



Bachelorarbeit (Informatikingenieurwesen)

Individuell Konfigurierbarer Authentifizierungsservice für Votings und Wettbewerbe

Autor

Christian Bachmann

Betreuung

Jaime Oberle

Auftraggeber

inaffect AG

Datum

23.12.2015

Inhaltsverzeichnis

1	Einführung	2
1.1	Motivation	2
1.2	Aufgabenstellung	3
1.2.1	Ausgangslage	3
1.2.2	Ziel der Arbeit	3
1.2.3	Aufgabenstellung	3
1.2.4	Erwartete Resultate	4
1.3	Rahmenbedingungen Bachelorarbeit	5
2	Projektmanagement	6
2.1	Grobe Projektplanung	6
2.2	Aufwand	7
2.3	Meilensteine	8
2.4	Termine	9
2.5	Infrastruktur	10
2.5.1	Quellcode-Verwaltung mit GitHub	10
2.5.2	Zeitmanagement mit toggl	10
2.5.3	Dokumentieren mit Pandoc und LaTeX	10
2.5.4	Design Mockup Balsamiq	10
2.5.5	yUML	11
2.5.6	Draw.io	11
3	Recherche	12
3.1	Fachbegriffe	12
3.2	Erläuterung der Grundlagen	12
3.2.1	Authentifizierung	12
3.2.2	Autorisierung	12
3.3	Grundlegende Sicherheitsprinzipien	13
3.3.1	KISS	13
3.3.2	Default-is-deny	13
3.3.3	Open Design	13
3.3.4	Zusammenfassung der Sicherheitsprinzipien	14
3.4	Ähnliche Produkte auf dem Markt	14
3.4.1	OAuth-Provider	14
3.4.2	playbuzz.com	17
3.4.3	WebSMS.com Zwei-Faktor-Authentifizierung	18
3.4.4	SuisselD	19
3.5	Fazit	19
3.6	Authetentifizierungskomponenten	20
3.6.1	Cookie	20
3.6.2	Flash-Cookies	20
3.6.3	Mehrfachteilnahme	21

3.6.4	IP-Adresse	21
3.6.5	Kosten	21
3.6.6	Captcha	22
3.6.7	Zwei-Faktor-Authentifizierung	22
3.6.8	E-Mail-Bestätigungscode	23
3.6.9	SMS- Bestätigungscode	23
3.6.10	Telefonanruf mit Bestätigungscode	24
3.6.11	Postversand	24
3.6.12	OAuth	25
3.6.13	SuisselD Integration	25
3.6.14	Automatisierungsmöglichkeit	26
3.6.15	Browser Fingerprints	26
4	Anforderungen	28
4.1	Akteure	28
4.2	Use-Cases	29
4.2.1	Use-Cases Diagramm	29
4.2.2	Use-Cases Beschreibung	30
4.3	Anforderungen	34
4.3.1	Aufbau	34
4.4	Funktionale Anforderungen	35
4.4.1	FREQ-111 Programmierer Registration	35
4.4.2	FREQ-112 Programmierer Login	35
4.4.3	FREQ-113 Programmierer Passwort vergessen	35
4.4.4	FREQ-114 Programmierer Passwort ändern	35
4.4.5	FREQ-211 Konfigurieren eines neuen Social-Media-Modul Authentifizierungsvorgangs	35
4.4.6	FREQ-212 Antworten der Umfrage in Authentifizierungsservice importieren	36
4.4.7	FREQ-213 Umfrageergebnisse zur Konfiguration nutzen	36
4.4.8	FREQ-214 Anpassen eines Authentifizierungsvorgangs	36
4.4.9	FREQ-215 Authentifizierungs-Stufe auswählen	36
4.4.10	FREQ-251 Generierung von Code für Einbinden in ein vorhandenes System	37
4.4.11	FREQ-311 Authentifizieren	37
4.4.12	FREQ-411 Report der Authentifizierungen generieren	37
4.5	Nicht Funktionale Anforderungen	38
4.5.1	NFREQ-110 Betriebssystemunabhängigkeit	38
4.5.2	NFREQ-115 Wartbarkeit	38
4.5.3	NFREQ-120 Einfache Integration	38
4.5.4	NFREQ-122 Einfache und verständliche visuelle Konfiguration	38
4.5.5	NFREQ-126 Einfache und verständliche Authentifizierung	38
4.5.6	NFREQ-130 Performance	39
4.5.7	NFREQ-132 Skalierbar	39
4.5.8	NFREQ-135 Hohe Verfügbarkeit	39
4.5.9	NFREQ-210 Programmierer kann aus Vielzahl von verschiedenen Sicherheitsstufen auswählen	39
4.5.10	NFREQ-212 Die verwendeten Sicherheitsstufen sind in der Schweiz verbreitet	39
4.6	Risiken	41
4.6.1	R-01 Akzeptanz	41

4.6.2	R-02 Kosten	41
4.6.3	R-03 Überkomplexität	41
4.6.4	R-04 Systemumfeldänderungen	41
4.6.5	R-05 Schlechte/Unzureichende Framework	42
4.6.6	R-06 Termineinhaltung	42
4.6.7	R-07 Auslastung	42
4.6.8	Risikomatrix	43
4.6.9	Massnahmen	43
5	Konzept	45
5.1	Architektur	45
5.2	Software Design	46
5.2.1	Webservice	46
5.2.2	46
5.3	Genereller Ablauf Authentifizierung	47
5.4	Domänenmodel Differenziert	48
5.5	Datenbankdesign	49
5.5.1	Entity-Framework	49
5.5.2	ERD	49
5.6	Integration der Schnittstelle	50
5.6.1	Bestehende Systeme für Votings, Wettbewerbe und Quizes	50
5.6.2	Wordpress PlugIn Hook	51
5.6.3	Parallelen im ähnliches Anwendungsfeld	53
5.6.4	Integrationsentscheid	55
5.6.5	Integrationskonzept	55
5.6.6	Integrationsparameter	55
5.7	Sicherheitsstufen integrieren	57
5.7.1	Sicherheitsstufen bewerten	58
5.7.2	Auswahl der zu integrierenden Sicherheitsstufen	58
5.8	Modularität und Erweiterbarkeit	60
5.8.1	Design by Contract	60
5.8.2	MEF - Managed Extensibility Framework	60
5.8.3	Entscheidung	61
5.8.4	Sicherheitsstufen Libaray-Übersicht anhand MEF	62
5.9	Mockup	63
5.9.1	Konfigurator Template	63
5.9.2	Authentifizierungs-Lightbox Template	65
5.9.3	Hinweis zur Zusammenarbeit mit dem Auftraggeber	65
5.10	Wahl des Applikation Hosters	65
5.10.1	Asp.net Shared Hosting	65
5.10.2	Cloud Hosting	68
5.10.3	Entscheidung	68
5.11	Validierung von Benutzereingaben	68
5.12	Testing	68
5.12.1	Wie kann getestet werden?	68
5.12.2	Was soll getestet werden?	69
5.12.3	Repository Pattern	69
5.13	Systemarchitektur	69

6	Proof Of Concept	70
6.1	Techologien	70
6.1.1	C-Sharp	70
6.1.2	ASP.net Web API 2 / ASP.net MVC Framework	70
6.1.3	Entity Framework	72
6.1.4	Grunt	72
6.1.5	AngularJS	72
6.1.6	JSON	72
6.2	Umsetzung Sicherheitsstufe	73
6.2.1	Plugin Entwicklung	73
6.2.2	Interface - Vertrag mit den Sicherheitsstufen	73
6.3	Finale Screens	73
6.3.1	AngularJS-Konfigurator	73
6.3.2	Authentifizierung-Lightbox mit Sicherheitsstufen	74
6.4	Implementation Authentifizierung	74
7	Studie	76
7.1	Definition der Begriffe aus Aufgabenstellung	76
7.2	Ziel der Studie	76
7.3	Art der Studie	76
7.3.1	Vor- und Nachteile schriftlicher Fragebogen	77
7.3.2	Fazit	78
7.3.3	Webapplikation für Umfrage	78
7.4	Aufbau Gesamtkonzept	78
7.4.1	Einleitung	78
7.5	Hauptteil/Fragen	80
7.5.1	Erste Frage Theorie	80
7.6	Erste Frage	80
7.7	Theorie Fragen	81
7.8	Fragen über Akzeptanz	82
7.9	Frage Anstrengung	83
7.10	Bonus "Frage", Umgehung der Absicherung	83
8	Weitere Fragen	84
8.1	Abschluss	84
8.2	Verständlichkeit	84
8.3	Auswertung	85
8.3.1	Repräsentativität	85
8.3.2	Gemogelt an Wettbewerben	85
8.3.3	Bonus "Frage", Umgehung der Absicherung	85
8.4	Anstrengung	86
8.5	Akzeptanz	86
9	Fazit	88
A	Glossar	89
B	Verzeichnisse	90
B.1	Abbildungsverzeichnis	90
B.2	Quellenverzeichnis	91

B.3 Tabellenverzeichnis	92
C Danksagung	93
D Personalienblatt	94
E Bestätigung	95

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 Kreuzworträtsel nicht nur auf den letzten Seiten der Klatschheftchen oder Zeitungen abgedruckt werden, sondern vermehrt online publiziert und durchgeführt werden. Dass bei meinungsbildenden Umfragen oder Abstimmungen weniger auf Telefonumfragen zurückgegriffen wird, sondern diese immer mehr im Internet durchgeführt werden, ist ebenso wenig erstaunlich.

In der Schweiz konnten die grossen Medienhäuser ihre Zugriffszahlen auch 2015 steigern und ihre Toprangierungen beibehalten.² Um ihren Werbegewinn und Resonanz zu bewahren oder sogar auszubauen, sind Medien darauf angewiesen, dass ihre Stories 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 “Playfull Contents” 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 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. Interaktivitäten bedürfen somit einer Authentifizierung, um Betrug oder falschen Stimmabgaben vorzubeugen. Die Eigenentwicklung der gewünschten 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 Möglichkeit eines Authentifizierungsservices erörtern. Mit dieser sollen Programmierer über eine visuelle Oberfläche die Bedürfnisse eines Angebots konfigurieren und in ihren jeweiligen Modulen einbinden können.

¹[Mil15]

²[Net]

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 Bachelorarbeit

Die vorliegende Bachelorarbeit umfasst gemäss Regelment unter anderem folgende Punkte:

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

³[Ste12]

2 Projektmanagement

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

2.1 Grobe Projektplanung

Der grobe Projektplan illustriert die Strukturierung der Bachelorarbeit über die knapp sechs Monate lange Projektzeit. Der Projektplan liefert einen generellen Überblick über den zeitlichen Ablauf der Bachelorarbeit und legt die Milestones fest. Als Soll-Aufwand der Bachelorarbeit wurden 376 Stunden veranschlagt. Der effektive Aufwand betrug xx Stunden.

[illegible]

2.2 Aufwand

Im Unterkapitel Rahmenbedingungen 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

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

2.3 Meilensteine

Meilensteine sind zum einen sehr wichtig für das Projektmanagement, da sie den gesamten Ablauf der Bachelorarbeit in mehrere kleine und überschaubarere Etappen und Zwischenziele einteilen. Dadurch kann auf dem Weg zur erfolgreichen Umsetzung der Bachelorarbeit immer wieder inne gehalten 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. ¹

Tabelle 2.2: Meilensteine

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

¹[Mei]

2.4 Termine

Tabelle 2.3: Termine der Bachelorarbeit

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

2.5 Infrastruktur

Im Unterkapitel “Infrastruktur” sollen die verwendeten Tools erläutert werden.

2.5.1 Quellcode-Verwaltung mit GitHub

Um einerseits eine Datensicherung zu gewährleisten und andererseits die Änderungen nachvollziehbar abzulegen, wird die Bachelorarbeit mittels Git und GitHub versioniert. Das Repository² ist für den Betreuer, Experten und Auftraggeber jederzeit einsehbar.

2.5.2 Zeitmanagement mit toggl

Beim Arbeiten an der Bachelorarbeit kann man sich schnell in Details verlieren. Das Zeitmanagement-Tool toggl³ 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 wird zuerst im Markdown Syntax geschrieben und mittels Pandoc in LaTeX umgewandelt. Basierend auf den Templates und Einstellungen in reinem LaTeX wird dann das endgültige PDF-Dokument generiert.

2.5.4 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. Balsamiq ist ein wireframing Tool. Dank den vielen konfigurierbaren Elementen kann rasch ein Design-Mockup von Webseiten erstellt werden.

²<https://github.com/coffeefan/bachelorarbeit>

³<https://toggl.com>

2.5.5 yUML

Um Ablaufe-Diagramm, Use Case-Diagramme und andere Uml-Diagramme zu visualisieren, bedarf es ein Tool, 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 designen 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.

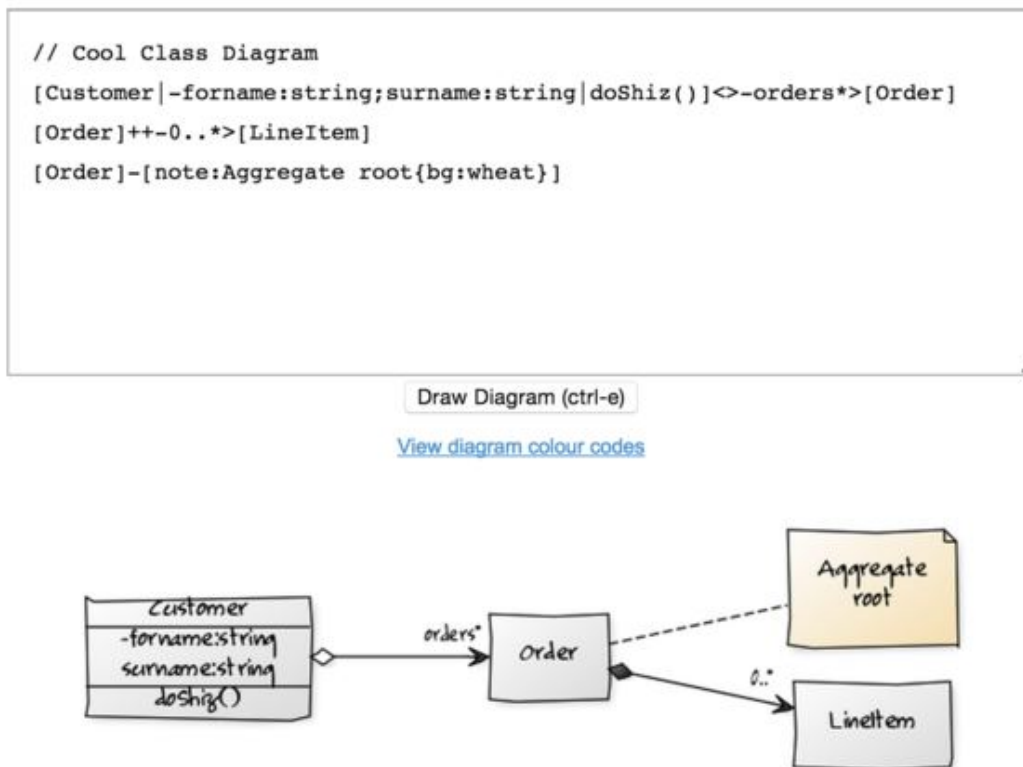


Abbildung 2.1: Screenshot yUML Beispiel Klassendiagramm

2.5.6 Draw.io

Alle Diagramme, welche nicht via yUML designt 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.

<

3 Recherche

3.1 Fachbegriffe

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

3.2 Erläuterung der Grundlagen

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

3.2.1 Authentifizierung

Duden: Authentifizierung - beglaubigen, die Echtheit von etwas bezeugen ¹

Eine Person oder Objekt eindeutig zu **authentifizieren** bedeutet zu ermitteln, ob die- oder derjenige auch die Person ist, als welche sie oder er sich ausgibt. ² 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 nahe zu grenzenlos. ³

3.2.2 Autorisierung

Autorisierung - Befugnis, Berechtigung, Erlaubnis, Genehmigung ⁴

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

Der Begriff Authentifizierung wird vielfach mit dem Begriff Autorisierung verwechselt. Die Authentifizierung wird vom Benutzer initiiert. Sie dient dem Nachweis, zur Ausübung bestimmter Rechte befugt zu sein. Die anschließende Autorisierung erfolgt automatisch durch das System selbst. Im Zuge der Autorisierung werden dem Benutzer seine Zugriffsrechte zugewiesen. [Aut]

¹[Dud]

²[Rou15]

³[Aut]

⁴[Dud]

3.3 Grundlegende Sicherheitsprinzipien

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

3.3.1 KISS

Keep It Stupid and Simple

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 Entwicklern machen den Fehler, Probleme zu wenig auseinanderzubrechen und alles in einem grossen Programm zu lösen, anstatt es in kleinen Paketen verständlich zu programmieren. [^apachekiss]

Die folgenden Punkte listen 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

KISS fördert die Sicherheit

Die Begründung, warum KISS die Sicherheit fördert, liefert Saltzer und Schroeder: Ungewollte Zugriffspfade können nur durch zeilenweise Codeinspektion entdeckt werden und 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. [^sicheresysteme_93]

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 Entwicklungsfirma nicht dieses Vorgehen verwenden. Zum Beispiel Filesysteme setzen auf Verbote anstatt auf explizite Erlaubnisse. [^sicheresysteme_94] [^defaultdeny]

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. [^sicheresysteme_95]

3.3.4 Zusammenfassung der Sicherheitsprinzipien

Die wichtigsten Sicherheitsprinzipien lauten zusammengefasst wie folgt:

- 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.

[^sicheresysteme_93] : [KS09, pp.93] [^sicheresysteme_94] : [KS09, pp.94] [^sicheresysteme_95] : [KS09, pp.95] [^apachekiss]: [Han15] [^defaultdeny]: [Rot15]

3.4 Ähnliche Produkte auf dem Markt

Dieses Unterkapitel erläutert existierenden Produkte auf dem Markt.

3.4.1 OAuth-Provider

OAuth

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

Das Bedürfnis nach OAuth

2006 implementierte Blaine Cook OpenID für Twitter. Ma.gnolia 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. Oktober 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 geschaffen 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

Die grössten OAuth-Provider wie Google, Facebook und Twitter erzielen eine weite Verbreitung weltweit:

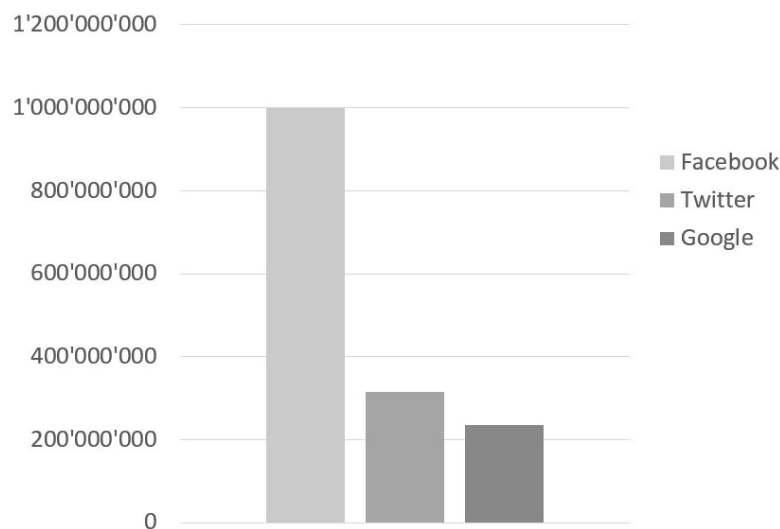
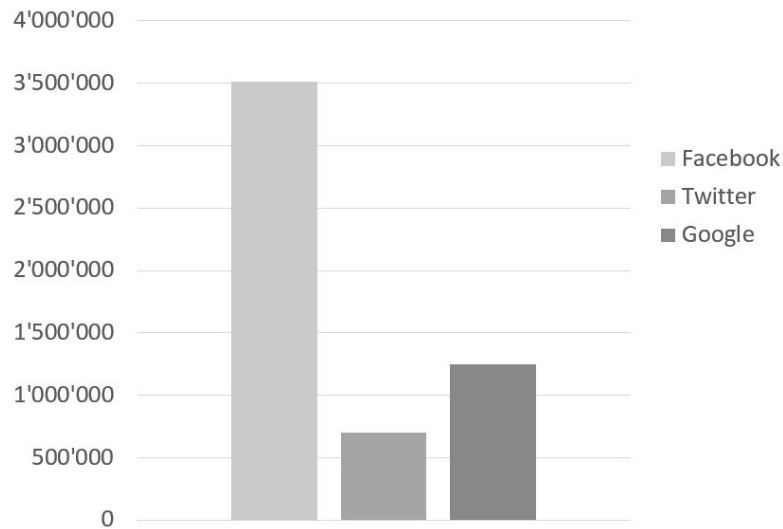


Abbildung 3.1: Aktive Nutzer Weltweit ⁵

Ganze 78% [Int15] der Schweizer Bevölkerung nutzten SocialMedia und besitzen dadurch einen OAuth-Account:

⁵Die Statistik wurde basierend auf den Daten von SocialMedia-Institute [Smi]erstellt. Facebook- und Twitter-Daten sind am 5. November 2015 und die Google-Daten im 2014 erhoben worden.

⁶Die Statistik wurde basierend auf den Daten von Goldbach Interactive [Int15] generiert. Die Daten sind im März 2015 erhoben.

Abbildung 3.2: Anzahl Schweizer Nutzer ⁶**Vorteile**

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

Nachteile

Mehrfachregistrierungen sind möglich. Je nach 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 tiefere Programmierkenntnisse möglich.

3.4.2 playbuzz.com

Youtube von Google ist im Jahr 2015 mit Abstand die meist verbreiteste Videopublishing-Plattform⁷. 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 Premie Minister von Israel Ehuad Olmert) und Tom Pachys ins Leben gerufen. Der offizielle Launch war im Dezember 2013. Im Juni 2014 wurde Playbuzz bereits das 1. Mal unter den Top 10 Facebook Shared Publishers aufgelistet. Im Juni 2014 konnte Playbuzz bereits 70 Millionen unique views aufweisen. Im September 2014 kamen 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 Endnutzer und Redakteuren einfache Verwendung.^{8 9}

Vorteile

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

Nachteile

Der Verweis auf Playbuzz ist immer klar ersichtlich. Auch beim Posten auf den SocialMedia-Kanälen ist die Herkunft von Playbuzz offensichtlich. Die Möglichkeiten in Funktionalität und Design haben hingegen Grenzen. Individuelle Erweiterungen sind nicht einfach möglich. Bestehende Interaktivitäten oder Interaktivitäten, welche nicht von PlayBuzz erstellt werden, können nicht verwendet werden. Mehrfachteilnahmen waren möglich.

⁷[Staa]

⁸[T3n]

⁹[Pla]

3.4.3 WebSMS.com Zwei-Faktor-Authentifizierung

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

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.¹¹ Dadurch ist eine eindeutige Authentifizierung über Mobilnummern gewährleistet. Die Mobilefunkanbieter 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 Chatprotokoll¹² 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 verschiedenem Kaufspersonal ein Prepaidhandy eingekauft. Beim Einkauf des sechsten Handys wurde der Verkauf von der 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 verschiedenem Kaufspersonal ein Swisscom Prepaidhandy. Beim Einkauf des sechsten Handys wurde der Verkauf von der Kasse abgelehnt. Die Nummer liess sich nicht erneut auf den Kunden registrieren, da er schon fünf SIM Karten bei der Swisscom besessen hat.

Sunrise

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

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

¹¹Meldung des UVEKS über Gesetzesänderung: [Uve]

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

¹³Kopie Bestell- und Lieferbedingungen <http://bit.ly/sunrise-bedingungen>

SALT

Bei der Firma SALT konnte mir ebenfalls kein Dokument mit der Kennzahl gegeben werden. SALT vergibt gemäss ihrer schriftlichen Auskunft ¹⁴ pro Person maximum drei SIM Karten.

Vorteile

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

Nachteile

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

3.4.4 SuisselD

Die SuisselD 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 SuisselD kostet den Endkunden eine beträchtliche Summe Geld. Der Anbieter der Authentifizierung erwarten keine grossen Kosten. Dadurch ist eine kleine Verbreitung für privaten Nutzen offensichtlich. Entwickler von Integrationen erhalten eine ganzes 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 Enduser sind die Nachteile von SuisselD.

3.5 Fazit

Auf dem Markt sind verschiedene Anbieter, welche Interaktivitäten schützen können oder gar 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.
¹⁵

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

¹⁵Stand 4. Januar 2016

3.6 Authentifizierungskomponenten

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 manipuliert werden.¹⁶¹⁷

Automatisierungsmöglichkeit und Mehrfachteilnahme

Die Automatisierung ist ohne IT-Knowhow 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 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 kann diese Speicherung auch clientseitig manipuliert werden. Seit Steven Jobs mit Apple keinen Support für die mobilen Geräte in Aussicht stellte und auf die Probleme und Risiken hinwies, verliert die Plattform gestärkt durch immer wieder auftretende Sicherheitsprobleme an Usern. So haben am 1. Januar noch knapp 10%^[^flashusage] aller Webseitenbesucher den Flash-Player.

^[^flashusage]^[w3t16]

¹⁶^[cookie-centra]

¹⁷^[Gooc]

3.6.3 Mehrfachteilnahme

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

Automatisierungsmöglichkeit

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

Kosten

Cookies verursachen keine direkten Kosten.

3.6.4 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. Deshalb auch der naheliegende Name IP-Adresse. Generell wird im Internet über den "IP Version 4 Standard" 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 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.¹⁸

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.

3.6.5 Kosten

Das authentifizieren via IP-Adresse verursacht keine direkten Kosten.

¹⁸[Kir05]

3.6.6 Captcha

Captcha ist ein Test, mit dem festgestellt werden kann, ob sich ein Mensch oder ein Computer eines Programms bedient ¹⁹.

Im Jahr 2000 wurde das Captcha an der Carnegie Mellon University erfunden. Captcha steht für **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. Luis von Ahn, Professor der Entwickler-Gruppe, erklärte die Dringlichkeit von Captcha damals so: "Anybody can write a program to sign up for millions of accounts, and the idea was to prevent that". **** ²⁰

Captcha Zahlen

In 2014 wurden 200 Million Captchas pro Tag eingegeben. Dabei braucht ein User durchschnittlich 10 Sekunden das entspricht 500'000 Stunden.²¹

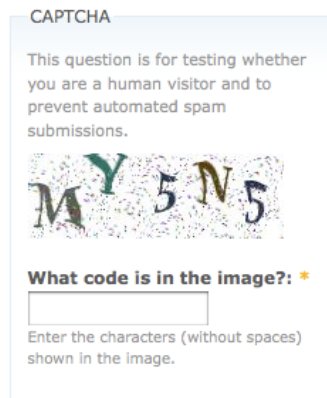


Abbildung 3.3: Beispiele von Captchas *Quelle:drupal.org*

3.6.7 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. [[^]cnet-2fa]

Die Zwei-Faktor-Authentifizierung ist in der Schweiz durch das E-Banking bekannt geworden. Der User gibt als erstes 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 ein Passwort auswendig gemerkt, welches er eingibt.

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

¹⁹[Dud]

²⁰[Bur12]

²¹Die statistischen Daten wurden von Google 2014 in ihrem Blog publiziert [Goob]

3.6.8 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-Mailadresse auch tatsächlich existiert und der User darauf Zugriff hat. Der User soll also auch bei der Authentifizierungsschnittstelle seine E-Mailadresse 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 Mail ²² stellen auf Knopfdruck für einige Minuten eine temporäre E-Mail Adresse zur Verfügung. Dadurch können schnell einige E-Mailadressen erstellt werden. Diese Domains müssen über eine aufwendige Blacklist gefiltert werden oder durch ein zeitversetztes Bestätigungsmail ausgehebelt werden.

Kosten

Das Versenden von E-Mails über einen SMTP-Server ist generell kostenlos. Bei hohem Gebrauch dieser Komponente lohnt es sich, die E-Mails über eine professionelle Infrastruktur für Massenversendungen zu versenden und zu analysieren. Beispiele dafür sind Mailchimp ²³ oder Sendgrid ²⁴

3.6.9 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 Mobilnummer 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 Mobilnummer gehört. Zum Versenden der SMS ist ein SMS-Gateway nötig.

Automatisierungsmöglichkeit

Die Automatisierung kann als nicht möglich eingestuft werden.

²²10-Minute Mail [10m]

²³www.mailchimp.com

²⁴sendgrid.com

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.²⁵

3.6.10 Telefonanruf mit Bestätigungscode

Nacheingabe der Telefonnummer oder Mobilenummer erhält der User einen digitalen Anruf. Die Computerstimme liest dem User einen Code vor, welcher er danach in der Webpage 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 0.65.²⁶

3.6.11 Postversand

Wie kann sichergestellt werden, dass eine Person auch tatsächlich am angegebenen Ort wohnt? Im Telefonbuch digital oder analog waren früher fast alle Personen erfasst. Immer weniger Personen haben heute einen Fixanschluss und einige lassen ihre 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.²⁷ Das simple Konzept kann auch für den Authentifizierungsschnittstelle umsetzt

²⁵Die Preise wurden am 1. März 2016 auf aspsms.ch/instruction/prices.asp, tropo.com/pricing und twilio.com/sms/pricing abgefragt

²⁶Die Preise wurden am 1. März 2016 auf nexmo.com/products/voice/, tropo.com/pricing und twilio.com/voice/pricing abgefragt

²⁷[Gooa]

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. Dieser "Jemand" kann als Service z.B. beim schweizer Startup pingin.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 1.65.²⁸

3.6.12 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.

3.6.13 SuisselD Integration

SuisselD wurde bereits im Kapitel SuisselD erläutert.

²⁸Die Preise wurden am 10. März 2016 auf pingin.com abgefragt

3.6.14 Automatisierungsmöglichkeit

Eine Automatisierung ist nahezu unmöglich.

Mehrfachteilnahme

Eine Mehrfachteilnahme ist nahezu unmöglich.

Kosten

Für den Betreiber fallen geringe Kosten an. Der Enduser zahlt aber einen bemerkenswerten Preis.

3.6.15 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 gehen 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 somit fertiggestellt. Dieses Muster ändert sich bis zur Auflösung des Körpers nach dem Tod nicht mehr.²⁹



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 Augenn sichtbar und wir hinterlassen das Muster der Papillarleisten auf Gegenständen wie Glas.

²⁹[Son13]

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 würde, der sowohl eindeutig, beständig und abrufbar ist. Immer wieder versuchten unter dem Thema "Browser Fingerprint" Personen ein Verfahren zu entwickeln, das genau dies ermöglicht. Microsoft führte laut eigenen Angaben ³⁰ 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 Registrierungsschlüssel Massnahmen getroffen werden.

Auch der Browser übermittelt an den Server verschiedene Informationen:

[^cnet-2fa] [^cnet-2fa]: [Cne]

Cookies

³⁰[Xpa]

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 Authentifizierungsschnittstellen-Service schützen.

User Der User ist der Endkunde. Er nimmt am Social-Media-Modul teil und authentifiziert sich über den Authentifizierungsschnittstellen-Service.

4.2 Use-Cases

Im Nachfolgenden werden alle UseCases 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.

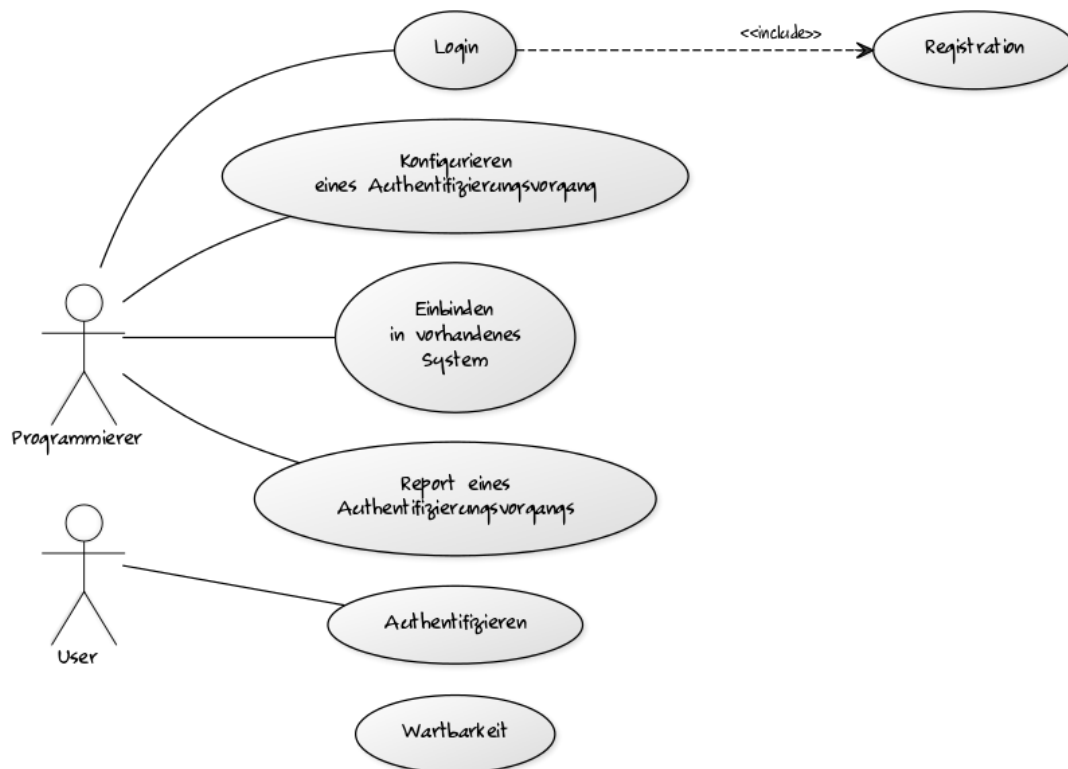


Abbildung 4.1: Use-Case Diagram

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

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

UC-12 Login Konfigurator

UseCase	
Ziel	Ein Programmierer kann sich beim Authentifizierungsschnittstellen-Service registrieren.
Beschreibung	Ein Programmierer muss sich am Authentifizierungsschnittstellen-Service 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 Authentifizierungsschnittstellen-Service ein.
Alternativszenario	Der Programmierer sendet sich das verpasste Passwort per E-Mail zu. Er erstellt über den im erhaltenden E-Mail enthaltenen Link ein neues Passwort und loggt sich mit E-mail und dem neuen Passwort am Authentifizierungsschnittstellen-Service ein.

UC-21 Konfigurieren eines Authentifizierungsvorgang

UseCase	
Ziel	Es ist ein neuer Authentifizierungsvorgang für ein neues Social Media-Modul konfiguriert.

UseCase	
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 verwendende(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 Authentifizierung in vorhandenes System einbinden

UseCase	
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. Der Programmierer hat einen neuen Authentifizierungsvorgang konfiguriert.
Ergebnis	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

UseCase	
Ziel	Der User ist authentifiziert oder der User abgelehnt.

UseCase	
Beschreibung	Der User probiert sich über den Authentifizierungsschnittstellen-Service zu authentifizieren um an einem Social-Media Modul teilzunehmen.
Akteure	User
Vorbedingung	Der Programmierer hat den Authentifizierungsvorgang konfiguriert und in seinem System eingebunden.
Ergebnis	Der Authentifizierungsschnittstellen-Service authentifiziert den User oder lehnt ihn ab.
Hauptszenario	Der User wird vom Social-Media-Modul an den Authentifizierungsschnittstellen-Service weitergeleitet. Der User authentifiziert sich. Der User kann die Eingabe des Social-Media Moduls erfolgreich abschliessen.
Alternativszenario	Der User wird vom Social Media-Modul an den Authentifizierungsschnittstellen-Service weitergeleitet. Der User wird vom System abgelehnt. Der User kann die Eingabe des Social-Media-Modul nicht erfolgreich abschliessen.

UC-41 Report eines Authentifizierungsvorgangs

UseCase	
Ziel	Die Verwendung des Authentifizierungsvorgangs ist übersichtlich dargestellt.
Beschreibung	Um den Verwendung des Authentifizierungsvorgangs auszuwerten, soll ein Report erstellt werden.
Akteure	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

UseCase	
Ziel	Der Authentifizierungsschnittstellen-Service 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.

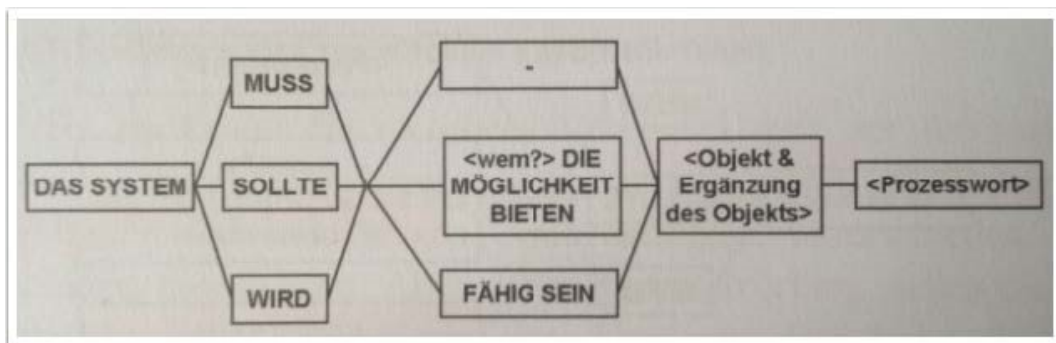


Abbildung 4.2: Basis Schablone *Quelle Rupp*¹

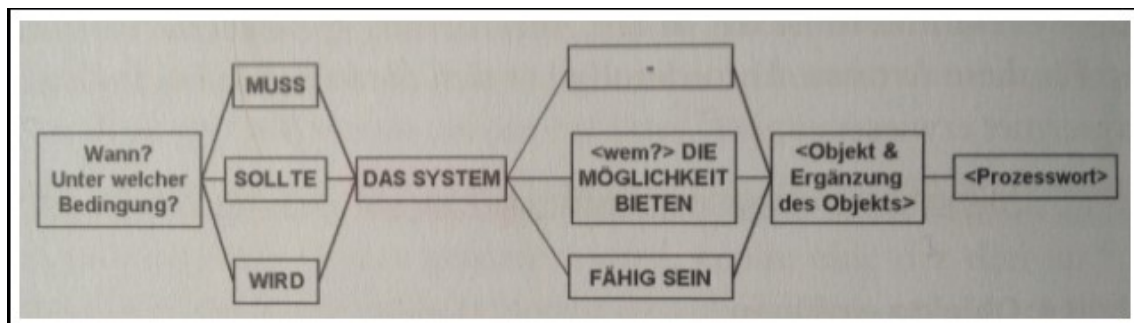


Abbildung 4.3: Erweiterte Schablone *Quelle Rupp*²

¹Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering [Rup11]

²Rupp Bilder sind aus dem Buch Basiswissen Requirements Engineering [Rup11]

4.4 Funktionale Anforderungen

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

Funktionale Anforderungen werden als *FREQ-Identifikation* bezeichnet.

4.4.1 FREQ-111 Programmierer Registration

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

4.4.2 FREQ-112 Programmierer Login

UC-Referenz	UC-12
Beschreibung	Ein Programmierer muss sich beim Authentifizierungsschnittstellen-Service 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 Social-Media-Modul Authentifizierungsvorgangs

UC-Referenz	UC-21
Beschreibung	Ein Programmierer kann einen neuen Authentifizierungsvorgang für sein neues Social-Media Modul 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 über 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 Authentifizierungsvorgangs 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 ein neues Social-Media-Modul erfassen
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 Authentifizierungsschnittstellen-Service authentifizieren um am Social-Media-Modul teilzunehmen. Der Authentifizierungsschnittstellen-Service authentifiziert oder lehnt den User ab.
Techn. Risiko	Mittel
Business Value	Sehr Hoch

4.4.12 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 *FREQ-Identifikation* bezeichnet.

4.5.1 NFREQ-110 Betriebssystemunabhängigkeit

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

4.5.4 NFREQ-122 Einfache und verständliche visuelle Konfiguration

UC-Referenz	UC-25, UC-21, UC22
Beschreibung	Der Authentifizierungsschnittstellen-Service 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 konfiguriert werden können.
Techn. Risiko	Sehr hoch
Business Value	Mittel

4.5.6 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

4.5.7 NFREQ-132 Skalierbar

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

4.5.8 NFREQ-135 Hohe Verfügbarkeit

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

4.5.9 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 Aspekte "Mehrfachteilnahme" und "Automatisierung" definiert worden. Beide Aspekte können durch eine Sicherheitsstufe mehr oder weniger verhindert werden. Abhängig von 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

4.5.10 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 Authentifizierungsschnittstellen-Service 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 Architekturentscheide 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 fixe Abgabetermin der Semesterarbeit 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

Schadensausmass	hoch			5		
		1	3	7	6	
	mittel		4			
	tief		2			
		tief	mittel	hoch	Eintrittswahrscheinlichkeit	

Abbildung 4.4: Risikomatrix ³

Legende

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.

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

Das Projekt ist über eine Anzahl von Feiertagen gelegt, welche gebraucht werden könnten. Zusätzlich wurde vom Studenten eine Arbeitswoche Ferien genommen, welche im Notfall auch für die Arbeit verwendet werden könnte. Durch diese Massnahmen sollte das Risiko 6 Termin-einhaltung minimal bleiben. Das Risiko 7 "Auslastung" kann nicht direkt vermindert werden. Die Aktivitäten im Bereich der freiwilligen Arbeit wurde auf ein Minimum reduziert. Für die restliche freiwillige Arbeit wurde mit Freunden ein Notfallszenario entwickelt, 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 wurden 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 von einander zu entwickeln, wird bei der Entwicklung der Architektur des Authentifizierungsservice darauf geachtet möglichst geringe Kopplung aufzuweisen.

5.1 Architektur

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

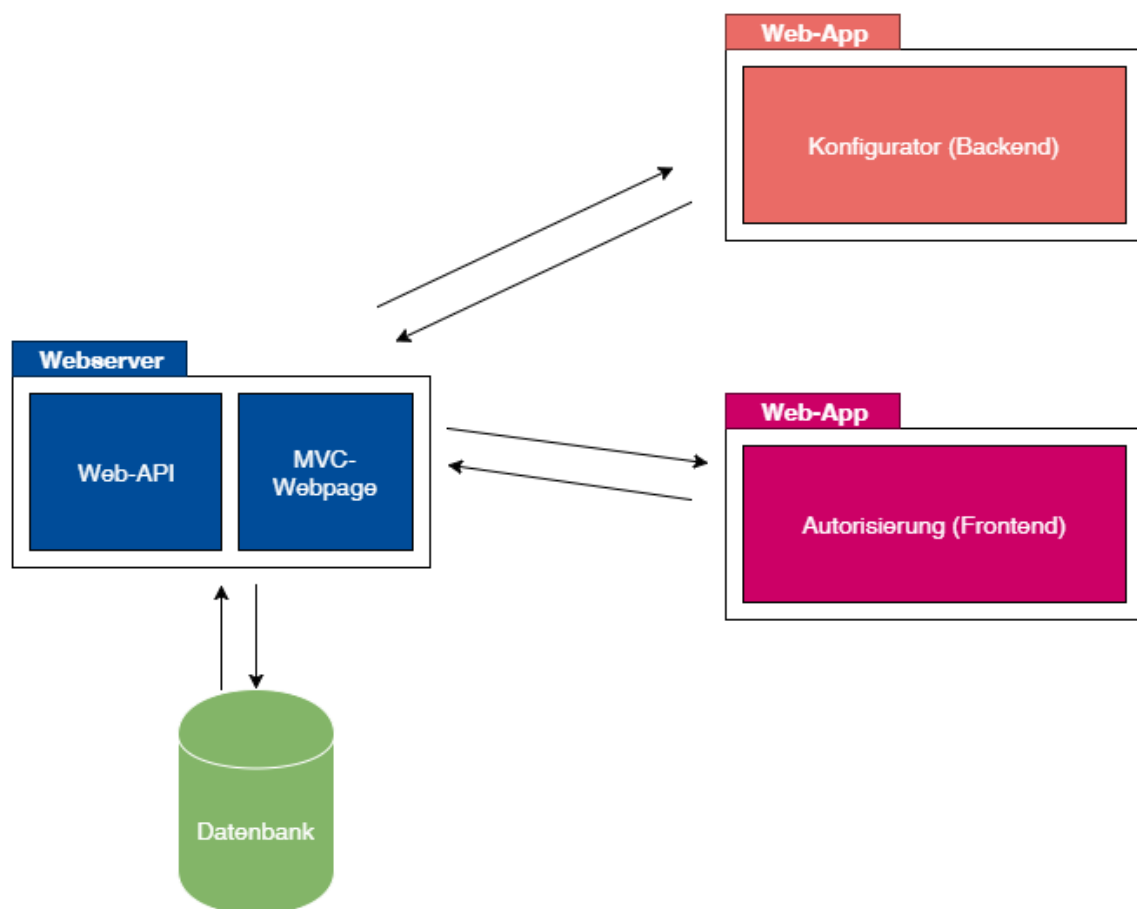


Abbildung 5.1: Übersicht der Hauptkomponenten

5.2 Software Design

5.2.1 Webservice

5.2.2

5.3 Genereller Ablauf Authentifizierung

Der User nimmt an einer Interaktivität eines Anbieters teil. Dabei füllt er den Wettbewerb, 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 Datengespeichert 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 Identität im gewünschten Masse sicher zustellen. User und das Anbieter System werden über erfolgreiche Authentifizierung informiert. Nach Möglichkeit wird auch eine fehlerhafte Authentifizierung mitgeteilt.

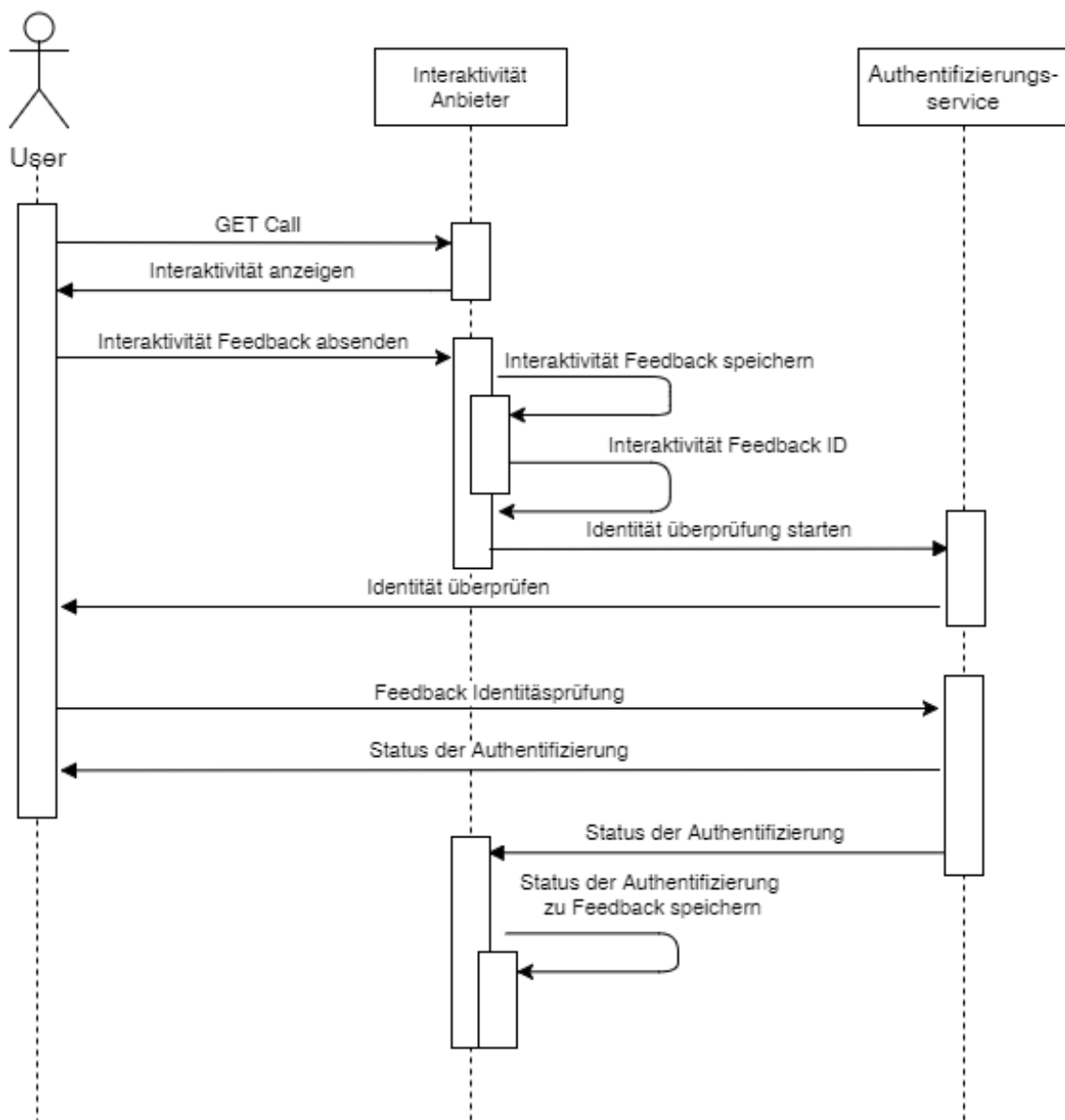


Abbildung 5.2: Aufbau Inhalt im Card-Design

5.4 Domänenmodel Differenziert

Ein differenziertes Domänenmodel oder auch Domänenmodel Basis Level genannt, erlaubt eine vereinfachte Kommunikation zwischen Kunde/Auftraggeber und Entwicklungsteam/Entwicklungsperson. Die Denkweise im Model erfordert keine Programmierkenntnisse und fördert die strukturierte Wiedergabe von Datengefassen. Beim Domänenmodel werden die Begriffe aus der Domäne des Kunden verwendet und fördern so die Verständlichkeit auf beiden Seiten.

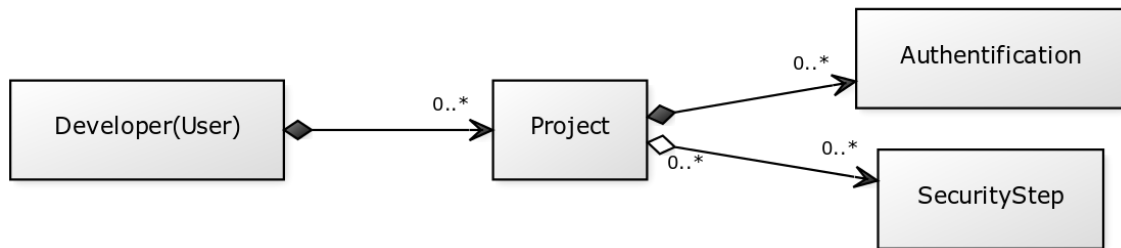


Abbildung 5.3: Differenziertes Domänenmodel des Authentifizierungservice

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.¹ 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 Datenbank designt. Das Entity-Framework bildet aus der Datenbank die POCO-Klassen² ab. Sollten Anpassungen an den Entitäten ergeben, werden diese zuerst in der Datenbank implementiert 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 selbständig generiert

¹[New06]

²Eine 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 der Anforderungsanalyse und 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 evtl für diese Systeme eine spezifisch einfach Integration zu entwickeln.

5.6.1 Bestehende Systeme für Votings, Wettbewerbe und Quizes

Das bestehende Social-Media Modul wird als Teil einer Webseite in einer Webapplikation geführt. Webapplikation, welche Inhalte verwalten, werden sinngemäss Content Management Systeme genannt. Die Abkürzung CMS hat sich im IT-Fachjargon etabliert. Statista.com wertet mehrmals im Jahr die Verbreitung der verschiedenen CMS aus³. Folgend ist die Erhebung aus dem November 2015 abgebildet:

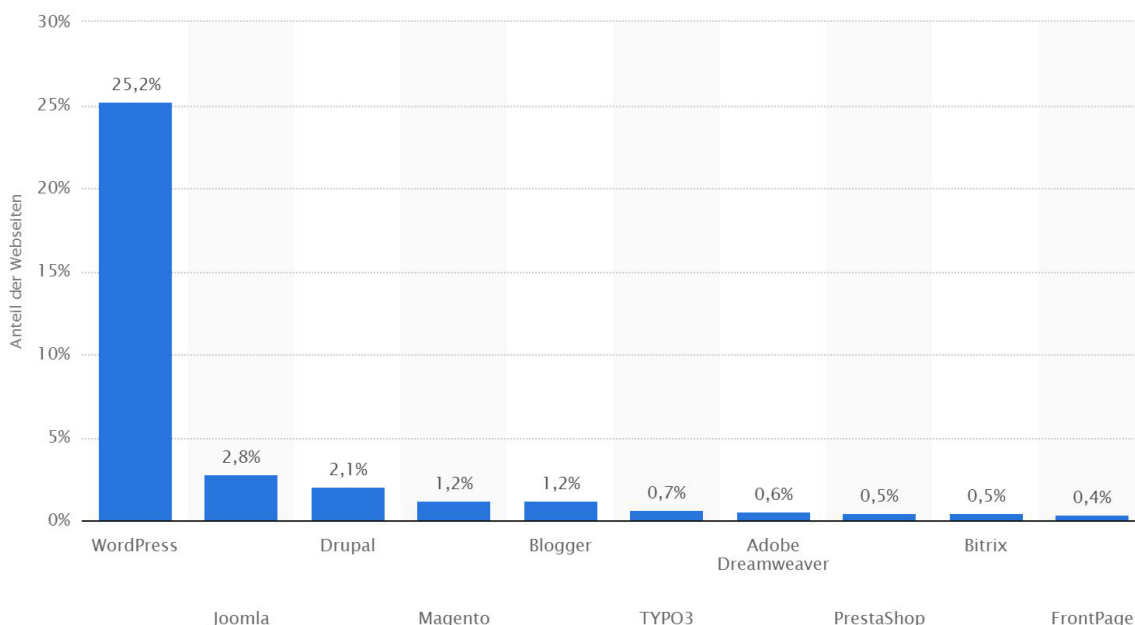


Abbildung 5.4: Nutzungsanteil CMS weltweit *Quelle:de.statista.com*

Die von statista.com veröffentlichten Zahlen wurden mit Werten von W3techs.com verglichen⁴. Die Unterschiede sind für unsere Verwendung minimal und liegen im 10tels Prozentbereich. Da beide bekannten Statistik unternehmen auf die selben Werte gekommen sind, kann von einem hohen Wahrheitsgrad ausgegangen werden. Beim Betrachten der Statistik fällt auf das Wordpress mit 25,2 mit Abstand am meisten genutzt wird. Alle dynamischen Webseiten unter den Top 10 basieren auf Systemen in PHP⁵. Adobe Dreamviewer und FrontPage sind keine Systeme welche auf dem Server betrieben werden. Sie sind Editoren welche auf dem jeweiligen Computer ausgeführt werden und danach mehrheitlich HTML, CSS und Javascript Code an den Server ausliefern. Funktionalitäten werden mit den beiden Editoren manuell geschrieben.

³CMS Nutzungsstatistik von statista.com [Stab]

⁴CMS Nutzungsstatistik von w3techs.com [Stac]

⁵Die Information wurde von den jeweiligen Hersteller- bzw. Communitywebseiten bezogen.

Basierend auf diesen statistischen Erkenntnissen lohnt es sich die Wordpress Welt kennen zu lernen und 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 natürlich manuell installiert werden. Zum Beispiel in dem man ein Plugin selber programmiert oder beim Hersteller oder über das Plugin-Verzeichnis von Wordpress[^plugin-verzeichnis] downloadedt. Wordpress sammelt zugleich die aktiven Installationen der Plugins (sofern man als Entwickler den Informationsaustausch nicht unterbindet). Die Gesamtzahl wird im CMS-Backend Wordpress und auf Ihrer Plugin-Verzeichnis Webseite[^plugin-verzeichnis] veröffentlicht. Dank dieser Kennzahl kann nun die meist verbreiteten Plugins herausgefunden werden.

Wordpress basiert auf einem sogenannten Hook-System. "Hook" eins zu eins übersetzt bedeutet "Haken", "Aufhänger" oder "Greifer". Ein Hook ist im Wordpress eine definierte Codestelle bei der man seinen eigenen Code einhängen kann. Der Plugin Entwickler definiert diese Hooks um anderen Plugins oder Funktionalitäten zu erlauben sein Plugin zu erweitern. Auch der Core vom Wordpress enthält solche Hooks. Dadurch soll verhindert werden, dass Plugin's oder der Core von Wordpress direkt umgeschrieben werden muss und dann nicht mehr einfach so unabhängig upgedatet werden kann. Um unsere Schnittstelle einzubinden, könnten wir eventuell also solche Hooks verwenden. Dieser "Hook"/Haken hat lustigerweise auch einen Haken: Der Plugin-Entwickler kann selbständig bestimmen ob und wo er solche Hooks einsetzen will und welche Möglichkeiten dann zur Verfügung stehen. Kommerzielle Plugin's verfolgen vielfach den Weg möglichst verschlossen zu agieren um mögliche Erweiterungen monetär umzusetzen und so eine Abhängigkeit zu erzeugen. Diese These gilt es nun zu untersuchen. Dafür wurden verschiedene Social Plugin's ausgewählt. Die Top 1000 installierten Wordpress Plugins welche von der Art Social-Media Modul waren, ein paar Stichproben von kommerziellen Plugins und Stichproben aus in Beiträgen empfohlenen Plugins: ^{6, 7}

Tabelle 5.1: Recherche Plugin's

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.

⁶Das Pluginverzeichnis befindet sich unter <http://de.wordpress.org/plugins>

⁷Envato bietet eine Plattform für den Verkauf von Wordpress-Plugin's an <http://market.envato.com>

Plugin	Kosten	Installation	Info zu Hooks
Responsive Poll	15\$	-	Keine Hooks. Laut Hersteller sind welche geplant (Zeitpunkt ungewiss)
TotalPoll Pro	18\$	-	Hooks vorhanden. Ähnlich wie bei WP-Polls könnte man evtl. den erstellten Datensatz löschen. Jedoch ist dies ohne Kauf nicht ersichtlich.
Easy Polling	15\$	-	-
Opinion Stage	kostenlos	10000+	-
Wedgies	Freemium	800+	-

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

5.6.3 Parallelen im ähnliches Anwendungsfeld

Der vertieften Research der letzten Kapitel wird verlassen und es wird probiert einen anderen Herangehensweise zur Findung der Lösung zu nehmen: Forscher adaptieren immer wieder erfolgreiche Modelle aus anderen Bereich in ihr Gebiet. Vielfach wird die Natur als erfolgreiches Vorlagemodell genommen. Ganz soweit wird hier nicht gegangen. Payment-Gateways wie der Schweizer Anbieter Datatrans müssen Webshop-Entwicklern auch eine Möglichkeit bieten das Gateway einfach in Ihren Webshop einbinden zu können. Auch bei Ihnen steht die Sicherheit auf der obersten Stufe und eine einfache Integration ist für den Erfolg trotz internationalem Druck von nöten. Dabei fährt Datatrans eine Zweiwegstrategie. Sie stellen für bekannte Shoppingsysteme gleich ganze PlugIns zur Verfügung⁸. Auf der anderen Seite bieten Sie ausführliche beschriebene und einfache Schnittstellen an.

Datatrans Zahlungsablauf

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

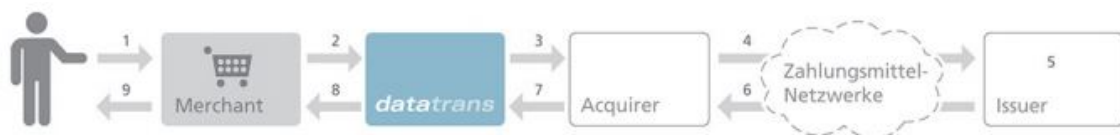


Abbildung 5.5: Nutzungsanteil Zahlungsablauf Webshop mit Datatrans *Quelle: datatrans*

1. Der Endkunde wählt Produkt aus und schliesst die Bestellung ab
2. Der Webshop/Merchant zeigt Zahlungsseite von Datatrans, Karteninhaber gibt seine Kartendaten ein. 3.-7. Datatrans autorisiert und verarbeitet wennmöglich die Transaktion zum Acquirer.
3. Datatrans zeigt den Status dem Kunden an und sendet Status dem Merchant zurück.
4. Merchant zeigt dem Karteninhaber die Antwortseite (erfolgreich oder abgelehnt) ⁹

⁸Übersicht der Web-Shop PlugIn's [Datb]

⁹Für die Bachelorarbeit wurde die V 9.1.13 verwendet [Data]

Datatrans XML/SOAP API Lightbox Mode

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

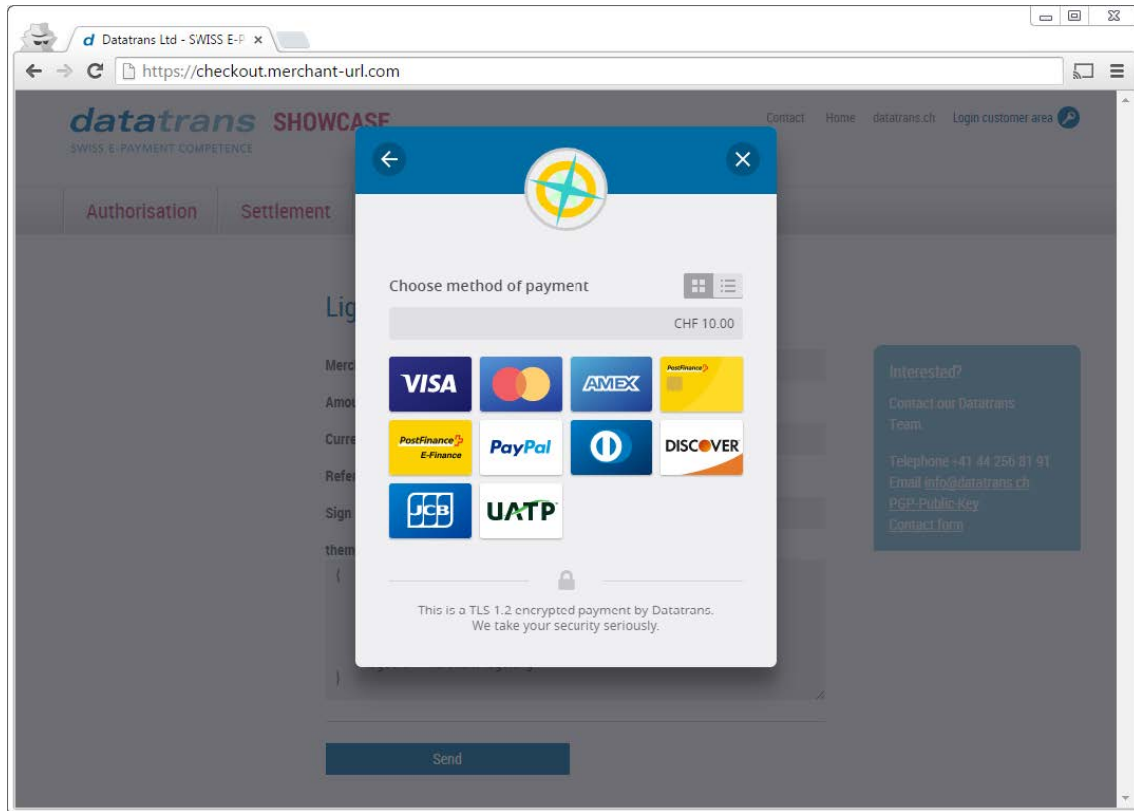


Abbildung 5.6: Datatrans Lightbox Integration *Quelle: datatrans*

Das Gateway muss eine minimum an Informationen erhalten, um den Zahlungsvorgang überhaupt starten zu können. So muss es wissen, wer der Verkäufer ist. Datatrans regelt dies über eine Merchant-ID. Wie viel 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 singemäss refno. Die Ganzen Parameter werden optional mit einem sign-Parameter gesichert und mittels Html-Form dem Javascript übergeben:¹⁰

¹⁰Für die Bachelorarbeit wurde die V 9.1.13 verwendet [Data]

Implementierungscode der Datatrans:

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

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

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

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 nahe zu entgegen. Dadurch ist eine Hohe Effektivität gegeben. Der User bleibt auf der selben 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 mit geladen. 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-Anbiter 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 das Benutzer und Entwickler den Authentifizierungsservice als ein sicheres und glaubwürdiges Produkt für Interaktivitäten wahrnehmen wird so versteckt werden.

5.6.5 Integrationskonzept

5.6.6 Integrationsparameter

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 Signature

Die Verwendung einer einfachen Signatur beugt Eingabefehler vor. Wenn auch nur geringfügig, der Aufwand erschwert zusätzlich den Missbrauch. Um eine korrekte Signatur zu erstellen werden folgende Parameter konkateniert und mit einem Plus separiert.

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

Beispiel: 30045+12+BUQHFMNZ4P3T8XNVN0LK

Der daraus resultierende String wird mit MD5 verschlüsselt.

Beim Beispiel gäbe es die Signatur b37b3d4cd7cd8cba3f409f07d6f6d9bd

5.7 Sicherheitstufen integrieren

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

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 Teilnahme als 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.

IP-Adresse

Durch Speicherung der IP-Adresse soll ein Benutzer der bereits an einer Interaktivität teilgenommen hat, identifiziert werden. Eine IP Adressen vertritt gegen Aussen alle Benutzer mit dem selben "Internetanschluss"!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 und Verhinderung von Automatisierung als ungenügend bewerten. Die Methode kann als kostenlos eingestuft werden und generiert beim Endbenutzer keinen Aufwand

Browser Fingerprint

Durch Generierung eine Browser Fingerprints (siehe Recherche) identifiziert werden. Das Verfahren kann zu 94% ein User wiedererkennen. Dass Verwenden mehrerer Browser oder Geräte führt zu verschiedenen Browser Fingerprints. iPhone taugt nicht für die 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.

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 5 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.

Telefon Authentifizierung

Der Benutzer gibt seine Telefonnummer ein. Der Benutzer wird automatisiert angerufen und die Computerstimme liest ein 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.

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, deshalb wird Unique mit gut und nicht sehr gut bewertet. 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 erhalten auf einer Webseite quittieren

5.7.1 Sicherheitstufen 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 Schweizer Schulnote vergeben.

Tabelle 5.3: Übersicht der Authentifizierungs Methoden

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

5.7.2 Auswahl der zu integrierenden Sicherheitsstufen

SuisseID und Flash-Cookies erreichen beim Musskriterium Verbreitung in der Schweiz (NFREQ-212) keine genügende Note und wird daher ausgeschlossen. Um die geforderte Breite an Sicherheitsmethoden zu erlangen wurden die folgenden Methoden mit verschiedenen Stärken in

Aspekten durch den Auftraggeber ausgewählt:

5.8 Modularität und Erweiterbarkeit

Wie in der Einführung zur Architektur 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. Andererseits kann sich auch die Authentifizierungsmethoden an sich komplett verändern. Sehr realistisch ist, dass für einen Browser Fingerprint neue Berechnungsmethodiken bekannt werden. Der Anbieter der hinter eine Authentifizierungsmethode steht, kann sich verändern oder dessen Anbindung. Kurz gesagt, die Modularität der Authentifizierungsmethoden muss unbedingt gewährleistet sein. Eine Implementation der Sicherheitsstufe SMS wie im folgenden einfachen Beispiel sollte nicht verwendet werden.

```
SMSSecurityStep inst = new SMSSecurityStep();
```

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. Die Verträge enthält besteht aus

- precondition: "Die Zusicherung die der Aufrufer einzuhalten hat"
- postcondition: "Die Zusicherung die der Aufgegrufene einhalten wird"
- Invariants: "Invariants sorgen dafür, dass bei Eintritts- und Austrittspunkten des Server Codes gewisse Conditions 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:

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

ISecurityStep-Vertrag ist im Beispielcode der Vertrag. Die Instanz proxy liefert ein Objekt zurück, welches das 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 SMSSecurityStep und CookieSecurityStep die Schnittstelle ISecurityStep implementieren.

SomeFactory muss für die Umsetzung von Design by Contract 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 ¹¹

5.8.2 MEF - Managed Extensibility Framework

MEF das Managed Extensibility Framework ist seit der Version 4.0 Bestandteil des 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.

¹¹[Hau06]

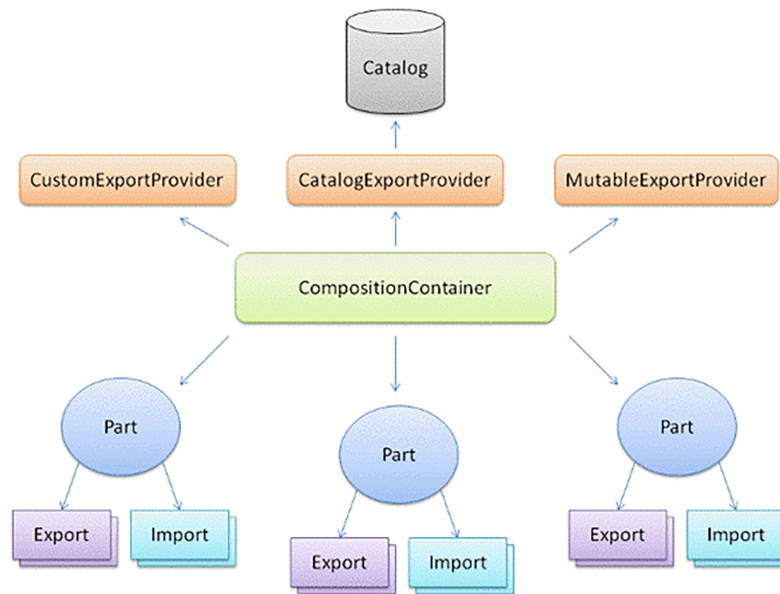


Abbildung 5.7: Vereinfacht die Architektur des Managed Extensibility Framework Quelle: msdn.microsoft.com

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 instanziiert 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. Die Variable proxy vom Type ISecurityStep die die Instanz dieser Komponente enthalten soll, wäre ein „Import“ in einer MEF Anwendung. Der SMSSecurityStep oder CookieSecurityStep wären in einer MEF Anwendung ein Export.

MEF automatisiert die Instanziierung mit Hilfe von Catalog und Container.

5.8.3 Entscheidung

Der Ansatz der Umsetzung des Design by Contract bräuhete eine geeignete Integration für die Factory um die Modularität für [NFREQ-115] sicherzustellen. MEF stellt den vollen Umfang an Funktionalität, zur Lösung der Problematik, zu Verfügung. MEF bietet des weiteren die Möglichkeit die DLL's zur Laufzeit auszutauschen und eine automatisierte Instanziierung. Deshalb sind die Sicherheitsstufen des Authentifizierungsservice basierend auf MEF zu integrieren.

5.8.4 Sicherheitsstufen Library-Übersicht anhand MEF

Basierend auf dem Managed Extensibility Framework wird der Aufbau unstrukturiert. 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.

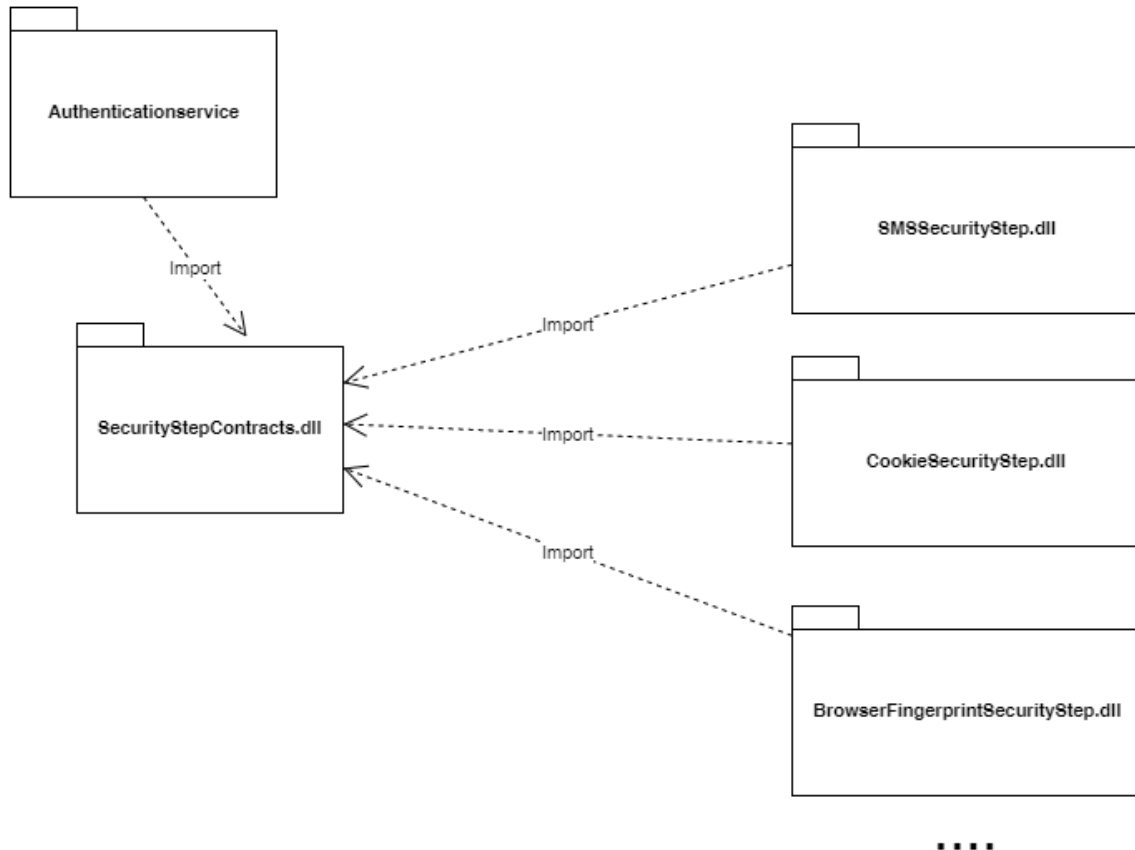


Abbildung 5.8: UML Library Overview

5.9 Mockup

Ein Mockup ist eine grobe Vorlage für die Design-Umsetzung. Es ist eine ideale Möglichkeit das visuelle Konzept ab zu bilden 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 arbeitet. Für Auswertungen und Präsentationen kann der Programmierer durchaus auch mobile Endgeräte verwenden. Deshalb soll die Umsetzung responsive gestaltet werden.

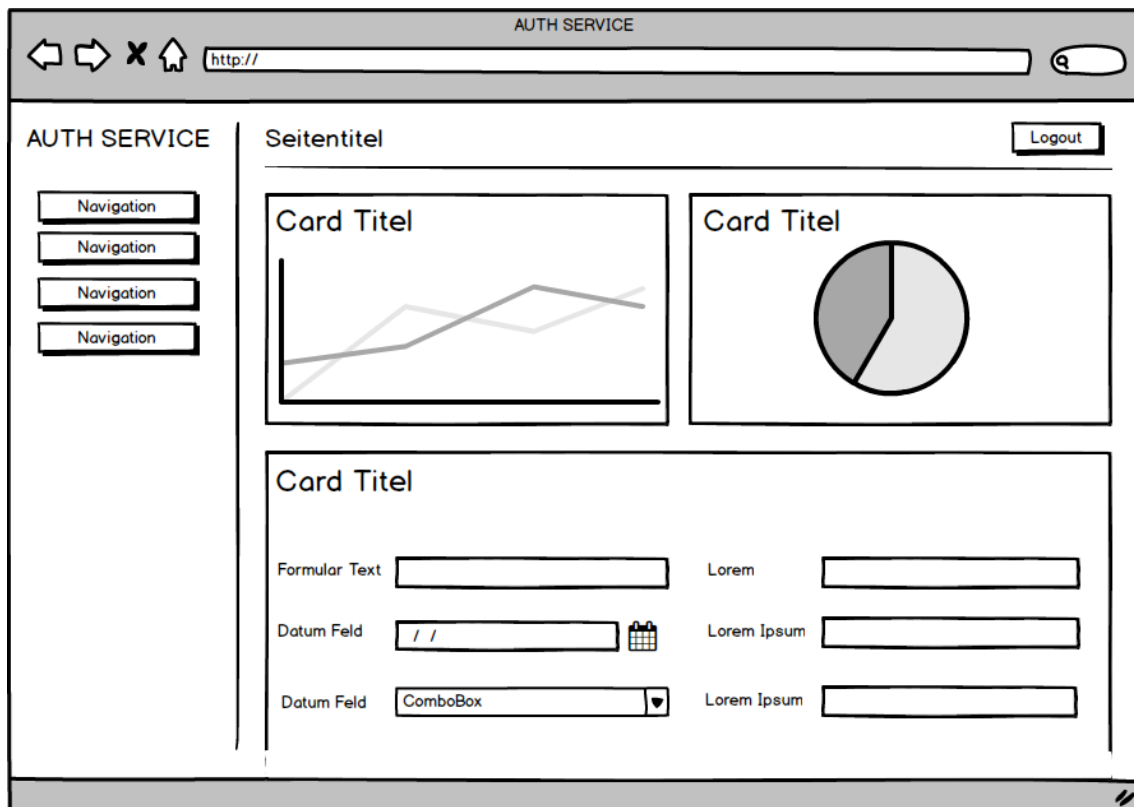


Abbildung 5.9: Mockup Konfigurator Template Desktop

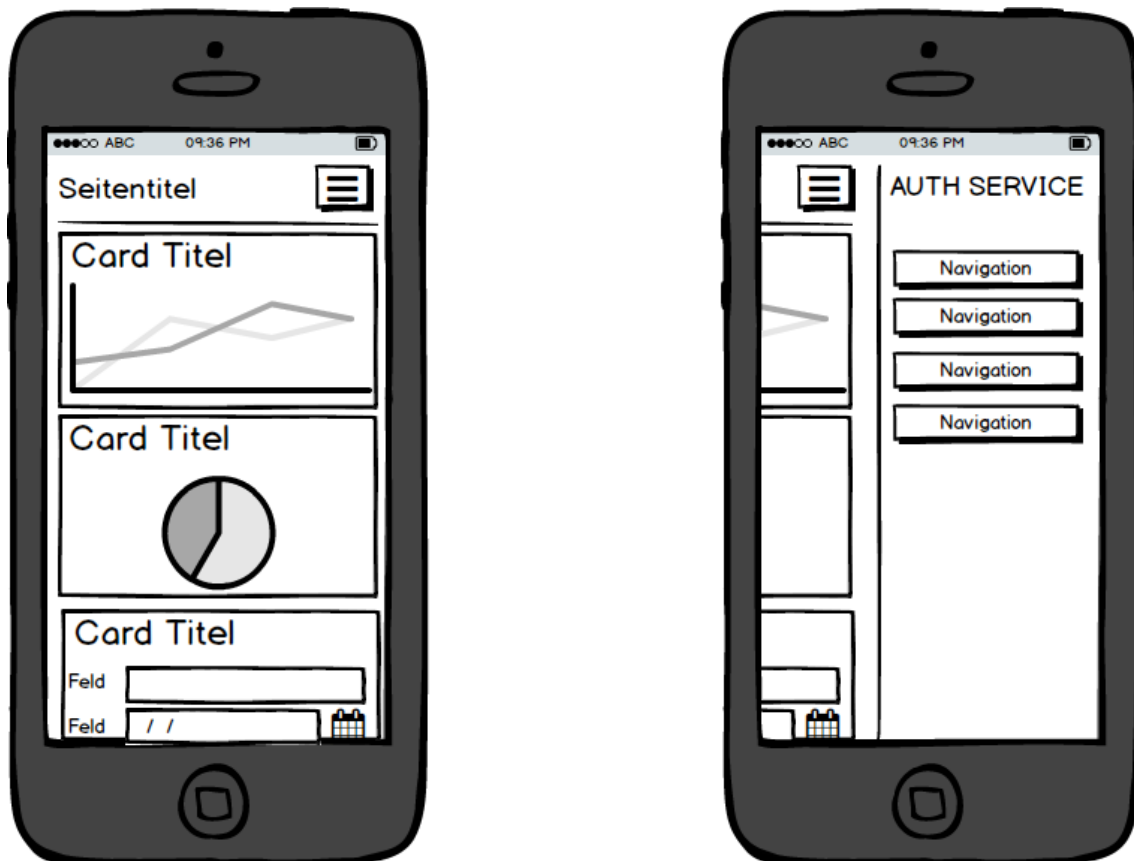


Abbildung 5.10: Mockup Konfigurator Template Mobile

Seitenaufbau

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

Navigation

Im Designkonzept wurde 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 kann in der Desktopansicht links immer alle Navigationspunkte angezeigt werden. Der Programmierer kann rasch auf die gewünschte Seite switchen. 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 bekräftigt durch den Wunsch den Konfigurator gestalterisch mit Farb und Bild aufzuwerten. Dies ist über die linke Spalte einheitlich und einfach umsetzbar.

Inhaltsaufbau

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. Die selbe Struktur soll 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 English genannt 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 (wenn auch repetitiv) dem Anwender kommuniziert, was für ein Inhalt im Breich Content der "Card" zu erwarten ist.¹²

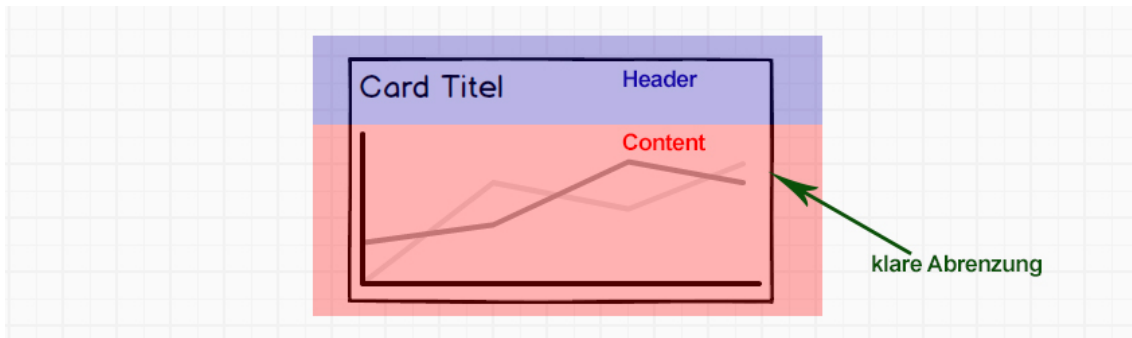


Abbildung 5.11: Aufbau Inhalt im Card-Design

5.9.2 Authentifizierungs-Lightbox Template

5.9.3 Hinweis zur Zusammenarbeit mit dem Auftraggeber

Die hier abgebildeten Mockups und weitere Ansichten sind das Ergebnis aus den Absprache mit dem Auftraggeber. Sie sind vom Auftraggeber abgenommen und zur Impelmentation freigegeben¹³

5.10 Wahl des Applikation Hosters

5.10.1 Asp.net Shared Hosting

Ein Asp.net Shared Hosting ist durchaus für komplexere Webapplikationen wie der Authentifizierungservice 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 aktualisiert werden. 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 Datencenter sind meist nicht redundant geführt. Fällt das Datencenter aus ist, die Applikation nicht verfügbar.

¹²Weitere Informationen und Beispiele auf webdesigner.com [Car]

¹³Alle Freigaben sind in der Beilage-Datei oder auf dem github-Account einsehbar

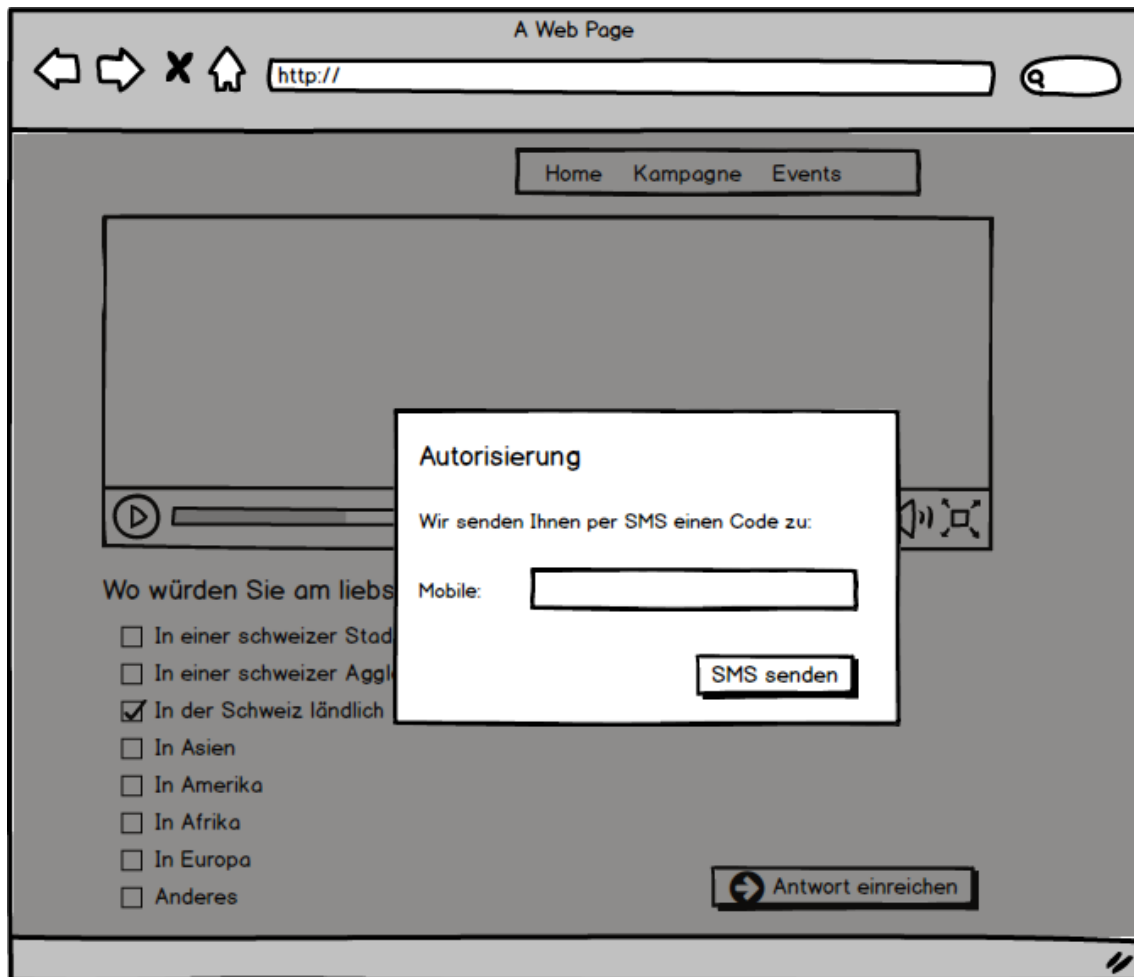


Abbildung 5.12: Aufbau Inhalt im Card-Design



Abbildung 5.13: Aufbau Inhalt im Card-Design

5.10.2 Cloud Hosting

Die Serverkosten sind direkt von der eigentlichen Nutzung abhängig. Das Hosting ist skalierbar und kann sich automatisiert an den aktuellen Nutzungsbedürfnissen anpassen. Die realen Kosten sind im vornherein schwerer zu definieren. Die Daten sind in der Cloud redundant geführt. Fällt ein Datencenter aus kann ein anderes dessen Aufgabe übernehmen. Ein Anbieter der direkt Asp.net Webservice als Hostingservice anbietet wurde nicht gefunden.¹⁴ Indirekt über z.b. über ein Docker Image könnte auch ein Schweizer Anbieter berücksichtigt werden. Die genutzten Serverdienste können komplett an seinen eigenen Bedürfnissen angepasst werden.

5.10.3 Entscheidung

Die in [NFREQ-132] geforderte Skalierbarkeit, nutzungsabhängige Kosten, Freiheit in der Serverdienst-Konfiguration überwiegen der einfachen Speicherung der Daten in der Schweiz. Ausserdem wird das einfache publishen (veröffentlichen) einer Web-Application aus dem Visual Studio bei allen Cloudanbieter angeboten (bei Shared Hosting sind es nur vereinzelt Anbieter), was den Development Workflow erheblich unterstützt. Deshalb ist der Authentifizierungsservice im Cloud Hosting zu betreiben.

5.11 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-Klassen/POCO-Klassen werden die gültigen Wertebereiche mittels Annotationen festgelegt. Microsoft MVC und Microsoft Web-API stellen eine "ModelState.Valid()" Methode zur Verfügung welche das angelieferte Datenobjekt automatisch gegen die Annotationen prüft. Bei MVC Implementierungen werden mittels Microsoft jQuery Validate Standart 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.

5.12 Testing

Die gewählte Architektur sowie Dependency Injection vereinfachen das Testing.

5.12.1 Wie kann getestet werden?

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

¹⁴Stand 18. Dezember 2015

5.12.2 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.

5.12.3 Repository Pattern

Wie im Kapitel Testing beschrieben, sollte eine Möglichkeit geschaffen 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 Collectionartigen 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. Weiter 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.¹⁵

5.13 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.

¹⁵[HM16] ##Domänenmodell ###Entitäten

6 Proof Of Concept

Das Ziel 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# orientiert sich stark an Java, C++, Haskell und Delphi. Daher liegt es Nahe das C# eine objektorientierte Programmiersprache ist und der Wechsel von den zu vorgenannten Programmiersprachen auf C# einfach fällt.

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

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

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

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

¹Quelle:[MSD15a]

die vom Framework bereitgestellten Komponenten unterstützt. Um RESTful-Webservices einfach entwickeln zu können stellt Microsoft mit ASP.net Web API 2 eine einfache zu verwendendes und starkes Software Paket zur Verfügung. ASP.net Web API 2 basiert auf dem ASP.net MVC Framework. ²

²Quelle:[MSD15a]

6.1.3 Entity Framework

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

6.1.4 Grunt

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

6.1.5 AngularJS

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

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

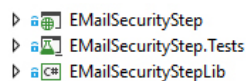
6.1.6 JSON

Zwischen der AngularJS WebApp und dem Webservice dient JSON(JavaScript Object Notation) als Datenübertragungsformat. JSON zeichnet sich durch seine schlanke Notation und der objektnahen Darstellung aus [^efbasic]: Quelle [MSD15b] [^angularjsbasic]: Quelle [San14]

6.2 Umsetzung Sicherheitsstufe

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 3 VisualStudio Projekte angelegt. Im Hauptprojekt der Sicherheitstufe wird die klassische Runtimeumgebung für Webprojekte mit den benötigten Standardreferenzen und Templates für Microsoft MVC und Microsoft WebAPI 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 im Hauptprojekt als DLL-Klassenbibliothek zu generieren die ClassLibrary-Projekt. 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 unser Plugin.



```
▶ EMailSecurityStep
▶ EMailSecurityStep.Tests
▶ EMailSecurityStepLib
```

6.2.2 Interface - Vertrag mit den Sicherheitsstufen

Für den Endbenutzer startet der Authentifizierungsprozess mit Öffnen der Authentifizierungs-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 Parametern ProjektID und ProviderID mit, ob die Validierung erfolgreich ist. Das MEF-Contracts Interface aller Sicherheitsstufen enthält ausserdem zwei Methoden zur Abfrage und Speicherung individueller Konfiguration der Sicherheitsstufen und die Methode zur Abfrage der Vergleichsparameter.

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 Mockups³

Hier würden ein paar Screenshots gezeigt werden

Der Programmierer kann bei Auswahl der Sicherheitsstufe die Bewertungen vom Auftraggeber in affect AG und die Umfrageergebnisse einsehen.

³Siehe Kapitel Konfigurator Template

```

1 using System.Collections.Generic;
2
3 namespace SecurityStepContract
4 {
5     public interface ISecurityStepInfo
6     {
7         object getConfigParameters(int projectId);
8         string saveConfigParameters(IDictionary<string, string> 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; }
20    }
21 }
22 }
23

```

Abbildung 6.1: ISecurityStep

6.3.2 Authentifizierung-Lightbox mit Sicherheitsstufen

Die Authentifizierung-Lightbox mit Sicherheitsstufen wurde für den Endbenutzer entworfen. Dieses Kapitel zeigt die finalen Screens welche von den Mockups⁴ abgeleitet wurden.

6.4 Implementation Authentifizierung

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 diese jQuery nicht im Authentifizierungsjavascript mitgeliefert.

⁴Siehe Kapitel Authentifizierungs-Lightbox Template ##Testing #Unit-Test Sicherheitsstufe und Authentifizierungsservice Die verschiedenen Sicherheitsstufen können unabhängig geprüft werden. Jede Sicherheitsstufe 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.

```

<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Beispiel Implementation</title>
  <script src="http://iaauth.christianbachmann.ch/include/js/jquery-1.12.3.min.js"></script>
  <script src="http://iaauth.christianbachmann.ch/include/js/lity.js"></script>
  <link type="text/css" rel="stylesheet" href="http://iaauth.christianbachmann.ch/include/css/lity.css" />
</head>
<body>

<h1></h1>
<!--OnClick Event on data-iaauthButton -->
<button data-iaauthButton>GO</button>
<div id="inline">
  <form id="paymentForm" action="https://iaauth.azurewebsites.net/Loading/Home/Validate" target="authframe">
    <input type="hidden" name="projectId" value="30045" />
    <input type="hidden" name="providerId" value="12" />
    <!--Generate sign=mdd5(projectId+providerId+validationCode)-->
    <input type="hidden" name="sign" value="b37b3d4cd7cd8cba3f409f07d6f6d9bd" />
  </form>
</div>
<script type="text/javascript">
$(document).ready(function() {
  var iaauthlightbox = lity();
  iaauthlightbox();
});
</script>

</body>
</html>

```

implementation_lightbox

✓ EMailSecurityStep_Status_INVALID	< 1 ms
✓ EMailSecurityStep_Status_NOTOPEN	< 1 ms
✓ EMailSecurityStep_Status_Update	< 1 ms
✓ EMailSecurityStep_Status_VALID	< 1 ms
✓ Generate_Code_6CharactersLong	< 1 ms
✓ Generate_Code_6CharactersLong	< 1 ms
✓ Generate_Code_IsNumeric	5 ms
✓ Generate_Code_IsNumeric	4 ms
✓ GenerateMailText	< 1 ms
✓ GenerateMailText	< 1 ms
✓ Send_Mail	518 ms

Summary
Last Test Run Failed (Total Run Time 0:00:06)
 ✓ 28 Tests Passed

Abbildung 6.2: Screenshot Unit-Test E-Mail Sicherheitsstufe

7 Studie

7.1 Definition der Begriffe aus 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 Authentifizieren 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 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 andererseits soll die empfundene Anstrengung der Benutzer für das Authentifizieren pro Sicherheitsstufe visualisiert werden.

7.3 Art der Studie

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

7.3.1 Vor - und Nachteile schriftlicher Fragebogen

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

- Die Kosten sind geringer. Hippler ¹ definiert den Richtwert von einem Viertel der Kosten zu einer persönlich-mündlichen oder telefonischen Studie.
- Schriftliche Befragungen mit Fragebogen kann in einem relativ kurzen Zeitraum realisiert werden
- Dem zu Befragenden kann eine grössere Anonymität gegeben werden
- Verteilung in verschiedene Regionen einfach und zeitnah möglich. Insbesondere bei Online Umfrage.
- Einfluss von aussen gering. Zahlreiche Studien² belegen, dass Personen welche eine Studie im Interview die Beantwortung beeinflussen
- Die Antworten der befragten sind durch die Abwesenheit des Interviewers und durch die Anonymität ehrlicher. Dieser Punkt ist wissenschaftlich jedoch noch ziemlich umstritten. Schnell bezweifeln verschiedene Psychologen und Soziologen diesen Umstand. So auch Dr. Reuband in seinem Paper "Möglichkeiten und Probleme des Einsatzes postalischer Befragungen" ³

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

- Wenn eine Studie eine zu grosse Nonresponse-Rate hat, ist eine Verallgemeinerung der Resultate unzulässig. Kurz die Bachelorarbeit würde mit der Studie das Ziel verfehlen. Bei einer schriftlichen Studie kann die Ausfallquote aber nicht im Vorherein 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 Vorherein geplant werden.
- Bestimmte Bevölkerungsteile werden durch diese Art der Studie ausgeschlossen. Zum Beispiel Analphabeten oder bei Onlineumfragen Personen mit zu wenig technischem Know-How oder Hardware.

¹[Hip88]

²Studien und Erklärungen zu Fremdbestimmung durch François Höpflinger[Hö11]

³[Reu01]

7.3.2 Fazit

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, dass Rechnung getragen werden muss um nicht eine ungültige Studie zu erhalten. Damit die Problematik Nonresponse-Rate gering gehalten wird und eine geeignete Umgebung für die Datenerhebungssituation vorhanden ist, gilt es sich weiter den korrekten Aufbau einer Studie zu recherchieren.

7.3.3 Webapplikation für Umfrage

Basierend auf den Empfehlungen⁴ 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 Automatisierung 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”⁵

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 geben. Die folgenden Fragen wurden durch das Institut für webbasierte Kommunikation und E-Learning zusammen getragen [Pra01] und für die Studie dieser Bachelorarbeit beantwortet:

Wer wird befragt?

Mit Absprache des Auftraggebers soll die die Zielgruppe sind Schweizer oder Personen welche in der Schweiz wohnen welche Deutsch sprechen und zwischen 16 und 65 Jahre alt sind sein. Die Angabe begründete der Auftraggeber dadurch, dass sich darin die Hauptzielgruppen seiner Kunden widerspiegelt. Die Teilnehmer sollen die technische Know-How besitzen an einer Interaktivität teilzunehmen und den Internetzugriff haben. Dieses minimale technische Know-How werden sie Beweisen indem sie an der Umfrage teilnehmen können.

⁴Die Universitäten sind offizielle Kunden von umfrageonline.ch

⁵Zitat vom Institut für webbasierte Kommunikation und E-Learning und Gräf et al. 2001 [Pra01]

Was ist der Zweck bzw. das Ziel der Untersuchung?

Die Studie dient dem Programmierer 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 werden ⁶. 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 sollte zur Beginn der Studie genannt werden. Folgend ist das Diagramm aus der Studie von Bosnjak und Batini ⁷ abgebildet. Die Erkenntnis aus der Studie zeigt, dass nicht nur unter dem Motto je kürzer desto besser gehandelt werden sollte. Die Studie ist jedoch schon 15 Jahren alt und ist deshalb differenzierter zu sehen. Die Studie der Bachelorarbeit streben einen Aufwand von 8-12 Minuten an.

⁶[Pra01]

⁷[Bos00]

7.5 Hauptteil/Fragen

Offensichtlich stellt der Hauptteil den Löwenanteil des Aufwands dar.

7.5.1 Erste Frage Theorie

Die erste Frage ist nach Dillman⁸ von grosser Bedeutung. Mit ihr wird Motivation und Einsatz für den ganzen Fragebogen gesetzt. Diese Frage soll als Interesse und Neugier der Befragten bewirken.

Das Institut für webbasierte Kommunikation und E-Learning hat dafür aus verschiedenen Studien die wichtigsten Kriterien für eine erfolgreiche erste Frage zusammen getragen⁹: - **Einfache Formulierung** Der Befragte versteht sofort um was es geht und glaubt daran dass er die Fragen meistern kann - **Kurze Beantwortungszeit, keine offenen Fragen** Ein schnelles Überwinden der ersten "Hürde" motiviert den Teilnehmer - **Angstabbauend** Ängste wie z.B. die des nicht Beantworten können soll abgebaut werden. - **Inhaltlich einführen** Die Frage soll in das Thema einführen und im Idealfall Interesse und Neugier wecken - **Keine Fragen zur Person oder zur Ihrem demographischen Eigenschaften**

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

⁸[Dil78]

⁹[Pra01]

7.7 Theorie Fragen

Fragen sollen eine Funktion übernehmen. Dabei schlägt Kleber¹⁰ folgende Klassifizierung vor:

- Übergangs- und Vorbereitungsfragen für Themenwechsel, - Ablenkungs- und Pufferfragen zur Minderung von Ausstrahlungseffekten, - Filterfragen zum Übergehen von eventuell irrelevanten Fragen, - Rangier- und Konzentrationsfragen zum Auflockern langer Darstellungen, - Motivationsfragen zur Stärkung des Selbstvertrauens und Verminderung von Hemmungen, - Kontrollfragen als Wahrheitskontrolle der Antworten bzw. Sichtbarmachen von Widersprüchen.

Diese Klassifizierung soll helfen den Fragebogen zu gestalten.

Frageart

Bei der Stellung der Frage sollte festgestellt werden welche Art von Frage gestellt wird. Da sich dadurch die Antwort markantlich unterscheidet. Folgende 3 Hauptgruppen gibt es - **Einstellungsfragen** Dieser Fragestellung bezieht sich auf "Wunschbarkeit oder negativen bzw. Beurteilung", den Befragte mit bestimmten Statements verbinden. - **Verhaltensfragen** Dabei wird direkt auf das Verhalten des Befragten Bezug genommen. Dabei muss beachtet werden, dass der Befragte sein Verhalten selbst beschreibt. Einerseits entspricht die Selbstwahrnehmung der Teilnehmer teilweise nicht der Realität andererseits 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.

Fragetypen

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 Teilnehmer kann sich 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 die Frage ist hoch. Auswahlmöglichkeiten für die Antwort könnten irrelevant sein.

¹⁰[Hip92]

7.8 Fragen über Akzeptanz

Es wird die folgende Hypothesen verfolgt: “Die Akzeptanz von Sicherheitsstufe ist nicht beständig. Sie ist abhängig von den Bedienungen der Interaktivität: Seriosität des Anbieters, Wichtigkeit der Umfrage und möglicher Verdienste bei der Teilnahme” Der Programmier soll bei der Konfiguration das Umfeld der Interaktivität kategorisieren können. Die Hauptbereiche sind aus der Aufgabenstellung entnommen. Die anderen Kategorisierungen ergeben sich aus der Thesis.

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

Aus jeder Kategorie wird in der Studie erfragt welche Sicherheitsstufen eingesetzt der Umfrageteilnehmer einsetzen würde. Es wird pro Kategorie eine geschlossene Frage gestellt. Der Fragetyp ist Mehrfachauswahl. Die Fragen sind von der Klassifizierung 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? *

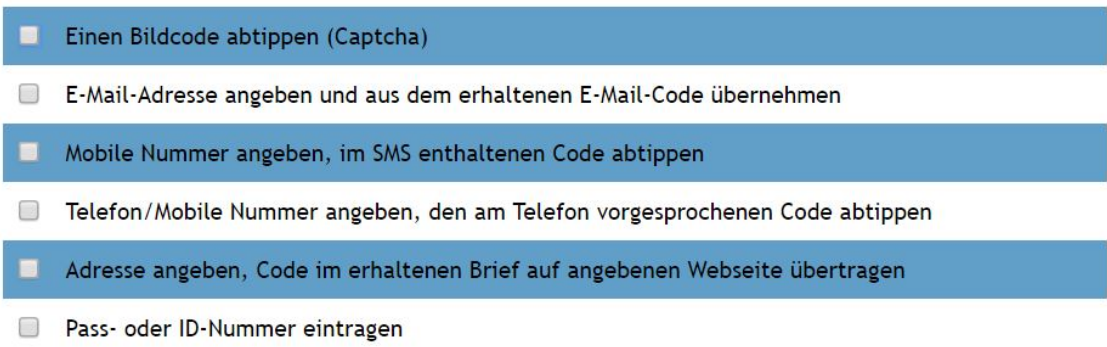
- 
- ☒ Einen Bildcode abtippen (Captcha)
 - ☐ E-Mail-Adresse angeben und aus dem erhaltenen E-Mail-Code übernehmen
 - ☒ Mobile Nummer angeben, im SMS enthaltenen Code abtippen
 - ☐ Telefon/Mobile Nummer angeben, den am Telefon vorgesprochenen Code abtippen
 - ☒ Adresse angeben, Code im erhaltenen Brief auf angegebenen 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 Einstellungsfragen. Der User gibt bewertet seine Einstellung zu den Sicherheitsstufe anhand der Anstrengung.

Wie anstrengend finden Sie die folgenden Authentifizierungstypen? *

	Sehr anstrengend	anstrengend	neutral	angenehm	sehr angenehm	keine Antwort
Einen Bildcode abtippen (Captcha)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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 enthaltenen Code abtippen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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 angebenen Webseite übertragen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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"/>

Abbildung 7.2: Screenshot der Umfrage zur Anstrengung

7.10 Bonus “Frage”, Umgehung der Absicherung

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, mehrfach an einer Umfrage teilzunehmen. Die Hypothese wird aufgestellt, dass ein Teilnehmer mit genügend technischem Know-How insbesondere bei diesem Umfragethema mehrfach teilnehmen wird.

8 Weitere Fragen

Weiter werden die 3 Eigenschaftsfragen gestellt. Dabei soll Alter, Geschlecht und ob es sich um einen Schweizer oder Bewohner der Schweiz handelt angegeben werden.

8.1 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 Untersucher Hinweise zukommen lassen die für die Auswertung und weitere Untersuchungen dienlich sind. Dieser Möglichkeit wird nach der Erfahrung von Reuband¹ gewürdigt.

8.2 Verständlichkeit

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



Abbildung 8.1: Beispiele der Illustrationen für die Umfrage

¹[Reu01]

8.3 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 optimaler für den Enduser seine Konfigurationen wählen. Damit ist das Ziel der Studie erreicht und die Möglichkeit der Auswertung erreicht.

Weiter werden noch einige Anmerkungen zu den Fragen erläutert.

8.3.1 Repräsentativität

Laut Bundesamt für Statistik ist enthält die definierte Zielgruppe 3.3 Millionen Personen². Diese Zahl beinhaltet die Deutschschweizer welche zwischen 16 und 65 Jahre alt sind. An der Umfrage haben 176 Personen teilgenommen. Daraus lässt sich ein 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 8.2: Berechnungsformel für Repräsentativität

n= Strichprobengrösse=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%

8.3.2 Gemogelt an Wettbewerben

Über 65% der Befragten gehen davon aus, dass sie noch nie an einem Wettbewerb teilgenommen haben, an welchem gemogelt hätte können. 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.

8.3.3 Bonus "Frage", Umgehung der Absicherung

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

²[bfs]

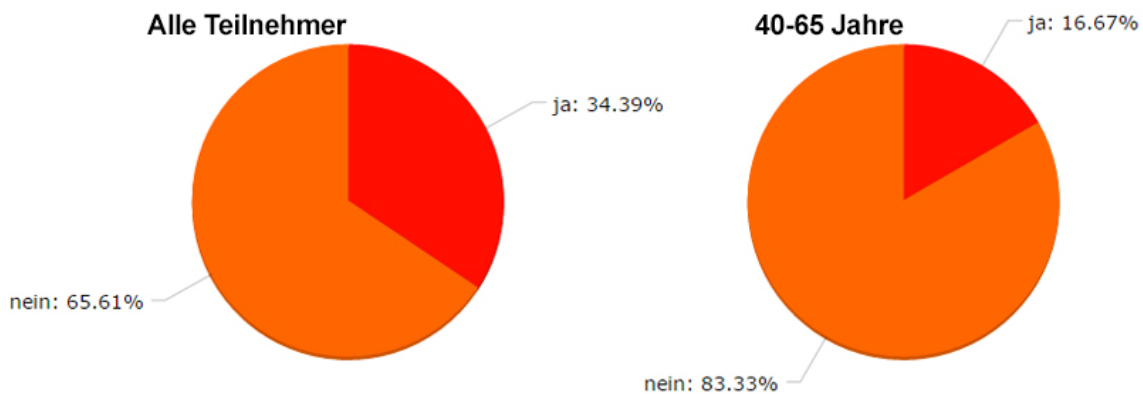
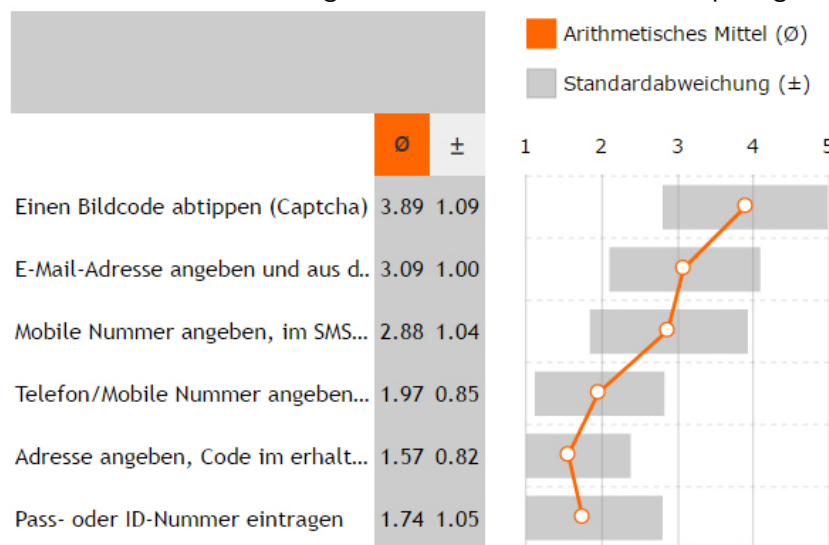


Abbildung 8.3: Ergebnisse Frage zu mögeln an Onlinewettbewerben

8.4 Anstrengung

Auf einer 5 stufigen 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.



8.5 Akzeptanz

Die Hypothese, dass 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 wie 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 Fixnettelefon 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 Anbieter, würden 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 diesem geben kann.

9 Fazit

A Glossar

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

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

CRUD-Operationen CRUD steht für Create, Read, Update, Delete. Diese 4 Operationen sind die Grundlage für alle Interaktionen mit der Datenbank.

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

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

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. System welche die REST Architektur einhalten nennt man RESTful. REST System kommunizieren allgemein über das HTTP-Protokoll und nutzen die gleichen HTTP verbs wie ein Browser der eine Webseite abfragt. Neben GET und POST werden die weniger bekannten Verben PUT und Delete verwendet. Die URI beschreibt die zu beziehende oder verändernde Webresource.

B Verzeichnisse

B.1 Abbildungsverzeichnis

2.1	Screenshot yUML Beispiel Klassendiagramm	11
3.1	Aktive Nutzer Weltweit	15
3.2	Anzahl Schweizer Nutzer	16
3.3	Beispiele von Captchas <i>Quelle:drupal.org</i>	22
3.4	Fingerabdruck Mit Kohlepulver werden Fingerabdrücke sichtbar gemacht und auf Klebefolie gesichert <i>Quelle:phi-hannover.de</i>	26
4.1	Use-Case Diagram	29
4.2	Basis Schablone <i>Quelle Rupp</i>	34
4.3	Erweiterte Schablone <i>Quelle Rupp</i>	34
4.4	Risikomatrix	43
5.1	Übersicht der Hauptkomponenten	45
5.2	Aufbau Inhalt im Card-Design	47
5.3	Differenziertes Domänenmodell des Authentifizierungsservice	48
5.4	Nutzungsanteil CMS weltweit <i>Quelle:de.statista.com</i>	50
5.5	Nutzungsanteil Zahlungsablauf Webshop mit Datatrans <i>Quelle:datatrans</i>	53
5.6	Datatrans Lightbox Integration <i>Quelle:datatrans</i>	54
5.7	Vereinfacht die Architektur des Managed Extensibility Framework <i>Quelle:msdn.microsoft.com</i>	61
5.8	UML Library Overview	62
5.9	Mockup Konfigurator Template Desktop	63
5.10	Mockup Konfigurator Template Mobile	64
5.11	Aufbau Inhalt im Card-Design	65
5.12	Aufbau Inhalt im Card-Design	66
5.13	Aufbau Inhalt im Card-Design	67
6.1	ISecurityStep	74
6.2	Screenshot Unit-Test E-Mail Sicherheitsstufe	75
7.1	Screenshot einer Akzeptanzfrage	82
7.2	Screenshot der Umfrage zur Anstrengung	83

8.1	Beispiele der Illustrationen für die Umfrage	84
8.2	Berechnungsformel für Repräsentativität	85
8.3	Ergebnisse Frage zu mogeln an Onlinewettbewerben	86

B.2 Quellenverzeichnis

- [10m] *10minutemail.com*. <http://www.10minutemail.com>. [Online; accessed 28-02-2016]. 2016.
- [Aut] <http://authentifizierung.org>. <http://authentifizierung.org/>. [Online; accessed 23-12-2015]. 2015.
- [Bos00] Michael Bosnjak. *Internet für Psychologen*. Hogrefe Verlag, 2000. ISBN: 978-3801712266.
- [Bur12] Stacey Burling. *CAPTCHA: The story behind those squiggly computer letters*. <http://phys.org/news/2012-06-captcha-story-squiggly-letters.html>. [Online; accessed 22-12-2015]. 2012.
- [Car] *A Serious Look At Card Based Design*. <http://webdesignledger.com/card-based-design/>. [Online; accessed 04-03-2016]. 2014.
- [Cne] *Two-factor authentication: FAQ*. <http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>. [Online; accessed 28-02-2016]. 2016.
- [Data] *Datrans eCom - Technical Implementation Guide*. https://pilot.datrans.biz/showcase/doc/Technical_Implementation_Guide.pdf. [Online; accessed 22-02-2016]. 2016.
- [Datb] *Webshop*. <https://www.datrans.ch/de/e-payment/shop-schnittstellen>. [Online; accessed 21-02-2016]. 2016.
- [Dil78] Don A. Dillman. *Mail and telephone surveys. The total design method*. New York: John Wiley & Sons Inc, 1978. ISBN: 978-0471215554.
- [Dud] *Duden*. Vol. 26. Dudenredaktion, 2014. ISBN: 978-3-411-04650-8.
- [Gooa] *Google Business*. <https://www.google.com/business/>. [Online; accessed 02-03-2016]. 2016.
- [Goob] *reCAPTCHA Digitization Accuracy*. <http://www.google.com/recaptcha/digitizing>. [Online; accessed 10-01-2015]. 2014.
- [Gooc] *So verwendet Google Cookies*. <https://www.google.ch/intl/de/policies/technologies/cookies>. [Online; accessed 08-01-2016]. 2016.
- [Han15] Filip Hanik. *Kiss*. <https://people.apache.org/~fhanik/kiss.html>. [Online; accessed 29-12-2015]. 2015.
- [Hau06] Matthias Hausherr. *Design By Contract in Java*. <http://www.gruntz.ch/courses/sem/ws06/DBC.pdf>. [Online; accessed 10-03-2016]. 2006.
- [Hip88] Hans-Jürgen Hippler. *Methodische Aspekte schriftlicher Befragungen: Probleme und Forschungsperspektiven*. 1988.

-
- [Hip92] Hans-Jürgen Hippler. *Diagnostik in pädagogischen Handlungsfeldern*. Weinheim, München: Juventa Verlag, 1992.
- [HM16] Edward Hieatt and Rob Mee. *Repository*. <http://martinfowler.com/eaaCatalog/repository.html>. [Online; accessed 05-03-2016]. 2016.
- [Hö11] François Höpflinger. *Standardisierte Erhebungen - methodische Hinweise zu Umfragen*. <http://www.hoepflinger.com/fhtop/Umfragemethodik.pdf>. [Online; accessed 11-02-2016]. 2011.
- [Int15] Goldbach Interactive. *Nutzerzahlen der wichtigsten Plattformen*. <https://twitter.com/revogt/>. [Online; accessed 28-12-2015]. 2015.
- [Kir05] Alexander Kirk. *IP Adresse*. <http://www.computerlexikon.com/begriff-ip-adresse>. [Online; accessed 08-01-2016]. 2005.
- [KS09] Walter Kriha and Roland Schmitz. *Sichere Systeme*. Xpert.press. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. ISBN: 978-3-540-78958-1.
- [Mei] *Projektmanagement: Definitionen, Einführungen und Vorlagen*. <http://projektmanagement-definitionen.de/glossar/meilenstein/>. [Online; accessed 24-12-2015]. 2015.
- [Mil15] Sven Millischer. *Die digitale Revolution*. handelszeitung.ch/digitalisierung/hz-sonderausgabe-die-digitale-revolution-874557. [Online; accessed 02-01-2016]. 2015.
- [MSD15a] MSDN. *Einführung in die Programmiersprache C# und in .NET Framework*. <https://msdn.microsoft.com/de-de/library/z1zx9t92.aspx>. [Online; accessed 01-02-2016]. 2015.
- [MSD15b] MSDN. *Entity Framework*. <https://msdn.microsoft.com/de-ch/data/ef.aspx>. [Online; accessed 01-02-2016]. 2015.
- [Net] *NET-Matrix-Audit*. <http://netreport.net-matrix.ch/audit/>. [Online; accessed 02-01-2016]. 2015.
- [New06] Ted Neward. *The Vietnam of Computer Science*. <http://blogs.tedneward.com/post/the-vietnam-of-computer-science/>. [Online; accessed 10-03-2016]. 2006.
- [Pla] *PlayBuzz*. <http://www.playbuzz.com>. [Online; accessed 28-12-2015]. 2015.
- [Pra01] Axel Pratzner. *Wissenschaftlich fundierter Aufbau von Fragebogen*. Institut für webbasierte Kommunikation und E-Learning, 2001.
- [Reu01] Prof. Dr. Karl-Heinz Reuband. *Möglichkeiten und Probleme des Einsatzes postalischer Befragungen*. 2001.
- [Rot15] Mike Rothman. *Default Deny*. <https://securosis.com/blog/network-security-fundamentals-default-deny>. [Online; accessed 29-12-2015]. 2015.
- [Rou15] Margaret Rouse. *Authentifizierung - Definition*. <http://www.searchsecurity.de/definition/Authentifizierung>. [Online; accessed 23-12-2015]. 2015.
- [Rup11] K. P. Rupp. *Basiswissen Requirements Engineering*. dpunkt.verlag, 2011.
- [San14] Panda Sandeep. *AngularJS Novice to Ninja*. Sitepoint Pty. Ltd., 2014.
- [Smi] *SMI (SocialMedia Institute)*. <http://socialmedia-institute.com/>. [Online; accessed 28-12-2015]. 2015.
-

-
- [Son13] Bernhard Sondereggerl. *Der Fingerabdruck*. Bern, Nussbaumstrasse 29: Bundesamt für Polizei fedpo, 2013.
- [Staa] *Statistik Plattform*. <http://de.statista.com/>. [Online; accessed 28-12-2015]. 2015.
- [Stab] *Top 10 CMS November 2015*. <http://de.statista.com/statistik/daten/studie/320685/umfrage/nutzungsanteil-der-content-management-systeme-cms-weltweit/>. [Online; accessed 21-01-2016]. 2015.
- [Stac] *Usage of content management systems for websites*. http://w3techs.com/technologies/overview/content_management/all. [Online; accessed 01-12-2015]. 2015.
- [Ste12] Olaf Stern. *Reglement Bachelorarbeit*. Zürcher Hochschule für Angewandte Wissenschaften, 2012.
- [T3n] *Interview mit Shaul Olmert*. https://www.youtube.com/watch?v=X_fQ1uG9rFY. [Online; accessed 28-12-2015]. 2015.
- [Uve] *NET-Matrix-Audit*. news.admin.ch/message/index.html?lang=de&msgid=13600. [Online; accessed 06-01-2016]. 2004.
- [w3t16] w3techs. *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]. 2016.
- [Xpa] *Technical Details on Microsoft Product Activation for Windows XP*. <https://technet.microsoft.com/en-us/library/bb457054.aspx>. [Online; accessed 02-03-2016]. 2001.

B.3 Tabellenverzeichnis

2.1	Soll/Ist Analyse	7
2.2	Meilensteine	8
2.3	Termine der Bachelorarbeit	9
5.1	Recherche PlugIn's	51
5.2	Parameter Authentifizierungsservice Lightbox	56
5.3	Übersicht der Authentifizierungs Methoden	58

C Danksagung

D Personalienblatt

Name, Vorname Bachmann, Christian Adresse Bahnhofstrasse 2 Wohnort 8355 Aadorf Geboren
5. September 1986 Heimatort Feusisberg

E Bestätigung

Hiermit bestätigt der Unterzeichnende, dass die Bachelorthesis mit dem Thema “Individuell Konfigurierbarer Authentifizierungsservice für Votings und Wettbewerb” gemäss freigegebener Aufgabenstellung ohne jede fremde Hilfe im Rahmen der gültigen Reglements selbständig 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 10.05.2016

Christian Bachmann