e-Voting.at – Vom e-Government zur elektronischen Demokratie

Alexander Prosser/Robert Kofler/Robert Krimmer

Institut für Informationsverarbeitung, Abteilung Produktionsmanagement,
Wirtschaftsuniversität Wien
A-1200 Wien, Pappenheimgasse 35/5
{alexander.prosser, robert.kofler, robert.krimmer}@wu-wien.ac.at

Schlagworte: Elektronische Demokratie, e-Voting

Abstract: Elektronische Transaktionen über das Internet, insbesondere das World Wide Web sind zu einem entscheidenden Faktor im täglichen Wirtschaftsleben geworden. In der jüngeren Vergangenheit begann auch der öffentliche Sektor das Internet für die Abwicklung von administrativen Transaktionen zu entdecken. Diese Arbeit analysiert, wie ein elektronisches Wahlsystem unter Einhaltung der allgemeingültigen Wahlgrundsätze in Österreich realisiert werden kann und im Besonderen wird dabei auf Probleme in Zusammenhang mit der Verwendung einer Signaturkarte eingegangen.

1. Voraussetzungen für e-Voting

Für die Durchführung von Wahlen über das Internet gelten auch die allgemeinen Wahlrechtsgrundsätze entsprechend Art 26 B-VG, die von einem gleichen, unmittelbaren, geheimen und persönlichen Wahlrecht[1] ausgehen. Als spezielle Vorraussetzungen für elektronische Wahlen kann man die Ausarbeitung des Internet Policy Institutes heranziehen [IPI2001]:

- *Freie Wahlen*: jeder Wähler muss in der Lage sein, sein Wahlrecht geheim und ohne Einflussnahme durch einen Dritten abgeben zu können. Die Stimme muss unverändert in der Wahlurne ankommen.
- *Geheime Wahl*: Keine Person darf Kenntnis von der abgegebenen Stimme einer anderen Person erlangen können; die Auszählung der Stimmen muss solange verzögert werden, bis eine genügende Anzahl an Stimmen abgegeben wurde, sodass kein Rückschluss auf das

[1] Für eine weitergehende Behandlung der rechtlichen Rahmenbedingungen in Österreich für e-Voting siehe den Beitrag von *Menzel* in diesem Tagungsband.

Wahlverhalten eines Einzelnen möglich ist (dies ist vergleichbar mit einer Mindestgröße der Sprengel).
- *Gleiche Wahl*: Jede Stimme muss dasselbe Gewicht haben – Keine Stimme darf aufgrund technischer Schwierigkeiten verloren gehen oder ungültig werden. Des Weiteren darf das Recht zu Wählen nicht weiter eingeschränkt werden als in den gesetzlichen Vorgaben.
- *Nachvollziehbarkeit*: Der gesamte Wahlprozess muss nachvollziehbar und wiederholbar sein.

2. Grundproblem: Identifikation und Anonymität

Während die Wahlgrundsätze der Gleichheit und Unmittelbarkeit durch organisatorische Maßnahmen leicht zu bewältigen sind, leitet sich aus den Grundsätzen des persönlichen und geheimen Wahlrechts das technische Grundproblem ab: Wie kann ich im Rahmen eines elektronischen Transaktionsprozesses mich eindeutig identifizieren und dann eine anonyme Stimme abgeben?

Von technischer, wie auch rechtlicher Sicht lehnt man sich bei den Spezifikationen für eine elektronische Wahl an der bewährten (aber in Europa nur in Deutschland, Frankreich und der Schweiz erlaubten) Briefwahl an. [DUJ00]. In Analogie identifizierten *Nurmi*, *Salomaa* und *Santean* bereits 1991 [NSS91] im Rahmen einer eingehenden Analyse des Wahlverfahrens zwei unterschiedliche Vorgänge:

- Der Registrierungsschritt, während dem sich der Wähler eindeutig identifiziert
- Die Stimmabgabe, die anonym erfolgt

Obwohl e-Voting ein verhältnismäßig neues Konzept ist, wurden in den letzten Jahren zahlreiche Systeme entwickelt, die bereits am Markt angeboten werden bzw sich noch im Prototypenstadium befinden. Die Systeme verfolgen dabei die unterschiedlichsten Lösungsansätze, doch haben sich drei Methoden zur Identifikation des Wählers herauskristallisiert:

2.1. PIN-basierte Systeme

Der Wählende arbeitet hier als identifizierter Benutzer über das Internet, nach dem Login kann der Wahlzettel ausgefüllt und abgeschickt wer-

den, wobei die Kommunikation zwischen Browser und Wahlserver kryptographisch gesichert ist.[2]

2.2. TAN-basierte Systeme

Bei solchen Systemen werden TANs ausgegeben, die Wahl ist üblicherweise über eine Internetschnittstelle unter Angabe des TAN möglich. Der Webverkehr zwischen Wählendem und Wahlserver erfolgt verschlüsselt, der Schlüssel wird von einem Trust Center [FFW99], [FiWh00] zugebracht. Der Wählende erhält dabei eine Zufallszahl als Quittung, mit der man an einem anderen Terminal überprüfen kann, ob die Stimme korrekt gezählt wurde.

Bei einer Kollusion der beiden Stellen zur TAN-Ausgabe und Stimmabgabe kann natürlich die Anonymität nicht mehr gewährleistet werden. Als weiterer Nachteil kommt die physische Distribution von TANs pro Wahlakt.

Aufgrund der bisherigen Diskussion stellen die Autoren die falsifizierbare Hypothese auf, dass weder PIN-noch TAN-basierte Systeme für den Einsatz bei Wahlen zu Vertretungskörpern von Körperschaften öffentlichen Rechts über das Internet geeignet sind, da die Sicherung der Anonymität weder bei TANs noch bei PINs technisch garantiert werden kann, sondern von der Integrität der Wahlorganisatoren bzw ihrer technischen Erfüllungsgehilfen abhängt; sowie PIN und TAN als Identifikationsmittel keine gesetzliche Grundlage aufweisen. Die weitere Diskussion konzentriert sich daher auf die dritte Variante, die Realisierung mittels signaturkartenbasierter Systeme unter Verwendung kryptografischer Verfahren.

3. Wahlalgorithmen

3.1. Verfahren nach [FOO93]

Für die Sicherstellung der Anonymität haben *Fujioka*, *Okamoto* und *Ohta* in ihrem Ansatz die Wahlbehörde in zwei voneinander unabhängige Einheiten (Server) unterteilt:

---

[2] Das hier diskutierte Verfahren der PIN-basierten Identifikationssysteme ist nicht zu verwechseln mit der Eingabe von PIN für die Zugriffssicherung bei Signaturkarten.

- Registrierungsserver
- Urnenserver

Das einphasige Verfahren nach [FOO93] sieht vor, dass der gesamte Prozess in einem Vorgang abgewickelt wird. Es beginnt damit, dass der Wähler seinen Stimmzettel ausfüllt und dann mit einem symmetrischen Schlüssel verschlüsselt. Anschließend bereitet er den verschlüsselten Stimmzettel auf die blinde Signatur vor[3]. Diesen unterschreibt er und schickt es an den Registrierungsserver <*k (SZ)*>. Dort überprüft der Server die Identität des Wählers anhand der digitalen Signatur und wenn sie gültig ist, unterschreibt er den Stimmzettel. Darauf wird das blind signierte Dokument dem Wähler zurückgeschickt <*b sig (k (SZ))*> und vom ihm entschlüsselt. Nun besitzt der Wähler einen verschlüsselten, vom Registrierungsserver unterschriebenen, Stimmzettel, den er an den Urnenserver schickt <*b sig (k (SZ))*>. Dieser überprüft die Unterschrift auf dem Stimmzettel, ob diese auch wirklich vom Registrierungsserver stammt. Nach erfolgter positiver Prüfung schreibt der Urnenserver beim ursprünglichen Protokoll die verschlüsselten Stimmzettel auf eine Liste, die nach Ende der Wahl veröffentlicht wird. Der Wähler kann dann überprüfen ob sein verschlüsselter Stimmzettel auf der Liste ist, und wenn ja, dann schickt er dem Urnenserver den Entschlüsselungsschlüssel <*k'*>. Diesen verwendet der Server anschließend um die Stimmzettel zu entschlüsseln und auszuzählen. Nach Ende der Auszählung werden die Schlüssel und die Stimmzettel wiederum auf einer öffentlichen Liste publiziert, damit jeder Wähler unabhängig das Wahlergebnis überprüfen kann.

---

[3] Das Verfahren der blinden Signatur wird im allgemeinen Sprachgebrauch mit der Leistung der Unterschrift auf einem Blaupapierkuverts verglichen. Für eine eingehendere Erklärung siehe [Chau82].

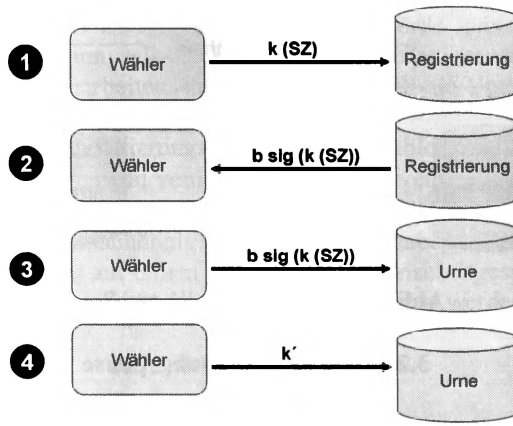

Abbildung 1: *Ablaufdiagramm [FOO93]*

Dieses Verfahren wurde bereits vielfach variiert und hat doch in allen Varianten ein grundlegendes Problem: Es ist als Ein-Phasen-Algorithmus konzipiert, das bedeutet, dass die zwei Schritte Identifizierung und Wahlvorgang in einem erledigt werden. Das ermöglicht, wenn der Registrierungs- und der Urnenserver zusammenarbeiten, das Brechen der Anonymität sowie das Einschleusen von Stimmen für wahlberechtigte Personen, die nicht zur Wahl gegangen sind.

3.2. Verfahren nach *Prosser/Müller* [PrMü01]

Auch dieser Algorithmus geht von den zwei unabhängigen Wahlbehördeeinheiten Registrierungs- und Urnenserver aus. Allerdings gibt es einen grundsätzlichen Unterschied, denn hier wird basierend auf der Analyse von [NSS91] der Wahlprozess in zwei nacheinander ablaufenden, aber zeitlich unabhängigen Phasen getrennt:

- Phase (1): Die Registrierungsphase, während der der Wähler identifiziert ist, wobei sich der Wähler zusätzlich bei seinem Trust Center eine blind signierte Bestätigung holt.
- Phase (2): Die Stimmabgabenphase, bei der die anonyme Stimme abgegeben wird und bei der der Wähler nicht identifiziert werden kann.

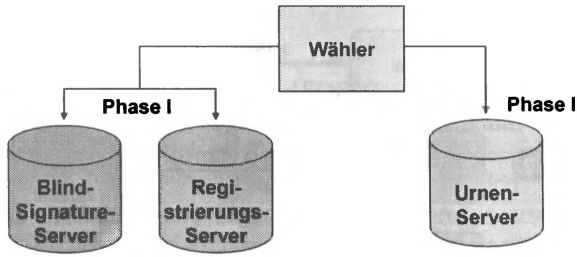

Abbildung 2: *Die beteiligten Parteien*

3.2.1. Die Registrierungsphase

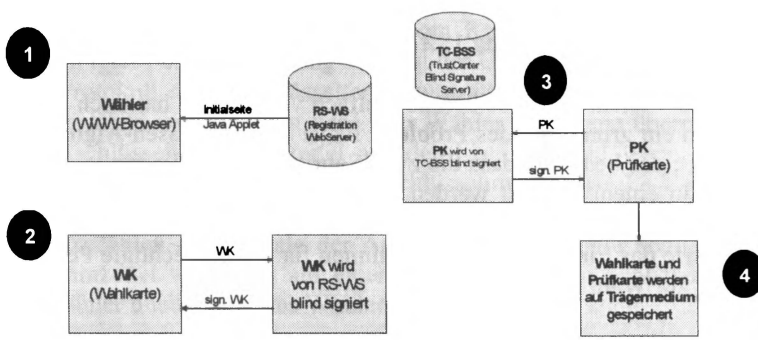

Abbildung 3: *Ablaufdiagramm Registrierungsphase*

3.2.1.1. Schritt 1 – Registrierung

Zuerst generiert der Wähler ein Token und bereitet sie auf die blinde Unterschrift vor, das er dann mit der digitalen Unterschrift seiner Signaturkarte unterschreibt. Dieses Paket schickt er nun an den Registrierungsserver, der seine Wahlberechtigung aufgrund der Unterschrift überprüft, dieses blind unterschreibt und an den Wähler retourniert. Der Wähler entschlüsselt das Paket und hat damit ein vom Server unterschriebenenes Token bzw eine von der Wahlbehörde unterschriebene elektronische Briefwahlkarte.

Anschließend wird der selbe Vorgang wie mit dem Registrierungsserver mit dem Blind Signature Server im Trust Center wiederholt, um sich

die elektronische Briefwahlkarte auch vom ihm blind unterschreiben zu lassen. Dies hat den Zweck, dass die Wahlbehörde keine gefälschten Stimmen abgeben kann, selbst wenn der Registrierungsserver und der Urnenserver zusammenarbeiten, da sie ja immer auch die Unterschrift vom unabhängigen Blind Signature Server benötigen.

Am Ende der Registrierungsphase hat der Wähler eine elektronische Briefwahlkarte, die sowohl vom Registrierungsserver als auch vom Blind Signature Server im Trust Center blind unterschrieben wurde. Nachdem die Phase 1 zeitlich unabhängig von der Stimmabgabephase ist, muss diese Wahlberechtigung auf einem Trägermedium zwischengespeichert werden und auf die Anonymität des Mediums Wert gelegt werden.

3.2.2. Stimmabgabephase

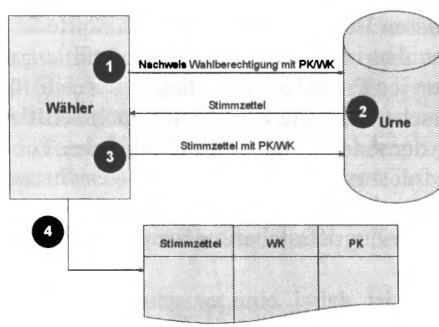

Abbildung 4: *Ablaufdiagramm Stimmabgabephase*

Die zweite Phase des Wahlprozesses findet am eigentlichen Wahltag statt. Damit der Wähler wählen kann, verwendet er seine elektronische Briefwahlkarte (Token), die auf dem Trägermedium gespeichert ist. Er schickt diese an den Urnenserver, der die Validität mittels der öffentlichen Schlüssel von Registrierungs- und Blind Signature Server überprüft. Sind beide gültig, schickt er dem Wähler einen Stimmzettel. Das wird dann vom Wähler ausgefüllt und zusammen mit der Wahlberechtigung an den Urnenserver geschickt. Nach Ende der Wahl veröffentlicht der Urnenserver eine Liste mit Stimmzettel und zugehöriger elektronischer Briefwahlkarte.

3.2.3. Die Zwischenspeicherung und das Trägermedium

Die Wahl des Trägermediums ist der kritische Faktor für die Durchführbarkeit einer Wahl basierend auf dem Prosser/Müller Algorithmus. Für diese Zwischenspeicherung der elektronischen Briefwahlkarte (Token) sehen wir grundsätzlich drei Möglichkeiten:

3.2.3.1. Auf der Signaturkarte

Vorteil der Speicherung des Token auf der Signaturkarte des Wahlberechtigten ist der Schutz vor Datenverlust gegenüber konventionellen Speichermedien und der Schutz vor dem Auslesen, wenn das Token durch einen PIN gesichert wird. Diese Variante hat aber zwei wesentliche Schwierigkeiten:

- zum einen muss das Signaturgesetz des betreffenden Landes einen frei beschreibbaren Bereich in einer Signaturkarte überhaupt zulassen (in der EU ist dies durch die Signaturrichtlinie gegeben) und der betreffende Service Provider muss diesen Bereich für die Benutzung tatsächlich vorsehen bzw die Karte dafür auch zertifiziert sein.
- zur Sicherung der Anonymität beim Senden des Tokens an die Urne, darf es keine frei auslesbaren, nicht PIN-gesicherten Informationen auf der Karte geben, die Rückschlüsse auf den Karteninhaber zulassen, die ohne Zugriffssicherung ausgelesen werden können.

Der letzte Punkt ist dabei eine entscheidende Einschränkung und ergibt sich vollkommen unabhängig, ob Registrierung und Stimmabgabe in einer oder in zwei Phasen erfolgen. Regelmäßig wird nämlich von den Providern der Name des Karteninhabers ungeschützt im Klartext auf der Karte gespeichert, außerdem hat jede Signaturkarte der Welt eine eindeutige Seriennummer, die bei Erzeugung der Karte gesetzt wird, wobei diese Seriennummer ein Tracking der Karte von der Initialisierung beim Trust Center-Betreiber über die Ausgabe an den Kunden bis hin zum Karteninhaber zulässt. Selbst wenn die Software des Wahlbetreibers im Sourcecode offen gelegt wird und dieser Code nachweislich nicht auf die Kartenseriennummer oder andere Klartextinformation auf der Karte zugreift, wird dies als Absicherung in einem solch sensiblen Bereich vermutlich kaum reichen, um Akzeptanz beim Bürger zu erreichen. Alternativ wäre auch eine Modifikation des Betriebssystems der Signaturkarte denkbar, wodurch ein Auslesen dieser Seriennummer verhindert werden könnte bzw mit einem zusätzlichen Zugriffsschutz (PIN) versehen würde.

3.2.3.2. Auf einem beliebigen Datenträger analog zu einer elektronischen Geldbörse

Diese Variante löst sofort die eben diskutierten Probleme mit Seriennummer und Klartextinformation: bei Registrierung legt der Wählende beispielsweise eine Diskette oder einen USB-Schlüssel ein und das Token wird darauf zwischengespeichert. Die Implementierung wäre einfach und benötigte ausschließlich allgemein verfügbare Infrastruktur, wie Diskettenlaufwerke oder USB-Ports. Der Nachteil dieser Lösung besteht im unsicheren und gegen Kopieren und Auslesen keinerlei geschützten Medium. Sichere USB-Schlüssel sind derzeit in Entwicklung aber noch nicht ausgereift.

3.2.3.3. auf einer anderen Prozessor-Chipkarte als der Signaturkarte

Die Signaturkarte wird ausschließlich zur Identifikation beim Registrator eingesetzt, die Speicherung der elektronischen Briefwahlkarte erfolgt auf der zweiten Karte und wird durch End-to-End-Verschlüsselung gesichert. Bei der Stimmabgabe im Dialog mit der Urne wird ausschließlich die zweite Karte eingesetzt.

Die Nachteile dieser Variante bestehen im komplizierteren Handling (während des Registrierens muss die Karte umgesteckt werden) und in der Tatsache, die Karte mit der Wahlberechtigung nun nicht mehr einer Person zugeordnet ist, wie dies bei der Signaturkarte der Fall war.

4. Schlusswort

Dieser Beitrag zeigt, dass Design und Realisierung eines e-Votingsystems komplex und keinesfalls trivial sind, wenn die Einhaltung der Wahlrechtsgrundsätze bei der Abwicklung der Wahl technisch garantiert werden sollen. Erschwert wird die Implementierung durch die offensichtliche Nichteignung der vorhandenen Signaturkarten für die Zwischenspeicherung bzw den Einsatz einer anonymen Wahlberechtigung, die erst durch ein entsprechendes Redesign überwunden werden kann; insbesondere indem dem Anwender die volle Kontrolle darüber gegeben wird, welche Daten von einer Applikation ausgelesen werden, die auf die Karte zugreift.

Literatur

[Chau82] *Chaum, D.*: Blind Signatures for Untraceable Payments in: *Chaum, D., Rivest, R.L., Sherman A.T.* (Hrsg): Advances in Cryptology, Proceedings of Crypto 82, S 199-203.

[DUJ00] *Dujmovits, W*: Auslandsösterreicherwahlrecht und Briefwahl, Verlag Österreich, Vienna 2000.

[FFW99] *Feghhi, J., Feghhi, J., Williams, P.*: Digital Certificates – Applied Internet Security; Addison-Wesley, Reading, 1999.

[FiWh00] *Fish, E.A., White, G.B.*: Secure Computers and Networks, Analysis, Design and Implementation; CRC Press, Boca Raton, 2000.

[FOO93] *Fujioka, A., Okamoto, T., Ohta, K.*: A Practical Secret Voting Scheme for Large Scale Elections; Advances in Cryptology – AUSCRYPT92, Springer-Verlag, Berlin, 1993, S 244-251.

[IPI01] Internet Policy Institute; Report on the National Workshop on Internet Voting downloadable unter http://www.internetpolicy.org/research/e_voting_report.pdf (13.05.2001).

[NSS91] *Nurmi, H., Salomaa, A., Santean, L.*: Secret ballot elections in computer networks; Computers and Security 36 (10), 1991, S 553-560.

[ProMü01] *Prosser, A., Müller, R.*: Vom E-Government zur E-Democracy, eingereicht bei Wirtschaftsinformatik.