

Einführung in E-Voting und dessen Probleme

Bülent Demirbas
Hochschule für Technik

31. Januar 2007

Inhaltsverzeichnis

1	Einleitung	1
2	Grundlegendes	2
2.1	Defintion E-Voting	2
2.2	Vorteile E-Voting	2
2.3	Nachteile E-Voting	2
3	Elektronische Wahlen	3
3.1	Wahlarten	3
3.1.1	Präsenzwahl	3
3.1.2	Distanzwahl	4
3.2	Anforderungen für eine Wahl	5
3.2.1	Gesetzliche Anforderungen	5
3.2.2	Notwendige Sicherheitsanforderungen	6
4	Lösungsansätze	8
4.1	Einfacher Ansatz	8
4.2	Einsatz von Kryptographie in E-Voting	9
4.2.1	Einsatz asymmetrischer Kryptographie	9
4.2.2	Einsatz von digitaler Signatur	10
4.2.3	Einsatz von blinder Signatur	11
5	Zusammenfassung	12

1 Einleitung

57,8 % der deutschen Bevölkerung 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 über „Online-shopping“ oder Bankgeschäfte via „Online-Banking“ über das Internet durchgeführt.

Somit versucht sich auch der Staat in der Politik anzupassen. Es sollen elektronische Wahlen, auch E-Voting genannt, stattfinden. 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 oder einer höheren Wahlbeteiligung führen könnte, insbesondere durch die jüngeren Wähler [1].

Um aber elektronische Wahlen durchführen zu können, ist es erforderlich, dass die gesetzlichen Wahlvorschriften nach Artikel 38 des Grundgesetzes eingehalten werden. Diese Anforderungen sind folgende: geheim, allgemein, gleich, frei, unmittelbar.

Mit diesen Anforderungen versucht man die elektronischen Wahlen umzusetzen. Im Hinblick auf das Grundgesetz erweist sich dies als problematisch. 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 im weiteren Verlauf dieser Arbeit angesprochen werden. Eine Änderung des Grundgesetzes ist, wie im Kapitel 3.2.1 erklärt wird, nicht möglich. Aber in der Informatik wird versucht, Lösungen zu finden, um die elektronischen Wahlen an das Grundgesetz anzupassen.

Mit dieser Arbeit sollen die Schwierigkeiten der Durchführung von elektronischen Wahlen auf den Punkt gebracht werden. Des Weiteren werden Lösungsansätze zu den elektronischen Wahlen geschildert.

In Kapitel 2 wird zunächst Grundlegendes und die dazugehörigen Vorteile und Nachteile von E-Voting geschildert. Kapitel 3 beschäftigt sich mit den elektronischen Wahlen und dazugehörigen Themen wie Wahlarten, gesetzlichen Anforderungen und die Sicherheitsanforderungen. Kapitel 4 zeigt Lösungsansätze wie den einfachen Ansatz und auch andere Lösungsansätze unter Verwendung der Kryptographie.

2 Grundlegendes

2.1 Defintion E-Voting

Der Begriff E-Voting kommt vom englischen Electronic Voting (deutsch: Elektronische Wahl). Mit E-Voting oder elektronische Wahl bezeichnet man die elektronische Form einer Wahl. Die Stimmabgabe findet nicht wie bei einer herkömmlichen Wahl statt, sondern über das Internet oder einen Wahlcomputer.

2.2 Vorteile E-Voting

Von E-Voting erhofft man sich die folgenden Vorteile [2].

- **Höhere Wahlbeteiligung**
Durch die einfachere Stimmabgabe wird erwartet, dass die Bürger sich stärker an den elektronischen Wahlen beteiligen. Laut Statistik [1] gilt dies insbesondere für die jüngeren Wähler.
- **Exakte Auszählung der Stimmen**
Mit der Unterstützung der Technik werden beim Auszählen der Stimmen Fehler vermieden. Grundlage ist eine fehlerfreie Software.
- **Effizienzsteigerung**
Die Auszählung der Stimmen ist bei E-Voting schneller als jedes manuelle Verfahren.

2.3 Nachteile E-Voting

Die Nachteile werden im weiteren Verlauf der Ausarbeitung deutlich.

3 Elektronische Wahlen

Unter den Begriff elektronische Wahlen werden alle Wahlmethoden zusammengefasst, die sich mittels einer elektronischen Tätigkeit durchführen lassen wie z.B. Abgeben der Stimme, Identifizierung des Wählers oder die Auswertung der Stimmen [4].

3.1 Wahlarten

Um hier einen besseren Überblick zu bekommen, werden die Wahlmethoden der Präsenzwahl und Distanzwahl zugeordnet [4].

3.1.1 Präsenzwahl

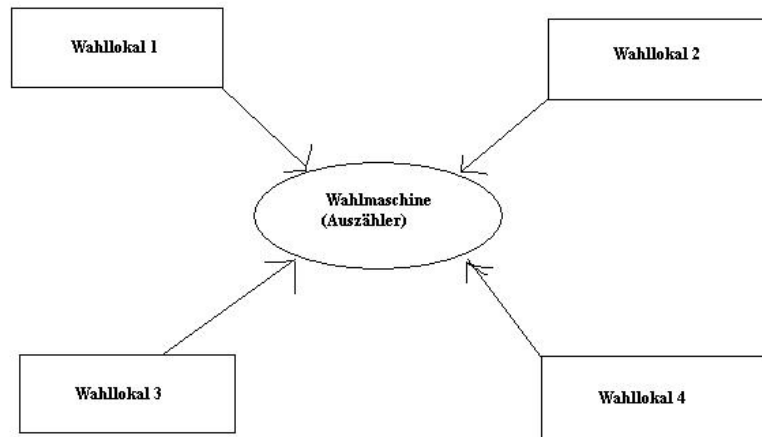


Abbildung 1: Präsenzwahl bei der Online-Wahl

- **Online-Wahl**
Man spricht von der Online-Wahl, sobald die Wahllokale untereinander elektronisch vernetzt sind und die abgegebenen Stimmen auf elektronischem Weg in die Urne gelangen. Die Online-Wahl wird als ein übergeordneter Begriff angesehen.
- **Internet-Wahl**
Die 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 ein offenes Netzwerk, das Internet oder ein geschlossenes Netzwerk, ein Intranet handelt. Ein Beispiel wäre dazu, dass innerhalb einer Firma über das Intranet Betriebsratswahlen stattfinden.

- Kiosk-Voting

Darunter versteht man, dass die Wahlgeräte außerhalb der Wahllokale an öffentlichen Orten stehen, wie z.B. öffentlichen Gebäuden oder Universitäten.

3.1.2 Distanzwahl

- Remote Internet Voting
- Home-Online-Voting
- I-Voting

Alle drei Begriffe sind untereinander und zum E-Voting synonym. Der Unterschied zur Präzenzwahl ist nur dieser, dass die Stimmabgabe über ein privates Eingabegerät (Wahlclient) erfolgt, wie z.B. der heimische Internetfähige Rechner, aber auch über beliebige andere Rechner, die nicht gerade für die Internetwahl aufgestellt wurden. Das hat zu Folge, dass der Wähler seine Stimme unabhängig vom Ort seines Wohnsitzes abgeben kann und eine Verlagerung der Stimmabgabe aus öffentlichen in private Räume stattfindet.

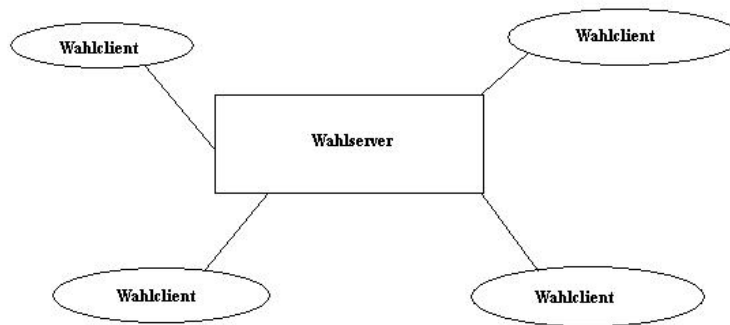


Abbildung 2: Distanzwahl

3.2 Anforderungen für eine Wahl

In der Einleitung sind 5 Anforderungen geschildert, die im Grundgesetz stehen. Im Kontext elektronische Wahlen 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 die gesetzlichen Anforderungen eingegangen, da sie für das Verständnis der Arbeit unverzichtbar sind und sich daraus die Sicherheitsanforderungen an Internetwahlen ableiten lassen [6].

3.2.1 Gesetzliche Anforderungen

- * Allgemein
Der Grundsatz der allgemeinen Wahl garantiert die Gleichheit beim Zugang der Wahl. Das Wahlverfahren muss ausfallsicher sein.
- * Unmittelbar
Dieser Punkt sagt aus, dass zwischen der Stimmabgabe und der Stimmenwertung keine weitere Instanz liegen darf, da sonst das Wahlergebnis beeinflusst werden könnte. Des Weiteren 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 die Beeinflussung durch Wahlpropaganda mittel Pop-ups¹ oder bezahlte Bannerwerbung² 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 bedingt, dass nur der Wähler seine Stimme kennen darf. Bei elektronischen Wahlen bedeutet dies, dass keine abgegebene Stimme zurückverfolgbar werden kann und jede dauerhaft geheim bleiben muss.

¹Kleines Feld, das auf einer besuchten Seite erscheint, um Informationen oder Werbung anzuzeigen.

²Bannerwerbung ist eine Werbeform im Internet. Die Werbung wird in die Webseite eingebunden.

3.2.2 Notwendige Sicherheitsanforderungen

Im folgenden werden die Sicherheitsanforderungen aus gesetzlichen abgeleitet und konkretisiert. Die Anforderungen werden jeweils der zugehörigen Punkte zugeordnet [4].

Wahlgeheimnis:

- * Das Wahlgeheimnis muss gewahrt werden. Niemand außer dem Wähler selber darf in Erfahrung bringen dürfen, was dieser gewählt hat.
- * Zuständige Mitarbeiter bzw. Administratoren dürfen nicht die Möglichkeit haben, die abgegebenen Stimmen zu sehen.

Korrektheit des Ergebnisses:

- * Das System darf keine Fehler hervorbringen und muss ein korrektes Ergebnis ermitteln. Alle Wahlberechtigten dürfen höchstens einen Stimmzettel abgeben.
- * Es muss sichergestellt werden, dass bei einem Systemausfall, die abgegebenen Stimmen bitgenau³ übernommen werden müssen, um somit nicht das Wahlergebnis zu verändern.
- * Der Wahl-Server könnte von dritten Personen als ein Ziel angesehen werden, um somit die Wahlergebnisse zu manipulieren. Somit müssen sämtliche Server der Wahlen einbruchsicher sein.
- * Die Ergebnisse müssten so berechnet werden, dass selbst ein durch die Hardware erzeugter Bitfehler das Ergebnis nicht beeinflussen kann.

Client - Rechnersicherheit:

- * Alle Anforderungen, die für das Onlinewahlssystem gelten, müssen auch für die Wahl-Clients gelten.
- * Es muss garantiert werden, dass die Software des Clients selbständig auf jedem beliebigen Rechner läuft und nicht andere Programme als Voraussetzung benötigt.

Verfügbarkeit:

- * Es muss sichergestellt werden, dass die Wahl an dem festgesetzten Tag durchzuführen ist. Deshalb muss das Wahlsysteme an

³Bit ist die kleinste Informationseinheit im Computer.

dem Tag der Wahl funktionsfähig und verfügbar sein.

- * Es muss gewährleistet werden, dass bei einem Systemausfall in einem der Wahllokale die Wähler sich in andere Wahllokale begeben können.

Transparenz:

- * Die Komponenten wie der Quell-Code⁴ der Online-Wahl und die eingesetzte Hardware muss der Öffentlichkeit bekannt gegeben werden, um Vertrauen für das Wahlsysteme zu gewinnen.

⁴Unter Quell-Code versteht man in einer Programmiersprache geschriebener Text, der durch ein Übersetzungsprogramm in eine ausführbare Form umgesetzt wird.

4 Lösungsansätze

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

4.1 Einfacher Ansatz

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 Wahlwirt) und das System, das die Stimmen zählt bzw. Auszähler (Wahlurne). Jeder Wähler erhält eine eindeutige ID⁵ und StZ (Stimmzettel). 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 der Stimmzettel weitergeleitet an den Auszähler. Nach der Wahl gibt der Auszähler die Ergebnisse bekannt [3]. (vgl. Abbildung 1)

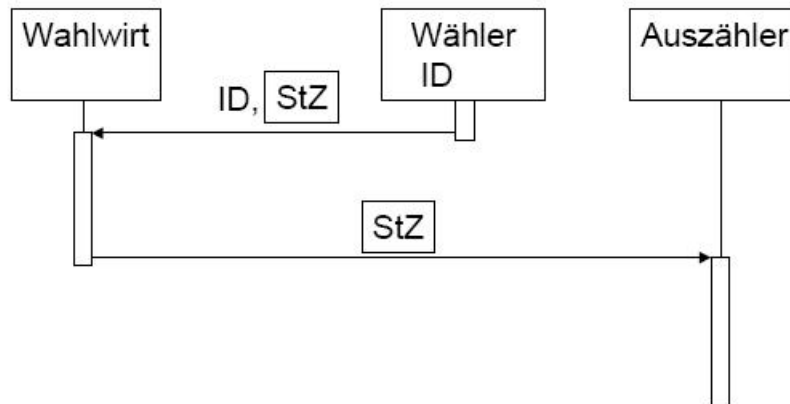


Abbildung 3: einfacher Ansatz [3]

Dieser Wahlvorgang zeigt Mängel, die dieses Verfahren unbrauchbar

⁵ID steht allgemein für eine Identifikationsbezeichnung oder Identifikationsnummer.

machen. Die Gründe sind:

- * Das Wahlgeheimnis wird gebrochen, da die Wahlhelfer herausbekommen können, 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.
- * Ein Wahlbetrug, sowohl von externe Angreifern als auch von Wahlhelfern, kann unbemerkt bleiben.

4.2 Einsatz von Kryptographie in E-Voting

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 [7].

Die Kryptographie wird unterteilt in symmetrische und asymmetrische 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 einem öffentlichen und einem privaten Schlüssel besteht, das zur Signierung und zur Verschlüsselung eines Dokuments dienen kann.

Da das symmetrische Verfahren keine Rolle spielt, wird nur auf die asymmetrische Kryptographie näher eingegangen.

4.2.1 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 seinen Stimmzettel und verschlüsselt seinen Stimmzettel mit dem öffentlichen Schlüssel und sendet seinen Stimmzettel mit seiner ID an das Wahllokal. Der Kontrolleur entschlüsselt die Nachricht und kann anhand der Signatur feststellen, dass der Stimmzettel tatsächlich vom Wähler mit der angegebenen ID stammt [3]. Falls dies zutrifft, wird die Stimme weitergeleitet an den Auszähler.

Mängel bei diesem Wahlverfahren:

- * Im System können Stimmzettel verändert, hinzugefügt oder auch verworfen werden.
- * Ein Wahlbetrugsversuch kann nur aufgedeckt werden, wenn die Software des Herstellers bekannt ist, da sonst die Softwarehersteller nach eigenem Ermessen die Wahl steuern könnten. Zudem müsste auch vermerkt werden, welche Personen auf die Datenbank zugegriffen haben.

- * Der Wähler selbst kann nicht überprüfen, ob sein eigener Stimmzettel gezählt worden ist.

4.2.2 Einsatz von digitaler Signatur

Bei dieser Durchführung werden drei Instanzen gebildet. Der Wähler, Kontrolleur und der Auszähler. Jede dieser Instanzen bekommt jeweils ein Schlüsselpaar (asymmetrische Verschlüsselung). Der Wähler vermerkt seine Stimme 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 geheimen Schlüssel verschlüsselt (diese Verschlüsselung dient dem Kontrolleur) und mit der ID des Wählers an den Kontrolleur gesendet. Um nochmals einen Schutz von Angreifer 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 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 [5]. (vgl. Abbildung 4)

Dieses Wahlverfahren zeigt auch Mängel, die auch dieses Verfahren unbrauchbar machen. Die Gründe sind:

- * Das 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 die Identität des Wählers ermittelt werden. Somit wäre das Wahlgeheimnis gebrochen.

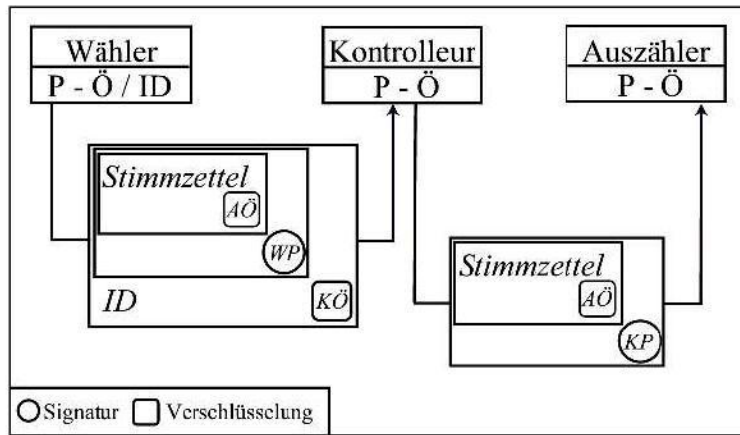


Abbildung 4: digitale Signatur [5]

4.2.3 Einsatz von blinder Signatur

Auf dieses Thema wird nicht näher eingegangen, da dieses Thema den Rahmen dieser Ausarbeitung sprengen würde.

5 Zusammenfassung

Abschließend lässt sich sagen, dass aufgrund der hohen Sicherheitsanforderungen und mit der jetzigen Technik das E-voting nicht umgesetzt werden kann. Außer den bereits genannten lassen sich die folgenden Probleme aufführen:

- * Es kann nicht nachgeprüft werden, ob auch die tatsächliche Software läuft, die vom Hersteller vorgegeben ist.
- * Ein weiteres Problem ist das Vertrauen der Menschen in die Wahlmaschinen. Die Menschen müssen Vertrauen in die Systeme haben, da die Wahl der Grundwert unserer Demokratie ist. [8]
- * Die Kosten sind bei den elektronischen Wahlen ein weiteres Thema. Die Hersteller von Wahlmaschinen vermeiden Aussagen, das E-Voting billiger sei. Die Kosten einer Wahl sind in den Niederlanden von 1,6 auf 2,7 Millionen Euro gestiegen [8].

Wenn in der Zukunft keine neue Techniken gefunden wird, die diese Probleme lösen, dann kann auch kein Einsatz von E-Voting stattfinden.

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.digitalechancen.de/content/stories/index.cfm/aus.2/key.2456/secid.16/secid2.49> Abgerufen am 15.11.06
- [2] Minh Pan, elektronische Evaluationsbogen Internet: <http://www.ks.uni-freiburg.de/download/studienarbeit/SS05/08-05-EEval-MPhan/ElektronEvaluation-MPhan.pdf> Version Januar 2006 - Studienarbeit Abgerufen am 17.11.06
- [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 Abgerufen am 15.11.06
- [4] Bernd Ziska, E-Voting Internet: <http://www.rechtsprobleme.at/doks/ziska-e-voting.pdf> Version Juni 2004 - Seminararbeit Abgerufen am 15.11.06
- [5] Iris Vojtech, Elektronische Wahlen Internet: <http://www.net.informatik.tu-muenchen.de/teaching/SS04/security/docs/9.pdf> Version Sommersemester 2004 - Seminararbeit Abgerufen am 17.11.06
- [6] Markus Ullmann, Frank Koob, Harald Kelter, Anonyme Online-Wahlen - Lösungsansätze für die Realisierung von Online - Wahlen Internet: http://mitglied.lycos.de/mac_o_mania/extdoc/OnlinewahlenDUD.pdf Version 1998 Abgerufen am 21.11.06
- [7] J.Heckel, D.Holzer,R.Kron, H.Ratzesberger, S.Strauss, A.Veitscheger, M.Weidhofer, M.Wiesinger E-Government in Österreich Internet : <http://www.swe.unilinz.ac.at/teaching/lva/ss04/projektstudium/prost246.556/Endbericht-E-Government-Linz.pdf> Projektarbeit - Sommersemester 2004 Abgerufen am 21.11.06
- [8] Richard Stietmann, *Die Nicht-Lösung eines nicht existierenden Problems*, Computer Technik, 30.10.06 (online Zeitschrift)