Chipkarten für elektronische Wahlen: Eine Anforderungsanalyse

Martin Karl Unger

Institut für Informationsverarbeitung und Informationswirtschaft,
Abteilung Produktionsmanagement
Wirtschaftsuniversität Wien,
A-1090 Wien, Augasse 2–6
martin.unger@wu-wien.ac.at

Schlagworte: Chipkarte, smart card, e-voting

Abstract: Die aus den Phasen Wahlkartenausstellung und Stimmabgabe bestehende Vorgehensweise der Initiative e-Voting.at[1] stellt an die idealer Weise zu verwendenden Chipkarten Anforderungen in Bezug auf die Identifizierung des Wahlberechtigten, die Anfertigung digitaler Signaturen, die Speicherkapazität, Zugriffsschutz sowie die Implementierbarkeit kryptographischer Algorithmen.

1. Begriff e-Voting[2]

Unter e-Voting (electronic voting) wird hier die elektronische Distanzwahl über das Internet verstanden. Der Wähler soll kein Wahllokal aufsuchen müssen. Dadurch erfolgt eine Abgrenzung zur Stimmabgabe mittels einer in der Wahlzelle aufgestellten Wahlmaschine. Das hier vorgestellte System lässt sich allerdings auch einsetzen, indem in einer Wahlzelle ein Computer mit Internetanschluss aufgestellt wird.

Das hier besprochene System der Initiative e-Voting.at kann durch seine zweiphasige Vorgehensweise und durch die Verwendung eines speziellen kryptographischen Verfahrens, welches als „blinde digitale Signatur" bekannt ist, auch die in Artikel 26 der österreichischen Bundesverfassung festgeschriebenen Wahlrechtsgrundsätze des gleichen Wahlrechts (jeder Wahlberechtigte darf nur eine Stimme abgeben) und des geheimen Wahlrechts (niemand darf das Abstimmungsverhalten eines bestimmten Wählers erfahren) auf technischem Weg garantieren.

---

[1] Nähere Informationen zur Forschungsgruppe e-Voting.at findet sich auf der Website http://www.e-Voting.at.

[2] Vgl *Prosser, A., Kofler, R., Krimmer, R., Unger, M.-K.*, The Role of Digital Signature Cards in Electronic Voting, Proceedings of 37th Annual Hawaii International Conference on System Sciences (CD/ROM), Computer Society Press, 2004.

2. Zweiphasige Vorgehensweise

Die Vorgehensweise der Initiative e-Voting.at besteht aus zwei zeitlich voneinander getrennten Phasen: der Wahlkartenausstellung und der Stimmabgabe.

2.1. Wahlkartenausstellung

Bei der Phase der Wahlkartenausstellung wird der Wahlberechtigte eindeutig identifiziert. Der Computer des Wahlberechtigten kommuniziert über das Internet mit zwei anderen Computern, um die elektronische Wahlkarte zu erzeugen. Das ist ein fälschungssicherer Datenbestand, der in einer kleinen Datei auf einem Datenträger des Wahlberechtigten gespeichert wird. Aus der Sicht der Software, die auf dem Computer des Wahlberechtigten läuft, lässt sich dieser Vorgang vereinfacht in sieben Schritten darstellen:

(1) *Identifikationsdaten einsenden:* Der Wahlberechtigte stellt Daten zur Verfügung, welche ihn eindeutig identifizieren. Das kann zum Beispiel die Stammzahl des österreichischen Bürgerkartenkonzepts[3] sein. Diese Daten werden über das Internet an einen Computer der Wahlbehörde gesendet, welcher anhand seiner als „elektronische Wählerevidenz" bezeichneten Datenbank feststellt, ob die durch die betreffenden Daten identifizierte Person an der Wahl, für die eine elektronische Wahlkarte beantragt wird, teilnehmen darf.

(2) *Wahlkreisinformation empfangen:* Der Computer des Wahlberechtigten empfängt vom Computer der Wahlbehörde wahlkreisspezifische Daten: Die Bezeichnung des Wahlkreises und den öffentlichen Schlüssel des Wahlkreises. (Der zu diesem öffentlichen Schlüssel gehörende private Schlüssel ist auf dem Computer der Wahlbehörde gespeichert und bleibt geheim.)

(3) *Blinde Signatur vorbereiten:* Der Computer des Wahlberechtigten ermittelt zwei geeignete ganze Zahlen, die im weiteren als T und R bezeichnet werden. Jede dieser Zahlen besteht aus mehr als hundert Ziffern. Die Zahl T wird unter Verwendung der Zahl R und des öffentlichen Schlüssels des Wahlkreises verschlüsselt. Das Ergebnis dieser Verschlüsselung ist eine große ganze Zahl und wird im weiteren als X bezeichnet.

(4) *Antrag einsenden:* Der aus einem kurzen Antragstext, der Wahlkreisbezeichnung und der im vorigen Schritt ermittelten Zahl X bestehende Antrag auf Ausstellung einer elektronischen Wahlkarte kann vom

[3] Laut E-Government-Gesetz kann die eindeutige Stammzahl auch ein anderer Identifikationsfaktor sein, etwa die Matrikelnummer auf Studentenservicecards.

Wahlberechtigten elektronisch signiert werden (wofür zum Beispiel die Signaturfunktionalität der österreichischen Bürgerkarte verwendet werden kann) und wird dann an den Computer der Wahlbehörde gesendet, welcher den Antrag (und die ihn ihm enthaltene Zahl X) mit dem privaten Schlüssel des Wahlkreises elektronisch signiert und in der Wählerevidenz vermerkt, dass eine elektronische Wahlkarte ausgestellt wurde.

(5) *Blinde Signatur empfangen:* Der Computer des Wahlberechtigten empfängt die im vorigen Schritt erstellte digitale Unterschrift.

(6) *Blinde Signatur auflösen:* Der Computer des Wahlberechtigten berechnet aus der vom Computer der Wahlbehörde erstellten digitalen Unterschrift diejenige Zahl, die entstanden wäre, wenn der Computer der Wahlbehörde die Zahl T (und nicht die Zahl X) digital unterschrieben hätte. Das Ergebnis ist eine große ganze Zahl, die als T^D bezeichnet wird.

(7) *Elektronische Wahlkarte speichern:* Der erwähnte Antragstext, die Wahlkreisbezeichnung und die Zahlen T und T^D bilden Teile der elektronischen Wahlkarte, die auf einem Speichermedium des Wahlberechtigten, zum Beispiel seiner Bürgerkarte, gespeichert wird. Da der Computer der Wahlbehörde nur die Zahl X, aber nicht die Zahlen T und R gesehen hat, ist die elektronische Wahlkarte anonym und enthält keinen Hinweis auf die Identität des Wahlberechtigten.

Tatsächlich führt die Software auf dem Computer des Wahlberechtigten mehr als sieben Schritte aus. Sie kontaktiert noch einen zweiten Computer (zwecks Anfertigung einer zweiten blinden digitalen Signatur), sie ermöglicht die Verschlüsselung der elektronischen Wahlkarte durch ein vom Wahlberechtigten gewähltes Passwort und sie sichert den Wahlberechtigten gegen den Schaden, der entsteht, wenn während Schritt Nummer fünf die Internetverbindung zusammenbricht. Aus der Sicht des Wahlberechtigten besteht der ganze Vorgang, der nur zwei oder drei Minuten dauert, aus weniger als sieben Schritten.

2.2. Stimmabgabe

Am Wahltag, also einige Tage oder Wochen nach der Ausstellung der Wahlkarte, benutzt der Wahlberechtigte die elektronische Wahlkarte, um ohne Preisgabe seiner Identität nachzuweisen, dass er wahlberechtigt ist. Auch aus der Sicht der Software auf dem Computer des Wahlberechtigten lässt sich der Vorgang in sieben Schritten darstellen:

(1) *Wahlkarte einlesen:* Die elektronische Wahlkarte wird vom Speichermedium des Wahlberechtigten gelesen.

(2) *Wahlkarte einsenden:* Die Wahlkarte wird über das Internet an einen als „elektronische Wahlurne" bezeichneten Computer der Wahlbehörde geschickt, welcher die Korrektheit der elektronischen Wahlkarte prüft, aus ihr aber nichts über die Identität des Wahlberechtigten erfährt. Bei dieser Prüfung wird unter anderem die Zahl T^D mit dem öffentlichen Schlüssel des Wahlkreises verschlüsselt. Das Ergebnis muss gleich der Zahl T sein.
(3) *Stimmzettel empfangen:* Der Computer des Wahlberechtigten empfängt von der elektronischen Urne den Stimmzettel.
(4) *Stimmzettel anzeigen:* Der Stimmzettel wird am Bildschirm angezeigt und der Wahlberechtigte nimmt durch Mausklick seine Wahl vor.
(5) *Schutz vor Übereilung:* Um zu vermeiden, dass der Wählerwille durch eine Fehlbedienung der Maus verfälscht wird, zeigt die Software dem Wahlberechtigten, was er angekreuzt bzw angeklickt hat, und er kann einen eventuellen Fehler korrigieren.
(6) *Stimmzettel verschlüsseln:* Der Stimmzettel wird mit den öffentlichen Schlüsseln der Wahlkommissionsmitglieder verschlüsselt. Die privaten Schlüssel der Wahlkommissionsmitglieder werden erst nach dem Ende der für die Stimmabgabe anberaumten Zeitspanne der elektronischen Wahlurne übermittelt.
(7) *Stimmzettel einsenden:* Der verschlüsselte Stimmzettel wird an die elektronische Wahlurne gesendet.

3. Resultierende Anforderungen

Die aus dem beschriebenen Ablaufschema resultierenden Anforderungen lassen sich in die Kapitel Datenerzeugung, Datenverarbeitung und Datenspeicherung untergliedern.

3.1. Datenerzeugung

In der Phase „Wahlkartenausstellung" werden Identifikationsdaten, Signaturen und blinde Signaturen benötigt.

Als *Identifikationsdaten,* also Daten, die den Wahlberechtigten identifizieren, kommt zum Beispiel die Stammzahl der österreichischen Bürgerkarte in Frage. Weniger geeignet für die Wahlkartenausstellung im Rahmen der Stimmabgabe über das Internet scheinen dem Autor biometrische Daten, wie etwa Fingerabdruck und Netzhautmuster, weil sie vor der Wahl gesammelt werden müssten, um in der elektronischen Wählerevidenz aufzuscheinen, und Transaktionsnummern, weil sie vor der Wahl auf einem sicheren Transportweg verteilt werden müssten, um bei der Wahlkartenausstellung eingesetzt werden zu können.

Zur *Authentisierung* des Antrags auf Ausstellung einer elektronischen Wahlkarte kommt vor allem die elektronische Signatur in Frage, wie sie mit der österreichischen Bürgerkarte oder einer anderen Signaturkarte erstellt werden kann. Vorbereitung und Auflösung der *blinden digitalen Signatur*[4] erfordern die Erzeugung von Daten, die für diesen kryptographischen Algorithmus geeignet sind.

3.2. Datenverarbeitung

Der Algorithmus der blinden digitalen Signatur erfordert „lokale Intelligenz" auf dem Rechner des Wahlberechtigten, wie sie zB durch die Java Laufzeitumgebung zur Verfügung gestellt wird. Die benötigte Version 1.4 wird von der Herstellerfirma Sun Microsystems zum kostenfreien Download im Internet angeboten.[5]

Die mögliche Auslagerung der zur blinden digitalen Signatur gehörenden kryptographischen Operationen auf den Prozessor der Chipkarte macht die Phase der Wahlkartenausstellung resistent gegen eventuell auf dem Computer des Wahlberechtigten vorhandene Viren und andere Schadprogramme. Diese Auslagerung erfordert, dass die benötigten kryptographischen Routinen auf der Chipkarte vorhanden sind und dort abgearbeitet werden können.

Die sichere Datenübertragung zwischen dem Computer des Wahlberechtigten und den Computern der Wahlbehörde kann durch Verschlüsselung auf der Chipkarte oder durch Verwendung des Datenübertragungsprotokolls SSL[6] (Secure Sockets Layer) gewährleistet werden.

3.3. Datenspeicherung

Die elektronische Wahlkarte soll auf einem *transportablen Speichermedium* aufbewahrt werden, damit Wahlkartenausstellung und Stimmabgabe von unterschiedlichen Orten aus erfolgen können. Idealerweise wird die elektronische Wahlkarte auf der selben Chipkarte gespeichert, mit der auch die elektronische Unterschrift zur Authentisierung des Antrags auf Ausstellung der Wahlkarte erstellt wird, und die der Wahlberechtigte, ähnlich einer

---

[4] *Chaum, D.*, Untraceable electronic mail return addresses and digital pseudonyms, in: Communications of the ACM, Vol 24(2)/1981, 84–88.

[5] Siehe http://java.sun.com/j2se/1.4.2/download.html, abgerufen am 18. 4. 2004.

[6] Das SSL v3 Protokoll wurde von Netscape entwickelt (siehe *Netscape*, SSL 3.0 Specification, 1996, http://wp.netscape.com/eng/ssl3/3-SPEC.HTM, abgerufen am 20. 4. 2004), auf dessen Basis der TLS 1.0 Standard von der Internet Engineering Task Force entwickelt wurde (siehe *IETF*, Request for Comment #2246, 1999, http://www.ietf.org/rfc/rfc2246.txt, abgerufen am 20. 4. 2004.

Kreditkarte oder Bankomatkarte, ständig mit sich führt. Trotz ihrer geringen Größe von wenigen Kilobyte beansprucht die elektronische Wahlkarte einen Großteil der Speicherkapazität mancher heutiger Signaturkarten, woraus sich für die Chipkarte die Anforderung der *ausreichenden Speicherkapazität* ergibt.

Der unbedingt notwendige *Schutz der Wahlkarte vor unberechtigten Personen* wird erreicht, indem sie vor der Speicherung mit einem vom Wahlberechtigten vergebenen Passwort verschlüsselt wird, oder indem sie auf einem durch ein Passwort gesicherten Bereich der Chipkarte (wie etwa einer „Infobox" der österreichischen Bürgerkarte) gespeichert wird.

Die Verwendung ein und derselben Chipkarte für die Speicherung der den Wähler identifizierenden Daten (zB Stammzahl der österreichischen Bürgerkarte) und für die Speicherung der elektronischen Wahlkarte erfordert den *Schutz der Identifikationsdaten vor unberechtigten Programmen*, damit nicht bei der Stimmabgabe die Identität des Wahlberechtigten von seiner Chipkarte gelesen werden kann.

4. Zusammenfassung

Die Chipkarte in der Hand des Wahlberechtigten kann das aus zwei Phasen bestehende Verfahren der elektronische Distanzwahl ideal unterstützen, wenn sie folgende Anforderungen erfüllt:

1. Schutz der elektronischen Wahlkarte vor unberechtigtem Zugriff,
2. Identifizierung des Wahlberechtigten bei Ausstellung der e-Wahlkarte,
3. Authentisierung des Antrags auf Ausstellung einer elektronischen Wahlkarte durch Erstellung einer digitale Signatur unter diesen Antrag,
4. Schutz der den Wahlberechtigten identifizierenden Daten vor unberechtigtem Zugriff,
5. ausreichende Speicherkapazität zur Aufbewahrung der elektronischen Wahlkarte,
6. im Prozessor der Chipkarte ausführbare kryptographische Routinen zur Vorbereitung und Auflösung der blinden digitalen Signatur.

Die österreichische Bürgerkarte[7] erfüllt zur Zeit die ersten drei, nicht aber die letzten drei aufgezählten Anforderungen.

[7] Vgl *„Bürgerkarte – Wer hat Zugriff auf die Bürgerkarten-Daten?"* an der URL http://www.buergerkarte.at/de/datenschutz/wer_hat_zugriff.html, abgerufen am 1. 5. 2004.