Ver- / Misstrauen Schaffende Maßnahme beim e-Voting

Melanie Volkamer[1], Robert Krimmer[2]

[1]Deduktion und Multiagentensysteme
Deutsches Forschungszentrum
für Künstliche Intelligenz
Stuhlsatzenhausweg 3
D-66123 Saarbrücken
volkamer@dfki.de

[2]E-Voting.CC
Kompetenzzentrum für Elektronische
Partizipation und Elektronische Wahlen
Liechtensteinstrasse 143/3
A-1090 Wien
r.krimmer@e-voting.cc

Abstract: Eine wichtige Voraussetzung für die Einführung von e-Voting und insbesondere von Online-Wahlen ist die Transparenz und das Vertrauen in das eingesetzte System. Durch die Verlagerung der Kontrolle vom Wahlvorstand zur Technik werden zusätzliche Verifikationsmöglichkeiten gefordert, damit sich der Wahlvorstand, die Wähler sowie die Kandidaten davon überzeugen können, dass die Wahl ordnungsgemäß abgelaufen ist. Dieser Beitrag zeigt, dass einige der Überprüfungstechniken zwingend eingesetzt werden müssen, andere sinnvoll sind aber wieder andere zu Misstrauen schaffenden Maßnahmen werden können und auch aus Benutzerfreundlichkeitsgründen indiskutabel sind.

1 Einleitung

e-Voting wird in Deutschland schon länger und intensiver diskutiert als in anderen Ländern. So können bereits seit 1999 elektronische Wahlgeräte zu Bundestags- und Europaratswahlen eingesetzt werden. Bei der Bundestagswahl 2005 waren immerhin 2100 der 80000 Wahllokale mit den Geräten ausgestattet. Erste Überlegungen zum Thema Online-Wahlen werden ebenfalls seit Ende der 90er Jahre angestellt. Die kürzlich durchgeführten Online-Wahlen der Gesellschaft für Informatik e.V., der Initiative D21 und der T-Systems zeigen, dass auch Online-Wahlen inzwischen nicht mehr nur theoretisch diskutiert werden sondern auch in der Praxis eingesetzt werden. Trotz der gesetzlichen Reglung für Wahlgeräte und den zahlreichen Online-Wahltests, wird e-Voting auf keiner Ebene und in keiner Form flächendeckend eingesetzt. Im Bereich von Wahlgeräten werden meist die enormen Kosten für die Anschaffung der Geräte genannt. Im Bereich von Online-Wahlen sind verschiedene Gründe zu nennen: Angefangen mit technischen Bedenken bis hin zu soziologischen Überlegungen und den fehlenden gesetzlichen Rahmenbedingungen.

Einen ganz wesentlichen Grund für die ausbleibende Einführung aus Sicht aller Beteiligten (Wähler, Wahlveranstalter und Kandidaten) ist sowohl für Wahlgeräten als auch für Online-Wahlen das *fehlende Vertrauen und die mangelnde Transparenz der e-Voting Systeme*: Ist meine Stimme wirklich gespeichert und wird sie richtig gezählt? Arbeitet die Auszählprozedur richtig? Kann jemand sehen wie ich gewählt habe? Kann der Hersteller oder der Wahlvorstand, das Ergebnis verändern?

Die Wichtigkeit der Nachvollziehbarkeit und Verifikationsmöglichkeiten aller Beteiligten spiegelt sich nicht nur in den aktuellen Diskussionen in den USA wieder sondern ganz aktuell auch in Hamburg im Zusammenhang mit dem digitalen Wahlstift. als neue Form des elektronischen Wahlgerätes. Der digitale Wahlstift bietet die Möglichkeit eines klar durch den Wähler verifizierbaren Papierbelegs. Geplant ist, dass die elektronische Stimme die ist die gezählt wird. Um Vertrauen in das System zu schaffen, ist dennoch geplant in einzelnen Wahllokalen die Papierstimmen auch auszuzählen und mit dem elektronischen Ergebnis zu vergleichen. Im Bereich von Online-Wahlen spiegelt sich diese Forderung nach Verifizierbarkeit in der Protokollarchitektur wieder. Beispielsweise schlagen [OMAFO99] und [Smi05] vor, dem Wähler die Möglichkeit zu geben, überprüfen zu können, ob seine Stimme auf dem so genannten Bulletin Board gespeichert ist.

An dieser Stelle setzt unser Beitrag an. Es wird untersucht, welche Möglichkeiten e-Voting bietet, um das Vertrauen der Wähler in das System zu stärken und die Transparenz zu erhöhen. Diese werden nach erforderlichen, sinnvollen und Misstrauen schaffende Maßnahmen klassifiziert. Dabei werden wir zwischen den klassischen Wahlgeräten im Wahllokal und Online-Wahlen unterscheiden. Ausgangspunkt der Betrachtung ist eine Analyse, der Verifikationsmöglichkeit der Beteiligten bei den traditionellen Wahlformen: Urnenwahl im Wahllokal und Briefwahl.

2 Vertrauen in traditionelle Wahlformen

In Deutschland unterscheidet man zwei traditionelle Papier-Wahlformen; Die Urnenwahl im Wahllokal und die Briefwahl, die als Ausnahmeregelung zugelassen ist. In den folgenden Unterkapitel betrachten wir die Mechanismen, die eingesetzt werden damit die beteiligten Gruppen (Wähler, Wahlvorstand und Kandidaten) Vertrauen in den korrekten Ablauf der Wahl und damit das Ergebnis haben – einmal bei der Urnenwahl und anschließend bei der Briefwahl.

2.1 Urnenwahl

Zunächst ist die Urnenwahl für alle Beteiligten nachvollziehbar und transparent. Dennoch hat der Wähler die Möglichkeit und auch das gesetzliche Recht [BWG02] zu Beginn des Wahltages zu überprüfen, ob die Urne auch wirklich leer ist. Der Wahlvorstand stellt sicher, dass der Wähler seine Stimme unbeobachtet abgeben kann und den anonym ausgefüllten Stimmzettel in die Urne werfen kann. Nach seiner Stimmabgabe kann er im Wahllokal anwesend bleiben, um sich davon zu überzeugen, dass niemand seine Stimme aus der Urne entfernt. Ebenfalls hat der Wähler das Recht der Auszählung der Stimmen im Wahllokal beizuwohnen und kann sich davon überzeugen, dass die Stimmen in seinem Wahllokal richtig ausgezählt werden. In der Praxis tut dies allerdings kaum ein Wähler, sondern die Wähler vertrauen dem Wahlvorstand. Wirklich verifizieren tut der Wähler nur, dass seine Stimme in der Urne gelandet ist. Dieses Vertrauen ist berechtigt, da der Wahlvorstand sich aus Personen unterschiedlichen Interessens (Parteien) zusammensetzt.

Diese kontrollieren sich gegenseitig. Darüber hinaus werden die Stimmen mindestens zweifach ausgezählt, um Fehler zu vermeiden. Durch diese Maßnahmen vertrauen auch die Kandidaten, in die Wahl. Neben diesem in der Informatik unter dem „Vier-Augen-Prinzip“ bekanntem Vertrauen schaffenden Mechanismus, bieten Papierstimmzettel die Möglichkeit sie jederzeit erneut auszuzählen, falls doch jemand Zweifel am Ergebnis haben sollte.

2.2 Briefwahl

Das Briefwahlverfahren ist nicht ganz so transparent für den Wähler, da zwischen dem Einwerfen in den Briefkasten und dem Auszählen beim Wahlvorstand *die Black-Box „Post“* liegt. Die Stimmen werden nicht anonym verschickt, sondern im Umschlag befinden sich neben der Stimme auch die Wählerdaten. Der Briefwähler vertraut daher der Post nicht nur, dass sie den Wahlbrief am Wahlamt abliefert sondern auch, dass sie ihn nicht öffnet. Hierbei beruft sich der Wähler auf das Briefgeheimnis und seine positiven Erfahrungen mit der Post im herkömmlichen Briefverkehr. Außerdem vertraut der Wähler darauf, dass der Wahlvorstand, die Wählerdaten vor dem Öffnen des Stimmumschlages ordnungsgemäß entfernt und auch alle Stimmen zählt. Das Vertrauen ist auch hier wieder auf die gegenseitige Kontrolle des Wahlvorstandes gestützt. Allerdings ist zu beachten, dass der Wähler bei der Briefwahl - im Gegensatz zur Wahl im Wahllokal - dem Wahlvorstand zusätzlich bzgl. der Einhaltung des Wahlgeheimnisses vertrauen muss. Für die Kandidaten ändert sich in Bezug auf das Vertrauen nichts im Vergleich zur Urnenwahl im Wahllokal, da ihr Hauptinteresse in der korrekten Auszählung liegt. Die Nachzählung ist auch bei der Briefwahl möglich, aber bzgl. denkbarer Angriffe auf dem Postweg sowie bzgl. des Wahlgeheimnisses im Wahllokal wenig aussagekräftig.

3 Vertrauen bei e-Voting Systemen

Analog zur Unterteilung in Nah—und Fernwahl bei traditionellen Wahlen, werden wir nun zunächst die Wahlgeräte und anschließend Online-Wahlen in Bezug auf Vertrauensaspekte untersuchen. Im Falle von e-Voting kommt eine neue Gruppe ins Spiel: der Hersteller

3.1 Wahlgeräte

Die Wahlgeräte der Firma Nedap, wie sie in Deutschland eingesetzt werden, zeichnen sich dadurch aus, dass sie nur zur Stimmabgabe dienen und dem Wähler keinen Papierbeleg anbieten. Der Wahlvorstand schaltet das Gerät frei, der Wähler kann anschließend seine Stimme abgeben. Diese wird an einer zufälligen Speicherstelle abgelegt und die Speicherung erfolgt redundant in vier verschieden Speichermodulen. Die erfolgreiche Speicherung wird dem Wähler signalisiert und das Gerät gesperrt. Am Ende des Wahltages aktiviert der Wahlvorstand die Auszählung und kann das Ergebnis dann ausdrucken.

Die Stimmenspeicher werden zu einem späteren Zeitpunkt an einer zentralen Stelle erneut ausgezählt. Jeweils ein Muster einer Bauart ist von der Physikalisch Technischen Bundesanstalt (PTB) geprüft und vom Bundesministerium des Inneren nach der Wahlgeräteverordnung [BW99] zugelassen worden.

Nach einer Prüfung durch die PTB können wir sicher sein, dass die geprüfte Bauart korrekt funktioniert. Nun müssen alle Beteiligten darauf Vertrauen, dass die eingesetzten Wahlgeräte die gleiche Bauart haben, wie das geprüfte Muster-Gerät. An dieser Stelle kann das Vertrauen erhöht werden, indem ein Siegel dem Wähler erkennen lässt, dass das Gerät nicht manipuliert wurde. Dieses Siegel muss insbesondere so angebracht sein, dass Manipulationen am Gerät nur durch Beschädigung des Siegels möglich werden. Außerdem muss der Wähler in der Lage sein, sich von der Unversehrtheit des Siegels zu überzeugen. Derzeit bleiben zwei mögliche Angriffe: Entweder der Hersteller liefert absichtlich falsche Geräte aus oder es geling einer Dritten Partei falsche Wahlgeräte mit dem richtigen Siegel in Umlauf zu bringen. Durch einen solchen Angriff kann das Wahlergebnis unbemerkt manipuliert werden oder eine Möglichkeit zum Abrufen von Zwischenergebnissen über eine externe Schnittstelle (z.B. Bluetooth) eingerichtet werden. Um zusätzlich das Wahlgeheimnis zu brechen, müssten die Wahlhelfer notieren, in welcher Reihenfolge die Wähler ihre Stimme abgegeben haben, da das Gerät selber keine Wählerinformationen kennt. An dieser Stelle ist wirklich Vertrauen gefragt, denn jegliche äußere Überprüfung ohne das Gerät zu öffnen kann der „Angreifer“ mit manipuliert haben.

3.2 Online-Wahlen

Online-Wahlen zählen genau wie die Briefwahl zur Distanzwahl. Die Stimmen werden statt auf dem Postweg über das Internet zu einem zentralen Server transportiert. Ein vereinfachtes Verfahren (vgl. [Epp04]), dass die Briefwahl abbildet, könnte aus folgenden zwei Nachrichten bestehen:

(1) Wähler → Wahlserver : $\boldsymbol{sig}_{\text{Wähler}}(\boldsymbol{ver}_{\text{Wahlserver}}(\text{ Stimme }))$

(2) Wahlserver → Wähler: $\boldsymbol{sig}_{\text{Wahlserver}}$(„Nachricht erhalten“)

Die Stimme wird zunächst verschlüsselt (entspricht dem Einpacken des Papierstimmzettels bei der Briefwahl in den inneren Umschlag) und dann vom Wähler signiert (entspricht der Unterschrift und dem Einpacken in den Äußeren Umschlag). Diese Nachricht wird dann an den Wahlserver geschickt, der die Stimme speichert und den Erhalt dem Wähler bestätigt. Am Ende der Wahl wird der Wahlserver vom Netz getrennt und die Auszählprozedur wird gestartet. Dabei wird analog zur Briefwahl zunächst anhand der Signatur überprüft, ob der Sender der Stimme wahlberechtigt ist. Ist dies der Fall wird die Signatur entfernt und die verschlüsselte Stimme an einem separaten Speicherplatz aufbewahrt. In einen zweiten Schritt werden dann die anonymen Stimmen ausgezählt. Die Sicherung des Wahlgeheimnisses am Wahlserver erfolgt damit analog zur Briefwahl. Der Unterschied liegt in der Übertragung.

Die Post kann nach Auslieferung eines Wahlbriefes das Wahlgeheimnis nicht mehr brechen, was ein Angreifer, der die Nachricht auf dem Internet mitliest und kopiert, diese entschlüsseln kann, wenn er die entsprechenden Schlüssel kennt.

Die Online-Wahl bietet im Vergleich zur Briefwahl aber die Möglichkeit, den Eingang der Stimme zu bestätigen (siehe auch [KrVo05]). Die Rückmeldung darf aber wegen der Sicherung des Wahlgeheimnisses nicht den Inhalt der Stimme bestätigen sondern nur die Tatsache, dass eine Stimme angekommen und gespeichert wurde. Dies ist im Wesentlich als Vertrauen schaffende Maßnahme zu sehen. Denn genau genommen sagt der Erhalt einer solchen Rückmeldung nichts aus, da sowohl ein entsprechend manipulierter Rechner als auch ein Angreifer auf dem Netz die Nachricht erzeugt haben kann.

Wie sieht es nun mit dem Vertrauen des Wählers aus? Nehmen wir an, dass das Online-Wahlsystem analog zu den Wahlgeräten geprüft wurde. Damit muss der Wähler analog zu den Wahlgeräten darauf vertrauen, dass auch genau dieses System eingesetzt wird. Außerdem muss er darauf vertrauen, dass die Entschlüsselungsschlüssel entsprechend geheim gehalten werden, da sonst das Wahlgeheimnis nicht mehr sicher ist. Eine Vertrauen schaffende Überprüfungsmöglichkeit kann hier analog zu den Wahlgeräten in Form von Serverzertifikaten angeboten werden. Die Überprüfung solcher „Siegel“ erfordert allerdings ein größeres Fachwissen vom Wähler, verglichen mit den Siegeln am Wahlgerät in der Kabine. Die Hauptunterschiede zum Wahlgerät liegen zum einen darin, dass das Online-Wahlsystem auf einem Server betrieben wird, der über das Internet eine breitere Angriffsfläche bietet als die Wahlgeräte im Wahllokal und zum anderen dass die Endgeräte beim Wähler (sein PC) zu vielfältig sind, als das man sie in die Prüfung des Systems einbeziehen könnte. Daher muss der Wähler entweder darin vertrauen, dass sein eigenes Endgerät nicht manipuliert ist oder aktiv etwas dafür tun, dass eine entsprechende Sicherheit gegeben ist.

4 Erforderliche Maßnahmen

Die Wichtigkeit einer externen Prüfung ist in Deutschland bereits erkannt worden. Die Vorgehensweise für die Prüfung von Wahlgeräten ist gut durchdacht und inzwischen auch durch viel Erfahrung geprägt. Die Ansätze gehen allerdings von einer eher elektronischen und keiner reinen Softwarelösung aus und konzentrieren sich auf die funktionale Korrektheit. Die Vorgehensweise muss für Softwarelösungen wie etwa im Falle einer Onlinewahl in einigen Punkten erweitert werden. Daher sind hier zwei unterschiedliche Prüfungen durchzuführen: Einmal auf der funktionalen Ebene und in diesem Zusammenhang vor allem ein Sourcecodereview der Auszählfunktion und zum anderen eine Prüfung und Zertifizierung nach den Common Criteria CC for Information Technology Security Evaluation. Da die „Wahlgeräte“ in Form von Wahlservern am Internet angeschlossen sind, muss insbesondere die Resistenz des Wahlservers gegen Angriffe aus dem Internet untersucht werden. Bisher sind Online-Wahlsysteme in Deutschland noch keiner offiziellen Prüfung und Zertifizierung unterzogen worden, dies soll sich aber ändern. Um die sehr aufwendige und kostspielige Überprüfung zu vereinfachen wird derzeit ein entsprechendes Schutzprofil entwickelt.

Ziel beider Prüfungen ist es auszuschließen, dass der Hersteller unabsichtliche Fehler im System hat bzw. auf Ansätzen aufbaut, die Schwachstellen verursachen. Teil der Zertifizierung nach CC ist die Auslieferung, sprich der Hersteller muss angeben, wie er sicherstellt, dass das authentische und integere Online-Wahlsystem eingesetzt wird.

e-Voting System müssen wichtige Events mit protokollieren. Hierzu zählen das Starten des Systems und das Beenden, sowie auftretende Fehler oder Neustarts. Die Protokollierung muss dabei so geschehen, dass nach Wahlende der Wahlvorstand entscheiden kann, ob die Wahl gültig ist oder nicht. Zu den Überprüfungen zählt unter anderem ein Abgleich zwischen Anzahl der Wähler im Wählerverzeichnis und Anzahl der abgegeben Stimmen.

Unabhängig von der eingesetzten Technik, kann Vertrauen in ein e-Voting System nur dann geschaffen werden, wenn die Wähler früh über die neue Technik informiert werde, u.a. auch durch einen Testlauf.

5 Missbildende Maßnahmen

Seit den Präsidentschaftswahlen von 2000 sind Wahlgeräte in den US heiß diskutiert. Insbesondere werden Voter Verfied Audit Trail also Papierbelege für den Wähler gefordert. Wahlgeräte mit dieser Funktionalität sind auch teilweise schon im Einsatz, wie z.B. in Brasilien und auch in Deutschland geht der digitale Wahlstift in diese Richtung. Warum Papierbelege? In den USA mag das in sofern Sinn machen, da dort die eingesetzten Wahlgeräte keiner Prüfung wie in Deutschland unterzogen werden. Falls eine angemessene Prüfung durchgeführt wurde, bringt diese Maßnahme aus sicherheitstechnischer Sicht keinen Gewinn. Sondern dient maximal dazu das Vertrauen des Wählers zu erhöhen. Tut es das wirklich?

Wir betrachten zwei unterschiedliche Typen von Wählern. Nehmen wir zunächst den Wähler, der der Technik eh kritisch gegenübersteht und nicht glaubt, dass das e-Voting System funktioniert. Für einen solchen Wähler ist ein Papierbeleg ein Einladung, durch eine falsche Aussage mistrauen zu verbreiten: Er behauptet fälschlicherweise, der Ausdruck stimme nicht mit dem Überein was er gewählt hat. Und nun? Der Wahlvorstand hat auch keine Möglichkeit seine Aussage zu widerlegen. Die andere Kategorie Wähler sind die, die den Nachweis dankend annehmen und damit dem System vertrauen, aber was sagt der Beleg aus? Wenn jemand das Gerät wirklich manipulieren möchte, dann druckt er den Wählerwillen aus, speichert aber eine andere Stimme. Dies würde nur auffallen, wenn die Papierbelege ausgezählt würden, aber das widerspricht ja dem Einsatz von e-Voting, zwecks Zeit- und Kostenersparnis. Aus unserer Sicht ist ein solcher Papierbeleg bei geprüften Wahlgeräten daher eher als Misstrauen schaffende Maßnahme anzusehen.

Als weiter Möglichkeit Vertrauen zu schaffen könnte daran gedacht werden, dass alle elektronischen Stimmzettel später veröffentlicht werden und zum einen jeder selbst das Ergebnis berechnen kann, bzw. sich eine entsprechende Prozedur schreiben kann und zum anderen der Wähler anhand der veröffentlichten Stimmen überprüfen kann, ob seine Stimme dabei ist. Ersteres ist sicherlich eine vertrauensbildende Maßnahme, von der in der Praxis allerdings nicht Gebrauch gemacht werden würde, da der Aufwand zur eigenständigen Nachzählung zu groß ist. Außerdem wer versichert, dass die veröffentlichten Stimmen, die sind, die auch wirklich abgegeben wurden? Der zweite Ansatz ist bzgl. der Anonymität kritisch. Der Wähler müsste eine art Beleg mit aus dem Wahllokal nehmen können, um später überprüfen zu können ob seine Stimme gezählt wurde. Dies funktioniert aber nicht, ohne das Wahlgeheimnis zu brechen. Es wären an dieser Stelle zwar Ansätze auf der Basis von Zero-Knowledge Proofs (ZKP) einsetzbar, aber hier wäre für den Wähler nicht mehr transparent, ob seine Stimme wirklich gezählt wurde, da er die komplexen Verfahren nicht verstehen kann. Darüber hinaus müsste der Wähler der Implementierung des ZKP vertrauen. Damit kann der Wähler auch nach einem positiven ZKP nicht sicher sein, dass seine Stimme auch wirklich korrekt gezählt wurde und analog zu dem Beleg im Wahllokal könnte der Wähler auch diesen nutzen, um mit einer Falschaussage, die nicht widerlegt werden kann, mistrauen zu schaffen.

Allgemein sind alle Maßnahmen, die man dem Wähler oder dem Wahlvorstand zur Verifikation anbieten kann zu untergraben und damit nicht wirklich aussagekräftig. Ganz im Gegenteil, sie können dazu verwendet werden, Misstrauen in das System zu erwecken. Es sollte außerdem beachtet werden, dass kein e-Voting System 100%ige Sicherheit bietet, genau wie die traditionellen Systeme auch nicht und man darüber hinaus sich bewusst sein muss, dass man nie zweigen kann, dass e-Voting korrekt funktioniert, man kann ggf. nur das Gegenteil zeigen (Popper – Falsifizierung).

Bei einem Online-Wahlsystem sind die Probleme ähnlich. Hier kommt noch dazu, dass eine spätere Überprüfung nur dann Möglich ist, wenn entsprechende Daten / Zwischenergebnisse geheim und integer beim Wähler gespeichert werden können. Darüber hinaus dürfen diese nicht dazu verwendet werden können, die Wahlentscheidung zu beweisen. Neben den obigen Problemen sollte man bei dem Einsatz von Verifikationsmechanismen auch beachten, dass diese mit einem Mehraufwand für den Wähler verbunden sind Er muss sich zum späteren Zeitpunkt wieder an dem System anmelden, um die Überprüfung vorzunehmen.

6 Zusammenfassung

In der Literatur wurden sowohl für Wahlgeräte als auch für Online-Wahlen verschiedene Verifikationsmechanismen vorgeschlagen. In Deutschland ist der aktuelle Stand der, dass man sich auf die Prüfung verlässt und dann darin vertraut, dass auch wirklich die geprüften Geräte zum Einsatz kommen. Damit reduziert sich der Aufwand für den Wähler auf ein Minimum. Er muss im Wesentlichen nur das Siegel überprüfen. Allerdings gibt es Stimmen, die prinzipiell in der Nutzung von Wahlgeräten eine Verletzung der öffentlichen Auszählung sehen.

Die Erfahrungen, die man bei Wahlgeräten über die Jahre gesammelt hat stehen bei Online-Wahlen noch aus. Eine offizielle Prüfung eines der Systeme steht ebenfalls noch aus. Außerdem sind die Angriffsflächen für eine Manipulation hier größer und die Transparenz weniger gegeben, da teilweise komplizierte kryptographische Verfahren eingesetzt werden. Wir haben gezeigt, dass diesem nicht mit den vorgeschlagenen Verifikationsmaßnahmen begegnet werden kann, sondern diese eher Mistrauen bildenden Charakter haben. Daher ist es wichtig, Online-Wahlen schrittweise einzuführen. Nur so kann das Vertrauen bei allen Beteiligten langfristig aufgebaut werden und auch die ältere Generation für die Wahlreform gewonnen werden.

Literaturverzeichnis

[BW99] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, 1975. BGBl I 1975, 2459, Zuletzt geändert durch Art. 1 V v. 20. 4.1999 I 749;

[BWG02] Bundeswahlgesetz (BWG) – In der Fassung der Bekanntmachung vom 23. Juli 1993. BGBl. I S. 1288, 1594. Zuletzt geändert durch Artikel 1 des Gesetzes vom 7. Mai 2002 (BGBl. I S. 1529, 2964);

[Epp04] Maaten, E.: Towards Remote E-Voting: Estonian case. In: Prosser, A., Krimmer, R.: Electronic Voting in Europe. 2004, S. 83-100.

[KrVo05] R. Krimmer, M. Volkamer: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In EGOV (Workshops and Posters), 2005.

[Oh99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto: An Improvement on a Practical Secret Voting Scheme, ISW'99, S. 225-234, 1999.

[Smi05] W. D. Smith: New cryptographic voting scheme with best-known theoretical properties, Frontiers in Electronic Elections FEE 2005, Milan Italy, 2005.