

# E-VOTING.AT – EIN IMPLEMENTIERUNGSBERICHT

Alexander Prosser, Robert Kofler, Robert Krimmer<sup>1</sup>

*Weltweit entwickeln Forschungsgruppen elektronische Wahlsysteme (e-Voting), die verschiedene Ansätze verfolgen, aber alle ohne rechtliche Grundlage. In Österreich hat der Nationalrat beschlossen, elektronische Wahlen unter Verwendung von digitalen Signaturen für öffentliche Wahlen im Bereich der Hochschülerschaft und der Wirtschaftskammer zu ermöglichen. Bis jetzt wurde noch kein Algorithmus entwickelt, der abgesehen von den zuvor erwähnten hohen Anforderungen, das grundsätzliche technische Problem gelöst hat: Wie kann ein Wähler eindeutig und zweifelsfrei identifiziert werden und dabei die Anonymität seiner Stimme garantieren wenn dabei auch noch der Wahlbetrug durch die Wahladministration verhindert werden muss. In diesem Artikel berichten die Autoren über ihre Erfahrungen bei der Implementierung der ersten Phase des von ihnen vorgeschlagenen Algorithmus, der diese Anforderungen durch die strikte Separation der Registrierung von der Stimmabgabephase.*

## 1. Einleitung

Unter dem Sammelbegriff E-Voting wird derzeit weltweit von verschiedensten Gruppen Forschung betrieben, um eine sichere und rechtsgültige Wahl über das Internet zu ermöglichen, es existiert auch bereits eine Reihe von Prototypen. Folgende technische Grundprobleme sind dabei zu bewältigen:

- der Wählende muß eindeutig identifiziert werden, dabei aber trotzdem
- anonym seine Stimme abgeben können,
- die auch durch die Administratoren des Wahlsystems nicht verfälscht werden kann.

Die Wahlbeteiligung in Österreich war bei nationalen Wahlen immer über 90 % bis zum Jahr 1994, als sie zum ersten Mal unter diese Marke fiel und 1999 den niedrigsten Stand mit 80,4 % erreichte [1]. Wenn auch im internationalen Vergleich diese Zahl noch sehr hoch erscheinen mag, so fanden sich auch erste Initiativen, die die Einführung von Formen der Distanzwahl für öffentliche Wahlen forderten [2]. Bis jetzt ist es nur Auslandsösterreicher

---

<sup>1</sup> Abteilung Produktionsmanagement, Wirtschaftsuniversität Wien, Pappenheimgasse 35/5, A-1200 Wien, {alexander.prosser, robert.kofler, robert.krimmer}@wu-wien.ac.at. Die Arbeit von Krimmer und Kofler wurde vom Jubiläumsfonds der Stadt Wien gefördert.

möglich an Wahlen mittels einer Wahlkarte an Nationalrats- und Bundespräsidentenwahlen teilzunehmen, die auch als sogenannte Wahlen erster Ordnung bezeichnet werden [3].

Im Jahre 2001 wurden vom österreichischen Parlament allerdings zwei Gesetze erlassen, die das Verfahren der elektronischen Stimmabgabe (e-Voting) im Rahmen von zwei Organisationen erlaubt: bei der Hochschülerschaft und bei der Wirtschaftskammer. Diese Gesetze setzen voraus, dass die zum Einsatz kommenden e-Voting Systeme digitale Signaturen benutzen und von der Datenschutzkommission genehmigt werden. Zusätzlich ist auch ein Gutachten von der Signaturprüfstelle A-SIT notwendig.

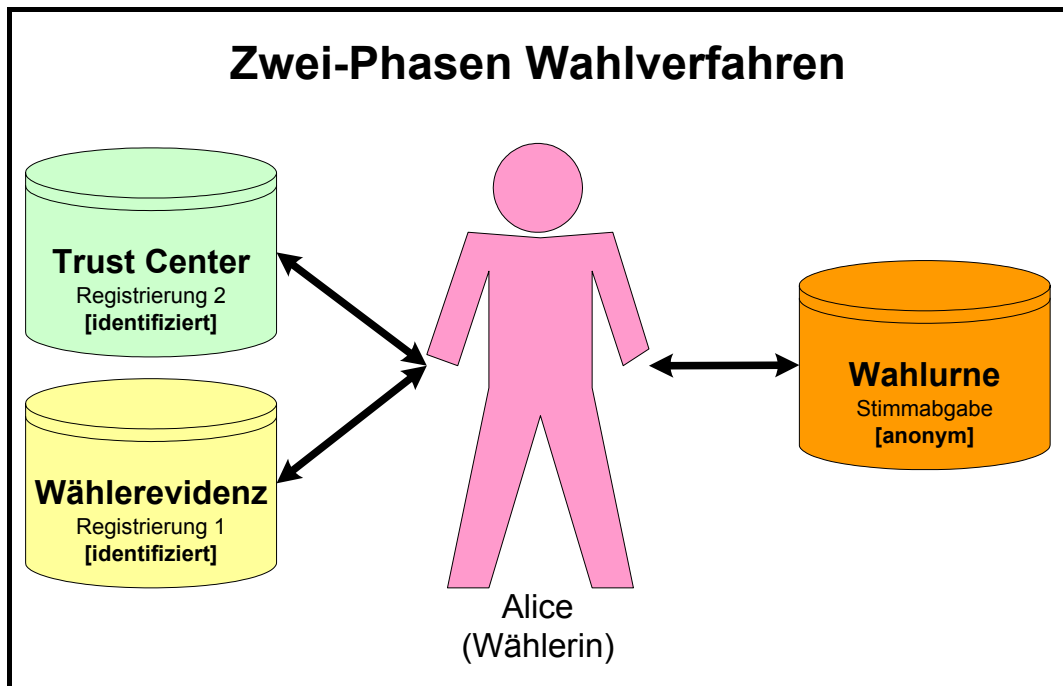
In einem von der Stadt Wien geförderten Projekt wird derzeit an der Abteilung für Produktionsmanagement ein e-Voting Prototyp in zwei Entwicklungsschritten entwickelt: Zuerst wird eine e-Voting-fähige Wählerevidenz implementiert und anschließend eine darauf aufbauende elektronische Wahlurne um den Prototyp zu vervollständigen.

Die Autoren erklären in dieser Arbeit zuerst den verwendeten Algorithmus und erklären dann in einem Prozessmodell wie das Konzept implementiert wurde und in welchen Bereichen der Algorithmus erweitert werden musste aufgrund von Weiterentwicklungen im Bereich des e-Government. Ein prominentes Beispiel dafür ist das Konzept der österreichischen Bürgerkarte, das zum Zeitpunkt der ursprünglichen Entwicklung des Algorithmus nicht verfügbar war.

## 2. Algorithmus

Der hier besprochene Algorithmus wurde erstmals in [4] vorgeschlagen und dann im Zuge der Vorbereitung des Implementierungsprojekts für die Stadt Wien weiterentwickelt. Der wesentliche Unterschied zu anderen Ansätzen ist die strikte Unterscheidung in Wählerregistrierung und Stimmabgabe, die erstmals von Nurmi et.al. in 1991 [5] identifiziert wurden:

- **Phase Eins – Wählerregistrierung:** Die Wahlberechtigung des Wählers wird überprüft und dieser erhält eine blind-signierte Wahlkarte, die sicher zur späteren Verwendung zwischengespeichert wird.
- **Phase Zwei – Stimmabgabe:** Der Wähler benutzt die zwischengespeicherte Wahlkarte um einen Stimmzettel zu beziehen und ausgefüllt zu retournieren.



**Abbildung 1:** *Beteiligte Parteien beim Zwei-Phasen Wahlverfahren*

Bevor der Algorithmus im Detail diskutiert wird, hier eine Aufzählung der verwendeten Begriffe:

<b>RS</b>	Wählerevidenz Server
<b>TC</b>	Trust Center Server
<b>US</b>	Wahlurnen Server
<b>SZ</b>	Stimmzettel
<b>c</b>	Wahlkreis
<b>e, d</b>	Öffentlicher / Privater Signaturschlüssel der Wählerevidenz
<b>k, l</b>	Öffentlicher / Privater Kryptoschlüssel der Wählerevidenz
<b>ε, δ</b>	Öffentlicher / Privater Signaturschlüssel des Trust Centers
<b>κ, λ</b>	Öffentlicher / Privater Kryptoschlüssel des Trust Centers
<b>u, v</b>	Öffentlicher / Privater Signaturschlüssel des Wählers
<b>w, z</b>	Öffentlicher / Privater Kryptoschlüssel des Wählers
<b>u, ω</b>	Öffentlicher / Privater Signaturschlüssel der Wahlurne
<b>ω, ζ</b>	Öffentlicher / Privater Kryptoschlüssel der Wahlurne
<b>t</b>	Wahlkarte
<b>τ</b>	Prüfkarte
<b>r</b>	Blindisierung (Blaupapierkuvert) für die Wahlkarte
<b>ρ</b>	Blindisierung (Blaupapierkuvert) für die Prüfkarte
<b>m, m'</b>	Asymmetrisches Kryptoschlüsselpaar für den Wahlvorgang

## 2.1 Phase Eins - Wählerregistrierung

Der Wähler kann sich eine bestimmte Zeit vor dem eigentlichen Wahltag registrieren. Nachdem der Stimmzettel bei der Registrierung nicht ausgehändigt wird, können sich Wähler sogar registrieren, wenn die Kandidatenliste noch nicht komplett ist. In einem ersten Schritt generiert der Wähler eine Zufallszahl  $\tau$  als elektronische Prüfkarte und bereitet diese auf die Blinde Signatur<sup>2</sup> vor (indem man es mit  $\rho^e$  multipliziert, sprich mit einem Blaupapierkuvert, versieht) und fügt einen Text hinzu, der dem rechtlichen Antrag auf Ausstellung einer elektronischen Prüfkarte entspricht und unterschreibt diesen mit seinem privaten Signaturschlüssel  $v$ , was dann folgendes Paket ergibt:  $[\tau\rho^e, \text{Antrag}]^v$ . Die Nachricht wird dann verschlüsselt mit dem öffentlichen Kryptoschlüssel des Trust Centers und an dieses in **(1a)** geschickt  $\{[\tau\rho^e, \text{Antrag}]^v\}^k$ . Der Server überprüft dann das Paket des Wählers, indem er den öffentlichen Signaturschlüssel des Wählers  $u$  lädt. Wenn der Wähler wahlberechtigt ist, unterschreibt das Trust Center die „blindisierte“ Prüfkarte  $\tau\rho^e$ , welches  $[\tau\rho^e]^\delta$  ergibt. Dies ist verfahrenstechnisch gesehen der gleiche Vorgang wie in dem einphasigen (und daher unsicheren) Wahlverfahren von Fujioka et.al. [7] und löst ebenfalls das Problem der Anonymität der Stimmabgabe bei eindeutiger Identifizierung zur Überprüfung der Wahlberechtigung. Doch nachdem hier die Prüf-/Wahlkarte anstelle des Stimmzettels unterschrieben wird, kann eine wesentlich kleinere Nachricht erwartet werden, was das Speichern auf sicheren Datenträgern (z.B. der Signaturkarte) erleichtert. Die Prüfkarte wird dann in **(1b)** an den Wähler mit dessen öffentlichem Kryptoschlüssel  $w$  verschlüsselt geschickt.

---

<sup>2</sup> Die Funktion der Blinden Signatur wurde von David Chaum 1982 [6] entwickelt. Man kann dies mit dem Verwenden eines Blaupapierkuverts vergleichen.

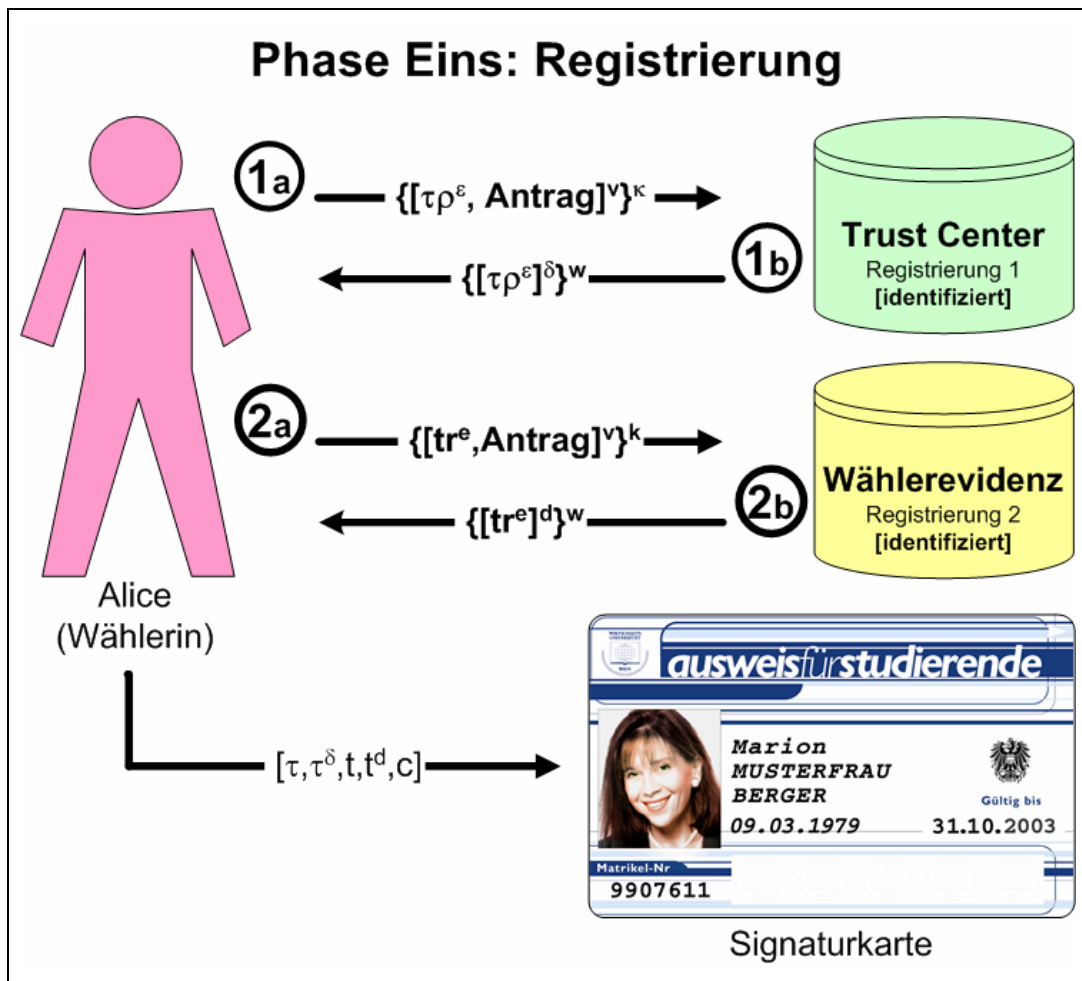


Abbildung 2: Registrierungs-Prozess beim Zwei-Phasen Wahlverfahren

Ein ähnlicher Vorgang wird mit der Wählerevidenz wiederholt: Der Wähler generiert eine zweite Karte, die so genannte Wahlkarte  $t$ , blindisiert diese und sendet sie an die Wählerevidenz Center in (2a) und erhält das blind signierte  $[(t)r^e]^d$  in (2b). Dies ist notwendig, da nur damit die dritte Problematik des Wahlbetrugs durch eine Zusammenarbeit der Wählerevidenz und der Wahlurne verhindert werden kann. Diese würde immer die blinde Signatur Bestätigung durch das Trust Center benötigen, um eine einzelne Stimme zu fälschen. Die Wählerevidenz speichert den elektronischen Antrag ebenfalls und verzeichnet die Ausgabe der elektronischen Wahlkarte, womit der Wähler auf herkömmlichem Weg nicht mehr wahlberechtigt ist. Daneben speichert sie auch  $[tr^e]^d$ , wenn die ursprüngliche Wahlkarte verloren geht und der Wähler erneut um eine Wahlkarte ansucht, wird die Evidenz immer mit der Wahlkarte aus dem Antrag antworten, um ein mögliches Problem mit der Ausgabe mehrerer Wahlkarten zu vermeiden.

Da die meisten Wahlverfahren die Zuordnung der Wähler zu Wahlkreisen  $c$  vorsehen, wird diese Information auch dem Wähler übermittelt und muss am Wahltag ebenfalls übermittelt werden, um anzuzeigen, zu welchem Wahlkreis die Stimme gehört. Um eine mögliche Manipulation von  $c$  zu vermeiden, können die blinden Signaturschlüssel, die für  $[tr^e]^d$  benutzt werden, wahlkreisabhängig gemacht werden. Daher müssen das  $c$ , das am Wahltag übermittelt wird und die von der Evidenz herausgegebene Wahlkarte zum selben  $c$  verweisen. Der Wähler selbst besitzt am Ende der ersten Phase zwei Authentisierungskarten (die Wahlkarte von der Evidenz und die Prüfkarte vom Trust Center), und die Wahlkreisinformation in Form eines Pakets  $[t, t^d, \tau, \tau^\delta, c]$ , das dann auf der Signaturkarte gespeichert wird. Dieses gesamte Paket wird benötigt, um sich am Wahltag als berechtigter Wähler auszuweisen und einen Stimmzettel zu bekommen.

## 2.2 Phase Zwei - Stimmabgabe

Am Wahltag verwendet der Wähler seine Wahl- und Prüfkartenkombination beim Wahlurnenserver, um einen Stimmzettel zu bekommen. Diese Übertragung wird nicht vom Wähler signiert und die einzige Legitimationsform dabei ist die zuvor erhaltene Kartenkombination. Der Wähler generiert ein asymmetrisches Schlüsselpaar  $\mathbf{m}$  und  $\mathbf{m}'$  um die Kommunikation zu sichern (ohne dabei seine Identität zu verraten, denn dies wäre der Fall, wenn das ebenfalls asymmetrische Kryptoschlüsselpaar auf der Signaturkarte verwendet werden würde). Vom Wähler wird zudem noch die Information  $\mathbf{TC}$  über das verwendete Trust Center beigefügt, die nicht benötigt wird um den Wähler zu identifizieren oder einen öffentlichen Kryptoschlüssel zu erhalten, sondern um den richtigen Trust Center Schlüssel zu wählen, um die blinde Signatur aufzulösen und so die Wahlberechtigung zu überprüfen. Die resultierende Nachricht  $[\tau, \tau^\delta, t, t^d, c, \mathbf{TC}, \mathbf{m}]$  ist mit dem öffentlichen Kryptoschlüssel  $\omega$  verschlüsselt und wird in (1) an die Urne geschickt. Nach der Entschlüsselung wird überprüft, ob  $\mathbf{tr}^e$  und  $\mathbf{\tau p}^e$  authentisiert werden können und falls ja, verschlüsselt die Wahlurne den (noch) leeren Stimmzettel  $\mathbf{SZ}$  mit  $\mathbf{m}$  und sendet  $\mathbf{m}[\mathbf{SZ}^\omega]$  an den Wähler in (2). Dieser entschlüsselt mit  $\mathbf{m}'$  und füllt den Stimmzettel aus. Dann wird mit den Wahlkarten kombiniert und erneut mit dem öffentlichen Kryptoschlüssel  $\mathbf{w}$  verschlüsselt und an die Urne in (3) geschickt. Diese authentisiert die Kartenkombination und speichert den Stimmzettel und die anderen vom Wähler erhaltenen Informationen im letzten Schritt (4).

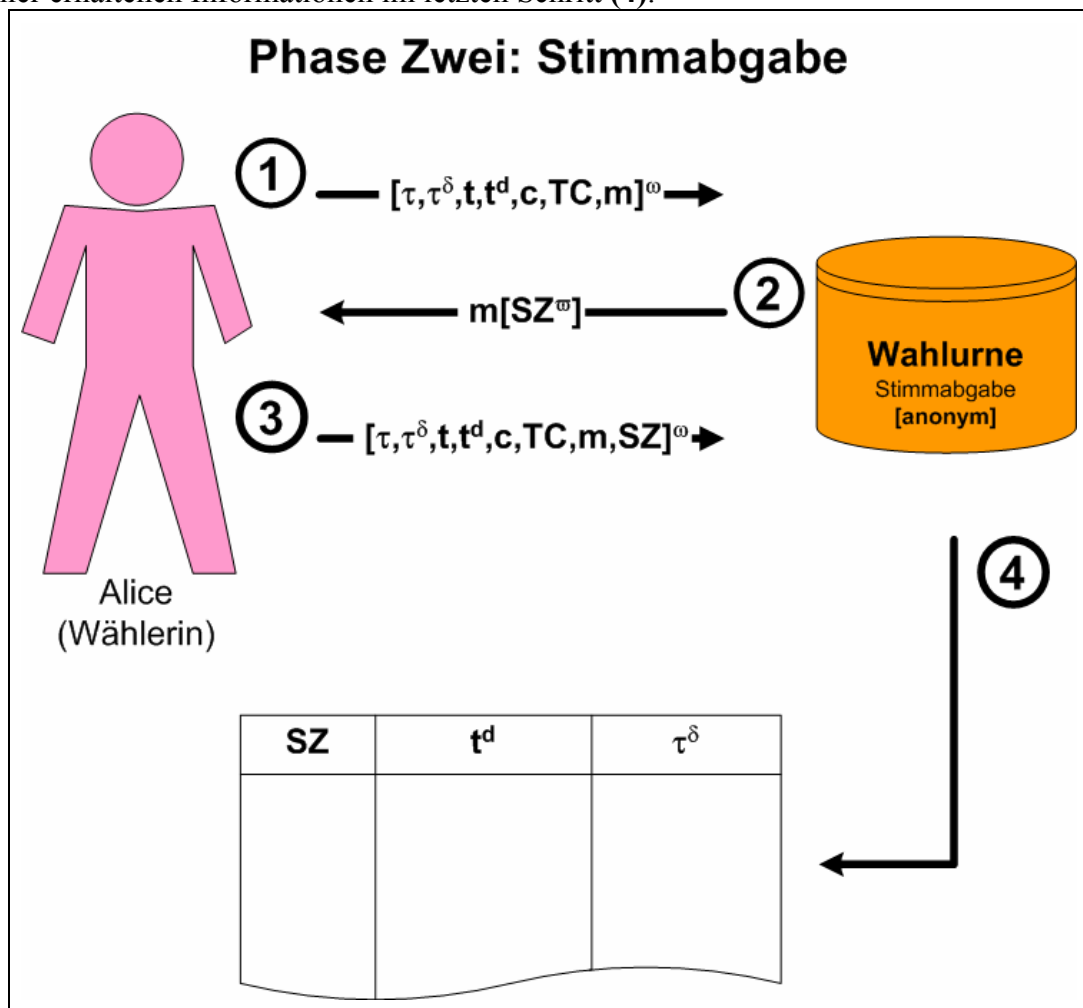


Abbildung 3: Stimmabgabe-Prozess beim Zwei-Phasen Wahlverfahren

Abgesehen von dem Faktum, dass dem Wähler die Anonymität garantiert werden kann, insofern unterschiedliche Rechner (IP-Adressen) für Registrierung und Wahlphase benutzt

wurden, kann ein Wahlbetrug durch die Server Administration der Wählerevidenz und der Wahlurne ausgeschlossen werden. Es können keine Stimmen gefälscht werden, weil diese ja auch noch vom Trust Center authentisiert werden müssen. Nur so kann daher die eingangs erwähnte Grundproblematik vollständig gelöst werden.

### 3. Implementation

Die Konzepte von e-Government und e-Administration haben in Österreich einen hohen Stellenwert auf der Tagesordnung der Politiker bekommen. So wurde das Chief Information Office (CIO) installiert, dessen Hauptaufgabe es ist, eine koordinierte Strategie für e-Government in der österreichischen Verwaltung zu entwickeln [8].

Die dort entwickelte Strategie konzentriert sich vor allem auf den Bereich der Infrastrukturentwicklung und dadurch bekommt die Einführung der Bürgerkarte (National ID card) basierend auf der Europäischen Signaturrechtlinie bzw. dem daraus folgenden österreichischen Signaturgesetz ein Projekt erster Ordnung.

Wie in der Einleitung erwähnt, ist die Identifizierung des Benutzers mittels der digitalen Signatur eine der wesentlichen Bedingungen der entsprechenden österreichischen Gesetze für e-Voting<sup>3</sup>. Werden SmartCards benutzt um digitale Dokumente zu signieren, so kann weltweit jede Person überprüfen ob die digitale Signatur gültig ist. Aber wenn man einen Benutzer eindeutig identifizieren will, so reicht dieses Verfahren nicht aus. Denn selbst wenn der Name des Benutzers und sein Geburtstag übereinstimmen mit der Wahlberechtigten Person, kann man noch nicht sicher sein, dass es sich um die ein und dieselbe Person handelt, denn diese Merkmale reichen nicht aus um eine Person eindeutig zu identifizieren. Dieses Problem kann man nun auf zwei Arten lösen, (i) wenn man als Organisation, bei der Ausgabe einen Match zwischen der Signaturkarte und der realen Person gemacht oder wenn man (ii) als eindeutiges Unterscheidungsmerkmal eine Kennzahl wie die österreichische Zentrale Melderegisternummer, die in der Personenbindung (**pi**) auf der Signaturkarte gespeichert ist. Während die erste Lösung sinnvoll ist bei Wahlen, wo die Organisation die volle Kontrolle über die Identifikationskarte ihrer Wähler hat, so kann diese nicht für Wahlen benutzt, wo der Wähler eine beliebige Signaturkarte benutzen kann. Die zweite vorgeschlagene Variante setzt eine Infrastruktur voraus, bei der alle Benutzer/Wähler zentral in einer Meldedatenbank erfasst werden. Bei dieser zentralen Datenbank hat man nicht nur die Probleme mit der Datenerfassung und –wartung sondern auch mit dem Datenschutz ganz allgemein. In Österreich wurde im Meldegesetz von 1995 – trotz der Datenschutzbedenken [10]– das zentrale Melderegister eingeführt und nahm den operativen Dienst am 1. März 2001 auf. Im Zuge der Inbetriebnahme wurde jedem österreichischen Staatsbürger die eindeutige ZMR-Nummer zugewiesen. Durch die Speicherung dieser ZMR-Nummer in der Personenbindung auf der Signaturkarte des Wählers wird diese Karte zur sogenannten National ID Card bzw. auf Deutsch „Bürgerkarte“. Damit lässt sich diese Karte für den Identifikationsprozess und die Wahlberechtigungsüberprüfung benutzen.

Eine weitere sehr nützliche Entwicklung der nationalen Koordinationsstelle für die Informations und Kommunikationstechnologie, die Chief Information Office Operative Unit hat den sogenannten Security Layer entwickelt [11]. Dieses Programm ist im wesentlichen ein Standard Application Interface für die Signier- und Verifikationszwecke, das in Form eines lokalen http-Servers implementiert wurde. Dieses Programm kümmert sich um alle Zugriffe zwischen der Signaturkarte und dem Benutzer und kann über Standard http-Requests angesprochen werden und ermöglicht einen Verzicht auf Java.

---

<sup>3</sup> Die erste größere Zahl an Signaturkarten, die in Österreich ausgegeben werden, sind die Studentenausweise der Studenten an der Wirtschaftsuniversität Wien [9].

Basierend auf diesen Entwicklungen haben die Autoren dieses Artikels nun die erste Phase des hier diskutierten e-Voting-Prototypen implementiert. Dies führt im Vergleich zum zuvor vorgestellten Ablauf nun zu einem fünf Schritte umfassenden Prozess:

1. Download der Java Applets
2. Vorbereitung der Prüfkarte
3. Überprüfung der Wahlberechtigung und Vorbereitung der Wahlkarte
4. Blinde Unterschrift der Prüfkarte
5. Blinde Unterschrift der Wahlkarte

### 3.1 Schritt Eins: Download des Java Applets

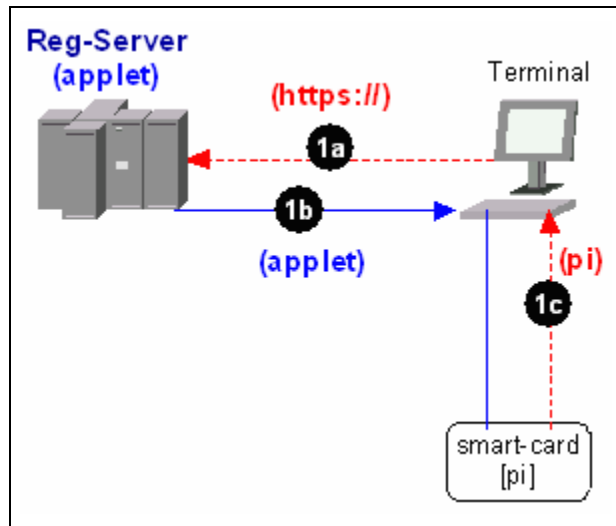


Abbildung 4: Download des Java Applets

Am Anfang beginnt der Wähler den elektronischen Distanzwahlvorgang durch Eingabe der Internet-Adresse, die ihm von der Wahlbehörde mitgeteilt wurde (1a). Der Web-Browser des Wählers lädt dann das Java Applet vom Registrierungsserver (1b). Die erste Aktion ist dann das Laden der Personenbindung in (1c) (via Security Layer) zur Vorbereitung der Wahlberechtigungsüberprüfung im Schritt (3).

### 3.2 Schritt Zwei: Vorbereitung der Prüfkarte

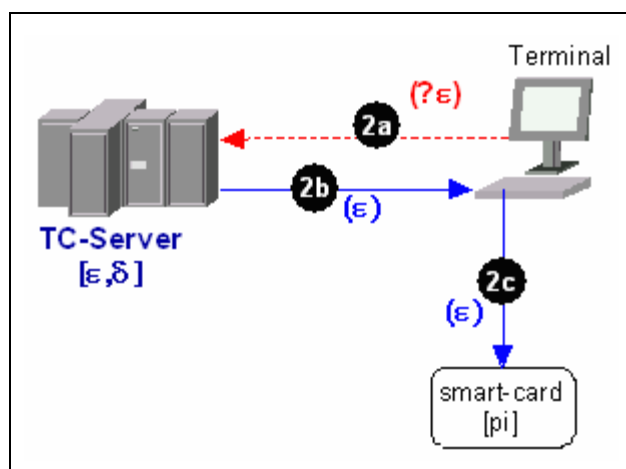


Abbildung 5: Vorbereitung der Prüfkarte

Für den Blindisierungsvorgang nimmt man eine Zufallszahl  $\rho$  signiert sie mit dem öffentlichen Signaturschlüssel  $\epsilon$  des TrustCenters, was dann  $\rho^\epsilon$  ergibt. Daher beantragt das Applet den öffentlichen Schlüssel in (2a) vom Trust Center und erhält diesen in (2b) und

speichert ihn zwischen auf der Signaturkarte für den Blindisierungsprozess der Prüfkarte in (2c).

### 3.3 Schritt Drei: Überprüfung der Wahlberechtigung und Vorbereitung der Wahlkarte

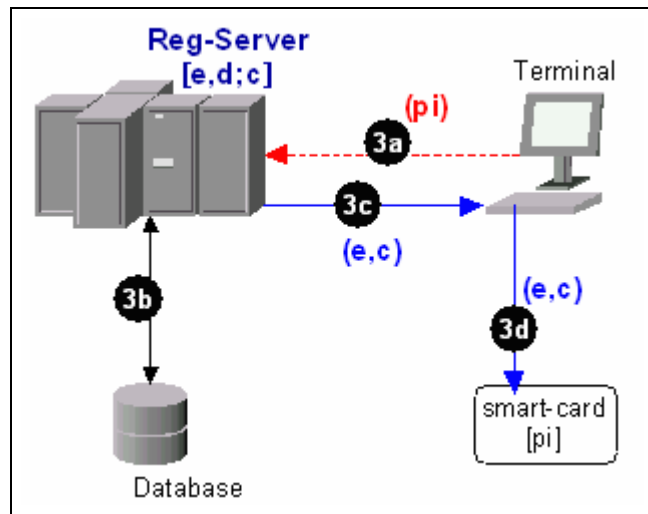


Abbildung 6: Überprüfung der Wahlberechtigung und Vorbereitung der Wahlkarte

Dieser dritte Schritt ist praktisch eine Wiederholung des zweiten Schritts, mit dem Unterschied, dass es mit dem Registrierungsserver durchgeführt inklusive der Überprüfung der Wahlberechtigung des Wählers. Hierdurch wird dem Wähler der Wahlkreis  $c$  zugewiesen. Um dies zu ermöglichen sendet das Applet, die zuvor geladene Personenbindung  $pi$  an den Registrierungsserver und beantragt zugleich den öffentlichen Schlüssel (3a). Auf Basis der Wählerevidenz ermittelt der Server die Wahlberechtigung des Wählers und damit dessen Wahlkreis  $c$  (3b). Nach Erhalt von  $e$  und  $c$  in (3c) speichert das Applet diese auf der Signaturkarte (3d) um dann die Wahlkarte zu blindisieren.

### 3.4 Schritt Vier: Blinde Unterschrift der Prüfkarte

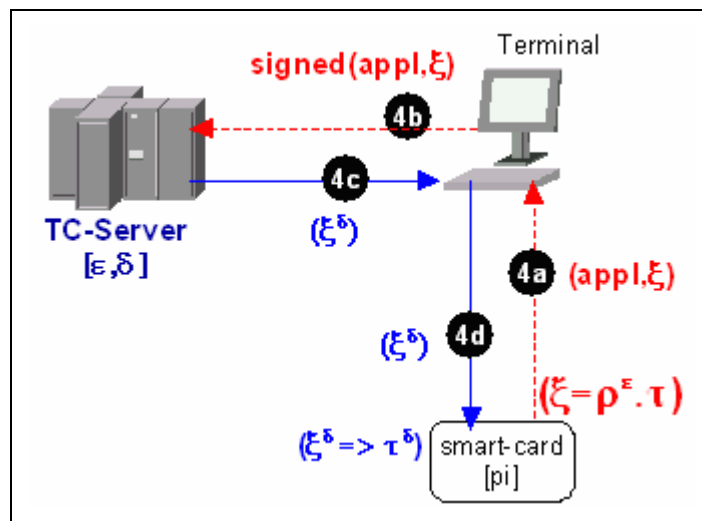


Abbildung 7: Blinde Unterschrift der Prüfkarte

Die Prüfkarte wird in (4a) blindisiert indem man die Zufallszahl  $\rho$  nimmt und sie mit  $\epsilon$  signiert, welches dann die blindisierte Prüfkarte  $\xi = (\rho^\epsilon \tau)$  ergibt. Dann wird diese blindisierte Prüfkarte zusammen mit einem Antrag ("Ich will elektronisch wählen") in (4b) an das Trust Center geschickt. Das TC unterschreibt dies und das ergibt dann  $\xi^\delta$  und schickt das dann an

den Wähler zurück (4c). Im vorletzten Schritt (4d) speichert der Wähler dies auf der Signaturkarte, wo dann durch Division durch  $r$  die finale Prüfkarte erhalten wird (4e).

### 3.5 Schritt Fünf: Blinde Unterschrift der Wahlkarte

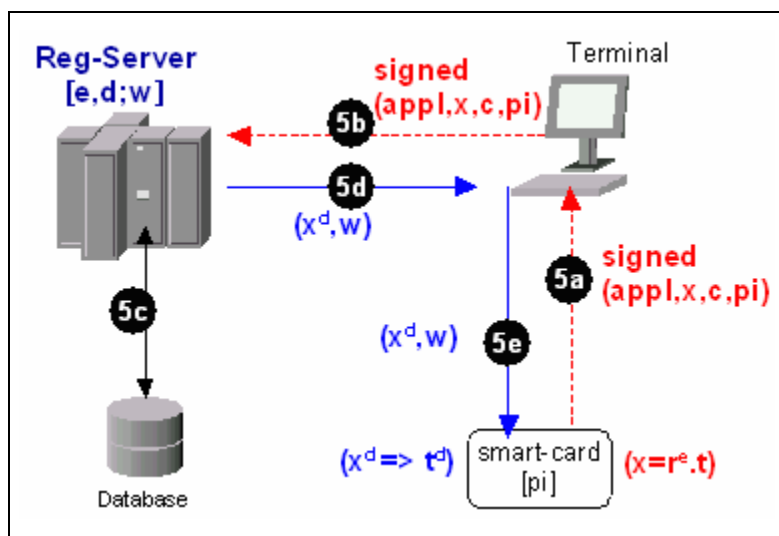


Abbildung 8: Blinde Unterschrift der Wahlkarte

Der letzte Schritt besteht aus dem Wähler, der die Wahlkarte beantragt, durch Laden der blindisierten Wahlkarte  $x$ , die aus  $(tr^e)$  besteht, von der Signaturkarte (5a). Anschließend wird diese zusammen mit der Personenbindung  $pi$ , der Wahlkreisinformation  $c$  und dem Wahlkartenantrag **„Ich will elektronisch wählen“** zum Registrierungsserver geschickt (5b). Die Registrierung überprüft dann erneut die Wahlberechtigung und den Wahlkreis des Wählers anhand der Personenbindung. Nach positiver Prüfung wird die blindisierte Wahlkarte  $x$  unterschrieben. Weiters sendet der Server  $x^d$  mit der Wahlkreisinformation zurück an den Wähler (5d) und markiert den Wähler in der Wählerevidenz mit einer Information „hat elektronische Wahlkarte bekommen“ (5c). Der letzte Schritt ist dann (5e)  $x^d$  und  $c$  auf der Signaturkarte zu speichern, wo dann daraus  $t^d$  erzeugt ist durch die Division mit  $r$ .

## 4. Zusammenfassung

Dieser Artikel beschreibt einen Algorithmus für die Durchführung von öffentlichen Wahlen mittels e-Voting über das Internet. Nicht nur wird darin das Problem der anonymen Stimmabgabe gelöst, sondern der Algorithmus ist auch unter „unfreundlichen“ Bedingungen sicher, z. B. wenn die Administration des Registrierungsservers und der Wahlurne zusammenarbeiten.

Nachdem aber Wahlprozeduren von Land zu Land variieren, muß die Implementation von solchen Algorithmen sich immer an den lokalen Gegebenheiten und neuen Entwicklungen des Landes anpassen.

In Österreich haben zwei Entwicklungen dieses Projekt wesentlich beeinflusst. Auf der einen Seite die klaren rechtlichen Regelungen für den Einsatz eines elektronischen Wahlsystems und auf der anderen Seite die österreichische Bürgerkarte und der zugehörige Security Layer. Die weitere Arbeit der Autoren konzentriert sich nun auf die Implementierung der zweiten Phase des Prototypen<sup>4</sup>, damit der Algorithmus in einer realen Umgebung getestet werden kann um Erkenntnisse für die Verbesserung des Algorithmus zu finden.

<sup>4</sup> Der hier vorgestellte Prototyp kann frei auf der Website der Autoren unter <http://www.e-Voting.at> auf Englisch und Deutsch heruntergeladen werden.

## LITERATUR

- [1] Die österreichischen Nationalratswahlen von einst bis heute, [http://www.modernpolitics.at/publikationen/jahrbuch/wahlergebnisse/wahlen\\_index.htm](http://www.modernpolitics.at/publikationen/jahrbuch/wahlergebnisse/wahlen_index.htm), abgerufen am 2002-09-25.
- [2] J. Weiss, Gesetzesantrag >>Einführung der Briefwahl auf Landes- und Gemeindeebene<<, [http://www.parlinkom.at/pd/pm/XXI/I/his/000/I00005\\_.html](http://www.parlinkom.at/pd/pm/XXI/I/his/000/I00005_.html), abgerufen am 2002-08-15.
- [3] W. Dujmovits, *Auslandsösterreicherwahlrecht und Briefwahl*. Wien: Verlag Österreich, 2000.
- [4] A. Prosser and R. Müller-Török, "Electronic Voting via the Internet", präsentiert bei International Conference on Enterprise Information Systems ICEIS2001, Setúbal, 2001.
- [5] H. Nurmi, A. Salomaa, and L. Santeau, "Secret Ballot Elections in Computer Networks", *Computers and Security* 36 (10), S. 553-560, 1991.
- [6] D. Chaum, "Blind Signatures for Untraceable Payments", präsentiert bei Advances in Cryptology, 1982.
- [7] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", präsentiert bei Advances in Cryptology - AUSCRYPT92, Berlin, 1993.
- [8] e-Austria in e-Europe, [http://www.austria.gv.at/aktuell/database/topnews/german/20000414\\_713.html](http://www.austria.gv.at/aktuell/database/topnews/german/20000414_713.html), abgerufen am 2002-08-15.
- [9] Homepage der Wirtschaftsuniversität Wien, <http://www.wu-wien.ac.at>, abgerufen am 2002-12-15.
- [10] ARGE Daten, Überflüssiges Meldegesetz, <http://www.ad.or.at/news/20010108.html>, abgerufen am 2002-12-15.
- [11] A. Hollosi and G. Karlinger, "Security-Layer für das Konzept Bürgerkarte", BMÖLS, CIO Unit, Wien 2002.