



✕ Elektronische Wahlen

Eine Informationsbroschüre für den Wahlbürger

Peter Wilm
wilm@elektronische-wahlen.de

Version 1.1 18. Januar 2004
<http://www.elektronische-wahlen.de/staatlich/>

Autor:

Peter Wilm
Heilmannring 55a
13627 Berlin
Tel./Fax: 030 345 06936
E-Mail: wilm@elektronische-wahlen.de

**Download der jeweils aktuellen Version dieser Broschüre unter:
<http://www.elektronische-wahlen.de/staatlich/>**

Über diese Broschüre

Diese Broschüre will über die Möglichkeiten und Risiken bei der Einführung von elektronischen (internetbasierten) Wahlsystemen bei den Wahlen zu den staatlichen Volksvertretungen informieren. Dabei wird eine kurze Motivation und ein kleiner Überblick über die aktuelle Situation gegeben, der rechtliche Rahmen für Wahlen in der Bundesrepublik beschrieben, es werden Eigenschaften des bisherigen papierbasierten Systems dargelegt, die Situation bei den elektronischen, nicht an das Internet angebundenen Wahlgeräten dargestellt, notwendige Anforderungen an ein internetbasiertes Online-Voting-System aufgestellt, Bemerkungen zu einer möglichen Novellierung der Bundeswahlgeräteverordnung und zur Konzeption von Internet-Voting-Systemen gemacht, aktuelle Prototypen für Internet-Voting-Systeme vorgestellt, politische Motivationen zur Einführung von Internet-Wahlsystemen dargestellt, Forderungen an die Bundesregierung und den Gesetzgeber gestellt und eine knappe Zusammenfassung dieses Heftes und Literaturtips gegeben, sowie eine Klassifizierung und Bewertung existierender Wahlprotokolle vorgenommen.

„Die Auszählung der Stimmen in einem Wahllokal ist für jeden nachvollziehbar, die Speicherung der Stimme in einem Zentralcomputer nicht.“

Johann Hahlen, Bundeswahlleiter, 18.09.2001, Deutscher Internet-Kongress Karlsruhe

Inhaltsverzeichnis

1	Worum geht es?	5
2	Rechtlicher Rahmen	7
3	Die bisherige Wahlmethode	10
4	Wahlgeräte ohne öffentliche Vernetzung	10
5	Notwendige technische Anforderungen an ein Internet-Wahlssystem	12
6	Mögliche Novellierung der BWahlGV	21
7	Bemerkungen zur Konzeption von Internet-Wahlssystemen	22
8	Existierende Prototypen für Internetwahlssysteme	25
9	Politische Motivationen	28
10	Häufig gehörte Argumente	30
11	Empfehlungen an die Bundesregierung und den Gesetzgeber	33
12	Zusammenfassung	34
A	Literaturtips	36
B	Wahlprotokolle	36
C	Glossar	52

1 Worum geht es?

Die Einführung von elektronischen Wahlsystemen bei staatlichen Wahlen ist mit einigen Gefahren behaftet. Auf Grund von politischen Motivationen besteht jedoch das Risiko, elektronische Wahlen einzuführen ohne diese Risiken ausreichend zu beachten.

Diese Broschüre möchte über die technischen Aspekte und Risiken bei der Einführung von staatlichen elektronischen Wahlen informieren.

Sie basiert auf Erkenntnissen, die der Autor während des Entwurfs und der Implementierung eines sicheren, skalierbaren und robusten Voting-Systems zur Entscheidungsfindung in großen Communities (bei nicht-staatlichen Wahlen) erzielt hat. Dabei habe ich mich automatisch auch mit dem verwandten Gebiet der Voting-Systeme für staatliche Wahlen beschäftigt. In keiner Weise bin ich in irgendeiner Form beruflich mit der Einführung von elektronischen Wahlsystemen bei staatlichen Wahlen befasst. Somit handelt es sich hierbei um eine Informationsbroschüre eines einfachen Wahlbürgers für seine Mit-Wahlbürger.

1.1 Bedeutung des Wahlsystems für die Gesellschaft

Die Glaubwürdigkeit der Korrektheit der Durchführung der Wahl, der obligatorischen Einhaltung des Wahlgeheimnisses, sowie der korrekten Ermittlung des Wahlergebnisses ist entscheidend für die Legitimation der bei dem Vorgang gewählten Staatsorgane verantwortlich.

Es ist somit nicht ausreichend, für einen korrekten Wahlablauf und eine korrekte Ergebnisermittlung zu sorgen. Jeder wahlberechtigte Bürger will von der Korrektheit überzeugt werden, soll das Ergebnis nicht nur vom Bundes- oder jeweiligen Landeswahlleiter, sondern auch allgemein anerkannt werden.

Die allgemeine Anerkennung des Wahlergebnisses ist wiederum für das Funktionieren unseres politischen Systems von zentraler Bedeutung: Die durch die gewählten Volksvertreter gefällten Entscheidungen werden in unserer Gesellschaft allgemein akzeptiert – jedoch nur unter der Prämisse, dass die Ermittlung der Mehrheitsverhältnisse bei der Wahl der Volksvertretungen auch tatsächlich korrekt abläuft.

Also sind eher kleine technische Details des Wahlvorgangs in ihrer Gesamtheit – obwohl wegen des hervorragenden Funktionierens unserer aktuellen Wahlmetho-

de zur Zeit wenig beachtet – ein zentraler Stützpfeiler für unser Staatssystem.

1.2 Mangelnde Transparenz bei Internet-Wahlsystemen

Eine wesentliche Schwierigkeit bei der Einführung von internetbasierten Wahlsystemen ist die Schaffung einer ausreichenden Transparenz bei der Ergebnisermittlung und somit die erwähnte notwendige Vertrauensbildung in der Wahlbevölkerung.

Der Herr Bundeswahlleiter Johann Hahlen äußerte sich dazu am 18.09.2001 auf dem Deutschen Internet-Kongress Karlsruhe [dpa]:

„Die Auszählung der Stimmen in einem Wahllokal ist für jeden nachvollziehbar, die Speicherung der Stimme in einem Zentralcomputer nicht.“

Auch Will [Wil02], S.153 hat dazu ähnliche grundlegende Bedenken:

„Grundsätzlich problematisch ist bei der Internetwahl bspw. die immanente qualitative Verlagerung öffentlicher Wahlen aus dem öffentlichen Bereich hinaus. Gemeint ist nicht nur der Vorgang der Wahl, der – zumindest bei der individuellen Internetwahl – wie bei der Briefwahl im privaten Umfeld erfolgen kann. Bedeutsam ist vor allem der Prozess der Verarbeitung und Auszählung der Wahldaten, der sich bei der Internetwahl nicht mehr dezentral und öffentlich, sondern durch den Einsatz bestimmter Software funktional zentralisiert und für die Öffentlichkeit nicht unmittelbar kontrollierbar vollzieht. ... Damit würde die Wahl dem öffentlichen Raum entzogen, was sich ganz konkret in einer Erschütterung des Vertrauens niederschlagen könnte, ...“

1.3 Aktuelle Situation

Das jetzige Wahlsystem der Bundesrepublik Deutschland funktioniert hervorragend: Es basiert vor allem auf einer Dezentralisierung und einer vollständigen Transparenz für den Bürger. Ein Wahlbetrug ist äußerst schwierig vorzunehmen, da es einer Verschwörung einer ganzen Reihe von Wahlhelfern bedarf. Zudem ist

selbst bei einer erfolgreichen Verschwörung lediglich das Ergebnis einer einzelnen Wahlurne verfälschbar. Jeder Bürger kann den Wahlvorgang zudem beobachten und hat somit die Möglichkeit, den korrekten Wahlablauf in seinem Wahllokal persönlich zu verifizieren. Mittels dieser vollkommenen Transparenz der aktuellen, viele Jahrzehnte lang bewährten Wahlmethode wird in der Bundesrepublik die Legitimation der gewählten Staatsorgane gewährleistet.

Spätestens seit dem Jahr 2001 verfolgt die Bundesregierung das Ziel, stufenweise internetbasierte Volksvertreterwahlen einzuführen. Dazu wurde bereits im Oktober 2000 eine Arbeitsgruppe Online-Wahlen im Bundesinnenministerium eingerichtet [Kör01].

Des Weiteren hat die Forschungsgruppe Internetwahlen mit dem von ihr entwickelten System i-vote bis zum Mai 2003 bereits sieben Testwahlen (wie zum Beispiel Personalratswahlen und Hochschulwahlen) durchgeführt [For04]. Bei dieser Forschungsgruppe (inzwischen Teil des Konsortiums W.I.E.N., welches durch des Bundesministerium für Wirtschaft und Arbeit maßgeblich finanziell unterstützt wird) handelt es sich um einen zentralen Stützpfeiler für die Bemühungen der Bundesregierung. Zwar wurden einige Arbeitsberichte veröffentlicht [For02], jedoch wird aus ihnen nicht die tatsächliche Architektur des Systems i-vote ersichtlich. Auch existieren keine formalen Anforderungsdefinitionen an das System.

2 Rechtlicher Rahmen

Bislang gibt es innerhalb der Europäischen Union keine vereinheitlichte Regelung der Wahlvorgänge. Vielmehr gibt sich jeder Mitgliedsstaat seine eigene Wahlgesetzgebung.

Auch in den USA gibt es keine einheitliche Ordnung. Eine wesentliche Richtlinie ist jedoch die Empfehlung der Federal Election Commission aus dem Jahr 2001 [Fed01]. Eine informelle Sammlung von Anforderungen an Voting-Systeme hat auch eine vom California Secretary of State eingesetzte Kommission zusammengetragen [Cal00].

2.1 Rechtliche Regelungen in der BRD

In Deutschland legen das Grundgesetz [Par49], das Bundeswahlgesetz [Bun93], die Bundeswahlordnung [Bun02] und die Bundeswahlgeräte-Verordnung [Bun75]

die Anforderungen an Wahlen und Wahlverfahren fest. Diese vier Gesetze und Verordnungen legitimieren sich gegenseitig in einer absteigenden Hierarchiekaskade. Wahlprüfungen werden durch das Wahlprüfungsgesetz [Bun51] geregelt. Analog zum Bundeswahlgesetz und zur Bundeswahlordnung werden die Wahlen der Abgeordneten des Europäischen Parlamentes aus der BRD durch das EuWG [Bun78] und die EuWO [Bun88] geregelt.

Das Grundgesetz gibt sowohl für die Bundestagswahlen, als auch für Wahlen in den Ländern, Kreisen und Gemeinden eine klare Vorgabe:

Art. 38 Abs. 1 S. 1 GG: „Die Abgeordneten des Deutschen Bundestages werden in **allgemeiner, unmittelbarer, freier, gleicher und geheimer** Wahl gewählt.“

Art. 28 Abs. 1 S. 2 GG: „In den Ländern, Kreisen und Gemeinden muss das Volk eine Vertretung haben, die aus **allgemeinen, unmittelbaren, freien, gleichen und geheimen** Wahlen hervorgegangen ist.“

Die genannten Bestimmungen regeln die ordnungsgemäße Durchführung der Wahlen zu den Volksvertretungen in der Bundesrepublik Deutschland. Alle weiteren durchgeführten Wahlen und Abstimmungen sind davon nicht betroffen. Die Wahlen innerhalb Organisationen jeglicher Art in Deutschland werden durch die Satzung der jeweiligen Organisation geregelt. Für Vereine gibt das Bürgerliche Gesetzbuch [Bun96] Vorgaben, für Aktiengesellschaften ist es das Aktiengesetz [Bun65] und für Parteien das Parteiengesetz [Bun67]. Regelungen zur Rechtsgültigkeit von digitalen Signaturen sind im Signaturgesetz [Bun01] festgelegt.

Einen umfangreichen allgemeinen Überblick über das Wahlrecht der BRD liefern Zicht und Fehndrich [ZF04]. Eine ausführliche Darstellung der rechtlichen Vorgaben zu elektronischen staatlichen Volksvertreter-Wahlen liefern Will [Wil02] und Rüß [Rüß02]. Rechtliche Möglichkeiten zur Virtualisierung von Hauptversammlungen und Parteitag liefern Noack [Noa00] und Mausch [Mau02].

Elektronische Wahlen der Vorstände in Vereinen und Parteien sind im BGB und im PartG nicht explizit vorgesehen. Dadurch entsteht eine juristisch unklare Situation, in der die Gerichte die einzelnen Satzungen individuell begutachten müssen. Als erstem Verein ist es der Initiative D21 e.V. gelungen [Ini03], eine Satzung zu implementieren, die gerichtlich anerkannte Online-Vorstandswahlen zulässt. Für die Zukunft wäre es jedoch sinnvoll, wenn der Gesetzgeber eine explizite Regelung im BGB verankern würde.

Das Aktiengesetz verhindert mit § 118 Abs 1 AktG eine direkte Online-Stimmabgabe bei einer Hauptversammlung. Es sind Präsenz-Veranstaltungen vorgeschrieben. Lediglich die Benennung eines Bevollmächtigten zur Stimmabgabe ist mög-

lich. Auch hier könnte der Gesetzgeber sehr einfach die bestehende Regelung ändern.

2.2 Zuständige Behörden und Organe in der BRD

Die folgenden Organe und Behörden sind mit den Wahlen der Mitglieder der staatlichen Volksvertretungen befasst:

Deutscher Bundestag Der Deutsche Bundestag beschließt über Änderungen in der Wahlgesetzgebung.

Bundeswahlleiter Der Bundeswahlleiter ist für die Überwachung der ordnungsgemäßen Durchführung der Wahl zuständig. Er wird durch den Bundesinnenminister auf unbestimmte Zeit benannt. Meist ist er in Personalunion der Präsident des Statistischen Bundesamtes. Er sitzt automatisch dem Bundeswahlausschuss vor. Er ermittelt das vorläufige Endergebnis und gibt dieses bekannt. Bei der Erfüllung seiner Aufgaben ist er nicht an Weisungen aus dem Bundesinnenministerium, sondern lediglich an die bestehende Wahlgesetzgebung gebunden. Auch kann er den verschiedenen Wahlorganen keine Weisungen erteilen, jedoch hat er das Recht, Einspruch im Wahlprüfungsverfahren zu erheben [Gei02].

Bundeswahlausschuss Der Bundeswahlausschuss ermittelt das amtliche Endergebnis der Wahl. Er ist zuvor insbesondere mit der Zulassung von Parteien zur Wahl betraut.

Bundesinnenministerium Das Bundesinnenministerium ist die mit der Wahldurchführung und -koordinierung beauftragte Behörde.

Physikalisch Technische Bundesanstalt Die Physikalisch Technische Bundesanstalt entscheidet über die Zulassung einzelner Wahlgeräte nach der Bundeswahlgeräteverordnung.

Bundesamt für Sicherheit in der Informationstechnik Das Bundesamt für Sicherheit in der Informationstechnik nimmt zwar keine offizielle Rolle bei staatlichen Wahlen ein, verfügt jedoch über hohe technische Kompetenzen hinsichtlich einer möglichen Einführung von staatlichen Onlinewahlen.

3 Die bisherige Wahlmethode

Die aktuelle, papierbasierte Wahlmethode zeichnet sich durch eine vollkommene Transparenz für den Bürger aus. Im Folgenden werden die einzelnen Eigenschaften dargestellt, die zu dieser Transparenz führen.

- Das System ist dezentral organisiert.
- Jeder Bürger kann kontrollieren, ob die Ergebnisse seines jeweiligen Wahllokals auch korrekt in seiner Tageszeitung / im amtlichen Endergebnis veröffentlicht werden.
- Die Einzelergebnisse lassen sich addieren, so dass die Ergebnisermittlung der Behörden durch jedermann kontrolliert werden kann.
- Ein möglicher Wahlbetrug kann sich demnach allenfalls auf die Stimmen eines Wahllokals erstrecken.
- Innerhalb eines Wahllokals sorgt ein mehrköpfiger Wahlvorstand für eine korrekte Ergebnisermittlung. Damit ein Wahlbetrug durchgeführt werden kann, müssen sämtliche Mitglieder des Wahlvorstandes konspirieren.
- Während des gesamten Wahlzeitraumes ist es jedem Wahlbürger möglich die ordnungsgemäße Durchführung der Wahl persönlich zu kontrollieren. Da das System papierbasiert arbeitet, ist dies auch tatsächlich sehr einfach möglich.

Der bisher wohl einzige Fall eines Wahlbetrugs fand im Jahr 2001 in der Stadt Dachau bei den Oberbürgermeisterwahlen statt.

4 Wahlgeräte ohne öffentliche Vernetzung

Eine Zwischenstufe zur Ersetzung des papier- durch ein internetbasiertes System stellt die Einführung von elektronischen Wahlgeräten dar, die in den Wahllokalen aufgestellt werden und jeweils einzeln die Stimmen zählen. Nach Beendigung des Wahlganges müssen die Ergebnisse lediglich addiert, nicht jedoch manuell ausgezählt werden. Bei diesen Geräten handelt es sich meist um direkte Aufzeichnungssysteme (vgl. B.2.3).

4.1 Aktuelle Situation in der BRD

Seit 1975 gibt es die „Bundeswahlgeräteverordnung“ (BWahlGV), die Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland [Bun75]. In ihr wird die notwendige Beschaffenheit von elektrischen oder elektronischen Wahlgeräten festgelegt.

Doch erst in den letzten Jahren wurde in einigen Wahlkreisen tatsächlich das papierbasierte System durch elektronische Geräte ersetzt. So z.B. in Köln bei der Bundestagswahl 2002. Hier wurden elektronische Wahlgeräte zu einem Stückpreis von 4000 Euro angeschafft.

Möchte ein Privatunternehmen den lokalen Wahlbehörden ein elektronisches Wahlgerät anbieten dürfen, so bedarf es dazu laut Bundeswahlgeräteverordnung der Betriebsgenehmigung des Bundesinnenministeriums, welches dazu ein Gutachten der Physikalisch Technischen Bundesanstalt einholt.

4.2 Erfahrungen in den USA

In den USA werden bereits seit etlichen Jahren elektronische Wahlgeräte eingesetzt. Diese Entwicklung wurde durch das Wahldebakel mit den lochkartenbasierten Systemen des Bundesstaates Florida bei der Stimmauszählung der Präsidentschaftswahl 2000 deutlich beschleunigt.

Dabei bieten die Hersteller jeweils Closed-Source-Produkte an, deren Funktionsweise sie der breiten Öffentlichkeit nicht offen legen.

4.2.1 Der Diebold-Skandal

Ein eindrucksvolles Beispiel für die Gefahren, die der Einsatz von Closed-Source-Produkten bei staatlichen Volksvertreterwahlen in sich bergen kann, hat die Firma Diebold geliefert.

Sie hat in den vergangenen Jahren ein direktes Aufzeichnungssystem angeboten, mit Hilfe dessen Wahlkartenlesesysteme in den USA verdrängt werden sollten. Die gesamte Software der angebotenen Wahlkioske wurde als Closed-Source vertrieben.

Der Firma Diebold gelang es, derartige Wahlkioske an die US-Bundesstaaten Georgia und Maryland zu verkaufen. Letzterer zahlte 56 Mio. US \$ [Sch03].

Im Januar 2003 wurde versehentlich auf einem öffentlichen FTP-Server der Firma Diebold der komplette Source-Code zu einem direkten Aufzeichnungssystem veröffentlicht [Jon03].

Kohno, Stubblefield und Rubin analysierten den Code [KSRW03] und äußerten die Vermutung, dass es sich dabei um den tatsächlich in den vertriebenen Wahlmaschinen zum Einsatz gekommen Code handeln könnte. Sie fanden Unmengen von spektakulären Sicherheitsschwachstellen. Unter anderem kann jeder beliebige Wähler mit sehr geringem technischen Know-How und einer Investition von 100 US \$ Smartcards erstellen, mit denen er beliebig oft seine Stimme abgeben kann. Auch können Offizielle der Wahlbehörden Stimmzettel beliebig manipulieren. Beides lässt sich nachträglich nicht mehr nachweisen.

Die mit diesen Geräten ermittelten Wahlergebnisse (u.a. bundesstaatsweite Parlamentswahlen in Georgia) haben nach diesen Erkenntnissen wohl keinerlei Wert mehr.

Der Fall Diebold stellt somit ein besonders abschreckendes Beispiel dafür dar, was passieren kann, wenn Wahlbehörden den Reklameaussagen von Voting-System-Herstellern Glauben schenken. Mit Hilfe des Einsatzes von Smart-Cards lässt sich einfach Werbung betreiben. Jedoch sollte sich jeder Bürger von der Sicherheit der Systeme selber überzeugen können, indem der Source Code und sämtliche Architekturdetails öffentlich gemacht werden.

5 Notwendige technische Anforderungen an ein Internet-Wahlssystem

Dieser Abschnitt will zumindest eine Teilmenge der notwendigen technischen Anforderungen an ein Internet-Voting-System ermitteln, soll es eine Qualität aufweisen, das dem jetzigen System ebenbürtig ist.

Art. 38 Abs. 1 Satz 1 GG [Par49] nennt fünf Anforderungen an eine Volksvertreterwahl: „Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.“

Es gibt einige Veröffentlichungen zu den rechtlichen Folgen der Vorgaben des Grundgesetzartikels für mögliche Onlinewahlssysteme. Hier sollen jedoch techni-

sche Implikationen aufgeführt werden.

Wird eine Anforderung unmittelbar durch einen der fünf Wahlrechtsgrundsätze impliziert, so wird dieser Grundsatz in Klammern aufgeführt.

5.1 Wahlgeheimnis

✗ **ANF 1** Das Wahlgeheimnis muss gewahrt werden. Niemand außer dem Wähler selber darf in Erfahrung bringen dürfen, was dieser gewählt hat.
(Geheimheit)

Der Schutz des Wahlgeheimnisses soll gegenüber Jedermann gelten:

✗ **ANF 2** Auch Administratoren des Onlinewahlsystems dürfen nicht die technischen Möglichkeiten haben, das Wahlgeheimnis zu brechen.
(Geheimheit)

Soll der Wähler seine Wahl frei von privatem und öffentlichem Druck abgeben können, so muss gewährleistet sein, dass der Wähler nicht käuflich, oder erpressbar sein kann, er also seine Wahl nicht nachweisen kann.

✗ **ANF 3** Der Wähler darf nach dem Wahlvorgang nicht nachweisen können, was er gewählt hat (Quittungsfreiheit). Gibt ihm das System Informationen in die Hand, mit der er die Zählung seiner Stimme überprüfen kann, so muss mathematisch nachgewiesen worden sein, dass aus diesen Informationen keine Quittung über den Inhalt seines Stimmzettels generiert werden kann. Dabei ist es unerheblich, ob der Wahl-Client vom Wahlamt signierte Informationen dem Wähler vorenthält. Es muss sichergestellt werden, dass der Wähler auch bei Manipulation seines Wahl-Clients keine Möglichkeit hat, in den Besitz einer durch eine an der Wahl beteiligten Instanz signierte Quittung seiner Wahl zu gelangen.
(Geheimheit)

Beim heutigen Wahlsystem gilt das Wahlgeheimnis zeitlich absolut. Dies sollte es bei einem neu einzuführenden Onlinewahlssystem zumindest für einen ausreichenden Zeitraum (von vielen Jahrzehnten), so dass auch Persönlichkeiten des öffentlichen Lebens keine Angst vor einer späteren Veröffentlichung ihres Abstimmungsverhaltens zu haben brauchen.

✗ **ANF 4** Es muss sichergestellt werden, dass auch bei einem Mitschnitt der Kommunikation zwischen Wahl-Client und Wahlamt ein potentieller Angreifer aller Voraussicht nach frühestens nach Ablauf einer Zeitspanne von vielen Jahrzehnten in den Besitz von Technologie gelangen können, um den Klartext des ermittelten Stimmzettels entschlüsseln zu können.
(Geheimheit)

5.2 Korrektheit des Ergebnisses

✗ **ANF 5** Das System muss ein korrektes Ergebnis ermitteln.
(Allgemeinheit, Gleichheit)

Dazu muss jede wahlberechtigte Person einen Stimmzettel abgeben dürfen, jedoch nicht mehrfach wählen dürfen:

✗ **ANF 6** Das System muss exakt einen Wahlzettel pro wahlberechtigter Person pro Wahlgang annehmen.
(Gleichheit)

Es ist davon auszugehen, dass bei einem derart großen System, auch bei Verwendung von besonders ausfallsicherer Hardware eine hohe Wahrscheinlichkeit besteht, dass Teilsysteme ausfallen. Dies darf das Wahlergebnis nicht beeinflussen. Es muss also bei einer redundanten Ausfallsicherung von Teilsystemen das übernehmende Teilsystem den Zustand des ausgefallenen Teilsystem on the fly und bitgenau übernehmen.

✗ **ANF 7** Fällt ein beliebiges Teilsystem aus, so muss dessen Zustand exakt rekonstruiert werden können. Der plötzliche Totalausfall einer beliebigen Teilkomponente (z.B. zu simulieren durch das Ziehen sämtlicher Strom- und Netzwerkstecker, sowie Batterien) in einer beliebigen Situation darf das Wahlergebnis nicht um eine Stimme verändern. Jeder vom System angenommene Stimmzettel muss genau einmal gezählt werden.
(Allgemeinheit, Gleichheit)

Es ist ebenfalls davon auszugehen, dass Netzverbindungen zwischen dem Client-Rechner und den Wahl-Servern unterbrochen werden können:

✗ **ANF 8** Wurde ein Stimmzettel vom System nicht angenommen, so ist dies dem Wähler zweifelsfrei mitzuteilen. Er ist deutlich aufzufordern, die Wahl zu wiederholen. Mögliche Missverständnisse, ob der Stimmzettel gezählt wurde oder nicht, sind unter allen Umständen auszuschließen.
(Allgemeinheit)

Die Korrektheit des Wahlergebnisses darf nicht von der moralischen Integrität einzelner Systemadministratoren abhängig sein.

✗ **ANF 9** Kein Systemadministrator darf in der Lage sein, das Ergebnis zu manipulieren. Dazu muss es mindestens eine Verschwörung von n Systemadministratoren bedürfen (bei vorab frei wählbarem n), falls nicht ein Wahlprotokoll zum Einsatz kommen soll, dass eine universelle Verifizierbarkeit des Wahlergebnisses durch alle Wahlteilnehmer zulässt – in diesem Fall ist jedoch auf die Einhaltung von ✗ **ANF 3** zu achten.
(Gleichheit)

Die Wahl-Server stellen für Außenstehende sicherlich ein besonders attraktives Angriffsziel dar.

✘ ANF 10 Sämtliche Server der Wahlinstanzen müssen einbruchsicher sein. Die gesamte eingesetzte Wahlsoftware und sämtliche darunterliegende Systemsoftware muss fehlerfrei sein. Dies muss nachgewiesen werden (zumindest durch exzessive vollständige Code-Audits). Reklameaussagen oder sogar eidesstattliche Versicherungen von Herstellern über deren Systemeigenschaften sind nicht ausreichend.
(Gleichheit)

Das aktuelle Wahlrecht sieht in Zweifelsfällen Neuauszählungen vor. Dies macht für ein Onlinewahlssystem wenig Sinn, da im Falle einer Manipulation ebenso gut die gespeicherten Wahlzettel manipuliert worden sein können. Es besteht die Gefahr, dass durch die Möglichkeit von Neuauszählungen suggeriert wird, Zweifel am ermittelten Wahlergebnis seien minder gravierend, da das Ergebnis ja neu ermittelt werden könne.

✘ ANF 11 Sollen Mehrfachauszählungen zwecks Wahlprüfungen zugelassen werden, so ist die Unmöglichkeit eines erfolgten Entfernens, Hinzufügens oder Manipulierens von Stimmzetteln mathematisch zweifelsfrei nachzuweisen. Dieser Nachweis ist gegenüber der Wahlprüfungskommission zu führen.
(Gleichheit)

Um auch Fehlerquellen durch Hardwarefehler auszuschließen muss gelten:

✘ ANF 12 Ergebnisse sind so zu berechnen, dass selbst bei durch Hardware erzeugten Bitfehlern das Ergebnis nicht beeinflusst wird.
(Gleichheit)

5.3 Client-Rechnersicherheit

Oftmals wird bei der Entwicklung von Prototypen von internetbasierten Onlinewahlssystemen für staatliche Volksvertreterwahlen die Sicherheit der Clients vernachlässigt.

Unterschwellig wird damit argumentiert, dass durch einen Angriff auf den Wahl-Client maximal ein einzelner Stimmzettel gefälscht werden kann. Dies ist im Zeitalter von Viren, Trojanern und Würmern jedoch nicht mehr der Fall. Attacken auf eine große Anzahl von Rechnern lassen sich automatisieren. Ist ein System angreifbar, so sind es mit nahezu konstantem Aufwand auch alle baugleichen.

Es muss also gelten:

✗ ANF 13 Der Wahl-Client ist Teil des Onlinewahlsystems. Sämtliche Anforderungen an die Sicherheit des Onlinewahlsystems müssen auch durch den Wahl-Client erfüllt werden.
(Allgemeinheit, Gleichheit, Geheimheit)

✗ ANF 14 Es muss für eine ausreichende Sicherheit der Konfiguration des Rechners, auf dem die Wahl-Client-Software laufen soll gesorgt werden. Die Verantwortung hierfür liegt beim Betreiber der Wahl und nicht beim Wähler.
(Allgemeinheit, Gleichheit, Geheimheit)

Zudem ist – um die Allgemeinheit der Wahl zu gewährleisten – dem Wähler nicht zuzumuten, selbstständig Software- oder Hardware-Installationen oder -Konfigurationen an seinem Rechner vorzunehmen.

✗ ANF 15 Soll der Wähler von beliebigen Rechnern aus wählen können (nicht nur von zuvor präparierten Wahl-Kiosken), so ist ihm dies zu ermöglichen, ohne dass Annahmen über seine Betriebssystem- oder Softwarekonfiguration zu machen sind. Spezielle Web-Browser, Java Virtual Machines o.ä. sind nicht vorauszusetzen.
(Allgemeinheit)

5.4 Verfügbarkeit

Um die Allgemeinheit der Wahl zu gewährleisten, muss gelten:

✘ ANF 16 Den Wählern ist während des vollständigen Wahlzeitraumes der Wahlservice ununterbrochen zur Verfügung zu stellen. Insbesondere sind technologische Gegenmaßnahmen zu Distributed Denial of Service-Attacken auf die Bandbreite der Internetanbindung der Wahl-Server, deren Prozessorlast und anderen System-Ressourcen vorzubereiten.
(Allgemeinheit)

Da anzunehmen ist, dass es nicht möglich sein wird, eine Verfügbarkeit des Wahlservices über den vollständigen Zeitraum mit absoluter Sicherheit zu garantieren, ist den Wählern die Möglichkeit zu geben, im Notfall ein Wahllokal nach fehlgeschlagenem Online-Wahlversuch persönlich zu besuchen:

✘ ANF 17 Der Wähler muss die Möglichkeit haben, sich zu jedem Zeitpunkt des Wahlzeitraumes zwischen Onlinewahlen und Wahl in einem Wahllokal zu entscheiden. Die Vernetzung der Wahllokale zwecks Abgleich der Wählerlisten ist über dedizierte nicht-öffentliche Netzwerke (kein Internet, kein Virtual Private Network) vorzunehmen, um Distributed Denial Of Service-Attacken auf die Wahllokale auszuschließen.
(Allgemeinheit)

Gleichwohl darf bei einer Dezentralisierung nicht der wesentlich erhöhte Arbeitsaufwand der Administration der dezentralisierten Systeme vernachlässigt werden.

✘ ANF 18 Auch bei einer Dezentralisierung des Systems dürfen keine Ausfallzeiten entstehen. Eine lückenlose kompetente Administration muss auch bei gleichzeitigem Ausfall verschiedener Systeme in verschiedenen Wahllokalen gewährleistet sein.
(Allgemeinheit)

5.5 Transparenz

Soll die Legitimation der gewählten Volksvertreter in den Augen der Wähler nicht durch den Einsatz eines Onlinewahlsystems leiden, so muss dessen Funktionsweise mindestens ebenso transparent sein wie die des jetzigen Systems.

Dabei geht es nicht darum, ob jeder Bürger tatsächlich jeden Aspekt des Systems nachvollzogen hat – die Frage ist, ob er es könnte. Sicherlich ist eine formale Bauartzulassung des Bundesinnenministeriums notwendig, bei der das Ministerium eine Reihe von Gutachten einholt. Dies ist jedoch nicht ausreichend, soll wirkliches Vertrauen in der Bevölkerung aufgebaut werden. Dies kann nur mit einer rückhaltlosen Offenlegung jedes Systemdetails geschehen.

✗ **ANF 19** Eine deutliche Zeit vor dem Beginn des Einsatzes eines Onlinewahl-systems sind

- die Anforderungsdefinition
- die Beschreibung der Architektur in verschiedenen Abstraktionsebenen und mit Erläuterungen für Personen mit unterschiedlichem Kenntnisstand
- die Beschreibung des eingesetzten Wahlprotokolls
- eine umfassende Sicherheitsrisiko-Analyse
- der vollständige Source-Code der Onlinewahl-Software
- der vollständige Source-Code der sonstigen verwendeten Software (Betriebssystem, Compiler, System-Tools, etc.)
- sämtliche Konfigurationsdateien der Onlinewahl-Software und des Betriebssystems
- die exakten Spezifikationen der eingesetzten Hardware

für jedermann offen zugänglich gemacht zu werden.
(Allgemeinheit, Gleichheit, Geheimheit)

Eine Geheimhaltung der eingesetzten Software und Systemkonfiguration wäre kontraproduktiv, da dadurch dem Bürger der Eindruck vermittelt würde, dass die involvierten Behörden selber der Auffassung sind, das System sei unsicher und nur mittels Minimierung des Personenkreises, der Zugriff auf die Systeminforma-

tionen hat, abzusichern. Es stellte sich dann aber die Frage, wie hoch das Risiko sei, dass die eingeweihten Personen ihr Wissen über die Systemdetails nutzen, um Wahlen zu manipulieren und damit den Staat an einer seiner empfindlichsten Stellen zu treffen.

Im Falle einer Geheimhaltung des Source-Codes kann die zertifizierende Behörde auch in einen einseitigen Druck geraten: Die Herstellerfirma und das Bundesinnenministerium haben ein Interesse an der Durchführung eines möglicherweise bereits anvisierten Projektes. Nur wenn der Source-Code offen gelegt wird, steht die zertifizierende Behörde auch unter einem gegensätzlichen Druck: Die Striktheit des durchschrittenen Zertifizierungsprozesses kann von jedem interessierten Bürger beobachtet werden.

Eine Herstellerfirma muss in erster Linie an die Interessen ihrer Aktionäre denken. Deshalb muss es zwingend das ökonomische Ziel eines Herstellers sein, gerade nur so viel Arbeitszeit in die Qualitätsverbesserung ihres Produktes zu investieren, wie notwendig ist, damit sie die Ausschreibung um das Online-Voting-System gewinnt. Diesen ganz natürlichen Interessen der Herstellerfirma muss ein Kontrollsystem entgegengestellt werden, dass derart viel Druck erzeugt, dass die Motivationen des Herstellerunternehmens, möglichst wenig in die Qualität des Voting-Systems zu investieren, neutralisiert werden.

Auch muss die Möglichkeit vorgesehen werden, die öffentlich gemachte Systemkonfiguration zu überprüfen. Das heißt, es muss nachgewiesen werden, dass tatsächlich der Programmcode und die Konfiguration die publiziert wurde auf den entsprechenden Rechnern läuft.

✗ ANF 20 Es muss interessierten Bürgern oder Organisationen die Möglichkeit eingeräumt werden, sich davon zu überzeugen, dass das eingesetzte Onlinewahlssystem bitgenau mit dem übereinstimmt, von dem vorgegeben wird, dass es eingesetzt wird. Dabei ist sicherzustellen, dass bei diesen Überprüfungen eine Manipulation des Systems ausgeschlossen wird.
(Allgemeinheit, Gleichheit, Geheimheit)

Die aufgeführten Anforderungen wurden an Hand von Beobachtungen der Eigenschaften des aktuellen papierbasierten Systems ermittelt und haben keinerlei Bezug zur aktuellen Fassung der Bundeswahlgeräteverordnung. Sicherlich sind einige dieser Anforderungen nur unter größten Anstrengungen – und damit mit ganz enormem finanziellen Aufwand zu erfüllen. Sie stellen jedoch eine Teilmenge der

absolut notwendigen technischen Anforderungen dar, die an ein Onlinewahlssystem für staatliche Volksvertreterwahlen zu stellen sind, soll sich die Qualität gegenüber dem jetzigen System nicht verschlechtern. Sicherlich gibt es noch eine große Zahl weiterer notwendiger Anforderungen.

6 Mögliche Novellierung der BWahlGV

Die Bundeswahlgeräteverordnung ist in ihrer heutigen Form nicht ausreichend auf die Erfordernisse von Internet-Voting-Systemen ausgelegt.

Zum Einen sind einige dort gestellten Anforderungen übertrieben. So ist es z.B. möglicherweise nicht dringend notwendig, dass eine unterbrechungsfreie Stromversorgung von Wahlgeräten gefordert wird (siehe Anlage 1 zu §2, Abschnitt B 2.5), auch falls diese in Form eines PCs im Wohnzimmer des Wählers stehen. Hier könnte es ja u.U. ausreichen im Falle eines Stromausfalls ein entsprechendes Angebot im örtlichen Wallokal bereitzuhalten.

Auf der anderen Seite sind die Anforderungen der aktuellen Bundeswahlgeräteverordnung nicht annähernd ausreichend, soll ein Internet-Voting-System eingeführt werden, welches die Qualität der jetzigen papierbasierten Wahl nicht verringern soll.

Soll ein Internet-Voting-System eingeführt werden, so ist es also notwendig, für eine entsprechende Neufassung der Verordnung zu sorgen.

Eine besonders vernünftige Anforderung in der aktuellen Fassung der Bundeswahlgeräteverordnung stellt jedoch die Forderung nach einer Rückwirkungsfreiheit (siehe Anlage 1 zu §2, Abschnitt B 2.4) dar: „Bei Anschluss von nicht zur Bauart gehörenden Komponenten arbeitet das Wahlgerät rückwirkungsfrei.“. Bleibt diese Anforderungen in einer etwaigen novellierten Fassung der Verordnung erhalten, so ist demnach jegliche Manipulation des Wahlvorgangs durch Teile des Internets, die nicht zum Voting-System gehören ausgeschlossen.

7 Bemerkungen zur Konzeption von Internet-Wahl-systemen

Im Folgenden sollen einige Bemerkungen zur Konzeption von Internet-Voting-Systemen gemacht werden, die sich mit häufig anzutreffenden Denkfehlern beschäftigen.

7.1 Online-Voting vs. Online-Banking

Um die Sicherheit des Clients zu gewährleisten, muss bei der heutigen Architektur der meisten Anwender-Rechner die Sicherheit in vier Bereichen kontrolliert werden:

1. Hardware – Die Hardware und ihre physische Sicherheit stellt die Grundvoraussetzung an ein sicheres System. Denkbare Angriffsmöglichkeiten könnten u.a. Wanzen sein, die Tastatureingaben per Funk weitergeben, Monitorabstrahlungen, die aufgezeichnet werden, oder Designfehler in der Architektur, die es Angreifern ermöglichen, Zugang zu Daten oder Kontrolle über Software zu erlangen.
2. BIOS – ursprünglich als „Basic Input Output System“ bezeichnet, war das BIOS ein System, das dem Betriebssystem eine einheitliche Schnittstelle zu unterschiedlichen Hardwareprodukten bieten sollte. Heute dient es dazu, den Boot-Loader eines Systems zu starten, der wiederum das Betriebssystem eines Rechners startet. Durch Bestrebungen der BIOS-Hersteller, ihre Produkte vor dem Aussterben zu bewahren, werden jedoch immer mehr Funktionalitäten in das BIOS eingebaut. So plant der Hersteller Phoenix eine Integration eines Web-Browsers in sein BIOS. Denkbar sind also in Zukunft möglicherweise auch Angriffsmöglichkeiten auf das BIOS.
3. Betriebssystem und sonstige Software-Umgebung – Das Betriebssystem und sämtliche Software, die neben dem eigentlichen Voting-Client auf dem Rechner läuft ist ebenfalls angreifbar. Solange der Anwender seine sonstige Software nicht abgesichert hat und deren Funktionsweise bis ins Detail kennt, kann der Voting-Client keine Annahmen über seine Umgebung machen.
4. Anwendungssoftware – Die Voting-Client-Software selber bietet sicherlich die meisten Möglichkeiten eines Angriffs.

Oftmals wird beim Entwurf von internetbasierten Voting-Systemen die Notwendigkeit der Gewährleistung der Sicherheit des Systems in den ersten drei Schichten nicht ernst genommen. Teilweise wird dem Wähler eine Java-Software zur Verfügung gestellt, dass dieser mit Hilfe seines Web-Browsers aus dem Internet laden muss und mit Hilfe seiner selbst installierten Java Virtual Machine ausführen muss. Dabei werden eine ganze Reihe von Annahmen über den Browser, die Java Virtual Machine und das Betriebssystem des Wählers gemacht. Jede dieser Komponenten kann jedoch bereits vorab von Angreifern manipuliert worden sein. Diese Manipulation könnte im großen Stil automatisiert erfolgen.

Das gleiche Risiko wird z.B. beim Online-Banking eingegangen. Die Bank und der Kunde verständigen sich dabei darauf, dass der Kunde ein ordentlich gewartetes System zur Verfügung stellt, auf dem er die Online-Banking-Software nutzt. Ist dies nicht der Fall und entsteht ein Schaden durch einen Angreifer, so liegt dies in der Verantwortung des Kunden – nicht der Bank. Beim eVoting können die Verantwortungen nicht analog verteilt werden, da ein erfolgreicher Angriff nicht nur den einzelnen Wähler, dessen Stimmzettel manipuliert wurde, betrifft, sondern – erfolgt der Angriff bei einer Vielzahl von Wählern im großen Stil – den gesamten Staat schädigt. Es liegt also in der Verantwortung der Betreiber des Wahlvorgangs für eine ausreichende Sicherheit der Rechnersysteme der Wähler zu sorgen.

7.2 Dezentralisierung und Online-Wahlen

Die Dezentralisierung des Wahlvorgangs ist zwar bei papierbasierten Wahlsystemen ein Sicherheitsvorteil, nicht jedoch bei internetbasierten. Da anzunehmen ist, dass jedes dezentrale System eine ähnliche Funktionsweise hat, macht es also für einen Angreifer kaum einen Unterschied ein Zentralsystem, oder automatisiert eine große Anzahl dezentraler Systeme anzugreifen.

7.3 Smartcards

Seit einigen Jahren sind so genannte Smartcards oder Chip-Karten auf dem Markt. Es handelt sich um rechteckige Plastik-Karten, die das vertraute Format einer Kreditkarte, jedoch in ihrem Innern einen Mikrochip eingebaut haben. Dieser oder diese Mikrochip(s) verfügen über eine recht geringe Rechenleistung und ein klein wenig festen Speicher (ROM), Arbeitsspeicher (RAM), sowie veränderbaren Festspeicher (EPROM, EEPROM). Über auf der Oberfläche der Karte angebrachte elektrische Kontakte können derartige Karten mit der Außenwelt kommunizieren.

Smartcards sind zunächst prinzipiell universell einsetzbar. Sehr sinnvolle Einsatzmöglichkeiten sind die Verwendung als Zahlungsmittel, wie etwa als Telefonkarte und als Geld-Karte der Sparkassen, als Authentifikationswerkzeug bei Türschlössern und als Speichermedium, wie etwa bei Versicherten-Karten, die die Krankenkassen in Deutschland ausgeben.

Vielfach wird der Einsatz von Chip-Karten zur Identifizierung des Wählers bei der Entwicklung von Voting-Systemen propagiert, oder sogar gefordert, wie durch die Initiatoren des Projektes i-vote [Ott02]. Im EU-Projekt Cybervote wird sogar der Einsatz von Chip-Karten zur Wähleridentifizierung als Anforderung festgeschrieben [Cyb00b] S.19, ohne dass die Notwendigkeit hierzu begründet wird.

Der Grund für diese Empfehlungen ist psychologischer Natur: Es erscheint zunächst enorm sicher, ein geschlossenes Hardwaregerät einzuführen, das den Schlüssel des jeweiligen Wählers hält. Damit lässt sich dann natürlich sehr gut Marketing betreiben und potentiellen Wählern und auch Entscheidungsträgern zum Einsatz dieses Systems eine Sicherheit des angebotenen Voting-Systems suggerieren.

Technologisch gesehen bietet der Einsatz von Smartcards im Bereich der Wähler-Authentifikation bei elektronischen Wahlen, im Gegensatz zum Einsatz als elektronisches Zahlungsmittel, etc. jedoch keine zusätzliche Sicherheit gegenüber anderen Verfahren wie z.B. PIN/TAN-Verfahren dar. Zwar wird die Signatur auf der Chip-Karte selber vorgenommen, somit ist es nicht möglich, den Schlüssel, der auf der Chip-Karte ist, zu stehlen. Jedoch weiß der User immer noch nicht, was er signiert. Der Inhalt des Wahlzettels, der auf dem Bildschirm angezeigt wird, muss nicht mit dem Wahlzettel übereinstimmen, der signiert wird. Diese Annahmen können im Zeitalter von Trojanern, Viren und Würmern nur dann gemacht werden, wenn die Annahme, dass der Client-Rechner, an dem die Chip-Karte angeschlossen ist, ausreichend abgesichert ist, begründet werden kann. Bei privaten PCs ist dies nur in Einzelfällen der Fall, weshalb der Einsatz von Chip-Karten keine zusätzliche Sicherheit erbringt.

Sicherlich flößt es dem Wähler zunächst mehr Vertrauen in die Sicherheit ein, wenn er zur Wahl eine zusätzliche Hardware benötigt. Die Frage ist aber, was geschieht, wenn in der breiten Öffentlichkeit publik wird, dass die Sicherheit immer noch von der des angeschlossenen PCs abhängt. Das Vertrauen in das Voting-System könnte wohl deutlich abnehmen. Die Wirkung des Marketingeffekts könnte somit also vorübergehend sein.

Um eine Client-seitige Sicherheit garantieren zu können, muss das gesamte System, auf dem das Ausfüllen des Wahlzettels vorgenommen wird, kontrolliert werden. Dies ist nicht allein mit einer reinen Chip-Karten-Lösung zu erreichen, des-

sen Einführung pro Wähler zudem beträchtliche Kosten verursacht.

Ein tatsächlicher möglicher Grund für den Einsatz von Smartcards kann der Wunsch sein, Signaturen nach dem Signaturgesetz (SigG) durchführen zu wollen. Da die BWahlGV jedoch zur Einführung von Internetwahlen sowieso novelliert werden muss und elektronische Signaturen auch jetzt noch nicht in der BWahlGV verankert sind, würde es sich hier lediglich um politische Motivationen handeln (beispielsweise, um die Verbreitung von Smartcard-Terminals bei Heimanwendern zu steigern) – nicht jedoch um technische.

7.4 Bootfähiges System auf CD

Eine Lösung für die Gewährleistung der Sicherheit des Betriebssystems, sowie der gesamten weiteren Software-Umgebung, ist das Starten des Voting-Clients von einer bootfähigen CD, die wohlkonfiguriert ist. Auf diese Weise ist die Wahlbehörde in der Lage, die vollständige Software-Umgebung des Wählers zu kontrollieren. Dieser hat nicht mehr die Verantwortung, selber für die Sicherheit seiner Systemkonfiguration zu sorgen.

Hier ergeben sich jedoch wieder neue Schwierigkeiten: So muss während des Bootvorgangs von der CD eine automatische Hardwareerkennung gewährleistet sein. Gelingt dies nicht bei allen Rechnertypen erfolgreich, könnte man den Allgemeinheitsgrundsatz der Wahl als gefährdet ansehen.

Seit einiger Zeit werden selbstbootende CDs für eine ganze Reihe von Anwendungen eingesetzt. Typischerweise wird hierfür ein angepasstes KNOPPIX [Kno04] eingesetzt.

8 Existierende Prototypen für Internetwahlsysteme

8.1 Cybervote

Cybervote ist ein von der Europäischen Union finanziertes Projekt, welches mit einem Budget von 3.24 Mio.€ und einer Arbeitszeit von 27 Mannjahren ausgestattet ist. Die Zielsetzung von Cybervote ist es, einen Prototypen für ein universelles Voting-System zum Einsatz bei staatlichen Volksvertreter-Wahlen zu erstellen. Der Fokus dieses Projektes ist auf ehrgeizige Ziele zur praktischen Einsetzbarkeit gerichtet. So soll der Wähler von jedem etablierten Betriebssystem und Browser

aus wählen können. Zudem soll es möglich sein, auch Nokia Communicators als Wahl-Client-Rechner einsetzen zu können. Diese Entscheidung wurde getroffen, da die Firma Nokia Teilnehmer des Projektes war.

Nach Auskunft des Projektkoordinators Stéphane Brunessaux ist Cybervote trotz des Fokuses auf die gute Benutzbarkeit durch den Wähler jedoch leider nicht für einen realen produktiven Einsatz konzipiert worden:

„The project was about developing a research prototype and about conducting election trials. The project is not about developing an industrial product to be used daily.“

8.1.1 Dokumentation

Das Projekt ist umfangreich dokumentiert [Cyb03]. Jedoch fehlen leider noch einige wesentliche Details. Der Source-Code soll nach Auskunft des Projektkoordinators Stéphane Brunessaux nicht veröffentlicht werden. Da es sich ja lediglich um eine Technologiestudie handelt, ist dies dann wohl auch verschmerzbar.

Es werden recht detaillierte Beschreibungen über Möglichkeiten des Betriebs von Cybervote gegeben. Insbesondere werden auch Überlegungen zur Konfiguration der Umgebung von Cybervote angestellt.

8.1.2 Praxistauglichkeit

Cybervote wurde bereits bei einigen rechtsgültigen Testwahlen eingesetzt. Da das System äußerst flexible Anforderungen an Client-Rechner stellt, ist es durch sehr breite Wählergruppen einsetzbar. Der Umstand, dass der Wähler selber die Installation des Clients und des Java Runtime Environments sowie die korrekte Konfiguration des Rechners vornehmen muss, schränkt diesen Vorteil wieder ein wenig ein.

Entscheidend für die konkrete Praxistauglichkeit bleibt jedoch die vollständige Offenlegung des Source-Codes.

8.2 i-vote

Die Forschungsgruppe Internetwahlen hat in den Jahren 1999 und 2000 finanziert durch die Bundesregierung das Voting-System i-vote [For04] entwickelt, welches von der Firma ivl GmbH Leverkusen weiterentwickelt wurde. Es soll auf einem blinden Beglaubigungsverfahren basieren.

Die Forschungsgruppe Internetwahlen legt sehr großen Wert auf die Praxistauglichkeit ihres Systems. Insbesondere legen sie ein großes Augenmerk auf die rechtliche Realisierbarkeit der Einführung von i-vote bei den Wahlen zu den Volksvertretungen in der Bundesrepublik. Aus diesem Grund wurde bei der Entwicklung großer Wert auf die Bezugnahme auf das Signaturgesetz (SigG), gelegt [Bun01]. Für die rechtsgültige Signatur ist im Signaturgesetz die Verwendung von Smart-Cards vorgesehen.

Mit dem System i-vote wurden bereits eine Reihe von – teilweise rechtsgültigen – Testwahlen durchgeführt. So wurde es u.a. zur Online-Personalratswahl im Landesbetrieb für Datenverarbeitung und Statistik (LDS) Brandenburg [LDS03] im Mai 2002 und zu Wahlen zum Betriebsrat bei T-Systems CSM [T-S03] ebenfalls im Mai 2002 eingesetzt.

Inzwischen haben sich die Forschungsgruppe Internetwahlen, die Firma T-Systems CSM Darmstadt (welche zusammen mit Daimler Chrysler auch die Firma Toll-Collect (Mautsystem) betreibt), die Firma ivl GmbH Leverkusen, sowie der Landesbetrieb für Datenverarbeitung und Statistik Brandenburg zur Forschungsgruppe W.I.E.N. (Wählen in elektronischen Netzen) zusammengeschlossen [For03]. Das Projekt der Forschungsgruppe wird vom Bundesministerium für Wirtschaft und Technologie (BMWI) maßgeblich gefördert.

8.2.1 Dokumentation

Weitergehende Architekturdetails, sowie der komplette Source-Code wurden nicht offen gelegt. Auch in einem Bericht [Cyb00a], S. 58 des Projektes Cybervote 8.1 wurde bereits im Jahr 2001 die mangelnde Transparenz des Systems kritisiert. Prof. Dr. Otten von der Forschungsgruppe Internetwahlen verweist auf sich im Verlauf befindliche Patentanmeldungen, die abgewartet werden müssen, bevor Architekturdetails veröffentlicht werden können.

8.2.2 Praxistauglichkeit

Nach den ersten informellen Gehversuchen wie das Projekt „Wahlkreis 329“ [Ott98] wurden inzwischen bereits einige konkrete Wahlen (z.B. Wahlen der Vertreter im Studierenden-Parlament) durchgeführt, die tatsächlich eine rechtsgültige Wirkung hatten.

Entscheidend für die konkrete Praxistauglichkeit bleibt jedoch die vollständige Offenlegung des Source-Codes.

8.3 Polyas

Die Firma Micromata entwickelte das System Polyas [Mic04], welches bei der ersten rechtsgültigen Vorstandswahl eines Vereins in der BRD, zusammen mit dem System i-vote eingesetzt wurde.

Auch die Firma Micromata veröffentlicht praktisch keinerlei Architekturdetails zu ihrer Software.

9 Politische Motivationen

Im Folgenden sollen einige politische Motivationen aufgeführt werden, die bei der Entscheidung zur Einführung eines internetbasierten Voting-Systems bei staatlichen Wahlen eine Rolle spielen könnten.

9.1 Aktuelle politische Situation

Spätestens seit dem Jahr 2001 verfolgt die Bundesregierung das Ziel, stufenweise internetbasierte Volksvertreter-Wahlen einzuführen. Dazu wurde bereits im Oktober 2000 eine Arbeitsgruppe Onlinewahlen im Bundesinnenministerium eingerichtet [Kör01].

Es ist geplant, bis zum Jahr 2006 eine Vernetzung der Wahllokale untereinander zu erreichen, so dass es bei der nächsten Bundestagswahl eine zentrale bundesweite Datenbank der Wahlberechtigungen gibt, damit jeder wahlberechtigte Bürger ohne Anmeldung in jedem beliebigen Wahllokal seine Stimme abgeben kann.

Unklar ist, in welchem Tempo nach dem Jahr 2006 ein internetbasiertes Voting-System eingeführt werden soll.

9.2 Modernes Image für die Bundesregierung / die BRD

Ein möglicher Anreiz zur Einführung eines Internet-Voting-Systems könnte der Wunsch sein, das Wahlverfahren zu modernisieren, um damit ein moderneres Image für die Bundesregierung und die BRD generieren zu können.

Da immer mehr Verwaltungsakte des Staates automatisiert abgewickelt werden, erscheint es selbstverständlich zeitgemäß zu sein, auch Wahlen elektronisch durchführen zu wollen.

Da immer mehr Bankkunden ihre Bankgeschäfte online abwickeln, wird es auch sehr schwer werden zu kommunizieren, weshalb eine Internetwahl technisch schwierig zu realisieren ist.

9.3 Lobbying von Herstellern

Jedes politische Thema unterliegt dem Einfluss von Lobbyisten. Im Bereich des Internet-Votings wird es sich wohl um Herstellerfirmen von Voting-Systemen handeln, deren Interesse es naheliegenderweise ist, die Bundesregierung zum Einsatz Ihrer Produkte zu bewegen.

9.4 Bereits getätigte Investitionen und Bemühungen

Ein weiteres Argument sind die getätigten Investitionen der Bundesregierung. So wurde die Forschungsgruppe Internetwahlen zur Erstellung des Systems i-vote finanziell gefördert. Inzwischen fördert das Bundesministerium für Wirtschaft und Arbeit die Forschungsgruppe W.I.E.N., an der unter anderem die Forschungsgruppe Internetwahlen und eine Tochter der Deutschen Telekom beteiligt ist. Auch existiert die Arbeitsgruppe Onlinewahlen im Bundesinnenministerium. So könnte sich die Bundesregierung also möglicherweise von der Opposition unter Druck gesetzt fühlen, einmal begonnene Bestrebungen auch bis zum Ende durchzuführen.

9.5 Dämpfer: Toll-Collect

Ein möglicher politischer Dämpfer für die Einführung eines aufwendigen Internet-Voting-Systems ist natürlich der Fall Toll-Collect (Mautsystem), der zeigt, welche enormen Schwierigkeiten und Risiken, technologisch wie politisch, ein derartiges Großprojekt erbringen kann.

Interessant ist, dass die Firma T-Systems zusammen mit Daimler Chrysler die Firma Toll-Collect betreibt. T-Systems beteiligt sich nun auch zusammen mit der Forschungsgruppe Internetwahlen an W.I.E.N., um gemeinsam das i-vote System weiter voran zu bringen.

9.6 Problem: Kostenbegrenzung vs. Qualität

Bei jedem technischen Großprojekt sind natürlich die Kosten ein entscheidender Faktor. Die Gefahr bei der Einführung von Internetwahlen besteht darin, dass zunächst darüber entschieden wird, ob es zu einer derartigen Einführung kommen soll, um danach um technologische Details zu verhandeln. Sollte es zu dieser Vorgehensweise kommen, so ist es selbstverständlich notwendig, dass auch die Anforderungen an ein Internet-Voting-System in einem vernünftigen Verhältnis zu den Kosten stehen müssen, demnach also möglicherweise die aktuellen Qualitätsstandards einer Wahl abgesenkt werden müssen.

Bei einer solchen Diskussionsführung wird außer Acht gelassen, dass es zur Zeit ein hervorragend funktionierendes papierbasiertes Wahlsystem gibt, das jahrzehntelang erfolgreich erprobt wurde.

Es ist somit unbedingt darauf zu achten, dass vor der Entscheidung zur Einführung eines Internet-Voting-Systems die Politik einen festen Anforderungskatalog verabschiedet und sich Gedanken über die Realisierbarkeit des Projektes macht. Es besteht keinerlei zwingende Notwendigkeit zur Absenkung der Qualitätskriterien für allgemeine, unmittelbar, freie, gleiche und geheime Wahlen, da sich bereits ein hervorragendes System im Einsatz befindet.

10 Häufig gehörte Argumente

An dieser Stelle soll einigen häufig gehörten Argumenten entgegnet werden.

Ökonomische Realitäten Argument: Bei der Definition von Anforderungen an Voting-Systeme für staatliche Volksvertreter-Wahlen müssen auch die ökonomischen Realitäten gesehen werden: Es ist einfach wirtschaftlich nicht machbar, extreme Sicherheits- und Transparenzforderungen zu erfüllen.

Erwiderung: Bei dieser Argumentation wird von der Prämisse ausgegangen, dass es unbedingt zur Einführung von Online-Wahlsystemen für staatliche Volksvertreterwahlen kommen soll. Dabei wird außer Acht gelassen, dass es bereits ein hervorragend funktionierendes Wahlsystem gibt, das jahrzehntelang erprobt wurde. Es ist nicht sinnvoll, sich erst für den Einsatz von elektronischen Wahlsysteme zu entscheiden und erst danach ökonomische Rahmenbedingungen und technische Aspekte zu bedenken. Diese Aspekte sind bereits in die Diskussion Online-Wahlsystem vs. Papier-Wahlsystem mit einzubeziehen.

Interessant ist, dass oftmals gleichzeitig suggeriert wird, mit der Einführung von Online-Wahlsystemen Kosten zur Wahldurchführung einsparen zu können.

Testwahlen Besonders die Forschungsgruppe Internetwahlen setzt Testwahlen auch als Instrument ein, um die korrekte Funktionsweise und die Sicherheit ihres Wahlsystems zu demonstrieren. Sicherlich sind Testwahlen sehr wertvoll, um die einfache Bedienbarkeit der Software durch den Wähler und sozialwissenschaftliche Aspekte des Wählerverhaltens untersuchen zu können. Jedoch helfen sie nicht bei der Bemühung weiter, die Sicherheit und Korrektheit der Software bewerten zu wollen. Eine erfolgreiche Testwahl zeigt lediglich an, dass das System Eingaben durch den Wähler entgegengenommen hat und schließlich ein Ergebnis veröffentlicht hat. Das Ergebnis einer erfolgreichen Testwahl kann beliebig manipuliert worden sein, ohne dass die Wahlbetreiber dies bemerkt hätten. Die einzige Methode, die Korrektheit eines Ergebnisses nachzuweisen ist der Einsatz eines universell verifizierbaren Wahlprotokolls. Jedoch ist nicht davon auszugehen, dass die Forschungsgruppe Internetwahlen für das System i-vote ein solches einsetzt.

Aus diesem Grund ist es notwendig, dass der vollständige Source-Code eines Internet-Wahlsystems veröffentlicht wird – auch lange vor dessen Einsatzes bei einer Bundestagswahl.

Vertrauensbildung mittels paralleler Möglichkeit zur Papierwahl Argument: Um die Allgemeinheit der Wahl zu gewährleisten, ist es sowieso notwendig, parallel zu einer Internetwahl immer noch papierbasierte Wahlen in Wahllokalen durchzuführen, da nicht jeder Bürger über einen Internetanschluss

verfügt. Deshalb ist es kein Problem, wenn einige Bürger kein Vertrauen in die korrekte Durchführung der Internetwahl haben. Diese können ja immer noch ihre Stimme in einem Wahllokal abgeben und so vollkommen sicher sein, dass diese auch gezählt wird.

Erwiderung: Es ist nicht ausreichend, dass man sich sicher sein kann, dass seine im Wahllokal abgegebene Stimme korrekt gezählt wurde. Die bei der Wahl gewählten Volksvertreter bestimmen über die politischen Geschicke der gesamten Gesellschaft. Wird bei dem internetbasierten Teil der Wahl ein Wahlbetrug vorgenommen, so betrifft das Ergebnis auch diejenigen, die ihre Stimme papierbasiert abgegeben haben.

Vertrauensbildung durch Gewöhnung und durch Werbemaßnahmen

Argument: Um das notwendige Vertrauen in die korrekte Arbeitsweise eines einzuführenden Internetwahlsystems in der Wahlbevölkerung zu schaffen, ist es zweckmäßig zuvor möglichst viele Testwahlen sowie Werbemaßnahmen durchzuführen, um die Bürger an den Gedanken der Internetwahl zu gewöhnen, damit auf diese Weise das Vertrauen wächst.

Erwiderung: Selbstverständlich handelt es sich bei Vertrauen um ein psychologisches Phänomen, welches auch mit psychologischen Mitteln (wie Testwahlen und Werbung) angegangen werden muss. Dies kann jedoch erst ein zweiter Schritt sein: Zunächst muss zweifelsfrei feststehen, dass das System technologisch einwandfrei arbeitet, damit ein Debakel bei einer real durchgeführten Wahl zweifelsfrei ausgeschlossen werden kann. Kommt es zu einem offensichtlichen Wahlbetrug, so helfen die besten Werbemaßnahmen und Testwahlen aus der Vergangenheit nicht mehr weiter: Ein Teil der Bevölkerung wird vermutlich die Wahl akzeptieren, ein anderer wieder nicht und es kann zu einem großen Streit um die Zusammensetzung des jeweils gewählten Parlaments kommen. Schließlich ist es möglich, dass Bevölkerungsgruppen die Legitimität des jeweiligen Parlaments und damit auch dessen Entscheidungen anzweifeln – unabhängig von den Entscheidungen des Bundeswahlleiters und der Wahlprüfungskommission.

Somit wird klar, dass es sich bei den vertrauensbildenden Maßnahmen zwar um sinnvolle Methoden handelt, die Einführung eines Internetwahlsystems politisch durchsetzbar zu machen. Jedoch darf nicht vergessen werden, dass zuvor jegliche technologischen Fehler und Unzulänglichkeiten mit absoluter Sicherheit ausgeschlossen werden müssen, will man nicht die Funktionstüchtigkeit unseres politischen Systems aufs Spiel setzen.

Eine ähnliche Auffassung vertreten auch die Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Ullmann, Koob und Kelter [UKK01]:

„Insbesondere ist ein Vorgehen nach dem Motto „Erfahrung und Gewöhnung schafft Vertrauen“ bei der Einführung eines neuen Wahlverfahren sehr gefährlich, weil Fehlschläge oder Sicherheitsmängel im Umfeld von politischen Wahlen sehr negative Auswirkungen haben werden. Als Beispiel dafür seien die letzten Präsidentschaftswahlen in Amerika genannt. Die Autoren regen deshalb ein sehr umsichtiges Vorgehen bei der Einführung eines neuen Wahlverfahrens an.“

11 Empfehlungen an die Bundesregierung und den Gesetzgeber

Im Folgenden sind Empfehlungen aufgeführt, die der Autor dieser Broschüre dem Bundesinnenministerium und dem Gesetzgeber gibt, mit dem Ziel, dass bei der Einführung eines Onlinewahlsystems bei den staatlichen Volksvertreterwahlen nicht die Korrektheit des ermittelten Wahlergebnisses und die Qualität der Einhaltung des Wahlheimnisses gegenüber der aktuellen Situation vermindert werden möge.

Das Bundesinnenministerium und der Gesetzgeber möchten bitte im Falle des Wunsches der Einführung von Onlinewahlssystemen dafür sorgen, dass

- 1. eine klare (vor allem zeitliche und argumentative) Trennung zwischen der Festlegung eines Zertifikationsprozesses für Onlinewahlssysteme und der Entwicklung eines solchen Systems gezogen wird.** Zunächst sollte eine entsprechende Novellierung der BWahlGV vorgenommen werden. Erst danach und unabhängig davon sollten sich Gedanken über die ökonomische Realisierbarkeit der Einführung eines Onlinewahlsystems gemacht werden, welches die in der BWahlGV festgesetzten Erfordernisse erfüllt.
- 2. bei einer etwaigen Novellierung der BWahlGV das Niveau der Sicherheit bei der Ergebnisermittlung und die Transparenz der Ergebnisermittlung für den Wahlbürger nicht gegenüber dem jahrzehntlang bewährten aktuellen, papierbasierten System vermindert wird.** Um dies zu erreichen müssen zwingende Anforderungen an ein Onlinewahlssystem, welches zertifiziert werden will in der BWahlGV verankert werden, die u.a. mindestens die Anforderungen 1–20 aus Abschnitt 5 dieser Broschüre umfassen.

3. **der Prozess der Findung eines Entwurfes zur Novellierung der BWahlGV für jedermann öffentlich einsehbar stattfindet.** Wäre dies nicht der Fall, so bestünde die Gefahr, dass einzelne Protagonisten, wie z.B. die Forschungsgruppe Internetwahlen, oder das Konsortium W.I.E.N. unter Ausschluss der Öffentlichkeit Einfluss auf die Entwürfe zu den Gesetzesänderungen nehmen, ohne dass die breite Öffentlichkeit Einsicht in diesen Prozess nehmen kann. Im Gegensatz zur Einführung von anderen technischen Systemen, wie z.B. das Maut-Erfassungssystem der Firma Toll-Collect hat die Einführung eines Onlinewahlsystems einen sehr großen Einfluss auf einen unserer zentralen Stützpfeiler unseres Gesellschaftssystems – der Demokratie. Vorbereitende Schritte wie Gesetzesänderungen bedürfen daher einer breiten gesellschaftlichen Diskussion – auch wenn es um technische komplizierte Sachverhalte geht.
4. **bei der Diskussion um die Einführung von Onlinewahlssystemen nicht vergessen wird, dass es in der Bundesrepublik Deutschland ein seit Jahrzehnten bewährtes und hervorragend funktionierendes papierbasiertes Wahlsystem gibt.** Bei der Argumentation zur Einführung eines Onlinewahlsystems ist also darauf zu achten, ob die Vorteile eines Onlinewahlsystems die dadurch auch neu geschaffenen Nachteile tatsächlich überwiegen. Insbesondere ist zu bedenken, dass die aktuelle, vollständige Transparenz des papierbasierten Systems entscheidend zur Akzeptanz des durch den Bundeswahlleiter festgestellten Wahlergebnisses in der Bevölkerung beiträgt. Diese Akzeptanz des Wahlergebnisses ist für das Funktionieren des politischen Systems der BRD von entscheidender Bedeutung. Ihr wurde lediglich deswegen in der Vergangenheit keine große Relevanz beigemessen, weil das existierende System bisher so transparent, einfach und reibungslos funktionierte.

12 Zusammenfassung

Arbeitsgruppe Onlinewahlen des BMI Spätestens seit dem Jahr 2001 verfolgt die Bundesregierung das Ziel, stufenweise internetbasierte Volksvertreterwahlen einzuführen. Dazu wurde bereits im Oktober 2000 eine Arbeitsgruppe Onlinewahlen im Bundesinnenministerium eingerichtet. Schon bei den nächsten Bundestagswahlen soll es zu einer Vernetzung der Wahllokale kommen, damit es mit Hilfe einer zentralen Datenbank der Wahlberechtigungen ermöglicht wird, dass jeder Wähler in einem beliebigen Wahllokal sein Kreuz machen kann.

Aktuelles System funktioniert hervorragend Das aktuelle papierbasierte Wahlsystem funktioniert hervorragend. Es basiert auf einer Dezentralisierung und einer vollständigen Transparenz für den Bürger.

Notwendiges Vertrauen der Wahlbürger in das Ergebnis Oberstes Ziel eines Wahlsystems ist die Schaffung eines großen Vertrauens der wahlberechtigten Bürger in die Einhaltung der Grundsätze Allgemeinheit, Unmittelbarkeit, Freiheit, Gleichheit und Geheimheit der Wahl. Das Vertrauen der Wahlbürger in die korrekte Ermittlung des Ergebnisses bildet einen zentralen Stützpfeiler unseres politischen Systems.

Verhältnisse in den USA In den USA kam es in der Vergangenheit bereits zum Einsatz von elektronischen Wahlmaschinen, die auf einfachste Weise eine Manipulation des Wahlergebnisses zuließen (Firma Diebold), bzw. die absurd falsche Ergebnisse lieferten (deutlich mehr abgegebene Stimmen als Wahlberechtigte), (Firma Microvote). Dabei kommen jeweils Closed-Source-Produkte zum Einsatz, dessen Funktionsweisen von den Herstellern geheim gehalten werden.

Gefahr: i-vote Die Forschungsgruppe Internetwahlen entwickelte das Internet-Voting-System i-vote. Zu diesem System wurden praktisch keinerlei Details zur Funktionsweise veröffentlicht. Vielmehr wird versucht, mit einer Reihe von Testwahlen Vertrauen in die korrekte Funktionsweise des Systems zu generieren. Die Bundesregierung förderte dieses Projekt und es besteht sicherlich aus Kostengründen eine enorme Versuchung dieses, lediglich als Prototypen konzipierte System als tatsächliches Produktivsystem einzusetzen.

Gefahr: Absenkung der aktuellen Qualitätsstandards Eine große Gefahr für die Qualität des Wahlsystems der BRD besteht darin, dass es zunächst zu einer Entscheidung für den Einsatz eines Internet-Voting-Systems kommen könnte und sich erst danach Gedanken über die Kosten, notwendigen Anforderungen und Realisierbarkeit des Projektes gemacht werden. Dies würde bedeuten, dass es zu einer Absenkung des aktuell sehr hohen Qualitätsstandards der Wahlen kommen würde, da alles Andere wohl finanziell zu aufwändig wäre.

Notwendigkeit der Offenlegung des Source-Codes Ein Herstellerunternehmen hat das natürliche Interesse, möglichst wenig Arbeitszeit in die Optimierung der Qualität ihres Voting-Systems zu stecken. Eine zertifizierende Behörde wird so lange unter einseitigem Druck stehen, ein System möglichst zu zertifizieren, wie kein Gegendruck vorhanden ist, in dem der breiten Öffentlichkeit der Source-Code des Systems zur Einsicht zur Verfügung steht.

A Literaturtips

Möchte man sich über die technischen Aspekte von elektronischen Wahlen informieren, so ist ein kurzer Überblicksartikel von Phillippsen [Phi01], eine Diplomarbeit von Steinbach [Ste98], eine Doktorarbeit von Schlifni [Sch00], die beide einen guten Überblick über bestehende Wahlprotokolle liefern, sowie die technischen Berichte des Projektes Cybervote [Cyb03] als erste Einstiegsliteratur zu empfehlen. Allgemeine kryptographische Grundlagen stellt Schneier dar [Sch96].

Einen guten allgemeinen Überblick über das Wahlrecht der BRD geben Zicht und Fehndrich [ZF04]. Für die verfassungsrechtlichen Aspekte der Einführung von Internetwahlen für staatliche Volksvertreterwahlen sei das Buch von Will [Wil02], sowie der Artikel von Rüß [Rüß02] empfohlen.

B Wahlprotokolle

Seit mehr als zwanzig Jahren beschäftigt sich die Mathematik und die theoretische Informatik mit der Entwicklung von Wahlprotokollen. Aus diesem Grund gibt es eine große Anzahl von Wahlprotokollen, die sich jedoch überschaubar klassifizieren lassen.

B.1 Protokoll-Eigenschaften

Die Untersuchung folgender Eigenschaften dient zur Bewertung von Voting-Protokollen:

Authentifikation Wird sichergestellt, dass nur Wahlberechtigte an einer Wahl teilnehmen dürfen?

Korrektheit Wird die Korrektheit des Wahlergebnisses sichergestellt?

Übertragungsintegrität Wie wird die Integrität der Nachrichten während ihrer Übertragung gewährleistet?

Nichtvermehrbarkeit Ist es möglich, Stimmzettel zu duplizieren und somit mehrfach abzugeben?

Robustheit Wird sichergestellt, dass kein Teilnehmer in der Lage ist, die Wahl zu unterbrechen oder die Auswertung zu verzögern?

Allgemeinheit Wird sichergestellt, dass jeder Wahlberechtigte auch tatsächlich seinen Stimmzettel abgeben kann – unabhängig von technischen Pannen?

Fairness Wird sichergestellt, dass keine Zwischenergebnisse bekannt werden?

Wahlgeheimnis Wird sichergestellt, dass keine Information über das Stimmverhalten eines Wählers ohne seine Mithilfe bekannt wird?

Unmittelbarkeit Ist die Stimmabgabe unmittelbar? (Unmittelbarkeit setzt Quittungsfreiheit voraus).

Quittungsfreiheit Wird sichergestellt, dass Wähler ihr Stimmverhalten nicht belegen können?

Individuelle Verifizierbarkeit Wie wird sichergestellt, dass jeder Wähler in der Lage ist zu überprüfen, ob seine Stimme korrekt gezählt wurde?

Universelle Verifizierbarkeit Wie wird sichergestellt, dass jedermann in der Lage ist, zu jedem Zeitpunkt die Korrektheit des veröffentlichten Wahlergebnisses zu überprüfen?

Kommunikationskomplexität Wie groß ist die Menge der übertragenen Daten zwischen den einzelnen Teilnehmern?

Effizienz Wie groß ist der Rechenaufwand der einzelnen Wahlteilnehmer?

Skalierbarkeit Wie gut ist die Skalierbarkeit?

Physische Voraussetzungen Werden physikalische Voraussetzungen gemacht?

Flexibilität des Stimmzettel-Formats Welche Arten von Stimmzetteln können verwendet werden?

Ortsunabhängigkeit Ist die Stimmabgabe an einen bestimmten Ort gebunden?

Bei einigen Protokollen werden aus Effizienzgründen lediglich einzelne Eigenschaften untersucht, falls bereits durch sie klar wird, dass sie völlig ungeeignet für den anvisierten Anwendungsbereich sind.

B.2 Bestehende Protokolle

Im Folgenden werden die in der Literatur aufgefundenen Protokolle beschrieben, klassifiziert und bewertet. Diese Darstellung ist in weiten Teilen an Steinbach [Ste98] S. 47–131, Schlifni [Sch00] S.125–177, Cybervote [Cyb02] S. 14–26, Philippsen [Phi01], Prosser und Müller-Török [BSW01] und Mürk [Mür00] S. 33–44 angelehnt. Die Grenzen zwischen den einzelnen Protokoll-Klassen sind nicht immer scharf. Einige Protokolle gehören zu mehreren Klassen. Die Klassifizierung sowie die Bewertung der Protokolle ist an Schlifni angelehnt.

B.2.1 Dezentrale Verfahren

Dezentrale Wahlprotokolle sehen keine Wahlbehörden vor. Die Wahl wird alleine von der Gemeinschaft der Wähler durchgeführt.

Allgemeinheit Durch die fehlende Robustheit ist auch keine Allgemeinheit garantiert.

Authentifikation Es kann eine korrekte Authentifikation sichergestellt werden.

Korrektheit Wenn alle Wähler kooperieren, so ist das Wahlergebnis korrekt.

Übertragungsintegrität Eine Verfälschung der übertragenen Daten kann nachgewiesen und auf den Angreifer zurückverfolgt werden.

Nichtvermehrbarkeit Stimmzettel sind nicht vermehrbar.

Robustheit Die Protokolle sind nicht robust. Sie liefern nur dann ein Wahlergebnis, falls sämtliche Wahlberechtigte ausnahmslos innerhalb einer engen Zeitspanne nahezu gleichzeitig wählen.

Fairness Das Ergebnis wird erst nach Ende der Wahlzeit ermittelt.

Wahlgeheimnis Das Wahlgeheimnis wird gewährleistet.

Unmittelbarkeit Die Unmittelbarkeit kann nicht gewährleistet werden.

Individuelle Verifizierbarkeit Die Korrektheit des Ergebnisses ist individuell verifizierbar.

Universelle Verifizierbarkeit Die Korrektheit des Ergebnisses ist universell verifizierbar.

Effizienz Sowohl die Kommunikationskomplexität, als auch der Berechnungsaufwand sind bei einer großen Anzahl Wähler hoch.

Skalierbarkeit Das System lässt sich praktisch gar nicht skalieren. Wahlen mit mehr als wenigen dutzend Wählern machen keinen Sinn.

Flexibilität des Stimmzettel-Formats Der Einsatz beliebiger Wahlscheine ist möglich.

Wegen der hohen Kommunikationskomplexität und der fehlenden Robustheit kann die Verwendbarkeit von Protokollen aus dieser Klasse für staatliche Volksvertreterwahlen ausgeschlossen werden.

B.2.2 Wahlkarten-Lesesysteme

Seit den 60er Jahren werden in den USA vielerorts Wahlkarten-Lesesysteme eingesetzt. Der Wähler erhält anstelle eines Stimmzettels eine Wahlkarte, die er mit Hilfe einer Schablone und eines Lochstanzers derart markieren kann, dass die Karten anschließend maschinell ausgezählt werden können.

Hauptkritikpunkt dieses Systems ist seine Unzuverlässigkeit. Der Stanzmechanismus verschafft keine ausreichende Klarheit, ob eine Auswahlmöglichkeit markiert wurde, oder nicht.

Zwar wurde laut Schlifni [Sch00] bereits 1988 vom National Institute of Standards and Technology empfohlen, die Verwendung dieses Verfahrens einzustellen. Dennoch wurde es zwölf Jahre später bei den Wahlen zum US-Präsidenten weiterhin im Bundesstaat Florida benutzt und führte dort durch ungenaue und unklare Ergebnisse zu einem mehrwöchigen Spektakel, in dem die Stimmzettel in einigen Wahlkreisen manuell ausgezählt werden mussten, bis die Auszählung schließlich durch den Supreme Court zu einem willkürlich festgesetzten Zeitpunkt gestoppt wurde.

Eine nachträgliche, diesmal vollständige manuelle Neuauszählung in sämtlichen Wahlbezirken Floridas durch einen Zusammenschluss mehrerer großer amerikanischer Zeitungen ergab jedoch ein anderes Ergebnis als das amtliche Endergebnis [NOR01], [Isi01] und [Was01]/. Demnach stellte sich heraus, dass bei korrekter Funktionsweise des Wahlsystems ein anderer Kandidat Präsident der USA geworden wäre, als es dann tatsächlich der Fall war.

Damit ist die größte auch nur theoretisch konstruierbare Panne eines Voting-Systems in der Realität eingetreten - und zwar bei der Wahl zum Staatsoberhaupt

des mächtigsten Staates der Welt. Der weitere Einsatz von Wahlkartensystemen in staatlichen Volksvertretungswahlen ist nun nicht mehr aus technischen Überlegungen heraus erklärbar.

Ein seit langer Zeit andauerndes Missverständnis ist der Glaube, das Wahlergebnis sei bei der Verwendung von Wahlkarten-Lesesystemen universell verifizierbar. Dies ist lediglich eingeschränkt der Fall, da einige Wahlkarten nur teilweise oder gar nicht gestanzt sind, so dass jede kleinste mechanische Handhabung der Wahlkarten das Ergebnis verändern kann, indem die vorperforierten Löcher aufgerissen werden können. Diese Problematik war ein wesentlicher Diskussionsstoff bei den manuellen Nachauszählungen der US-Präsidentschaftswahlen 2000, bei denen jede einzelne Stimmkarte durch mehrköpfige Bewertungskommissionen und dahintergelagerte Schiedskommissionen ausgiebigen Untersuchungen unterzogen werden musste. Es ist somit wohl nicht möglich bei zwei manuellen Auszählungen das exakt gleiche Ergebnis zu erzielen.

Des Weiteren ist es bei diesem System möglich Wahlkarten zu entfernen oder hinzuzufügen, ohne dass dies nachträglich verifizierbar ist.

Allgemeinheit Jeder kann einen Stimmzettel abgeben.

Authentifikation Die Authentifikation muss extern durch Wahlhelfer erfolgen.

Korrektheit Das System liefert unkorrekte Ergebnisse, wodurch bereits eine Person als Präsident der USA eingesetzt wurde, obwohl nach geltendem Wahlrecht ihr Mitbewerber gewonnen hätte. Wahlergebnisse, die mittels Wahlkarten-Lesesysteme ermittelt wurden, können nicht mehr ernst genommen werden.

Übertragungsintegrität Nicht garantierbar. Es ist möglich, Wahlkarten nachträglich zu manipulieren oder auszutauschen.

Nichtvermehrbarkeit Nicht garantierbar. Es ist möglich, beliebig viele Wahlscheine hinzuzufügen, ohne dass dies nachgewiesen werden kann.

Robustheit Einzelne Wähler können den Fortgang der Wahl nicht aufhalten.

Fairness Durch böswillige Wahlhelfer können Stimmzettel bereits frühzeitig ausgezählt und Zwischenergebnisse veröffentlicht werden.

Wahlgeheimnis Das Wahlgeheimnis wird gewahrt, sofern die Wahlkarten kein Wählerspezifischen Informationen tragen und Wahlkabinen benutzt werden.

Unmittelbarkeit Wird die Wähleridentität festgestellt und eine Wahlkabine benutzt, so ist die Unmittelbarkeit gewährleistet.

Quittungsfreiheit Das System ist quittungsfrei.

Individuelle Verifizierbarkeit Keine individuelle Verifizierbarkeit möglich.

Universelle Verifizierbarkeit Universelle Verifizierbarkeit ist nur zum Teil möglich: Zum Einen werden durch die Handhabung der Wahlzettel diese verändert. Zum Anderen können zwischen zwei Auszählungen Wahlzettel entfernt oder hinzugefügt worden sein.

Effizienz Hohe Kosten durch einen großen Personalaufwand.

Skalierbarkeit Durch eine dezentrale Positionierung der Wahllokale beliebig skalierbar.

Physische Voraussetzungen Wahllokale und Wahlzellen müssen vorhanden sein.

Flexibilität des Stimmzettel-Formats Es sind lediglich Multiple-Choice-Wahlzettel möglich.

Ortsunabhängigkeit Wähler müssen zu Wahllokalen erscheinen. Das System kann durch Briefwahlen ergänzt werden.

Angeichts der fehlenden Korrektheit kann die Verwendbarkeit von Protokollen dieser Klasse für staatliche Volksvertreterwahlen ausgeschlossen werden.

B.2.3 Aufzeichnungssysteme

Aufzeichnungssysteme repräsentieren die denkbar trivialsten elektronischen Voting-Systeme. Zu unterscheiden sind direkte Aufzeichnungssysteme und Online-Aufzeichnungssysteme. In beiden Fällen werden die Daten durch elektronische Eingabe-Medien erfasst und dann im Klartext zu einem zentralen System übertragen, das die Stimmen aufzeichnet und anschließend auszählt.

Direkte Aufzeichnungssysteme Direkte Aufzeichnungssysteme stellen ein geschlossenes System dar. Sie werden oftmals in Parlamenten eingesetzt, um Abstimmungen per Handzeichen effizienter zu gestalten. Seit einigen Jahren werden sie auch stellenweise in den USA zu Volksvertretungswahlen eingesetzt und dort als Direct Record Voting Systems (DRVS) bezeichnet.

Als abschreckendes Beispiel für die schlechtmöglichste Implementierung eines direkten Aufzeichnungssystems lässt sich das System der Firma Diebold anführen (4.2.1).

Online-Aufzeichnungssysteme Online-Aufzeichnungssysteme übermitteln die Daten unverschlüsselt über ein öffentliches Netz, wie das Internet oder das Telefonnetz. Hierzu zählen unter anderem Telefonabstimmungssysteme, die am Rande von Fernsehshows eingesetzt werden, sowie einfache webbasierte Online-Meinungsumfragesysteme. Das „naive Verfahren“ von Philippsen [Phi01] S. 4 gehört ebenfalls zu dieser Protokoll-Klasse. Offensichtlich lässt sich bei derartigen Systemen keinerlei Sicherheit garantieren, da eine Reihe von banalen Angriffsmöglichkeiten denkbar sind. Aus diesem Grund sind Online-Aufzeichnungssysteme für die hier betrachteten Einsatz-Zwecke nicht praktikabel.

Eigenschaften

Authentifikation Eine Authentifikation lässt sich nur mit direkten Aufzeichnungssystemen realisieren.

Korrektheit Das System liefert nur dann ein korrektes Ergebnis, wenn die technischen Teilkomponenten fehlerfrei funktionieren.

Übertragungsintegrität Eine Übertragungsintegrität ist bei Online-Aufzeichnungssystemen nicht gewährleistet. Bei direkten Aufzeichnungssystemen ist dies nur unter bestimmten Bedingungen der Fall.

Nichtvermehrbarkeit Böartige Wahlbehörden können unentdeckt Stimmen für Nicht-Wähler abgeben.

Robustheit Das System ist in den meisten Fällen robust.

Fairness Böswillige Wahlbehörden können Zwischenergebnisse veröffentlichen.

Wahlgeheimnis Das Wahlgeheimnis kann bei Online-Aufzeichnungssystemen garantiert werden, wenn z.B. die Wähler über öffentliche Telefone wählen.

Unmittelbarkeit Eine Unmittelbarkeit kann nur durch den Einsatz von Wahlzellen erreicht werden.

Quittungsfreiheit Die Quittungsfreiheit ist konfigurierbar.

Individuelle Verifizierbarkeit Die Zählung einzelner Stimmen kann durch die Veröffentlichung der Stimmen und die Ausgabe einer Quittung realisiert werden.

Effizienz Eine hohe Effizienz ist realisierbar.

Skalierbarkeit Die Systeme sind im Allgemeinen beliebig skalierbar.

Physische Voraussetzungen unterschiedliche direkte Aufzeichnungssysteme können verschieden physische Voraussetzungen stellen.

Flexibilität des Stimmzettel-Formats Das Stimmzettelformat ist beliebig flexibel.

Orts-Unabhängigkeit Online-Aufzeichnungssysteme realisieren Ortsunabhängigkeit.

B.2.4 Blinde Beglaubigungssysteme

Blinde Signaturen Folgende Darstellung ist an die von Schneier [Sch96] S.112–115 u. 549–550 angelehnt: Oftmals werden blinde Unterschriften benötigt. Das bedeutet, dass die unterschreibende Instanz nicht weiß, welche Daten sie unterschreibt. Blinde Signaturen haben also zwei Vorteile:

1. Es handelt sich um eine echte Signatur mit allen Eigenschaften einer einfachen Signatur. Es kann zweifelsfrei nachgewiesen werden, wer die Nachricht unterschrieben hat. Nur der Besitzer des Private Keys ist in der Lage, eine gültige Signatur zu leisten.
2. Die unterschreibende Instanz hat keinerlei Möglichkeit festzustellen, was der Inhalt der Nachricht ist, die unterschrieben wurde.

Chaum stellte dazu ein Verfahren [Cha85] vor, dass auf den ebenfalls von ihm entwickelten anonymen Kommunikationskanälen [Cha81] basiert. Das Verfahren ist recht simpel: Angenommen, Alice möchte, dass Bob eine Nachricht unterschreibt, ohne dass dieser den Inhalt der Nachricht erfährt. Alice erzeugt eine Zufallszahl („Blinding-Factor“). Die Nachricht multipliziert sie mit dieser Zufallszahl und schickt das Ergebnis an Bob. Der signiert die mit der Zufallszahl multiplizierte Nachricht und schickt das Ergebnis an Alice. Schließlich dividiert diese die multiplizierte und signierte Nachricht durch ihre Zufallszahl und erhält damit ihr Original-Dokument – nun jedoch signiert.

Nebenbedingung ist, dass die Signatur-Funktion und die Multiplikation kommutativ ist.

Blinde Beglaubigungssysteme Blinde Beglaubigungssysteme nutzen anonyme Kanäle, um Wahlzettel zwischen dem Wahl-Client und den Behörden zu verschicken. Bei dieser Protokoll-Klasse können Wahlzettel beliebigen Formates verwendet werden. Die Prüfung der Wahlberechtigung und die Auszählung der Stimmen werden von unterschiedlichen Behörden vorgenommen. Durch die anonyme Kommunikation wird sichergestellt, dass auch durch eine Konspiration beider Wahlbehörden nicht auf eine Verbindung zwischen Identität des Wählers und seinem Wahlverhalten geschlossen werden kann.

Um dennoch wirksam die Wahlberechtigung überprüfen zu können, wird das Blind-Signature-Verfahren eingesetzt, welches bereits in B.2.4 beschrieben wurde und auf der Arbeit von Chaum [Cha85] aufbaut. Die die Wahlberechtigung prüfende Behörde signiert den Stimmzettel des Wählers blind. Die notwendigen anonymen Kommunikationskanäle wurden ebenfalls von Chaum entwickelt [Cha81].

Auf Grund der Aufteilung der Prüfung der Wahlberechtigung und der Stimmmzählung ist ein wesentliches Merkmal der blinden Beglaubigungssysteme, dass das Protokoll aus Sicht des Wählers aus zwei Phasen besteht. Dies hat in der Realität konkrete technische Nachteile, die auch nicht durch den Wahl-Client gekapselt werden können. Verliert der Client seinen blind beglaubigten Stimmzettel, bevor er ihn in der zweiten Phase an den Stimmauszähler senden konnte (z.B. bei Ausfall der Stromversorgung des Client-Rechners, Hardwareschaden des Client-Rechners, etc.), so ist die Wahlberechtigung verloren gegangen, ohne dass der Wähler von seinem Stimmrecht tatsächlich Gebrauch machen konnte. Allen blinden Beglaubigungssystemen ist also eine *fehlende Allgemeinheit* der Wahl gemein.

Schwache blinde Beglaubigungssysteme Schwache blinde Beglaubigungssysteme beruhen entweder auf keinem anonymen Kanal oder auf einem schwachen Mix-Kanal, der die Worst-Case-Annahme „Sicherstellung der Anonymität bei NMAX-1 konspirativen Einheiten nicht erfüllen kann.“ Ein Beispiel hierfür ist Sensus von Cranor und Cytron [CC97], das beispielhaft implementiert wurde.

Der eigentliche Vorteil blinder Beglaubigungssysteme – die unbedingte Wahrung des Wahlgeheimnisses – wird somit durch die mangelnde Qualität der Anonymität wieder reduziert oder ganz zunichte gemacht.

Konventionelle blinde Beglaubigungssysteme Konventionelle blinde Beglaubigungssysteme setzen ein blindes, standardisiertes Signaturverfahren, sowie externe, anonyme Kanalsysteme ein.

Blinde Multisignatursysteme Bei einem blinden Multisignatursystem wird jeder Wahlschein von mehreren voneinander unabhängigen Zertifizierungsservern signiert. Dadurch kann eine unzulässige Stimmvermehrung verhindert werden – unter der Voraussetzung, dass nicht sämtliche Zertifizierungsserver konspirieren.

Authentifizierbare Abgabesysteme In einem authentifizierbaren Abgabesystem wird ein blindes Standard-Signaturschema, sowie ein interner, anonymer Kanal eingesetzt. Die Öffentlichkeit kann zu jedem Zeitpunkt die Teilnehmer identifizieren. Dadurch wird eine unzulässige Vermehrung oder Hinzufügen von Stimmen praktisch unmöglich gemacht.

Eigenschaften

Allgemeinheit Die Allgemeinheit der Wahl ist nicht gegeben, da bei Ausfall des Client-Rechners nach Erhalten des blind signierten Stimmzettels, aber noch vor dessen Versenden an den Stimmzähler, die Wahlberechtigung des Wählers verloren geht, ohne dass seine Stimme gezählt worden wäre.

Authentifikation Die Authentifikation der Wähler ist gewährleistet.

Korrektheit Das Wahlergebnis kann durch ein böswilliges Wahlamt manipuliert werden, da die Nichtvermehrbarkeit nicht gegeben ist.

Übertragungsintegrität Die Übertragungsintegrität wird mittels des Einsatzes von Signaturen garantiert.

Nichtvermehrbarkeit Wähler können einen blind signierten Wahlschein nicht mehrfach versenden, da dies vom Stimmzähler kontrolliert wird. Jedoch kann das Wahlamt Stimmzettel für Nichtwähler generieren, ohne dass dies nachgewiesen werden könnte.

Robustheit Das Verfahren ist, bis auf Angriffe auf die Netzkapazität oder die Rechenleistung der Server, robust.

Fairness Wird die Registrierungs- und die Wahlphase zeitlich voneinander getrennt, so dass die Einsendung der Stimmzettel erst nach Schließung der Wahllokale beginnt, so ist eine Verhinderung der frühzeitigen Veröffentlichung von Zwischenergebnissen möglich.

Wahlgeheimnis Die Wahrung des Wahlgeheimnisses hängt von der Güte der anonymen Kanäle ab.

Unmittelbarkeit Nicht möglich. Ausnahme: Schlifnis Gamma-System, welches jedoch spezialisierte Hardware erfordert.

Quittungsfreiheit Blinde Beglaubigungssysteme sind nicht quittungsfrei, da der Wähler ja den blind signierten Stimmzettel erhält. Zwar kann er damit nicht nachweisen, ob er gewählt hat, jedoch kann er zeigen, was er gewählt hat, falls er gewählt hat.

Individuelle Verifizierbarkeit Das Ergebnis ist individuell verifizierbar, falls ein Bulletin-Board-System (BBS) eingesetzt wird, um die Listen der blind signierten Stimmzettel zu veröffentlichen.

Universelle Verifizierbarkeit Das System ist nicht universell verifizierbar, da keine Nichtvermehrbarkeit vorhanden ist.

Kommunikationskomplexität Die Kommunikationskomplexität ist tolerabel, allerdings höher als bei anderen Systemen, da der Stimmzettel drei Mal versendet wird.

Effizienz Es gibt schon einen gewissen Rechenaufwand für die zahlreichen kryptographischen Operationen.

Skalierbarkeit Das System ist prinzipiell mittels Verteilung beliebig skalierbar.

Flexibilität des Stimmzettel-Formats Beliebige Stimmzettel sind einsetzbar.

Ortsunabhängigkeit Blinde Beglaubigungssysteme lassen ortsunabhängige Wahlen zu.

Beim Einsatz von blinden Beglaubigungssystemen sind die Vorteile der Verifizierbarkeit mit dem Nachteil des möglichen Stimmverlustes abzuwägen.

B.2.5 Sichere, vergessliche Transfer-Systeme

All-Or-Nothing Disclosure of Secrets (ANDOS) Das All-Or-Nothing Disclosure of Secrets-Protokoll ermöglicht es Alice Bob eine Reihe von Geheimnissen anzubieten, von denen Bob genau ein Geheimnis auswählen kann. Alice geht kein Risiko ein, ein zweites Geheimnis preiszugeben. Bob verrät in diesem Protokoll Alice nicht, welches Geheimnis er wählt.

Eine detaillierte Beschreibung liefert Schneier [Sch96] S.543-546.

Transfersysteme arbeiten mit dem All or nothing Disclosure Of Secrets-Protokoll. Ein Client kann aus einer Menge von Geheimnissen, die der Server ihm anbietet eines auswählen, ohne dass der Server erfährt, welches ausgewählt wurde.

Es handelt sich bei sicheren, vergesslichen Transfersystemen um sehr umständliche Protokolle, die somit einen hohen Implementierungsaufwand und damit auch eine hohe Wahrscheinlichkeit des Einbaus von Sicherheitsrisiken bei der Implementierung haben.

B.2.6 Protokolle mit Homomorpher Verschlüsselung

Bei Protokollen mit homomorpher Verschlüsselung werden Wahlzettel mit einem oder mehreren öffentlichen Schlüsseln verschlüsselt. Zur Ermittlung des Ergebnisses werden sämtliche verschlüsselten Wahlzettel addiert. Die Summe ist gleich der verschlüsselten Summe der Addition der unverschlüsselten Wahlzettel. Jede der n Wahlbehörden besitzt einen Teilschlüssel zur Entschlüsselung des Ergebnisses.

Das Wahlgeheimnis ist dann gewahrt, sobald eine administrative Einheit korrekt arbeitet. Durch den Einsatz homomorpher Verschlüsselung ist die Korrektheit der verdeckten Auswertung nachvollziehbar und erzwingbar.

Schlifni [Sch00], Kap. 4 bezeichnet Protokolle mit homomorpher Verschlüsselung als *verdeckte Auswertungssysteme* und unterscheidet zwei Unterklassen.

Zero-Knowledge-Proofs Mit Hilfe eines Zero-Knowledge-Proofs kann der Besitzer eines Geheimnisses nachweisen, dass er im Besitz dieses Geheimnisses ist, ohne dieses Geheimnis selber preis zu geben. Eine übersichtliche Darstellung findet sich bei Schneier [Sch96], S.101–111.

Das erste Verfahren hierzu wurde von Goldwasser, Micali und Rackoff entwickelt. Möchte Victor von Peggy den Beweis erbracht bekommen, dass diese über ein bestimmtes Geheimnis verfügt, so stellt er ihr eine Reihe von Fragen. Die Fragen sind derart gestellt, dass ihre Beantwortung nicht das Geheimnis selbst preis gibt. Kennt Peggy das Geheimnis nicht, so muss sie die Antworten erraten. Da Victor jedoch eine ganze Reihe von Fragen stellt, steigt mit ihrer Anzahl die Wahrscheinlichkeit, dass Peggy auffliegt. Dieses interaktive Verfahren muss Peggy jedoch mit jeder Person wiederholen, die zweifelt, dass sie im Besitz des Geheimnisses ist, da Dritte nicht wissen, ob sich Peggy und Victor zuvor Abmachungen über die zu stellenden Fragen getroffen haben.

Non-Interactive Zero-Knowledge-Proofs Damit der Beweis auch geführt werden kann, ohne dass jedes Mal, wenn jemand vom Besitz des Geheimnisses überzeugt werden soll, eine Frage-Antwort-Runde durchgeführt werden muss, wurden Verfahren entwickelt, die nicht-interaktiv sind. Sie basieren auf Einweg-Hash-Funktionen.

Wahrscheinverteilende verdeckte Auswertungssysteme Bei wahrscheinverteilenden, verdeckten Auswertungssystemen findet ein verifizierbarer Secret-Sharing-Algorithmus eine Anwendung. Der Client zerlegt sein Votum in mehrere Teilstimmen, die er auf eine fixe Menge von Auswertungsservern verteilt. Im Bulletin-Board-System (BBS) publiziert der Client einen Zero-Knowledge-Beweis B.2.6, aus dem hervorgeht, dass sein Votum richtig gewählt wurde.

Die Wahlscheinformate sind weitgehend auf Ja/Nein - Entscheidungen reduziert. Die Effizienz verringert sich deutlich mit einer Zunahme der Komplexität des Abfrageformates.

Wahrscheinaggregierende, verdeckte Auswertungssysteme Dort wird auf eine Verteilung des Wahlscheines, sowie auf die Existenz privater Kanäle verzichtet.

Eigenschaften

Authentifikation Da jeder Wähler seinen signierten Stimmzettel zum Bulletin-Board sendet, ist die Authentifikation universell möglich.

Korrektheit Die Korrektheit des Wahlergebnisses kann universell verifiziert werden.

Übertragungsintegrität Die Übertragungsintegrität wird mittels der Signatur gewährleistet.

Nichtvermehrbarkeit Stimmzettel sind nicht vermehrbar, da sie signiert sind.

Fairness Eine Veröffentlichung des Zwischenergebnisses ist nur durch die Verschwörung von n Auswertern möglich.

Wahlgeheimnis Das Wahlgeheimnis hängt von der Sicherheit des gewählten Chiffres ab, sowie davon, dass nicht n Auswerter ihre geteilten Schlüssel zusammenschließen.

individuelle Verifizierbarkeit Jeder Wähler kann die Veröffentlichung seines Stimmzettels überprüfen.

universelle Verifizierbarkeit Jeder Teilnehmer und jeder Außenstehender kann die Ermittlung des Ergebnisses aus den veröffentlichten Stimmzetteln nachvollziehen.

Effizienz Das System ist so lange effizient, sofern nur Ja/Nein-Abstimmungen realisiert werden. Kommen komplexere Formate zum Einsatz steigt, der Rechenaufwand enorm an.

Skalierbarkeit Das System ist gut skalierbar.

Flexibilität des Stimmzettel-Formats Es sind nur Ja/Nein- bzw. Multiple-Choice-Wahlen effizient realisierbar.

Ortsunabhängigkeit Die Protokolle lassen ortsunabhängige Wahlen zu.

Protokolle mit homomorpher Verschlüsselung kommen für die hier vorliegenden Anwendungsfälle nicht in Betracht, da lediglich Stimmzettel mit Ja/Nein-Entscheidungen effizient realisiert werden können und dies nicht ausreichend flexibel ist.

B.2.7 Protokolle mit universell verifizierbaren Mixes

Mixer sind sichere, anonyme Kanalsysteme. Jeder Mixer verschlüsselt und vertauscht seine Eingaben derartig, dass aus einer Ausgabe nicht auf die dazugehörige Eingabe geschlossen werden kann.

Durch eine Reihenschaltung lässt sich die Sicherheit des Wahlgeheimnisses weiter steigern – arbeitet ein Mixer korrekt, so bleibt das Wahlgeheimnis gewahrt.

Protokolle dieser Klasse können meist auch der Klasse der blinden Beglaubigungssysteme zugerechnet werden.

Steinbach-Mixes Exemplarisch sei im Folgenden ein einfaches Protokoll mit beruhend auf einem Mix beschrieben. Die Darstellung ist an Steinbach angelehnt [Ste98] S. 88–91. Das Verfahren besteht aus zwei Phasen:

In der ersten Phase wird ein anonymes Wählerverzeichnis erstellt. In der zweiten Phase wird mit dessen Hilfe die Wahl durchgeführt. Jeder Wähler verschlüsselt seinen öffentlichen Schlüssel zusammen mit einer Zufallszahl mit dem öffentlichen Schlüssel des Mixers und schickt diese Daten zusammen mit seinen Wahlunterlagen (signiert) an das Wahlamt. Dieses überprüft, ob der Wähler wahlberechtigt ist und zum ersten Mal die Unterlagen einwendet. Er entfernt die Signatur und die Wahlunterlagen und sendet das Ergebnis an den Mixer, ohne dass es selber den öffentlichen Schlüssel des Wählers lesen könnte. Der Mixer anonymisiert das Datenpaket und entschlüsselt es. Als Ergebnis veröffentlicht dieser am Ende der Registrierungsphase eine Liste mit sämtlichen, öffentlichen Schlüsseln der registrierten Wähler.

In der eigentlichen Wahlphase sendet der Wähler seinen Stimmzettel signiert mit seinem geheimen Schlüssel, versehen mit seinem öffentlichen Schlüssel (als Adressangabe in der Wählerliste) einer Zufallszahl und verschlüsselt mit dem öffentlichen Schlüssel des Mixers an diesen. Der Mixer entschlüsselt den Wahlzettel, prüft die Signatur, prüft, ob der anonyme Wähler nicht bereits schon einmal gewählt hat, und zählt die Stimme.

Eigenschaften

Allgemeinheit Das Protokoll besteht aus zwei Phasen. Diese sind – um größtmögliche Anonymität zu erlangen – sogar zeitlich strikt getrennt. Dadurch muss der Client seinen privaten und öffentlichen Schlüssel während dieses Zeitraumes aufbewahren. Geht er verloren, so ist auch die Wahlberechtigung des Wählers verloren, ohne dass dieser eine Stimme abgegeben hätte.

Authentifikation Die Authentifikation der Wähler ist gewährleistet.

Korrektheit Der Mix kann Stimmen unterschlagen. Dies fällt nur auf, falls die betreffenden Wähler das Ergebnis kontrollieren. Das Wahlamt kann Wähler selber registrieren, die sich in der Wahlphase nicht registriert haben. Dies

fällt nur auf, wenn die Wähler die betreffende Liste mit den Namen der registrierten Wähler kontrollieren.

Übertragungsintegrität Die Übertragungsintegrität wird mit Hilfe von Signaturen gewährleistet.

Nichtvermehrbarkeit Die Wahlzettel sind nicht vermehrbar, da sie signiert sind.

Robustheit Wähler können die Wahl nicht aufhalten.

Fairness So der Mix korrekt arbeitet, werden keine Zwischenergebnisse verfrüht veröffentlicht.

Wahlgeheimnis Das Wahlgeheimnis bleibt gewahrt, so lange der Mixer – bzw. mindestens ein Mix aus einer Reihe hintereinandergeschalteter Mixer – korrekt arbeitet.

Unmittelbarkeit Die Unmittelbarkeit ist nicht gewährleistet, da keine Quittungsfreiheit vorliegt.

Quittungsfreiheit Der Wähler kann seine Wahl mit Hilfe seines Schlüsselpaares beweisen.

Individuelle Verifizierbarkeit Die Zählung der Stimme ist individuell verifizierbar.

Universelle Verifizierbarkeit Das Wahlergebnis ist universell als Summe der einzelnen Stimmzettel verifizierbar. Ob alle Stimmzettel veröffentlicht wurden und ob nicht Wähler von einer böswilligen Wahlbehörde registriert wurden, die gar nicht registriert werden wollten, lässt sich nicht universell verifizieren.

Kommunikationskomplexität Die Kommunikationskomplexität ist recht hoch, da es (bei möglicherweise mehreren Mixern) eine ganze Reihe von Teilnehmern an einem einzigen Wahlvorgang gibt.

Effizienz Die Effizienz ist nicht allzu hoch, da eine große Menge von kryptographischen Operationen pro Wahlvorgang notwendig sind.

Skalierbarkeit Das System ist mittels Verteilung recht gut skalierbar.

Flexibilität Es sind beliebige Stimmzettel einsetzbar.

Ortsunabhängigkeit Mit dem Protokoll lassen sich ortsunabhängige Wahlen durchführen.

Generell können Protokolle dieser Klasse durchaus für staatliche Voting-Systeme geeignet sein. Auch hier ist jedoch – analog zu den blinden Beglaubigungssystemen – das Risiko zu bewerten, dass Wahlzettel durch den Einsatz eines mehrstufigen Verfahrens auf dem Client-Rechner verloren gehen können. Zudem konnte nicht letztendlich geklärt werden, ob einige dieser Verfahren sowohl universell verifizierbar, als auch quittungsfrei sind. Derartige Behauptungen wurden in der Vergangenheit schon oftmals revidiert.

B.2.8 Zusammenfassende Bewertung der Protokollklassen

Insgesamt scheinen blinde Beglaubigungssysteme bzw. Protokolle mit universell verifizierbaren Mixes am ehesten für den Einsatz bei staatlichen Volksvertreterwahlen geeignet zu sein. Leider weist jedoch keines der Protokolle sämtliche wünschenswerten Eigenschaften auf.

C Glossar

In dieser Broschüre wird die folgende Terminologie für elektronische Abstimmungssysteme verwendet:

Abstimmungssystem Als Abstimmungssystem wird ein System bezeichnet, welches dazu geeignet ist, Meinungen von einer Menge von Personen zu erheben und diese zu einem Ergebnis zusammen zu fassen.

Elektronisches Abstimmungssystem Ein elektronisches Abstimmungssystem ist ein Abstimmungssystem, welches moderne Informationstechnologie einsetzt.

Polling-System Ein Polling-System ist ein elektronisches Abstimmungssystem, welches Wert auf sehr einfache Benutzbarkeit und Effizienz legt, dafür aber die Korrektheit des Ergebnisses, das Wahlgeheimnis, oder andere Eigenschaften von Wahlen opfert. Als Beispiel seien sehr einfache Web-Polls genannt.

Elektronisches Voting-System Ein elektronisches Voting-System ist ein elektronisches Abstimmungssystem, welches Wert auf die korrekte Ermittlung des Ergebnisses, die Einhaltung des Wahlgeheimnisses, oder ähnliches legt und dafür einfachste Benutzbarkeit und Effizienz opfert.

Elektronisches Voting-System für Wahllokale Ein elektronisches Voting-System für Wahllokale ist ein System, welches Wahlen ausschließlich in Wahllokalen, also an offiziellen Orten, an denen die Wahlbedingungen, die eingesetzte Technik und die Netzwerke gut kontrollierbar sind, zulässt.

Elektronisches Voting-System mit Wahl-Kiosken Ein elektronisches Voting-System mit Wahl-Kiosken ist ein System, welches Wahlen an Wahl-Stationen zulässt, deren Konfiguration gut kontrolliert werden kann. Diese können an beliebigen öffentlichen Orten aufgestellt sein. Somit ist die Technik und das Netzwerk, nicht jedoch die Wahlumgebung kontrolliert.

Online-Voting-System oder internetbasiertes Voting-System Ein internetbasiertes Voting-System ermöglicht es dem Benutzer von einem beliebigen Rechner mit Internet-Verbindung aus zu wählen. Die Netzanbindung, sowie die Hardware-Konfiguration und die Wahlumgebung sind nicht zu kontrollieren, wohl aber die eingesetzte Wahlsoftware.

Web-basiertes Voting-System Ein Web-basiertes Voting-System lässt den Wähler von einem beliebigen Web-Browser aus wählen. Hier ist weder die Wahlumgebung, noch die Netzanbindung, die Hardware-Konfiguration, oder die Software-Sicherheit des Clients kontrollierbar.

Literatur

- [BSW01] BEUTELSPACHER, A., J. SCHWENK und K.-D. WOLFENSTETTER: *Moderne Verfahren der Kryptographie - Von RSA zu Zero-Knowledge*. Vieweg - Verlag, Wiesbaden, 4. Auflage, 2001.
- [Bun96] BUNDESMINISTERIUM DER JUSTIZ: *Bürgerliches Gesetzbuch*, 1896. RGBI 1896, 195, Neugefasst durch Bek. v. 2. 1.2002 I 42, 2909; 2003, 738; zuletzt geändert durch Art. 7 G v. 15.12.2003 I 2676, <http://bundesrecht.juris.de/bundesrecht/bgb/> Stand: 17.01.2004.
- [Bun51] BUNDESMINISTERIUM DER JUSTIZ: *Wahlprüfungsgesetz*, 1951. BGBI I 1951, 166, FNA 111-2, Geltung ab: 3. 7.1975, zuletzt geändert durch Art. 1 G v. 28. 4.1995 I 582, im Saarland eingeführt durch § 15 Buchst. b G v. 23.12.1956 101-2, <http://www.bundestag.de/gesetze/wpg/> Stand: 17.01.2004.
- [Bun65] BUNDESMINISTERIUM DER JUSTIZ: *Aktiengesetz*, 1965. BGBI I 1965, 1089, zuletzt geändert durch Art. 73 V v. 25.11.2003 I 2304, <http://bundesrecht.juris.de/bundesrecht/aktg/> Stand: 17.01.2004.
- [Bun67] BUNDESMINISTERIUM DES INNERN: *Gesetz über die politischen Parteien*, 1967. BGBI I 1967, 773, Neugefasst durch Bek. v. 31. 1.1994 I 149; zuletzt geändert durch Art. 3 G v. 28. 6.2002 I 2268, <http://www.bundestag.de/gesetze/pg/> Stand: 17.01.2004.
- [Bun75] BUNDESMINISTERIUM DES INNERN: *Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland*, 1975. BGBI I 1975, 2459, Zuletzt geändert durch Art. 1 V v. 20. 4.1999 I 749, <http://bundesrecht.juris.de/bundesrecht/bwahlgv/> Stand: 17.01.2004.
- [Bun78] BUNDESMINISTERIUM DES INNERN: *Gesetz über die Wahl der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland*, 1978. BGBI I 1978, 709, FNA 111-5, Stand: Neugefasst durch Bek. v. 8. 3.1994 I 423, 555; zuletzt geändert durch Art. 1 u. 2 G v. 15.8.2003 I 1655 <http://bundesrecht.juris.de/bundesrecht/euwg/> Stand: 17.01.2004.
- [Bun88] BUNDESMINISTERIUM DES INNERN: *Europawahlordnung EuWO*, 1988. BGBI I 1988, 1453 BGBI I 1989, 228, FNA 111-5-4, Textnachweis ab: 19. 8.1988, Stand: Neugefasst durch Bek.

- v. 2. 5.1994 I 957; zuletzt geändert durch Art. 3 G v. 27. 4.2002 I http://bundesrecht.juris.de/bundesrecht/euwo_1988/ Stand: 17.01.2004.
- [Bun93] BUNDESMINISTERIUM DES INNERN: *Bundeswahlgesetz (BWG)*, 1993. 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) <http://www.bundestag.de/gesetze/bwg/> Stand: 17.01.2004.
- [Bun01] BUNDESMINISTERIUM DES INNERN: *Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, 2001. BGBl I 2001, 876, Geändert durch Art. 2 G v. 16. 5.2001 I 876, http://bundesrecht.juris.de/bundesrecht/sigg_2001/ Stand: 17.01.2004.
- [Bun02] BUNDESMINISTERIUM DES INNERN: *Bundeswahlordnung*, 2002. in der Fassung der Bekanntmachung vom 19. April 2002 (BGBl. I S. 1376), zuletzt geändert durch 8. ÄndVO vom 27. August 2002 (BGBl. I S. 3429), <http://www.bundestag.de/gesetze/bwo/> Stand: 17.01.2004.
- [Cal00] CALIFORNIA INTERNET VOTING TASK FORCE: *A Report on the Feasibility of Internet Voting*. Technischer Bericht, California Secretary of State, 2000. <http://www.ss.ca.gov/executive/ivote/> Stand: 17.01.2004.
- [CC97] CRANOR, L. und R. CYTRON: *Sensus: A security-conscious electronic polling system for the Internet*. In: *Proceedings of the Hawai'i International Conference on System Sciences*, Wailea, Hawaii, 1997. <http://lorrie.cranor.org/pubs/hicss/> Stand: 17.01.2004.
- [Cha81] CHAUM, D.: *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM, 24(2), February 1981. <http://world.std.com/franl/crypto/chaum-acm-1981.html> Stand: 17.01.2004.
- [Cha85] CHAUM, D.: *Security without identification: Transaction systems to make big brother obsolete*. Communications of the ACM, 28(10):1030–1044, October 1985.
- [Cyb00a] CYBERVOTE: *Report on electronic democracy projects, legal issues of Internet voting and users (i.e. voters and authorities representatives) requirement analysis*. Technischer Bericht D4 Volume 1, Cybervote, 2000. <http://www.eucybervote.org/KUL-WP2-D4V1-v1.0.pdf> Stand: 17.01.2004.

- [Cyb00b] CYBERVOTE: *Report on mock-ups of architectures and overall system architecture*. Technischer Bericht D7 - Volume 2, Cybervote, 2000. <http://www.eucybervote.org/MSI-WP2-D7V2-V1.0.pdf> Stand: 17.01.2004.
- [Cyb02] CYBERVOTE: *Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting*. Technischer Bericht D6 - Volume 1, Cybervote, 2002. <http://www.eucybervote.org/TUE-WP2-D6V1v1.0.pdf> Stand: 17.01.2004.
- [Cyb03] CYBERVOTE: *Technical Reports*, 2003. <http://www.eucybervote.org/reports.html> Stand: 17.01.2004.
- [dpa] DPA: *Bundeswahlleiter: Internetwahl bleibt vorerst Zukunftsvision*. Das Parlament, (39). http://www.das-parlament.de/2001/39/Kehrseite/p_a_39.html Stand: 17.01.2004.
- [Fed01] FEDERAL ELECTION COMMISSION: *Voting System Standards Draft*, 2001. <http://www.fec.gov/pages/vss/vssdraft.pdf> Stand: 17.01.2004.
- [For02] FORSCHUNGSGRUPPE INTERNETWAHLEN: *i-vote Report - Chancen, Möglichkeiten und Gefahren der Internetwahl*. Technischer Bericht, Forschungsgruppe Internetwahlen, 2002. <http://www.wahlkreis300.net/fgiw/uploader/data/Kurzfassung.pdf> Stand: 17.01.2004.
- [For03] FORSCHUNGSPROJEKT W.I.E.N.: *Wählen in elektronischen Netzwerken*, 2003. <http://www.forschungsprojekt-wien.de/> Stand: 17.01.2004.
- [For04] FORSCHUNGSGRUPPE INTERNETWAHLEN: *Strategische Initiative in der Bundesrepublik Deutschland: Wählen im Internet*, 2004. <http://www.internetwahlen.de> Stand: 17.01.2004.
- [Gei02] GEIERT, CONSTANZE: *Bundestagswahl 2002: Die Aufgaben des Bundeswahlleiters*, 2002. <http://www.bundeswahlleiter.de/download/adbwl.pdf>, Stand: 17.01.2004.
- [Ini03] INITIATIVE D21 E.V.: *Die D21-Vorstandswahl 2003 - Informationen zur Online Wahl der Initiative D21 e.V.* Technischer Bericht, 2003. http://www.initiaved21.de/themen/egovernment_weitere/doc/37_1071075505.pdf Stand: 17.01.2004.
- [Isi01] ISIKOFF, MICHAEL: *The Final Word?* Newsweek, Nov. 19th 2001.

- [Jon03] JONES, DOUGLAS W.: *The Case of the Diebold FTP Site*, July 2003. <http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html> Stand: 17.01.2004.
- [Kno04] KNOPPER, K.: *Knoppix*, 2004. <http://www.knopper.net/knoppix> Stand: 17.01.2004.
- [KSRW03] KOHNO, TADAYOSHI, ADAM STUBBLEFIELD, AVIEL D. RUBIN und DAN S. WALLACH: *Analysis of an Electronic Voting System*, July 2003. <http://www.avirubin.com/vote.pdf> Stand: 17.01.2004.
- [Kör01] KÖRPER, FRITZ RUDOLF: *Voraussetzung für die Durchführung von Online-Wahlen*, 2001. Rede des Parlamentarischen Staatssekretärs im Bundesministerium des Innern im Deutschen Bundestag am 11. Oktober 2001, <http://www.koerperspdp.de/berlin/redenarchiv/r010019.php> Stand: 17.01.2004.
- [LDS03] LDS BRANDENBURG: *Erste verbindliche Online-Wahl im LDS Abschlussbericht über Online-Personalratswahl im Landesbetrieb für Datenverarbeitung und Statistik (LDS) Brandenburg im Mai 2002*. Technischer Bericht, 2003. <http://www.forschungsprojekt-wien.de/pdf/lds.pdf> Stand: 17.01.2004.
- [Mau02] MAUSCH, MARC: *Wahlen und Abstimmungen auf dem virtuellen Parteitag*, Kapitel 7, Seiten 113–126. Online-Wahlen. Hubertus Buchstein, 2002.
- [Mic04] MICROMATA: *Polyas Online Voting System*, 2004. <http://www.micromata.de/produkte/polyas.jsp>, Stand: 28.06.2005.
- [Mür00] MÜRK, OLEG: *Electronic Voting Schemes*. Technischer Bericht, Tartu University, Institute of Computer Science, 2000. <http://math.ut.ee/olegm/papers/evs.ps> Stand: 17.01.2004.
- [Noa00] NOACK, U.: *Möglichkeiten und Grenzen der Hauptversammlung im Netz*, 2000. DAI-Seminar Investor Relation im Internet, Frankfurt/M, 23.11.2000 <http://www.jura.uni-duesseldorf.de/service/hv/DAI1.pdf> Stand: 17.01.2004.
- [NOR01] NORC: *Florida Ballots Project*, 2001. <http://norc.org/fl> Stand: 17.01.2004.
- [Ott98] OTTEN, D.: *„Mehr Demokratie im Internet...“ -Abschlussbericht zum Projekt „Wahlkreis 329“*. Technischer Bericht, Universität Osnabrück,

1998. <http://www.wahlkreis300.net/fgiw/uploader/data/WK329-Report.pdf> Stand: 17.01.2004.
- [Ott02] OTTEN, D.: *Modernisierung der Präsenzwahl durch das Internet*, Kapitel 5, Seiten 71–90. Online-Wahlen. Hubertus Buchstein, 2002.
- [Par49] PARLAMENTARISCHER RAT: *Grundgesetz für die Bundesrepublik Deutschland*, 1949. vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Gesetz vom 26. Juli 2002 (BGBl. I S. 286) <http://www.bundestag.de/gesetze/gg/> Stand: 17.01.2004.
- [Phi01] PHILIPPSEN, M.: *Internetwahlen: Demokratische Wahlen über das Internet?* Informatik Spektrum, 25, 2 2001. <http://www2.informatik.uni-erlangen.de/download/Papers/wahlen.pdf> Stand: 17.01.2004.
- [Rüß02] RÜSS, OLIVER: *Rechtliche Voraussetzungen und Grenzen von Online-Wahlen*, Kapitel 2, Seiten 39–50. Online-Wahlen. Hubertus Buchstein, 2002.
- [Sch96] SCHNEIER, B.: *Applied Cryptography*. John Wiley & Sons, 1996.
- [Sch00] SCHLIFNI, M.: *Electronic Voting Systems and Electronic Democracy, Participatory E-Politics for a new Wave of Democracy*. Doktorarbeit, TU Wien, 2000. <http://members.chello.at/manhard.schlifni/Webpub/Menu/indexii.html> Stand: 17.01.2004.
- [Sch03] SCHWARTZ, JOHN: *Computer Voting Is Open to Easy Fraud, Experts Say*, July 24th 2003. <http://www.nytimes.com/2003/07/24/technology/24VOTE.html> Stand: 17.01.2004.
- [Ste98] STEINBACH, JULIA: *Wahlschemata auf Computernetzwerken*. Diplomarbeit, Fachbereich Informatik, Johann-Wolfgang-Goethe-Universität Frankfurt am Main, 1998. <http://www.mi.informatik.uni-frankfurt.de/research/masterthesen/steinbach.diplom.1998.ps.gz> Stand: 17.01.2004.
- [T-S03] T-SYSTEMS CSM: *Onlinewahlen T-Systems CSM - Abschlussbericht der elektronischen Wahlen zum Betriebsrat bei T-Systems CSM im Mai 2002*. Technischer Bericht, 2003. http://www.forschungsprojekt-wien.de/pdf/t_systems.pdf Stand: 17.01.2004.

- [UKK01] ULLMANN, M., F. KOOB und H. KELTER: *Anonyme Wahlen - Lösungsansätze für die Realisierung von Online-Wahlen*. Datenschutz und Datensicherheit, 22(11), 2001. http://mitglied.lycos.de/mac_o_mania/extdoc/OnlinewahlenDUD.pdf Stand: 18.01.2004.
- [Was01] WASHINGTON POST: *Who Remembers Chad?* Washington Post, Seite A46, November 15 2001.
- [Wil02] WILL, MARTIN: *Internetwahlen. Verfassungsrechtliche Möglichkeiten und Grenzen*, Band 2 der Reihe *Recht und Neue Medien*. Boorberg, 2002.
- [ZF04] ZICHT, WILKO und MARTIN FEHNDRICH: *Wahlen, Wahlrecht und Wahlsysteme*, 2004. <http://www.wahlrecht.de/> Stand: 17.01.2004.

Index

- Übertragungsintegrität, 36, 38, 40, 42, 45
- Abgabesysteme
 - authentifizierbare, 45
- Abstimmungssystem, 52
- Aktiengesetz, 8
- All or nothing Disclosure Of Secrets, 47
- All-Or-Nothing Disclosure of Secrets, 47
- Allgemeinheit, 37, 38, 40, 45
- ANDOS, 47
- anonyme Kommunikationskanäle, 43
- Anwendungssoftware, 22
- Arbeitsgruppe Onlinewahlen, 7, 34
- Aufzeichnungssystem, 41
 - direktes, 41
 - Online-, 42
- Auswertungssysteme
 - verdeckte, 47
- Authentifikation, 36, 38, 40, 42, 45
- authentifizierbare Abgabesysteme, 45
- Bürgerliches Gesetzbuch, 8
- Banking
 - Online-, 22
- Beglaubigungssysteme
 - blinde, 43
- Betriebssystem, 22, 25
- BGB, 8
- BIOS, 22
- Blind-Signature, 43
- Blinde Beglaubigungssysteme, 43
 - schwache, 44
- blinde Beglaubigungssysteme
 - konventionelle, 45
- blinde Multisignatursysteme, 45
- Blinde Signaturen, 43
- Blinding-Factor, 43
- Bundewahlgeräte-Verordnung, 7
- Bundewahlgesetz, 7
- Bundewahlordnung, 7
- BWahlGV
 - Novellierung, 21, 33
- CD
 - bootfähige, 25
- Chip-Karten, 23
- Client-Rechnersicherheit, 16
- Cybervote, 24, 25
- Dezentrale Protokolle, 38
- Dezentralisierung, 23
- Effizienz, 37, 39, 41, 43, 46, 49
- Elektronisches Abstimmungssystem, 52
- Empfehlungen, 33
- Europäische Union, 7
- Fairness, 37, 38, 40, 42, 46, 49
- FEC, 7
- Federal Election Commission, 7
- Flexibilität, 37, 39, 41, 43, 46, 49
- Forschungsgruppe Internetwahlen, 7, 27
- Geld-Karte, 24
- Grundgesetz, 7
- Hardware, 22
- homomorphe Verschlüsselung, 47
- i-vote, 7, 27, 35
- Image
 - modernes, 29
- individuelle Verifizierbarkeit, 37, 41, 43, 46
- Internet-Voting-System, 53
- Investitionen, 29
- Kommunikationskomplexität, 37, 46

- Korrektheit, 14, 36, 38, 40, 42, 45, 48
- Kostenbegrenzung, 30
- Literaturtips, 36
- Lobbying, 29
- Maut-System, 30
- Mixes
 - universal verifiable, 49
- Multisignatursysteme
 - blinde, 45
- Neuauszählung, manuelle, 39
- Nichtvermehrbarkeit, 36, 38, 40, 42, 45, 49
- Non-Interactive Zero-Knowledge-Proofs, 48
- Online-Banking, 22
- Online-Voting-System, 53
- Orts-Unabhängigkeit, 43
- Ortsunabhängigkeit, 37, 41, 46, 49
- papierbasierte Wahlmethode, 10
- Parteiengesetz, 8
- physische Voraussetzungen, 37, 41, 43
- politische Motivationen, 28
- Polling-System, 52
- Protokoll
 - eigenschaften , 36
 - Aufzeichnungssystem-, 41
 - dezentrales, 38
 - mit homomorpher Verschlüsselung, 47
 - mit universal verifiable Mixes, 49
 - mit Wahlkarten-Lesesysteme, 39
- Qualität, 30
- Qualitätsstandards
 - Absenkung, 35
- Quittungsfreiheit, 37, 41, 42
- Robustheit, 36, 38, 40, 42, 45
- Sicherheit
 - physische, 22
- Signatur-Funktion, 44
- Signaturgesetz, 27
- Skalierbarkeit, 37, 41, 43, 46
- SmartCard, 23, 27
- Source-Code
 - Offenlegung, 35
- Stimmzettel
 - format, 37
- Telefonkarte, 24
- Testwahlen, 27, 31
- Toll-Collect, 30
- Transfer-Systeme
 - sichere, vergessliche, 47
- Transparenz, 6, 19
- Trojaner, 24
- universal verifiable Mixes, 49
- Universelle Verifizierbarkeit, 49
- universelle Verifizierbarkeit, 37, 38, 41, 46
- Unmittelbarkeit, 37, 38, 41, 42, 46
- USA, 7
- verdeckte Auswertungssysteme, 47
- Verfügbarkeit, 17
- Verifizierbarkeit
 - individuelle, 37, 41, 43, 46
 - universelle, 37, 38, 41, 46, 49
- Versicherten-Karte, 24
- Vertrauen, 24
- Virus, 24
- Voraussetzungen
 - physische, 41, 43
- Voraussetzungen, physische, 37
- Voting-System
 - elektronisches, 52
 - elektronisches für Wahllokale, 53
 - elektronisches mit Wahl-Kiosken, 53
 - Online-, 53

Webbasiert, 53

Wähler-Identifizierung, 24

Wahlgeheimnis, 13, 37, 38, 40, 42, 46,
49

Wahlkarten-Lesesysteme, 39

Wahlkreis 329, 28

Wahlmethode

 papierbasiert, 10

Wahlprotokolle, 36

Wahlsystem

 gesellschaftliche Bedeutung, 5

Wurm, 24

Zero-Knowledge-Proof, 47