel [Wordpress-Plugin Hook](#) eine Implementation der Authentifizierung-Lightbox erhalten. Dafür wurde eine neue Wordpress-Installation mit einem Standartlayout aufgesetzt und das PlugIn integriert. Statt den Code hardkodiert zu integrieren, wurde ein eigenes PlugIn entworfen, dass nun mit minimaler Konfiguration wieder verwendet werden kann. Die Integration ist erfolgreich verlaufen und auf dem github Account verlinkt.⁷⁸

⁷⁸<https://github.com/coffeefan/bachelorarbeit>

6.5 Testing

6.5.1 Unit-Test Sicherheitsstufe und Authentifizierungsservice

Die verschiedenen Sicherheitsstufen können unabhängig geprüft werden. Jede Sicherheitstufe hat ein eigenes Testprojekt. Die verschiedenen Testprojekte der Sicherheitsstufen und das Testprojekt des Authentifizierungsservice basieren auf dem Template des Visual Studio 2015 Unit-Test Frameworks. Die Unit-Tests sind direkt im Visual Studio eingebettet.

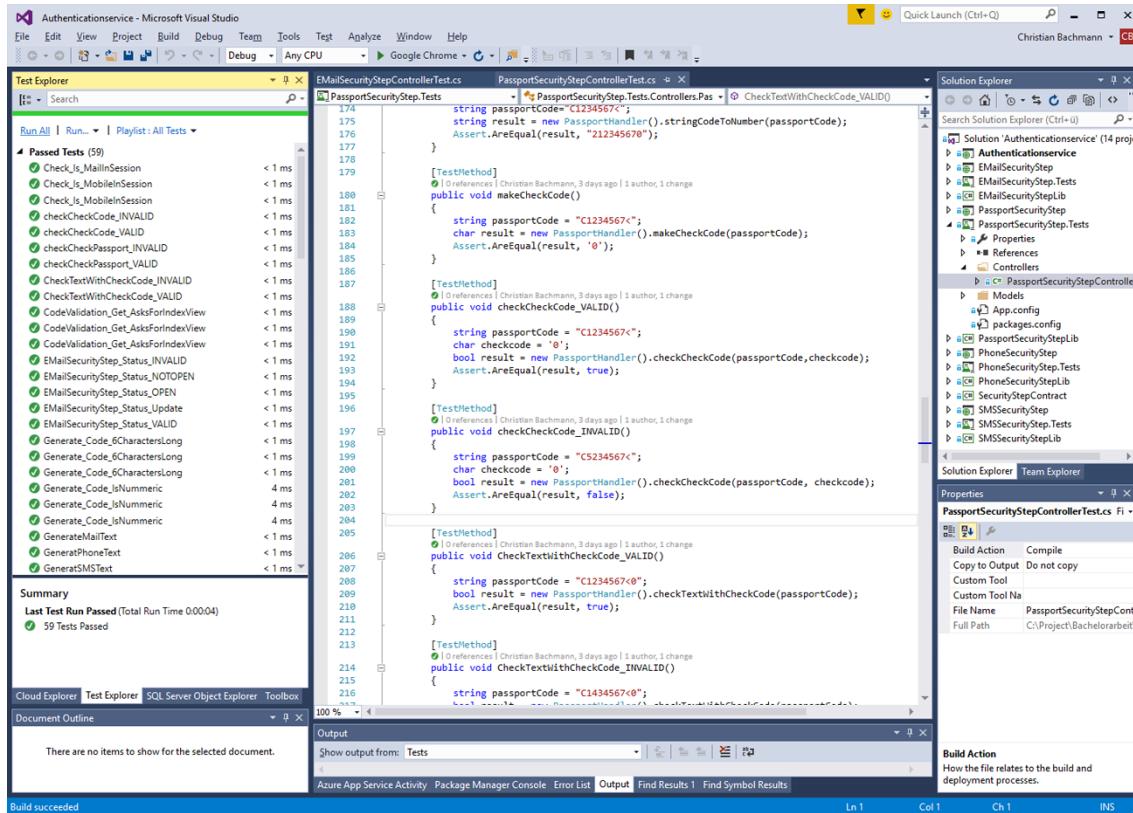


Abbildung 6.11: Screenshot Unit-Test E-Mail Sicherheitsstufe

7 Studie

7.1 Definition der Begriffe aus der Aufgabenstellung

Während den Besprechungen zur Definition der Anforderungen wurde der Begriff "Geschwindigkeit" aus der Aufgabenstellung diskutiert. Der Auftraggeber versteht den Begriff der Geschwindigkeit nicht als objektiv eindeutigen Parameter Zeit, sondern als eine subjektive Wahrnehmung. Dadurch kann nicht wie angenommen, einfach die Zeit, die ein Umfrageteilnehmer zum Anwenden einer Authentifizierung hat, gemessen werden, sondern die Wahrnehmung muss auch erfragt werden. Während der Diskussion wurde der Begriff "Anstrengung" verwendet. Deshalb wird auch die Umfrage auf diesem eindeutigeren Begriff "Anstrengung" aufgebaut.

7.2 Ziel der Studie

Das Ziel ist es, den Programmierer bei der Konfiguration des Authentifizierungsservice mit visualisierten Kennzahlen zu unterstützen. Der Programmierer soll die Akzeptanz der Sicherheitsstufen unter verschiedenen Bedingungen einsehen können und anderseits soll die empfundene Anstrengung der Benutzer für das Authentifizieren pro Sicherheitsstufe visualisiert werden.

7.3 Art der Studie

Wie die Aufgabenstellung und der Auftraggeber fordern, 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.

7.3.1 Vor - und Nachteile schriftlicher Fragebogen

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

- Die Kosten sind geringer. Hippler⁷⁹ definiert den Richtwert von einem Viertel der Kosten zu einer persönlich-mündlichen oder telefonischen Studie.
- Schriftliche Befragungen mit Fragebogen können in einem relativ kurzen Zeitraum realisiert werden.
- Dem zu Befragenden kann eine grössere Anonymität gegeben werden.
- Verteilung in verschiedene Regionen ist einfach und zeitnah möglich. Insbesondere bei Online Umfragen.
- Einfluss von aussen gering. Zahlreiche Studien⁸⁰ belegen, dass Personen welche eine Studie im Gespräch beantworten, sich durch den Interviewer 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 bezweifeln verschiedene Psychologen und Soziologen diesen Umstand. So auch Dr. Reuband in seinem Paper "Möglichkeiten und Probleme des Einsatzes postalischer Befragungen".⁸¹

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 verfehlt. Bei einer schriftlichen Studie kann die Ausfallquote aber nicht im Vornherein eingeschätzt werden.
- 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 Bevölkerungssteile werden durch diese Art der Studie ausgeschlossen. Zum Beispiel Analphabeten oder bei Onlineumfragen Personen mit zu wenig technischem Know-How oder Hardware.

⁷⁹(Hippler 1988)

⁸⁰Studien und Erklärungen zu Fremdbestimmung durch François Höpflinger(Höpflinger 2011)

⁸¹(Reuband 2001)

7.3.2 Findings

Es gilt also die Vorteile der schriftlichen Fragebogen bei der Gestaltung der Studie zu nutzen. Der ausgeschlossene Bevölkerungsteil verfälscht das Ergebniss nicht, da die Zielgruppe für die Umfrage nur gerade die Personen sind, welche auch tatsächlich an einer Onlineumfrage teilnehmen können. Die Nonresponse-Rate ist ein Risiko, dem Rechnung getragen werden muss, um nicht eine ungültige Studie zu erhalten. Damit die Problematik Nonresponse-Rate gering gehalten werden kann und eine geeignete Umgebung für die Datenerhebungssituation vorhanden ist, gilt es, weiter den korrekten Aufbau einer Studie zu recherchieren.

7.3.3 Webapplikation für Umfrage

Basierend auf den Empfehlungen⁸² der Universität St. Gallen und der Universität Freiburg wurde das Schweizer Unternehmen enuvo GmbH mit ihrer Webapplikation umfrageonline.ch ausgewählt. Umfrageonline stellt Studenten den Funktionsumfang für ihre Studien nach Autorisierung kostenlos zur Verfügung.

7.4 Aufbau Gesamtkonzept

“Ein Fragebogen soll als Gesamtkonzept (Einleitung, Hauptteil, Endteil, Design, Aufmachung) betrachtet werden, in dem die Reihenfolge und die Struktur der Frage wichtige Einflussfaktoren zur Erlangung korrekter Daten sind”⁸³

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

7.4.1 Einleitung

Die Einleitung soll die Befragten motivieren an der Studie teilzunehmen und allgemeine Hinweise zur Studie zu geben. Die folgenden Fragen wurden durch das Institut für webbasierte Kommunikation und E-Learning zusammengetragen⁸⁴ und für die Studie dieser Bachelorarbeit beantwortet:

Wer wird befragt?

Mit Absprache des Auftraggebers soll die Zielgruppe deutsch sprechende Schweizer oder Personen sein, welche in der Schweiz wohnen und zwischen 16 und 65 Jahre alt sind. Die Angabe begründete der Auftraggeber dadurch, dass sich darin die Hauptzielgruppen seiner Kunden wiederspiegeln. Die Teilnehmer sollen das technische Know-How besitzen, um an einer Interaktivität teilnehmen zu können und Internetzugriff haben. Dieses minimale technische Know-How werden sie beweisen, indem sie an der Umfrage auf umfrageonline.ch teilnehmen können.

⁸² Die Universitäten sind offizielle Kunden von umfrageonline.ch

⁸³ Zitat vom Institut für webbasierte Kommunikation und E-Learning und Gräf et al. 2001 (Pratzner 2001)

⁸⁴ Zitat vom Institut für webbasierte Kommunikation und E-Learning und Gräf et al. 2001 (Pratzner 2001)

Was ist der Zweck bzw. das Ziel der Untersuchung?

Die Studie dient dem Programmierern zur richtigen Konfiguration 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 Veröffentlichung der Ergebnisse kann besonders Vertrauen und Wohlwollen gewonnen werden⁸⁵. Deshalb soll das Kapitel Studie der Bachelorarbeit auf Wunsch den Befragten per E-Mail zugesendet werden.

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 benötigten Zeit und Anzahl der Fragen sollten zur Beginn der Studie genannt werden. Aus der Studie von Bosnjak und Batini⁸⁶ ergebt sich die Erkenntnis, dass nicht nur unter dem Motto "Je kürzer desto besser" gehandelt werden sollte. Die Studie besagt, dass die Mehrzahl mindestens 10 Minuten in eine Studie investieren würden, da kurze Studien weniger bedeutsam sind. Die Studie ist jedoch schon 15 Jahren alt und ist deshalb differenzierter zu sehen. Die Studie dieser Bachelorarbeit strebt einen Aufwand von 8-12 Minuten an.

⁸⁵(Pratzner 2001)

⁸⁶(Bosnjak 2000)

7.5 Hauptteil/Fragen

7.5.1 Erste Frage Theorie

Die erste Frage ist nach Dillman⁸⁷ von grosser Bedeutung. Mit ihr wird Motivation und Einsatz für den ganzen Fragebogen gesetzt. Diese Frage soll 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 getragen⁸⁸:

- **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 sollen abgebaut werden.

- **Inhaltlich einführen**

Die Frage soll in das Thema einführen und im Idealfall Interesse und Neugier wecken

- **Keine Fragen zur Person oder zur ihren demographischen Eigenschaften**

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

7.6 Erste Frage

Die 1. Frage der Studie dieser Bachelorarbeit:

Hatten Sie schon einmal das Gefühl, dass an einem Onlinewettbewerb gemogelt werden kann?

0 Ja 0 Nein

⁸⁷(Dillman 1978)

⁸⁸(Pratzner 2001)

7.7 Theorie Fragen

Fragen sollen eine Funktion übernehmen. Dabei schlägt Kleber⁸⁹ 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 drei Hauptgruppen gibt es:

- Einstellungsfragen

Dieser Fragestellung bezieht sich auf "Wunschbarkeit" oder negativer Beurteilung, die 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

- Eigenschaftsfragen

Diese Fragestellung fragt nach den Eigenschaften von Personen. Vielfach sind es persönliche und demographische Daten.

Fragearten

Die Fragen können generell in zwei Typen unterteilt werden:

Offene Frage

Der Aufwand bei der Auswertung ist sehr hoch. Ungeübte Teilnehmer können unverwertbare Antworten niederschreiben. Antworten sind schwer vergleichbar, Dafür kann sich der Teilnehmer so ausdrücken, wie er möchte. Er wird nicht durch vorgegebene Antworten beeinflusst.

Geschlossene Frage

Die geschlossene Frage kann leicht ausgewertet werden. Die Gefahr besteht, dass der Teilnehmer ratet und durch die Antworten beeinflusst wird. Der Vorbereitungsaufwand für diese Frage ist hoch. Auswahlmöglichkeiten für die Antwort könnten irrelevant sein.

⁸⁹(Hippler 1992)

7.8 Fragen über Akzeptanz

Es wird folgende Hypothese verfolgt: "Die Akzeptanz von Sicherheitsstufen ist nicht beständig. Sie ist abhängig von den Bedienungen der Interaktivität: Seriosität des Anbieters, Wichtigkeit der Umfrage und möglicher Verdienste bei der Teilnahme" Der Programmierer soll bei der Konfiguration das Umfeld der Interaktivität kategorisieren können. Die Hauptbereiche sind aus der Aufgabenstellung entnommen. Die anderen Kategorisierungen ergeben sich aus der Absprache mit dem Arbeitgeber.

- Voting
 - einfache
 - Casting
- Wettbewerb
 - Seriöse Firma
 - * Gewinn unter 200 Franken
 - * Gewinn über 200 Franken
 - Unbekannte Firma
 - * Gewinn unter 200 Franken
 - * Gewinn über 200 Franken

Aus jeder Kategorie wird in der Studie erfragt, welche Sicherheitsstufen der Umfrageteilnehmer einsetzen würde. Es wird pro Kategorie eine geschlossene Frage gestellt. Der Fragetyp ist Mehrfachauswahl. Die Fragen sind von der Klassifizierung her Verhaltensfragen. Es wird abgeklärt, unter welchen Bedienungen sich der User so verhält, dass er die Sicherheitsstufe akzeptiert. Der User kann pro Kategorie die Sicherheitsstufen auswählen, welche er bereit ist zu verwenden.

Ein vertrauenswürdiges Unternehmen, wie das Schweizer Fernsehen, Züri Versicherung oder die SBB verlost Preise im Wert von mehr als 200 Franken. Was wären Sie bereit auszufüllen, damit am Wettbewerb nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angebenden Webseite übertragen
- Pass- oder ID-Nummer eintragen

Abbildung 7.1: Screenshot einer Akzeptanzfrage

7.9 Frage Anstrengung

Die verschiedenen Sicherheitsstufen sollen für den User direkt vergleichbar beantwortet werden können. Dafür eignet sich eine geschlossene Frage vom Type Bewertungsmatrix. Es wurden fünf Abstufungen zur Einschätzung der Anstrengung definiert. Außerdem kann der User bei Unsicherheit keine Antwort geben. Diese Frage ist eine Einstellungsfrage. Der User bewertet seine Einstellung zu den Sicherheitsstufe anhand der Anstrengung.

Wie anstrengend finden Sie die folgenden Authentifizierungstypen? *



Abbildung 7.2: Screenshot der Umfrage zur Anstrengung

7.10 “Bonus Frage”

Umfrageonline.ch enthält die Sicherheitsstufe Cookie und IP-Adresse. Wobei die Sicherheitsstufe IP-Adresse standardmäßig deaktiviert ist. Diese beiden Sicherheitsstufen, erlauben es, wie mehrfach in dieser Bachelorarbeit dokumentiert, mehrmals an einer Umfrage teilzunehmen. Die Hypothese wird aufgestellt, dass ein Teilnehmer mit genügend technischem Know-How insbesondere bei diesem Umfragethema mehrfach teilnehmen wird.

7.11 Weitere Fragen

Weiter werden die drei Eigenschaftsfragen gestellt. Dabei sollten Alter, Geschlecht und ob es sich um einen Schweizer oder Bewohner der Schweiz handelt, angegeben werden.

7.12 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 Befragte dem Untersuchter Hinweise zukommen lassen, die für die Auswertung und weitere Untersuchungen dienlich sind. Dieser Möglichkeit wird nach der Erfahrung von Reuband⁹⁰ gewürdigt.

7.13 Verständlichkeit

Als der Umfragebogen Personen mit geringem technischem Know-How vorgelegt wurde, wurde klar, dass die genannten Authentifizierungsmethoden nicht bekannt sind. Selbst der Begriff Authentifizieren konnte nicht erklärt werden. Deshalb wurden die zu analysierenden Methoden erklärt und illustriert.



Abbildung 7.3: Beispiele der Illustrationen für die Umfrage

7.14 Auswertung

Die Umfragedaten werden in den entworfenen Authentifizierungsservice eingespielt. Jeder Programmierer kann während dem Konfigurieren seiner Sicherheitsstufe die gewünschten Diagramme zusammenstellen. Anhand der visualisierten Daten kann er die Meinung seiner Enduser einschätzen und für diese seine Konfigurationen optimaler wählen. Damit ist das Ziel der Studie und die Möglichkeit der Auswertung erreicht.

Weiter werden noch einige Anmerkungen zu den Fragen erläutert.

⁹⁰(Reuband 2001)

7.14.1 Repräsentativität

Laut Bundesamt für Statistik enthält die definierte Zielgruppe 3.3 Millionen Personen⁹¹. Diese Zahl beinhaltet die Deutschen, welche zwischen 16 und 65 Jahre alt sind. An der Umfrage habe 176 Personen teilgenommen. Mit Hilfe der Berechnungsformel für Stichprobengröße lässt sich die Variable d, das Konfidenzintervall von 7,4% errechnen.

$$n = \frac{\frac{t^2 * p * q}{d^2}}{1 + \frac{1}{N} * \left(\frac{t^2 * p * q}{d^2} - 1 \right)}$$

Abbildung 7.4: Berechnungsformel für Stichprobengröße

n= Stichprobengröße=176 Umfrageteilnehmer

N= Grundgesamtheit = 3.3 Millionen Menschen in der Zielgruppe

p= Stichprobenanteil bei Normalverteilung

q= 1-p (Vereinfachte Darstellung)

t= Normalverteilungsnormierung 1,96 = 95% Trefferquote

d= Gesuchter Wert, das Konfidenzintervalls Fehlertoleranzwert= 7,4%

7.14.2 Gemogelt an Wettbewerben

Über 65% der Befragten gehen davon aus, dass sie noch nie an einem Wettbewerb teilnommen haben, an welchem gemogelt wurde. Bei den 40-65 jährigen sind es sogar über 83 Prozent. Die Einstiegsfrage, welche zur Einführung ins Thema gedacht ist, zeigt überraschend ein hohes Vertrauen in Onlinewettbewerbe.

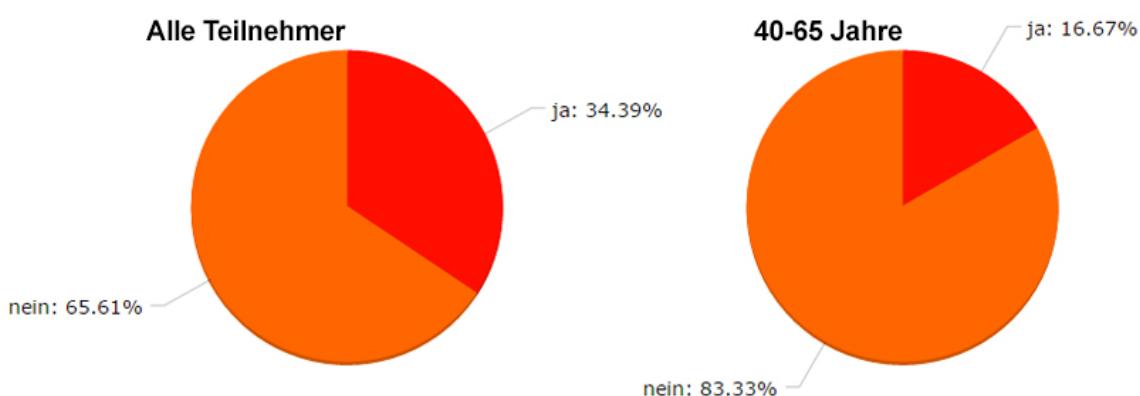


Abbildung 7.5: Ergebnisse Frage zu mogeln an Onlinewettbewerben

⁹¹(Statistik 2015)

7.14.3 “Bonus Frage”

Drei Umfrageteilnehmer konnten mit den zur Verfügung stehenden technischen Mittel als Mehrfachteilnahme registriert werden. Die Bonusfrage wurde wie angenommen gelöst. Die Thematik der Umfrage bewegte die Teilnehmer offensichtlich zum Ausprobieren. Ein Teilnehmer brauchte nach Ende seiner 1. Teilnahme genau 17 Sekunden, bis er erneut mit der Umfrage starten konnte.

7.15 Anstrengung

Auf einer fünfstufigen Skala sind die Sicherheitsstufen nach Anstrengung bewertet: 1 Punkt für sehr anstrengend, 5 Punkte für sehr angenehm. Anhand dieser Punkte konnte nun ein arithmetisches Mittel errechnet werden. Das Empfinden der Anstrengung ist bei allen Teilnehmer ähnlich feststellbar und mit einer Standardabweichung von 0.85 bis 1.1 Punkte festgelegt. Dabei ist feststellbar, dass unser Authentifizierungsservice Sicherheitsstufen mit angenehmem empfinden bis Sicherheitsstufen mit sehr anstrengendem Empfinden zur Verfügung stellt. Die gewünschte Breite des Arbeitgebers konnte auch in diesem Aspekt gefunden werden.

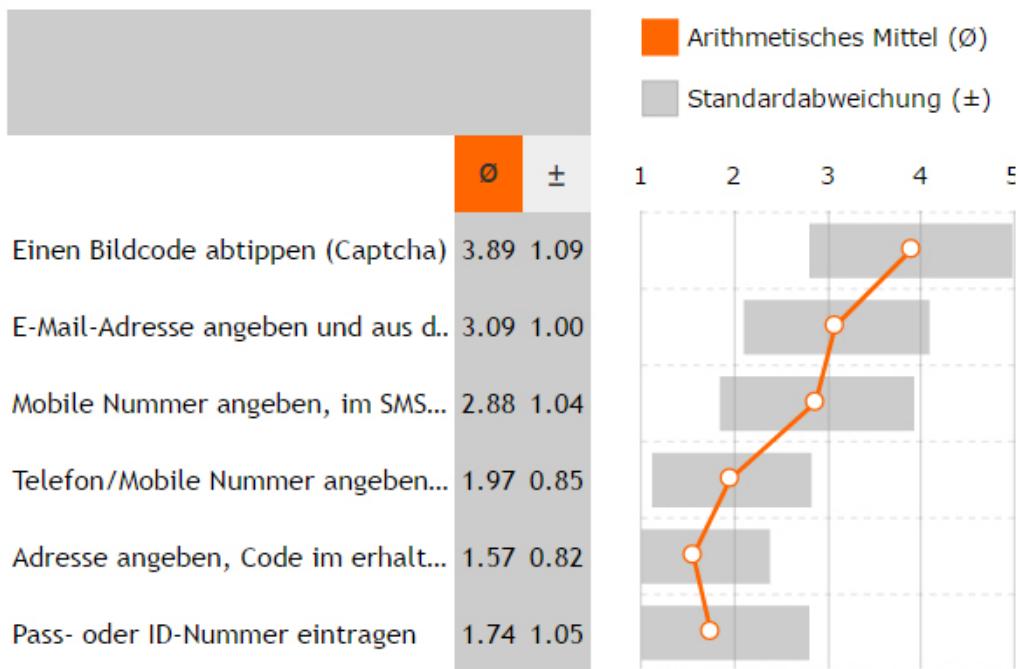


Abbildung 7.6: Übersicht der Ergebnisse zur Umfrage der Anstrengung mit Arithmetischem Mittel und Standardabweichung

7.16 Akzeptanz

Die Hypothese, dass sich die Akzeptanz zum Einsatz von Sicherheitsstufen mit Seriosität des Anbieters, Wichtigkeit und möglichen Verdienst verändert, zeigt das Umfrageergebnis in allen Altersstufen. Interessant ist, dass die Akzeptanz von einem automatischen Telefonanruf geringer ist, als die Akzeptanz einer SMS von einer Mobilenummer. Diese Erkenntnis kann auf alle Fragen angewendet werden, ist also unabhängig von Bedienungen der Interaktivitäten. Die Angabe seiner eigenen Mobilenummer wird dem mühsamen Abtippen des Anrufes auf ein mögliches Fixnetztelefon vorgezogen. Der Pass oder die ID-Nummer wird nur bei einem vertrauenswürdigen Unternehmen angegeben. Der zu erhoffende Gewinn hat keinen bedeutenden Einfluss. Bei unbekannten Unternehmen als Anbietern, würde die grosse Mehrheit der Teilnehmer ausser Captcha und E-Mail-Adresse, keine Sicherheitsstufe verwenden. Keine andere Sicherheitsstufe konnte bei diesem Anbieter bei mehr als einem 1/5 der Teilnehmer Akzeptanz erhalten. Der grosse Unterschied bei den Ergebnissen macht nicht der mögliche Verdienst oder die Wichtigkeit des Resultats. Vielmehr ist es der Anbieter und das Vertrauen, das der Endbenutzer in diesem hat.

8 Fazit

8.1 Ausblick

Der erstellte Prototyp wird nun dem Auftraggeber, der Firma inaffect AG, übergeben. In der Übergabephase werden entstandene Änderungs- und Erweiterungswünsche umgesetzt. Das erste Projekt, welches bei erfolgreicher Betaphase den Authentifizierungsservice verwenden soll, ist eine Netzwerk-Eventveranstaltungsreihe mit Aufschaltungsdatum in drei Monaten.

Einen Verkauf an oder Lizenzierung mit einem grösseren Medienunternehmen wäre möglich. Ein grösseres Medienunternehmen möchte vielfach alles inhouse betreiben. Diesem Wunsch entspricht das Konzept des Authentifizierungsservice. Der Service kann auch auf jedem besseren IIS-Server, auf welchem Microsoft-MVC und Web-API ausführbar und eine SQL-Datenbank installiert ist, betrieben werden. Die ausgelagerten Konfigurationsdateien und Views erlauben es, die Authentifizierung ohne neue Kompilierung der Logik den optischen und inhaltlichen Ansprüchen anzupassen.

Es konnte gezeigt werden, dass es möglich ist, mit verschiedenen Sicherheitsstufen eine genügend eindeutige Authentifizierung zu erreichen, jedoch ist dies immer mit Bekanntgabe von persönlichen Daten verbunden. Die Angst, dass diese Daten missbraucht werden, ist hoch. Dies wurde mehrfach ungefragt in den Bemerkungen der Studienumfrage erwähnt. Ein Lösungsansatz wäre, für Authentifizierungen wie bei Onlinezahlungen ein vertrauliches Gateway zu schaffen. Diese Bachelorarbeit beschreibt genau dieses Gateway als Konzept. Nun müsste nur noch eine Firma den Schritt wagen, dieses Konzept als Produkt zu vermarkten und es dem Endkunden bekannt zu machen.

8.2 Offene Fragen

Q1 Wie soll das Konzept als Produkt einem breiten Publikum bekannt gemacht werden?

Q2 Wie kann dem Publikum hinreichend Sicherheit für das Konzept vermittelt werden? Q2 Wie skaliert das System bei gleichzeitiger Nutzung von über 500 Endbenutzern?

8.3 Limitationen

Im Prototyp sind vier Sicherheitsstufen implementiert worden. Für eine grössere Konfigurationswahl sollen weitere Sicherheitsstufen integriert werden. Der Authentifizierungsservice verrechnet die Kosten noch nicht selbständig an den Programmierer weiter. Hier sollte ein geeignetes Preismodell definiert und eine automatisierte Abrechnung implementiert werden. Das Produkt ist für die Deutschschweiz entwickelt worden. Auch wenn Multilingualität keine Anforderung war, wurde sie angedacht und in grossen Teilen des Prototyps implementiert. Für den multilingualen Betrieb müssten insbesondere Textbausteine für andere Sprachgebiete entworfen werden und in den fehlenden Teilen die Multilingualität implementiert werden.

8.4 Validation

Die erarbeiteten Konzepte haben im Prototyp funktioniert. Nachfolgend wird die Erfüllung der Aufgabenstellung überprüft.

Bereich	Beschreibung	Status	Verweise
Recherche	Wurde eine Marktanalyse bestehender Produkte recherchiert und dokumentiert? Wurden verschiedene Sicherheitsstufen (Arten und Methoden der Sicherheits- und Identitätsüberprüfung) recherchiert und dokumentiert?	erfüllt	Marktanalyse
Analyse	Wurden die Anforderungen der Authentifizierungsschnittstelle mit dem Arbeitgeber analysiert und dokumentiert?	erfüllt	Anforderungen
Konzept	Wurde die Evaluation von geeigneten Authentifizierungsmethoden für verschiedene Stufen dokumentiert? Wurden eine Spezifikation einer Prototypenapplikation für die Authentifizierungsschnittstelle entworfen und dokumentiert? Wurde eine Spezifikation einer Prototypenapplikation für das Verwalten der Authentifizierungsschnittstelle entworfen und dokumentiert? Wurde die Software-Architektur der Authentifizierungsschnittstelle und dessen Verwaltung konzeptioniert?	erfüllt erfüllt erfüllt	Sicherheitsstufen integrieren, Sicherheitsstufen bewerten Konzept
Studie	Wurde eine Studie über Akzeptanz und Geschwindigkeit(Anstrengung) von Authentifizierungsmethoden ausgearbeitet? Wurde die Durchführung der Studie dokumentiert? Wurde die Auswertung dokumentiert und im Prototyp integriert?	erfüllt erfüllt erfüllt	Studie Anhang Studie Studie Auswertung, Visualisierung der Umfrageergebnisse
Proof of Concept	Wurden die Prototypen der Authentifizierungsschnittstelle und der Verwaltung entwickelt?	erfüllt	Proof of Concept, AngularJS-Konfigurator, Authentifizierungs-Lightbox

Bereich	Beschreibung	Status	Verweise
	Wurden die Studienresultate im Prototypen integriert?	erfüllt	Visualisierung von Daten , Visualisierung der Umfrage resultate
Fazit	Wurde das Fazit dokumentiert?	erfüllt	Fazit

8.5 Schlusswort

Bei der Erarbeitung dieser Bachelorarbeit konnte ich mich intensiv mit AngularJS und den Microsoft Web-Technologien auseinandersetzen. Insbesondere die Implementierung der Plugin-Architektur für die Sicherheitsstufen forderte die Erarbeitung eines tiefen Wissens der Core-Entwicklung von .Net Web -PI und MVC. Bei Ladungen des Plugins zur Laufzeit mussten Methoden gefunden werden, um kein Memoryleak zu generieren. Dadurch konnten tieferen Einblick in die Techniken und Standards gewonnen werden. Im Zusammenhang mit den Sicherheitsstufen-Plugins war die Definition des geeigneten Interfaces eine konzeptionelle Herausforderung. Einerseits sollte die Definition möglichst flexibel sein um jegliche Arten von Sicherheitsstufen einzubinden. Andererseits sollten doch klare Richtlinien geschaffen werden, um nicht unnötig mehrfach den gleichen Code schreiben oder mit komplexen Algorithmen die Daten prüfen zu müssen.

Ich konnte im Verlauf des Projekts alle gesetzten Ziele erreichen.(Siehe Kapitel [Validation](#)). Die Bachelorarbeit hatte viele verschiedene Komponenten, welche ineinander spielen mussten. Die breite Abstützung des gewählten Themas, sowie die Terminplanung dieser Arbeit war durchaus gewagt. Doch gerade diese Freiheit ermöglichte es mir, tief in das Themengebiet vorzustossen. Der klare Projektplan verhalf mir dabei immer wieder fokussiert zu arbeiten. Das Vorgehen der Anforderungsanalyse habe ich in Anlehnung an das Modul "Software Engineering" und basierend auf dem Buch "Basiswissen Requirements Engineering" umgesetzt. Rückblickend bin ich überrascht, dass sich in dieser Zeit so viel Unklares und Unausgesprochenes basierend auf diesem Muster herausfinden liess. Dieses Vorgehensmuster werde ich deshalb auch in Zukunft versuchen einzusetzen.

Bei der Studie hat mich überrascht, dass so viele Personen davon ausgehen, dass Sie noch nie an einer Umfrage teilgenommen haben, an welcher gemogelt hätte werden können.

Mit dem Resultat meiner Arbeit bin ich sehr zufrieden. Nicht nur durfte ich durch das Erarbeiten der Studie Einiges lernen, sondern ich konnte auch einen funktionsfähigen Prototypen zur Lösung der Problematik für den Arbeitgeber entwickeln. Es hat mir viel Spass bereitet, neue Technologien und Lösungsansätze zu erkunden.

A Anhang

A.1 Glossar

2FA

2FA bedeutet Zwei-Faktor-Authentifizierung. Weitere Infos im Kapitel [Authentifizierungskomponenten](#)

API

API steht für Application Programming Interface und beschreibt eine Schnittstelle, über welche ein Client Daten vom Server abrufen kann.

Browser

Webbrowser oder allgemein auch Browser sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web. Webbrowser stellen die Benutzeroberfläche für Webanwendungen dar.

Github

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

CRUD-Operationen

CRUD steht für Create, Read, Update, Delete. Diese vier Operationen sind die Grundlage für alle Interaktionen mit der Datenbank.

Non-Response

Nichtbeantwortung einer oder mehrerer Fragen. Die Repräsentativität einer Befragung hängt stark von der Rücklaufquote ab, 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 können.

POCO POCO Klassen

POCO ist die Abkürzung für Plain Old CLR Object. Eine POCO-Klasse ist ein ganz normales .NET-Objekt, das keine durch die Infrastruktur bedingte Basisklasse, Annotationen oder eine Enhancement auf Bytecode-Ebene (MSIL/CIL) erfordert. Damit ist es geeignet schlank Daten zu transportieren.

REST / Restfull

REST steht für Representational State Transfer. REST ist eine Software-Architektur des Webs. Systeme 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 Web-Ressource.

Sicherheitsstufe

Das Wort Sicherheitsstufe ist eine domänenspezifische Beschreibung eines einzelnen Authentifizierungsvorgangs auch Authentifizierungsart genannt.

A.2 Verzeichnisse

A.2.1 Abbildungsverzeichnis

2.1 Projektplan der Bachelorarbeit	6
3.1 Aktive Nutzer weltweit und in der Schweiz	15
3.2 Beispiel der maschinenlesbaren Zone einer Identitätskarte und eines Passes	21
3.3 Beispiele von Captchas <i>Quelle:drupal.org</i>	23
3.4 Fingerabdruck: Mit Kohlepulver werden Fingerabdrücke sichtbar gemacht und auf Klebefolie gesichert. <i>Quelle:phi-hannover.de</i>	28
4.1 Use-Case Diagram	32
4.2 Basis Schablone <i>Quelle Rupp</i>	37
4.3 Erweiterte Schablone <i>Quelle Rupp</i>	37
4.4 Risikomatrix	46
5.1 Übersicht der Hauptkomponenten	49
5.2 Sequenzdiagramm Ablauf der Authentifizierung	50
5.3 Differenziertes Domänenmodell des Authentifizierungsservice	51
5.4 Nutzungsanteil CMS weltweit <i>Quelle:de.statista.com</i>	53
5.5 Datatrans Lightbox Integration <i>Quelle:datatrans</i>	57
5.6 Vereinfachte Architektur des Managed Extensibility Framework <i>Quelle: msdn.microsoft.com</i>	64
5.7 UML Library Overview	65
5.8 Interface ISecurityStepInfo	66
5.9 Mockup Konfigurator Template Desktop	67
5.10 Mockup Konfigurator Template Mobile	68
5.11 Aufbau Inhalt im Card-Design	69
5.12 Mockup Konfigurator Template Mobile	70
6.1 Screenshot VisualStudio der drei Projekte der Sicherheitsstufe E-Mail	78
6.2 Startseite und Registration des Konfigurators	81
6.3 Dashboard mit Auswertungen der Authentifizierungen	82
6.4 Detailproduktansicht des Konfigurators	83
6.5 Screenshot Spider-Diagramm mit Bewertungen vom Auftraggeber	84
6.6 Screenshot Umfrageergebnisse pro Interaktivität	84
6.7 Screenshot Umfrageergebnisse pro Interaktivität und Alter	85
6.8 Desktop-Computer-Ansicht der Authentifizierungs-Lightbox	86
6.9 Mobileansicht der Authentifizierung-Lightbox	87
6.10 Screenshot Konfiguration Wettbewerb und Projekt	89
6.11 Screenshot Unit-Test E-Mail Sicherheitsstufe	91
7.1 Screenshot einer Akzeptanzfrage	98
7.2 Screenshot der Umfrage zur Anstrengung	99
7.3 Beispiele der Illustrationen für die Umfrage	100
7.4 Berechnungsformel für Stichprobengröße	101
7.5 Ergebnisse Frage zu mogeln an Onlinewettbewerben	101

7.6 Übersicht der Ergebnisse zur Umfrage der Anstrengung mit Arithmetischem Mittel und Standardabweichung	102
A.1 Umfrage	115
A.2 Umfrage	116
A.3 Umfrage	117
A.4 Umfrage	118
A.5 Umfrage	119
A.6 Umfrage	120

A.2.2 Quellenverzeichnis

- 10minutemail.com (2016). <http://www.10minutemail.com>. [Online; accessed 28-02-2016].
- A Serious Look At Card Based Design (2014). <http://webdesignledger.com/card-based-design/>. [Online; accessed 04-03-2016].
- Beyer, Jutta (2015). "Du" oder "Sie" – Ansprache auf der Website. <http://contentkiste.de/du-oder-sie-ansprache-auf-der-website/>. [Online; accessed 24-02-2016].
- Bosnjak, Michael (2000). *Internet für Psychologen*. Hogrefe Verlag. ISBN: 978-3801712266.
- Burling, Stacey (2012). CAPTCHA: The story behind those squiggly computer letters. <http://phys.org/news/2012-06-captcha-story-squiggly-letters.html>. [Online; accessed 22-12-2015].
- Datatrans eCom - Technical Implementation Guide (2016). https://pilot.datatrans.biz/showcase/doc/Technical_Implementation_Guide.pdf. [Online; accessed 22-02-2016].
- Dillman, Don A. (1978). *Mail and telephone surveys. The total design method*. New York: John Wiley & Sons Inc. ISBN: 978-0471215554.
- Duden (2014). Vol. 26. Dudenredaktion. ISBN: 978-3-411-04650-8.
- Google Business (2016). <https://www.google.com/business/>. [Online; accessed 02-03-2016].
- Hanik, Filip (2015). Kiss. <https://people.apache.org/~fhanik/kiss.html>. [Online; accessed 29-12-2015].
- Hausherr, Matthias (2006). *Design By Contract in Java*. <http://www.gruntz.ch/courses/seminars/ws06/DBC.pdf>. [Online; accessed 10-03-2016].
- Hieatt, Edward and Rob Mee (2016). Repository. <http://martinfowler.com/eaaCatalog/repository.html>. [Online; accessed 05-03-2016].
- 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>. [Online; accessed 11-02-2016].
- <http://authentifizierung.org> (2015). <http://authentifizierung.org/>. [Online; accessed 23-12-2015].
- Interactive, Goldbach (2015). Nutzerzahlen der wichtigsten Plattformen. <https://twitter.com/revogt/>. [Online; accessed 28-12-2015].
- Interview mit Shaul Olmert (2015). https://www.youtube.com/watch?v=X_fQ1uG9rFY. [Online; accessed 28-12-2015].
- Kirk, Alexander (2005). IP Adresse. <http://www.computerlexikon.com/begriff-ip-adresse>. [Online; accessed 08-01-2016].

-
- Kriha, Walter and Roland Schmitz (2009). *Sichere Systeme*. Xpert.press. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-78958-1.
- Millischer, Sven (2015). *Die digitale Revolution*. handelszeitung.ch/digitalisierung/hz-sonderausgabe-die-digitale-revolution-874557. [Online; accessed 02-01-2016].
- MSDN (2015a). *Einführung in die Programmiersprache C# und in .NET Framework*. <https://msdn.microsoft.com/de-de/library/z1zx9t92.aspx>. [Online; accessed 01-02-2016].
- (2015b). *Entity Framework*. <https://msdn.microsoft.com/de-ch/data/ef.aspx>. [Online; accessed 01-02-2016].
- NET-Metrix-Audit (2004). news.admin.ch/message/index.html?lang=de&msg-id=13600. [Online; accessed 06-01-2016].
- NET-Metrix-Audit (2015). <http://netreport.net-metrix.ch/audit/>. [Online; accessed 02-01-2016].
- Neward, Ted (2006). *The Vietnam of Computer Science*. <http://blogs.tedneward.com/post/the-vietnam-of-computer-science/>. [Online; accessed 10-03-2016].
- Pass und Identitätskarte (2016a). <https://www.ch.ch/de/pass-identitatskarte/>. [Online; accessed 11-02-2016].
- Pass und Identitätskarte (2016b). <http://adi.kousz.ch/artikel/IDCHE.htm>. [Online; accessed 30-12-2015].
- PlayBuzz (2015). <http://www.playbuzz.com>. [Online; accessed 28-12-2015].
- Pratzner, Axel (2001). *Wissenschaftlich fundierter Aufbau von Fragebogen*. Institut für web-basierte Kommunikation und E-Learning.
- Projektmanagement: Definitionen, Einführungen und Vorlagen (2015). <http://projektmanagement-definitionen.de/glossar/meilenstein/>. [Online; accessed 24-12-2015].
- reCAPTCHA Digitization Accuracy (2014). <http://www.google.com/recaptcha/digitizing>. [Online; accessed 10-01-2015].
- 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-default-deny>. [Online; accessed 29-12-2015].
- Rouse, Margaret (2015). *Authentifizierung - Definition*. <http://www.searchsecurity.de/definition/Authentifizierung>. [Online; accessed 23-12-2015].
- 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/>. [Online; accessed 28-12-2015].
- So verwendet Google Cookies (2016). <https://www.google.ch/intl/de/policies/technologies/cookies>. [Online; accessed 08-01-2016].

-
- Sondereggerl, Bernhard (2013). *Der FingerabDruck*. Bern, Nussbaumstrasse 29: Bundesamt für Polizei fedpo.
- Stadtpolizei. *Vorlage Risikomatrix*. <http://bitly.com/risikomatrix-stadtpolzeizh>. [Online; accessed 17-01-2016].
- statista (2011). *Wie möchten Sie in Social Media von Unternehmen angesprochen werden?* <http://de.statista.com/statistik/daten/studie/218841/umfrage/von-nutzern-bevorzugte-ansprache-in-social-media-durch-unternehmen>. [Online; accessed 24-02-2016].
- Statistik, Bundesamt für (2015). *Statistik Schweiz*. <http://www.bfs.admin.ch>.
- Statistik Plattform* (2015). <http://de.statista.com/>. [Online; accessed 28-12-2015].
- Stern, Olaf (2012). *Reglement Bachelorarbeit*. Zürcher Hochschule für Angewandte Wissenschaften.
- Technical Details on Microsoft Product Activation for Windows XP* (2001). <https://technet.microsoft.com/en-us/library/bb457054.aspx>. [Online; accessed 02-03-2016].
- Tillmann, Henning (2013). *Browser Fingerprinting*. <http://www.henning-tillmann.de/2013/10/browser-fingerprinting-93-der-nutzer-hinterlassen-eindeutige-spuren/>. [Online; accessed 18-01-2016].
- Top 10 CMS November 2015* (2015). <http://de.statista.com/statistik/daten/studie/320685/umfrage/nutzungsanteil-der-content-management-systeme-cms-weltweit/>. [Online; accessed 21-01-2016].
- Two-factor authentication: FAQ* (2016). <http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>. [Online; accessed 28-02-2016].
- Usage of content management systems for websites* (2015). http://w3techs.com/technologies/overview/content_management/all. [Online; accessed 01-12-2015].
- w3techs (2016). *Historical trends in the usage of client-side programming languages for websites*. http://w3techs.com/technologies/history_overview/client_side_language/all. [Online; accessed 08-01-2016].
- Web Technologies of the Year 2015* (2016). http://w3techs.com/blog/entry/web_technologies_of_the_year_2015. [Online; accessed 10-04-2016].
- Webshop* (2016). <https://www.datatrans.ch/de/e-payment/shop-schnittstellen>. [Online; accessed 21-02-2016].

A.2.3 Tabellenverzeichnis

2.1	Soll - Ist Analyse/Vergleich	7
2.2	Meilensteine	7
2.3	Termine der Bachelorarbeit	8
3.1	Übersicht möglicher passiven Daten	29
3.2	Komplexere Kennzahlen aktives Fingerprinting	29
5.1	Recherche Plugins	55
5.2	Parameter Authentifizierungsservice Lightbox	59
5.3	Übersicht der Authentifizierungs Methoden	62
5.4	Auflistung von Vorurteilen	71

A.3 Arbeitsergebnisse

Die Bachelorarbeit in PDF-Form und alle Arbeitsergebnisse können unter folgendem github-Link heruntergeladen werden:

<https://github.com/coffeefan/Bachelor>

A.4 Danksagung

Zunächst möchte ich mich bei meinem Betreuer Jaime Oberle vielmals bedanken. Seine Fähigkeit, im richtigen Mass zu hinterfragen, herauszufordern und zu loben, unterstützte mich dabei, motiviert und fokussiert an der Bachelorarbeit zu arbeiten.

Auch meinem Auftraggeber, insbesondere Thomas Joss, möchte ich für die Bereitschaft und Zeit ein grosses Dankeschön aussprechen.

Mein grosser Dank gilt allen, die mir auf meinem Weg in der Studienzeit und während der Bachelorarbeit in vieler Hinsicht geholfen haben. Für ihre Unterstützung/oder ihren positiven Einfluss möchte ich mich insbesondere bedanken bei: Natanja Hofer, Martin Eigenmann, Thomas Bachmann, Christian Wyder, Ursula Hollenstein, Michael Eisenburger, Matthieu Jacquier, Ruth Bachmann, Ursi Hofer, Damaris Denzler, Benjamin Golder, Salome Leutert, Kathleen Wunderli, Benjamin Schwenter und Damaris Hollenstein.

A.5 Bestätigung

Hiermit bestätigt der Unterzeichnende, dass die Bachelorarbeit mit dem Thema "Individuell Konfigurierbarer Authentifizierungsservice für Votings und Wettbewerbe" gemäss freigegebener Aufgabenstellung mit Freigabe vom 18.11.2015 ohne jede fremde Hilfe im Rahmen der gültigen Reglements selbstständig ausgeführt wurde.

Alle öffentlichen Quellen sind als solche kenntlich gemacht. Die vorliegende Arbeit ist in dieser oder anderer Form zuvor nicht zur Begutachtung vorgelegt worden.

Aadorf den 09.05.2016

Christian Bachmann

A.6 Umfrage

Zürcher Hochschule
für Angewandte Wissenschaften



Sichere Interaktivitäten wie Votings und Wettbewerbe

Seite 1

Lieber Umfrage-Teilnehmer

Bei den meisten angebotenen Umfragen, Abstimmungen und Wettbewerben ist es relativ simpel, technisch das Resultat zu beeinflussen. Dieses Mögeln ist auf zu einfach realisierte Programmierungen zurückzuführen, was der Glaubwürdigkeit solcher Angebote schadet. Interaktivitäten wie Umfragen, Abstimmungen oder Wettbewerben bedürfen somit einer Authentifizierung, um Betrug oder falschen Stimmabgaben vorzubeugen. Die Authentifizierungsmethoden sind verschieden aufwendig und es müssen verschiedene persönliche Daten zur Verfügung gestellt werden.
Danke, dass Sie ca. 5-10 Minuten dafür investieren, Informatikem zu helfen, jeweils die richtige Authentifizierungsmethode für eine Interaktivität zu finden und so glaubwürdige und sichere Interaktivitäten unterstützen.
Die Ergebnisse stehen Programmierem von Interaktivitäten zur Konfiguration zur Verfügung. Geme senden wir Ihnen bei Angabe Ihrer E-Mail-Adresse die Ergebnisse zu.

Die Umfrage wird von ZHAW Student Christian Bachmann durchgeführt.

Hatten Sie schon einmal an einem Onlinewettbewerb teilgenommen, an welchem nach Ihrer Ansicht gemogelt wurde?

- ja
- nein

Seite 2

Mit den folgenden Fragen soll herausgefunden werden, mit welchen Methoden Sie bereit sind ein Voting oder Wettbewerb sicher auszufüllen. Die Methoden werden nun kurz erklärt.

Einen Bildcode abtippen (Captcha)



Bei einem Captcha soll der Benutzer die Zeichen aus dem Bild abtippen, und so zeigen, dass ein Mensch und nicht ein Computer das Formular ausfüllt. Der Captcha-Test dient also der Unterscheidung zwischen Mensch und Computer. Im Beispiel sieht das Captcha so aus, dass in einer Grafik mehrere Zeichen verschwommen und verzerrt dargestellt werden. Da Computer diese nicht automatisch scannen und erkennen können, ist es nur Menschen möglich die Zeichen korrekt abzutippen.

Abbildung A.1: Umfrage

E-Mail-Adresse angeben und aus dem erhaltenen E-Mail Code übernehmen



Bei der Validierung über die E-Mail-Adresse, trägt der Teilnehmer im 1. Schritt seine E-Mail-Adresse im Formular ein. An seine E-Mail Adresse wird ein Code gesendet. Diesen trägt der Teilnehmer im 2. Schritt in das Formular ein. Stimmt der Code weiss der Validierungsservice, dass die angegebene E-Mail-Adresse dem Teilnehmer gehört und vorhanden ist.

Mobile Nummer angeben, im SMS enthaltenen Code abtippen



Bei der Validierung per SMS trägt der Teilnehmer im 1. Schritt seine Mobile Nummer im Formular ein. An seine Mobile Nummer wird ein Code gesendet. Diesen trägt der Teilnehmer im 2. Schritt in das Formular ein. Stimmt der Code, dann weiss der Validierungsservice, dass die angegebene Mobile Nummer dem Teilnehmer gehört und vorhanden ist.

Telefon/Mobile Nummer angeben und den am Telefon vorgesprochenen Code abtippen



Bei der Validierung per Telefon trägt der Teilnehmer im 1. Schritt seine Telefonnummer im Formular ein. Der Telefonroboter ruft dann die eingetragene Telefonnummer an und spricht dem Teilnehmer am Telefon einen Code vor. Diesen trägt der Teilnehmer im 2. Schritt in das Formular ein. Stimmt der Code, dann weiss der Validierungsservice, dass die angegebene Telefonnummer dem Teilnehmer gehört und vorhanden ist.

Abbildung A.2: Umfrage

Adresse angeben, Code im erhaltenen Brief auf angebene Webseite übertragen



Bei der Post-Validierung trägt der Teilnehmer im 1. Schritt seine Adresse im Formular ein. Im Verlaufe der nächsten Tage erhält der Teilnehmer einen Code per Post. Diesen trägt der Teilnehmer im 2. Schritt in das Formular ein. Stimmt der Code, dann weiß der Validierungsservice, dass die angegebene Adresse des Teilnehmers stimmt.

Pass- oder ID-Nummer eintragen



Bei der Identitätskarten- und Pass-Validierung überträgt der Teilnehmer die Ausweisnummer ins Formular auf der Webseite.

Seite 3

Eine Online-Zeitung (z.B. blick.ch, 20min.ch) möchte anhand einer Umfrage die Meinung der Schweizer analysieren. Was wären Sie bereit auszufüllen, damit an der Umfrage nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angebene Webseite übertragen
- Pass- oder ID-Nummer eintragen

Bei einem Casting (Job, Talente, BlickGirl,...) soll der Gewinner vom Webpublikum bestimmt werden . Was wären Sie bereit auszufüllen, damit an der Umfrage nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angebene Webseite übertragen
- Pass- oder ID-Nummer eintragen

Abbildung A.3: Umfrage

Seite 4

Ein vertrauenswürdiges Unternehmen, wie das Schweizer Fernsehen, Zurich Versicherung oder die SBB verlost Preise im Wert von 50-200 Franken. Was wären Sie bereit auszufüllen, damit am Wettbewerb nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angegebenen Webseite übertragen
- Pass- oder ID-Nummer eintragen

Ein vertrauenswürdiges Unternehmen, wie das Schweizer Fernsehen, Züri Versicherung oder die SBB verlost Preise im Wert von mehr als 200 Franken. Was wären Sie bereit auszufüllen, damit am Wettbewerb nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angegebenen Webseite übertragen
- Pass- oder ID-Nummer eintragen

Ein Ihnen unbekanntes Unternehmen verlost Preise im Wert von 50-200 Franken. Was wären Sie bereit auszufüllen, damit am Wettbewerb nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angegebenen Webseite übertragen
- Pass- oder ID-Nummer eintragen

Ein Ihnen unbekanntes Unternehmen verlost Preise im Wert von mehr als 200 Franken. Was wären Sie bereit auszufüllen, damit am Wettbewerb nicht gemogelt werden kann? *

- Einen Bildcode abtippen (Captcha)
- E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
- Mobile Nummer angeben, im SMS enthaltenen Code abtippen
- Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
- Adresse angeben, Code im erhaltenen Brief auf angegebenen Webseite übertragen
- Pass- oder ID-Nummer eintragen

Abbildung A.4: Umfrage

Seite 5

Wie anstrengend finden Sie die folgenden Authentifizierungstypen? *

	Sehr anstrengend	anstrengend	neutral	angenehm	sehr angenehm	keine Antwort
Einen Bildcode abtippen (Captcha)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile Nummer angeben, im SMS erhaltenen Code abtippen	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adresse angeben, Code im erhaltenen Brief auf angegebenen Webseite übertragen	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Pass- oder ID-Nummer eintragen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Seite 6

Wie häufig nehmen Sie an einer Interaktivität (Umfrage, Wettbewerb, Abstimmung...) im Internet teil? *

- mehrmals wöchentlich
- wöchentlich
- monatlich
- seltener als monatlich

Ihr Geschlecht: *

Bitte wählen...

Ihr Alter: *

-16 Jahre

Ich bin SchweizerIn oder wohne in der Schweiz: *

- ja
- nein

Wollen Sie die Umfrageresultate erhalten? Dann tragen Sie Ihre E-Mail-Adresse ein:

Abbildung A.5: Umfrage

Seite 7

Herzlichen Dank



Vielen Dank, dass Sie sich Zeit genommen haben die Umfrage auszufüllen.

Bemerkungen

» [Umleitung auf Schlussseite von Umfrage Online](#)

Abbildung A.6: Umfrage