Die erste Internet-Wahl Österreichs: Ein Erfahrungsbericht von e-Voting.at

The first Internet-Election in Austria: The Findings by e-Voting.at

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

Arbeitspapiere zum Tätigkeitsfeld
Informationsverarbeitung und Informationswirtschaft
Working Papers on
Information Processing and Information Management

Nr./No. 04/2003

Herausgeber / Editor:
Institut für Informationsverarbeitung und Informationswirtschaft
Wirtschaftsuniversität Wien · Augasse 2-6 · 1090 Wien
Institute of Information Processing and Information Management
Vienna University of Economics and Business Administration
Augasse 2-6 · 1090 Vienna

pm production management

E-Mail: e-Voting@wu-wien.ac.at
WWW: http://www.e-Voting.at

Die erste Internet-Wahl Österreichs: Ein Erfahrungsbericht von e-Voting.at

Internetwahlen (e-Voting) sind zu einer realen Möglichkeit geworden, es müssen aber die allgemeinen Wahlrechtsgrundsätze eingehalten werden. Mithilfe des Jubiläumsfonds der Stadt Wien wurde an der WU Wien das weltweit erste System zur Stimmabgabe über das Internet entwickelt, das die Einhaltung der Wahlrechtsgrundsätze technisch garantieren kann.

Bei der Entwicklung eines e-Voting-Systems müssen vor allem folgende Probleme gelöst werden:

- 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**.

Der vorliegende Prototyp basiert auf einem von Prof. Alexander Prosser am Institut für Informationsverarbeitung und Informationswirtschaft der WU Wien entwickelten Verfahren, das international publiziert und damit der öffentlichen Diskussion und Prüfung zugänglich ist. Zur absoluten Sicherung der Anonymität teilt das Verfahren die Wahl in

- die **Registrationsphase**, bei der sich der Wahlberechtigte identifiziert und die Ausstellung einer elektronischen Wahlkarte beantragt sowie
- die **Stimmabgabephase**, bei der die elektronische Briefwahlkarte für die anonyme Stimmabgabe eingesetzt wird.

ANMELDUNG

Das Verfahren ist für die Verwendung der Bürgerkarte ausgerichtet. Der Prototyp nutzt daher auch die reale Infrastruktur der Bürgerkarte und des Zentralen Melderegisters (ZMR) und bietet eine standardisierte Schnittstelle zu Trust Center-Diensten zur Authentisierung:

Benutzersicht	*Technischer Prozess*
➢ Aufruf der Web-Page zum Lösen einer Briefwahlkarte.	➢ Signiertes Java Applet, das den Benutzer durch die kommenden Schritte führt, wird vom Registrationsserver geladen.
➢ Einlegen der Bürgerkarte.	➢ Die Personenbindung wird an den Registrationsserver geschickt, ➢ Prüfung der Wahlberechtigung.
➢ Signieren des Antrages auf Ausstellen einer elektronischen Wahlkarte.	➢ Die elektronische Wahlkarte wird an den Registrationsserver geschickt und von diesem blind signiert; i.e., es wird authentisch unterschrieben, der Unterschreibende sieht aber nicht, was er unterschreibt; **wird die Wahlkarte daher später verwendet, kann sie zum Antragsteller nicht rückverfolgt werden.**

➢ Signieren des Antrages auf Ausstellen einer elektronischen Prüfkarte durch das Trust Center des/der Wahlberechtigten.	➢ Prüfkarte wird an das Trust Center zur blinden Signatur geschickt, ➢ unterschriebene Prüfkarte retourniert. ➢ Trust Center Prüfkarte und Wahlkarte werden auf der Bürgerkarte gespeichert, ➢ Ausstellen der elektronischen Wahlkarte wird in der Wählerevidenz vermerkt.
➢ Entnehmen der Bürgerkarte.	

Anmerkungen:

- Die Personenbindung der österreichischen Bürgerkarte verknüpft das digitale Zertifikat der Signaturkarte, die vom Trust Center vergeben wird, untrennbar mit der ZMR-Zahl des Wahlberechtigten. Damit werden die digitale Identität und die reale Person untrennbar miteinander verbunden.

- Die digitale Unterschrift des Antrages auf Ausstellung einer elektronischen Wahl- bzw. Prüfkarte erfolgt unter Nutzung des Security Layers der Bürgerkarte.

- Nach Lösen der elektronischen Wahlkarte wird der Wahlberechtigte aus der konventionellen Wählerevidenz entfernt – eine Doppelwahl ist nicht möglich.

- Sollte die elektronische Wahl- oder Prüfkarte während der Übertragung verloren gehen, so ist ein Wiederanlauf möglich, d.h. die blind signierte Wahlkarte wird nochmals an den Antragsteller geschickt – mithilfe kryptographischer Verfahren ist sichergestellt, dass niemand außer dem Antragsteller die Wahlkarte entschlüsseln (und damit verwenden) kann.

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.

Der geheime Schlüsselteil verbleibt zunächst beim jeweiligen Wahlbeobachter bzw. wird bei einem Notar hinterlegt.

Benutzersicht	*Technischer Prozess*
➢ 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.	Die Urne prüft ➢ ob die Wahlkarte bereits verwendet wurde, ➢ sowie die Authentizität der Unterschriften von Wahlkarte und Prüfkarte. ➢ Im Gutfall erhält der Wählende einen Stimmzettel.
➢ Der Stimmzettel wird ausgefüllt und an die Urne geschickt.	➢ Der Stimmzettel wird mit den Schlüsseln der Wahlbeobachter vercodiert und zusammen mit Wahl- und Prüfkarte an die Urne geschickt. ➢ Die Authentizität von Wahl- und Prüfkarte wird nochmals geprüft. ➢ Im Gutfall wird die codierte Stimme gespeichert.
➢ Die Wähler/in erhält eine Quittung, dass die Stimme angekommen ist (ohne Nennung der Liste).	

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 (S‘) veröffentlicht – und ist damit öffentlich festgeschrieben. Die Wahlbeobachter stellen sodann ihre geheimen Schlüssel zur Verfügung, mit denen die Stimmen entschlüsselt werden können (S).

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

Weitere kryptographische Verfahren verhindern das Löschen von codierten S’ und das Einschleusen von Stimmen durch die Administratoren des e-Voting-Systems vor Ende der Wahl.

BÜRGERKARTE

Die Bürgerkarte ist das ideale Medium für e-Voting und schafft somit in Österreich günstige Voraussetzungen für die Umsetzung von Internet-Wahlen. Zwei Aufgaben werden dabei von der Bürgerkarte erfüllt: die Signatur des Antrages auf Ausstellung einer elektronischen Wahlkarte und die Zwischenspeicherung von Wahl- und Prüfkarte. Um diese Funktion als Speichermedium erfüllen zu können, müssen aber bestimmte datenschutzrelevante Anforderungen durch die Bürgerkarte erfüllt werden:

- Wahl- und Prüfkarte müssen vor unbefugtem Auslesen geschützt und somit in einem PIN-gesicherten Bereich gespeichert werden – dies ist bereits heute möglich.

- 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.

UMSETZUNG UND TESTWAHL

Der im Rahmen des Projektes entwickelte Prototyp wurde in einer Testwahl im Mai 2003 parallel zur Wahl der Österreichischen Hochschülerschaft an der WU Wien erstmals eingesetzt. Dieser Prototyp wurde von einem – gerade im internationalen Vergleich – sehr kleinen Team von Prof. Alexander Prosser und drei temporären Projektmitarbeitern bzw. Dissertanten der Abteilung Produktionsmanagement entwickelt. Umso bemerkenswerter ist, dass hier die erste Internet-Wahl Österreichs und darüber hinaus die erste Internet-Wahl weltweit durchgeführt werden konnte, bei der ein System zum Einsatz kommt, das die Einhaltung der Wahlrechtsgrundsätze technisch garantieren kann. Hier hat die WU Wien eine weltweite Pionierrolle übernommen.

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

- die Identifizierung erfolgte über die Standard-Login-Maske des Universitätsrechenzentrums,

- die elektronische Wahlkarte wurde auf einem beliebigen Speichermedium gespeichert.

980 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 Mitglieder der Wahlkommission (Repräsentanten der drei stärksten Fraktionen an der ÖH WU) entschlüsselt und gezählt.

EVALUIERUNG DER TESTWAHL

Alle Komponenten des Systems – Lösen der elektronischen Wahlkarte, Stimmabgabe und Öffnen der elektronischen Wahlurne – funktionierten einwandfrei. Zum Support der Benutzer wurde ein Helpdesk eingerichtet, wobei sich kaum Benutzerprobleme ergaben. Andererseits gingen zahlreiche Anfragen von Studierenden ein, warum das System nicht für die reale ÖH-Wahl eingesetzt wurde. Es zeigte sich, dass Personen, die einen Web-Browser handhaben können, auch mit dem e-Voting-System umgehen können.

Anzumerken ist, dass bei Verwendung der Bürgerkarte als Speichermedium einige diesmal noch notwendige Schritte wegfallen würden (z.B. der Dialog zum Speichern und Einlesen der elektronischen Wahlkarte). Ein reales e-Voting-System wäre also noch einfacher zu bedienen als der Prototyp.

Bezüglich der Ergebnisse von Internet-Wahlen geht e-Voting.at von 2 zentralen Hypothesen aus:

- H1: e-Voting steigert die Wahlbeteiligung
- H2: e-Voting erzeugt dieselbe Verteilung der Stimmen auf die kandidierenden Listen wie die papierbasierte Wahl

Die „Wahl“beteiligung an der Testwahl betrug 36%, diejenige zur realen ÖH-WU-Wahl dagegen knapp 26%, obwohl klar kommuniziert wurde, dass es sich hier um eine für das reale Wahlergebnis irrelevante Testwahl handelte.

Die Verteilung der Stimmen bei der Testwahl entsprach bis auf wenige Zehntelprozentpunkte dem realen Ergebnis.

The first Internet-Election in Austria: The Findings by e-Voting.at

Internet elections (e-voting) have become a real possibility, but the General Voting Principles have to be guaranteed in either way. Funded by the Anniversary Fund of the City of Vienna the first system to vote via the Internet has been developed that technically guarantees these constitutional voting principles.

When developing an e-voting-system one has to solve the following problems:

- Unambiguous identification of the voter,
- Absolute anonymity when casting the vote
- The administration must not be able to (a) corrupt the anonymity or (b) to manipulate any vote.

The actual prototype is based on a protocol developed by Prof. Alexander Prosser, Institute for Information Processing and Information Economics at WU Vienna that has been published internationally. It is thereby available for public discussion and examination. For absolute protection of the anonymity the protocol divides the election in two stages:

- Registration phase, where the voter identifies him/herself and applies for an electronic voting token and
- The vote casting phase, where the electronic voting token is used to cast a vote anonymously.

REGISTRATION

The protocol is designed for use with the Austrian National ID card. The prototype uses the real infrastructure of the National ID card and the central register (ZMR) and offers a standardized interface for trust center services for authentication:

Userview	*Technical process*
➢ Opening the Web page to apply for a voting token.	➢ A signed Java applet that guides the user through the following steps is loaded from the registration server.
➢ Inserting the National ID card	➢ The personal identification with the ZMR-Number of the eligible voter is sent to the registration server, ➢ Check of voting egibility.
➢ Signing the application for issuing an electronic voting token.	➢ The electronic voting token is sent to the registration server and this server is signing it blindly (i.e. it is signed authentically but the signing server dows not see the signed document. **When using the token later on, it cannot be traced back to the applicant.**

➢ Signing the application for a validation token by the trust center.	➢ Validation token is sent to the trust center for the blind signature ➢ Signed validation token is returned. ➢ Trust center validation token and voting token is saved on the National ID card. ➢ The issue of the voting token is marked in the voter register

Remarks:

- The personal identification of the Austrian National ID card combines the digital certificate of the signature card, that is issued by the trust center, with the ZMR-number of the eligible voter. Hereby the digital identity and the real person can be combined.
- The digital signature of the application is facilitated by the use of the Security Layer of the National ID card.
- After issuing the electronic voting token the eligible voter is removed from the conventional voter register. Double voting is prevented.
- If the electronic voting token or the validation token is lost in transfer, a reissue is possible, i.e. the blindly signed voting token will again be sent to the applicant – using cryptographic procedures it is secured that no one besides the applicant can decrypt the voting token.

VOTE CASTING

When the eligible voter casts the vote on Election Day, then the authentication is done using the electronic voting / validation token. This step is completely anonymous.

The election committee known from conventional voting is emulated, it serves as measure to prevent manipulation by the administration of the election servers. Its members are nominated by the candidating parties. Each member creates an asynchronous key pair, and the ballot sheet is encoded with each separate public key of the comissioners. The secret (private) key is kept secret.

Userview	*Technical process*
➢ Opening the Web page for casting the vote.	➢ The signed Java applet that guides the user through the following steps is loaded from the ballot box server.
➢ Inserting the National ID card and sending the voting and validation token.	➢ The ballot box server checks ➢ If the voting token has already been used, ➢ the authenticity of the signatures on the voting and validation token. ➢ If authorised, the voter receives the ballot sheet.

➢ Ballot sheet filled in and sent to the ballot box.	➢ Ballot sheet is encoded with the public keys of the comissioners and sent with the voting/validation tokens to the ballot box server. ➢ The authenticity of the voting/validation token is again checked. ➢ In positive cases the coded vote is saved.

COUNTING

The votes are submitted encoded; they can only be read after the members of the election committee have entered their private keys in the system. After the end of the election the encoded results will be published in the Internet. The committee members can then provide their private keys for the results to be decoded and counted.

All key pairs of the election committee members are also published so that everybody can reconstruct the final result.

Further cryptographic protocol parts prevent the administration from inserting votes or from deleting encoded votes before the end of the election.

NATIONAL ID CARD

The National ID card is the best medium for e-voting and brings Austria in an exceptional position for implementing e-voting. Two tasks are taken over by the National ID card: the signature of the application for an electronic voting token and the intermediate storage of the voting and validation token. To fulfill the function as storage medium the National ID card has to be adapted in the following points due to data-security related issues:

- The voting and validation token has to be protected from unauthorized access – this is already possible by PIN protecting the tokens – this is already today possible,

- On Election Day it must be technically guaranteed that the ballot box application only reads the voting and validation token and nothing else by which anonymity could be compromised. This requirement is currently not fulfilled by the National ID card as the digital certificate and the personal identification is freely accessible.

The last point shows that the National ID card has been designed for a total different scenario, where anonymous e-government applications did not play any role. This is especially a problem when combining National ID card and ATM-card.

IMPLEMENTATION AND TEST ELECTION WU 2003

The prototype that has been developed in this project has first been used during the test election in may 2003 in parallel to the Austrian Student Union elections at WU Vienna. This prototype has been developed by a – measured by international numbers – small team of Prof. Prosser and three temporary project assistants respectively Ph.D. students. This is even more astonishing that here the first Austrian Internet election has been conducted and the first Internet election world wide that could guarantee the General Voting Principles.

As at this test election the National ID card was not available in large enough numbers, the project team had to replace the two National ID card roles, by

- Using the identification facilities by the WU computer center.

- The electronic voting token was saved on a non-specific medium.

978 students that major in IT relevant studies were eligible to participate in the test election. The application for the voting/validation token could be signed from 1st of May to 19th of May 2003, the vote casting itself took place during the regular student union voting days, from 20th – 22nd of May. On 22nd of May at 3 pm the ballot box was opened and decoded by the election committee and votes were decoded and entered the tally.

EVALUATION OF THE TEST ELECTION WU 2003

All components of the system – registration, vote casting and the opening/counting of the ballot box worked perfectly well. For the support of the user a helpdesk was available where hardly any user request had to be solved. Rather more students called to ask why this vote was not valid for the regular student union election. It was also shown that persons that can use a web browser can also use an e-voting system.

Using National ID cards will facilitate the use of the e-voting system even further, as all read and store operations will be done automatically by the card readers – the respective file dialogues which are necessary in the current prototype will be eliminated.

For the results of the Internet election, e-voting.at defined two hypotheses:

- H1: e-voting raises the voter turn out
- H2: e-voting results in the same results in the digital voting process as in the paper based voting process.

The voter turnout for the test election has been 36%; the real paper-based student union election could attract 26%, hence the turn-out in the electronic election was 40% higher than in the conventional, paper-based system.

The allocation of the votes in the test election corresponded to the result in the real election.