

Einführung in E-Voting und deren Probleme

Bülent Demirbas
Hochschule für Technik

8. Dezember 2006

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlegendes	2
2.1	Defintion E-Voting	2
2.2	Vorteile E-Voting	2
3	Wahlrechtsgrundsätze und Wahlarten	3
4	Elektronische Wahlen	4
4.1	Verfahren zur Stimmabgabe	4
4.1.1	Präsenzwahl	4
4.1.2	Distanzwahl	4
4.2	Organisatorische und Technische Anforderungen für eine Wahl .	5
4.2.1	Politische Anforderungen	5
4.2.2	Notwendige Sicherheitsanforderungen an e-Voting Systeme	6
5	Lösungsansätze	8
5.1	Einfacher Einsatz	8
5.2	Kryptographie	8
5.2.1	Einsatz asymmetrischer Kryptographie	9
5.2.2	Einsatz von digitaler Signatur	9
6	Weitere Probleme	11
7	Zusammenfassung	12

1 Einleitung

57,8 % der Bevölkerung in Deutschland nutzen das Internet. Das bestätigen die Zahlen aus einer Studie der Arbeitsgemeinschaft Online Forschung [1]. Das Internet hat sich in den vergangenen Jahren zu einem riesigen Markt entwickelt. Es werden Einkäufe wie „online-shopping“ oder Bankgeschäfte wie „online-Banking“ über das Internet durchgeführt.

Somit versucht sich auch der Staat in der Politik an die moderne Zeit anzupassen. Es finden Wahlen via Internet statt, das „E-voting“ genannt wird. Das E-voting bezeichnet die elektronische Wahl. Das Ziel soll sein, dass der Bürger von seinem Computer aus wählt und mittels unserer jetzigen Kommunikationsmöglichkeiten seine Stimme in der Urne ankommt. Das klingt nicht schwer, da man seine Stimme abgibt und auf senden drückt, um seine Stimme zu versenden. Der Vorteil von E-voting ist, dass es zu einer schnelleren Auswertung führen könnte oder die Wahlbeteiligung könnte erhöht werden insbesondere durch die jüngeren Wähler. Um aber elektronische Wahlen durchführen zu können, wird verlangt, dass die gesetzlichen Wahlvorschriften nach „Artikel 38 des Grundgesetzes“ eingehalten werden. Diese Anforderungen sind:

- Geheime Wahl
- Allgemeine Wahl
- Gleiche Wahl
- Freie Wahl
- Unmittelbare Wahl

Es wird versucht, mit diesen Anforderungen die elektronischen Wahlen umzusetzen, was aber nicht einfach ist - im Hinblick auf das Grundgesetz. Wie soll eine geheime Stimme abgegeben werden, wenn Administratoren die technische Möglichkeit haben, die Stimme zu identifizieren bzw. zu verändern? Das ist eines von vielen Problemen, die weiter unten im Hauptteil genannt werden. Aufgrund der Probleme kann das Grundgesetz nicht geändert werden, aber es werden Lösungen entwickelt, um die elektronischen Wahlen an das Grundgesetz anzupassen.

Mit dieser Arbeit wird versucht, die Schwierigkeiten von den elektronischen Wahlen auf den Punkt zu bringen. Es werden Lösungsansätze vorgeschlagen.

In Kapitel 2 wird zunächst Grundlegendes und Vorteile von E-voting geschildert. In Kapitel 3 werden die Wahlrechtsgrundsätze und Wahlarten vorgestellt. Kapitel 4 werden die elektronischen Wahlen mit ihren dazugehörigen Punkte wie Verfahren zur Stimmabgabe und organisatorische und technische Anforderungen gezeigt. Kapitel 5 beschäftigt sich mit den Lösungsansätzen. Zum Schluss ergibt sich dann das Fazit.

2 Grundlegendes

2.1 Defintion E-Voting

Der Begriff E-Voting kommt von Electronic Voting. Unter E-Voting oder elektronische Wahl bezeichnet man die elektronische Form einer Wahl oder Volksabstimmung.

2.2 Vorteile E-Voting

Im folgenden werden die Vorteile von elektronischen Wahlen näher erläutert.

- **Höhere Wahlbeteiligung**
Durch die leichtere Stimmabgabe wird erwartet, dass die Bürger an den elektronischen Wahlen mehr beteiligt sind. Zudem ist noch zu rechnen, dass die jüngeren Wähler aufgrund der Statistik mehr an den Wahlen teilnehmen.
- **Exakte Auszählung der Stimmen**
Mit der Unterstützung der Technik werden beim auszählen der Stimmen Fehler vermieden.
- **Effizienzsteigerung**
Es ist leicht vorher zu sehen, dass die Auszählung der Stimmen schneller als jedes manuelle Verfahren ist. Ein weiterer Punkt ist auch der, dass die Technik, wenn alles gut läuft, keine Fehler bei der Auszählung der Stimmen verursacht. Zudem ersetzt es noch Wahlhelfer.
- **Ortsunabhängigkeit**
Am Wahltag ist man nicht gebunden, sich am Wohnort aufzuhalten.

3 Wahlrechtsgrundsätze und Wahlarten

Bevor weiter über die elektronischen Wahlen diskutiert wird, sollen als erstes die allgemeinen Wahlrechtsgrundsätze aufgezeigt werden. Sie sind im Grundgesetz der Bundesrepublik Deutschland im Artikel 38 festgelegt und im Absatz 1 lautet : „Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.[...]“. Diese Grundsätze gelten natürlich auch für die elektronische Wahl.[3]

Im folgenden werden die fünf Wahlgrundsätze näher beschrieben.

- Allgemein
Jeder Wahlberechtigte muss wählen können, die das Wahlalter erreicht haben.
- Unmittelbar
Die abgegebenen Stimmzettel dürfen weder geändert noch entfernt werden. Es werden genau die abgegebene Stimmzettel gezählt.
- Frei
jeder Wähler darf seine Stimme geheim abgeben und darf nicht von dritten Personen beeinflusst werden. Die abgegebene Stimme sollte in der Urne so ankommen wie abgegeben.
- Gleich
alle Wähler verfügen über die gleiche Zahl von Stimmen, deren Gewicht ebenfalls gleich ist
- Geheim
niemand darf mitbekommen was der einzelnen Wähler gewählt hat.

Bevor auf die elektronischen Wahlen näher eingegangen wird, ist es auch noch wichtig zwischen der Präsenzwahl und Distanzwahl zu unterscheiden.[5]

- Präsenzwahl
Der Wähler geht ins Wahllokal und gibt unter Aufsicht von den Wahlhelfern seine Stimme persönlich ab.
- Distanzwahl
Der Wähler gibt seine Stimme ab und sendet seine Wahlkarte per Post an die Wahllokale. In manchen Ländern wird die Distanzwahl als Briefwahl bezeichnet.

Diese Unterscheidung ist notwendig und spielt bei den elektronischen Wahlen bei der Stimmabgabe eine wichtige Rolle. Dazu mehr im nächsten Kapitel.

Besonders schwierig wird es jetzt. Diese Anforderungen müssen bei den elektronischen Wahlen erfüllt werden. Aber wie kann das funktionieren, wenn einerseits die Stimme geheim bleiben soll und andererseits muss die Stimme identifiziert werden, da jeder Wähler höchstens eine Stimme abgeben darf? Im folgenden werden auf die zu erfüllende technische und organisatorische Anforderungen näher eingegangen. Des weiteren werden für die Anforderungen Lösungsansätze geschildert.

4 Elektronische Wahlen

Unter den Begriff „elektronische Wahlen“ werden alle Wahlmethoden zusammengefasst, die mittels sich einer elektronischen Tätigkeit behelfen lassen wie z.B. Abgeben der Stimme, Identifizierung des Wählers oder die Auswertung der Stimmen. Um es deutlicher zu machen ist es wichtig zu unterscheiden, welche Wahlmethode benutzt wird mithilfe von elektronischen Hilfsmittel, da es für jeden Wahlvorgang unterschiedliche Bezeichnungen gibt.

4.1 Verfahren zur Stimmabgabe

Um hier einen besseren Überblick zu bekommen, werden die Wahlmethoden der Präsenzwahl und Distanzwahl zugeordnet.

4.1.1 Präsenzwahl

- Online-Wahl
Man spricht von der Online-Wahl, sobald die Wahllokale untereinander elektronisch vernetzt sind und die abgegebene Stimme elektronisch in der Urne ankommt. Die Online-Wahl wird als ein übergeordneter Begriff angesehen.
- Internet-Wahl
Das Internet-Wahl ist nichts anderes als die Online-Wahl, da hier die Stimme auch über das Internet befördert wird. Jedoch könnte hier unterschieden werden ob es sich um offenes Netzwerk oder geschlossenes Netzwerk handelt. (Intranet) Ein Beispiel wäre dazu, dass innerhalb einer Firma über das Intranet Betriebsratswahlen stattfinden.
- Kiosk-Voting
Darunter versteht man, wenn die Wahlgeräte außerhalb der Wahllokale in öffentlichen Orten stehen wie z.B. öffentliche Gebäuden oder Universitäten.

4.1.2 Distanzwahl

- Remote Internet Voting
- Home-Online-Voting
- I-Voting
Alle drei Begriffe haben dieselbe Bedeutung und sind dasselbe wie E-Voting. Der Unterschied zur Präsenzwahl ist nur dieser, dass mit diesen Wahlen ausserhalb der Wahllokale gewählt werden kann mittels eigenen oder fremden Computern und das Internet als Transportmedium der Stimme verwendet wird. Weiter oben wurden 5 Anforderungen vorgestellt, die im Grundgesetz stehen. Um es jetzt auf elektronische Wahlen zu übertragen, definieren diese Anforderungen die Sicherheit des Wählers. Daraus

ist zu schliessen, dass für jede elektronische Wahl diese Anforderungen erfüllt sein müssen. Im Folgenden wird näher auf diese eingegangen, da sie für das Verständnis der Arbeit unverzichtbar sind und sich daraus die Sicherheitsanforderungen an Internetwahlen ableiten lassen.

4.2 Organisatorische und Technische Anforderungen für eine Wahl

Weiter oben wurden 5 Anforderungen vorgestellt, die im Grundgesetz stehen. Um es jetzt auf elektronische Wahlen zu übertragen, definieren diese Anforderungen die Sicherheit des Wählers. Daraus ist zu schliessen, dass für jede elektronische Wahl diese Anforderungen erfüllt sein müssen. Im Folgenden wird näher auf diese eingegangen, da sie für das Verständnis der Arbeit unverzichtbar sind und sich daraus die Sicherheitsanforderungen an Internetwahlen ableiten lassen.

4.2.1 Politische Anforderungen

- Allgemein
Der Grundsatz der allgemeinen Wahl garantiert dass jeder die Gleichheit zur Zugang der Wahl hat. Das Wahlverfahren muss ausfallsicher sein. Wie die Briefwahl, könnte eine Internetwahl die Allgemeinheit der Wahl steigern, da Abwesende, Kranke usw. ihre Stimme von einem beliebigen Ort aus abgeben können.
- Unmittelbar
Dieser Punkt sagt aus, dass zwischen der Stimmabgabe und der Stimmenwertung keine weitere Instanz liegen darf, da sonst das Wahlergebnis beeinflusst werden könnte. Desweiteren darf der Wähler überprüfen, ob seine Stimme korrekt und unverändert gezählt wurde. Bei dieser Überprüfung dürfen diese Quittungen für die anderen Wähler nicht sichtbar sein, da sonst die Wahlentscheidung des Wählers sichtbar wäre.
- Frei
Dies sagt dass der Wähler seine Stimme frei abgeben kann, ohne jegliche Beeinflussung durch dritte. Bei Internetwahlen könnte das durch Wahlpropaganda mittel Pop-ups oder bezahlte Bannerwerbung passieren, die dann den Wähler beeinflussen könnten.
- Gleich
Der Grundsatz der gleichen Wahl stellt sicher, dass jede Stimme den gleichen Zählwert hat und somit den gleichen Einfluss auf das Wahlergebnis. Darum muss bei elektronischen Wahlen die Mehrfachwahl ausgeschlossen werden.
- Geheim
Dieser Grundsatz sagt aus, dass nur der Wähler seine Stimme kennen darf.

Bei elektronischen Wahlen bedeutet dies, dass seine abgegebene Stimme nicht zurückverfolgbar sein darf und auch dauerhaft Geheim bleiben muss.

4.2.2 Notwendige Sicherheitsanforderungen an e-Voting Systeme

Im folgenden werden die Sicherheitsanforderungen von elektronischen Wahlen vorgestellt, die erfüllt werden müssen, um gleichzeitig die politischen Anforderungen zu erfüllen. Die Anforderungen werden jeweils der zugehörigen Punkte zugeordnet.

Wahlgeheimnis:

- Das Wahlgeheimnis muss gewahrt werden. Niemand außer dem Wähler selber darf in Erfahrung bringen dürfen, was dieser gewählt hat.
(Geheimheit)
- Es muss sichergestellt werden, dass niemand eine Aufzeichnung des verschlüsselten Textes zwischen Wahl-Client und Wahlamt durchführt, weil evtl. viele Jahre später neue Technologien entwickelt werden können, um solche verschlüsselten Stimmzettel zu entschlüsseln.
(Geheimheit)
- Zuständige Mitarbeiter bzw. Administratoren dürfen nicht die Möglichkeit haben, die abgegebenen Stimmen zu sehen.
(Geheimheit)

Korrektheit des Ergebnisses:

- Das System darf keine Fehler hervorbringen und muss ein korrektes Ergebnis ermitteln. Alle wahlberechtigten dürfen höchstens einen Stimmzettel abgeben.
(Allgemeinheit, Gleichheit)
- Es muss sichergestellt werden, dass bei einem Systemausfall, die abgegebenen Stimmen Bitgenau übernommen werden müssen, um somit nicht das Wahlergebnis zu verändern.
(Allgemeinheit, Gleichheit)
- Wurde die abgegebene Stimme nicht angenommen zwecks den Client-Rechnern und den Wahl-Servern, so ist es sofort dem Wählenden mitzuteilen.
(Allgemeinheit)
- Die Systemadministratoren dürfen nicht die Ergebnisse manipulieren.
(Gleichheit)
- Die Wahl-Server könnten von dritten Personen als ein Ziel darstellen um somit die Wahlergebnisse zu manipulieren. Somit müssen sämtliche Server der Wahlen einbruchssicher sein.
(Gleichheit)

- Die Ergebnisse müssten so berechnet werden, dass selbst durch die Hardware erzeugten Bitfehler das Ergebnis nicht beeinflussen kann.
(Gleichheit)

Client - Rechnersicherheit:

- Alle Anforderungen, die für das Onlinewahlssystem gelten, müssen auch für die Wahl-Clients gelten.
(Allgemeinheit, Gleichheit, Geheimheit)
- Dem Wähler ist es nicht zuzumuten, selbständige Konfigurationen bzw. Software-installationen zwecks des Clients durchführen zu lassen. (Allgemeinheit)
- Es muss garantiert werden, dass die Software des Clients auf jedem beliebigen Rechner läuft und keine jeglichen Programme Voraussetzungen für die Software sind.
(Allgemeinheit)

Verfügbarkeit:

- Es muss sichergestellt werden, dass die Wahl an dem festgesetzten Tag durchzuführen ist. Deshalb muss das Wahlsysteme an dem Tag der Wahl funktionsfähig und verfügbar sein.
(Allgemeinheit)
- Es muss gewährleistet werden, dass bei einem Systemausfall in einer der Wahllokale die Wähler sich an die anderen Wahllokale begeben können.
(Allgemeinheit)

Transparenz:

- Die Komponenten wie der Source-Code der Online-Wahl, die eingesetzte Hardware und die Beschreibung des eingesetzten Wahlprotokolls muss der Öffentlichkeit bekannt gegeben werden, um Vertrauen für das Wahlsysteme zu gewinnen.
(Allgemeinheit, Gleichheit, Geheimheit)
- Für die interessierten Bürger und Organisationen muss es eine Möglichkeit geben, sich überzeugen zu lassen, dass das Wahlsysteme genau die Vorschrift einhält was auch vorgeschrieben ist.
(Allgemeinheit, Gleichheit, Geheimheit)

5 Lösungsansätze

Im Folgenden werden verschiedene Lösungsansätze zur Elektronischen Wahlen untersucht, mit denen versucht wird, die genannten Sicherheitsanforderungen zu erfüllen.

5.1 Einfacher Einsatz

Dieses Wahlverfahren ist das einfachste und entspricht wie beim Zettelverfahren der Präsenzwahl. An dieser Wahl sind drei Instanzen beteiligt. Der Wähler (Wahlberechtigter), Kontrolleur(entspricht dem Wahllokal)und das System dass die Stimmen zählt bzw. Auszähler(Wahlurne). Jeder Wähler erhält eine eindeutige ID. Der Wähler sendet seine Stimme mit seiner ID an die Kontrolleure. Die schauen in ihren Verzeichnissen nach, ob der Wähler bereits gewählt hat oder nicht. Falls nicht, wird im Verzeichnis die ID durchgestrichen und die Stimme weitergeleitet an den Auszähler. Nach der Wahl gibt der Auszähler die Ergebnisse bekannt.[3]

Problematik:

Dieser Wahlvorgang zeigt Mängel, dass dadurch dieses Verfahren unbrauchbar wird.

- Das Wahlgeheimnis wird gebrochen, da die Wahlhelfer rauskriegen, wer der Wählende ist.
- Für den wählenden besteht keine Möglichkeit, zu überprüfen, ob sein eigener Stimmzettel gezählt worden ist.
- Die Wahlhelfer können die Stimmen manipulieren.
- Jeder Wahlbetrug kann nicht bemerkt werden.(externe Angreifer und sowohl als auch von Wahlhelfern)

5.2 Kryptographie

Das Stimmgeheimnis stellt Sicherheitsanforderungen, dass das Stimmgeheimnis gewahrt werden muss.

Kryptographie ist die Technik der Verschlüsselung von Daten. Ihre Aufgabe ist es, Daten vor Kenntnisnahme Unbefugter zu schützen. Die Kryptographie bietet die Möglichkeit, anhand von mathematischen Verfahren, Daten so umzuwandeln, dass sie nur mit einem passenden Schlüssel wieder zurückverwandelt werden kann. Die Kryptographie wird unterteilt in symmetrischer und asymmetrischer Verfahren. Das Symmetrische Verfahren basiert auf einem einzigen Schlüssel, der sowohl zur Verschlüsselung der Nachricht als auch zur Entschlüsselung dient. Beim asymmetrischen Verfahren hat jeder Benutzer ein oder mehrere Schlüsselpaare, wobei das Schlüsselpaar aus einen öffentlichen und einen geheimen Schlüssel besteht, das zur Signierung und zur Verschlüsselung eines

Dokuments dienen kann.

Da die beiden Verfahren fast identisch sind, wird nur auf die asymmetrische Kryptographie näher eingegangen.

5.2.1 Einsatz asymmetrischer Kryptographie

Bei dieser Methode werden die Wähler, Kontrolleure und der Auszähler jeweils mit einem Schlüsselpaar ausgestattet. (Vor jeder Wahl wird bei Ausgabe der Schlüssel registriert welcher Schlüssel wem gehört). Der Wähler signiert sein Stimmzettel und verschlüsselt es mit dem öffentlichen Schlüssel und sendet es mit seiner ID an die Wahllokale. Der Kontrolleur entschlüsselt die Nachricht und kann anhand der Signatur feststellen, dass der Stimmzettel tatsächlich vom Wähler mit der angegebenen ID stammt.

Problematik:

- Im System können Stimmzettel verändert, hinzugefügt oder auch verworfen werden.
- Ein Wahlbetrugsversuch kann nur aufgedeckt werden, wenn die Software des Herstellers bekannt ist. Zudem müsste auch vermerkt werden, welche Personen auf die Datenbank zugegriffen haben.
- Der Wähler selber kann nicht überprüfen, ob sein eigener Stimmzettel gezählt worden ist.

5.2.2 Einsatz von digitaler Signatur

Bei dieser Durchführung werden drei Instanzen gebildet. Der Wähler, Kontrolleur und der Auszähler. Jeder dieser Instanzen bekommen jeweils ein Schlüsselpaar (asymmetrische Verschlüsselung). Der Wähler vermerkt seine Stimmen auf dem Stimmzettel und die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel des Auszählers. Anschließend kommt die Signierung für den Kontrolleur. Diese verschlüsselte Nachricht wird nochmals mit dem Privaten Schlüssel verschlüsselt (diese Verschlüsselung dient für den Kontrolleur) und mit der Identifikationsnummer des Wählers an den Kontrolleur gesendet. Um nochmals ein Schutz von außen zu haben, wird das Gesamtpaket nochmals mit dem öffentlichen Schlüssel verschlüsselt.

Der Kontrolleur entschlüsselt die erste Schicht mit dem privaten Schlüssel. Er erhält die Identifikationsnummer. In der zweiten Schicht ist die Signatur vermerkt. Er entschlüsselt beide Verschlüsselungen, um die Identifikationsnummer und die Signatur abzugleichen. Falls beides nicht übereinstimmt, wird dies dem Auszähler nicht weitergeleitet und somit wird eine Mehrfachwahl vermieden. Falls Identifikationsnummer und die Signatur übereinstimmen, muss der Kontrolleur in seiner Wahlliste vermerken, dass derjenige gewählt hat. Um sicherzugehen, dass nur die abgegebenen Stimmen beim Auszähler ankommen, verschlüsselt der Kontrolleur dies nochmals mit seinem privaten Schlüssel.

Der Auszähler entschlüsselt seine zwei Verschlüsselungen und summiert die Ergebnisse auf.

Problematik:

- Wahllokal muss vermerken, wer eine Stimme abgegeben hat oder nicht, um Mehrfachwahlen auszuschließen.
- Der Wähler kann nicht kontrollieren ob seine Stimme gezählt wurde oder nicht.
- Falls Kontrolleur und Auszähler sich vereinen, könnte man die Identität des Wähler rauskriegen. Somit würde man das Wahlgeheimnis brechen.

6 Weitere Probleme

Hier werden Probleme geschildert, die in oberen Punkten nicht zur Diskussion standen.

- Es kann nicht nachgeprüft werden, ob auch die tatsächliche Software läuft, die vom Hersteller vorgegeben ist. Dies kann durch ein Zulassungsverfahren geprüft werden, aber wie kann zum Beispiel der Vorstand der Wahllokale sagen, dass auch wirklich die Software läuft, die vorgegeben wurde.
- Ein weiteres Problem ist das Vertrauen der Menschen zu den Wahlmaschinen. Im ganzen Land gehen die Wählenden zu den Wahllokalen, gehen an einem Computer den Sie nicht verstehen und drücken einen Knopf, damit dieser ihnen das Resultat ausgibt. Ohne die Auszählung von Papierstimmzetteln muss die Mehrheit der Wahlmaschine glauben, dass dies seine Richtigkeit hat.
- Die Kosten sind bei den elektronischen Wahlen ein weiteres Thema. Die Hersteller von Wahlmaschinen vermeiden Aussagen, das E-Voting billiger sei. Eine Wahl sei in Holland 1,6 auf 2,7 Millionen gestiegen.[2]

7 Zusammenfassung

Zum Schluss lässt sich sagen, dass aufgrund der hohen Sicherheitsanforderungen, gesetzliche Vorschriften und mit der jetzigen Technik das E-voting nicht in die Realität umgesetzt werden kann. Bevor versucht wird, die Internetwahlen durchzusetzen, ist es sinnvoller in kleinen Kreisen wie Wahllokale zu beginnen um daraus in den kleinen Wahllokalen entstehende Probleme auf die Internetwahlen zu übertragen.

Sollte es soweit sein, müsste auch in der gesetzlichen Regelung eine Änderung bzw. Ergänzungen in Betracht bezogen werden. Ein weiterer Schritt ist auch von großer Bedeutung, dass die Wahlbürger, die über das e-Voting wählen, Vertrauen in die Wahlsysteme bringen.

Literatur

- [1] Jeanette Christu, Stiftung Digitale Chancen *AGOF Internet facts 2006-II - Aktuelle Daten zur Internetnutzung in Deutschland* PM AGOF vom 30.11.06 (online Zeitschrift) <http://www.digitale-chancen.de/content/stories/index.cfm/aus.2/key.2456/secid.16/secid.2.49> Abgerufen am 15.11.06
- [2] Richard Stietmann, *Die Nicht-Lösung eines nicht existierenden Problems*, Computer Technik, 30.10.06 (online Zeitschrift)
- [3] Michael Philippsen, Internetwahlen - Demokratische Wahlen über das Internet, Internet: <http://www2.informatik.uni-erlangen.de/Forschung/Publikationen/download/wahlen.pdf?language=de> Version Oktober 2001 - Seminararbeit
- [4] Bernd Ziska, E-Voting Internet: <http://www.rechtsprobleme.at/doks/ziska-e-voting.pdf> Version Juni 2004 - Seminararbeit
- [5] Iris Vojtech, Elektronische Wahlen Internet: <http://www.net.informatik.tu-muenchen.de/teaching/SS04/security/docs/9.pdf> Version Sommersemester 2004 - Seminararbeit