DuD
Datenschutz und Datensicherheit

Online-Wahlen für Gremien

Wahlen in Gremien als Einsatzgebiet für Wahlen ohne vertrauenswürdige Instanz

Ammar Alkassar, Robert Krimmer, Melanie Volkamer

Anspruchsvolle Wahlprotokolle, die ohne vertrauenswürdige Wahlzentrale auskommen, galten lange Zeit als nicht praxistauglich.[1] Im vorliegenden Beitrag stellen die Autoren das Projekt „E-Voting for Academics“ vor, mit dem sie zeigen möchten, dass diese komplexen Systeme in bestimmten Anwendungsfeldern umsetzbar sind.

Dipl.-Inform. Ammar Alkassar

Vorstandsvorsitzender der Sirrix AG security technologies, Kommunikationssicherheit und Multi-Level Security

E-Mail: alkassar@sirrix.de

Mag. Robert Krimmer

Wirtschaftsuniversität Wien, E-Government (insbesondere E-Democracy und E-Voting)

E-Mail: krimmer@wu-wien.ac.at

Dipl.–Inform. Melanie Volkamer

Wissenschaftliche Mitarbeiterin am Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI), E-Voting, Sicherheit in verteilten Netzen.

E-Mail: volkamer@dfki.de

Einleitung

Elektronische Wahlen sind heute in vielen Bereichen mehr denn je in der Diskussion. Neben der erhofften höheren Partizipation, ist vor allem die Erleichterung der Wahlorganisation ein wichtiges Argument, welches auch im 19. Jahrhundert zur Anwendung des ersten elektronischen Wahlapparates in Deutschland führte. Werner von Siemens stellte 1860 mit seinem Abstimmungstelegraphen das automatische Abstimmungssystem für das preußische Abgeordnetenhaus vor [Siem1891]. Etwas mehr als 100 Jahre später ist in Deutschland seit 1975 die Durchführung elektronischer Urnenwahlen bei Bundestagswahlen, mit der Hilfe nichtvernetzter elektronischer Wahlgeräte in Wahllokalen, durch die Bundeswahlgeräteverordnung [BWahlG] geregelt.

Wesentlich komplexer als der Einsatz von Wahlmaschinen im Wahllokal stellt sich die elektronische Variante der Briefwahl, die Online-Wahl dar, d.h. die elektronische Wahl, die über öffentliche Netze durchgeführt wird. Sichere Online-Wahlen wurden erst durch neue kryptographische Verfahren wie beispielsweise die blinden Signaturen [Chau85] oder die Idee der MIXE [Chau81] Anfang der 80er Jahre möglich.

Die breite Öffentlichkeit interessiert sich seit dem Einzug des Internet in die Büros und die Verwaltungen Ende der neunziger Jahre zunehmend für das Thema Online-Wahlen, für die damit erstmals auch die technische Infrastruktur bereitstand. Der anfängliche Enthusiasmus führte dazu, dass weltweit zahlreiche Projekte ins Leben gerufen wurden, deren Ziel es war, zu zeigen, dass Online-Wahlen auch für den Praxiseinsatz geeignet sind. Dabei kamen bei den entwickelten Systemen eine Vielzahl der in den Jahren zuvor veröffentlichten kryptographischen Protokolle und Konzepte zum Einsatz [Ullm01].

Deutschland erreichte dabei mit Projekten wie i-vote der Forschungsgruppe Internetwahlen [i-vote], dem Projekt „Elektronische Stimmabgabe im Internet“ [ESI] und der Wahl zum Jugendgemeinderat Fellbach [Fell01] eine besondere Vorreiterrolle. Dabei kamen sowohl Online-Wahlsysteme zum Einsatz, die als festinstallierte Kiosksysteme im Wahllokal oder als Remote-Systeme von beliebigen internetfähigen Rechnern betrieben wurden.

Nach dem ersten großen Boom der Online-Wahlen und den eher ernüchternden Ergebnissen, verlor das Thema in Deutschland insbesondere in der Politik an Interesse.

Im Gegensatz zu Deutschland setzen eine Reihe von europäischen Ländern Online-Wahlen bereits auf politischer Ebene rechtsverbindlich ein, wie beispielsweise die Schweiz [Brau03] und England [Prat04] oder Estland (für die nächsten Wahlen geplant, [Maat04]).

In Deutschland orientiert man sich zunehmend an dem Konzept des stufenweisen Erfahrungsaufbaus [Karg03] und konzentriert sich auf den nicht-parlamentarischen Bereich. Insbesondere der Bereich von Vereinswahlen erscheint dabei attraktiv. So hat beispielsweise die D21 ihre Vorstandswahl 2003 [D21-2002] und die Gesellschaft für Informatik 2004 ihre Präsidiumswahlen mit 20.395 Wahlberechtigten erfolgreich online durchgeführt. Die GI plant auch in diesem Jahr die Vorstands- sowie die Präsidiumswahlen in Form einer Kombination aus Brief- und Onlinewahl anzubieten [GI-WAHL]. Die Vereine Digitale Brücken e.V. und Digital Bridges e.V. führten 2004 ihre Vorstandsbeschlüsse zur Fusion der beiden Vereine und der diesbezüglichen Details in einem Pilotprojekt über handelsübliche Handys durch [Maus04].

[1] Eine Übersicht der verschiedenen Realisierungsansätze findet sich in [Ullm01].

Neben Vereinswahlen gibt es einen interessanten Einsatzbereich, der bisher aber weitestgehend unberücksichtigt blieb: der Einsatz von Wahl- und Abstimmungssystemen innerhalb von Gremien und Vorständen. Genau an dieser Stelle setzt das Projekt „E-Voting for Academics“ an, das wir in diesem Beitrag vorstellen.

1 Motivation

Ein interessantes Anwendungsfeld sind Wahlen und Abstimmungen im universitären Umfeld. Dabei sind sowohl die Wahlen zu den studentischen Selbstverwaltungsorganen wie dem Studierendenparlament als auch Wahlen zu und vor allem in den universitären Gremien wie dem Senat oder den Fakultätsräten als Evaluationsfeld für Online-Wahlen von besonderem Interesse.

So können in der studentischen Selbstverwaltung die maßgeblichen Ordnungen mit relativ geringem Aufwand angepasst werden. Generell zeichnen sich viele Wahlen und Abstimmungen im universitären Umfeld oftmals durch komplexe Wahlverfahren mit einem hohen personellen Aufwand in der Durchführung aus.

Vereinfacht wird der Einsatz von Online-Wahlen in diesem Umfeld durch die gut ausgebaute Netzinfrastruktur. Erleichtert wird der Einsatz von Internetwahlen darüber hinaus durch die allgemeine Verfügbarkeit vernetzter Rechner bei allen Beteiligten. Dies ermöglicht den Einsatz von weitaus komplexeren Wahlprotokollen.

Die Einführung von Internetabstimmungen/-wahlen bei Universitätsgremien hat auch einen funktionalen Mehrwert: Viele der Entscheidungen, die oftmals in der Eilkompetenz des Vorsitzenden getroffen werden, können mit einem solchen System ohne große Vorlaufzeit für die Gremiensitzungen regulär getroffen werden. Dies ist aus der Sicht der universitären Selbstverwaltungsorgane ein signifikanter Vorteil, da Eilentscheidungen durchaus problematisch sein können.

Weitere interessante Anwendungsfelder ergeben sich beispielsweise bei Abstimmungen innerhalb von Unternehmens-, Partei- und Vereins-Vorständen. Insbesondere bei überregionalen organisierten Verbänden und Unternehmen können Online-Abstimmungen Entscheidungsprozesse erheblich vereinfachen.

2 Wahlprotokolle ohne vertrauenswürdige Instanz

Seit Anfang der 80er Jahre wurden zahlreiche Wahlprotokolle veröffentlicht und teilweise in Wahlsystemen umgesetzt (einen guten Überblick über die unterschiedlichen Protokolle bietet [SMITH05]). Einige der publizierten Wahlprotokolle (z.B. [BeYu86] und [DM83]) wurden in der Vergangenheit aber für den praktischen Einsatz kaum beachtet, obwohl sie über interessante Sicherheitseigenschaften verfügen.

> Diese Protokolle arbeiten ohne zentrale Wahlserver und ermöglichen damit ein weit sichereres Vertrauensmodell. Protokolle, die mit einem oder mehreren zentralen Wahlservern arbeiten, haben den Nachteil, dass die Wähler diesen Servern nahezu uneingeschränkt vertrauen müssen. Die gezielte Manipulation eines dieser Server kann ausreichen, das Wahlergebnis unbemerkt zu verändern.

Wahlprotokolle ohne zentrale Wahlserver verwenden meist Secret Sharing Verfahren oder beruhen auf dem Prinzip des zufälligen Verwürfelns bzw. Vermischens der Stimmen, wobei die Wahlsoftware als eine Art MIX [CHAU81] fungiert. Die Protokolle sind derart gestaltet, dass (a) jede Wählerin/jede Wählersoftware das Ergebnis selbst berechnet und somit keiner zentralen Stelle vertrauen muss, (b) diese das Ergebnis korrekt berechnet und (c) korrekt veröffentlicht. Außerdem kann jeder Wähler bei diesen Protokollen selbstständig sicherstellen, dass sein Stimmgeheimnis gewahrt bleibt, unabhängig von dem Verhalten eines oder mehrere Server und unabhängig vom Verhalten der anderen Wähler beim Protokolldurchlauf.

Der Nachteil dieser Protokolle liegt im Nachrichtenaufkommen, welches mit der Anzahl der Wähler quadratisch zunimmt. Diese Ineffizienz bei großen Wählergruppen führte dazu, dass diese Protokolle für den praktischen Einsatz nie ernsthaft in Betracht gezogen wurden.

Im Projekt „E-Voting for Academics“ zeigen wir, dass Wahlprotokolle ohne zentrale Wahlserver für kleine Wählergruppen durchaus sinnvoll einsetzbar sind und realisieren ein entsprechendes System. Die Software „eVote“ ist ein Wahlsystem für Universitätsgremien, wie Forschungsausschuss, Fakultätsräte oder den Senat. Diese Gremien haben üblicherweise eine überschaubare Anzahl an Mitgliedern (meist zwischen 10 und 30), die an eine Infrastruktur wie etwa das Universitätsnetz angeschlossen sind, die das hohe Nachrichtenaufkommen vertretbar macht.

3 *eVote* Systembeschreibung

Das in *eVote* umgesetzte Protokoll ist eine Erweiterung des bereits in [DM83] veröffentlichten Ansatzes von Michael Merritt und beruht auf dem Prinzip des Mischens der Stimmen. Jeder Wähler erhält nach seiner eigenen Stimmabgabe nacheinander zweimal alle Stimmen in verschlüsselter Form und durchmischt diese zufällig. Nach Protokollabschluss verfügt jeder Wähler über alle Stimmen im Klartext und kann das Ergebnis selbst berechnen.

3.1 Voraussetzungen

Dabei wird vorausgesetzt, dass jeder Wähler über ein eigenes Schlüsselpaar verfügt und die integeren öffentlichen Schlüssel der anderen Gremienmitglieder kennt. Dies ist bei kleinen Wählergruppen aber keine Hürde, da eine PKI in dem Sinne nicht erforderlich ist. Der mit *eVote* erzeugte Schlüssel kann problemlos offline ausgetauscht werden.

Angenommen wird außerdem – wie bei allen anderen Wahlsystemen auch – dass die zur Wahl eingesetzten Rechner sicher sind, also insbesondere keine Malware die abgegebene Stimme vor dem Verschicken verändert und auch keine Information über den Inhalt einer Stimme verbreiten kann.

Wir gehen von einem aktiven Angreifer aus, der das Netzwerk vollständig kontrolliert, der aber kryptographisch beschränkt ist. Zu den Angreiferzielen zählen die Offenlegung des Stimmgeheimnisses sowie die Manipulation des Wahlergebnisses.

3.2 Protokoll

Insgesamt umfasst das Protokoll fünf Runden, die im Folgenden erläutert werden:

- **Verschicken der Wahlberechtigung:** Der Vorsitzende und damit Initiator W_i der Wahl verschickt die Wahlbenachrichtigung an alle *n* Wähler, Die Wahlbenachrichtigung enthält neben den eigentlichen Stimmzettel auch die Wählerliste, wobei die Reihenfolge der Wähler in

dieser Liste ($W_1, W_2, \ldots, W_n$) eine entscheidende Rolle für das weitere Protokoll spielt.

- **Generierrunde:** Die Generierrunde beginnt mit der Stimmabgabe des einzelnen Wählers. Die Stimme wird mehrfach verschlüsselt und an Wähler W_1 zur Weiterverarbeitung verschickt. Im Einzelnen wird die Stimme nacheinander zweimal mit dem öffentlichen Schlüssel jedes Wählers aus der Wählerliste verschlüsselt, beginnend mit dem öffentlichen Schlüssel von W_n. Dabei wird nur für die äußeren Verschlüsselungen ein semantisch sicherer Verschlüsselungsalgorithmus eingesetzt und für die innere ein deterministisches Verfahren, da für spätere Überprüfungen die einzelnen Zwischenschritte nachvollzogen werden müssen.
- **Vertauschen-Runde:** In dieser für die Geheimhaltung der Wählerstimme entscheidenden Runde erhält jeder Wähler W_i in der entsprechenden Reihenfolge alle verschlüsselten Stimmen und geht folgendermaßen vor: Zunächst überprüft er anhand der gespeicherten Zwischenergebnisse, ob seine eigene Stimme in der Liste enthalten ist, dann entfernt er eine Verschlüsselung, durchmischt die immer noch verschlüsselten Stimmen zufällig und schickt den so entstandenen Datensatz an seinen Nachfolger W_{i+1} weiter. Am Ende der Runde erhält jeder von Wähler W_n eine Liste von Stimmen, die jetzt nur noch einmal mit jedem Wähler-Schlüssel verschlüsselt sind. Jeder Wähler überprüft, ob seine Stimme dabei ist und schickt ggf. eine Bestätigungsnachricht an den Wähler W_1.
- **Konsistenzprüfung:** Mit dem Erhalt aller Bestätigungsnachrichten beginnt W_1 die nächste Runde. Nacheinander erhält wieder jeder die Liste mit den verschlüsselten Stimmen, um eine Verschlüsselungschicht zu entfernen. Dies wird solange fortgesetzt bis die Stimmen beim Wähler W_n im Klartext vorliegen. Im Unterschied zur vorherigen Runde werden die Stimmen nicht durchmischt und die Liste wird nicht nur an den Nachfolger, sondern an alle Wähler geschickt. Außerdem entfernt der Wähler die entsprechende Verschlüsselungsschicht erst dann, wenn alle Wähler bestätigt haben, dass die erhaltene Liste konsistent zur vorherigen ist und damit alle Stimmen enthalten sind.
- **Auszählen:** Nachdem W_n alle Stimmen im Klartext hat, schickt er sie an alle Wähler, die nach einem Konsistenzcheck zur vorherigen Runde die Stimmen auszählen.

Eine detaillierte Beschreibung des Protokolls ist in [eVote] zu finden. Hier steht auch der Prototyp zum Download bereit. Im Gegensatz zu anderen verfügbaren Wahlsystemen kann jedes Gremium *eVote* ohne die Hilfe eines Providers kostenlos einsetzen, da der Initiator der Wahl das Wählerverzeichnis sowie den Inhalt des Stimmzettels selbstständig generieren kann. Das System kann auch eingesetzt werden, um mehrere Wahlen parallel durchzuführen.

4 Sicherheitsanalyse

Anforderungen an Wahlen in Deutschland werden im Wesentlichen von den fünf Wahlrechtsgrundsätzen (freie, allgemeine, geheime, unmittelbare, gleiche Wahl) abgeleitet. Diese sind im Grundgesetz verankert. Die *unmittelbare* Wahl fordert, dass keine Wahlmittelmänner gewählt werden, die dann über das eigentliche Wahlergebnis abstimmen. Aus diesem Wahlrechtsgrundsatz lassen sich keine spezifischen Anforderungen an ein Online-Wahlsystem ableiten und er wird daher bei der folgenden Analyse nicht weiterbetrachtet.

Der Wahlrechtsgrundsatz der *freien* Wahl verlangt, dass der Wähler seine Stimme ohne Zwang und Druck sowie ohne Beeinflussung abgeben kann. Bei remote Online-Wahlen ergibt sich hier also eine Verschiebung. Während bisher im Wahllokal die Wahlhelfer und in der Versammlung der Vorsitzende sicherstellen musste, dass die Wähler ihre Stimme unbeeinflusst abgeben können, ist der Wähler, der seine Stimme im privaten Umfeld abgibt, selber dafür verantwortlich, dass er seine Stimme unbeeinflusst abgibt. Damit ergeben sich auch aus diesem Wahlrechtsgrundsatz keine spezifischen Anforderungen an ein Online-Wahlsystem als solches, sondern es muss auf einer anderen Ebene diskutiert werden, ob es vertretbar ist, die Verantwortung für die freie Stimmabgabe in die Hände des Wählers zu legen.

Die Anforderungen, die sich aus den anderen drei Wahlrechtsgrundsätzen ergeben, werden von *eVote* erfüllt. Im Gegensatz zu anderen Wahlsystemen können sich die Wähler sogar selber davon überzeugen und brauchen keiner Instanz/ keinem Server diesbezüglich zu vertrauen.

Der Wahlrechtsgrundsatz der *allgemeinen* Wahl verlangt, dass alle Wahlberechtigten die Möglichkeit haben an der Wahl teilzunehmen und der Grundsatz der *gleichen* Wahl, dass alle Wähler hierzu die gleiche Möglichkeit haben, d.h. alle Wähler genau einmal ihr Stimmrecht ausführen können und jede abgegebene Stimme genau einmal gezählt wird mit dem Inhalt, für den sich der Wähler entschieden hat. Diese beiden Wahlrechtsgrundsätze werden von *eVote* gewährleistet, da jeder Wähler anhand der Wahlnachricht/dem Stimmzettel überprüfen kann, ob alle Mitglieder des Gremiums gelistet sind. Außerdem kann am Ende nur dann ein Ergebnis ermittelt werden, wenn von jedem Wähler/Gremienmitglied eine Stimme abgegeben wurde. Es ist also nicht möglich, unbemerkt Stimmen zu entfernen. Auch das Austauschen von Stimmen fällt bei der Konsistenzprüfung in der zweiten Runde auf, so dass auch hier die gleiche und allgemeine Wahl nicht verletzt wird.

An einer Stelle setzt *eVote* den Wahlrechtsgrundsatz der allgemeinen Wahl sehr stark um, vermutlich für einige Wahlverfahren zu strikt. Das Wahlprotokoll durchläuft nur dann alle Runden, wenn auch alle Wahlberechtigten ihre Stimme abgegeben haben. Dies bedeutet, dass eine Art Wahlpflicht vorausgesetzt wird. Angriffe auf die Verfügbarkeit (beispielsweise durch Denial of Service Angriffe) und damit indirekt auf die allgemeine Wahl werden nicht betrachtet, da dies wie bei jeder Internetanwendung ein noch zu lösendes Problem ist.

Der Wahlrechtsgrundsatz der *geheimen* Wahl fordert zum Einen, dass es keinen Zusammenhang zwischen Wähler und seiner Stimme geben darf, und zum Anderen, dass das Wahlsystem ihm keine Möglichkeit geben darf, zu beweisen, für welche Kandidaten er sich entschieden hat oder allgemein welche Auswahl er getroffen hat. Auf diese Weise wird der Stimmenkauf unterbunden. Dieser Grundsatz wird durch eine Art MIX-Verfahren sichergestellt: Die bei einem Wähler/einer Wahlsoftware ein- und ausgehenden verschlüsselten Stimmzettel können durch die Entfernung einer Verschlüsselungsschicht, das zufällige Durchmischen und die Tatsache, dass die Verschlüsselung der äußeren Schicht semantisch sicher ist, einander nicht mehr zugeordnet werden. Damit kann der Wähler selbst die geheime Wahl sicherstellen –

unabhängig davon, ob die anderen Wähler die Stimmen ordnungsgemäß durchmischen oder nicht.

Das Entfernen einzelner Stimmen zwecks Brechen der geheimen Wahl ist in der ersten Runde sicherheitskritisch: Hier sieht der Angreifer, wessen Stimme er entfernt hat, da der entsprechende Wähler das Protokoll spätestens im letzten Schritt der ersten Runde abbricht. Dies bedeutet insbesondere, dass der entnommene Datensatz nicht im Klartext vorliegt und der Angreifer damit nicht den Inhalt der Stimme erfährt. Ein Entfernen einer Stimme im Verlauf der letzen Runde führt zwar auch zum Protokollabbruch, aber hier brechen alle Wähler das Protokoll ab, so dass der Angreifer den abgegriffenen Datensatz keinem Wähler zuordnen kann.

Fazit

Besonders die Wahlen in kleinen Gruppen, wie etwa in akademischen Gremien oder in Vorständen eignen sich für die Einführung von Online-Wahlen. Insbesondere der Notwendigkeit, kurzfristige Entscheidungen zu treffen, kann mittels Online-Wahlen Rechnung getragen werden.

Im Projekt *eVote* haben wir gezeigt, dass in diesen Bereichen theoretisch anspruchsvolle Protokolle eingesetzt werden können, bei denen das Datenaufkommen zwar höher, die Verfahren aber bezüglich des Vertrauensmodells sicherer sind. Hierzu haben wir eine Erweiterung des Merritt-Protokolls [DM83] im Rahmen des Projektes „E-Voting for Academics“ prototypisch implementiert und die Realisierbarkeit demonstriert.

Literatur

[BeYu86] Benaloh, J. D., Yung, M.: Distributing the power of a government to enhance the privacy of voters. S. 52–62, 1986.

[BWahlG] Bundesministerium des Inneren: (BWahlGV) Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, Zuletzt geändert 20. 4.1999; http://bundesrecht.juris.de/bundesrecht/bwahlgv/ [ABRUFDATUM 06-07-2005]

[Brau03] Braun, N.: E-Voting in der Schweiz. In: Schweighofer, E., Menzel, T. et.al. IT in Recht und Staat, Internationales Rechtsinformatik Symposium Salzburg, 2003.

[CF85] Cohen (Benaloh), J. D., Fischer, M. J.: A robust and verifiable cryptographically secure election scheme. In: Proc. 5th ACM Symposium on the Foundation of Distributed Computing (PODC), 1986

[Chau81] Chaum, D., Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communication of the ACM, Vol. 24, No. 2, Februar 1981

[Chau85] Chaum, D., Security without identification: Transaction systems to make big brother obsolete, Communications of the ACM, 28,10 (Oktober 1985)

[Chev04] Chevallier, M.: Internet Voting – Geneva Experiences. Presentation at ESF TED E-Voting in Europe Workshop, Bregenz, 2004.

[D21-2002] Forderungen der Initiative D21 für die nächste Legislaturperiode zur Gestaltung der Informationsgesellschaft in Deutschland (12 Aktionen nach der Wahl), 2002, http://www.initiative21.de/druck/news/publikationen2002/doc/33_1053504444.doc [ABRUFDATUM 06-07-2005]

[DM83] DeMillo, R., Merritt, M..: Protocols for Data Security. In: Computer v. 16, n. 2, 1983

[ESI01] Erfahrungsbereicht zum Projekt „Elektronische Stimmabgabe im Internet“; Landratswahl des Landkreises Marburg-Biedenkopf am 16.09.2001; http://www.wahlen.hessen.de/Internetwahl.doc [ABRUFDATUM 11-06-2005]

[eVote] Gessner, S., Volkamer, M.: eVote – elektronisches Wahlsystem für Gremien, 2003. http://www-krypt.cs.uni-sb.de/projects/evote/ [ABRUFDATUM 06-07-2005]

[Fell01] Dokumentation zur Wahl zum Jugendgemeinderat Fellbach; abrufbar unter: http://www.fellbach.de/kommunalpolitik/jugendgemeinderat/Dokumentation_JGR Onlinewahl.pdf [ABRUFDATUM 11-06-2005]

[FOO92] Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting system for large scaled elections. In: Advances in Cryptology – AUSCRYPT ,1992

[Full63] Fuller, B. R.: No more Second-Hand God, Southern Illinois University Press, 1963.

[GI-WAHL] Gesellschaft für Informatik e.V., Gesellschaft für Informatik hat Onlinewahl erfolgreich erprobt, Pressemitteilung vom 10.12.2004, http://www.gi-ev.de/informatik/presse/presse_041210.shtml [ABRUFDATUM 06-07-2005]

[KrVo05] Krimmer, R., Volkamer, M.: Wählen auf Distanz: Ein Vergleich zwischen elektronischen und nicht elektronischen Verfahren in Recht und Staat, Internationales Rechtsinformatik Symposium Salzburg, 2005 (in Druck).

[i-vote] Bundesministerium für Wirtschaft und Arbeit (BMWA) als Projektförderr: „Wählen via Internet“ („i-vote“). http://www.i-vote.de/ [ABRUFDATUM 06-07-2005]

[Karg03] Karger, P., Rüß, O.R.: Sicherheit ist conditio sine qua non. In:Braun, N., Heindl, P., et.al., Working Paper 02/03 Institut für Informationsverarbeitung, Wirtschaftsuniversität Wien, 2003.

[Maus04] Mausch, M.: Mobile Fusion, Mimori Group, http://www.mimori-group.com/obj/Dokumente/Mobile_Fusion.pdf [ABRUFDATUM 08-07-2005]

[Maat04] Maaten, E.: Towards Remote E-Voting: Estonian case. In: Prosser, A., Krimmer, R.: Proceedings ESF TED E-Voting in Europe Workshop, Bregenz, 2004.

[Nedap] HSG – Wahlsysteme: Elektronische Wahlgeräte mit Wahl- und Geräteanwendungssoftware; http://www.wahlsysteme.de/Homepage.htm [ABRUFDATUM 06-07-2005]

[Prat04] Pratchett, L., Wingfield, M.: Electronic voting in the United Kingdom. Lessons and limitations from the UK Experience. In: Kersting, N., Baldersheim, H.: Electronic Voting and Democracy: A Comparative Analysis, Palgrave, London, 2004.

[Siem1891] Werner von Siemens: Elektrischen Abstimmungs-Telegraphen, 1870, in: Wissenschaftliche und Technische Arbeiten von Werner Siemens, 2. Auflage, Verlag von Julius Springer (Siemens-Archiv), Berlin, S. 307 – 309, 1891.

[Smith05] Smith, W. D.:Cryptography meets voting, 2005. http://www.math.temple.edu/~wds/homepage/cryptovot.pdf [ABRUFDATUM 06-07-2005]

[Ullm01] Ullmann, Markus; Koop, Frank; Kelter, Harald: Anonyme Online-Wahlen. Datenschutz und Datensicherheit (DuD), 11/2001, S. 643-647.

[W.I.E.N.] Bundesministerium für Wirtschaft und Arbeit, T-Systems, LDS Brandenburg, Universität Osnabrück, Wählen in elektronischen Netzen (W.I.E.N.). Webseite http://www.forschungs projekt-wien.de/ [ABRUFDATUM 06-07-2005]