



## Bachelorarbeit (Informatikingenieurwesen)

### Individuell Konfigurierbarer Authentifizierungsservice für Votings und Wettbewerbe

<b>Autor</b>	Christian Bachmann
<b>Betreuung</b>	Jaime Oberle
<b>Auftraggeber</b>	inaffect AG
<b>Datum</b>	23.12.2015

# Inhaltsverzeichnis

<b>I. Präambel</b>	<b>2</b>
<b>1. Einführung</b>	<b>3</b>
1.1. Motivation und Fragestellung . . . . .	3
<b>2. Recherche</b>	<b>4</b>
2.1. Fachbegriffe . . . . .	4
2.2. Erläuterung der Grundlagen . . . . .	4
2.2.1. Authentifizierung . . . . .	4
2.2.2. Autorisierung . . . . .	4
2.2.3. Captcha . . . . .	4
2.2.4. OAuth . . . . .	6
2.3. Ähnliche Produkte auf dem Markt . . . . .	7
2.3.1. OAuth-Provider . . . . .	7
<b>3. Grundlagen</b>	<b>10</b>
3.1. Basisbegriffe . . . . .	10
3.1.1. Authentifizierung . . . . .	10
3.1.2. Autorisierung . . . . .	10
<b>4. Glossar</b>	<b>11</b>
<b>5. Verzeichnisse</b>	<b>12</b>
5.1. Abbildungsverzeichnis . . . . .	12
5.2. Quellenverzeichnis . . . . .	13
5.3. Tabellenverzeichnis . . . . .	14

**Teil I.**

# **Einleitung und Abgrenzung**

# **1. Einführung**

## **1.1. Motivation und Fragestellung**

Der Zugriff auf Services und Medien mittels mobiler Geräte steigt beständig an. So ist im Mai 2014, 60% der Zeit, die online verbracht wird, über Handy und Tablet zugegriffen worden - davon 51% mittels mobiler Applikationen. (Lipsman 2014)

## 2. Recherche

### 2.1. Fachbegriffe

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

### 2.2. Erläuterung der Grundlagen

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

#### 2.2.1. Authentifizierung

Authentifizierung - beglaubigen, die Echtheit von etwas bezeugen verfolgt das Ziel (*Duden* 2014)

Eine Person oder Objekt eindeutig zu **authentifizieren** bedeute zu ermitteln ob die oder derjenige auch der ist als welcher er sich ausgibt. (Rouse 2015) 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 Mobiletelefon häufig verbreitet. Die Möglichkeiten der Authentifizierung nahe zu grenzenlos. ("[Http://authentifizierung.org](http://authentifizierung.org)" 2015)

#### 2.2.2. Autorisierung

Autorisierung - Befugnis, Berechtigung, Erlaubnis, Genehmigung (*Duden* 2014)

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

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

#### 2.2.3. Captcha

Captcha - Test, mit dem festgestellt werden kann, ob sich ein Mensch oder ein Computer eines Programms bedient (*Duden* 2014)

Im Jahre 2000 wurde das Captcha an der Carnegie Mellon University erfunden. Captcha steht für **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. Luis von Ahn, Professor der Entwickler-Gruppe, erklärte die Dringlichkeit von Captcha damals so: "Anybody can write a program to sign up for millions of accounts, and the idea was to prevent that". (Burling 2012)

### Captcha Zahlen

In 2014 wurden 200 Million Captchas pro Tag eingegeben. Dabei braucht ein User durchschnittlich 10 Sekunden das entspricht 500'000 Stunden.<sup>1</sup>

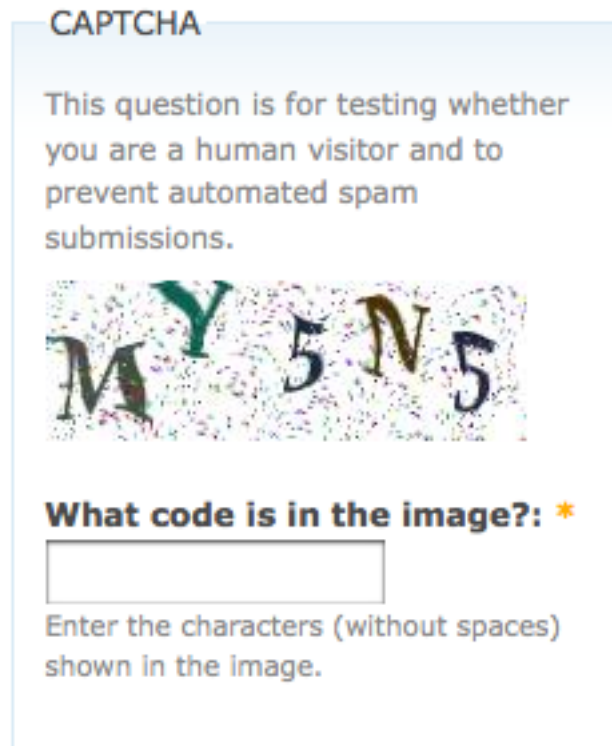


Abbildung 2.1.: Beispiele von Captchas *Quelle:drupal.org*

<sup>1</sup>Die statistischen Daten wurden von Google 2014 in ihrem Blog publiziert ("ReCAPTCHA Digitization Accuracy" 2014)

### 2.2.4. OAuth

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

#### Das Bedürfnis nach OAuth

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

#### Funktionalität von OAuth

Ein Programm/API (Consumer) stellt über das OAuth-Protokoll einem Endbenutzer(User) Zugriff (Autorisierung) auf seine Daten/Funktionalitäten zur Verfügung. Dieser Zugriff wird von einem anderen Programm (Service) gemanagt. Das Konzept ist nicht generell neu. OAuth ist ähnlich zu Google Auth-Sub, aol OpenAuth, Yahoo BBAuth, Upcoming api, Flickr api, Amazon Web Services api. OAuth studierte die existierenden Protokolle und standardisierte und kombinierte die existierende industriellen Protokolle. Der wichtigste Unterschied zu den existierenden Protokollen ist, dass OAuth sowohl offen ist und andererseits zu einem Standard geworden ist. Jeden Tag entstehen neue Webseiten welche neue Funktionalitäten und Services offeriert und dabei Funktionalitäten von anderen Webseiten braucht. OAuth stellt dem Programmierer einerseits eine standardisierte Implementierung zur Verfügung. Der Endbenutzer erhält dank dieses Protokolls die Möglichkeit Teile seiner Funktionalität/Daten bei einem anderen Anbieter zur Verfügung zu stellen. So kann der Endbenutzer bei der Facebook OAuth z.B. 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.net](http://oauth.net)<sup>1</sup>

## 2.3. Ähnliche Produkte auf dem Markt

Dieses Unterkapitel erläutert existierenden Produkte auf dem Markt.

### 2.3.1. OAuth-Provider

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

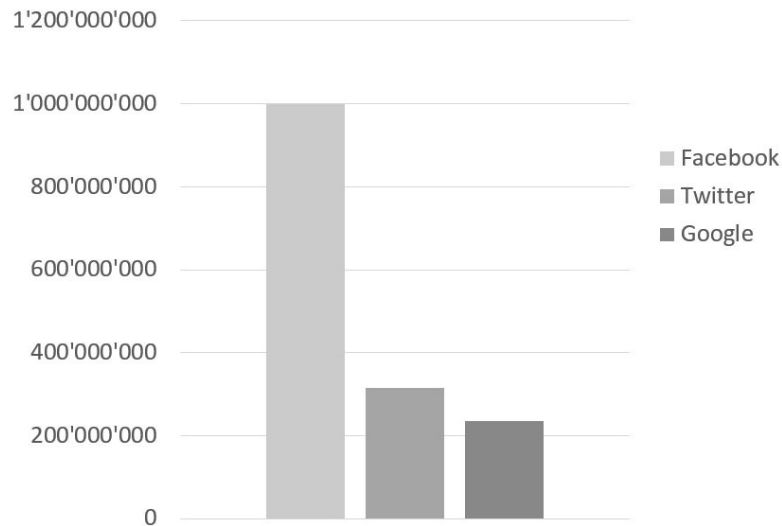


Abbildung 2.2.: Aktive Nutzer Weltweit<sup>2</sup>

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

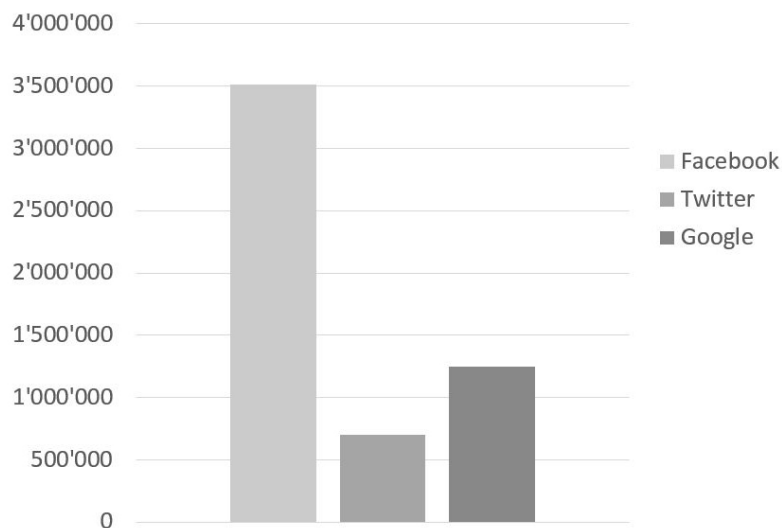


Abbildung 2.3.: Anzahl Schweizer Nutzer<sup>3</sup>

<sup>2</sup>Das Statistik wurde basierend auf den Daten von socialmedia-institute ("SMI (SocialMedia Institute)" 2015) erstellt. Facebook und Twitter Daten sind am 5. November 2015 und die Google Daten sind im 2014 erhoben worden.

<sup>3</sup>Das Statistik wurde basierend auf den Daten von Goldbach Interactive (Interactive 2015) generiert. Die Daten sind im März 2015 erhoben.



**Vorteile**

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 einen Abgleich der verschiedenen OAuth Provider wird vom OAuth-Protokoll nicht zur Verfügung gestellt. 22% der Bevölkerung müsste sich vor Nutzung noch registrieren. Die Implementierung ist trotz vielen Libraries nicht ohne tiefere Programmierkenntnisse möglich.

This is just a sample. You can play around with your own text right here.

...is really just ordinary text, *plain and simple*. How is it good for you?

- You just **type naturally**, and the result looks good.
- You **don't have to worry** about clicking formatting buttons.
- Or fiddling with indentation. (Two spaces is all you need.)

To see what else you can do with Markdown (including **tables**, **images**, **numbered lists**, and more) take a look at the Cheatsheet. And then try it out by typing in this box!

Right	Left	Center	Default
12	12	12	12
123	123	123	123
1	1	1	1



Abbildung 2.4.: This is the caption

Test	test2	saleti
olé	Thats the way	

This is the day

## **3. Grundlagen**

Dieses Kapitel erläutert die Grundlagen. Ein grosser Teil der Arbeit stützt sich auf den Grundlagen ab (Meier 2010, 7:105)

### **3.1. Basisbegriffe**

#### **3.1.1. Authentifizierung**

#### **3.1.2. Autorisierung**

Saleti

## 4. Glossar

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

**Node** Node oder Node.js ist eine Plattform welche es erlaubt JavaScript serverseitig auszuführen. <https://nodejs.org/>

**RPC** Remote Procedure Call ist eine Technologie um Funktionsbausteine in einem anderen Prozess aufzurufen.

**Jasmine** Jasmine ist ein verhaltensbasiertes Testframework für JavaScript. <http://jasmine.github.io>

**Karma** Karma ist ein Testrunner-Framework zur kontinuierlichen Ausführung von UnitTests. <http://karma-runner.github.io>

**Mocks** Mocks sind Code-Attrappen, die es ermöglichen, noch nicht vorhandene oder nicht verfügbare, Funktionalitäten und Objekte zu simulieren. <http://de.wikipedia.org/wiki/Mock-Objekt>

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

# 5. Verzeichnisse

Neues Verzeichnisse

## 5.1. Abbildungsverzeichnis

2.1. Beispiele von Captchas <i>Quelle:drupal.org</i> . . . . .	5
2.2. Aktive Nutzer Weltweit . . . . .	7
2.3. Anzahl Schweizer Nutzer . . . . .	7
2.4. This is the caption . . . . .	9

## 5.2. Quellenverzeichnis

### 5.3. Tabellenverzeichnis

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

Duden. 2014. Vol. 26. Dudenredaktion.

"[Http://authentifizierung.org](http://authentifizierung.org)." 2015. <http://authentifizierung.org/>.

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

Lipsman, Andrew. 2014. "Major Mobile Milestones in May: Apps Now Drive Half of All Time Spent on Digital." [http://www.comscore.com/Insights/Blog/Major-Mobile-Milestones-in-May-Apps-Now-Drive-Half-o](http://www.comscore.com/Insights/Blog/Major-Mobile-Milestones-in-May-Apps-Now-Drive-Half-of)

Meier, Andreas. 2010. *Relationale Und Postrelationale Datenbanken*. Vol. 7. EXamen.pressSpringerLink. Berlin, Heidelberg: Springer Berlin Heidelberg.

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

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

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