

Die SuisseID als Unterstützung für E-Voting

Eine Analyse der Möglichkeiten und Handlungsoptionen

Bachelor Thesis

eingereicht im Studiengang

Datum der Einreichung

Modul

Verfasst von:

Bachelor in Wirtschaftsinformatik

Bern, den 13.05.2011

BTHW (Bachelor Thesis)

Pascal Müller

Erstgutachter/in:

Zweitgutachter/in:

Dr. Alessia Neuroni

Prof. Dr. Eric Dubuis

Inhaltsverzeichnis

MANAGEMENT SUMMARY	4
1 EINLEITUNG IN BACHELOR THESIS	5
1.1 Grundgedanke der Bachelor Thesis.....	5
1.2 Problemstellung.....	5
1.3 Zielsetzung	5
1.4 Methodik und Aufbau der Arbeit.....	5
1.4.1 Ausgangslage.....	5
1.4.2 Analyse von E-Voting Projekten.....	6
1.4.3 Folgerungen.....	6
1.5 Projektabgrenzung	6
1.6 Meilensteine	6
1.7 Projektorganisation.....	7
2 AUSGANGSLAGE	8
2.1 SuisseID	8
2.1.1 Einführung	8
2.1.2 Analyse der Stärken und Schwächen von SuisseID	13
2.1.3 Qualitativer Nutzen für die Benutzer und Unternehmen	18
2.1.4 Quantitativer (finanzieller) Nutzen für die Benutzer und Unternehmen.....	18
2.2 E-Voting.....	19
2.2.1 Einführung	19
2.2.2 Analyse der Stärken und Schwächen von E-Voting.....	24
2.2.3 Qualitativer Nutzen für die Benutzer und Verwaltungen	30
2.2.4 Quantitativer (finanzieller) Nutzen für die Benutzer und Verwaltungen	31
3 ANALYSE VON E-VOTING PROJEKTEN	32
3.1 Gemeinsamkeiten & Unterschiede zwischen den E-Voting Projekten.....	32
3.2 Beispielprozess für E-Voting	33
3.3 Beurteilung des Beispielprozesses	37
4 KOMBINATION VON SUISEID MIT E-VOTING	40
4.1 Einführung	40
4.2 Beispielprozess einer Kombination von SuisseID mit E-Voting	42
4.3 Vergleich zum ursprünglichen E-Voting Beispielprozess.....	43
4.4 Analyse des Beispielprozesses einer Kombination von SuisseID mit E-Voting.....	43
4.4.1 Nutzenanalyse einer Kombination von SuisseID mit E-Voting.....	43
4.4.2 Risikoanalyse einer Kombination von SuisseID mit E-Voting	44

5	FOLGERUNGEN.....	46
5.1	Problemfelder von E-Voting	46
5.1.1	<i>Problemfelder ohne Einsatz von SuisseID</i>	<i>46</i>
5.1.2	<i>Problemfelder mit Einsatz von SuisseID</i>	<i>46</i>
5.2	Mögliche Optimierungsmassnahmen für E-Voting.....	49
5.2.1	<i>Mit SuisseID oder ähnlichen Konzepten</i>	<i>49</i>
5.2.2	<i>Ohne SuisseID.....</i>	<i>50</i>
5.3	Beispielprozess bei Integration der Massnahmen	53
5.4	Prozessvergleich mit ursprünglichen Beispielprozessen	55
5.5	Schlusswort	56
	LITERATURVERZEICHNIS	57
	Bücher	57
	Internet.....	57
	Interviews.....	59
	ABBILDUNGSVERZEICHNIS	60
	TABELLENVERZEICHNIS	60
	ABKÜRZUNGSVERZEICHNIS.....	61
	ANHANG A: INTERVIEWBÖGEN.....	63
	Interview mit Herrn Bernold.....	63
	Interview mit Herrn Hassenstein	66
	Interview mit Denis Simonet.....	68
	Interview mit Annina Weber und Daniel Muster	71
	Interview mit Stefan Thöni	74
	Interview mit Vito Vizarro.....	74
	ANHANG B: ZUSAMMENFASSUNG DER DREI E-VOTING PROJEKTE	76
	E-Voting Projekt im Kanton Zürich	76
	E-Voting Projekt im Kanton Neuenburg	79
	E-Voting Projekt im Kanton Genf	82
	SELBSTÄNDIGKEITSERKLÄRUNG	85

Management Summary

Folgende Bachelor Thesis befasst sich mit der Frage, ob und wie die SuisseID als Unterstützung für E-Voting eingesetzt werden kann und wurde in die Blöcke Ausgangslage, Analyse von E-Voting Projekten und Folgerungen gegliedert.

Seit 2002 werden in der Schweiz E-Voting Pilot-Projekte im Rahmen von Vote électronique durchgeführt. Die drei Pionierkantone sind die Kantone Zürich, Genf und Neuenburg. Vote électronique beinhaltet verschiedene Aspekte, wobei E-Voting nur ein Teilaspekt davon ist. Die Pilot-Projekte verliefen meistens ohne grössere Probleme. Allerdings wurden die Punkte Transparenz, Anonymität und Sicherheit nicht in gleichem Masse erfüllt.

Die SuisseID ist der erste elektronische Identitätsnachweis und kann beispielsweise für Logins oder für digitale Unterschriften eingesetzt werden.

Eine Kombination von E-Voting mit der SuisseID bringt jedoch keine Verbesserung von E-Voting, weil die SuisseID nur am Rande als Unterstützung für E-Voting eingesetzt werden kann. Da der Stimmrechtsausweis nicht online zur Verfügung gestellt wird, weil zudem diverse Sicherheitsrisiken vorhanden sind und weil in der Schweiz aus strategischen Gründen kein Gesamtschweizerisches E-Voting System geplant ist, überwiegen die Nachteile einer Kombination den Vorteilen. Nur für ein Login auf das E-Voting System eignet sich die SuisseID. Da kein Gesamtschweizerisches E-Voting System geplant ist und zudem die Organisation und die Durchführung der Wahlen bei den Kantonen liegen, macht auch eine Optimierung respektive eine Definition eines idealen E-Voting Beispielprozesses aus den bisherigen E-Voting Prozessen der Pionierkantone wenig Sinn.

Auslandschweizer können nicht an der Urne abstimmen und bei einer brieflichen Abstimmung ist nicht sichergestellt, ob die Stimme tatsächlich in die Schweiz versendet wird. Daher hat E-Voting vor allem für Auslandschweizer den grössten Nutzen. Deshalb liegt der Fokus in den nächsten Jahren bei den Auslandschweizern. Jedem Auslandschweizer eine SuisseID zu überbringen, wäre sehr schwer zu gestalten und ohne Konzepterneuerung / -erweiterung nicht möglich. Dies ist ein weiterer Grund, weshalb eine Kombination wenig Sinn ergibt.

PI-Vote ist das E-Voting System der Piratenpartei und erfüllt die Punkte Transparenz, Anonymität und Sicherheit ideal. Allerdings ist PI-Vote sehr komplex, vor allem wenn es für Wahlen genutzt werden würde. Zudem besitzen die Auszähler / Autoritäten eine enorme Macht. E-Voting muss jedoch vor allem simpel und benutzerfreundlich sein. Da kleine Manipulationen nie ausgeschlossen werden können, müssen vor allem systematische Manipulationen unterbunden werden.

1 Einleitung in Bachelor Thesis

Folgendes Kapitel bietet einen Überblick über den Sinn und Zweck und die Ziele dieser Bachelor Thesis sowie über alle organisatorischen Elemente.

1.1 Grundgedanke der Bachelor Thesis

In den ersten vier Semestern als Wirtschaftsinformatik-Studenten wurde uns viel theoretisches Wissen übermittelt. Danach mussten wir uns für die letzten zwei Semester für eine Vertiefungsrichtung entscheiden. Ich entschied mich für die Vertiefungsrichtung „E-Government & E-Business“. Wir hatten die Vorgabe, dass sich unsere Abschlussarbeit, die Bachelor Thesis, im Gebiet unserer Vertiefungsrichtung bewegen soll. Da ich mich seit dem ersten Semester für das Thema E-Voting interessiere, wollte ich unbedingt meine Bachelor Thesis zu dieser Thematik erarbeiten.

1.2 Problemstellung

E-Voting ist eine relativ neue Technik, welche es Stimmbürgern erlaubt, per Internet abzustimmen oder an Wahlen teilzunehmen. Seit einigen Jahren laufen Pilotprojekte in verschiedenen Kantonen. Trotzdem konnte sich E-Voting noch nicht als Abstimmungskanal durchsetzen, weil es diverse kritische Stimmen und Probleme mit der Transparenz gibt.

Eine SuisseID ermöglicht es Personen Geschäfte online abzuwickeln, da mit der SuisseID eine elektronische Unterschrift möglich ist. Zudem besteht die Möglichkeit sich mit der SuisseID bei einer Applikation einzuloggen.

1.3 Zielsetzung

Die Zielsetzung dieser Bachelor Thesis ist folgende:

„Es soll überprüft werden, inwiefern SuisseID im Kontext von E-Voting-Vorhaben als Unterstützung eingesetzt werden kann.“

1.4 Methodik und Aufbau der Arbeit

Diese Bachelor Thesis ist gemäss Aufgabenstellung in folgende Blöcke gegliedert: Ausgangslage, Analyse von E-Voting Projekten und Folgerungen.

1.4.1 Ausgangslage

Die Ausgangslage behandelt die Grundlagen von E-Voting und SuisseID und zeigt anhand einer Analyse die Stärken und die Schwächen von beiden Themengebieten.

1.4.2 Analyse von E-Voting Projekten

Diverse Kantone führten bereits einige E-Voting Projekte durch. Im November 2010 kommen im Rahmen der eidgenössischen Abstimmung weitere Kantone hinzu. In diesem Block sollen zukünftige oder bereits durchgeführte E-Voting Projekte in der Schweiz untersucht werden. Dieser Block soll auch aufzeigen, welche Elemente sich bei einem Einsatz von SuisseID verändern, welcher Nutzen für die Stimmbürger und für die Verwaltungen dabei entsteht und welche Schwachstellen dabei verschwinden oder neu in Erscheinung treten.

1.4.3 Folgerungen

Im letzten Block erfolgen Vorschläge für Massnahmen zur Optimierung eines E-Voting Systems. Zusätzlich wird eine persönliche Einschätzung zur Thematik abgegeben.

1.5 Projektabgrenzung

Die Implementierung eines E-Voting Systems gehört nicht zur Aufgabenstellung. Ebenso wird auf eine technische Entwicklung und Spezifikation eines E-Voting Systems verzichtet. Es findet keine direkte Beteiligung an einem E-Voting Projekt statt. Allerdings muss Kontakt mit den entsprechenden Ämtern und Projektleitern aufgenommen werden, damit alle benötigten Informationen über die Projekte gesammelt werden können.

1.6 Meilensteine

Folgende Meilensteine wurden zwischen den Beteiligten definiert. Die Termine richten sich an den Projektplan aus dem Modul PPBT (Projektplan Bachelor Thesis).

Meilenstein	Zeitfenster	Geschätzte Seitenanzahl
Ausgangslage	02.11.2010 – 30.11.2010	Ca. 20 Seiten Inhalt
Analyse von E-Voting Projekten	02.12.2010 – 07.04.2011	Ca. 20 Seiten Inhalt
Folgerungen	08.04.2011 – 13.05.2011	Ca. 10 Seiten Inhalt
Abgabe Bachelor Thesis	13.05.2011, 12.00 Uhr	Total: 50 Seiten Inhalt

Tabelle 1 / Meilensteinplan

1.7 Projektorganisation

Folgende Grafik¹ zeigt die Projektorganisation dieser Bachelor Thesis.

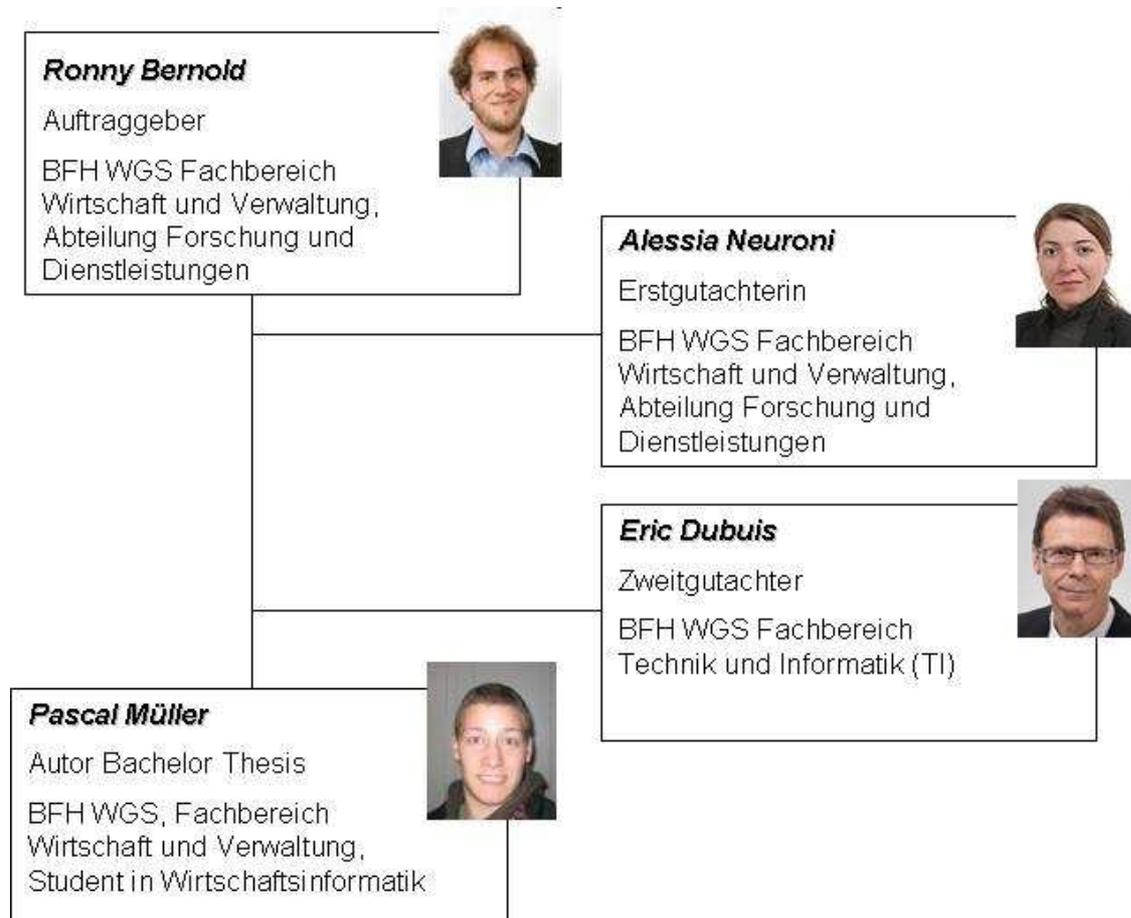


Abbildung 1 / Projektorganisation Bachelor Thesis

Damit der direkte Kontakt zum Auftraggeber und den Gutachtern gewährt ist, werden ungefähr ein Drittel der Bachelor Thesis im Kompetenzzentrum Public Management & E-Government an der Morgartenstrasse 2a im Büro A13 in 3014 Bern durchgeführt. Meetings finden im Durchschnitt jeden Monat mit allen Projektbeteiligten statt. Dabei werden der aktuelle Status sowie Unklarheiten und Probleme bezüglich Inhalt besprochen.

¹ Quelle: eigene Darstellung

2 Ausgangslage

In folgendem Kapitel sind die Grundlagen sowie eine Analyse der Stärken und Schwächen zu SuisseID und E-Voting aufgeführt.

2.1 SuisseID

Folgende Unterkapitel zeigen auf, was die SuisseID ist, wie diese SuisseID eingesetzt werden kann und welche Stärken und Schwächen bei SuisseID existieren.

2.1.1 Einführung

SuisseID ist ein standardisiertes Produkt, welches ermöglicht die Identität elektronisch nachzuweisen. Im dritten Konjunkturpaket des Bundes wurde beschlossen, dass die Verbreitung und Nutzung der SuisseID unterstützt wird. Deshalb ist es seit Mai 2010 möglich, sich für den reduzierten Preis von 65 Franken eine SuisseID zu beschaffen.

Eine SuisseID gibt es als Card und als USB-Stick. Aktuell ist die SuisseID in der Version 1.3 verfügbar. Dank einer SuisseID können heute Formulare und Verträge elektronisch abgeschlossen werden.² Momentan braucht es für einen Vertrag oder ein Formular oftmals die persönliche Unterschrift per Hand. Dadurch geht viel Zeit verloren. Auch entspricht dieses klassische Verfahren nicht den Bedürfnissen der „Digital Natives“, welche fast alle Tätigkeiten online und digital durchführen wollen.

„Defaultmässig“ wird die SuisseID mit Class 1 Readern genutzt. Diese Class 1 Reader besitzen nur über eine Schnittstelle, entweder USB oder einen Smart-Card Reader und haben den Nachteil, dass sensitive Informationen wie der PIN-Code durch einen Hacker im Klartext zu sehen sind. Deshalb kann auf Verlangen ein Class 2 Reader für die SuisseID eingesetzt werden. Class 2 Reader haben den Vorteil, dass zusätzlich noch ein Pinpad, beispielsweise eine Tastatur zum Einsatz kommt, wodurch sich die Sicherheit verbessert.³

Mit einer SuisseID können folgende drei Tätigkeiten durchgeführt werden.⁴

1. Elektronischer Identitätsnachweis
2. Qualifizierte elektronische Signatur
3. Elektronischer Funktionsnachweis

² SuisseID 1 (2010)

³ Cryptoshop (2004)

⁴ SuisseID 1 (2010)

Zurzeit sind nur die ersten zwei Elemente umgesetzt, während sich der elektronische Funktionsnachweis noch in der Pilot-Phase befindet.⁵

- Dank dem „elektronischen Identitätsnachweis (Nr.1)“ können sich Kunden oder Unternehmen authentisieren, als würden sie dies mit der gewöhnlichen Identitätskarte machen. Der „elektronische Identitätsnachweis“ basiert auf dem X.509 Standard.
- Dank der „qualifizierten, elektronischen Signatur (Nr.2)“ können Unterschriften digital abgegeben werden. Diese digitale Unterschrift ist genauso rechtsgültig wie eine Unterschrift per Hand. Auch die „qualifizierte, elektronische Signatur“ basiert auf dem X.509 Standard.

Aktuell sind diverse Projekte geplant oder umgesetzt, bei welchen die SuisseID zum Einsatz kommt. Viele Projekte sind erst seit kurzer Zeit produktiv, während diverse andere Projekte erst im nächsten Jahr in die Produktivität gelangen.⁶ Die SuisseID kann vielfältig eingesetzt werden, beispielsweise für sichere E-Mails, für qualifizierte elektronische Signaturen, für Dokumentenarchivierung oder für Kunden-Logins.

Die Laufzeit einer SuisseID beträgt maximal drei Jahre, danach muss eine Neue beschafft werden, damit die Gültigkeit des Zertifikates nicht erlischt.

a) Eigenschaften einer SuisseID⁷

Eine SuisseID besteht aus drei verschiedenen Teilen:

- **Sicherer Datenträger:** Der sichere Datenträger (Card oder USB-Stick) enthält zwei Zertifikate (Signatur und Authentisierung). Das erste Zertifikat ist ein „ZertES-konformes Zertifikat“, welches ermöglicht Dokumente zu unterschreiben. Das zweite Zertifikat ist ein „standardisiertes Authentisierungs-Zertifikat (IAC)“, welches ein sicheres Login bietet sowie für Signaturen bei E-Mails zum Einsatz kommen kann.
- **Die eindeutige Suisse-ID Nummer:** Jede SuisseID beinhaltet eine eindeutige, sechszehnstellige SuisseID-Nummer, welche auch bei Ablauf des Zertifikates erhalten bleibt.
- **Ein Identity Service Provider (IdP):** Dieser IdP besitzt Daten, welche irrelevant für das Zertifikat sind. Diese Daten können bei Bedarf nur vom jeweiligen SuisseID-Benutzer abgerufen werden. Beispielsweise enthält ein IdP Informationen wie Heimatort oder Geburtstag. Dies bedeutet, dass auf einem Zertifikat wirklich nur alle wichtigen Angaben vorhanden sind.

⁵ SuisseID 2 (2010)

⁶ SuisseID 3 (2010)

⁷ Hitech (2010)

ZertES ist das Bundesgesetz im Bereich Landesrecht „über Zertifizierungsdienste im Bereich der elektronischen Signatur“. Wenn ein „ZertES-konformes Zertifikat“ zum Einsatz kommt, ist die elektronische Unterschrift gesetzlich mit der Unterschrift per Hand gleichgestellt.⁸ Auf der SuisseID können unterschiedlich viele Informationen gespeichert werden. Minimal muss für jedes Zertifikat eine eindeutige Suisse-ID Nummer sowie den Benutzernamen und eine E-Mail-Adresse beinhalten. Anstatt eines Benutzernamens kann auch ein Pseudonym verwendet werden. Alle weiteren Informationen sind optional, wie beispielsweise Organisation oder Telefonnummer etc.⁹ Laut Prof. Gerhard Hassenstein¹⁰, kann die SuisseID nicht mit der echten ID (Identitätskarte) gleichgestellt werden, da jeder Mensch mehrere SuisseIDs besitzen kann und somit nicht eineindeutig ist.

b) Eigenschaften von X.509

X.509 ist ein Standard für PKI (Public Key Infrastructure). Sowohl der „elektronische Identitätsnachweis“ als auch die „qualifizierte, elektronische Signatur“ basieren auf dem X.509 Standard. Dieser Standard nutzt laut Denis Simonet¹¹ asymmetrische Kryptografie. Das Prinzip von X.509 basiert auf hierarchisch aufgebauten Zertifizierungsstellen. Dies bedeutet, dass nur übergeordnete Zertifizierungsstellen ein Zertifikat erstellen können.

Open PGP (Pretty Good Privacy) nutzt hingegen das „Web-of-Trust Modell“, welches im Gegensatz zu X.509 dezentral aufgebaut ist und bei welchem auch Teilnehmer auf der gleichen hierarchischen Stufe die Schlüssel der Gegenseite signieren dürfen. X.509 bietet ebenfalls die Möglichkeit, dass eine Zertifizierungsstelle eine SuisseID revozieren kann, wenn diese für ungültig erklärt werden muss (z.B. Verlust des PIN-Codes / Opfer eines Hackerangriffes oder wenn der private Schlüssel veröffentlicht wurde). Sämtliche revozierten Zertifikate könnten in einer Sperrliste durch die Zertifizierungsstelle aufgelistet werden.¹² Bei der SuisseID ist dies gemäss Denis Simonet¹³ jedoch nicht möglich.

X.509 nutzt eine asymmetrische Verschlüsselung, was bedeutet, dass jedes Zertifikat aus einem Public- und Private Key besteht. Wie der Name schon sagt, wird der Public Key veröffentlicht, während der Private Key unbedingt beim Besitzer bleiben muss. Bei einem Missbrauch oder Änderungen einer SuisseID müssen immer beide Schlüssel verändert werden.

⁸ SR 943.03 (2008)

⁹ Hitech (2010)

¹⁰ Hitech (2010)

¹¹ Interview Simonet (2011)

¹² X.509 (2011)

¹³ Interview Simonet (2011)

Hierarchische Modelle wie X.509 werden in einem Baum dargestellt. Bei der SuisseID befindet sich das Wurzel Zertifikat (Root-Zertifikat genannt) beim SECO (Staatsekretariat für Wirtschaft), dem Auftraggeber der SuisseID. Mit dem Private Key kann die SECO die Zertifikate der untergeordneten Stufe signieren.

Auf dieser untergeordneten Stufe befinden sich die SuisseID Reseller, wie die Post oder QuoVadis. Durch den Public Key der SECO können diese Reseller überprüfen, ob ihr Zertifikat tatsächlich durch das SECO signiert wurde.

Die Reseller können dann mit ihrem Private Key die SuisseID Zertifikate signieren. Diese Zertifikate landen dann auf der Smartcard, welche dem SuisseID Benutzer ausgehändigt werden. Mit dem Public Key der Reseller kann wiederum überprüft werden, ob das Zertifikat tatsächlich durch den Reseller signiert wurde.

Gemäss Denis Simonet¹⁴ ist es ein Problem, wenn ein Private Key des Resellers an die Öffentlichkeit gelangt, da jede Signierung dieses Resellers wertlos wird. Dadurch würde die Möglichkeit entstehen, dass man sich selbst eine SuisseID mit dem Zertifikat des Resellers erstellt. Um dies zu verhindern, müsste der Reseller vom SECO ein neues Schlüsselpaar erhalten (Public- und Private Key). Das alte Zertifikat müsste für ungültig erklärt werden.

Wie bereits erwähnt, ist für die SuisseID nicht vorgesehen eine Sperrliste für ungültige Zertifikate zu erstellen. Die Konsequenz daraus wäre, dass jede SuisseID eines Resellers neu ausgestellt werden muss.

c) Einsatz der SuisseID

Der Einsatz der SuisseID kann auf drei verschiedene Arten erfolgen.¹⁵

1. Authentisierungs-Zertifikat (IAC): Dabei findet eine gewöhnliche Authentisierung mit dem IAC statt.
2. Identity Service Provider (IdP): Wenn neben den Attributen auf der SuisseID noch zusätzliche Attribute verlangt werden, können diese vom IdP geliefert werden.
3. Claim Assertion Service (CAS): Wenn weitere private Attribute verlangt werden, welche sich nicht auf der SuisseID oder dem IdP befinden, können diese externen Attribute über den Claim Assertion Service zur Verfügung gestellt werden.

¹⁴ Interview Simonet (2011)

¹⁵ SuisseID 4 (2010)

d) Sicherheit¹⁶

Laut den Herstellern erfüllt SuisseID hohe Sicherheitsstandards. Einerseits hält sich die SuisseID an die gesetzlichen Bestimmungen (Schweizerischen Signaturgesetzes, ZertES). Andererseits wird das digitale Zertifikat auf einem Chip gespeichert, was die Identität unverfälscht lassen soll. Zudem läuft der Zugriff auf die SuisseID per PIN. Genau wie bei Bankkarten, wird die SuisseID bei einer dreimaligen Falscheingabe des PIN gesperrt. Die SuisseID kommt in einem System zwischen Mensch, Computer und Internet zum Einsatz, deren Gesamtkontrolle ausserhalb der Möglichkeiten einer SuisseID liegt.

Jedes Element des Systems muss diese drei unterschiedlichen Sicherheitsaspekte berücksichtigen. Nur wenn alle drei beschriebenen Elemente auf aktuellem Stand sind, kann die SuisseID gemäss den Herstellern als sicher gelten.¹⁷

- **Mensch:** Laut Signaturgesetz muss der PIN analog zu anderen Chipkarten separat von der tatsächlichen Karte abgelegt werden. Zudem sollten auf Standard PIN verzichtet werden (z.B. 1234-1234-1234-1234). Eine fremde Person müsste nur Kenntnis vom PIN haben, danach könnte sie die SuisseID für ihre Zwecke missbrauchen.
- **Computer:** Die SuisseID kann mit diversen Betriebssystemen eingesetzt werden. Ohne aktuelles Anti-Viren Programm und ohne regelmässige Updates des Betriebssystems und Browsers ist der Computer aber gefährdet und somit auch die Nutzung der SuisseID. MELANI (Melde- und Analysestelle Informationssicherung) bietet auf ihrer Homepage¹⁸ einen detaillierten Überblick über den Umgang mit Sicherheitselementen wie Updates, Firewall, Datensicherung usw. Nach Nutzung der SuisseID sollte diese nicht unbeaufsichtigt herumliegen oder im Computer stecken bleiben. Ein weiterer Punkt um die Sicherheit zu erhöhen, ist der Einsatz von Class 2+ Readern. Eine SSL (Secure Socket Layer) Verschlüsselung bei der Übertragung ist zwingend einzusetzen.
- **Internet:** Für den Umgang mit dem Internet bietet MELANI ebenfalls Hinweise und Verhaltensregeln.¹⁹ Zudem ist es auch hilfreich, wenn der angeklickte oder eingegebene Link auf seine Korrektheit überprüft wird.

¹⁶ SuisseID 5 (2010)

¹⁷ SuisseID 5 (2010)

¹⁸ MELANI (2010)

¹⁹ MELANI (2010)

2.1.2 Analyse der Stärken und Schwächen von SuisseID

Die Stärken und Schwächen der SuisseID sind aus verschiedenen Blickwinkeln festzuhalten. Einerseits existieren Stärken und Schwächen für den Benutzer einer SuisseID, aber die Stärken und Schwächen für die Betreiber einer Applikation mit SuisseID müssen ebenfalls berücksichtigt werden. Sämtliche Stärken und Schwächen konnten einerseits durch die Analyse der Grundlagen, aber auch durch diverse Interviews erhoben werden.

Folgende vier Tabellen zeigen die Stärken getrennt von den Schwächen der SuisseID aus Sicht der Benutzer sowie aus Sicht der Betreiber von SuisseID Applikationen.

Stärken von SuisseID aus Sicht der Benutzer	
Technische Stärken	
Standardisiertes Produkt	Die SuisseID ist laut Herstellern der erste standardisierte und elektronische Identitätsnachweis und wird bereits durch viele Unternehmungen in unterschiedlichen Einsatzgebieten genutzt. Somit kann ein Benutzer seine SuisseID vielfältig bei verschiedenen Applikationen einsetzen.
Zwei Token zur Auswahl	Die SuisseID kann gemäss Herstellern als USB-Stick oder Smartcard gekauft werden. Je nach Computer eignet sich ein anderes Token, aber der Vorteil dabei ist, dass kein Benutzer zusätzliche Hardware anschaffen muss.
Drei Einsatzarten	Je nach Vertrauensverhältnis und je nach verlangten Attributen, kann eine Einsatzart den anderen beiden Einsatzarten vorgezogen werden.
Sicherheit	Die SuisseID kann laut Herstellern (mit Ausnahme der Class 1 Reader) als sicher gelten, wenn sich Mensch, Computer und Internet an die vorgegebenen Sicherheitsrichtlinien halten. Absolute Sicherheit sei heute unmöglich. Allerdings muss berücksichtigt werden, dass auch die Unterschrift per Hand heute leicht zu manipulieren ist. Jedoch müssen die konkreten Applikationen, welche den Einsatz von SuisseID unterstützen, auch entsprechend geschützt werden. (siehe Sicherheit in Kapitel 2.1.1c: „Einführung in SuisseID“)
Minimum an Attributen	Auf der SuisseID befindet sich laut Herstellern zwingend neben der eindeutigen SuisseID Nummer nur noch ein Minimum an weiteren Attributen, was die Privatsphäre des Benutzers aufrecht erhält.
Datenschutz	Eine Referenz zu einem staatlichen Personenidentifikator, wie die AHV-Nummer, ist laut Herrn Hassenstein ²⁰ nicht erlaubt, wodurch keine Datenschutzprobleme entstehen.

²⁰ Interview Hassenstein (2011)

Stärken von SuisseID aus Sicht der Benutzer	
Organisatorische Stärken	
Freigabe von zusätzlichen Attributen	Werden durch die Applikation weitere Attribute wie Geburtsdatum verlangt, muss der Benutzer laut Herrn Bernold ²¹ die vom IdP oder CAS aufgelisteten Attribute bestätigen. Dabei kann der Benutzer sicherstellen, dass die Attribute der Wahrheit entsprechen, was zusätzliche Sicherheit bringt.
Offenes Konzept	Die SuisseID hat laut Herrn Bernold ²² kein starres Konzept sondern ein Offenes und basiert auf Open Source. Bei der Entwicklung wurde nicht in das letzte Detail geplant damit die SuisseID auch offen für Änderungen und Verbesserungen ist. Da die SuisseID auf Java basiert, kann ein Programmierer die Implementierung der SuisseID relativ einfach umsetzen.
Private Attribute	Im Vergleich zu Deutschland mit ihrem nPA (Neuer Personalausweis) dürfen in der Schweiz laut Herrn Bernold ²³ auch private Attribute (z.B. Grösse der Person) auf der SuisseID abgespeichert werden und nicht nur vorgegebene Attribute. Dieser Punkt bezieht sich auch wieder auf das offene Konzept der SuisseID. Mit dem Projekt myIDP kann dieses Vorhaben mit den privaten Attribute umgesetzt werden.

Tabelle 2 / Stärken von SuisseID aus Sicht der Benutzer

Schwächen von SuisseID aus Sicht der Benutzer	
Technische Schwächen	
CAS kann manipuliert sein	Wenn ein Benutzer einen CAS manipuliert, kann der CAS diesen beispielsweise als Arzt anerkennen, obwohl dieser gar nicht Arzt ist. Damit könnte man mit einer falschen Identität Schaden anrichten.
Softwareabhängigkeit	Für den Einsatz der SuisseID wird ein Treiber benötigt. Ist in einem Unternehmen dieser Treiber gesperrt, kann der Benutzer die SuisseID nicht verwenden.
X.509 Standard	Der X.509 Standard nutzt ein hierarchisches Modell. Es dürfen somit nur übergeordnete Stellen ein Zertifikat erstellen und für ungültig erklären lassen. Wenn also ein Private Key eines SuisseID Resellers in die Öffentlichkeit gelangt, müssen sämtliche SuisseIDs des Resellers für ungültig erklärt werden. (siehe X.509 in Kapitel 2.1.1b: „Einführung in SuisseID“)

²¹ Interview Bernold (2010)

²² Interview Bernold (2010)

²³ Interview Bernold (2010)

Schwächen von SuisseID aus Sicht der Benutzer	
Organisatorische Schwächen	
Funktionsnachweis noch nicht umgesetzt	Beim Funktionsnachweis wird aktuell das Konzept (Pilot-Projekt) erstellt. Das erste Einsatzgebiet des Funktionsnachweises wird laut Herrn Bernold ²⁴ das Anwaltsregister im Kanton Waadt sein. Gemäss Herrn Hassenstein ²⁵ ist auch Stand März 2011 dieser Funktionsnachweis noch nicht produktiv umgesetzt.
Mehrere SuisseIDs pro Person möglich	Jede natürliche Person kann mehrere SuisseIDs besitzen und diese verschieden einsetzen. Deshalb ist zwar eine SuisseID eindeutig (auf eine Person bezogen) aber nicht ein-eindeutig (da jede Person mehrere SuisseIDs haben kann). Im Hinblick auf eine Kombination mit E-Voting ist diese Tatsache ein Problem, da bei Verwendung einer SuisseID das Mehrfachabstimmen einfacher wird.
3 Jahre Laufzeit	Die Laufzeit einer SuisseID ist auf maximal drei Jahre beschränkt. Dies bedeutet, dass jede SuisseID nach dieser Zeit ersetzt werden muss. Dadurch können für die Benutzer Zusatzkosten oder zumindest ein Zusatzaufwand entstehen.
Kein direkter Vorteil für den Benutzer	Beim Kauf einer SuisseID hat ein Benutzer keinen direkten Vorteil. Er kann die SuisseID nur nutzen, wenn Applikationen den Einsatz dieser SuisseID unterstützen.

Tabelle 3 / Schwächen von SuisseID aus Sicht der Benutzer

Stärken von SuisseID aus Sicht der Betreiber	
Technische Stärken	
Spezialisiertes PKI Know-How vorhanden	Quovadis und Swisssign entwickelten die SuisseID im Auftrag der SECO. Beide Unternehmen sind Spezialisten im Gebiet PKI (Public Key Infrastructure) und besitzen das nötige Know-How um eine gute PKI Lösung zu entwickeln, was vor allem kleineren Unternehmen nützt, da diese keine PKI-Spezialisten benötigen ausser wenn eine Insellösung für eine spezifische Applikation entwickelt wird.
Gesetzliche Richtlinien	Die gesetzlichen Richtlinien sind vorhanden. ZertES ist das entsprechende Gesetz, auf welches sich die eingesetzten Zertifikate stützen. Auch gesetzlich festgehalten ist, dass die digitale Unterschrift mit SuisseID der Unterschrift per Hand gleichgestellt ist.

²⁴ Interview Bernold (2010)

²⁵ Interview Hassenstein (2011)

Stärken von SuisselD aus Sicht der Betreiber	
Technische Stärken	
Effizienzsteigerung durch kleineren Verwaltungsaufwand	Dank der Möglichkeit als Benutzer mit einer SuisselD online zu signieren, sinkt der Verwaltungsaufwand für Unternehmen, was wiederum zu einer Effizienzsteigerung führt, da es keinen physischen Kontakt braucht um Verträge mit einer Unterschrift abzuschliessen.
Zeitgemässes Medium	Das Bedürfnis nach elektronischen Unterschriften ist vorhanden, da viele Unternehmen heute bereits Ähnliches / Gleiches anbieten, aber jeweils nur als Einzellösung für die entsprechende Applikation.
Förderung der privaten Nutzung	Unternehmen können den Einsatz der SuisselD fördern, indem sie entweder nur die SuisselD als einzige Möglichkeit für das Login erlauben oder in dem beispielsweise jede Krankenkasse ihren Kunden eine SuisselD als Versicherungskarte anbietet. ²⁶
Organisatorische Stärken	
Unterstützt B2B, B2G, B2C, G2C Geschäfte	Der Fokus der SuisselD liegt auf der Business-Seite. Allerdings kommt die SuisselD auch bei B2G (Business to Government)- oder B2C (Business to Customer)-Geschäften zum Einsatz. Zudem wäre der Einsatz der SuisselD für E-Voting dann ein G2C (Government to Customer)-Geschäft.
Elektronische Verträge	Dank der SuisselD und der gesetzlichen Gleichstellung mit der Unterschrift per Hand, können Verträge auch elektronisch abgeschlossen werden.
Günstiger als Eigenlösung	Kleinere und mittlere Unternehmen können beim Einsatz der SuisselD die Aufwandskosten reduzieren, da keine Eigenlösung entwickelt werden muss und die Kosten durch viele Unternehmen getragen werden.

Tabelle 4 / Stärken einer SuisselD Applikation aus Sicht der Betreiber

²⁶ Interview Bernold (2010)

Schwächen von SuisseID aus Sicht der Betreiber	
Technische Schwächen	
Class 1 Reader	Class 2 und Class 3 Smartcard Reader werden von SuisseID Applikationen nicht unterstützt. (Stand Dezember 2010) Mittlerweile ist der Einsatz eines Class 2 Readers gemäss Herrn Hassenstein möglich, allerdings nur auf Verlangen. (Stand März 2011) Per Default erhält ein Benutzer einen Class 1 Reader. Diese Tatsache ist laut Denis Simonet ²⁷ eine Schwäche. Per Default sollte ein Class 2 Reader ausgehändigt werden.
Organisatorische Schwächen	
Kommunikation	Laut Denis Simonet ²⁸ wurden zuerst kritische Stimmen betreffend Sicherheit ignoriert, dann wurde trotzdem durch das SECO eingelenkt als Sicherheitsexperten von "Dreamlab" die SuisseID hacken konnten. Die Kommunikation nach aussen verlief bisher nicht ideal.
Handbuch	Ein Handbuch zur Nutzung der SuisseID ist nur Online verfügbar. Es wäre laut Denis Simonet ²⁹ für viele Benutzer hilfreicher, wenn ein Handbuch auf Wunsch mitgegeben wird. Zudem sollte im Internet eine Kampagne gestartet werden, welche auf die möglichen Gefahren bei der Nutzung der SuisseID hinweisen. Diese Kampagne könnte auch ins Handbuch integriert werden.
Organisatorische Schwächen	
Marketing	Das Vertrauen in die SuisseID sank in letzter Zeit, da viele kritische Medienberichte erschienen. Das Problem war, dass die SuisseID ständig als Sicherheitslösung angeboten wurde. Dabei ist eine absolute Sicherheit unmöglich, jedoch sind die Sicherheitsrisiken bei richtiger Anwendung auf ein Minimum reduzierbar. Das Marketing der SuisseID muss den Nutzen klar festhalten, beispielsweise, dass eben eine eigene PKI teurer sein kann als wenn die SuisseID verwendet wird.

Tabelle 5 / Schwächen einer SuisseID Applikation aus Sicht der Betreiber

²⁷ Interview Simonet (2011)

²⁸ Interview Simonet (2011)

²⁹ Interview Simonet (2011)

2.1.3 Qualitativer Nutzen für die Benutzer und Unternehmen

Aus zuvor genannten technischen und organisatorischen Stärken und Schwächen ergibt sich folgender qualitativer Nutzen für die Benutzer einer SuisseID:

Für die SuisseID Benutzer gibt es laut Herrn Bernold³⁰ und Herrn Hassenstein³¹ keinen direkten Vorteil. Durch den CAS oder dem Funktionsnachweis könnte ein Benutzer die Behördengänge vom Sofa aus durchführen. Dies gäbe einen Mehrwert, da der Benutzer unabhängig vom Ort und Zeit mit den Behörden in Kontakt treten könnten.

Die Unternehmen, welche die SuisseID einsetzen, haben einen Nutzen. Durch das Authentifizieren mit der SuisseID, können Manipulationen enorm minimiert werden, da das Unternehmen nun sehen kann, wer der Benutzer ist. Durch den Diebstahl der SuisseID inklusive dem PIN-Code, kann sich jedoch jemand unerlaubt authentifizieren. In diesem Fall würde laut Herrn Hassenstein³² dennoch der ursprüngliche SuisseID Benutzer haften, da dieser beim Verlust seiner SuisseID diese unmittelbar revozieren muss.

Auch das Abchecken, ob jemand 18 Jahre alt ist oder nicht (beispielsweise in einem Weinshop), bringt sehr viele Vorteile. Ursprünglich konnten solche Geschäfte nur per Kreditkarte durchgeführt werden. Dank SuisseID können auch erwachsene Personen ohne Kreditkarten Online Sachen bestellen, bei denen ein Mindestalter vorausgesetzt wird, da auf der SuisseID ein Attribut mit dem Geburtsdatum abgespeichert werden kann.

2.1.4 Quantitativer (finanzieller) Nutzen für die Benutzer und Unternehmen

Aus zuvor genannten technischen und organisatorischen Stärken und Schwächen ergibt sich folgender quantitativer Nutzen für die Benutzer einer SuisseID:

Der Nutzen ist laut Herrn Hassenstein³³ für beide Seiten (Unternehmen und Benutzer) nicht vorhanden. Allerdings könnte für Unternehmen der Verwaltungsaufwand kleiner werden, wenn die Adressbestätigung per SuisseID möglich wäre. Einerseits könnte dies über myIDP gelöst werden oder über einen Post CAS für Postadressen. Dadurch würde auch ein Nutzen für die Benutzer entstehen, da diese die Adressänderungen nicht mehr vor Ort durchführen müssten.

³⁰ Interview Bernold (2010)

³¹ Interview Hassenstein (2011)

³² Interview Hassenstein (2011)

³³ Interview Hassenstein (2011)

2.2 E-Voting

Folgendes Unterkapitel zeigt auf, was E-Voting ist, wie E-Voting zum Einsatz kommt und welche Stärken und Schwächen bei E-Voting existieren.

2.2.1 Einführung

E-Voting bedeutet elektronisches Wählen. E-Voting ist ein Bestandteil von E-Government, respektive E-Democracy. E-Government ist in folgende fünf Teile gegliedert:³⁴

- **E-Health**
- **E-Justice**
- **E-Education**
- **E-Administration**
- **E-Democracy**
 - **E-Participation**
 - **E-Voting**

E-Voting ist ein Bestandteil von E-Participation, was wiederum zu E-Democracy gehört. E-Voting ist ein relativ neuer Begriff, welcher viele Menschen noch nicht kennen, obwohl die meisten Menschen schon einmal E-Voting benutzten, nämlich zwecks einer Online-Umfrage.

E-Voting ist somit ein breiter Begriff mit vielen unterschiedlichen Eigenschaften. Einerseits gehören, wie bereits erwähnt, normale Online-Umfragen zu E-Voting. Andererseits existieren, wie bei den Wahlen in den USA, elektronische Wahlmaschinen, bei welchen nur die Stimmen pro Wahlmaschine elektronisch addiert werden können.³⁵

Der Fokus dieser Arbeit liegt jedoch bei Wahlen übers Internet von einem Computer aus. Dies wird auch „remote E-Voting“ oder „Internet Voting (I-Voting)“ genannt.

a) Vote électronique

Nach ersten erfolgreichen Schweizer Pilot-Projekten in drei Kantonen beschloss der Bundesrat am 31. Mai 2006, dass E-Voting in der Schweiz schrittweise eingeführt wird. In der Schweiz wird anstatt E-Voting der Begriff „Vote électronique“ verwendet.

³⁴ Schütz (2009, S. 58 - 59)

³⁵ Sidler (2003)

„Vote électronique“ umfasst folgende drei Elemente.³⁶

1. Elektronisches Abstimmen und Wählen

1a) Das Wählen und Abstimmen per Internet (I-Voting) inkl. der Entgegennahme, der Prüfung und der Auszählung der elektronischen Stimmen.

1b) Ermittlung der Resultate, der Statistiken sowie der Ergebnisveröffentlichung

1c) Die Unterstützung im Internet von Behörden und Parteien / Gruppierungen im Hinblick auf die Nationalratswahlen 2011 und zukünftige Nationalratswahlen

2. Elektronische Referenden und Initiativen

2a) Elektronische Sammlung, Prüfung und Zählung der digitalen Unterschriften

3. Elektronische Wahl – und Abstimmungsinformationen durch Behörden

3a) Online Bereitstellung von Informationen für die Stimmbürger zu Wahlen und Abstimmungen, wie beispielsweise das Abstimmungsbüchlein

3b) Online Beantwortung von Fragen, Wünschen und kritischen Anregungen

Diese Arbeit befasst sich ausschliesslich mit Punkt 1a) – dem Wählen und Abstimmen per Internet.

Seit 1. Januar 2008 gelten Änderungen im „Bundesgesetz über die politischen Rechte“. Dabei wurden Anpassungen gemacht, welche E-Voting fördern sollen. Jeder Kanton kann sich seit dem 1. Januar 2008 an „Vote électronique“ beteiligen. So wurde festgelegt, dass alle kommunalen und kantonalen Stimmregister harmonisiert werden. Seit über einem Jahr ist diese Harmonisierung abgeschlossen. Ohne eine solche Harmonisierung wäre es für Stimmbürger nicht möglich per E-Voting abzustimmen. Bis 2011 gilt die Einschränkung, dass E-Voting Tests nur für maximal 10 % der Stimmberechtigten durchgeführt werden dürfen. Dies entspricht ungefähr 500'000 Stimmberechtigten. Zudem ist es dem Bundesrat erlaubt, Tests bezüglich Ort und Zeit einzuschränken, um die potentiellen Risiken zu minimieren. Erst bei fünf erfolgreichen Tests, können die Kantone die Tests ausbauen, d.h. E-Voting weiteren Stimmbürger anbieten.³⁷

In der Schweiz soll es dadurch möglich sein, neben der brieflichen Wahl und dem Urnengang auch Online abzustimmen. Als Wahlen wird das Wählen von Personen (National-, Stände-, Gross-, Regierungs-, Gemeinderat inkl. Stichwahlen) aber auch das Abstimmen über Sachfragen (Initiativen, Referenden) bezeichnet.

³⁶ Bericht Villiger / Huber-Hotz (2002)

³⁷ Bundeskanzlei (2009)

Die Verantwortung für die Organisation und Durchführung der Wahlen und Abstimmungen liegt bei den Kantonen. Der Grund dafür ist, dass der personelle Aufwand nicht durch den Bund zu bewältigen wäre. Im Kanton Aargau braucht es beispielsweise für eine Abstimmung oder Wahl vom Anfang bis zum Ende über 70'000 Personen. Daher liegt auch die Verantwortung für E-Voting bezüglich Organisation und Durchführung auf kantonaler Ebene. Die Oberverantwortung bei E-Voting liegt jedoch analog zur brieflichen Abstimmung und dem Urnengang bei der Bundeskanzlei. Sie ist für die Koordination zuständig und nach dem Abschluss einer Abstimmung oder Wahl werden ihr die kantonalen Ergebnisse übermittelt. Danach addieren sie die Stimmen und veröffentlichen die Resultate.

Im Bundesgesetz über politische Rechte³⁸ sind die gesetzlichen Richtlinien zu Wahlen und Abstimmungen aufgeführt; im Artikel 8a³⁹ stehen die gesetzlichen Richtlinien für elektronische Wahlen. Der Artikel 10 Abs. 2⁴⁰ beschreibt, dass die Durchführung der Wahlen und Abstimmungen durch den Kanton erfolgen müssen und jeder Kanton dabei die kantonalen Anforderungen zu definieren haben.

Die Schweiz steht bezüglich E-Voting europäisch im vorderen Mittelfeld und führte bereits Pilot-Projekte durch. Nur Estland, die Niederlande und Grossbritannien sind bezüglich E-Voting vor der Schweiz platziert. In Estland ist es seit 2005 möglich, flächendeckend E-Voting für Parlamentswahlen einzusetzen, während die Niederlande und Grossbritannien die Versuche einstellten.⁴¹

b) Ziele⁴²

Die Einführung eines E-Voting Systems hat diverse Ziele:

- Laut Michael Pflughart⁴³ kann erwartet werden, dass die Stimmbeteiligung nicht weiter sinkt oder sich sogar steigern kann, da die Mehrheit der Stimmbürger heute über Internet verfügt und auch dieses auch mehrmals wöchentlich nutzt. Laut dem Bericht des Bundesrates⁴⁴, würden rund 30 % aller tatsächlichen Wähler E-Voting nutzen.
- Dank dem sinkenden Aufwand für die Administration (automatisches Zählen der Stimmen) können die Kosten gesenkt werden.
- Durch das automatische Zählen der Stimmen kann eine schnellere Präsentation der Wahlresultate erfolgen.

³⁸ SR 161.1 (2010)

³⁹ SR 161.1 (2010)

⁴⁰ SR 161.1 (2010)

⁴¹ Swissinfo (2008)

⁴² Schütz (2009, S. 58 - 59)

⁴³ eGov Präsenz (2004)

⁴⁴ Bericht Leuenberger / Huber-Hotz (2006)

- Da für das Abstimmen neben dem Stimmrechtsausweis nur ein Internet-Anschluss nötig ist, kann orts- und zeitunabhängig abgestimmt werden. Dies bringt vor allem Vorteile für Auslandsschweizer.
- Das Abstimmen über Internet spricht vor allem Digital Natives aber auch andere Bevölkerungsschichten an, da es sich um ein zeitgemässes Verfahren handelt.

Genau wie die briefliche Wahl und der Urnengang, müssen die demokratischen Grundsätze bei E-Voting in gleichem Masse eingehalten werden. Das bedeutet, dass die Wahl „allgemein, persönlich, geheim, frei, unmittelbar und gleich sein muss“.⁴⁵

c) Die demokratischen Grundsätze⁴⁶

Folgende Tabelle zeigt die demokratischen Grundsätze für rechtsgültige Wahlen und möglichen Umsetzungsschwierigkeiten bei E-Voting.

Grundsatz	Mögliche Probleme
Allgemein	Da nicht alle Stimmbürger Internet nutzen und oftmals mangelnde Computerkenntnisse haben, können diese Stimmbürger nicht per E-Voting abstimmen.
	Das Abstimmen darf dem Stimmbürger nichts kosten. Wenn kein Computer vorhanden ist, ist E-Voting nicht durchführbar.
Frei	Die Abgabe der Stimme muss unabhängig vom Einfluss anderer erfolgen.
	Das Wahlformular muss neutral geschrieben werden, respektive dem Wahlformular der Briefpost entsprechen. Werbung muss daher verboten oder ausgeglichen gestaltet sein.
Geheim	Die Entscheidung muss im geheimen getroffen werden und darf nicht durch Aussenstehende beeinflusst werden.
	Auch darf die Stimme nicht nachträglich manipuliert werden können.
	Es muss unmöglich sein eine Stimme einem Stimmbürger zuzuordnen.
Unmittelbar	Es darf keine Zwischenstation bei der Stimmausgabe geben.
Persönlich	Die Person muss eindeutig identifiziert werden können.
Gleich	Es dürfen nur stimmberechtigte Personen abstimmen.
	Eine mehrmalige Stimmausgabe muss ausgeschlossen sein.
	Das Wahlverfahren muss einheitlich aufgebaut und gestaltet werden.

Tabelle 6 / Demokratische Grundsätze für rechtsgültige Wahlen

⁴⁵ Schütz (2009, S. 22) beschreibt die sechs demokratischen Grundsätze

⁴⁶ Schütz (2009, S. 22 - 24)

d) Kryptografie⁴⁷

Aus den obengenannten demokratischen Grundsätzen ergeben sich folgende Anforderungen an die Kryptografie:

- Vertraulichkeit
- Integrität
- Authentifikation
- Verbindlichkeit

Dabei existieren verschiedene mögliche Verschlüsselungsverfahren, um E-Voting zu verschlüsseln:

Verschlüsselung	Algorithmen
Symmetrische Verschlüsselung	DES (Data Encryption Standard)
Asymmetrische Verschlüsselung	RSA (Rivest, Shamir and Adleman), Zero-Knowledge-Proof (Fiat Shamir)
Digitale Signaturen	Digitale Signatur, Blinde Signatur
PIN / TAN (Persönliche Identifikationsnummer / Transaktionsnummer)	Ist <u>kein</u> Verschlüsselungsverfahren
Hash-Funktionen	MD5 (Message Digest 5), SHA1 (Secure Hash Algorithm 1)

Tabelle 7 / mögliche Verschlüsselungsverfahren

Das grosse Problem bei den Verschlüsselungen ist, dass sowohl die asymmetrische Verschlüsselung, die digitale Signatur als auch das Verfahren mit PIN / TAN nicht alle demokratischen Grundsätze gleichmässig einhalten können.

⁴⁷ Schütz (2009, S. 41 - 50)

e) Erfolgsfaktoren⁴⁸

Allerdings genügen nicht nur Massnahmen zur Gefahrenreduktion um den Erfolg von E-Voting sicherzustellen. Weitere Faktoren werden benötigt, welche in folgender Tabelle aufgeführt sind:

Erfolgsfaktor	Erklärung
Technik	Nur wenn auf Seiten der Stimmbürger und den Betreibern des E-Voting Systems die Sicherheit auf aktuellem Stand ist. Nur wenn die Anzahl an Internetnutzern zunimmt, sind die technischen Voraussetzungen gegeben.
Wahlverfahren	Nur wenn die eindeutige Identifizierung des Stimmbürgers, aber auch gleichzeitig die Anonymisierung der Stimme vorhanden ist, kann das Wahlverfahren als ausreichend gelten.
Gesetz	Nur wenn das Gesetz spezifisch für E-Voting Systeme angepasst ist und nur wenn die Grundsätze betreffend Demokratie, Signaturen und Datenschutz der aktuellen Situation entsprechen, entspricht die rechtliche Situation den gesetzlichen Anforderungen.
Politik	Nur wenn eine politische Strategie erarbeitet wurde und nur wenn diese Strategie umgesetzt und ständig angepasst wird, sind die politischen Unterstützung und Akzeptanz gegeben.
Soziales	Nur wenn der Staat für die Akzeptanz von E-Voting sorgt, nur wenn die Stimmbürger vom Staat transparent informiert werden betreffend Angebot und Sicherheit, sind die sozialen Voraussetzungen vorhanden. Jedoch müssen Menschen ohne Computerkenntnisse die Möglichkeit haben, Schulungen zu besuchen, damit der digitale Graben geschlossen werden kann.

Tabelle 8 / Erfolgsfaktoren für E-Voting

2.2.2 Analyse der Stärken und Schwächen von E-Voting

Für die Analyse der Stärken und Schwächen von E-Voting, ist zuerst zu bestimmen, für wen die Stärken und Schwächen analysiert werden sollen. E-Voting bezieht sich auf natürliche, stimmberechtigte Privat-Personen. Deshalb werden zuerst die Stärken und Schwächen aus Sicht der Benutzer (= Stimmbürger) analysiert. Da ein solches E-Voting System von einer Behörde in Zusammenarbeit mit privaten Firmen entwickelt und betrieben wird, bezieht sich der zweite Teil der Analyse auf die Stärken und Schwächen aus Sicht der Entwickler / Betreiber. Die Stärken und Schwächen konnten einerseits durch Literatur und andererseits durch diverse Interviews zusammengestellt werden.

⁴⁸ Schütz 2009 (S. 56 - 57)

Folgende vier Tabellen zeigen die Stärken getrennt von den Schwächen von E-Voting aus Sicht der Benutzer sowie aus Sicht der Entwickler / Betreiber:

Stärken von E-Voting aus Sicht der Benutzer	
Technische Stärken	
Verschlüsselungsverfahren	Dank der Möglichkeit einzelne oder gemeinsame Verschlüsselungsverfahren einzusetzen, sinken die technischen Risiken eines Missbrauchs. (siehe Kryptografie in Kapitel 2.2.1d: „Einführung“)
Wahlverfahren	Die verschiedenen Wahlverfahren helfen zur Sicherheit der Stimmabgabe. (siehe Wahlverfahren in Kapitel 2.2.1e: „Einführung“)
Zusätzlicher Kanal	Dank E-Voting entsteht neben dem Urnengang und der brieflichen Stimmabgabe ein dritter Kanal, um die Stimme abzugeben.
Unterstützt die gängigen Browser	Jeder Stimmbürger mit Computer und Internet-Anschluss kann mit Hilfe eines gängigen Browsers (Internet Explorer, Mozilla Firefox, Apple Safari) auf ein E-Voting System zugreifen.
Organisatorische Stärken	
Zeitunabhängige Stimmabgabe	Dank E-Voting ist eine Stimmabgabe unabhängig vom Zeitpunkt möglich. Es muss nur ein Zeitfenster für die Abgabe der Stimmen definiert werden. In diesem Zeitfenster gilt diese Zeitunabhängigkeit.
Ortsunabhängige Stimmabgabe	Dank E-Voting benötigt ein Stimmbürger nur einen Internet-Zugang sowie seinen Stimmrechtsausweis. Dadurch ist das Abstimmen weltweit möglich, selbst wenn sich der Stimmbürger im Ausland befindet.
Bequeme Abstimmung	Dank E-Voting kann bequem von zuhause aus abgestimmt werden. Dies ermöglicht die einfachere Stimmabgabe für Menschen, welche weit entfernt von einem Zentrum leben.
Immobilität	E-Voting ermöglicht (geh-) behinderten Menschen die einfache Teilnahme an einer Abstimmung. Für die Abgabe der Stimme (egal ob Briefkasten oder Urne) wird kein Betreuer mehr benötigt.
Modernisierung	E-Voting wird dem Wunsch der „Digital Natives“ gerecht. Diese „Digital Natives“ nutzen heute oftmals „e-banking“. Dadurch erhöht sich für diese Stimmbürger die Attraktivität einer Abstimmung.
Auslandschweizer	Für Auslandschweizer ist E-Voting die ideale Lösung, da für sie ein Urnengang unmöglich ist und bei der brieflichen Abstimmung nicht immer sicher ist, ob die Stimme auch in der Schweiz ankommt, beispielsweise wenn Krieg herrscht oder bei Streiks.

Tabelle 9 / Stärken von E-Voting aus Sicht der Benutzer

Schwächen von E-Voting aus Sicht der Benutzer	
Technische Schwächen	
Malware und Hackerangriffe	Als Malware gelten Viren, Würmer und Trojaner. Malware kann die Stimmabgabe verhindern oder sogar die Stimmen manipulieren. Jeder Computer ist ohne ausreichenden Schutz durch einen Hacker angreifbar. Web Spoofing stellt hier eine grosse Schwäche dar.
Sonstige Sicherheitsrisiken	Wenn die Abstimmung per PIN oder TAN Code erfolgt, kann bei Diebstahl des PIN Codes durch eine fremde Person abgestimmt werden.
Datenschutz	Das E-Voting System muss sich von der Stimmabgabe bis zur Auszählung der Stimmen an den Datenschutz halten. Deshalb müssen die demokratischen Grundsätze für rechtsgültige Wahlen zwingend eingehalten werden. Vor allem der Grundsatz „Geheim“ steht im Fokus. Es darf zu keinem Zeitpunkt herausgefunden werden, welche Person wie abgestimmt hat.
Transparenz	Während dem ganzen Wahlverfahren, aber auch beim Auszählverfahren, ist die Transparenz nicht vorhanden, da ein E-Voting System für den Stimmbürger wie eine Black Box funktioniert. Der Algorithmus des E-Voting Systems wird laut Denis Simonet ⁴⁹ nicht offengelegt. Allerdings funktioniert sowohl die briefliche Stimmabgabe, als auch der Urnengang wie eine Black Box.
Organisatorische Schwächen	
Fehlendes Wissen	Viele Stimmbürger besitzen zu wenig Computer- oder Internetkenntnisse. Aber auch viele Stimmbürger mit Computer- und Internetkenntnissen haben kaum Ahnung im Umgang mit Sicherheitsrisiken. Deshalb müssen alle Stimmbürger ausreichend informiert werden, wie sie vorzugehen haben. (Einsatz einer Firewall)
Faktor Mensch	Ein E-Voting System funktioniert nicht ohne den Faktor Mensch. Beispielsweise werden die E-Voting Stimmen zwar elektronisch ausgezählt, jedoch durch Menschen überprüft. Diese Auszähler könnten gemäss Denis Simonet ⁵⁰ theoretisch durch Parteien oder private Unternehmen gekauft werden, damit die Auszähler das Resultat zu Gunsten der Partei / Unternehmen abändern. Das Vertrauen in die E-Voting Auszähler muss wie bei den anderen Kanälen jederzeit vorhanden sein.

⁴⁹ Interview Simonet (2011)

⁵⁰ Interview Simonet (2011)

Schwächen von E-Voting aus Sicht der Benutzer	
Organisatorische Schwächen	
Vertrauen	Durch die bestehenden Sicherheitsrisiken, die mangelnde Transparenz sowie kritische Stimmen, sinkt das Vertrauen in E-Voting. Falls eine Abstimmung manipuliert würde, wäre das Vertrauen in E-Voting laut Denis Simonet ⁵¹ endgültig weg.

Tabelle 10 / Schwächen von E-Voting aus Sicht der Benutzer

Stärken von E-Voting aus Sicht der Entwickler / Betreiber	
Technische Stärken	
Grosses Entwicklungspotential	Die Stimmbürger sind generell nicht abgeneigt E-Voting einzusetzen. Deshalb hat E-Voting ein Potential für die Zukunft. ⁵² Wenn eine optimale und sichere Lösung gefunden werden kann, könnte sich E-Voting als dritter Abstimmungskanal durchsetzen.
Genauigkeit der Stimmzählung	Stimmzettel mit ungenauen Angaben oder unleserlicher Schrift können im Vergleich zu den beiden ursprünglichen Kanälen nicht mehr vorkommen. Automatisch wird ein „Ja“ als „Ja“ und ein „Nein“ als „Nein“ identifiziert. Dadurch verschwinden „unsichere“ Stimmzettel. Dies ermöglicht eine effizientere Stimmzählung sowie eine schnellere Präsentation der Resultate.
Organisatorische Stärken	
Aufwandsreduktion bei der Auszählung	Bei E-Voting landen alle Stimmen auf dem gleichen, zentralen System. Der organisatorische und zeitliche Aufwand sinkt dadurch. Im Vergleich zu den anderen Kanälen, können die Stimmen automatisch und effizient ausgezählt werden. (siehe Ziele in Kapitel 2.2.1b: „Einführung“)
Kosteneinsparung	Der administrative Aufwand bezüglich Organisation und Auszählung sinkt im Vergleich zum Urnengang oder der brieflichen Abstimmung. (siehe Ziele in Kapitel 2.2.1b: „Einführung“)

Tabelle 11 / Stärken von E-Voting aus Sicht der Entwickler / Betreiber

⁵¹ Interview Simonet (2011)

⁵² Gfs.bern (2005)

Schwächen von E-Voting aus Sicht der Entwickler / Betreiber	
Technische Schwächen	
Komplexe Audits	Audits von E-Voting Systemen sind möglich. Allerdings geht dies laut Denis Simonet ⁵³ nur über ein privates Zertifikat. Dieses Verfahren ist sehr aufwändig und komplex. Deshalb können nur Spezialisten den Vorgang beim Audit verstehen. Darunter würde das Vertrauen der Bevölkerung in die Korrektheit der Audits leiden.
Keine Integration mit anderen Systemen	Da die Sicherheitsanforderungen als auch die gesetzlichen Anforderungen sehr hoch sind, darf kein E-Voting System in ein anderes System integriert werden. Deshalb werden durch das E-Voting System zusätzliche Infrastrukturkosten entstehen.
Nicht-Nachkontrollierbarkeit der Stimmen	Da bei E-Voting nie herausgefunden werden darf, wie und über welchen Kanal eine Person was abgestimmt hat, kann nicht überprüft werden, ob die Stimme korrekt im System landete.
Malware	Wie auf der Seite des Stimmbürgers, besteht auch bei den Betreibern des E-Voting System das Risiko von Malware. Allerdings sind die Auswirkungen bei Malware bei den Betreibern viel grösser.
Denial of Service	Wenn das E-Voting System mit Denial of Service angegriffen wird, besteht die Möglichkeit, dass das E-Voting System ausfällt und dadurch ein Abstimmen über das Internet zeitweise unmöglich wird.
Auswirkungen bei Manipulationen	Wenn heute in einem Wahlkreis manipuliert wird, hat dies kaum Auswirkungen auf das Endresultat. Bei einem E-Voting System müsste laut Herrn Hassenstein ⁵⁴ nur an einer Stelle manipuliert werden und tausende von Stimmen könnten verfälscht werden. Ein systematischer Missbrauch muss daher unbedingt verhindert werden. Kleine Missbräuche sind hingegen kaum zu verhindern. ⁵⁵
Organisatorische Schwächen	
Kosten vs. Nutzen	Eine flächendeckende Einführung würde in der Schweiz ca. 600 Mio. Franken kosten. ⁵⁶ Da jedoch die Stimmbeteiligung erst nach einiger Zeit zunimmt, aber gleichzeitig die beiden anderen Kanäle aufrecht erhalten bleiben, wäre der Nutzen im Vergleich zu den Kosten erst nach einigen Jahren zu spüren.

⁵³ Interview Simonet (2011)

⁵⁴ Interview Hassenstein (2011)

⁵⁵ Interview Muster / Weber (2011)

⁵⁶ Inside-it (2007)

Schwächen von E-Voting aus Sicht der Entwickler / Betreiber	
Organisatorische Schwächen	
Einhaltung der demokratischen Grundsätze	Die Einhaltung der demokratischen Grundsätze ist nicht zu 100% möglich. Beispielsweise ist eine Wahl per E-Voting nicht allgemein, da nicht jeder Stimmbürger Computer und Internet besitzt. Die grösste Herausforderung stellt jedoch der Grundsatz „geheim“ bezüglich der bereits beschriebenen Sicherheitsrisiken dar.
Föderalismus	Da fast jede Gemeinde in fast jedem Kanton in der Deutschschweiz die Einwohnerregister ihrer Bürger verwaltet, aus denen die Stimmrechtsausweise erstellt werden, müssen diese Stimmrechtsausweise zuerst auf kantonaler Ebene harmonisiert und verknüpft werden.
Keine schnelle Erhöhung der Stimmbeteiligung	Laut einer Studie von gfs.bern ⁵⁷ steigt die Stimmbeteiligung dank E-Voting. Aber Pilot-Projekte zeigen, dass die Stimmbeteiligung nicht im grossen Rahmen zunimmt. Jedoch vermutet man ⁵⁸ , dass eine Abnahme der Stimmbeteiligung verhindert wird.
Keine Ablösung der traditionellen Kanälen	Bei der Analyse von durchgeführten E-Voting Versuchen, ist zu sehen, dass die briefliche Stimmabgabe auch bei Einführung von E-Voting den grössten Teil der Stimmen ausmachen würde. Der Urnengang wäre am ehesten abzulösen, da die briefliche Stimmabgabe von mehr Stimmbürgern genutzt wird. Die Anzahl der Urnengänger blieb bei den E-Voting Versuchen jedoch relativ konstant.
Betriebs-, Verwaltungs- und Wartungskosten	Für den Betrieb, die Verwaltung und Wartung des E-Voting Systems benötigen die Behörden zusätzliche Infrastrukturen und Ressourcen. Wenn keiner der bestehenden Kanäle abgelöst wird, sind die Betriebs-, Verwaltungs- und Wartungskosten des E-Voting zusätzliche Kosten für die Behörden, respektive den Steuerzahler.
Rechtliche Unsicherheit	Es existieren noch kaum E-Voting spezifische Gesetze. Viele rechtliche Fragen sind momentan unklar. Beispielsweise ist unklar, wer haftet, wenn Stimmen verloren gehen und welche Folgen daraus entstehen. (Wahl wird für gültig oder ungültig erklärt)

Tabelle 12 / Schwächen von E-Voting aus Sicht der Entwickler / Betreiber

⁵⁷ Gfs.bern (2005)

⁵⁸ Chaos Computer Club Zürich (2010)

2.2.3 Qualitativer Nutzen für die Benutzer und Verwaltungen

Aus zuvor genannten technischen und organisatorischen Stärken und Schwächen ergibt sich folgender qualitativer Nutzen für die Benutzer und Verwaltungen von E-Voting:

Einerseits gibt es dank E-Voting keine unklaren Stimmen mehr. Jedes Kreuz ist nun eindeutig platziert und Namen von Politikern werden aus einer Liste ausgewählt und somit kann kein Name falsch geschrieben werden. Dadurch sinkt der Anteil an ungültigen Stimmen auf ein Minimum. Die Auszählung der Stimmen kann durch die Verwaltung automatisch mit einem Auswertungssystem durchgeführt werden. Somit können die Resultate schneller publiziert werden.

Das Bedürfnis nach E-Voting ist zudem grundsätzlich vorhanden. In Pilot-Projekten war zu sehen, dass die Anzahl an E-Voting Nutzern auf einem konstanten Level ist. Allerdings konnte es noch nicht wissenschaftlich bewiesen werden, ob durch E-Voting eine Erhöhung der Stimmbeteiligung erreicht wird.⁵⁹ Vor allem jüngere Stimmbürger würden E-Voting nutzen. Stimmbürger profitieren zudem von der Tatsache, dass eine Abstimmung unabhängig von Ort und Zeit durchgeführt werden kann. Stimmbürger müssen nur über Internet verfügen und ihren Stimmrechtsausweis dabei haben.

Für körperlich beeinträchtigte Menschen, Auslandschweizer und sehr mobile Personen ist zudem E-Voting sehr sinnvoll, da diese Zielgruppen ohne mühsamen Aufwand nicht an der Urne oder teilweise sogar nicht per Brief abstimmen können. Aber auch andere Personen profitieren von den Vorteilen von E-Voting.

Allerdings existieren auch Schwachstellen bei E-Voting. Ein E-Voting System funktioniert wie eine Black-Box. Die Transparenz ist sowohl bei der Stimmabgabe als auch bei der Stimmauszählung nicht gegeben. Kein Stimmbürger kann sich tatsächlich sicher sein, dass seine Stimme auf dem E-Voting System landete und wenn, ob seine Stimme korrekt übermittelt und ausgewertet wurde.

Durch die mangelnde Transparenz sinkt auch das Vertrauen in die Korrektheit von E-Voting. Jedoch sind auch die beiden anderen Kanäle wie eine Black Box. Von daher ist die Transparenz gemäss Bundeskanzlei⁶⁰ auf gleichem Level wie beim Urnengang und der brieflichen Stimmabgabe.

⁵⁹ Bericht Leuenberger / Huber-Hotz (2006)

⁶⁰ Interview Weber / Muster (2011)

Die Sicherheit wurde bisher nicht ausreichend umgesetzt. Einerseits sollte es sehr schwer sein, gekaufte oder geklaute Stimmen zu nutzen. Andererseits ist bisher kein E-Voting System ausreichend von allen möglichen Hackerangriffen geschützt. Da dieses Unterfangen kaum zu realisieren ist, soll gemäss Bundeskanzlei⁶¹ ein systematisches Manipulieren unmöglich sein. Kleinere Manipulationen sind genau wie beim Urnengang und der brieflichen Abstimmung kaum auszuschliessen.

Eine weitere Schwäche ist gemäss Denis Simonet⁶² der Faktor Mensch. Ohne Menschen ist kein E-Voting möglich. Deshalb muss nicht nur das Vertrauen zum E-Voting System vorhanden sein, sondern auch das Vertrauen in die Verantwortlichen des E-Voting Systems. Würden beispielsweise nur vier Personen Zugriff und das Recht auf die Auszählung haben, könnte ein privates Unternehmen oder eine Partei oder sonstige politische Organisation diese vier Personen kaufen (4 x 100'000 Fr.). Wenn ein Wahlergebnis dadurch manipuliert und verändert werden könnte, würde es je nach Umstand Wert sein, 4 mal 100'000 Fr. auszugeben.

2.2.4 Quantitativer (finanzieller) Nutzen für die Benutzer und Verwaltungen

Aus zuvor genannten technischen und organisatorischen Stärken und Schwächen ergibt sich folgender quantitativer Nutzen für die Benutzer und Verwaltungen von E-Voting:

Da der Stimmbürger durch E-Voting weder Geld verdient noch Geld ausgeben muss, entsteht kein finanzieller Nutzen für den Benutzer. Höchstens die eingesparte (Reise-)Zeit inkl. der Kosten für den Weg zur Urne oder die Briefmarken bei der brieflichen Stimmabgabe könnte als Nutzen ausgewiesen werden.

Für die Verwaltung ist der administrative Aufwand bei E-Voting kleiner als bei den beiden traditionellen Kanälen. Es braucht weniger menschliche Ressourcen bei E-Voting. Allerdings entstehen zusätzliche Kosten für das E-Voting System inkl. der ganzen Infrastruktur-, Betriebs-, Verwaltungs- und Wartungskosten.

⁶¹ Interview Weber / Muster (2011)

⁶² Interview Simonet (2011)

3 Analyse von E-Voting Projekten

Seit dem Jahr 2002 wurden die ersten E-Voting Pilotprojekte entwickelt und durchgeführt. Da diese erfolgreich waren, gibt es seit dem 31. Mai 2006 die Bestrebung des Bundesrats für eine Einführung von „Vote électronique“ in Schritten. Dies bedeutet, dass sich zusätzliche Kantone an E-Voting Projekten beteiligen können. Das letztendliche Ziel von „Vote électronique“ ist die flächendeckende Einführung von E-Voting als dritter Abstimmungskanal neben der Urne und der brieflichen Stimmabgabe. Deshalb wurde das „Bundesgesetz über die politischen Rechte“ anfangs 2008 entsprechend angepasst.⁶³ Bei jedem E-Voting Projekt findet eine intensive Zusammenarbeit zwischen den beteiligten Personen der Kantone und der Bundeskanzlei statt.

3.1 Gemeinsamkeiten & Unterschiede zwischen den E-Voting Projekten

Dieses Kapitel beschreibt die Gemeinsamkeiten und Unterschiede zwischen drei ausgewählten E-Voting Projekten in der Schweiz. Als Projekte wurden E-Voting Vorhaben im Kanton Zürich, Kanton Genf und Kanton Neuenburg untersucht. Der Grund für den Vergleich dieser drei E-Voting Projekte ist, dass das E-Voting in jedem dieser Kantone anders funktioniert und weil durch das direkte Vergleichen dieser drei Projekte ein optimaler E-Voting Prozess modelliert werden kann, welcher die Vorteile der verschiedenen Projekte zu kombinieren versucht. Dabei werden die für die Prozessmodellierung relevanten Gemeinsamkeiten und Unterschiede zwischen den drei untersuchten E-Voting Projekte aufgezeigt. Die eigentlichen Zusammenfassungen der E-Voting Projekte befinden sich im Anhang. Die untenstehenden Informationen sind aus diesen Zusammenfassungen im Anhang entnommen worden.

Gemeinsamkeiten und Unterschiede zwischen den E-Voting Projekten	
Gemeinsamkeiten zwischen den E-Voting Projekten	
Zürich zu Neuenburg	Harmonisierung und Verknüpfung der Stimmregister
Zürich zu Genf	PIN-Code mit Rubbelfeld / Fingerprint nutzbar
Genf zu Neuenburg	Zentrales Stimmregister geführt durch den Kanton
Unterschiede zwischen den E-Voting Projekten	
Zürich zu Neuenburg	Elemente des Stimmrechtsausweis / Registrierung und Anmeldung an E-Voting System nötig / Bar- & PIN-Code und UserID vs. Validierungs- und Bestätigungscode / Auswertung der Stimmen / dezentrale vs. zentrale Stimmregister / Online-Liste zur Überprüfung, ob die Stimme durch das E-Voting System aufgenommen wurde

⁶³ SR 161.1 (2010)

Gemeinsamkeiten und Unterschiede zwischen den E-Voting Projekten	
Unterschiede zwischen den E-Voting Projekten	
Zürich zu Genf	8- vs. 16-stellige User-ID / Bestätigungssymbol vs. Kombination mit Bild als Schutz vor Missbrauch / zentrales vs. dezentrales Stimmregister / Seite der Authentifikation zertifiziert / Auswertung durch WABSTI (Auswertungssystem) vs. Auswertung durch kantonale Behörden / C-Ausländer und Auslandschweizer auch stimmberechtigt
Genf zu Neuenburg	Elemente des Stimmrechtsausweis / Auswertung durch Kanton vs. Auswertung am Guichet Unique / Bar- & PIN-Code und UserID vs. Validierungs- und Bestätigungscode / Online-Liste zur Überprüfung, ob die Stimme durch das E-Voting System aufgenommen wurde

Tabelle 13 / Gemeinsamkeiten und Unterschiede zwischen den E-Voting Projekten

3.2 Beispielprozess für E-Voting

Folgender Abschnitt zeigt die Modellierung eines Beispielprozesses für E-Voting. Dieser Beispielprozess setzt sich aus den Stärken der drei untersuchten Projekte zusammen.

Bei der Betrachtung der drei E-Voting Projekte fällt auf, dass Genf und Zürich einen ähnlichen Ansatz verwenden während Neuenburg einen anderen Ansatz wählt. Für die flächendeckende Einführung ist es zwingend vor einer Nutzung von E-Voting eine Harmonisierung und Verknüpfung sämtlicher Stimmregister vorzunehmen.

Während in den meisten Westschweizer Kantone (auch Genf und Neuenburg) problemlos Stimmregister zentral durch den Kanton geführt werden, ist dies in der Deutschschweiz mit Ausnahme von Basel-Stadt nicht der Fall. E-Voting auf einem Portal wie in Neuenburg (Guichet Unique) oder auf einer Website mit https (Hypertext Transfer Control Protocol Secure), hat unterschiedliche Vor- und Nachteile. Beim Guichet Unique wird die Anzahl an potentiellen Stimmbürgern eingeschränkt, da diese sich zuerst beim Guichet Unique registrieren müssen. Allerdings bedeutet dies auch, dass das Missbrauchsrisiko (Klau eines Stimmrechtsausweis mit anschliessender Nutzung) kleiner ist.

Laut Giampiero Beroggi⁶⁴, dem Chef des Statistischen Amtes des Kantons Zürich, gibt es Probleme mit WABSTI, weshalb E-Voting im Jahr 2011 im Kanton Zürich nicht für gemeindeübergreifende Abstimmungen benutzt werden darf. Dies ist ein Problem, da meistens gleichzeitig mit den kommunalen Abstimmungen auch kantonale und eidgenössische Abstimmungen durchgeführt werden.

⁶⁴ DRS (2010)

E-Voting im Kanton Zürich hat auch den Nachteil, dass bei Entwendung oder Verlust eines Stimmrechtsausweises nur noch das Geburtsdatum eines Stimmbürgers herausgefunden werden muss, um für eine fremde Person abzustimmen. Ein Geburtsdatum herauszufinden ist jedoch dank „Social Networks“ heute relativ einfach.

In Genf wird dabei ein Attribut mehr verwendet. Dort muss nämlich zusätzlich noch die Heimatgemeinde eingegeben werden. Zudem wird die sechzehnstellige User-ID aus den zuvor genannten Attributen (Geburtsdatum und Heimatgemeinde) sowie dem Geschlecht generiert. Daher ist eine Manipulation schwieriger vorzunehmen.

Um im Kanton Genf Zugriff auf das E-Voting System zu erhalten, muss die sechzehnstellige User-ID eingegeben werden. In Neuenburg reichen die bei der Registrierung erstellten Login-Daten des Guichet-Unique, um auf das E-Voting System zuzugreifen. Um E-Voting auf dem Guichet Unique zusätzlich zu schützen, könnte zusätzlich wie in Genf ein sechzehnstelliger Code generiert werden, welcher dann innerhalb des Guichet Unique auf dem E-Voting System eingegeben werden muss, bevor der Stimmbürger Zugriff auf das E-Voting System erhält. Dadurch ist das E-Voting System doppelt geschützt vor unerlaubtem Zugriff.

Die eigentliche Stimmabgabe ist bei allen drei untersuchten E-Voting Projekten ähnlich. Im Kanton Zürich werden die Stimmen mit dem PIN-Code unter dem Rubbelfeld sowie einem Bestätigungssymbol und der Angabe des Geburtsdatums überprüft, im Kanton Neuenburg mit einem Validierungscode und in Genf mit dem PIN-Code unter dem Rubbelfeld sowie der Angabe des Datums und der Zeit der Stimmabgabe. Somit findet bei jedem Projekt eine Überprüfung der abgegebenen Stimmen statt.

Im Kanton Neuenburg wird zusätzlich nach der Abgabe der Stimme eine Empfangsbestätigung an den Stimmbürger übermittelt und gleichzeitig ein Bestätigungscode generiert, welcher ebenfalls dem Stimmbürger übermittelt wird. Der Bestätigungscode sollte dem Code auf dem Stimmrechtsausweis entsprechen.

Nach Abschluss der Abstimmung kann auf einer im Internet publizierten Liste überprüft werden, ob der persönliche Bestätigungscode aufgelistet ist. Ist dies der Fall, wurde die Stimme korrekt zum Guichet Unique übermittelt. Dieser Bestätigungscode wird getrennt von der Stimme generiert. Dadurch kann überprüft werden, WER E-Voting nutzte, jedoch nicht WIE abgestimmt wurde.

Aus den beschriebenen Gemeinsamkeiten und Unterschiede zwischen den drei untersuchten E-Voting Projekten, wurde folgender Beispielprozess⁶⁵ aus Sicht der Stimmbürger modelliert und definiert:

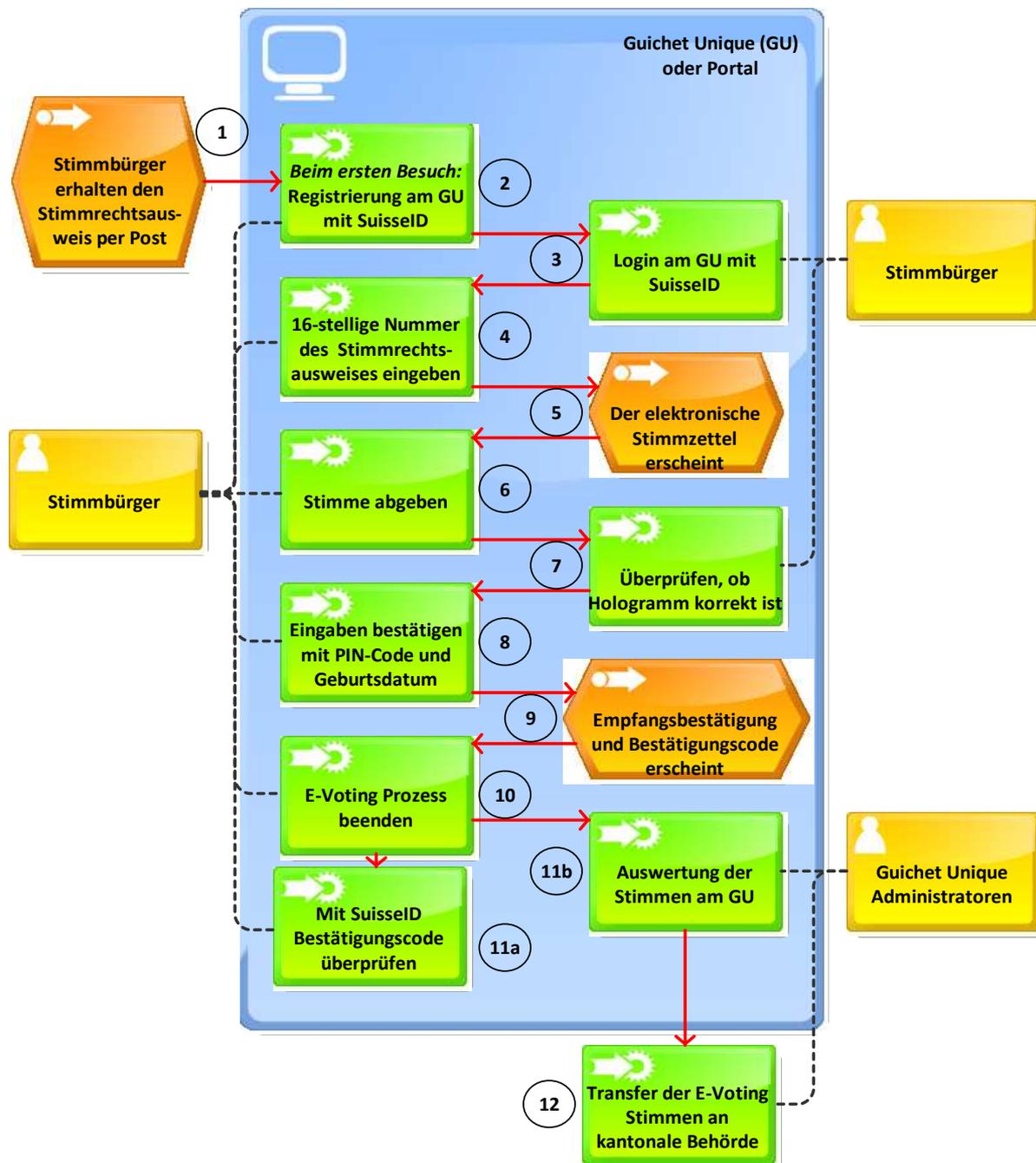


Abbildung 2 / Beispielprozess für E-Voting

⁶⁵ Quelle: eigene Darstellung

Folgende Tabelle erklärt den modellierten E-Voting Beispielprozess im Detail.

Nr.	Erklärung
1	Einige Wochen vor dem Wahlsonntag erhalten alle Stimmbürger ihren Stimmrechtsausweis, egal ob diese E-Voting Nutzen oder nicht.
2	Die Registrierung ist nur bei der erstmaligen Nutzung des Guichet Unique (GU) durchzuführen. Die Registrierung erfolgt persönlich bei einer amtlichen Stelle mit einem Formular und der Unterschrift per Hand.
3	Nach der Registrierung erhält der Stimmbürger die Login-Daten für den GU per Post. Mit diesen Login-Daten kann der Stimmbürger nun Zugriff auf den GU erhalten.
4	Um Zugriff auf das E-Voting System zu erhalten, muss der Stimmbürger die 16-stellige Nummer eingeben, welche sich auf dem Stimmrechtsausweis befindet.
5	Nach der Eingabe dieser Nummer wird dem Stimmbürger der elektronische Stimmzettel angezeigt.
6	Der Stimmbürger kann nun seine Stimme abgeben, in dem er einerseits bei Abstimmungen Kreuze setzt und andererseits bei Wahlen auf die gewünschten Personen / Parteien klickt.
7	Damit sichergestellt ist, dass sich der Benutzer tatsächlich auf dem E-Voting System befindet, erscheint auf der Seite der Stimmabgabe ein Hologramm mit dem Kantonswappen. Dieses Hologramm muss auf dem Stimmrechtsausweis genau gleich aussehen, ansonsten liegt Manipulation vor.
8	Stimmen beide Hologramme überein, wird im nächsten Schritt der elektronische Stimmzettel noch einmal angezeigt. Dadurch kann der Benutzer sicherstellen, dass seine Eingaben korrekt übernommen wurden. Durch die Eingabe des PIN-Codes und des Geburtsdatum wird der elektronische Stimmzettel an die elektronische Urne übermittelt. Der PIN-Code befindet sich auf dem Stimmrechtsausweis unter einem Rubbelfeld. Durch das Rubbelfeld kann sichergestellt werden, dass nicht schon jemand anderes diesen Stimmrechtsausweis nutzte.
9	Nach dem der elektronische Stimmzettel an die elektronische Urne übermittelt wurde, wird eine Empfangsbestätigung und zusätzlich ein Bestätigungscode angezeigt.
10	Der Stimmbürger beendet nun den E-Voting Prozess, in dem er sich aus dem System ausloggt.

Nr.	Erklärung
11a	Auf einer Online-Liste auf dem GU kann der Stimmbürger überprüfen, ob sein Bestätigungscode dort aufgelistet wird. Ist dies der Fall, kann der Stimmbürger sicher sein, dass seine Stimme korrekt in der elektronischen Urne landete.
11b	Die Administratoren, respektive die Hauptverantwortlichen des GU werten nun die E-Voting Stimmen der elektronischen Urne aus.
12	Damit die E-Voting Stimmen mit den Stimmen der physischen Urne und der brieflichen Abstimmung addiert werden können, werden die ausgewerteten E-Voting Stimmen gesichert an die kantonalen Behörden übermittelt.

Tabelle 14 / Detaillierterklärung E-Voting Beispielprozess

3.3 Beurteilung des Beispielprozesses

Wie beim Beispielprozess zu sehen ist, können die verschiedenen Stärken der untersuchten Projekte teilweise kombiniert werden. Der Zugriff auf das E-Voting System ist beispielsweise gleich wie in Neuenburg und erfolgt über ein Portal / Guichet Unique.

Gemäss der Bundeskanzlei⁶⁶ macht eine Optimierung für die Praxis kaum Sinn, da es nicht das Ziel ist, ein Gesamtschweizerisches E-Voting System zu entwickeln. Die Kantone Zürich, Genf und Neuenburg hatten drei unterschiedliche Ansätze gewählt. Dies geschah aus strategischen Gründen. Dadurch sollen die Stärken und Schwächen der unterschiedlichen E-Voting Systeme vergleichbar sein, um zu sehen, welcher Prozess wie gut funktioniert.

Ein weiterer Grund ist gemäss Herrn Muster⁶⁷ die Verhinderung eines Klumpenrisikos. Gäbe es nur ein Gesamtschweizerisches E-Voting System, könnten einerseits keine Vergleiche gemacht werden und andererseits könnte bei einem Ausfall des E-Voting Systems kein Stimmbürger, egal in welchem Kanton, E-Voting überhaupt nutzen. Zudem würde die Suche nach einer alternativen Lösung erschwert werden.

Zudem liegt die Verantwortung von E-Voting bei den Kantonen und es ist nicht vorgesehen, dass sich sämtliche Kantone zusammenschliessen, um ein gemeinsames E-Voting System zu definieren. Bezüglich des Aufwands wäre dies sehr schwer umzusetzen, da jeder Kanton unterschiedliche Fristen bei Wahlen kennt. Beispielsweise ist im Kanton Bern der Wahlanmeldeschluss am 08.08.2011 und am 15.08.2011 ist Listenbereinigungsschluss.

⁶⁶ Interview Weber / Muster (2011)

⁶⁷ Interview Weber / Muster (2011)

Im Kanton Zürich hingegen ist der Wahlanmeldeschluss am 11.08.2011 und erst am 29.08.2011 ist Listenbereinigungsschluss. In der Schweiz ist es üblich zwei Monate vor den Wahlen eine Vorlaufszeit zu geben, um die Wahlen vorzubereiten. Bei Stichwahlen sind diese Fristen jedoch kürzer und variieren von Kanton zu Kanton.

Würden nun Optimierungen oder Änderungen bezüglich Stimmrechtsausweise, bezüglich E-Voting oder bezüglich des generellen Wahlprozesses vorgenommen, könnten diese kaum umgesetzt werden. Der Grund dafür ist, neben den unterschiedlichen Fristen, dass in der Schweiz regelmässig Wahlen und Abstimmungen stattfinden. Da die Vorlaufszeit zu berücksichtigen ist, gäbe es nur kurze und nur wenige Zeitfenster, in welchen die Optimierungen oder Änderungen durchgeführt werden könnten.⁶⁸

Ein weiterer Fakt ist, dass fast jede Gemeinde eine andere Software für die Einwohnerkontrollregister benutzt. Aus diesen Einwohnerkontrollregistern werden Daten anschliessend für die Stimmregister extrahiert. Die Kantone schreiben nur die Formate der Dateien und die Schnittstellen vor. Teilweise nutzen die Gemeinden sogar Microsoft Excel oder Microsoft Access, um die Daten zu managen. Daraus ergeben sich grosse organisatorische Probleme bezüglich einer Harmonisierung der Stimmregister innerhalb eines Kantons.

eCH Standards versuchen dieses Problem zu minimieren durch die Entwicklung einer Standardisierung für den Austausch der Daten zwischen Bund, Kantonen und Gemeinden. eCH fördert, entwickelt und verabschiedet E-Government-Standards. Eine Schwierigkeit dabei ist, dass die Software, die Formate sowie die Schnittstellen heterogen sind. Trotz eines eCH Standards können Daten in verschiedenen Formaten geliefert werden, da diese Standards unterschiedlich interpretiert werden können. Beispielsweise kann die Adresse von der Hausnummer getrennt werden oder aber auch nicht. Bei der Erstellung der Stimmregister für Auslandschweizer ist diese Tatsache ein noch grösseres Problem, da beispielsweise die Adressen anders aufgebaut sein und andere Attribute beinhalten können.⁶⁹

Die Kantone haben deshalb grosse Mühe bei der Entwicklung eines Minimalstandards für die Stimmrechtsausweise. Sieben Kantone schlossen sich zusammen und wollten die Stimmrechtsausweise angleichen.⁷⁰ Nach langer Zeit konnten sich die beteiligten Kantone nur auf einen Minimalstandard einigen. Allerdings existieren trotz des Minimalstandards noch Unterschiede in den Stimmrechtsausweisen.

⁶⁸ Interview Weber / Muster (2011)

⁶⁹ Interview Vizarro (2011)

⁷⁰ Interview Weber / Muster (2011)

Solange die Stimmrechtsausweise in jedem Kanton anders aussehen, könnte keine Lösung für ein Gesamtschweizerisches E-Voting System gefunden werden.

Würden die Stimmregister kantonal geführt, würden die technischen Probleme auf ein Minimum reduziert, da nur noch eine Software verwendet wird. Allerdings erhöht sich der organisatorische Aufwand, da die nötigen Personalressourcen beim Kanton nicht vorhanden sind. Dadurch würde auch die Kundennähe oder Kundenfreundlichkeit reduziert werden.⁷¹

Es ist jedoch vorgesehen, dass die Stimmregister der Auslandschweizer in diversen Kantonen zentral durch den Kanton und nicht durch die Gemeinden geführt werden, wodurch der technische Aufwand und die Komplexität reduziert werden.

Bei der flächendeckenden Einführung von E-Voting würden solche Kantone jedoch zwei unterschiedliche Systeme für die Stimmregister verwenden. Ein System wäre für harmonisierte Stimmregister für Inlandschweizer, welches dezentral durch die Gemeinden geführt wird. Das andere System wäre ein zentrales System für Auslandschweizer, welches durch den Kanton geführt wird. Wegen der Nutzung von zwei unterschiedlichen Systemen entstehen dadurch aber Mehrkosten im Vergleich zu einer gemeinsamen Lösung für Inland- und Auslandschweizer.⁷²

Ausser den Kantonen Zürich, Genf und Neuenburg, können auch andere Kantone bei den Nationalratswahlen 2011 E-Voting nutzen. Diese anderen Kantone übernehmen gemäss Frau Weber⁷³ eines der drei bestehenden E-Voting Systeme. Diese Kantone erhalten den Source Code des ursprünglichen Kantons, welcher das E-Voting System entwickelte. Allerdings dürfen diese E-Voting Systeme in diesen anderen Kantonen bei den Nationalratswahlen 2011 nur für Auslandschweizer zum Einsatz kommen. Der Grund dafür ist einerseits, dass dadurch die Anzahl an E-Voting Benutzern überschaubar ist und andererseits haben die Auslandschweizer den grössten Nutzen von E-Voting.

⁷¹ Interview Vizarro (2011)

⁷² Interview Vizarro (2011)

⁷³ Interview Weber / Muster (2011)

4 Kombination von SuisseID mit E-Voting

In diesem Kapitel wird auf die Kombination der SuisseID mit E-Voting eingegangen und aufgezeigt, welcher Nutzen und welche Risiken dabei entstehen und was sich im Vergleich zu einem ursprünglichen E-Voting Prozess verändert.

4.1 Einführung

Im Gegensatz zur brieflichen Abstimmung und dem Urnengang ist es ein grosses Problem von E-Voting, dass es theoretisch möglich ist, an einer Stelle mehrere tausend Stimmen zu manipulieren. Die SuisseID könnte diese Manipulation einschränken. Auch der Kauf oder Diebstahl von Stimmen ist momentan bei E-Voting möglich, da der Stimmrechtsausweis und einige Attribute über den Stimmbürger (Geburtsdatum und Heimatort) ausreichen, um für jemand anderes abzustimmen.

Wie bereits erwähnt ist es ein Problem von E-Voting, dass es vergleichsweise einfach ist, mehrere tausend Stimmen zu stehlen, kaufen oder manipulieren. Die SuisseID würde diesem Problem entgegenwirken. Bei einer Kombination von E-Voting und SuisseID müsste ein Betrüger auch in Besitz einer fremden SuisseID sein und gleichzeitig den Stimmrechtsausweis von dieser fremden Person besitzen.

Der Stimmrechtsausweis kommt, unabhängig welcher Kanal für das Abstimmen genutzt wird, immer per Post an. Der Grund dafür ist, dass ein Stimmbürger bis zuletzt entscheiden kann, ob er E-Voting nutzen oder über einen anderen Kanal seine Stimme abgeben will. Da dieser Stimmrechtsausweis per Post und nicht online empfangen wird, besteht keine Möglichkeit diesen Stimmrechtsausweis zu unterschreiben, wenn E-Voting genutzt wird.

Sowohl beim Urnengang als auch bei der brieflichen Abstimmung ist die Unterschrift auf dem Stimmrechtsausweis zwingend nötig. Aus diesem Grund kann die SuisseID höchstens für die Registrierung am E-Voting System und für das Login auf das E-Voting System verwendet, nicht aber für das Unterschreiben des Stimmrechtsausweises genutzt werden

Da der Schwerpunkt bei E-Voting in der Schweiz bei den Auslandschweizern liegt, müsste überlegt werden, wie die SuisseID unter den Auslandschweizern verbreitet werden könnte. Eine Möglichkeit ist, gemäss Herrn Hassenstein⁷⁴, die Verbreitung der SuisseID durch die Botschaften. Wenn die Botschaften als Reseller fungieren könnten, dann könnten sich Auslandschweizer über die Botschaft oder ein Konsulat die SuisseID beschaffen.

⁷⁴ Interview Hassenstein (2011)

Allerdings bräuchte es eine Weiterentwicklung der SuisseID Infrastruktur und des SuisseID Konzeptes. Danach könnte die SuisseID für diverse Behördengänge eingesetzt werden, beispielsweise für den Kontakt mit der Botschaft oder dem Konsulat oder wenn ein Wohnortwechsel gemeldet werden muss. In flächenmässig grossen Ländern wäre dieses Vorhaben sehr sinnvoll, da die Auslandschweizer nicht mehr weite Reisen in Kauf nehmen müssten, um Behördengänge durchzuführen.

Die Pilotprojekte im Kanton Zürich und Kanton Genf wurden laut Medien⁷⁵ in der Zwischenzeit zurückgestellt. In Genf war die rechtliche Unsicherheit ausschlaggebend, während in Zürich die hohen Kosten pro Stimmabgabe als Grund genannt wurden. Darunter leiden die Auslandschweizer besonders, da der Nutzen und das Bedürfnis bezüglich E-Voting gegeben sind. Im Hinblick auf die Nationalratswahlen im Jahr 2015 soll es jedoch für Auslandschweizer möglich sein, E-Voting zu nutzen.⁷⁶

Allerdings entsprechen die Aussagen in den Medien nicht der ganzen Wahrheit. Beispielsweise können die Auslandschweizer in vier Kantonen E-Voting bei den Nationalratswahlen 2011 einsetzen.⁷⁷ Gemäss der Bundeskanzlei⁷⁸ funktioniert das E-Voting System sowohl im Kanton Zürich, als auch im Kanton Genf und im Kanton Neuenburg. Es tauchten nur organisatorische Probleme auf, mit Ausnahme des technischen Problems mit WABSTI im Kanton Zürich. Die involvierten Personen und Kantone müssen nun Routine sammeln und sich an den E-Voting Prozess gewöhnen.

Im Bereich der eDemocracy könnte die SuisseID die Möglichkeit bieten, Online Unterschriften für Initiativen und Referenden zu sammeln. Da diese Arbeit jedoch den Fokus auf E-Voting legt, wird auf den Nutzen der SuisseID für die eDemocracy nicht weiter eingegangen.

⁷⁵ Computerworld (2011)

⁷⁶ Interview Weber / Muster (2011)

⁷⁷ Auslandschweizer Organisation (2011)

⁷⁸ Interview Weber / Muster (2011)

4.2 Beispielprozess einer Kombination von SuisseID mit E-Voting

Folgender Abschnitt zeigt die Modellierung eines Beispielprozesses für E-Voting kombiniert mit SuisseID. Dieser⁷⁹ lehnt sich an den Beispielprozess aus Kapitel 3.2: „Beispielprozess E-Voting“, an.

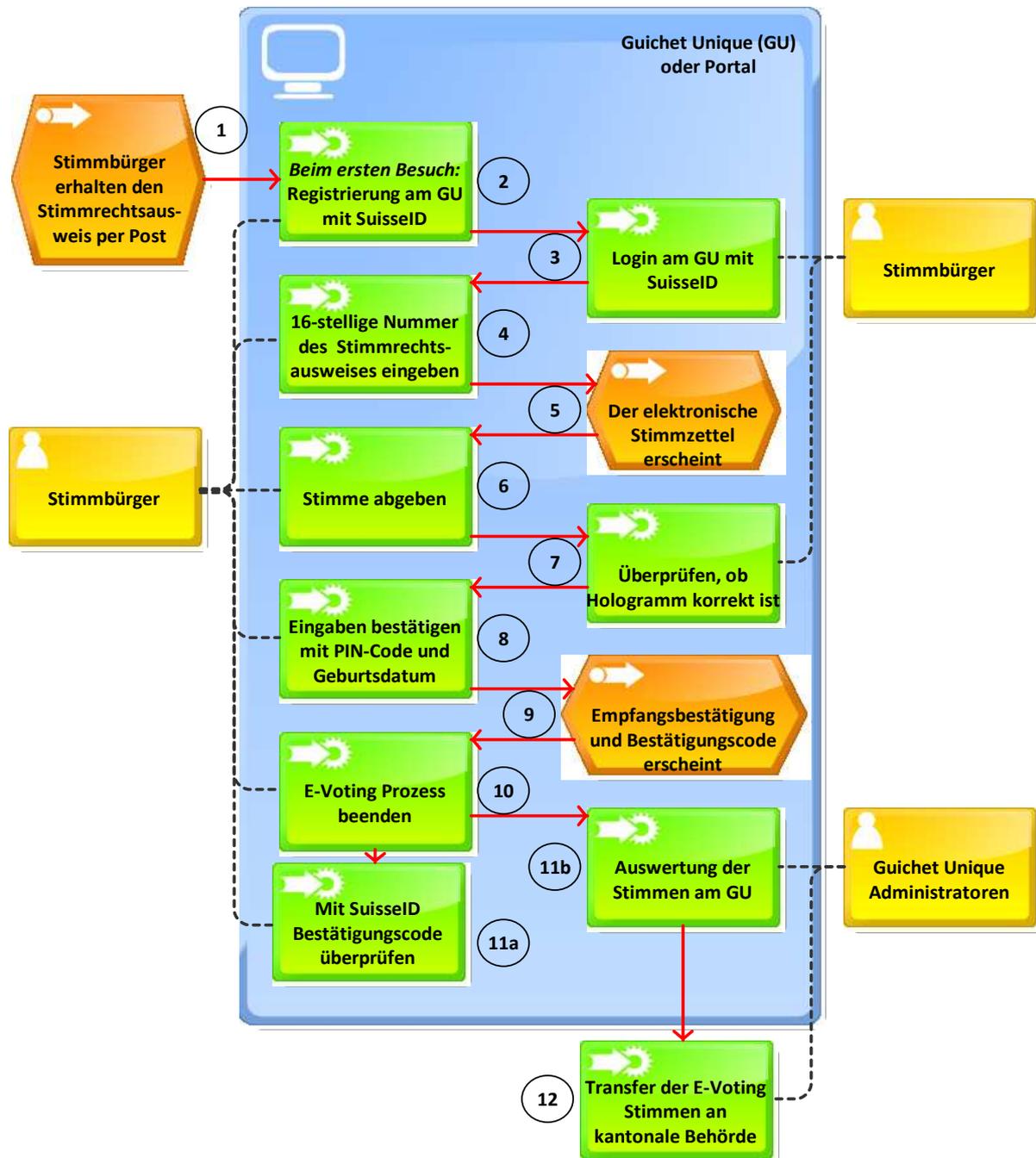


Abbildung 3 / Beispielprozess einer Kombination der SuisseID mit E-Voting

⁷⁹ Quelle: eigene Darstellung

4.3 Vergleich zum ursprünglichen E-Voting Beispielprozess

Folgende Tabelle zeigt, wie die SuisseID den ursprünglichen E-Voting Prozess verbessert und in welchen Schritten die Unterschiede ersichtlich werden.

Nr.	Ursprünglicher E-Voting Beispielprozess	Beispielprozess einer Kombination der SuisseID mit E-Voting
2	Der Registrierungsprozess muss physisch beim Gemeindeschalter erfolgen.	Der Registrierungsprozess kann Online durchgeführt werden.
3	Mit den per Post erhaltenen Login-Daten kann sich der Stimmbürger am E-Voting System einloggen.	Mit der SuisseID kann sich der Benutzer am E-Voting System einloggen.
11a	In einer Online-Liste muss der Stimmbürger manuell überprüfen, ob sein Bestätigungscode aufgelistet wird.	Mit der SuisseID kann der Stimmbürger direkt sehen, ob sein Bestätigungscode aufgelistet wird.

Tabelle 15 / Unterschiede zwischen den beiden Beispielprozessen

4.4 Analyse des Beispielprozesses einer Kombination von SuisseID mit E-Voting

Im zweiten modellierten Beispielprozess einer Kombination der SuisseID mit E-Voting ist zu sehen, dass die SuisseID nur beschränkt zum Einsatz kommen kann. Wie zu sehen ist, wird im Beispielprozess die SuisseID für drei Schritte verwendet. In den folgenden zwei Unterkapiteln wird auf den Nutzen und die Risiken einer solchen Kombination eingegangen.

4.4.1 Nutzenanalyse einer Kombination von SuisseID mit E-Voting

Folgende Tabelle beschreibt den Nutzen einer Kombination von SuisseID mit E-Voting im Detail.

Nutzen	Erklärung
Registrierung am Guichet Unique	Damit sich ein Stimmbürger am Guichet Unique registrieren kann, benötigt dieser nur noch eine SuisseID. Mit dieser SuisseID kann sich der Stimmbürger online registrieren und muss nicht mehr physisch am Schalter des Kantons oder der Gemeinde vorbei gehen. Allerdings ist dies beim Guichet Unique im Kanton Neuenburg nicht möglich und erlaubt, da die ID (Identitätskarte) vorgewiesen werden muss. Daher bräuchte es eine gesetzliche Lockerung, was das Registrieren an einem Guichet Unique betrifft.

Nutzen	Erklärung
Login am Guichet Unique (GU)	Nach der erfolgreichen Registrierung kann sich der Benutzer mit der SuisseID am GU einloggen. Im Gegensatz zum ursprünglichen Prozess benötigt der Stimmbürger keine Login-Daten vom Kanton sondern nur noch die SuisseID.
Überprüfung des Bestätigungscode	Mit der SuisseID kann der Bestätigungscode sofort angezeigt werden. Der Stimmbürger muss den Bestätigungscode nicht manuell überprüfen gehen.
Einschränkung von Stimmenklau, Stimmenkauf oder Mehrfachabstimmen	Stimmen zu klauen oder zu kaufen wird dank dem Einsatz der SuisseID wesentlich schwerer. Neben dem Stimmrechtsausweis müsste man noch im Besitz der SuisseID sein. Der Stimmenkauf würde sich nicht nur schwerer sondern auch teurer gestalten. Die Kosten für die SuisseID müssten auch bezahlt werden und zudem würde sich der ursprüngliche SuisseID Besitzer haftbar machen. Daher ist ein Stimmenkauf bei der Nutzung einer SuisseID um einiges kostspieliger.

Tabelle 16 / Nutzenanalyse einer Kombination von SuisseID mit E-Voting

4.4.2 Risikoanalyse einer Kombination von SuisseID mit E-Voting

Die Kombination der SuisseID mit E-Voting hat diverse Risiken. Folgende Tabelle beschreibt diese Risiken im Detail.

Nr.	Risiko	Erklärung
1	Stimmrechtsausweis kann nicht unterschrieben und online zur Verfügung gestellt werden	Solange der Stimmrechtsausweis für E-Voting Nutzer nicht Online zugestellt werden darf, ist es auch nicht möglich diesen Stimmrechtsausweis online zu signieren. Daher kann während der eigentlichen Stimmabgabe die SuisseID nicht sinnvoll eingesetzt werden. Wenn der Stimmrechtsausweis online verfügbar wäre, könnte dieser analog zum Urnengang und der brieflichen Abstimmung, unterschrieben werden. Allerdings ist dies gemäss Bundeskanzlei ⁸⁰ nicht vorgesehen, ansonsten hätte der Stimmbürger nicht die geheime Auswahl, über welchen Kanal er seine Stimme abgeben will. Daher ist die Wahrscheinlichkeit, dass dieses Risiko ständig bestehen bleibt bei 99,9 %.

⁸⁰ Interview Weber / Muster (2011)

Nr.	Risiko	Erklärung
2	Privatwirtschaft als Zielgruppe der SuisseID	Die SuisseID wurde für die Privatwirtschaft entwickelt. Der Fokus der SuisseID liegt bei B2B- und G2B-Geschäftsbeziehungen. Die Reseller sind in der Privatwirtschaft angesiedelt. E-Voting ist dagegen unter der Federführung des Bundes und der Kantone. Deshalb bringt eine Kombination gemäss Denis Simonet ⁸¹ die Gefahr, dass eine Abhängigkeit zur Privatwirtschaft entsteht.
3	Login bei falscher Zertifizierungsstelle	Auch das Login mit der SuisseID kann gemäss Denis Simonet ⁸² eine Gefahr darstellen, nämlich wenn die Zertifizierungsstelle manipuliert wird.
4	Keine staatlichen Attribute erlaubt	Wie bereits erwähnt wurde, ist die SuisseID vor allem für die Privatwirtschaft entwickelt worden. E-Voting richtet sich dagegen an eine andere Zielgruppe (G2C - Government to Customer). Diese Tatsache zeigt auf, dass der Einsatz einer SuisseID heikel ist. Deshalb sind auch keine staatlichen Attribute, wie die AHV-Nummer oder ID-Nummer zu verwenden, da sonst diese Attribute im Besitz von Unternehmen aus der Privatwirtschaft sind. Es macht wenig Sinn, wenn Stimmbürger für die Nutzung einer staatlichen Applikation die Privatwirtschaft miteinbeziehen.
5	Sonstige Sicherheitsrisiken der SuisseID	Die SuisseID als ganzes Konzept betrachtet ist nicht sicher genug, um es für E-Voting einzusetzen. Auch wenn sich die Sicherheit mit der Nutzung von Class 2 Reader erhöht, gibt es immer noch weitere Schwachstellen, wie das hierarchisch aufgebaute X.509 Zertifikat.
6	Einsatz mehrerer SuisseIDs	Da ein Stimmbürger mehrere SuisseIDs besitzen kann, müsste sichergestellt werden, dass nur eine SuisseID für E-Voting verwendet wird.
7	Kein gesamt-schweizerisches E-Voting System	Wie im Kapitel 3.3: „Beurteilung des Beispielprozesses“ erwähnt, wird es in der Schweiz kaum ein gesamtschweizerisches E-Voting System geben. Wenn nun jeder Kanton einen unterschiedlichen Ansatz wählt, dann muss auch die Nutzung der SuisseID von Kanton zu Kanton unterschiedlich ermöglicht werden. Die Kosten einer Kombination sind höher als der Nutzen.

Tabelle 17 / Risikoanalyse einer Kombination von SuisseID mit E-Voting

⁸¹ Interview Simonet (2011)⁸² Interview Simonet (2011)

5 Folgerungen

In diesem Kapitel wird auf Folgerungen aus den vorherigen Kapiteln eingegangen. Dabei werden zuerst die Problemfelder sowohl mit Einsatz der SuisseID als auch ohne den Einsatz der SuisseID beschrieben. Im nächsten Schritt werden mögliche Optimierungsmassnahmen definiert. Anschliessend wird überprüft, ob und wie sich der Beispielprozess verändern würde und welcher Nutzen dabei entsteht.

5.1 Problemfelder von E-Voting

E-Voting hat, wie bereits erwähnt, einige Stärken sowohl für die Stimmbürger als auch für die Verwaltungen. Allerdings sind gewisse Problemfelder vorhanden oder entstehen durch die Kombination von E-Voting mit SuisseID. In diesem Abschnitt werden diese Problemfelder detailliert beschrieben und jeweils begründet.

5.1.1 Problemfelder ohne Einsatz von SuisseID

Die Schwächen und Problemfelder von E-Voting ohne den Einsatz der SuisseID sind im Kapitel 2.2.2: „Analyse der Stärken und Schwächen von E-Voting“ in den Tabellen 14 und 16 aufgelistet.

5.1.2 Problemfelder mit Einsatz von SuisseID

Die im Kapitel 4.4.2: „Risikoanalyse einer Kombination von SuisseID mit E-Voting“ beschriebenen Risiken werden nun in einem Risikograph⁸³ klassifiziert, um danach auf mögliche Massnahmen einzugehen, falls sich das Risiko in einem kritischen Bereich befindet.

	Auswirkungen					Legende:
Wahrscheinlichkeit	0.2	0.4	0.6	0.8	1	
1	4	6	2, 5	1	7	Rot = kritisch
0.8						Gelb = zu beachten
0.6						Grün = tolerierbar
0.4					3	
0.2						

Abbildung 4 / Klassifizierte Risiken einer Kombination von SuisseID mit E-Voting

⁸³ Quelle: eigene Darstellung

Folgende Tabelle zeigt mögliche Massnahmen, um die vorhandenen und zuvor beschriebenen Risiken zu minimieren oder zu beseitigen, da sich kein Risiko in einem tolerierbaren Bereich befindet.

Nr.	Mögliche Massnahme	Bewertung
1	Da es nicht vorgesehen ist, dass die Stimmbürger den Stimmrechtsausweis online erhalten, kann dieses Risiko weder beseitigt, noch minimiert werden.	Die SuisseID mit dem heutigen Konzept kann E-Voting nur am Rande, wie beispielsweise beim Login auf das E-Voting System, unterstützen.
2	Mit einer Konzepterneuerung oder der Einführung von einer digitalen ID für E-Voting könnte dieses Problem mindestens minimiert werden. Im Kapitel 5.2.1: „Mit SuisseID oder ähnlichen Konzepten“ werden mögliche Optimierungsmassnahmen beschrieben.	Die SuisseID mit dem heutigen Konzept wurde für eine andere Zielgruppe entwickelt. Dies ist ein Risiko, da einerseits wenn die Zertifizierungsstelle brach liegt, die Nutzung der SuisseID nicht mehr möglich ist und andererseits weil dadurch eine staatliche Applikation abhängig von der Privatwirtschaft ist.
3	Es braucht eine Sensibilisierung der E-Voting Benutzer betreffend einer genauen Überprüfung, ob die Zertifizierungsstelle tatsächlich korrekt ist, da eine Manipulation fatale Folgen haben könnte.	Es ist schwer zu überprüfen und zu garantieren, dass jeder E-Voting Benutzer bei jeder Stimmabgabe eine Überprüfung der Zertifizierungsstelle vornimmt. Daher könnte dieses Risiko nur minimiert werden.
4	Nur mit einer Konzepterneuerung könnte es ermöglicht werden, staatliche Attribute zu verwenden. Allerdings bräuchte es eine Anpassung der gesetzlichen Richtlinien.	Die SuisseID mit dem heutigen Konzept, darf eindeutig identifizierende Attribute verwenden. Die Auswirkungen sind jedoch gering, da die Stimmbürger bei bisherigen E-Voting Systemen nur Attribute verwenden, welche auch die SuisseID besitzen darf.
5	Bei der Wahl eines dezentralen, nicht hierarchisch aufgebauten Zertifikates wie Open PGP, könnten zumindest die Nachteile des X.509 Zertifikates beseitigt werden. Die Nutzung der Class 2 Reader, wird bereits ermöglicht, allerdings nur auf Verlangen.	Es benötigt eine Konzepterneuerung, um die generellen Schwachstellen oder zumindest die Schwächen des X.509 Zertifikates zu beseitigen.

Nr.	Mögliche Massnahme	Bewertung
6	<p>Dafür gibt es gemäss Herrn Hassenstein⁸⁴ drei Möglichkeiten:</p> <ol style="list-style-type: none"> 1. Physischer Registrationsprozess: Wenn alle SuisseID-Benutzer in einer Liste geführt würden, könnte von der SuisseID Nummer ein Hash-Wert erzeugt werden, welcher mit dem SuisseID Benutzer verknüpft wird. Wenn einem SuisseID Benutzer mehrere Hash-Werte zugewiesen werden, wird dies sofort entdeckt. 2. Attribut, welches nur einmalig ist: Z.B. AHV-Nummer 3. PIN-Code: Mit einem PIN-Code wird erkannt, wenn ein Stimmbürger mit einer anderen SuisseID denselben PIN-Code eingibt. 	<p>Durch die von Herrn Hassenstein beschriebenen Möglichkeiten, wie der Einsatz mehrerer SuisseIDs unterbunden werden kann, können die Auswirkungen eines Versuchs einer Mehrfachabstimmung klein gehalten werden. Die zweite Möglichkeit ist allerdings auszuschliessen, weil die AHV-Nummer nicht verwendet werden darf.</p>
7	<p>Diese Risiko lässt sich weder minimieren noch lässt es sich beseitigen, da es sich um einen strategischen Entscheid handelt und somit unabhängig von der SuisseID ist, egal wie sicher diese ist. Daher müsste das ganze E-Voting Konzept erneuert werden, damit ein Gesamtschweizerisches E-Voting System entwickelt werden könnte.</p>	<p>Wegen dieser Tatsache würde die SuisseID in jedem Kanton unterschiedlich eingesetzt werden - wenn überhaupt. Dadurch entstehen Insellösungen, was die Benutzerfreundlichkeit auf ein Minimum reduziert, vor allem wenn ein Stimmbürger oft den Kanton wechselt.</p>

Tabelle 18 / Mögliche Massnahmen um die Risiken einer Kombination zu minimieren oder zu beseitigen

⁸⁴ Interview Hassenstein (2011)

5.2 Mögliche Optimierungsmassnahmen für E-Voting

Folgender Abschnitt beschreibt mögliche Optimierungsmassnahmen für E-Voting, sowohl bei einer Kombination mit der SuisseID als auch ohne die Nutzung einer SuisseID.

5.2.1 Mit SuisseID oder ähnlichen Konzepten

Damit die im Kapitel 4.4.2: „Risikoanalyse einer Kombination von SuisseID mit E-Voting“ erwähnten und beschriebenen Risiken beseitigt werden können, werden nun mögliche Optimierungsmassnahmen mit der SuisseID oder ähnlichen Konzepten beschrieben.

a) Staatliche E-Voting ID

Eine Möglichkeit ist die Entwicklung einer digitalen ID speziell für E-Voting oder E-Democracy. Dadurch könnte sichergestellt werden, dass der Bund der einzige Reseller ist, wodurch die Abhängigkeit zur Privatwirtschaft vermieden wird. Mit einer gesetzlichen Anpassung könnte auch erzielt werden, dass jede Person nur eine E-Voting ID besitzen kann. Zudem erhöht sich die Sicherheit, da nur noch eine Zertifizierungsstelle auf ihre Korrektheit überprüft werden muss. Allerdings überwiegen die Nachteile einer solchen Lösung. Eine E-Voting ID ist nicht sehr benutzerfreundlich, da diese ID nur für Abstimmungen und Wahlen (und evtl. für die Unterschrift bei Initiativen und Referenden) eingesetzt werden kann. Die SuisseID hingegen kann für diverse und total unterschiedliche Zwecke eingesetzt werden. Daher wäre der Kosten vs. Nutzen Effekt sehr wahrscheinlich negativ, da die Vorteile einer solchen Lösung kaum einen Mehrwert bringen.

b) Konzepterneuerung der SuisseID

Eine weitere Möglichkeit ist die Weiterentwicklung oder Konzepterneuerung der SuisseID. Einerseits könnte man durchsetzen, dass jede Person nur über eine SuisseID verfügen darf, wodurch ein Mehrfachabstimmen als auch beim Sammeln von Unterschriften für Initiativen und Referenden ein mehrfaches Unterschreiben verhindert würde. Allerdings würde ein solches Konzept wohl durch den Datenschützer nicht unterstützt werden, da eine SuisseID nicht als Identitätskarte dienen darf. Eine Konzepterneuerung könnte aber auch schon nur per Default die Nutzung von Class 2 Readern voraussetzen oder ein anderes Zertifikat wie Open PGP nutzen, wodurch sich die Sicherheitsrisiken erheblich reduzieren. Zudem könnten zusätzlich die Kantone oder der Bund als Reseller agieren, damit der Austausch von Informationen ohne die Privatwirtschaft stattfinden kann.

Bewertung E-Voting mit SuisseID oder ähnlichen Konzepten

Eine E-Voting ID kann nicht für das Unterschreiben des Stimmrechtsausweises verwendet werden, da diese weiterhin per Post an die Stimmbürger gelangen.

Das Gleiche gilt für eine Konzepterneuerung bei der SuisseID. Bisher war die Nutzung von E-Voting auch ohne die SuisseID oder einem anderen Konzept wie einer E-Voting ID möglich. Durch die Tatsachen, dass einerseits kein Gesamtschweizerisches E-Voting System geplant ist und andererseits dass die SuisseID an sich Schwachstellen besitzt, wären die Risiken einer solchen Lösung grösser als der daraus erzeugte Nutzen.

Die E-Voting ID müsste jedem Stimmbürger gratis überreicht werden, da die Stimmbürger keine Mehrkosten für E-Voting akzeptieren würden. Wenn die E-Voting ID für den Stimmbürger nicht kostenlos ist, würde dies dem demokratischen Grundsatz „Allgemein“ widersprechen. Eine Konzepterneuerung würde im Vergleich zu einer E-Voting ID benutzerfreundlicher sein, da der Einsatz vielfältiger ist und es sich dadurch eher lohnt, eine SuisseID zu beschaffen. Allerdings widerspricht dieser Ansatz dem demokratischen Grundsatz „Gleich“, denn Stimmbürger ohne SuisseID könnten nicht E-Voting nutzen. Die Voraussetzung einer SuisseID für die Nutzung von E-Voting ist eine Einschränkung, solange nicht jeder Stimmbürger eine SuisseID besitzt.

E-Voting hat vor allem für Auslandschweizer den grössten Nutzen. Deshalb müsste eine SuisseID oder eine E-Voting ID auch unter sämtlichen stimmberechtigten Auslandschweizern kostenlos verbreitet werden. Die einzige Möglichkeit wäre, dass die Botschaften / Konsulate als Reseller agieren. Ansonsten müssten die Auslandschweizer in die Schweiz kommen, um eine SuisseID oder eine E-Voting ID zu erhalten. Dadurch ist zu sehen, dass der Einsatz einer aktuellen SuisseID oder einer E-Voting ID besonders für Auslandschweizer wenig praktikabel wäre.

5.2.2 Ohne SuisseID

Folgender Abschnitt zeigt ein Beispiel eines optimierten E-Voting Systems ohne die Nutzung der SuisseID.

c) PI-Vote

Da E-Voting durchaus Stärken besitzt, entschied sich die Piratenpartei Schweiz für den Aufbau und die Nutzung von E-Voting und entwickelte das E-Voting System „PI-Vote“, das laut Partei sowohl sicher als auch transparent und anonym ist. Die drei im Kapitel 3.1: „Gemeinsamkeiten und Unterschiede zwischen den E-Voting Projekten“ untersuchten E-Voting Projekte konnten laut Denis Simonet⁸⁵ jeweils mindestens einer dieser drei Eigenschaften (Transparenz, Sicherheit, Anonymität) nicht ausreichend erfüllen.

⁸⁵ Interview Simonet (2011)

Deshalb erfüllt PI-Vote laut der Piratenpartei folgende drei Anforderungen:⁸⁶

1. Der Stimmbürger muss überprüfen können, ob seine Stimme korrekt auf dem E-Voting System ankam und auch mitgezählt wurde.
2. Eine Mehrfachabstimmung darf nicht möglich sein.
3. Eine Stimme darf nicht durch eine Drittperson manipuliert werden.

Die Piratenpartei macht diese Aussagen unter gewissen Annahmen:⁸⁷

1. Die verwendete Kryptografie ist ausreichend sicher.
2. Der Client ist weder manipuliert noch mit Malware infiziert.
3. Die Zertifizierungsstelle stellt nur Zertifikate für Stimmberechtigte (= Mitglieder der Piratenpartei) aus.

Damit die Stimme geheim ist, wird diese vor dem Senden an das E-Voting System homomorph verschlüsselt. Eine homomorphe Verschlüsselung bedeutet, dass die Stimmzettel verschlüsselt und dezentral zusammengezählt werden. Erst das Endergebnis als Ganzes kann zentral entschlüsselt, im Klartext betrachtet und veröffentlicht werden.

Bei PI-Vote kommen aus diesem Grund fünf durch die Piratenpartei bestimmten Autoritäten zum Einsatz. Um Manipulationen zu verhindern, wird sowohl der öffentliche als auch der private Schlüssel durch fünf Autoritäten generiert. Der öffentliche Schlüssel wird nach der Generierung für alle Stimmbürger publiziert.

Der Grund für die Wahl von fünf Autoritäten hat Sicherheitsgründe. Wenn sich drei Autoritäten zusammenschliessen, können diese trotzdem keine Informationen über den privaten Schlüssel erhalten – dies ist nur unter Einbezug aller fünf Autoritäten möglich.

Ein weiteres Problem bei E-Voting ist die Mehrfachabstimmung. Um eine Solche auszuschliessen, verwendet PI-Vote „Zero knowledge“.⁸⁸ Mit „Zero knowledge“ kann sichergestellt werden, dass ein Stimmberechtigter nur einmal abstimmen kann. Bei „Zero knowledge“ geht es darum, dass zwei Seiten (Stimmbürger mit E-Voting System) miteinander kommunizieren. Dabei kann das E-Voting System bestätigen, dass der Stimmbürger abgestimmt hat, ohne herauszufinden, wie der Stimmbürger abgestimmt hat. Das Stimmgeheimnis wird bewahrt und gleichzeitig kann ein Mehrfachabstimmen verhindert werden.⁸⁹

⁸⁶ PI-Vote Sicherheit (2010)

⁸⁷ PI-Vote Sicherheit (2010)

⁸⁸ PI-Vote Sicherheit (2010)

⁸⁹ Wiki.Zero-knowledge (2011)

Nach der Durchführung einer Abstimmung und der gleichzeitigen Schliessung der elektronischen Urne, kann jede Autorität eine Teilentschlüsselung vornehmen. Dies bedeutet, dass mit einer Teilentschlüsselung einer Autorität keine Auswertung und Veröffentlichung des Resultats möglich ist. Erst wenn sich vier Autoritäten zusammenschliessen, ist eine komplette Entschlüsselung des Resultates möglich. Dadurch können bis zu drei Autoritäten nicht mehr vertrauenswürdig sein, ohne dass eine Manipulation möglich ist. Erst wenn nur noch eine Autorität vertrauenswürdig wäre, könnte eine Manipulation durchgeführt werden.⁹⁰

Stimmbürger und Autoritäten benötigen ein Zertifikat, in welchem sich der öffentliche und private Schlüssel befindet. Dieses Zertifikat wird für die Identifizierung auf der Gegenseite verwendet. Um die Echtheit des Zertifikats zu überprüfen, wird das Zertifikat durch eine Zertifizierungsstelle signiert.⁹¹

Der Stimmbürger kann selbst überprüfen, ob die Stimme tatsächlich und korrekt in der elektronischen Urne landete. Er kann das Gesamtergebnis und die einzelnen Stimmen einer abgeschlossenen und ausgewerteten Abstimmung herunterladen. Anschliessend kann der Stimmbürger einerseits überprüfen, ob die eigene Stimme vom E-Voting System aufgenommen wurde und andererseits ob die addierten Stimmen tatsächlich dem veröffentlichten Resultat entsprechen.⁹²

Auch bei PI-Vote bleiben Restrisiken übrig. Die potentiellen Probleme:⁹³

- Sobald eine Drittperson Zugriff auf das Zertifikat und den Stimmzettel hat, kann diese Drittperson unbemerkt abstimmen. Aus diesem Grund muss stets überprüft werden, ob das Zertifikat vorhanden oder verschwunden ist. Ist das Zertifikat verloren gegangen, muss das Zertifikat für ungültig erklärt werden und der Stimmberechtigte erhält ein neues Zertifikat.
- Wie jedes computer-basierte System, ist auch PI-Vote durch Malware gefährdet. Die Piratenpartei empfiehlt die Nutzung einer besonders gesicherten Umgebung, wie beispielsweise einer virtuellen Maschine.
- Die verwendete Kryptografie kann heute als ausreichend sicher gelten, da ein Hacken nur über einen massiven Aufwand möglich ist. Würde sich diese Situation ändern, müsste PI-Vote den neuen Gegebenheiten angepasst werden.
- Es ist zudem durchaus möglich, dass aus Zufall ein PI-Vote Resultat als korrekt in Erscheinung tritt, obwohl manipuliert wurde.

⁹⁰ PI-Vote FAQ (2010)

⁹¹ PI-Vote Sicherheit (2010)

⁹² PI-Vote FAQ (2010)

⁹³ PI-Vote FAQ (2010)

Bewertung PI-Vote

Laut der Piratenpartei ist PI-Vote sowohl anonym als auch sicher und transparent. Jedoch bestehen dennoch Schwachstellen, welche zu beachten sind. So sind die Autoritäten, welche das Ergebnis entschlüsseln können ein Risikofaktor. Die Piratenpartei setzt PI-Vote nur für Abstimmungen ein. Laut Stefan Thöni⁹⁴ sind Wahlen mit Listen auch möglich. Dafür bräuchte es jedoch eine Änderung / Erweiterung des Benutzerinterfaces. Bei Abstimmungen muss nur auf eine entsprechende Antwort geklickt werden, was vergleichsweise einfach zu implementieren ist.

Bei Wahlen mit Listen und den Möglichkeiten zu Kumulieren und Panaschieren würde das ganze E-Voting System für die Stimmbürger, vor allem das Benutzerinterface, umfangreicher sein. Der Aufwand nimmt laut Stefan Thöni⁹⁵ „mit der Anzahl Optionen bzw. Kandidaten sowie mit der Anzahl abgegebener Stimmen linear zu“. Diese Aussage zeigt auf, weshalb die Piratenpartei PI-Vote vorerst nur für Abstimmungen einsetzt.

Gemäss Stefan Thöni⁹⁶ würde sich das Auszählen komplexer gestalten, wodurch nur Spezialisten, die Parteien und politischen Organisationen selbst an einer solch komplexen Auszählung interessiert wären. Dadurch ist die Unabhängigkeit der Autoritäten schwerer zu überprüfen und sicherzustellen.

Zudem müssten alle Kandidaten offiziell kandidieren, da eine Abgabe einer Stimme für eine nicht im E-Voting System vorhandene Person nicht möglich ist. Diese Tatsache ist eine Einschränkung und entspricht nicht den aktuell gültigen Vorgehensweisen und Möglichkeiten bei Wahlen.

5.3 Beispielprozess bei Integration der Massnahmen

a) Staatliche E-Voting ID: Der Beispielprozess bei der Nutzung einer staatlichen E-Voting ID verändert sich nicht. Die Registrierungs- und Login Möglichkeiten bleiben bestehen. Allerdings verschwinden gewisse Risiken. „Privatwirtschaft als Zielgruppe der SuisseID“, „Login bei falscher Zertifizierungsstelle“, „Keine staatlichen Attribute erlaubt“ sowie „Einsatz mehrerer SuisseIDs“ sind die Risiken, welche wegfallen. Da es jedoch immer noch nicht möglich ist, den Stimmrechtsausweis online zu unterschreiben und da auch kein Gesamtschweizerisches E-Voting System geplant ist, überwiegen bei einer staatlichen E-Voting ID die Nachteile sowohl für die Verwaltungen als auch für die Stimmbürger.

⁹⁴ Interview Thöni (2011)

⁹⁵ Thöni (2011), beschreibt im Interview unter Frage 3 die Zunahme des Aufwandes bei Wahlen

⁹⁶ Interview Thöni (2011)

b) Konzepterneuerung der SuisselD: Auch bei der Konzepterneuerung der SuisselD ändert sich der Beispielprozess nicht. Auch hier bleiben die Registrierungs- und Login Möglichkeiten bestehen, wobei auch wieder gewisse Risiken verschwinden. Die Risiken „Sonstige Sicherheitsrisiken der SuisselD“ und „Privatwirtschaft als Zielgruppe der SuisselD“ verschwinden, während das Risiko „Einsatz mehrerer SuisselDs“ erst verschwindet, wenn es legitimiert wird, das eine SuisselD eindeutig sein muss. Da es jedoch immer noch nicht möglich ist, den Stimmrechtsausweis online zu unterschreiben und da kein Gesamtschweizerisches E-Voting System geplant ist, überwiegen bei einer Konzepterneuerung der SuisselD die Nachteile sowohl für die Verwaltungen als auch für die Stimmbürger.

c) PI-Vote: Bei PI-Vote verändert sich der Prozess und basiert auf dem Austausch von Zertifikaten. Folgende Grafik⁹⁷ zeigt den Ablauf von E-Voting bei Verwendung von homomorpher Verschlüsselung mit „Zero knowledge“:

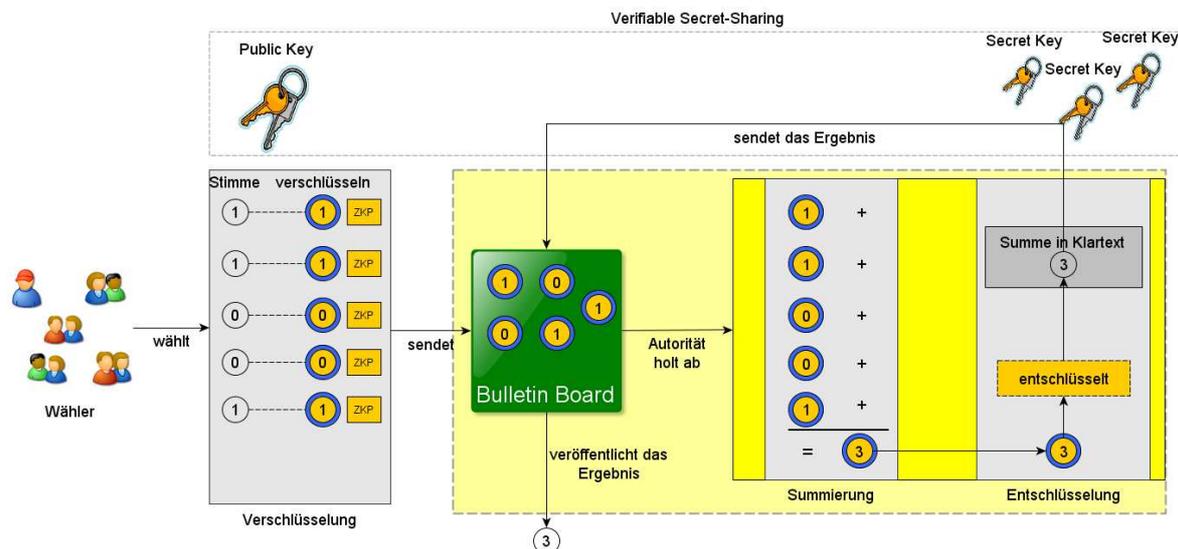


Abbildung 5 / E-Voting mit homomorpher Verschlüsselung und Zero knowledge

Die drei Anforderungen Sicherheit, Transparenz und Anonymität werden wie folgt erfüllt:

- Durch „Zero knowledge“ wird die Anonymität sichergestellt, da nur der Stimmbürger Kenntnis über seine Wahl hat.
- Dank der homomorphen Verschlüsselung kann die Sicherheit gewährleistet werden, weil die Stimmen bis zum Auszählen verschlüsselt bleiben.
- Auf dem Bulletin Board kann jeder Stimmbürger die Ergebnisse selbst nachzählen und überprüfen, ob das veröffentlichte Resultat tatsächlich dem richtigen Resultat entspricht, wodurch schlussendlich die Transparenz gewährleistet ist.

⁹⁷ Quelle: http://www.cdc.informatik.tu-darmstadt.de/reports/reports/Sami_Karabulut.bachelor.pdf (2010, S. 25)

5.4 Prozessvergleich mit ursprünglichen Beispielprozessen

Da sich der E-Voting Prozess bei einer E-Voting ID oder einer Konzepterneuerung der SuisseID nicht anders gestaltet, wird in diesem Abschnitt auf die Unterschiede zwischen dem PI-Vote Prozess und den selbst definierten Beispielprozessen eingegangen.

Prozessvergleich mit ursprünglichen Beispielprozessen	
Vorteile	
Beispielprozess 1	Simpler Prozess / Benutzerfreundlich / Überschaubar / Bereits vorhanden
Beispielprozess 2	Simpler Prozess / Einschränkung eines Stimmenkaufs oder Stimmen- diebstahls / Sichereres Login als bei Beispielprozess 1
PI-Vote	Transparenter, anonymer und sicherer Prozess dank homomorpher Verschlüsselung und Zero Knowledge und der Überprüfung der Resultate / Stimmenkauf oder Stimmenklau nur mühsam zu machen
Nachteile	
Beispielprozess 1	Nicht transparent / Stimmendiebstahl oder Stimmkauf relativ einfach
Beispielprozess 2	Nicht transparent / Nicht sicher / Risiken überwiegen dem Nutzen
PI-Vote	Komplexer Prozess / Nicht benutzergerecht / Autoritäten sind ein grosser Risikofaktor / Aufwand bei Wahlen und Auszählungen nach Wahlen gross / Keine Möglichkeit inoffizielle Kandidaten zu wählen / Zertifikatsdiebstahl

Tabelle 19 / Prozessvergleich mit ursprünglichen Beispielprozessen

Wie zu sehen ist, hat jeder Prozess diverse Vor- und Nachteile. Deswegen muss beachtet werden, in welchem Punkt der Fokus von E-Voting in der Schweiz liegt. Einerseits sollen in nächster Zeit vor allem Auslandschweizer von E-Voting profitieren, andererseits muss der E-Voting Prozess möglichst simpel gehalten werden, damit auch Menschen ohne grosse Computerkenntnisse E-Voting nutzen können. Da sich die Verbreitung und Nutzung einer SuisseID oder einem ähnlichen Konzept wie einer E-Voting ID besonders für Auslandschweizer schwer gestalten würde, ist der Beispielprozess 2 eher ungeeignet. Die im Kapitel 4.4.2: „Risikoanalyse einer Kombination von SuisseID mit E-Voting“ erwähnten Risiken überwiegen dem Nutzen.

E-Voting Systeme wie PI-Vote sind zwar transparent, anonym und sicher aber auch sehr komplex und daher nicht benutzerfreundlich. Während bei E-Voting kleine Manipulationen kaum verhindert werden können, müssen systematische Manipulationen immer entdeckt werden, da ansonsten das Endresultat verfälscht werden könnte. Wenn nun E-Voting Systeme analog zum Beispielprozess 1 genutzt werden, was in der Schweiz bisher der Fall war, dann muss die Transparenz verbessert und eine systematische Manipulation verhindert werden. Dadurch würden die Gefahren / Nachteile des Beispielprozesses 1 verschwinden.

5.5 Schlusswort

Die SuisseID eignet sich nur für das Login auf ein E-Voting System. Da die Nachteile einer Kombination von E-Voting mit der SuisseID überwiegen und weil mit dem bisherigen SuisseID Konzept eine Verbreitung der SuisseID unter sämtlichen Auslandschweizern unmöglich ist, wird die SuisseID zumindest in den nächsten Jahren nur teilweise für E-Voting zum Einsatz kommen. Beispielsweise kann sich heute ein Stimmbürger im Kanton Neuenburg mit der SuisseID am Guichet Unique einloggen. Die Voraussetzung einer SuisseID für E-Voting ist somit eher eine Einschränkung als ein Vorteil. Die SuisseID kann im Rahmen von Vote électronique trotzdem eingesetzt werden. Vor allem für das Sammeln von Unterschriften für Initiativen und Referenden per Internet kann die SuisseID ideal eingesetzt werden. Daher ist der Einsatz einer SuisseID in einigen Teilaspekten von Vote électronique durchaus denkbar.

Ich bin der festen Überzeugung, dass sich E-Voting in diesem Jahrzehnt als dritter Abstimmungskanal durchsetzen wird, schon nur aufgrund der genannten Vorteile besonders für Auslandschweizer oder Menschen, welche ständig mobil sind. Allerdings muss geschaut werden, dass die Punkte Sicherheit, Transparenz und Anonymität sichergestellt sind. Die bisherigen E-Voting Projekte in den Kantonen Zürich, Genf und Neuenburg konnten diese Punkte zwar nicht in gleichem Masse umsetzen, jedoch verliefen diese Projekte ohne grössere Probleme. PI-Vote ist sicher, transparent und anonym, jedoch sehr komplex vor allem bei Wahlen. Die Frage die sich stellt ist, ob E-Voting entweder absolut sicher, transparent oder anonym aber gleichzeitig komplex sein soll oder ob E-Voting wie bisher benutzerfreundlich und überschaubar bleiben soll unter der Einschränkung, dass zumindest die Transparenz nicht ideal umgesetzt wird. Ich glaube, dass in den nächsten Jahren die E-Voting Projekte in den Kantonen wegen der Benutzerfreundlichkeit wie bisher weitergeführt werden. Könnte nun die Komplexität eines E-Voting Systems wie PI-Vote reduziert werden und würde eine ideale Lösung bezüglich der Autoritäten gefunden werden, würde sich ein E-Voting System ähnlich wie PI-Vote gut eignen für die Schweiz. Allerdings würden die Kantone weiterhin eine eigene Lösung entwickeln, da bei einem E-Voting System für die ganze Schweiz der Nachteil des Klumpenrisikos entsteht und keine schnelle Alternative gefunden werden kann.

Ich finde es gut, dass der Fokus von E-Voting in der Schweiz bei den Auslandschweizern liegt, da der Nutzen bei dieser Zielgruppe am höchsten ist. Bei den Nationalratswahlen 2011 können Auslandschweizer in vier Kantonen E-Voting nutzen. Wenn diese E-Voting Projekte reibungslos verlaufen, wird dies dem Erfolg von E-Voting enorm entgegenkommen und das Vertrauen der Bevölkerung in E-Voting stärken. Gut finde ich im Speziellen, dass jeder Stimmbürger weiterhin selbst und geheim entscheiden kann, ob er E-Voting nutzen will oder nicht. Daher ist es gut, wird der Stimmrechtsausweis weiterhin per Post übermittelt.

Literaturverzeichnis

Bücher

Schütz G., 2009. E-Democracy und E-Voting. Grundlagen zu den Themen E-Democracy und E-Voting, Publikationsort: VDM Verlag

Internet

SuisseID 1 (2010). SuisseID – Auf Nummer sicher im elektronischen Geschäftsverkehr. Online: <http://www.suisseid.ch/endskunden/suisseid/index.html?lang=de> (04.11.2010)

SuisseID 2 (2010). SuisseID – Identitätsnachweis und elektronische Signatur. Online: <http://www.suisseid.ch/endskunden/suisseid/produktinformationen/index.html?lang=de> (04.11.2010)

SuisseID 3 (2010). SuisseID – Wo wird die SuisseID eingesetzt? Online: <http://www.suisseid.ch/endskunden/einsatzmoeglichkeiten/index.html?lang=de> (04.11.2010)

SuisseID 4 (2010). SuisseID – Wie wird die SuisseID eingesetzt? Online: <http://www.suisseid.ch/unternehmen/einsatzszenarien/index.html?lang=de> (05.11.2010)

SuisseID 5 (2010). SuisseID - Empfehlungen zum sicheren Umgang mit der SuisseID. Online: <http://www.suisseid.ch/endskunden/sicherheit/index.html?lang=de> (05.11.2010)

Cryptoshop (2004). Smart Card Reader mit oder ohne Pinpad (Class 1 / Class 2 Reader). Online: <http://www.cryptoshop.com/index.php> (28.03.2011)

Hitech (2010). SuisseID – der digitale Identitätsträger der Zukunft. Online: http://docs.google.com/viewer?a=v&q=cache:KJqiaW6aEnAJ:hitech.bfh.ch/fileadmin/data/2010_1/pdf/content_pages/deutsch/hitech1_10_20-21_d.pdf+suisseID+eigenschaften&hl=de&gl=ch&pid=bl&srcid=ADGEESildjSPJSyq6Ocdit8V7-fyJApZp6sMXvaoA57jLy2j049q2xCqiKNG4sQYDU-9dcCIPV6HFZCYLbj_ZFCdVhFKKFyAkUFDfWlq1-D1xWwFJLGXpgy81b47KPgG-sYaNwulJvH&sig=AHIEtbRRR4M-03qOLD2Ro1CivKFjxVvyTKw (05.11.2010)

SR 943.03 (2008). Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, vom 19. Dezember 2003 (Stand am 1. August 2008). SR 943.03. Online: http://www.admin.ch/ch/d/sr/943_03/index.html (02.12.2010)

SR 161.1 (2010). Bundesgesetz über die politischen Rechte vom 17. Dezember 1976 (Stand am 1. Februar 2010), SR 161.1. Online: http://www.admin.ch/ch/d/sr/161_1/index.html (12.04.2011)

X.509 Zertifikat (2011). X.509 als PKI Standard. Online: <http://de.wikipedia.org/wiki/X.509> (23.03.2011)

MELANI (2010). Melde- und Analysestelle Informationssicherung – Gefahren. Online: <http://www.melani.admin.ch/themen/00166/index.html?lang=de> (06.11.2010)

Sidler (2003). Master Thesis von Andreas Sidler: Datenschutz im E-Government. Online: http://www.ifi.uzh.ch/archive/masterthesen/DA_Arbeiten_2003/Sidler_Andreas.pdf (11.11.2010)

Bundeskanzlei (2009). Vote électronique. Online: <http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de> (11.11.2010)

Swissinfo (2008). E-Voting: Schweiz steht international gut da. Online: http://www.swissinfo.ch/ger/Home/Archiv/E-Voting:_Schweiz_steht_international_gut_da.html?cid=579628 (11.11.2010)

eGov Präsenz (2004). Erfüllt E-Voting die Erwartungen? Version 2/04. S. 26 – 28. Online: http://www.wirtschaft.bfh.ch/uploads/tx_frppublikationen/0402Gesamtausgabe.pdf (18.11.2010)

Gfs.bern (2005). Potential der elektronischen Stimmabgabe. S. 3. Online: <http://www.polittrends.ch/pub/vote-electronique.pdf> (25.11.2010)

Inside-it (2007). E-Voting kostet Schweiz 400 bis 600 Millionen Franken. Online: http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=12344 (25.11.2010)

Chaos Computer Club Zürich (2010). Kritische Analyse von E-Voting. Online: <http://zh.chaostreff.ch/E-voting> (02.12.2010)

DRS (2010). Keine Wahlen über E-Voting. Online: <http://www.drs.ch/www/de/drs/nachrichten/regional/zuerich-schaffhausen/227859.keine-wahlen-ueber-e-voting.html> (16.12.2010)

Statistisches Amt Kanton Zürich (2010). Ablauf von E-Voting im Kanton Zürich. Online: <http://www.statistik.zh.ch/produkte/evoting/index.php?p=5> (09.12.2010)

Bericht Leuenberger / Huber-Hotz (2006). Bericht des Bundesrates über die Pilotprojekte zum Vote électronique vom 31. Mai 2006. 06.056. S. 5473 – 5504. Online: <http://www.admin.ch/ch/d/ff/2006/5459.pdf> (13.01.2011)

Bericht Villiger / Huber-Hotz (2002). Bericht des Bundesrates über den Vote électronique inkl. Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 09. Januar 2002. 02.009. S. 651. Online: <http://www.admin.ch/ch/d/ff/2002/645.pdf> (20.01.2011)

Wabsti (2010). Auswertungssystem des Kantons Zürich. Online: <http://www.wabsti.ch/> (09.12.2010)

Gemeinde Bülach (2005). E-Voting-Projekt in Bülach. Online: <http://www.buelinet.ch/cgi-local/sfc.pl?p=/dialog/presse/7886914664.htm> (16.12.2010)

E-Voting Kanton Zürich (2011). Anleitung und Demo für E-Voting im Kanton Zürich. Online: https://evoting.zh.ch/MainPage/pdf/anleitung_evoting.pdf (05.05.2011)

Computerworld (2011). Kantone setzen elektronische Abstimmung aus. Online: <http://www.computerworld.ch/news/kommunikation/artikel/kantone-setzen-elektronische-abstimmung-aus-55379/> (23.03.2011)

Auslandschweizer Organisation (2011). Eidg. Parlamentswahlen: Zulassung des E-Voting für die «Fünfte Schweiz». Online: <http://www.aso.ch/de/information/pressemitteilungen/eidg.-parlamentswahlen-zulassung-des-evoting-fuer-die-fuenfte-schweiz?page=1> (28.04.2011)

PI-Vote Sicherheit (2010). Beschreibung der PI-Vote Sicherheit. Online: http://wiki.piratenpartei.ch/wiki/PIVote_Sicherheit (31.03.2011)

PI-Vote FAQ (2010). Häufig gestellte Fragen und Antworten zu PI-Vote. Online: http://projects.piratenpartei.ch/projects/pi-vote/wiki/PIVote_FAQ (06.04.2011)

Wiki.Zero-knowledge (2011). Beschreibung von Zero knowledge. Aus dem Englischen übersetzt von P. Mueller. Online: http://en.wikipedia.org/wiki/Zero-knowledge_proof (12.04.2011)

Interviews

Bernold R., Mitarbeiter Kompetenzzentrum Public Management & E-Government, 2010. Stärken & Schwächen der SuisseID, Interview vom 25.11.2010

Hassenstein G., Professor für Internet Security, 2011. Stärken & Schwächen inkl. Nutzen der SuisseID / Potential einer Kombination der SuisseID mit E-Voting, Interview vom 16.03.2011

Simonet D., Informatik Student an der BFH und Chef der Piratenpartei, 2011. Stärken & Schwächen der SuisseID und von E-Voting / Kombination der SuisseID mit E-Voting / kritische Analyse der SuisseID und von E-Voting / PI-Vote / Massnahmen zur Optimierung von E-Voting mit der SuisseID, Interview vom 21.03.2011

Weber A. Juristin, Projektleiterin Vote électronique Bundeskanzlei Sektion Politische Rechte, 2011. Juristische Fragen zu Vote électronique und E-Voting generell, Interview vom 07.04.2011

Muster D., Mitarbeiter Bundeskanzlei Sektion Politische Rechte, 2011. Technische Fragen zu Vote électronique inkl. Fragen zu einer möglichen Kombination mit der SuisseID, Interview vom 07.04.2011

Thöni S., Programmierer von PI-Vote und Mitglied der Piratenpartei, 2011. Technische Fragen zu PI-Vote, besonders zur erweiterten Nutzung für Wahlen, Interview vom 18.04.2011

Vizarro V., Projektleiter Stimmregisterharmonisation des Kantons Bern, 2011. Fragen über die Harmonisierung der Stimmregister im Zusammenhang mit E-Voting, Interview vom 29.04.2011

Abbildungsverzeichnis

Abbildung 1 / Projektorganisation Bachelor Thesis	7
Abbildung 2 / Beispielprozess für E-Voting.....	35
Abbildung 3 / Beispielprozess einer Kombination der SuisseID mit E-Voting.....	42
Abbildung 4 / Klassifizierte Risiken einer Kombination von SuisseID mit E-Voting.....	46
Abbildung 5 / E-Voting mit homomorpher Verschlüsselung und Zero knowledge	54
Abbildung 6 / Stimmrechtsausweis im Kanton Zürich.....	79

Tabellenverzeichnis

Tabelle 1 / Meilensteinplan.....	6
Tabelle 2 / Stärken von SuisseID aus Sicht der Benutzer	14
Tabelle 3 / Schwächen von SuisseID aus Sicht der Benutzer	15
Tabelle 4 / Stärken einer SuisseID Applikation aus Sicht der Betreiber	16
Tabelle 5 / Schwächen einer SuisseID Applikation aus Sicht der Betreiber	17
Tabelle 6 / Demokratische Grundsätze für rechtsgültige Wahlen.....	22
Tabelle 7 / mögliche Verschlüsselungsverfahren	23
Tabelle 8 / Erfolgsfaktoren für E-Voting.....	24
Tabelle 9 / Stärken von E-Voting aus Sicht der Benutzer.....	25
Tabelle 10 / Schwächen von E-Voting aus Sicht der Benutzer.....	27
Tabelle 11 / Stärken von E-Voting aus Sicht der Entwickler / Betreiber	27
Tabelle 12 / Schwächen von E-Voting aus Sicht der Entwickler / Betreiber	29
Tabelle 13 / Gemeinsamkeiten und Unterschiede zwischen den E-Voting Projekten.....	33
Tabelle 14 / Detaillierklärung E-Voting Beispielprozess	37
Tabelle 15 / Unterschiede zwischen den beiden Beispielprozessen	43
Tabelle 16 / Nutzenanalyse einer Kombination von SuisseID mit E-Voting.....	44
Tabelle 17 / Risikoanalyse einer Kombination von SuisseID mit E-Voting	45
Tabelle 18 / Mögliche Massnahmen um die Risiken einer Kombination zu minimieren oder zu beseitigen	48
Tabelle 19 / Prozessvergleich mit ursprünglichen Beispielprozessen	55
Tabelle 20 / Abkürzungsverzeichnis.....	62
Tabelle 21 / Allgemeine Informationen zum E-Voting Projekt im Kanton Zürich.....	76
Tabelle 22 / Lösung zum E-Voting Projekt im Kanton Zürich	78
Tabelle 23 / Allgemeine Informationen zum E-Voting Projekt im Kanton Neuenburg.....	79
Tabelle 24 / Lösung zum E-Voting Projekt im Kanton Neuenburg.....	81
Tabelle 25 / Allgemeine Informationen zum E-Voting Projekt im Kanton Genf.....	82
Tabelle 26 / Lösung zum E-Voting Projekt im Kanton Genf.....	84

Abkürzungsverzeichnis

Abkürzung	Erklärung
1:n	Art einer Beziehung: Einer Person können 1 bis unendlich viele SuisseIDs gehören, aber 1 SuisseID kann immer nur einer Person gehören.
AES	Advanced Encryption Standard: Symmetrische Verschlüsselung
AHV	Alters- und Hinterlassenenversicherung: Obligatorische Rentenversicherung in der Schweiz.
ASO	Auslandschweizer Organisation: Dachverband der Auslandschweizer
B2B	Business to Business: Art der Geschäftsbeziehung
B2C	Business to Customer: Art der Geschäftsbeziehung
B2G	Business to Government: Art der Geschäftsbeziehung
BFH	Berner Fachhochschule: Name des Studienortes
BWI	Bachelor Wirtschaftsinformatik: Art des Studienganges
CAS	Claim Assertion Service: externes Register für Attribute der SuisseID
DES	Data Encryption Standard: Symmetrische Verschlüsselung
DRS	Deutsche und Rätoromanische Schweiz (Schweizer Radio & Fernsehen)
Digital Natives	Digital Natives: Personen welche mit digitalen Technologien wie Computer und das Internet aufwuchsen.
e-banking	Online Abwicklung von Bankgeschäften
eCH	eCH: Fördert, entwickelt und verabschiedet Standards für E-Government
FBW	Fachbereich Wirtschaft: Abteilung der Berner Fachhochschule
FS	Frühlingssemester
G2C	Government to Customer: Art der Geschäftsbeziehung
GU	Guichet Unique: Elektronischer Schalter für Behördengänge
Homomorphe Verschlüsselung	Verschlüsselungsverfahren genutzt bei PI-Vote: Erlaubt das Addieren von verschlüsselten Stimmen um erst das Endergebnis zu entschlüsseln
HP	Hewlett Packard: Unternehmen
HS	Herbstsemester
https	Hypertext Transfer Protocol Secure: Verschlüsseltes Internetprotokoll
IAC	Authentifizierungszertifikat: Einsatzart der SuisseID
ID	Identifikationsnummer
IdP	Identity Service Provider: internes Register für Attribute der SuisseID
ITS	Informatikdienste: Abteilung an der Berner Fachhochschule
I-Voting	Internet Voting, auch Remote Voting genannt: Ist das Abstimmen und Wählen von einem privaten Computer
MD5	Message-Digest Algorithm 5: Hash-Funktion
myIdP	Projekt für die Nutzung von persönlichen Attributen bei der SuisseID
PDF	Portable Document Format: Dateiformat für Dokumente
PIN	Persönliche Identifikationsnummer
PI-Vote	Name des E-Voting Systems der Piratenpartei
PKI	Public Key Infrastructure: System für digitale Zertifikate
PPBT	Projektplanung Bachelor Thesis: Modul im 5. Semester
RSA	Rivest, Shamir und Adleman: Asymmetrische Verschlüsselung

Abkürzung	Erklärung
SECO	Staatssekretariat für Wirtschaft: Auftraggeber der SuisseID
SHA1	Secure Hash Algorithm: Hash-Funktion
SP2	Service Pack 2: Zweites Paket mit Softwareupdates für Windows XP
SR	Systematische Sammlung des Bundesrechts: Landes- und Staatsvertragsrecht
SSL	Secure Socket Layer: Verschlüsselungsprotokoll für eine sichere Übertragung von Daten im Internet
STORK	Secure Identity Across Borders Linked: EU-weite Mehrfachnutzung der digitalen Identität / Analoges Projekt zu SuisseID in der EU
TAN	Transaktionsnummer
WGS	Wirtschaft und Verwaltung, Gesundheit und Soziale Arbeit: Fachbereich der Berner Fachhochschule
XP	eXPerience: Betriebssystem von Windows
Zero Knowledge	Verschlüsselungsverfahren genutzt bei PI-Vote: Der Verifizierer bestätigt, dass er Informationen vom Beweiser erhalten hat, ohne Kenntnis vom Inhalt dieser Informationen zu haben.

Tabelle 20 / Abkürzungsverzeichnis

Anhang A: Interviewbögen

Interview mit Herrn Bernold

1. Ist der Funktionsnachweis tatsächlich noch nicht umgesetzt?

Konzept wird erstellt (Pilotprojekt), Anwaltsregister (Kanton Waadt)

Ist relevant für Sachen mit Unterschriften / Nur Anwalt/Notar kann beglaubigen

2. Wann denken Sie, dass dieser Funktionsnachweis umgesetzt wird?

Pilot 2010 umgesetzt, CAS für Firmenadressen

3. Stimmt es, dass die SuisseID nicht mit der Unterschrift per Hand gleichgesetzt werden kann?

Gesetzlich gleichgestellt (zertES) = wie Unterschrift per Hand

Nur bei Spezialfällen (Hauskauf mit Beurkundung) nicht erlaubt

Unterschrift per Hand IMMER fakebar

Digitale Unterschrift schwerer zu faken (da Hashwert)

PDF!!! Können Scripts ausführen (dabei sind auch digitale Unterschriften ungeschützt)

Änderung nach Signatur nicht mehr möglich (oder nur noch erkannt möglich)

4. Stimmt es, dass ein CAS auch ein Fake sein kann?

Absolut. Empfänger muss aber Provider vertrauen.

Eigenes Interesse (z.b. Arzt / Anwalt sein, wenn man gar nicht ist)

Im ersten schritt 1:1 trust zwischen Applikation und CAS

Unternehmung definiert, welche CAS Attribute liefern dürfen

5. Was für Attribute würden für eine eindeutige Identifizierung eines Stimmbürgers benötigt werden? Unterschrift?

Nur die SuisseID Nummer

Aber: was ist mit bei mehreren? Deshalb zusätzlicher Registrationsprozess!

SuisseID User ist eindeutig, aber nicht eineindeutig

Deshalb wäre mehrfaches abstimmen möglich

Physischer Registrationsprozess: (Liste mit suisseid-nutzer => dann hash-wert von SuisseID

Nummer und SuisseID User verknüpfen)

ODER: Attribut, welches nur einmalig ist (AHV (= schlechtes Beispiel))

ODER: PIN-Code

Rückverfolgung der Stimmen schon heute möglich (Brief öffnen und schon weiss man es)

6. Wo sehen Sie die Stärken der SuisseID?

Pragmatischer Ansatz, Standardisierung (viele Unternehmungen nutzen es), CAS (nur in CH,

sonst nirgends), offenes Konzept, nicht in letztes Detail geplant, offen für Änderungen, CAS

braucht keine Zertifizierung (= kein Geld für Kauf von Zertifikat), private Attribute auch möglich (da

offen) => nicht nur staatliche Attribute wie in Deutschland

7. Wo sehen Sie die Schwächen der SuisseID?

Kommunikation (Sicherheitsbedenken nicht beachtet)

Als Sicherheitslösung promotet = schlecht, zu wenig klar gemacht, weshalb SuisseID

Hardwareabhängigkeit, man braucht Treiber (wenn gesperrt, dann problem)

Class2/3 Reader sollte auch angeboten werden

8. Sehen sie Chancen, dass irgendwann fast alle Privatpersonen die SuisseID nutzen? Wenn ja, weshalb?

Ja, wenn Private es durch Firmen (z.b. Krankenkassen) erhalten

Überall wo Logins gebraucht werden

z.b. visana: online 3 fr. Günstiger

zwang zu online Login: nur SuisseID verwenden

Private müssen von firmen „nutzen aufgezwungen“ bekommen

9. Ist die SuisseID nicht vor allem für B2B oder G2B Geschäft entwickelt worden?

Auch B2C aber mit Vorteil für B

Wie fast überall: eine Hürde, Unternehmung will hauptsächlich Nutzen sehen

Bei e-voting: Hauptinteresse Staat

10. Existieren Datenschutzprobleme bei Einsatz einer SuisseID? Wo?

Rechtlich abgesichert => Daten werden von Person selbst freigegeben

11. Wo könnte die SuisseID bei E-Voting eingesetzt werden? Identifizierung, Authentifizierung (Login), Authentisierung?

Identifizierung Stimmbürger (Login) / Signieren der Stimme (sicherer als Brief)

12. Ist die Smartcard oder der USB sicherer / besser oder existieren keine Unterschiede?

USB besitzt auch Smartcard, deshalb beide gleich!!!

Class1: braucht nur Smartcard

2: Interaktion mit externem (SMS) = damit Sicherheit erhöht

13. Ist nicht dringend von einem Klasse1-Card-Leser abzuraten? In D wird davon abgeraten.

Falsch... auch Klasse 1 in D erlaubt

Sicherheit kostet!!! Nutzen vs. Risiken

Migrosbank online-banking mit klasse1 reader

14. Es ist bekannt, dass die SuisseID mit Metasploit Framework inklusive Keylogger oder mit USB over Network gehackt wurde.

Jedes System ist hackbar. Abschätzung Nutzen vs. Kosten

Unternehmungen werden aber wohl kulant sein

Klasse 2 Reader wäre Lösung

USB over Network = Problem (wie überall)

Hauptproblem aber: man in the browser: Zahlungen werden umgeleitet, Kontoauszug angepasst.

Nutzer merkt es nie

Sicherheit immer Kosten vs. Nutzen abwägen

15. Sind die rechtlichen Anforderungen nicht noch mal zu überprüfen und anzupassen?

Nein

16. Bräuchte es nicht ein grösseres Marketing und eine bessere Sensibilisierung über diese Thematik?

Fokus auf Firmen: SuisseID ist günstiger als Eigenlösung

Vor allem: wenn mit anderen Unternehmungen geteilt wird, noch günstiger

Marketing: dass PKI selber bauen teurer als wenn SuisseID eingesetzt

Vertrauen: auch Marketing machen

17. Sind Unternehmungen wie die Post nicht naiv, wenn sie behaupten, dass die SuisseID sicher ist, wenn Mensch, Computer, Internet korrekt aufeinander abgestimmt sind.

Absolut sicher = unmöglich, aber Risikominimierung

18. Wenn Unternehmungen SuisseID vertrauen, weshalb bietet UBS einen eigenen Access Key? Warum wurde nicht Know-How der Banken verwendet (PKI, Signaturen)

UBS => PKI aufgebaut: kostet viel Geld

Deshalb weiterhin ihre Lösung

Prestige!!! Image!!!

UBS: macht es auch nur, weil es so sicherer aussieht

Könnte auch SuisseID nehmen und Zusatz aufbauen

PKI KnowHow bei Quovadis und Swissign => sind Spezialisten im Gebiet PKI

PKI ist Identity Federation

Migrosbank = genau gleiche Lösung wie SuisseID

19. Sollte in Zukunft der Fokus eher auf C oder B gelegt werden?

Business

20. Wäre ein Verschlüsselungszertifikat nicht zwingend nötig um Schwächen zu reduzieren?

Bringt nichts für Sicherheit, da Reader immer noch unsicher

Vorteil: Anwendung verschlüsseln

Trennung: Sicherheit der Lösung (übergeordnet) und Sicherheit der Anwendung (untergeordnet)

Grund weshalb nicht gemacht: wenn Verlust von Verschlüsselungszertifikat, dann muss wieder entschlüsselt werden => wäre zu heikel, da keine Kopie vom Schlüssel erlaubt ist

Key Recovery Algorithmus => wäre mega teuer und Schlüssel wäre dort gespeichert

DB Verwalter hätten Vollzugriff....

Interview mit Herrn Hassenstein

1. Wie könnte die SuisseID für Auslandschweizer verbreitet werden? (Auslandschweizer haben das Bedürfnis nach E-Voting)

Das ist ein Problem an sich. Eine Möglichkeit wäre die Verbreitung durch die Botschaften. Die Auslandschweizer könnten dadurch den Registrierungsprozess in einer Botschaft oder einem Konsulat durchführen

Als Nutzen könnte beispielsweise die SuisseID für Behördengänge (z.B. Wohnortwechsel oder Kontakt mit Konsulat) eingesetzt werden. Dazu bräuchte es aber eine Weiterentwicklung der SuisseID Infrastruktur

In grossen Ländern mit weiten Distanzen zum Konsulat oder der Botschaft scheint dieses Vorhaben sehr sinnvoll zu sein. Der Auslandschweizer müsste nur noch über Internet verfügen und könnte für Behördengänge auf weite Reisen verzichten.

2. Ist der Funktionsnachweis nun umgesetzt oder nicht?

Der Funktionsnachweis befindet sich immer noch in der Pilot-Phase. Deshalb existiert auch aktuell (Stand Mitte März) kein produktiver Funktionsnachweis.

3. Finden Sie auch, dass durch den Einsatz eines Class 2+ Reader die SuisseID wesentlich sicherer ist? => Bereits möglich?

Der Einsatz eines Class 2 Readers ist bereits heute möglich. Quovadis und die Post ermöglichen den Einsatz eines Class 2 Reader. Allerdings muss der Benutzer dies ausdrücklich verlangen.

4. Finden Sie es eher eine Stärke oder Schwäche, dass ein Benutzer mehrere SuisseIDs haben kann? (E-Voting Mehrfachabstimmung) => Ist es weil SuisseID keine ID ist?

Es ist eine Schwäche und dadurch entstehen diverse Probleme. Einerseits ist das Managen von mehreren SuisseIDs sehr schwer, da schnell der Überblick verloren geht, wann welche SuisseID zum Einsatz kommen soll. Andererseits sind das Handling und der Preis Faktoren, welche dagegen sprechen, dass mehrere SuisseIDs einen Vorteil bringen.

5. Ist die dreijährige Laufzeit nicht negativ für den Erfolg / die Verbreitung der SuisseID?

Die dreijährige Laufzeit ist sehr sinnvoll, da das Zertifikat nach drei Jahren abläuft. Die drei Jahre beziehen sich somit auf die Zertifikatslaufzeit, welche gewöhnlich um die drei Jahre dauert. Die Frage, die sich eher stellt ist, ob der Preis der SuisseID mit der Zeit nicht günstiger wird und wie viel der Benutzer für eine neue SuisseID zu bezahlen hat. Durch das Schaffen von Anreizen, wie das kostenlose Erneuern der SuisseID würde dem Erfolg einer weiten Verbreitung der SuisseID entgegenkommen.

6. Wer ist für die Sicherheit zuständig (User vs. Betreiber/Entwickler)?

Die Benutzer müssen beispielweise durch ein sehr benutzerfreundliches und simples Handbuch aufmerksam gemacht werden, wie sie korrekt mit der SuisseID umzugehen haben, welche Sicherheitsrisiken zu berücksichtigen sind und an welche Richtlinien sich der Benutzer halten muss. Dieses Handbuch könnte beim Erwerben einer SuisseID automatisch mitgegeben werden.

7. Was können Sie zu den Sicherheitskosten sagen?

Für einen Service Provider sind die Sicherheitskosten = 0, da die SuisselD mit Open Source programmiert wurde. Der Quellcode kann somit heruntergeladen werden.

Für Applikationen, welche den Einsatz der SuisselD unterstützen, ist der Implementierungsaufwand relativ klein für geübte Programmierer, da die SuisselD auf Java basiert.

Dadurch wäre auch die Implementierung der SuisselD in einem E-Voting System problemlos durchzuführen.

8. Wo sehen Sie den quantitativen Nutzen für den Benutzer und die Unternehmen?

Der Nutzen ist für beide Seiten (Unternehmen und Benutzer) nicht unbedingt vorhanden. Allerdings könnte für Unternehmen der Verwaltungsaufwand kleiner werden, wenn die Adressbestätigung per SuisselD möglich wäre. Einerseits könnte dies über myIDP gelöst werden oder über einen Post CAS für Postadressen. Dadurch würde auch ein Nutzen für die Benutzer entstehen, da dieser die Adressänderung nicht mehr vor Ort durchführen müsste.

9. Wo sehen Sie den qualitativen Nutzen für den Benutzer und die Unternehmen? (Gesetzlich geregelt, schnellere Verträge)

Der qualitative Mehrwert ist für die Benutzer momentan noch nicht gegeben. Erst wenn das CAS und der Funktionsnachweis umgesetzt wären, könnte ein Benutzer die Behördengänge vom Sofa aus durchführen. Dies gäbe einen Mehrwert, da der Benutzer unabhängig vom Ort und Zeit mit den Behörden in Kontakt treten könnten.

Die Unternehmen, welche die SuisselD einsetzen, haben einen Nutzen. Einerseits durch das Authentisieren mit der SuisselD können Manipulationen enorm minimiert werden, da das Unternehmen nun sehen kann, wer der Benutzer ist. Der Benutzer ist somit relativ gut registriert. Nur durch den Klau der SuisselD inklusive dem PIN-Code, kann sich jemand unerlaubt authentisieren. In diesem Fall würde dennoch der ursprüngliche SuisselD Benutzer haften, da dieser beim Verlust seiner SuisselD diese unmittelbar revozieren muss.

Auch das Abchecken, ob jemand 18 ist oder nicht (beispielweise in einem Weinshop), bringt sehr viele Vorteile. Ursprünglich konnten solche Geschäfte nur per Kreditkarte durchgeführt werden. Mit der SuisselD wird dies überflüssig, da auf der SuisselD ein Attribut mit dem Geburtsdatum abgespeichert werden kann.

10. Wo sehen Sie das Potential einer möglichen Kombination von SuisselD mit E-Voting?

Die SuisselD könnte einerseits als Berechtigung eingesetzt werden. Jedoch darf mit der SuisselD der Stimmzettel nicht unterschrieben / signiert werden, da sonst zu sehen ist, welche Person wie abgestimmt hat. Die Wahl muss zwingend geheim / anonym bleiben.

Die SuisselD könnte jedoch für die Registrierung und das Login verwendet werden. Dadurch könnte man nur tatsächlich stimmberechtigten Bürgern den Zugriff auf das E-Voting System gewährleisten.

E-Voting hat höhere Anforderungen als die beiden anderen Kanäle, da per E-Voting vergleichsweise einfach tausende von Stimmen manipuliert werden können. Untersuchungen an einer Universität haben gezeigt, dass sehr viele Stimmbürger ihre Stimme für Geld verkaufen würden. Deshalb darf eine Massenmanipulation nicht möglich sein.

Die SuisseID würde diese hohe Anzahl an Manipulationen erschweren. Um Massenmanipulationen komplett zu verhindern, müsste eine technische Lösung gefunden werden. Diese technische Lösung könnte entweder mit blinden Signaturen oder mit homomorpher Kryptografie umgesetzt werden.

Mit der SuisseID sollte der Stimmbürger etwas erhalten, das nicht weitergegeben werden kann. Wenn der Stimmbürger nach der Registrierung per SuisseID seinen Stimmzettel erhält, muss geschaut werden, dass dieser Wahlzettel nicht weitergegeben wird. Ein kurzes Zeitfenster würde verhindern, dass der Wahlzettel weitergegeben werden kann.

Bei E-Voting dürfen Stimmen nachgezählt werden, aber nicht auf die Stimmbürger bezogen. Dies bedeutet, dass die Anzahl an E-Voting Nutzer mit der Anzahl an E-Voting Stimmen exakt übereinstimmen muss. Es gilt eine Null-Toleranz.

Wäre der Stimmrechtsausweis elektronisch, könnte dieser mit der SuisseID unterschrieben werden, wie beim Urnengang und der brieflichen Abstimmung. Dadurch wäre die Stimme immer noch vom Stimmbürger getrennt.

11. Wie könnte verhindert werden, dass ein Benutzer mit mehreren SuisseIDs abstimmt? (myIDP, Registrierung)

Nur durch eine Registrierung des Stimmbürger und seiner SuisseID könnte dies verhindert werden. Die optimale Lösung wäre das Abspeichern einer eindeutigen Nummer auf der SuisseID als Attribut. Dadurch würde es sofort klar werden, wenn jemand eine zweite SuisseID einzusetzen versucht. Aktuell dürfen staatliche Attribute nicht als Attribut auf der SuisseID landen. Wäre dies erlaubt, könnte auch eine eindeutige Nummer auf der SuisseID abgespeichert werden.

Interview mit Denis Simonet

1. Finden Sie auch, dass durch den Einsatz eines Class 2+ Reader die SuisseID wesentlich sicherer ist?

Viel sicherer. PIN-Eingabe => verhindert Manipulationen

SECO zuerst nur Class 1 Reader (ohne Class 2 Reader)

Default sollte Class 2 sein... Wäre nicht viel teurer

2. Findest du es eher eine Stärke oder Schwäche, dass ein Benutzer mehrere SuisseIDs haben kann? (E-Voting Mehrfachabstimmung)

Für Identifikation => Keine Schwäche (ausser E-Voting)

Sonst nicht tragisch => 1:n Beziehung, keine richtige ID

Keine direkte Gefahr

3. Wo siehst du den quantitativen Nutzen für den Benutzer? (Effizienz, keine Eigenlösung, elektronische Unterschrift ermöglicht Aufwandsreduktion usw.)

Gute Sache, solange nicht verpflichtend => Aufwandsreduktion

Idee: Gut

Umsetzung: schlecht, weil Sicherheitstechnisch und Kommunikation schlecht

Dreamlab bewies Unsicherheit

Handbuch auf Homepage erstellt => Handbuch mitgeben wäre gut (Auswahl ob man es will)

Kampagne im Internet (auf Gefahren hinweisen)

4. Was muss beim Marketing und bei der Kommunikation der SuisseID zukünftig besser laufen?

Keine Sicherheitslösung

5. Findest du, dass die Transparenz betreffend E-Voting in der Schweiz gut umgesetzt wird? Was braucht es noch um die Transparenz zu erhöhen?

Problem: Transparenz, nicht nur kryptografisch sicher, sondern auch Vertrauen

6. Wie sollen Audits bei E-Voting durchgeführt werden, wenn keine Stimme einem Bürger zugewiesen werden darf?

Audits möglich nur mit privaten Zertifikat

Sehr aufwändig, aber sicher, dafür komplex (niemand glaubt)

Vertrauen würde nicht da sein

7. Wo liegen die Schwächen bei E-Voting?

Transparenz => Sicherheit in Lösungen

Keine Offenlegung des Algorithmus

Keine Archivierung erlaubt (evtl. Datenschutzgründe)

Sonst würde per Klartext gesehen werden, wer wie abgestimmt hat

E-Voting würde Stimmbeteiligung zunehmen

8. Ist das Verfahren mit PIN / TAN nicht am besten? (wenn PIN nur im Kopf gespeichert => keine Chance für Manipulation)

Man weiss es nicht. Keine Nachprüfung möglich => kein Vertrauen

9. Wie schätzt du das Potential einer Kombination der SuisseID mit E-Voting ein? (Unterschrift nun möglich, Stimmenkauf / Stimmenklau schwerer, Unterschriften für Initiativen / Referenden nun auch elektronisch möglich)

X.509 unsicher

Revokelliste nicht vorhanden für intermediate certificat

Asymmetrische Kryptografie (public und private key)

Zertifikat nicht zurückzustellen

Irgendein Private key => alle SuisseIDs des Resellers ungültig

Besserer Standard als X.509 nehmen

Man schaut nur, ob Key ungültig ist (aber nicht ob gültig)

Nicht als Schwäche sondern als Tatsache => was aber dann als Schwäche herauspicken

10. Wo liegen Schwachstellen einer solchen Kombination (Manipulation, Abstimmen durch Dritte, Klau einer digitalen Unterschrift)?

SuisseID ist nicht brauchbar für E-Voting

Zu unsicher für dass es um digitale Unterschrift geht

11. Wo siehst du den qualitativen Nutzen von E-Voting (keine „unklaren“ Stimmen => Auszählung, Bedürfnis nach E-Voting decken)

Nutzen auch gegeben

Aber: Wie sicherstellen, dass Stimme in richtiger Urne landete

Sicherheit ist schlecht!!!

12. Wie beurteilst du meinen Beispielprozess? Wo liegen Schwachstellen, was ist überflüssig, was wurde übersehen? Wo könnte SuisseID eingesetzt werden

SuisseID für Login und Registrierung ok

13. Was sagst du zu den möglichen Risiken einer Kombination der SuisseID mit E-Voting?

Sicherheit

Etwas nehmen, dass eh schon unsicher ist?

SuisseID ist ein ganzes Konzept

Auch Login gefährlich => man geht bei Intermediate abfragen

Zertifizierungsstelle kann manipuliert

SuisseID => Privatwirtschaft

E-Voting staatlich, abhängig von Privatwirtschaft

Privates Attribut wieder abhängig von Privatwirtschaft

Vertrauen schlecht => Identifikation an Privatwirtschaft

Nicht vom Parlament beglaubigt

Entweder E-Voting ID

Oder neue SuisseID (totales Konzept erneuern)

Konzept SuisseID: inkl. Zertifikat, PKI, Zertifizierungsstellen

Prozess rundum bei e-Voting und SuisseID schlecht

Problem: Wie sicherstellen, dass Auszähler nicht käuflich sind

Man muss mit Faktor Mensch leben => E-Voting ohne Menschen nicht möglich

Interview mit Annina Weber und Daniel Muster

1. **Stimmt es, dass sowohl eine Archivierung der Stimmen als auch eine Nachzählung der Stimmen nicht möglich / nicht erlaubt ist? Ist es wegen dem Datenschutz oder anderen gesetzlichen Richtlinien?**

Archivierung erlaubt => müssen sogar, Bundesrat gültig erklärt (erwahren)

Nachzählungen möglich, aber nicht sehr sinnvoll!

Plausibilität prüfen

Archiviert genau wie bei brieflichen Abstimmung (wenn Fehler => Stimmen ausdrucken)

Stimmzettel ausdrucken und von Hand nachkontrolliert

2. **Wie steht es um die Transparenz bei E-Voting?**

Auch Problem bei Urnengang und Brief

Es wäre ein Zusatz... etwas Neues, ein Plus gegenüber anderen Kanälen

Muss den anderen Kanälen entsprechen

Verifizieren muss noch gemacht werden (würde Prozess verändern)

Artikel betreffend Kryptographie => Codevoting, individuelle Nummer für Anmeldung

Ja = Nummer, Nein = andere Nummer

Gut für einfache Abstimmung

Möglichkeiten bei Wahlen ist viel komplexer, wegen Personen welche unterschiedlich zu handhaben sind (leere Listen auch erlaubt)

3. **Vertrauen vs. Sicherheit Wie Aufwand reduzieren?**

SuisseID ist Authentifizierungsmittel

Abstimmung = anonym

Abstimmungsprozess passt nicht zu SuisseID

Kann nicht mehr getrennt werden

Stimmrechtsausweis mit vertraulichen Daten (Codes) sind individuell pro Stimmrechtsausweis gültig (immer andere Elemente vorhanden)

Deshalb nicht online stellen, wegen Anonymität

SuisseID hat keine Zertifizierung

Neuenburg nutzt auch SuisseID

Zürich => Bericht wie es weiter geht

Medien schreiben Unwahrheiten

WABSTI hat Probleme (ist nur Auswertung)!!!

Vote electronique aktuell nur für gemeinsinterne Wahlen

Medien schreiben falsche Tatsachen

4. Welches E-Voting Projekt wählte Ihrer Meinung nach den besten Ansatz? (Genf / Zürich ähnlich, Neuenburg anders => Portal, PIN)

Keine Probleme in den drei Kantonen (nur laut Medien)

Extra drei unterschiedliche Systeme wegen Stärken und Schwächen

Genf beherbergt Bern, Basel

Zürich für Ostschweizer Kantone

Nur GE, ZH, NE für Inlandschweizer

Alle die source-code von ZH, GE, NE nutzen, werden es nur für Auslandschweizer nutzen

Kein E-Voting System für ganze Schweiz

Wegen Klumpenrisiko => wäre schwer schnell eine Alternative zu finden

Vorlaufzeit 2 Monate (gibt Probleme wenn Optimierungen / Änderungen gemacht werden)

Strategischer Entscheid, dass es kein System für die ganze Schweiz gibt, sondern 3 unterschiedliche Systeme

Optimierung des Prozesses

Unterschiedliche Fristen

Abstimmung auf 3 Ebenen => Prozess: unterschiedliche Fristen

Wahlen und Abstimmung werden IMMER von Kanton durchgeführt

Bei Stichwahl fristen anders als normal

Optimierung wäre Sysphusarbeit, da jeder Kanton andere Richtlinien besitzt

Aber: Kantonssysteme könnten optimiert werden

Optimierung des Stimmrechtsausweis (7 Kantone haben sich zusammengeschlossen)

Bis Minimalstandard ging sehr viel Zeit verloren

Nur Minimalstandard... immer noch Unterschiede

5. Wie schätzen Sie das Verhältnis Kosten vs. Nutzen ein? (keine Ablösung = Zusatzkosten, keine höhere Stimmbeteiligung, rechtliche Unsicherheit, Vertrauen)

Alles nicht belegt

Vertrauen => nur Wissenschaftler und Informatiker sind misstrauisch, aber Stimmbürger vertrauen

Stimmbeteiligung konstant behalten = möglich und schon ein Erfolg

Brief erst seit 1994 => brauchte Zeit bis Akzeptanz vorhanden war

Pilotphase nur 4 % abstimmen per E-Voting

Noch keine ausreichenden Vergleichswerte wegen Stimmbeteiligung

Zielgruppen unterschiedlich (Auslandschweizer): bei Auslandschweizer ist Stimmbeteiligung bei E-Voting ca. 50 % (nur die, die abstimmen)

Mit der Zeit mitgehen...

Zentralisierung oder Harmonisierung (nur Auslandschweizer)

Inland: Einwohnerregister => daraus Stimmrechts

Unterschiedliche Software => Daten für Volksabstimmung

Auslandschweizer kantonal geführt (Auslandschweizer können unterschiedlich teilnehmen)

6. Wie könnte die SuisseID für Auslandschweizer verbreitet werden? (Auslandschweizer haben das Bedürfnis nach E-Voting => Urne nicht möglich, Brief geht mehrere Tage)

Extrem schwer => müssten in Schweiz vorbeikommen

Haftung für Hilfspersonen nicht ausschliessen

Zertifikat nur bei staatlicher Stelle

7. Was ist der Grund, weshalb die Stimmregister in Zürich (in der Deutschschweiz) kommunal geführt werden und nicht wie in Genf auf kantonaler Ebene?

Kantone geben Resultat an Bund bekannt

Organisation und Durchführung

Bundeskanzlei ist nur für Resultat und Koordination

Aargau 75'000 Personen für Hilfe (a bis Z)

Kantonaler Ebene = sinnvoll => Kantone führen es durch = wollen auf Verantwortung

Oberverantwortung bei Bundeskanzlei, sonst Kantone

Bundesgesetz über politische Rechte Art. 10

8. Als E-Voting Projektleiterin: Was lief besonders gut? Was wurde besonders gut umgesetzt? Wo gab es Probleme? Gab es viele Versuche einer doppelten Stimmabgabe? Hat E-Voting eine Zukunftsperspektive?

Bisherige Versuche erfolgreich

Probleme eher organisatorische Probleme

Systeme funktionieren

Gewöhnung an neuen Prozess

Auslandschweizer haben grössten Nutzen

Überschaubar, => Fokus auf Auslandschweizer

Nationalratswahlen in 4 Kantonen für Auslandschweizer

Zuerst Auslandschweizer (2015)

9. Da SuisseID eher ungeeignet: Private Attribute abhängig von Privatwirtschaft, Konzept der SuisseID nicht sicher (Zertifikat), nur für Registrierung und Login brauchbar

Lösung: Staatliche SuisseID (Evoting ID) => sonst abhängig von Privatwirtschaft

Verbreitung unter Auslandschweizer durch Konsulate und Botschaften

Staatliche Attribute, Bund als Entwickler und Verkäufer

=> dadurch keine Abhängigkeit von Privatwirtschaft

SuisseID Problem: Zertifikat nicht auf Person beziehen möglich, SuisseID Attribute nicht eindeutig

Koordination zwischen Eintrag Stimmregister und Zertifikat

Ausgabe privat

E-voting ID nicht benutzerfreundlich

Interview mit Stefan Thöni

1. **Wahlen mit Listen (wie bei Nationalratswahlen) auch möglich bei PI-Vote?**

Das wäre prinzipiell möglich, ist jedoch momentan weder implementiert, noch vorgesehen.

2. **Was sich daran an PI-Vote ändern würde?**

Solche Änderungen würden nur das Benutzerinterface betreffen. Eine Protokoll-, oder Datenhaltungsänderung wäre prinzipiell nicht nötig.

3. **Ob ein PI-Vote System sich überhaupt eignet für Wahlen? => Stichwort: Komplexität und Aufwand**

Die Komplexität und damit der Rechenaufwand nimmt mit der Anzahl Optionen bzw. Kandidaten sowie mit der Anzahl abgegebener Stimmen linear zu. Da eine Nationalratswahl sehr viele Kandidaten beinhaltet würde daher das Auszählen entsprechend rechenaufwändig werden. Das Auszählen wäre dann wohl nicht mehr für jedermann möglich, wohl aber für alle interessierten Parteien und Gruppierungen. Ob das praktikabel ist, ist mehr eine Frage der Organisation, denn der Technik.

Die grösste Einschränkung von Pi-Vote ist, dass die Optionen bzw. Kandidaten vorher bekannt sein müssen. Daher wäre z.B. eine Regierungsratswahl, wo jeder Wahlberechtigte wählbar ist, nicht möglich.

Interview mit Vito Vizarro

1. **Nutzt jede Gemeinde tatsächlich unterschiedliche Software für die Stimmregister?**

--> Ja, die Softwareanbieter, welche im Kanton Bern im Einsatz sind - Zertifizierte Software-Anbieter Einwohnerkontrollensoftware (daraus werden die Daten für das Stimmregister extrahiert):

Es gilt zu beachten, dass gewisse Gemeinden teilweise keine Software oder einfache Tabellen/Datenbanken (z. B. Excel oder Access) einsetzen.

2. **Falls ja: Weshalb setzt jede Gemeinde nicht die gleiche Software ein?**

--> Die Gemeinden sind frei zu wählen, welche Software sie einsetzen. Der Kanton schreibt lediglich das Format und die Schnittstellen vor (z. B. eCH Standard) und schränkt die Autonomie der Gemeinden nicht ein.

3. **Weshalb sehen die Stimmregister in jedem Kanton anders aus betreffend der erhobenen Daten?**

--> Dies hat teilweise historische aber auch technische Gründe. Das Bedürfnis der Gemeinde (welche Daten) oder die Datenbankstruktur des Softwareanbieters können das Format der erhobenen Daten massiv beeinflussen. Deshalb wird versucht, mit eCH-Standards den Datenaustausch zwischen Gemeinden, Kanton und Bund zu standardisieren, ohne jedoch zu fest in die Autonomie der Gemeinden/Softwarehersteller einzugreifen.

4. Was sind die aktuellen technischen Herausforderungen bezüglich der Harmonisierung der Stimmregister?

--> Die Heterogenität der Softwareprodukte, Schnittstellen und Formate. Vor allem die Datenbankstrukturen, welche beeinflussen, wie die Daten erfasst werden (z. B. Strasse und Hausnummer im gleichen oder in separaten Feldern) führen dazu, dass die Adresse trotz eCH-Standard in verschiedenen Formaten geliefert wird. Dies ist beim Zusammenführen aller Daten problematisch. Dazu kommt, dass die eCH-Standards für Schweizer Formate erstellt werden. Dies führt bei der Darstellung von ausländischen Adressen zu Problemen, da je nach Land ein anderes Adressformat verlangt wird. Weiter sind die eCH-Standards nicht immer eindeutig beschrieben, d.h. es besteht Interpretations-Spielraum. Dieser führt dazu, dass der gleiche Standard unterschiedlich eingeführt werden kann und dazu führt, dass bei einer Zertifizierung mehrere Varianten zugelassen werden müssen.

5. Würde das Problem nicht kleiner sein, wenn die Stimmregister kantonal geführt würden?

--> Aus technischer Sicht: Ja.

--> Aus organisatorischer Sicht: Nein. Die Datenhoheit liegt bei den Gemeinden. Diese verfügen über die notwendigen Personalressourcen, die anderenfalls beim Kanton geschaffen werden müssten. Ausserdem sind die Gemeindebehörden näher bei den Bürgern und können dadurch eine bessere "Kundenfreundlichkeit" gewährleisten.

Im Zuge der Einführung von E-Voting für Auslandschweizer haben verschiedene Kantone ein zentralisiertes, kantonal geführtes Auslandschweizer Stimmregister eingeführt. Dieses System ist aus technischer Sicht weniger anspruchsvoll als das Berner System mit dezentral geführten, harmonisierten Stimmregistern, die vor jeder Abstimmung über einen sogenannten Eventbus zu einem kantonalen Stimmregister zusammengezogen werden müssen.

Sollte in Zukunft allerdings E-Voting für alle Stimmberechtigten eingeführt werden, werden die Kantone mit einem zentralisierten Auslandschweizer Stimmregister über zwei parallele Systeme verfügen - ein kantonales, zentralisiertes Stimmregister für die Auslandschweizer und ein dezentral geführtes, harmonisiertes Stimmregister-System für die "Inlandschweizer". Diese Lösung wird mit höheren Kosten verbunden sein.

Anhang B: Zusammenfassung der drei E-Voting Projekte

E-Voting Projekt im Kanton Zürich

Die Gemeinden Bülach, Schlieren und Bertschikon gehören alle zum Kanton Zürich. In diesen drei Gemeinden wurde im Jahr 2005 zum ersten Mal in der Deutschschweiz eine Abstimmung mit E-Voting erfolgreich durchgeführt.⁹⁸ Der Kanton Zürich stellte deshalb am 20.12.2006 ein Gesuch, bei welchem darum gebeten wurde, dass Vote électronique bei der Abstimmung vom 17.06.2007 eingesetzt werden kann. Der Bund kam diesem Wunsch am 04.04.2007 nach, da sowohl die Verordnungen als auch das Bundesgesetz zu den politischen Rechten erfüllt waren. Die Verantwortung, dass die minimalen Anforderungen an den Prozess und die Technik eingehalten werden, musste der Kanton Zürich sicherstellen.

Allgemeine Projektinformationen⁹⁹

Element	Beschreibung
Zeitpunkt	Eidgenössische und kantonale Abstimmung vom 17.06.2007
Organisation	Kanton Zürich
Partnerunternehmen	Unisys (für die Anwendung, Hard- & Software)
Zielgruppe	Stimmbürger der Gemeinden Bülach, Schlieren und Bertschikon
Grösse der Zielgruppe	Total: 17'292
Prozentuale Nutzung	Bülach: 5,48 %, Schlieren: 4,4 %, Bertschikon: 12,96 % Total: 5,39 % (wenn Stimmbeteiligung = 100%)

Tabelle 21 / Allgemeine Informationen zum E-Voting Projekt im Kanton Zürich

Lösung / Entwicklung¹⁰⁰

Element	Beschreibung
Technischer Ablauf	Bei der Anmeldung am E-Voting System muss der Benutzer seine User-ID eingeben, welche auf dem neuen Stimmrechtsausweis zu sehen ist. Anschliessend erfolgt die Abgabe der Stimme. Um die Stimmabgabe auf ihre Korrektheit zu überprüfen, erscheint auf einer Bestätigungsseite ein Bestätigungssymbol. Entspricht dieses Symbol dem Symbol auf dem Stimmrechtsausweis, kann sichergestellt werden, dass die Stimme vom E-Voting System korrekt aufgenommen wurde. Um die Stimme abzugeben, muss der PIN-Code auf dem Stimmrechtsausweis freigerubbelt werden.

⁹⁸ Statistisches Amt Kanton Zürich (2010)

⁹⁹ Bericht Leuenberger / Huber-Hotz (2006)

¹⁰⁰ Bericht Leuenberger / Huber-Hotz (2006)

Element	Beschreibung
Organisatorischer Ablauf	<p>Sechs Wochen vor Wahlgang muss das Abstimmen mit E-Voting möglich sein. Aus diesem Grund erhalten die Stimmbürger in diesem Zeitraum einen neuen Stimmrechtsausweis, welcher zusätzliche Elemente für E-Voting besitzt. Diese Stimmrechtsausweise werden durch das Statistische Amt des Kantons Zürich erstellt. Sobald der Stimmrechtsausweis verfügbar ist, können auch alle Abstimmungsunterlagen online betrachtet werden.</p> <p>Vor der Abstimmung müssen zudem sämtliche kommunalen Stimmregister auf kantonaler Ebene harmonisiert oder verknüpft werden. Dies geschieht über eine sichere, verschlüsselte Verbindung.</p> <p>Bis um 12 Uhr am Wahlsonntag können Stimmbürger ihre Stimme per E-Voting abgeben. Ab 12 Uhr wird die elektronische Urne genau gleich wie die physische Urne geschlossen.</p>
Technische Eigenschaften	<p>E-Voting System:</p> <p>Die Identität des Stimmbürgers kann nur über den Bar-Code auf dem neuen Stimmrechtsausweis festgestellt werden. Da jedoch die Stimme getrennt von der Identität des Stimmbürgers gespeichert wird, ist ein Rückschluss auf das Stimmverhalten eines Bürgers unmöglich. Eine doppelte Stimmabgabe (einmal an der Urne und einmal per E-Voting) kann praktisch ausgeschlossen werden.</p> <p>Browsereinstellungen:</p> <ul style="list-style-type: none"> - Bei der Nutzung von E-Voting muss eine SSL Verbindung bestehen. - Nach Eingabe der User-ID müssen in jedem Fall das Wappen und der Name der Gemeinde erscheinen. - Das Bestätigungssymbol auf dem E-Voting System muss das gleiche Symbol wie auf dem Stimmrechtsausweis sein. - Das Löschen des Browser-Cache erhöht die Sicherheit von E-Voting
Organisatorische Eigenschaften	<p>Die ausgewerteten Stimmen werden an das kantonale Auswertungssystem gesendet. Dieses Auswertungssystem hat den Namen WABSTI und kann für sämtliche Wahlen eingesetzt werden (Initiativen, Referenden, Proporz- und Majorzwahl). WABSTI Version II lautet die aktuelle Version, welche auf jeder politischen Ebene (Gemeinde, Kanton, Bund) die Stimmen auswerten kann. Die Resultate der Auswertung können für weitere Analysen verwendet werden. Allerdings ist die Anonymisierung der Stimme auch bei diesen nachträglichen Analysen gewährleistet.¹⁰¹</p>

¹⁰¹ Wabsti (2010)

Element	Beschreibung
Technische Schwierigkeiten	<p>In Zürich konnte neben dem Internet auch per SMS abgestimmt werden. Da jedoch Schwierigkeiten mit der Benutzerfreundlichkeit bei Abstimmen per SMS entstanden, weil zudem die Nutzung sehr gering war und SMS als nicht-zukunftsfähig betrachtet werden, wurde Ende 2007 entschieden, das Abstimmen per SMS nicht mehr zu ermöglichen.</p> <p>Ein heikler und stets zu beachtender Risikofaktor ist die Harmonisierung / Verknüpfung der Stimmregister. Diese werden durch die Gemeinden auf dem aktuellen Stand gehalten. Ebenfalls sorgt die Gemeinde für die Auswertung der Stimmen. Um diese Stimmen jedoch auszuwerten können, erhält jede Gemeinde ein Passwort und einen Schlüssel um diese Stimmen zu öffnen und auszuwerten. Es ist möglich, dass Berechtigungsprobleme bei der Auswertung der Stimmen erscheinen. Aus diesem Grund muss jeder Gemeinde Support angeboten werden.</p> <p>Im Kanton Zürich existieren laut Giampiero Beroggi, dem Chef des Statistischen Amtes, aktuell Schwierigkeiten mit der Wahlsoftware. Aus diesem Grund wird in diesem Jahr (2011) E-Voting nur für Abstimmungen auf kommunaler Ebene verwendet.¹⁰²</p> <p>Die doppelte Stimmabgabe ist auch ein Faktor, welcher stets zu beachten ist. Eine doppelte Stimmabgabe hat rechtliche Konsequenzen, weil Wahlbetrug strafbar ist. Aus diesem Grund muss der Stimmbürger bei Erhalt des Stimmrechtsausweises überprüfen, ob das Rubbelfeld noch geschlossen ist. Ist das Rubbelfeld bereits geöffnet, muss dies der Gemeinde gemeldet werden. Danach wird überprüft, ob ein Wahlbetrug vorliegt. Diese Überprüfung des Rubbelfeldes muss in jedem Fall überprüft werden, auch wenn per Brief oder an der physischen Urne abgestimmt wird. Die Erkennung einer doppelten Stimmabgabe muss zudem ohne Rückschluss auf die genutzten Kanäle erfolgen.</p>
Organisatorische Schwierigkeiten	<p>Eine organisatorische Schwierigkeit stellt die Harmonisierung / Verknüpfung der dezentralen Stimmregister dar, da diese Stimmregister verknüpft werden müssen, ohne dass den Gemeinden die Eigenständigkeit verloren geht. Die Gemeinden müssen wie bereits erwähnt, die Stimmen selbst auswerten. Der Kanton wird schlussendlich nur noch die Stimmen addieren.¹⁰³</p>

Tabelle 22 / Lösung zum E-Voting Projekt im Kanton Zürich

¹⁰² DRS (2010)¹⁰³ Gemeinde Bülach (2005)

Stimmrechtsausweis

Auf dem Stimmrechtsausweis¹⁰⁴ im Kanton Zürich gelten die roten Elemente für E-Voting:

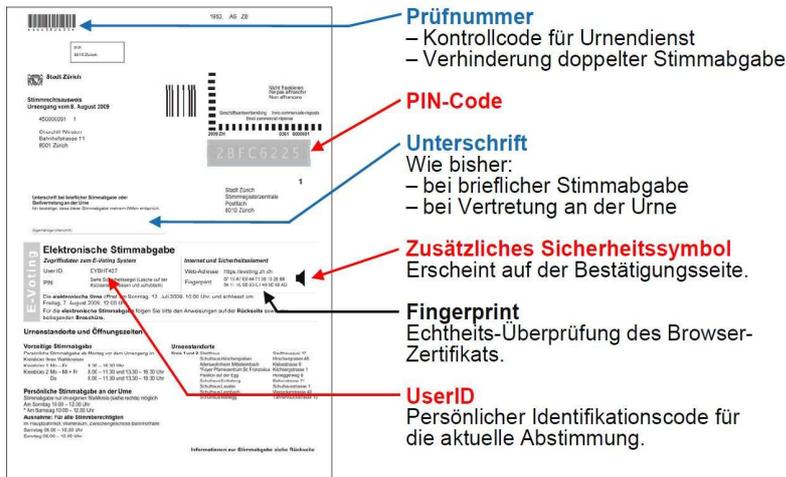


Abbildung 6 / Stimmrechtsausweis im Kanton Zürich

E-Voting Projekt im Kanton Neuenburg¹⁰⁵

Wie der Kanton Zürich, war der Kanton Neuenburg einer von drei Kantonen, welcher Pilot-Projekte zu E-Voting durchführten. Deshalb wurde auch Ende 2006 ein Gesuch an den Bund gestellt um die Erlaubnis zu erhalten, am 17.06.2007 Vote électronique einzusetzen. Der Bund kam diesem Wunsch ebenfalls am 04.04.2007 nach. Im Kanton Neuenburg müssen sich aber interessierte Stimmbürger zuerst am „Guichet Unique“ anmelden, einem elektronischen Schalter, welcher dem Bürger diverse Online-Dienstleistungen anbietet. Die Anmeldung erfolgt bei einer amtlichen Stelle mit einem Formular und der Unterschrift per Hand.

Allgemeine Projektinformationen

Element	Beschreibung
Zeitpunkt	Eidgenössische, kantonale und kommunale Abstimmung vom 17.06.2007
Organisation	Kanton Neuenburg
Partnerunternehmen	Arcantel (für die Anwendung) und ScytI (für die Verschlüsselung)
Zielgruppe	Auf dem „Guichet Unique“ registrierte Stimmbürger des Kantons
Grösse der Zielgruppe	Total: 4'151 Stimmbürger
Prozentuale Nutzung	Total: 35,99 % aller am GU registrierten Nutzer

Tabelle 23 / Allgemeine Informationen zum E-Voting Projekt im Kanton Neuenburg

¹⁰⁴ Quelle: https://evoting.zh.ch/MainPage/pdf/anleitung_evoting.pdf (S. 6)

¹⁰⁵ Bericht Leuenberger / Huber-Hotz (2006)

Lösung / Entwicklung

Element	Beschreibung
Technischer Ablauf	<p>Wenn der Stimmbürger E-Voting nutzen will, meldet sich dieser Stimmbürger am „Guichet Unique“ (GU) an. Bei erfolgreicher Anmeldung erhalten die Stimmbürger ein Login für ihr GU-Konto. Wenn sich der Stimmbürger einloggt, kann dieser E-Voting nutzen. Automatisch wird der Zugang zu Abstimmungen generiert, bei welchen auch eine tatsächliche Stimmberechtigung existiert.</p> <p>Bei der Stimmabgabe kreuzen die Stimmbürger die entsprechenden Kästchen auf dem elektronischen Stimmzettel an. Um die Korrektheit der Stimmabgabe zu überprüfen, zeigt GU noch einmal die Eingaben auf dem Stimmzettel an. Damit die Stimmen endgültig auf das E-Voting System übermittelt werden, muss der Validierungscode eingegeben werden. Dieser Validierungscode befindet sich auf dem Stimmrechtsausweis. Nach der Stimmabgabe erscheinen eine Empfangsbestätigung sowie ein Bestätigungscode. Der Bestätigungscode sollte dem Code auf dem Stimmrechtsausweis entsprechen. Ist dies der Fall, bedeutet dies, dass die Stimme dem Server korrekt übermittelt wurde.</p>
Organisatorischer Ablauf	<p>Anders als in Zürich dürfen auch Ausländer mit C-Ausweis an kantonalen Wahlen teilnehmen. Ausländer mit C-Ausweis haben jedoch keine Stimmberechtigung zu Wahlen auf Bundesebene. Registrierte und im Kanton Neuenburg stimmberechtigte Benutzer des „Guichet Unique“, erhalten vor der Wahl einen Stimmrechtsausweis, welcher wie im Kanton Zürich zusätzliche Elemente für E-Voting aufweist. Allerdings sind diese Elemente anders als in Zürich und bestehen aus einem Bestätigungs- und Validierungscode. Die Stimmregister der Gemeinden werden auf kantonaler Ebene verknüpft. Wie im Kanton Zürich muss die Stimmabgabe per E-Voting auch in Neuenburg sechs Wochen vor der tatsächlichen Abstimmung möglich sein. Aus diesem Grund erhalten die am GU registrierten Stimmbürger in diesem Zeitraum den neuen Stimmrechtsausweis.</p> <p>Nachdem die Stimmen ausgezählt sind, können die Stimmbürger in einer im Internet veröffentlichten Liste überprüfen, ob die Empfangsbestätigung dort publiziert wird. Ist die persönliche Empfangsbestätigung dort vorhanden, kann sichergestellt werden, dass die Stimme korrekt ausgezählt wurde.</p> <p>Die Empfangsbestätigung ist getrennt von der konkreten Stimmabgabe, deshalb ist es auch nicht möglich herauszufinden, welcher Stimmbürger wie abgestimmt hat.</p>

Element	Beschreibung
Technische Eigenschaften	<p>E-Voting System:</p> <p>Die Stimme ist von Anfang bis zum Ende verschlüsselt. Dadurch kann das Stimmgeheimnis eingehalten werden. Die Infrastruktur des GU befindet sich in streng gesicherten Räumlichkeiten, zu welchen nur Personen mit der entsprechenden Berechtigung Eintritt gewährleistet wird. Auf jedem Stimmrechtsausweis befindet sich wie im Kanton Zürich ein Barcode. Dadurch kann eine doppelte Stimmabgabe entdeckt werden.</p> <p>Browsereinstellungen:</p> <ul style="list-style-type: none"> - Bei der Nutzung von E-Voting muss eine SSL Verbindung bestehen. - Nach Eingabe der User-ID müssen in jedem Fall das Wappen und der Name der Gemeinde erscheinen. - Durch das Löschen des Browser-Cache kann die Sicherheit von E-Voting zusätzlich erhöht werden. - Die Empfangsbestätigung auf dem Stimmrechtsausweis muss der Empfangsbestätigung in der im Internet publizierte Liste entsprechen
Organisatorische Eigenschaften	<p>Sämtliche kommunalen Stimmregister werden vor einer Abstimmung in der aktuellsten Version an den GU übertragen. Dort wird anschliessend das zentrale Stimmregister erstellt. Damit keine doppelte Stimmabgabe möglich ist, wird die erste Stimmabgabe registriert. Während das zentrale Stimmregister erstellt wird, werden auch der Validierungs- und Bestätigungscode generiert. Beide landen am Schluss auf dem Stimmrechtsausweis. Diese Stimmrechtsausweise werden durch den Kanton gedruckt. Zur Sicherheit verfügt jeder Stimmrechtsausweis ein Hologramm mit dem Wappen des Kantons.</p>
Technische Schwierigkeiten	<p>Der Kanton Neuenburg prüfte ihr E-Voting System durch ein Unternehmen, welches auf Audits spezialisiert ist. Dabei konnten Stimmen vor dem Absenden abgefangen und manipuliert werden. Deshalb wurde die Sicherheit erhöht und noch einmal überprüft. Dabei wurden die technischen Schwierigkeiten im Authentifizierungsprozess entdeckt. Allerdings sind beiden Probleme in der Zwischenzeit gelöst.</p>
Organisatorische Schwierigkeiten	<p>Bevor E-Voting genutzt werden kann, muss eine Anmeldung am „Guichet Unique“ erfolgen. Aus diesem Grund müssen die Stimmregister ständig auf aktuellstem Stand sein und eine Anmeldung am GU muss ein Tag vor der Abstimmung auch noch möglich sein.</p>

Tabelle 24 / Lösung zum E-Voting Projekt im Kanton Neuenburg

E-Voting Projekt im Kanton Genf¹⁰⁶

Im Februar 2009 gab es im Kanton Genf eine Volksabstimmung über die Einführung von E-Voting. Obwohl eine Minderheit Sicherheitsbedenken äusserte, wurde die Vorlage von rund 70 % der Stimmberechtigten angenommen. Allerdings ist der Kanton Genf genau wie die Kantone Zürich und Neuenburg bereits seit einigen Jahren an Pilot-Projekten beteiligt. Im Rahmen der Pilot-Projekte, wurde die Nutzung von Vote électronique für die kantonale Abstimmung vom 24.04.2005 bewilligt, da frühere Tests zeigten, dass das E-Voting System in Genf ausreichende Sicherheit besitzt.

Allgemeine Projektinformationen

Element	Beschreibung
Zeitpunkt	Kantonale Abstimmung vom 24.04.2005
Organisation	Kanton Genf mit kantonseigenen Informatikdienst „Centre des technologies de l'information de l'État (CTI)“.
Partnerunternehmen	Hewlett Packard Schweiz (Hard- und Software), Wisekey (Verschlüsselungstechnologie) und blueinfinity (Sicherheit)
Zielgruppe	Bürger, welche im Kanton Genf stimmberechtigt sind.
Grösse der Zielgruppe	Total: 88'082
Prozentuale Nutzung	Total: 8,98 % (wenn Stimmbeteiligung = 100%)

Tabelle 25 / Allgemeine Informationen zum E-Voting Projekt im Kanton Genf

Lösung / Entwicklung

Element	Beschreibung
Technischer Ablauf	<ol style="list-style-type: none"> 1. Für den Zugang zum E-Voting System muss ein sechzehnstelliger Code eingegeben werden. Dieser Code wird durch das Geburtsdatum, das Geschlecht sowie der Heimatgemeinde generiert und befindet sich auf dem Stimmrechtsausweis. Nach der Eingabe des korrekten Codes, ist der Zugriff auf das E-Voting System gewährleistet. 2. Im nächsten Schritt kann der Stimmbürger seine Stimme abgeben. 3. Zur Bestätigung wird dem Stimmbürger seine Stimme angezeigt. Anschliessend erfolgt die Identifikation des Stimmbürgers mittels Geburtsdatum, Heimatgemeinde sowie einem sechsstelligen Geheimcode. Dieser Code wird für jeden Stimmrechtsausweis und pro Abstimmungssonntag neu generiert. 4. Im letzten Schritt wird dem Stimmbürger durch das E-Voting System bestätigt, dass die Stimme korrekt übermittelt wurde.

¹⁰⁶ Bericht Leuenberger / Huber-Hotz (2006)

Element	Beschreibung
Organisatorischer Ablauf	<p>In Genf dürfen Ausländer mit C-Ausweis auch an einer Abstimmung auf kantonaler teilnehmen. Zudem sind Auslandschweizer, welche ihre Heimatgemeinde im Kanton Genf haben, auch stimmberechtigt. Im Vergleich zu den beiden anderen E-Voting Projekten in Zürich und Neuenburg, hatte Genf von Anfang an ein kantonales Stimmregister. Dieses Stimmregister wird stets auf aktuellem Stand gehalten.</p> <p>Die Daten des Stimmregisters stammen einerseits aus dem Einwohnerregister aber auch aus dem Register für Auslandschweizer.</p> <p>Die Stimmabgabe wird verschlüsselt an das E-Voting System übermittelt. Dabei wird die Stimme mit Zufallszeichen kombiniert. Bei der unerlaubten Betrachtung des Stimmzettels wäre nur eine Reihe von Zeichen zu sehen. Die Bestätigung der Stimme wird an den Stimmbürger kombiniert mit einem Bild zurückgesendet. Durch diese Kombination mit einem Bild, ist der Inhalt dieser Bestätigung für Hacker nicht herauszulesen, weil für jede stimmberechtigte Person die Bestätigung mit einem anderen Bild kombiniert wird. Entspricht das Bild der Bestätigung dem Bild auf dem Stimmrechtsausweis, kann sichergestellt werden, dass eine korrekte Verbindung mit dem E-Voting System besteht.</p> <p>Wie in Zürich und Neuenburg muss die Stimmabgabe per E-Voting auch in Genf sechs Wochen vor der tatsächlichen Abstimmung möglich sein. Aus diesem Grund erhalten die Stimmbürger in diesem Zeitraum den neuen Stimmrechtsausweis.</p>
Technische Eigenschaften	<p>E-Voting System:</p> <p>Das zentrale Stimmregister wird vor der Wahl anonymisiert. Jeder Stimmbürger wird mit einem eindeutigen sechzehnstelligen Code registriert. Dieser Code befindet sich auf dem Stimmrechtsausweis neben einem anderen Code, dem sechsstelligen Geheimcode. Die Seite der Stimmeabgabe ist zertifiziert. Durch das Betrachten dieses Authentifikationszertifikates kann der Stimmberechtigte sicherstellen, dass er korrekt mit dem E-Voting System verbunden ist. Die Stimmabgabe und Authentifikation des Stimmbürgers werden in zwei unterschiedlichen Datenbanken gespeichert.</p> <p>Browser-Einstellungen:</p> <ul style="list-style-type: none"> - Bei der Nutzung von E-Voting muss eine SSL Verbindung bestehen. - Das Zertifikat bei der Stimmabgabe muss gültig sein. - Das Löschen des Browser-Cache erhöht die Sicherheit von E-Voting.

Element	Beschreibung
Organisatorische Eigenschaften	<p>Eine doppelte Stimmabgabe kann im Kanton Genf ebenfalls sofort entdeckt werden, nämlich wenn der Code freigerubbelt wurde, kann dies sowohl bei der Briefabgabe aber auch bei der Stimmabgabe an der physischen Urne entdeckt werden.</p> <p>Die Stimmen werden in Gebäuden der Kantonspolizei Genf ausgezählt. Dabei haben nur berechtigte Personen und Kontrolleure Zugriff in diese Räumlichkeiten. Danach der Computer, welcher die Stimmen auszählt, mit dem E-Voting System mit einem Kabel verbunden. Die Stimmen auf dem E-Voting System sind zu diesem Zeitpunkt noch verschlüsselt. Anhand von zwei Passwörtern können nun die Kontrolleure die Stimmen entschlüsseln und auszählen. Nach dem die Auszählung der E-Voting Stimmen abgeschlossen ist, werden die Stimmen mit denen der beiden anderen Kanälen verbunden.</p>
Technische Schwierigkeiten	<p>In den ersten E-Voting Durchläufen im Kanton Genf traten Probleme beim Entschlüsselungsprogramm auf. Allerdings konnte dieses Problem mit Hilfe von Audits gelöst werden.</p> <p>Bei technischen Problemen während der Abstimmung, muss der Systemadministrator sofort und automatisch alarmiert werden. In einem Massnahmenplan wurden Reaktionen für unterschiedlichste Schwierigkeiten definiert. Sind trotz dem Massnahmenplan technische Probleme vorhanden, muss ein Krisenstab entscheiden, ob der Zugang zum E-Voting System abgebrochen oder weiter aufrechterhalten bleibt. Nach der Abstimmung muss die Anzahl an für E-Voting genutzten Stimmrechtsausweisen den tatsächlichen per E-Voting abgegebenen Stimmen entsprechen. Dabei gilt eine Null-Toleranz. Ist auch nur eine Stimme zuviel per E-Voting abgegeben worden als dass Stimmrechtsausweise für E-Voting genutzt wurden, müssen sämtliche E-Voting Stimmen für ungültig erklärt werden.</p>
Organisatorische Schwierigkeiten	<p>Im Vergleich zu Zürich sind in Genf Ausländer mit C-Bewilligung bei kommunalen und kantonalen Abstimmungen auch stimmberechtigt. Zudem dürfen Auslandschweizer mit einer Heimatgemeinde im Kanton Genf an sämtlichen Abstimmungen E-Voting nutzen.</p>

Tabelle 26 / Lösung zum E-Voting Projekt im Kanton Genf

Selbständigkeitserklärung

Ich, Pascal Müller, bestätige die vorliegende Arbeit selbständig verfasst zu haben. Sämtliche Textstellen, die nicht von mir stammen, sind als Zitate gekennzeichnet und mit dem genauen Hinweis auf ihre Herkunft versehen. Die verwendeten Quellen sind im Literaturverzeichnis aufgeführt.

Bern, 13. Mai 2011

Pascal Müller