Die sichere Stimmabgabe über das Internet: Kryptographie und Infrastruktur

Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger

Abteilung Produktionsmanagement
Wirtschaftsuniversität Wien
Augasse 2-6
A-1090 Wien
{vorname.nachname}@wu-wien.ac.at

Robert Müller-Török¹

Beratungsgesellschaft für Beteiligungsverwaltung Leipzig GmbH
Ferdinand-Rhode Straße 16
D-04107 Leipzig
mueller.toeroek@bbvl.de

Abstract: Zahlreiche Prototypen und Feldversuche zeigen das bestehende Interesse an e-Voting. In jedem Fall sind aber die Wahlrechtsgrundsätze einzuhalten und insbesondere die Anonymität in der Stimmabgabe zu berücksichtigen. Der Beitrag analysiert zunächst das bestehende Angebot an kryptographischen Protokollen, doch ist diese kryptographische Anwendungsschicht nur ein Teil des Gesamtsystems. Ebenso sind die benötigte Infrastruktur und deren Absicherung zu beachten. Im Hinblick auf diese Kriterien berichtet der Beitrag über die im Mai 2003 durchgeführte e-Voting Testwahl an der Wirtschaftsuniversität Wien, insbesondere die dabei gemachten Erfahrungen in Bezug auf die Infrastruktur.

¹ Der Beitrag drückt die persönliche Meinung des Autors aus.

1. Problemstellung

Internetwahlen (e-Voting) sind zu einer realen Möglichkeit geworden, es müssen aber die Grundsätze der allgemeinen, gleichen, unmittelbaren, persönlichen, geheimen und freien Wahlen eingehalten werden [WaMe82, S. 93f]. Im folgenden wird e-Voting immer als remote e-Voting über das Internet verstanden – Systeme zur Automation der Wahlzelle oder remote e-Voting über andere Medien (z.B. SMS) sind nicht Gegenstand der Überlegungen. Das Internet Policy Institut hat speziell im Hinblick auf e-Voting daraus folgende Forderungen abgeleitet [IPI01, S. 7ff]: (i) korrektes Zählen der Stimmen, (ii) unehrliche Wähler können die Wahl nicht stören, (iii) permanente Anonymität, (iv) jeder Wähler kann nur einmal, gleich in welcher Form, ob konventionell oder mit e-Voting, wählen, (v) nur autorisierte Wähler können wählen, (vi) Unabhängigkeit (keine unstatthafte Einwirkung auf den Wähler), (vii) Nachvollziehbarkeit, (viii) Quittungsfreiheit (um Stimmenkauf zu vermeiden).

Für das Design eines kryptographischen Algorithmus lassen sich daraus drei Hauptforderungen zusammenfassen:

- eindeutige Identifizierung des Wahlberechtigten bei gleichzeitig
- vollkommen gesicherter Anonymität in der Stimmabgabe.
- Außerdem darf die Systemadministration der Wahlbetreiber keinerlei Möglichkeit haben (i) die Anonymität zu unterlaufen oder (ii) Stimmen zu manipulieren.

2. Wahlprotokolle

2.1 Nichtkryptographische Verfahren

Bei PIN-basierten Systemen arbeitet der Wähler als identifizierter Benutzer im Internet. Nach einem Login kann der Stimmzettel ausgefüllt und zur Wahlurne gesendet werden, wobei die Kommunikation zwischen Browser und dem Wahlserver mittels kryptographischer Standards gesichert wird. Es ist offensichtlich, dass in solchen Systemen die Anonymität nicht gesichert werden kann (für ein Beispiel siehe [SCCE01]).

Bei TAN-basierten Systemen werden Transaktionsnummern an die Wähler mittels herkömmlicher Post versandt. Jede einzelne TAN ermöglicht einem Wähler seine Stimme abzugeben (siehe [Fell01], [CEG00]). Der Wähler bekommt eine Quittung für die Stimmabgabe in Form einer Zufallsnummer, welche dann bei einer anderen Website zur Überprüfung eingesetzt werden kann, ob die eigene Stimme korrekt ins Endergebnis eingeflossen ist. Wenn die TAN-ausgebende Stelle mit der Stelle, die den Wahlurnenserver betreibt, kolludiert, dann kann die Anonymität leicht unterlaufen werden.

In der Literatur sind mehrere Ansätze bekannt, um unter Verwendung kryptographischer Protokolle elektronische Wahlen umzusetzen. In einer grundlegenden Publikation haben Nurmi et.al. [NSS91] zwei Basis-Elemente jedes e-Voting Systems identifiziert: Die Wählerevidenz zur Identifizierung und Zuordnung des Wählenden und die Wahlurne zur anonymen Stimmabgabe.

Anonymer Kanal

Diese e-Voting Prototypen gehen zurück auf den Vorschlag von Chaum's MIX Netzen [Cha81], bei der die ursprüngliche Nachricht mit den öffentlichen Schlüsseln mehrerer Server verschlüsselt wird und dann von einem Server an den anderen überreicht wird, und von jedem mittels dessen privaten Schlüssel dechiffriert wird. Anschließend wird die Nachricht an den jeweils nächsten Server in der Reihe mit einer anderen Reihenfolge (dies ist der entsprechende MIX Vorgang) weitergereicht. Dieser Ansatz – den Chaum für einen vollkommenen anderen Einsatzbereich vorgesehen hat – weist mehrere strukturelle Probleme in Zusammenhang mit e-Voting auf:

- Zumindestens einer der MIX-Server muss vertrauenswürdig sein; wenn die Zahl der Server laufend erhöht wird, wird das Protokoll langsamer und fehleranfälliger.
- Die Lösung stellt hohe Anforderungen an die Infrastruktur, die während der Wahltag benötigt wird.
- Um Mixer am Einschleusen von manipulierten Stimmen in den Mixer Prozess zu hindern, muss ein Mechanismus gefunden werden, um die Stimme zu authentisieren. Dies kann durch zwei Ansätze realisiert werden – entweder durch eine blinde Signatur nach [Cha87] von einem Dritten, dem vertraut wird, oder die Stimme wird durch den Wähler verschlüsselt und der Schlüssel wird zur Dechiffrierung später eingesendet. Vergleiche auch das Protokoll von [FOO93]. Dieser Schritt führt nicht nur zu einer erhöhten Komplexität, sondern kann auch zum Unterlaufen der Anonymität verwendet werden. Hiermit wird nämlich eine End-zu-End-Verknüpfung zwischen dem Wähler und dem Urnenserver aufgebaut, was durch den Mixer eigentlich verschleiert werden sollte.

Erweiterungen des ursprünglichen Protokolls können von Park et.al. [PIK94] und von Sako und Kilian [SaKi95] gefunden werden. Allerdings konnten beide Protokolle gebrochen werden [Pf89, HoMi96]. Spätere Versuche durch Abe [Abe98] und Jakobsson [Jak98, Jak99] trugen neben algorithmischen Verbesserungen vor allem zur Stabilität und zur Geschwindigkeit des Protokolls bei. Ebenso wurde der Verarbeitungsaufwand auf der Seite des Wählers (Client) drastisch reduziert (ein gemeinsamer Schlüssel anstelle von mehreren Schlüssel); diese Verbesserungen müssen dennoch erst analysiert und in Prototypimplementationen getestet werden, um zu sehen, ob die grundlegenden Schwierigkeiten in MIX Netzen komplett gelöst wurden.

All-or-nothing disclosure of secrets (ANDOS)

ANDOS Protokolle bieten einen anonymen Sender-Kanal. Sie emulieren dabei den anonymen Kauf eines Bitstrings [BCR87]. Folglich kann dieses Protokoll für ein- und zwei-phasige Protokolle verwendet werden. Nurmi et al. [NSS91] und Salomaa [Sal91] haben die Ausgabe von Wahlkarten mittels ANDOS vorgeschlagen, die dann für die anonyme Stimmabgabe benutzt werden können. Verbesserungen des Protokolls in Bezug auf die Effizienz und Komplexität wurden von Niemi [Nie94] und Hassler und Posch [HaPo95] vorgeschlagen. Die Hauptnachteile von ANDOS Protokollen sind ihre beschränkte Skalierbarkeit und die Möglichkeit des Stimmenkaufs, da der Wähler selbst nachweisen kann, wie er gewählt hat. Beide Nachteile werden durch diese Verbesserungen nicht behoben. Der Aspekt des Stimmenkaufs wurde von Niemi und Renvall in einem späteren Artikel angesprochen, allerdings setzt der Algorithmus die Verwendung einer sicheren Wahlzelle voraus und beansprucht hohe Computerrechenkapazität [NiRe95].

Homomorphismus

Die Stimme wird bei diesem Verfahren in einer binären Ja/Nein Darstellung der Stimme repräsentiert und in einem homomorphen Schema chiffriert. Dann wird die Stimme an mehrere Wahlurnen übermittelt. Aufgrund der Eigenschaft des Homomorphismus ist es möglich die Ja/Nein Stimmen zu summieren ohne die individuellen Stimmen zu kennen [CGS97]. Dieser Vorteil ist auch das Hauptproblem des Ansatzes, denn es können nur binäre Stimmen abgebildet werden. Es wäre natürlich denkbar die Auswahl einer Partei mittels einer Serie von Ja/Nein Entscheidungen abzubilden. Dies impliziert aber die Prüfung, dass nur ein Eintrag als Ja ausgewählt wird. Weiters bleibt es fragwürdig, ob ein solches Protokoll entsprechend skalierbar wäre.

Blinde Signatur

Der blinde Signatur Mechanismus kann in Verbindung mit MIX Netzwerken verwendet werden, um die Authentisierung einer Stimme zu ermöglichen, nachdem sie einen MIX Kanal durchlaufen hat oder als Abbildung in einem eigenständigen Wahlprotokoll. Die blinde Unterschrift kann hier entweder auf den Stimmzettel oder eine blind unterschriebene Wahlkarte aufgebracht werden, mit der dann der Stimmzettel anonym abgegeben werden kann.

Der bekannteste Ansatz dazu ist sicherlich der von Fujioka, Okamoto und Ohta [FOO93], der auch mehrfach implementiert wurde. Publierte Implementierungen können in [Riv03] und [CC97] gefunden werden; zwei kommerzielle Produkte von einer österreichischen und einer deutschen Firma scheinen auf dem gleichen Algorithmus aufzusetzen. Nachdem allerdings deren Algorithmus nicht öffentlich verfügbar ist, kann keine definitive Aussage über die verwendeten Algorithmen getroffen werden. Dieses Protokoll hat, trotz seiner Popularität, einige fundamentale Probleme in Bezug auf die Anonymität des Wählers und das Einschleusen falscher Stimmen für Nicht-Wähler von Seiten der Administration. Für eine umfangreiche Kritik siehe [PrMü02]. Das Problem der Einschleusung falscher Stimmen wurde von [BPS94] mit der Einführung von Pseudonymen für die Wähler adressiert. Diese Pseudonyme werden durch einen anonymen Kanal an alle Registrierungsserver geschickt, mit denen dann die Stimme authentisiert werden kann. Dies fügt eine beträchtliche Komplexität zu dem Protokoll und der Artikel äußert sich auch nicht näher über den notwendigen anonymen Kanal; dieser wäre ein entsprechender Ansatz für weitere Forschungsvorhaben. In einer anderen Erweiterung durch Okamoto [Oka96] wird das Problem durch mehrere blinde Signaturserver angegangen. Die Problematik der Anonymität wird durch die Verwendung eines MIX Netzwerks gelöst, was die oben erwähnten Einschränkungen aufwirft. Geschwindigkeitsprobleme mit mehrfachen blinden Signaturservern wurden im Protokoll von [HMP95] durch kaskadierte Mehrfachsignaturen gelöst.

Schneier schlug eine interessante Erweiterung zum blinden Signatur Wahlschema in [Sch96] vor. Sein Protokoll kombiniert Registrierung und Stimmabgabe in einer Phase und die Wähler generieren mehrere leere Stimmzettel und übermitteln diese zu einem Registrierungsserver. Der Server darf die Schlüssel zur Öffnung mancher dieser Stimmzettel anfragen, nur wird schlussendlich ein einziger mit einer blinden Signatur versehen und an den Wähler retour gesendet. Das Protokoll stellt sicher, dass keine falschen Stimmen blind signiert werden, allerdings sichert es in keiner anderen Weise die Anonymität als der Vorschlag in [FOO93]. Dies trifft in gleicher Weise auch auf [BoRi99] zu. Beide verwenden hierzu MIX Kanäle.

Prosser und Müller-Török schlugen ebenfalls ein auf der blinden Signatur-basierendes Protokoll vor, wo im Unterschied zu den oben erwähnten Protokollen eine Wahlkarte und nicht der Stimmzettel blind unterschrieben wird. Ähnlich zu [Oka96] wird ein zweiter blinder Signatur Server verwendet, aber die Anonymität ist nicht von Mixern abhängig. Das Protokoll schützt die Wahl vor korrupten Wählern, die den Wahlablauf stören wollen, als auch vor einer korrupten Wahladministration die Stimmen einschleusen will. Die Anonymität wird insbesondere durch die strikte Trennung von Registrierung und der eigentlichen Stimmabgabephase gesichert. In weiterer Folge ist es notwendig ein sicheres Speichermedium zu verwenden, auf dem die blind signierte Wahlkarte gespeichert wird. Das Protokoll wurde auch bereits implementiert und bestand die in Kapitel 3 und in [PKK03] beschriebene erste Testwahl ohne Probleme.

2.3 Der Protokollvorschlag von Prosser/Müller-Török

Das Protokoll ist für die Verwendung durch eine Bürgerkarte (National ID Card) ausgelegt, die zur Authentisierung/Identifizierung und als Speichermedium verwendet wird. Die generelle Verschlüsselung und die digitale Signatur der ausgetauschten Nachrichten werden in der Darstellung weggelassen, da es sich um Standardfunktionalitäten handelt. In Tab. 1 ist die erste Phase – die Registrierung – dargestellt.

2.3.1 Registrierung

<i>Benutzersicht</i>	<i>Technischer Prozess</i>
	Der Registrator hält ein nach dem RSA-Verfahren gebildetes Schlüsselpaar (e, d) pro Wahlsprengel w bereit; jedes für die Wahl verwendbare Trust Center ein Schlüsselpaar (ε, δ) .
Aufruf der Web-Page zum Lösen einer Briefwahlkarte.	Ein signiertes Java Applet wird geladen, das den Benutzer durch die folgenden Schritte führt.
Einlegen der Bürgerkarte.	Der Wahlberechtigte sendet sein Trust Center-Zertifikat an den Registrator, der nach Auflösen des Zertifikats gegen das Trust Center und der Prüfung der Wahlberechtigung die Kennung des Sprengels w und den zu w passenden Schlüssel e retourniert.
	Der Wahlberechtigte bildet zwei Token t, τ , es wird $b = r^e t \pmod{n}$ und $\beta = \rho^\varepsilon \tau \pmod{n}$ gebildet mit r, ρ als Zufallszahlen.
Signieren des Antrages auf Ausstellen einer elektronischen Wahlkarte durch Eingabe des Freigabe-PINs der Bürgerkartensignatur. Auf Wunsch kann der unterschriebene Text im Secure Viewer angezeigt werden.	Ein Paket aus b, w und ein standardisierter Antragstext für die Ausstellung eines Wahltokens wird signiert und an den Registrator gesendet. Nach der Prüfung der Wahlberechtigung signiert der Registrator $b^d \pmod{n}$ und sendet dies an den Wählenden zurück. Dieser „dividiert“ in der Restklasse durch r und erhält (t, t^d) .
Signieren des Antrages auf Ausstellen einer elektronischen Prüfkarte durch das Trust Center des/der Wahlberechtigten.	Der analoge Prozeß wird mit dem Trust Center durchgeführt, wodurch der Wahlberechtigte den zweiten Teil seines Wahltokens erhält, (τ, τ^δ) .
	Nach Ende der Registrierung werden die beiden Tokenteile $[(t, t^d), (\tau, \tau^\delta)]$ und w auf der Bürgerkarte abgespeichert.
Entnehmen der Bürgerkarte.	

Tabelle 1: Ablauf Phase 1 - Registrierung

2.3.2 Stimmabgabe

Will der/die Wahlberechtigte am Wahltag die Stimme abgeben, erfolgt die Authentisierung ausschließlich über die elektronische Wahl- und Prüfkarte. Dieser Schritt ist vollkommen anonym.

Als eine Maßnahme zur Sicherung gegen Manipulationen durch die Betreiber des e-Voting-Systems werden Wahlbeobachter (Wahlkommission) eingesetzt, die von den kandidierenden Listen gestellt werden. Diese Beobachter generieren vor der Wahl je ein Schlüsselpaar, mit dessen öffentlichem Teil die abgegebenen Stimmzettel vercodiert werden. Bezeichnen wir den Vektor der geheimen bzw. der öffentlichen Kommissionsschlüssel als g, g' . Der geheime Schlüsselteil verbleibt zunächst beim jeweiligen Wahlbeobachter bzw. wird bei einem Notar hinterlegt.

Bei den folgenden Kommunikationsschritten verwendet der Wählende seine digitale Signatur und auch beim Trust Center gehaltene Public Key Kryptographie nicht, da diese Schritte ja streng anonym erfolgen sollen. In Tab. 2 ist der Ablauf dieser Phase dargestellt.

<i>Benutzersicht</i>	<i>Technischer Prozess</i>
Aufruf der Web-Page zur Stimmabgabe.	Signiertes Java Applet, das den Benutzer durch die kommenden Schritte führt, wird von der elektronischen Urne geladen.
Einlegen der Bürgerkarte und Senden der Wahl- und Prüfkarte.	Der Wählende generiert die Session Keys (k, k') . Die beiden Tokenteile, w , die Kennung des Trust Centers und k' werden an die Urne gesandt. Die Urne kennt alle relevanten e und ε und überprüft, ob $(t^d)^e = t$ und $(\tau^d)^e = \tau$, ob das Token bereits eingesetzt wurde und ob w und e zusammenpassen. Im Gutfall wird ein laufend numerierter Stimmzettel SZ_m verschlüsselt als $k'(SZ_m)$ sowie g' an den Wählenden gesandt.
Der Stimmzettel wird ausgefüllt und an die Urne geschickt.	Dieser decodiert mit k , füllt SZ_m aus und sendet die beiden Tokenteile, k' , die Trust Center Kennung, $SZ_m, \varpi(SZ_m), u(SZ_m)$ an die Urne. Diese prüft nochmals die Berechtigung des Tokens und ob dieses noch nicht eingesetzt wurde und prüft im positiven Fall die Authentizität des Wahl-/Prüfkarten. Ist dies erfüllt wird $g'(SZ_m)$ gespeichert.
Die Wähler/in erhält eine Quittung, dass die Stimme angekommen ist (ohne Nennung der Liste).	

Tabelle 2: Ablauf der Phase 2 – die Stimmabgabe

2.3.3 Auszählung

Die abgegebenen Stimmen sind erst dann lesbar, wenn alle Wahlbeobachter ihre geheimen Schlüsselteile zur Verfügung gestellt haben. Nach Ende der Wahl wird daher zunächst der vercodierte Zustand der Stimmen $g'(SZ_m)$ veröffentlicht – und ist damit öffentlich festgeschrieben. Die Wahlbeobachter stellen sodann ihre geheimen Schlüssel g zur Verfügung, mit denen die Stimmen entschlüsselt werden können.

Alle Schlüsselpaare der Wahlbeobachter werden ebenfalls veröffentlicht, so dass für jeden nachvollziehbar ist, dass sich das aus den Klartextstimmen SZ_m ergebende Wahlergebnis aus den ursprünglich festgehaltenen $g'(SZ_m)$ und den Wahlbeobachterschlüsseln ableitet – also keine Manipulation vorliegt.

2.3.4 Anmerkungen zum Protokoll

Eine Bedrohungsanalyse des Protokolls findet sich in [PrMü02]. Der wesentliche Punkt ist die strikte Trennung zwischen identifiziertem Lösen einer Wahlkarte und der anonymen Stimmabgabe. Dies setzt jedoch die Zwischenspeicherung auf einem sicheren Speichermedium voraus. Das vorliegende Protokoll nutzt die Bürgerkarte in dreifacher Hinsicht:

1. Zur Identifikation und Authentisierung des/der Wahlberechtigten. Durch die Personenbindung kann die Bürgerkarte auch als „Ausweis“ und damit zur Identifikation des Wahlberechtigten verwendet werden. Die Personenbindung ist die vom Zentralen Melderegister (ZMR) unterschriebene Verknüpfung von digitalem Zertifikat und ZMR-Kennung des Bürgers. [HoKa02]

2. Zur Zwischenspeicherung von Wahl- und Prüfkarte. Um diese Funktion als Speichermedium erfüllen zu können, müssen aber bestimmte datenschutzrelevante Anforderungen durch die Bürgerkarte erfüllt werden: (i) Wahl- und Prüfkarte müssen vor unbefugtem Auslesen geschützt und somit in einem PIN-gesicherten Bereich gespeichert werden – dies ist bereits heute möglich; (ii) am Wahltag muss technisch garantiert werden, dass die elektronische Urne nur die Wahl- und Prüfkarte von der Bürgerkarte liest, nicht jedoch andere Information, mit der der Wählende identifizierbar ist. Diese Anforderung ist vom derzeitigen Bürgerkartendesign nicht erfüllt, da das digitale Zertifikat und die Personenbindung vollkommen frei auslesbar sind.

Gerade letzterer Punkt zeigt, dass die Bürgerkarte unter einem vollkommen anderen Paradigma entworfen wurde: ganz offensichtlich ist man davon ausgegangen, dass es keine legitime anonyme Verwendungsmöglichkeit gäbe. Im Zuge des Einsatzes der Bürgerkarte für verschiedene e-Government-Applikationen, aber auch durch eine Kombination von Bankomatkarte und Bürgerkarte ändert sich dieses Paradigma.

3. Als sicheres Rechenmedium. Der e-Voting-Report des Internet Policy Institute [IPI01] sieht als größtes technisches Hindernis die Unsicherheit des Endgeräts des Wählenden, wo durch fraudulente Software, Viren, Trojanische Pferde etc. Manipulationen vorgenommen werden könnten. Wäre dieses Argument jedoch zutreffend, so dürfte der PC auch nicht als Endgerät für die digitale Unterschrift genutzt werden. Die Lösung in diesem Bereich ist das Bereitstellen eines sicheren Tunnels zwischen einer Applikation zum Anzeigen der Daten, die signiert werden sollen, und den Signaturerstellungsdaten, die die Signaturkarte niemals verlassen.

Die entscheidenden Teile des Protokolls laufen in der Signaturkarte ab; dies ermöglicht auch einen Wiederanlauf: solange nämlich r und ρ auf der Karte gespeichert sind, können b^d bzw. β^δ beliebig oft angefordert werden (beispielsweise nach einem Verbindungszusammenbruch). Es ist sichergestellt, dass nur der Inhaber der Karte, der r und ρ gespeichert hat, die Hülle der blinden Signatur öffnen kann.

3. Implementierung und Testwahl

3.1 Testwahl

Ca. 1000 Studierende der Spezialisierungsprogramme des Instituts für Informationsverarbeitung und Informationswirtschaft hatten die Gelegenheit an der Testwahl teilzunehmen. Elektronische Briefwahlkarten konnten vom 1.5. bis 19.5. 2003 jew. 0-24:00 beantragt werden, die Stimmabgabe erfolgte im Zeitraum 20.5. 9:00 bis 22.5. 15:00. Am 22.5. 15:00 wurde die elektronische Urne geöffnet, die Stimmen durch die Wahlbeobachter (Repräsentanten der drei stärksten Fraktionen an der ÖH WU) entschlüsselt und gezählt. Bemerkenswerterweise erzielte die Testwahl eine um 40% höhere Wahlbeteiligung als die echte ÖH WU-Wahl. Die Verteilung auf die kandidierenden Listen in der Testwahl entsprach der Verteilung der realen Wahl.

3.2 Ersatz der Bürgerkarte

Da bei dieser Testwahl an der WU Wien keine Bürgerkarten zur Verfügung standen, wurde die Bürgerkarte in ihren oben geschilderten Rollen ersetzt:

1. Die Authentisierung erfolgte über das Standard-Login für WU-Studierende, mit dem verschiedene Universitätsdienste verfügbar sind. Um eine für die Administratoren anonymisierte Wähler evidenz zu schaffen, wurden die Matrikelnummern der teilnahmeberechtigten vom Zentralen Informatikdienst der WU (ZID) einem Hashverfahren (SHA-1 mit Padding der Matrikelnummer) unterzogen und dies als Evidenz verwendet. Zur Registrierung verwendete der Studierende das Standard-WU-Login des ZID, das auch die Paßwortüberprüfung vornahm und die Matrikelnummer demselben Hashverfahren unterzog und dies signierte. Vershen mit einer Timestamp erhielt der Studierende dieses Token und konnte sich damit beim e-Voting Registrationsserver authentisieren. Natürlich ist eine Identifizierung über, gleich welches, Login-Verfahren einer chipkartenbasierten Authentisierung immer unterlegen, da sie nur Wissen, nicht aber Wissen und Besitz (der Karte) voraussetzt. Andererseits ist sie die Lösung bei Nichtverfügbarkeit einer Bürger- bzw. Signaturkarte.

2. Sicheres Speichermedium. Die Testwahl verwendete ein beliebiges Speichermedium. Hier zeigen sich bereits deutlich die Nachteile bei einem Verfahren ohne Einsatz einer Chipkarte: einerseits ist das Medium u.U. fehleranfällig (Diskette), frei kopierbar und auch nicht an eine Person gebunden, wie die Bürgerkarte. Zur Sicherung der elektronischen Wahlkarte wurde diese verschlüsselt abgelegt.

3. Sicheres Rechenmedium. Da ein beliebiges Speichermedium verwendet wurde, mussten alle Rechenoperationen (insbesondere das kritische Auflösen der blinden Signatur) in den Java Applets und nicht auf der Karte durchgeführt werden. Dies mindert natürlich das Sicherheitsniveau entscheidend, da es die Integrität des Wahlprotokolls von der Integrität des verwendeten Endgeräts abhängig macht.

3.3 Lösungsszenario

Wie also soll in Situationen, in denen keine Bürger- bzw. Signaturkarte verfügbar ist, vorgegangen werden? Für die Funktionen „sicheres Speichermedium“ und „sicheres Rechenmedium“ kann natürlich auch eine beliebige Chipkarte verwendet werden, die ausreichenden Zugriffsschutz implementiert. Es bleiben die Fragen der Authentisierung und Identifizierung, sowie wie die auf dieser Karte gespeicherten Daten an die Person gebunden werden können.

Für den Funktionsblock Authentisierung/Identifizierung kommen Login-Lösungen, wie die oben beschriebene, oder aber die sog. „Verwaltungssignatur“ in Frage [Pos03]. Dabei liegen die Signaturerstellungsdaten auf einem Server eines Providers, der Benutzer kommuniziert bei der Unterschriftsleistung über das https-Protokoll mit diesem Signaturschlüssel; als zusätzliche Sicherung ist für die Freigabe der Signatur ein sessionspezifischer Code einzugeben, der dem Benutzer per Mobiltelefon als SMS geschickt wird. Diese Lösung kommt ohne die Distributionslogistik der kartenbasierten Signatur aus, doch sind vor dem Einsatz für e-Voting einige entscheidende Fragen zu klären:

- Reicht diese Form der Signatur rechtlich für die Beantragung einer (elektronischen) Wahlkarte?
- Wie werden die Signaturerstellungsdaten am Server gesichert?
- Wie erfolgt die End-zu-End-Sicherung zwischen der Anzeige des zu signierenden Textes/Dokumentes und dem (vermutlich hinter einem Proxy liegenden) Server mit den Signaturerstellungsdaten; das https-Protokoll kann diese Sicherung nicht bereitstellen.
- Wie erfolgt die End-zu-End-Sicherung des die Signatur freigebenden PINs?

4. Ausblick

E-Voting ist zu einer realen Möglichkeit geworden, sein Erfolg setzt jedoch zwei entscheidende Dinge voraus:

- Die strikte Einhaltung der Wahlrechtsgrundsätze durch das Gesamtsystem (nicht nur die kryptographische Anwendungsebene, isoliert für sich betrachtet). Die Versuchung mag gegeben sein, Systeme, die diese Anforderung nicht erfüllen, zum Einsatz zu bringen. Der verantwortungsvolle Umgang mit dem Thema gebietet jedoch hier, strenge Maßstäbe anzulegen. Letztlich handelt es sich bei diesem Anwendungsgebiet um einen der Kernprozesse unserer demokratischen Gesellschaftsordnung. Zweifelhafte Implementierungen würden die Akzeptanz von e-Voting in der Bevölkerung nachhaltig stören.
- Die Infrastruktur zur Authentisierung und Identifizierung des Wählenden. Diese muss einerseits in zufriedenstellender Flächendeckung bzw. Verfügbarkeitsgrad vorhanden sein – andererseits muss sie ein Sicherheitsniveau bieten, das die Sicherheitsstandards des kryptographischen Wahlprotokolls nicht korrumpiert.

Literaturverzeichnis

- [Abe98] Abe M.: Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Centers. In: Advances in Cryptology - EUROCRYPT '98, Springer-Verlag, Berlin, 1998, S. 437-447.
- [BCR87] Brassard, G., Crepeau, C., Robert, J.-M.: All-or-Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer-Verlag, 1987, S. 234-238.
- [BPS94] Baraani-Dastjerdi A., Pieprzyk J., Safavi-Naini R.: A Practical Electronic Voting Protocol Using Threshold Schemes. In: Center f. Computer Security Research, Department of Computer Science, University of Wollongong, Australia, 1994.

- [BoRi99] Borrell J., Riera A.: Practical Approach to Anonymity in Large Scale Electronic Voting Schemes. In: Universitat Autònoma de Barcelona, Departament d' Informàtica, Catalonia, 1999.
- [CEG00] Chancellerie d'Etat de Genève: Cahier des charges e-voting. http://www.geneve.ch/chancellerie/e-government/cahier_charges.html (2003-03-05).
- [Cha81] Chaum, D.: Untraceable electronic mail return addresses and digital pseudonyms. In: Communications of the ACM, Vol. 24(2), 1981, S. 84-88.
- [Cha87] Chaum, D.: Blinding for Unanticipated Signatures. In: Chaum, David; Price, Wyn (Eds.): Advances in Cryptology, EUROCRYPT '87, Springer-Verlag, Berlin, 1987, S. 227 –233.
- [CC97] Cranor, L. F., Cytron, R. K.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawaii International Conference on System Sciences (HICSS-97). Hawaii 1997. <http://lorrie.cranor.org/pubs/hicss/hicss.html> (2001-02-04).
- [CGS97] Cramer R., Gennaro R., Schoenmakers B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science 1233, Springer-Verlag, Berlin, 1997, S. 103-118
- [Fell01] Gemeinde Fellbach.: Jugendgemeinderat Fellbach. <http://www.fellbach.de/wahlen> (2001-11-20).
- [FOO93] Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology –AUSCRYPT92. Springer-Verlag, Berlin 1993, S.244 –251.
- [HaPo95] Hassler, V. Posch, R.: A LAN voting protocol. In: IFIP/SEC 95, Capetown, 1995, S.154-167.
- [HMP95] Horster P., Michels M., Petersen H.: Blind Multisignatures and their relevance for Electronic Voting. In: IEEE-Press, 11th Annual Computer Security Applications Conference, 1995, S. 149-156.
- [HoKa02] Hollosi, A. Karlinger, G.: Security-Layer für das Konzept Bürgerkarte, BMÖLS, Chief Information Unit, Wien, 2002. <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html> (2002-10-23).
- [HoMi96] Horster P., Michels M.: Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme. In: Asiacypt 96, LNCS 163, Springer-Verlag, Berlin, 1996, S. 125-132.
- [IPI01] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001. http://www.internetpolicy.org/research/e_voting_report.pdf (2001-11-20).
- [Jak98] Jakobsson M.: A Practical Mix. In: Advances in Cryptology - EUROCRYPT '98, Springer-Verlag, Berlin, 1998, S. 448-461.
- [Jak99] Jakobsson M.: Flash Mixing. In: Information Sciences Research Center, Bell Labs, New Jersey, <http://www.bell-labs.com/user/markusj> (2002-11-19).
- [Ni94] Niemi V.: Cryptographic protocols and voting. In: Results and Trends in Theoretical Computer Science, Springer LNCS, Springer-Verlag, Berlin, 1994, S. 307-316.
- [NiRe95] Niemi V., Renvall A.: How to Prevent the Buying of Votes. In: Advances in Cryptology-Asiacrypt 94, Springer-Verlag, Berlin, 1995, S. 164-170.
- [NSS91] Nurmi, H., Salomaa, A.; Santean, L.: Secret ballot elections in computer networks. In: Computers and Security 36 (1991) 10, S. 553-560.
- [Oka96] Okamoto T.: An Electronic Voting Scheme: IFIP '96, Advanced IT Tools, Chapman and Hall, London, 1996, S. 21-30.
- [Pf89] Pfitzmann B., Pfitzmann A.: How to Break the Direct RSA-Implementation of Mixes. In: Eurocrypt 89, Springer-Verlag, Berlin, 1989, S. 373-381.

- [PIK94] Park, C., Itoh, K., Kurosawa, K.: All/Nothing Election Scheme and Anonymous Channel. In: Lecture Notes in Computer Science 765, Advances in Cryptology Eurocrypt 93, Berlin, Springer-Verlag, 1994, S. 248-259.
- [PKK03] Prosser, A., Kofler, R., Krimmer, R.: Deploying Electronic Democracy for Public Corporations. In: DEXA/EGOV 2003, Prague, 2003.
- [Pos03] Posch, R.: Das Konzept der Bürgerkarte light. Chief Information Office, Wien, 2003.
- [PrMü01] Prosser, A., Müller-Török, R.: Electronic Voting via The Internet. In: 3rd International Conference on Enterprise Information Systems ICEIS-2001, Setubal, 2001, S. 1061-1066.
- [PrMü02] Prosser, A., Müller-Török, R.: E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. In: Wirtschaftsinformatik 44(2002) 6, S. 545-556.
- [Riv99] Rivest, R.: Cryptography and Information Security Group Research Project: E-Voting. In: <http://theory.lcs.mit.edu/~cis/voting/voting.html> (2001-11-19).
- [SaKi95] Sako, K., Kilian, J.: Receipt-Free, Mix-Type Voting Scheme. In: Lecture Notes in Computer Science 921, Advances in Cryptology Eurocrypt 95, Berlin, Springer-Verlag 1995, S. 393-403.
- [Sal91] Salomaa, A.: Verifying and Recasting Secret Ballots in Computer Networks. In: Maurer, H.A. (Eds.): New Results and New Trends in Computer Science, Springer-Verlag, Berlin, 1991, S.283 –289.
- [SCCE01] Soundcode VoteHere Inc.; Compaq Computer Corp.; Cisco Systems Inc.; Entrust Inc.: VoteHere Gold. Soundcode Inc., Bellevue, 2001. <http://www.soundcode.com/voteheregold.html> (2001-07-20).
- [Sch96] Schneier B.: Applied Cryptography, Addison-Wesley, Boston, 1996.
- [WaME82] Walter, R., Mayer, H.: Grundriß des österreichischen Bundesverfassungsrechts; Manz Verlag, Wien, 1982.