



---

# Vollständige Verifizierbarkeit des Genfer E-Voting Systems

Bachelorthesis

Studiengang:	Informatik
Autor/in:	Christian Wenger
Betreuer/in:	Dr. Rolf Haenni
Auftraggeber/in:	[Auftraggeber/in einfügen]
Experten:	Thomas Hofer
Datum:	25.09.18

## Management Summary

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue dui dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit.

# Inhaltsverzeichnis

1	Einleitung	4
2	Überschrift 1	5
	2.1 Überschrift 2	5
	2.2 Überschrift 2	5
3	Überschrift 1	5
	3.1 Überschrift 2	5
	3.1.1Überschrift 3	5
	3.1.1.1 Überschrift 4	5
	3.1.1.1.1 Überschrift 5	5
4	Harum as enimusfuga	6
5	Schlussfolgerungen/Fazit	7
6	Abbildungsverzeichnis	8
7	Tabellenverzeichnis	8
8	Glossar	8
9	Literaturverzeichnis	8
10	Anhang	9
11	Selbständigkeitserklärung	10

# 1 Einleitung

Das Internet ist heute aus unserem Leben nicht mehr wegzudenken. Wir kaufen online ein, holen von Google was wir wissen wollen, ja sogar unser Bewerbungen können wir damit verschicken. Dieser Fortschritt machte auch keinen Halt vor der Politik. So begann das Parlament im Jahr 2002 mit den Vorbereitungen für die elektronische Stimmabgabe kurz E-Voting. Zurzeit gibt es zwei vorhandene Systeme. Einmal jenes des Kanton Genf (CHVote) und dasjenige der Schweizerischen Post. Ein grosses Problem dieser Systeme ist die vollständige Nachvollziehbarkeit der einzelnen Schritten. Die sogenannte vollständige Verifizierbarkeit ist ein Kernelement der bundesrechtlichen Sicherheitsanforderungen.

## 2 Projektmanagement

In diesem Kapitel werden die verschiedenen Schritten der Projektplanung erläutert. Dies beinhaltet die Methodik, die Anforderungen und Anwendungsfälle sowie der Zeitplan

Da es sich hierbei um ein Einmann-Projekt handelt, bietet sich eine agile Methodik an. Es wurde aber kein richtiges Modell wie «SCRUM» gewählt, da dies den Rahmen dieses Projektes sprengen würde. Es wurde entschieden sich alle 2 Wochen zu Treffen und den aktuellen Stand zu präsentieren, sowie die nächsten Schritte zu besprechen.

### 2.1 Anforderungen

In einem ersten Schritt galt es den Rahmen der Applikation zu bestimmen. Dazu muss abgeklärt werden, was die Applikation können muss. Dies wurde vom Studierenden definiert und vom Betreuer genehmigt.

#### 2.1.1 Allgemeine Anforderungen

ID	Beschreibung	Priorität	Status
A.1	Alle Tests von der Projektarbeit 2 sind nach Definition implementiert.	Muss	Geprüft
A.2	Die bestehende Applikation zur Visualisierung des Genfer E-Voting-System wird mit dem Verifier vervollständigt	Muss	Geprüft
A.3	Eine Konsolenanwendung, um die Tests lokal auszuführen, wird entwickelt. Dazu ist eine Schnittstelle zur bestehenden Applikation nötig.	Kann	Geprüft
A.4	Die Applikation kann in Deutsch, Englisch und Französisch genutzt werden	Kann	Geprüft
A.5	Ein Script für die Generierung der Abstimmungsdaten einer Volksabstimmung wird entwickelt.	Kann	Geprüft

#### 2.1.2 Verifier Visualisierung

ID	Beschreibung	Priorität	Status
A.6	Der Benutzer muss jederzeit nachvollziehen können, wie viel der Verifier schon getestet hat und bei welchem Test er gerade ist.	Muss	Geprüft
A.7	Der Benutzer erhält am Ende der Tests einen Überblick, welche Tests erfolgreich waren und welche nicht.	Muss	Geprüft
A.8	Im Überblick gibt es die Möglichkeit zu jedem Test detaillierte Informationen anzuzeigen	Muss	Geprüft
A.9	Der Benutzer kann das Ergebnis als PDF exportieren	Kann	Geprüft

## 2.2 Zeitplan und Meilensteine

Im nächsten Schritt wurde der Zeitplan und die Meilensteine definiert

Folgende Meilensteine wurden anhand der Anforderungen definiert

- M1: Projekt Initialisierung ist fertig / Es können nun Anpassungen an der Bestehenden Applikation gemacht werden.
- M2: Implementation der Tests in Python ist Abgeschlossen
- M3: Die GUI-Programmierung ist Abgeschlossen
- M4: Das Backend ist mit dem Frontend verknüpft / Alle Muss-Kriterien sind erfüllt
- M5: Alle Kann-Kriterien wurden erfüllt.
- M6: Dokumentation ist abgeschlossen

### 3 Schlussfolgerungen/Fazit

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit.

## 4 Abbildungsverzeichnis

Abbildung 1: Et ut aut isti repuditis qui ium	6
-----------------------------------------------	---

## 5 Tabellenverzeichnis

Tabelle 1: Et ut aut isti repuditis qui ium	6
---------------------------------------------	---

## 6 Glossar

<b>Auinweon</b>	
Et ut aut isti repuditis qui ium	7
<b>Batnwpe</b>	
Et ut aut isti repuditis qui ium	9
<b>Cowoll</b>	
Et ut aut isti repuditis qui ium	11

## 7 Literaturverzeichnis

<b>Literatureintrag</b>	
<i>Autorname, Autorvorname, Buchtitel, Verlag, Ort, Ausgabe, Jahr</i>	7
<b>Literatureintrag</b>	
<i>Autorname, Autorvorname, Buchtitel, Verlag, Ort, Ausgabe, Jahr</i>	9
<b>Literatureintrag</b>	
<i>Autorname, Autorvorname, Buchtitel, Verlag, Ort, Ausgabe, Jahr</i>	11



## 8 Anhang

Et ut aut isti repuditis qui ium nonsecturia quis incientiae laborem elliquis et quatur, sitiur aut od moluptatur aut ea consequere peri sim erro essequisit remporia dem et landi dest, cone poris quunt volecab ipidero quatur ad quibusamus.

## 9 Selbständigkeitserklärung

Ich bestätige, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Textstellen, die nicht von mir stammen, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen.

Ort, Datum:

Unterschrift: