Electronic Voting: Algorithmic and Implementation Issues

Article · January 2003

DOI: 10.1109/HICSS.2003.1174319 · Source: CiteSeer

3 authors, including:

Robert Krimmer

E-Voting.CC

248 PUBLICATIONS **2,205** CITATIONS

SEE PROFILE

Alexander Prosser

Vienna University of Economics and Business

111 PUBLICATIONS **429** CITATIONS

SEE PROFILE

Electronic Voting: Algorithmic and Implementation Issues

Robert Kofler, Robert Krimmer, Alexander Prosser[1]
Department Production Management
Vienna University for Business Administration and Economics
Pappenheimgasse 35/5, A-1200 Vienna, Austria; Telephone +43 (1) 31336/5615
{robert.kofler, robert.krimmer, alexander.prosser}@wu-wien.ac.at

Abstract

Electronic Transactions over the Internet, particularly using the World Wide Web have become an integral part of economic life. Recently also the public sector has started to use the new medium for its administrative processes. This paper analyses several approaches to implement an electronic voting system and discusses them with a view to voter anonymity and protection from manipulations.

The paper then develops an algorithm designed to guarantee anonymity of the voter and to avoid the risk of manipulation of votes. The algorithm is based upon the strict separation of voter registration and submission of votes, which implies that certain information has to be stored on a secure media. The paper discusses the security criteria and possible implementation options for such secure storage.

Key Words: Electronic Voting, Electronic Democracy, Internet Applications

1. Introduction

In the past years many governments have started to adopt Internet-based applications for their administrative processes; applications range from the simple download of forms to Internet-based submission of applications or tax declarations to full-scale electronic procurement systems. The first mover in this area was the U.S. Federal Government with the Federal Acquisition Network (for an analysis see [1]), in the meantime similar systems are being deployed in several EU countries [2]. [3].

Such systems use commercially available technology and basically automate administrative processes. The question arises whether Internet services could also be used for voting processes and, if so, to derive the design principles of such systems.

Let us first clarify some notions:

- We consider electronic government to be the application of Internet technology to support administrative processes; Internet technology comprises Web applications, electronic mail, electronic data interchange as well as mobile access to the Internet via WAP or UMTS terminals.
- Electronic democracy would be the use of such technology to support the participation of the citizen in democratic decision-making, such as elections, petitions, referendums, and the advertising prior to them,
- of which electronic voting (e-voting) is a subset, that is the support of an anonymous voting procedure, which is the main theme of this paper.

The term "electronic voting" has been used for a large variety of systems, ranging from hand-held infrared devices used, for instance, at the shareholder meeting of a publicly listed corporation, kiosk systems with touch screens to be used in polling stations to remote voting via the Internet. In the following, we will focus on Internet voting only. It should be noted, that any Internet voting system can also be used as a kiosk system in the polling station.

The following Section 2 analyzes the requirements for an electronic voting system (2.1 and 2.2) and discusses several approaches to implement electronic voting found in the literature (2.3 and 2.4); Section 3 proposes an alternative algorithm, which is the basis for an e-voting system currently developed for the City of Vienna (Austria). Implementation issues resulting from the requirements of the algorithm are also discussed in Section 3.3. Section 4 outlines further research.

2. Requirements for e-voting

2.1. Voting Principles

In General, the requirements for conventional, "paper-based" voting also apply to e-voting. These principals for democratic elections can be expected to be universal; of course, voting procedures may differ in many details. Taking the Austrian Federal Constitution as an example

[1] The work of Kofler and Krimmer was supported by the City of Vienna under grant number JUB0109.

(Art. 26 B-VG) the right to vote is defined as common, direct, equal, personal and secret. The Internet Policy Institute [4] specified these principles with a view to electronic voting:

Free elections: the citizen must be able to use her/his voting rights without being coerced and without undue influence of a third party. The vote must reach the election authority without the chance of manipulation.

Secret voting: no person must know the vote of another person, counting of votes must be delayed until a sufficient number of votes ensures that no conclusions as to the vote of the individual voter can be drawn.

Equal voting rights: each vote must have the same weight. No vote must become invalid by predictable technical problems or must be lost on its way to the voting authority. Also, the right to vote must not be made dependent on factors other than those enumerated in the Law (e.g., a criminal conviction).

Audibility: the whole voting process must be transparent and reproducible.

Reliability: the whole voting system should work robustly (i.e. so that no votes are lost), even if failures occur like loss of Internet communication or malfunctioning voting machines.

Flexibility: the system should be configurable for many different election scenarios (like different ballot question formats or multiple languages etc.) and on a technical level compatible with multiple operation system platforms as well.

Uniqueness: No voter should be able to vote more than once.

Integrity: votes as such should not be modifiable, forged or deleted without detection and the possibility to repair the manipulation.

Convenience: election systems should not require extra skills to be usable and without unreasonable need for equipment.

2.2. Authentication vs. Anonymity

As it is rather uncomplicated to fulfill the requirements for equal and direct elections, the main technical problem for the deployment of e-voting can be derived from the requirement for personal and secret elections. How can a person be identified unequivocally and her credentials checked in the voting process and yet be able to cast an anonymous vote? Any e-voting protocol has to solve this central issue.

Internet-based e-voting can best be compared to mail voting, which has already existed for quite some time in some European countries, for instance, in Germany and France; recently it was also introduced in Switzerland; Austria currently limits the use of mail voting to citizens living abroad [5]. In mail voting, the voter has to register before the elections and can cast her vote within a given timeframe anywhere. The vote is sent to the election authorities by mail. In many respects Internet voting can be seen as an analogy. In a fundamental contribution, *Nurmi*, *Salomaa* and *Santean* [6] identified the two basic elements in any e-voting system:

1) The registration process during which the voter is **identified** unambiguously

2) The voting process as such, where the voters is **anonymous**

2.3. Identification

The systems can be grouped in 3 different classes: PIN-based or TAN-based systems and systems using smart cards for identification.[2]

2.3.1. PIN-based Systems. The voter is an identified user on the Internet, after Login the ballot sheet can be filled out and sent in, where the communication between the browser and the voting server is secured using cryptographic standards, however, it is obvious that anonymity cannot be guaranteed.

As an example, the system of Soundcode called “Vote here gold” [7] offers a PIN-based system that can be used via the Internet. The voter works as an identified user that can fill out and hand in the ballot sheet after a login, where the communication between WWW browser and election server is secured cryptographically. Using this system, anonymity can obviously not be guaranteed to the voter and it has to be relied on the integrity of the election authority. The main applications for such a system are (i.e. student) union, faculty or interest group elections where absolute anonymity is not necessary, the most important issue or where it is planned to hold open and public elections. Such systems can lower the transaction costs for elections drastically and in the case of dislocated voters be prerequisite for a fast election. An example could be a strike ballot of an airline.

2.3.2. TAN-based Systems. In such systems Transaction Numbers are issued and the election is usually possible by using the TAN in a Web browser. The connection between the voter and the Web server is also secured and the cryptographic key is issued by a Trust Center (for an introduction, see [8], [9]). The voter receives a random number as a receipt for casting the vote, which can be used to check whether the vote entered the tally correctly at a different Website.

[2] The PIN-based identification method is to be differentiated from the entry of a PIN for securing access to data stored on a smart card, which is discussed later.

If the party issuing the TANs and the party running the election server collecting the votes collude, anonymity cannot be guaranteed. Also, the distribution of TANs for each single election is costly and errors may occur.

The election.com system is an example for a TAN-based system that was used in May 2002 to elect the EU-Student-council [10]. In this case TANs are used and the election itself is possible by entering the TAN using an Internet-application. The Web-traffic between the voter and the election server is securely encrypted and the key is provided by a Trust Center.

The voter receives a random number as a receipt, with that it is possible to check at a different terminal if the vote was counted correctly.

A similar system was used for the election of the Jugendgemeinderat (young city council, an unofficial advisory board) at the German town of *Fellbach* in 2001 [11].

2.3.3. Smart Card-based Systems. Hence, neither PIN- nor TAN based systems can be used for democratic elections, however, both are relatively easy to implement and can be used for a wide range of voting applications, where requirements for anonymity are less stringent (e.g., workers representatives, chambers or professional organizations) or where anonymity is not a requirement at all (e.g., in the Swiss canton Appenzell Innerrhoden votes are traditionally still cast openly at the commencement of the *Landsgemeinde*, where all persons entitled to vote come together to elect the *Ständerat* [12]).

Anonymity can not be guaranteed technically for any of the two systems, but is dependent on the integrity of the election organizers and their server administration. Also, neither PIN nor TAN have a legal foundation as means of identification as is the case with digital signatures. Hence, the further discussion will concentrate on e-voting systems using smart cards for digital signatures, which also enables the use of cryptographic methods.

2.4. One-stage Smart Card-based Systems

The algorithm by *Fujioka*, *Okamoto* and *Ohta*, which was first published in 1993 [13], has become the algorithmic basis of a considerable number of systems (for example Lorrie Cranor's Sensus [14] or the German system i-Vote [15]).

Let us first introduce some notation:

BS	.............Ballot Sheet
B	...............Ballot box Server
R	..............Registration Server
V	...............voter
m , m'	.... Symmetric crypto key
$S_{\{priv,pub\}}^{\{V,R,B\}}$	.....The voter's, the registration's and the ballot box server's signature key pair
$K_{\{priv,pub\}}^{\{V,R,B\}}$	....Their key pair for encryption

The algorithm assumes the use of a Trust Center for obtaining each party's public signature or crypto key, the respective calls are not shown.

In its basic layout, the algorithm follows the registration - ballot box approach proposed by [NSS91].

Consider Figure 1. The algorithm starts with the voter filling out the ballot sheet BS , which is encrypted with a symmetric key $(m(BS))$, which is then blinded (i.e. prepared for the blind signature[3]) $blinded(m(BS))$. This packaged is then signed by the voter and encrypted with the public key of the registration K_{pub}^{R} and finally sent to the registration server $K_{pub}^{R}\left[S_{priv}^{V}(blinded(m(BS)))\right]$. The registration checks the identity of the voter by resolving the signature with the voter's public signature key and whether the applicant is entitled to vote. If the checks are positive, the server signs $blinded(m(BS))$ "blindly" giving $\sigma(blinded(m(BS)))$ (i.e., not knowing the encrypted ballot sheet $m(BS)$, let alone BS itself, signs with the standard private signature key S_{priv}^{R} and sends the message $S_{priv}^{R}(\sigma(blinded(m(BS))))$ back to the voter. This message can be encrypted either by the voter's public encryption key maintained by a Trust Center, or a session key could be negotiated between voter and registration beforehand.

The voter first authenticates the registration's digital signature S_{priv}^{R} at the latter's Trust Center and then removes the blinding layer from the signature obtaining $\sigma(m(BS))$. The voter obtains a pair of $m(BS),\sigma(m(BS))$ authenticated by the registration.

This authenticated ballot sheet is sent to the ballot box server, which checks the private signature of the registration server. In the original protocol the encrypted ballot sheet $m(BS)$ is written on a list that is published after the end of the election. The voter then checks if the encrypted vote is on the list and sends the symmetric decryption key m' to the ballot box server. The server uses this key to decrypt the ballot sheet and to count the vote. Finally, after the end of the count the keys and the ballot sheets are added to the public list so every voter can

[3] The blind signature model was developed by David Chaum in 1982 [Chau82]. In general language it can be compared with the signature on a blue paper envelope.
(e,d) ... the server's blind signature pair according to the RSA system
$blinded(m(BS)) = r^{e}m(BS)\bmod(n)$ with r as random
$\sigma(blinded(m(BS))) = \left(r^{e}m(BS)\right)^{d}$ which is then divided by r giving
$$\frac{r^{e^{d}}\left(m(BS)\right)^{d}}{r} = \left(m(BS)\right)^{d}$$

check the authenticity of the election and that it was not manipulated. Hence registration and submission of vote are done in one phase, most implementations also integrate the last phase of sending m' into the main registration/submission phase.

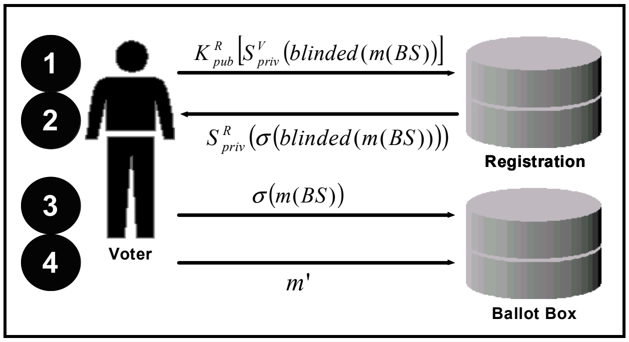
1
2
3
4
$K^{R}_{pub}\left[S^{V}_{priv}(blinded(m(BS)))\right]$
$S^{R}_{priv}(\sigma(blinded(m(BS))))$
$\sigma(m(BS))$
m'
Voter
Registration
Ballot Box

Figure 1: process model for [FOO93]

This algorithm has been implemented in various variations but all variants still maintained the basic problem: it is a one-phased algorithm, which means that both steps, identification and voting, are completed in one stage. When the administration of the registration and ballot box servers collude, it is possible to break the anonymity as well as to vote for voters that were entitled to vote but did not do so. The algorithm is secure on the application level, however, if the browser-based application (e.g., a Java applet) provided by the registration to perform the registration step fraudulently stores the IP address for each blindly signed ballot sheet, and passes on this information to the ballot box, the $m(BS)$ - and eventually also the clear-text ballot sheet after submission of m' - can be linked to a voter later. Also temporary files could be used for this purpose.[4]

Hence, anonymity cannot be guaranteed if registration and vote submission are processed in one stage.

3. Proposing A Two-stage Protocol

The proposal outlined here is a further development based on the algorithm proposed in [17].

This proposed algorithm strictly separates registration and vote submission stage following the original requirements set by [6]:

- **Registration phase**. The voter's credentials are checked and the voter receives a blindly signed election token, which is securely stored (see Section 4).

- **Voting phase**. The voter uses the election token to obtain a ballot sheet and casts her vote.

Figures 2-4 depict the proposal, in addition to the notation that was used in the last section, the voter's Trust Center T will also be used for the voting protocol.

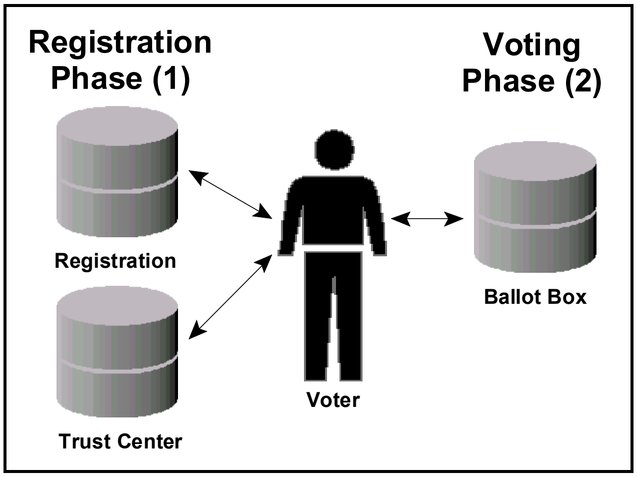

Figure 2: the two phases and the participating parties

3.1. Registration

Voters can register an arbitrary period of time before election day; since the ballot sheet is not handed out upon registration, voters can register even at a time when the list of candidates is not complete yet. As the first step the voter generates a random token t and prepares it for the blind signature, adds a text where she applies for e-voting and signs: $S^{V}_{priv}(blinded(t),\text{"I want to vote electronically"})$. The message is encrypted with R 's public key and sent to the registration $K^{R}_{pub}\left[S^{V}_{priv}(blinded(t),\text{"I want to vote electronically"})\right]$, which verifies the voter's credentials by resolving the public signature key of the voter. If the voter is entitled to vote, the registration signs t blindly giving $\sigma_{R}(blinded(t))$. This is basically the same mechanism as with [13], however, since only a token is signed instead of the ballot sheet, the resulting message can be expected to be considerably shorter, which makes it easier to store the message on a secure medium.

The registration stores the electronic application and strikes the voter off the conventional voter's register. Also $\sigma_{R}(t)$ is stored; if the original signed token is lost and the voter re-applies for another token, the registration will always respond with the original $\sigma_{R}(t)$ to avoid the issue of multiple tokens.

[4] Such files could also be unintended „left-overs“ from the registration process, which happened during the students union election at the University of Osnabrück in 2000 [16]

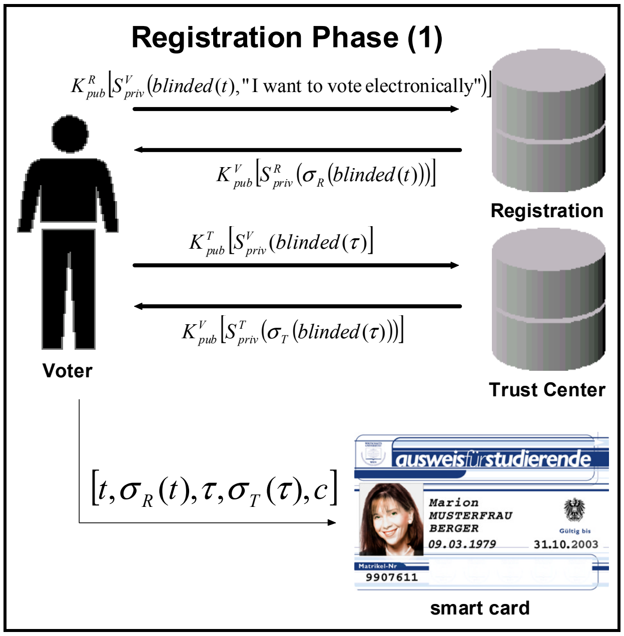
Registration Phase (1)
$K^R_{pub}[S^V_{priv}(blinded(t),\text{"I want to vote electronically"})]$
$K^V_{pub}[S^R_{priv}(\sigma_R(blinded(t)))]$
Registration
$K^T_{pub}[S^V_{priv}(blinded(\tau))]$
$K^V_{pub}[S^T_{priv}(\sigma_T(blinded(\tau)))]$
Voter
Trust Center
$[t,\sigma_R(t),\tau,\sigma_T(\tau),c]$
ausweisfürstudierende
Marion
MUSTERFRAU
BERGER
09.03.1979
Gültig bis
31.10.2003
Matrikel-Nr
9907611
smart card

Figure 3: process model registration phase

In most elections, voters will be organized in constituencies c, this information is also sent back to the voter and has to be submitted on election day to indicate in which constituency the vote is to be counted. To avoid possible manipulation of c the blind signature keys used for $\sigma_R(t)$ can be made specific to the constituency. Hence the clear-text c submitted on election day and the authentication token issued by the registration have to point to the same c.

A similar process is repeated with the Trust Center: The voter issues a second token τ, blinds it and obtains the blindly signed $\sigma_T(\tau)$. This is required as it is the only way to make a collusion of the registration server and the ballot box server useless, as they always need the blind signature authentication of the Trust Center as well in order to forge a vote.

At the end of the registration phase, the voter holds two authentication tokens and her constituency information $[t,\sigma_R(t),\tau,\sigma_T(\tau),c]$, both tokens are needed to cast a vote on election day.

3.2. Voting

On election day the voter sends the tokens to the ballot box server to obtain a ballot sheet. This submission is not signed by the voter and the only means of authentication are the two tokens obtained earlier. The voter generates an asymmetric key m, m' to secure the communication (without disclosing the identity of the voters which would be case when using it's asymmetric crypto key pair on the signature smart card). The voter also adds the identification T of the Trust Center used, which is not used to verify the voter's identity or to obtain any public crypto key, but to choose the right Trust Center key for resolving the blind signature. The message $[c,T,m,t,\sigma_R(t),\tau,\sigma_T(\tau)]$ is encrypted with K^B_{pub} and sent to the ballot box. After decrypting the ballot box resolves the signatures $\sigma_R(t)$ and $\sigma_T(\tau)$ and if the tokens can be authenticated the ballot box issues an empty ballot sheet and encodes it with the symmetric key $(m(BS))$. The voter receives and decrypts it with m' and fills out the ballot sheet. This is then combined with the tokens, c and T, encrypted again with the public crypto key of the ballot box and sent. After authentication of the tokens, the ballot box server stores the ballot sheet and the other information received from the voter.

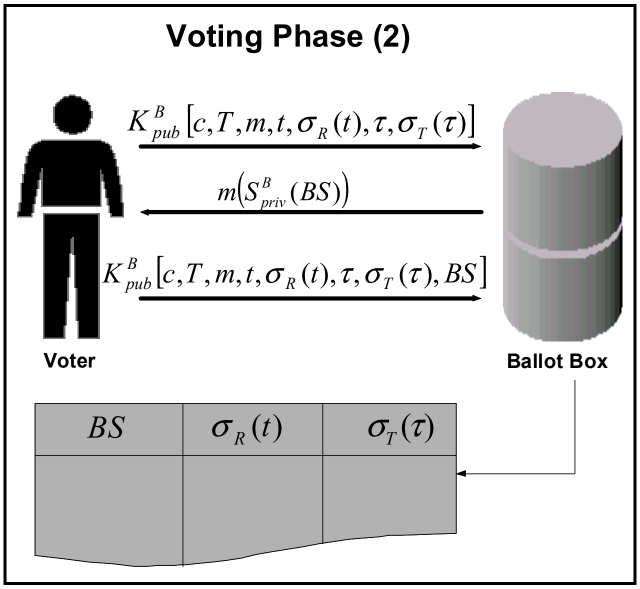
Voting Phase (2)
$K^B_{pub}[c,T,m,t,\sigma_R(t),\tau,\sigma_T(\tau)]$
$m(S^B_{priv}(BS))$
$K^B_{pub}[c,T,m,t,\sigma_R(t),\tau,\sigma_T(\tau),BS]$
Voter
Ballot Box
BS
$\sigma_R(t)$
$\sigma_T(\tau)$

Figure 4: process model voting phase

Apart from the fact that anonymity can be guaranteed to the voter, if he uses different terminals (IP addresses) for registration and submission of vote, the server administration of the registration and the ballot box collude, votes cannot be forged, as a valid vote also has to be authenticated by a Trust Center.

3.3. Storage Media

As the algorithm uses a two-phase-protocol there is the need to temporarily store the token on a secure, anonymous medium. At this point we see three possible ways to store this token:

a) On the smart card used for the digital signature. The advantage of storing the token on the voter's smart card is the protection from data loss as compared to conventional storage media and the protection from unauthorized access when the token is secured by a PIN from reading. This method has two main problems:

- Firstly the legal provisions governing digital signatures have to allow write access at least to some area of the smart card's storage medium and the respective service provider needs to actually prepare the storage area for the storage of a token and the smart card needs to be certified for such a storage process.
- To ensure anonymity when sending the token to the ballot box there must not be any freely accessible data on the smart card identifying the card holder in a storage area which is not secured by a PIN.

The second requirement constitutes a serious problem when implementing electronic voting.

Typically, the card holder's name and other personal data is stored on the card for free read access which means that any application accessing the card can read them without any restriction. Also, every smart card has an identification number that is unique worldwide. This number is initialized during production and it enables tracing the card (and thereby the card owner) whenever it is used.

Of course, the source code of the e-voting software can be made generally available and can be submitted to certification by an independent authority showing that neither the personal data nor the card number is accessed by the voting software, however, (i) it seems doubtful whether this will be sufficient to gain public acceptance and (ii) since the election token resides on the card between registration and election day, any other application accessing the card may read the personal information plus the token stored on the card thereby enabling a third party to trace the vote later.

This shows that the common processor-smart card (as well as the whole PKI/TrustCenter-infrastructure) was designed for a completely different paradigm: Obviously it was assumed that there is no legitimate anonymous application for such a card.

Hence, smart cards used for digital signature can only be used to store the token after a fundamental redesign giving the cardholder full control as to which data is actually read from the card.

b) On any storage medium similar to an electronic purse. This variant solves the problems with serial number and clear text information discussed above: The voter uses a floppy disk or an USB-memory-key during the registration process and the token is saved on it. The implementation would be easy and would rely on general-purpose infrastructure which is available off the shelve.

The disadvantage of this solution is the relative unreliability of the medium. Especially disks are susceptible to read/write errors and the data would have to be secured manually by passwords. These media also allow unrestricted copying; even a regular backup-process can lead to multiple copies of the token. The proposed algorithm is secured against multiple use of one token, however, free duplication of the tokens is not intended – it is easy to imagine that a token that is saved on disk without any safeguard (i.e. with a PIN or password) can be found-out and can be used to undermine the voter's anonymity later.

c) On a smart card other than the smart card used for digital signature. Another possibility would also be the use of a processor smart card, whose serial number is not registered (or safeguarded by a PIN) or a storage card with a minimum of processor functionality (for an introduction cf. [18]). Pure storage cards can be read and written to by general purpose card readers and in both variations there is no need for additional hardware.

In both cases, the card used for the digital signature is used only for identification purposes during the registration phase only and the token is stored on the second card. During the voting phase, only the storage card is used and anonymity can be preserved.

The disadvantages of this method is that handling becomes more complicated (the cards need to be changed during the registration phase), the additional costs of a second card and possible security leakages due to the fact that the card holding the token is not associated with a particular person, as was the case with the signature smart card.

4. Resume

The paper proposed a protocol for secure e-voting via the Internet. The main technical problem in the implementation is the inability of current smart cards used for digital signature to hold an election token that can be used anonymously on election day. We believe that the best solution for enabling the use of smart cards for e-voting will be to protect the user-specific information on the card (particularly the certificate and the card ID) from unauthorized access. This could be implemented by a PIN; however, since several applications can be expected to store confidential information on the card, this may lead to a large number of PINs to be remembered by the card holder (confidential Medicare information, various access data, or an election token). The alternative would be to use only one PIN for all such applications, however, this would lead to the rather unsatisfactory situation that an application that is granted access to one confidential information would also be granted access to all confidential data on the card – including the election token.

In our view, the solution can only be to grant card holders complete control over which data is actually read from the card by an application. In an analogy to the secure viewing applications for digital signatures (the text to be signed is securely displayed on screen), the user has to see and to acknowledge the information read from the card before any application can actually access it. Hence, fraudulent and unauthorized access of data on the card which is of no concern to an application can be prevented. This will also enable the use of smart cards for the purposes of electronic voting.

The protocol outlined in this paper is currently being implemented as a software prototype under a research grant of the City of Vienna. Implementation experience so far shows that - apart from security issues - the unique identification of voters is one of the primary questions in e-Voting. Here, digital smart cards are used for identification, the voter is identified via his/her citizen number in the Central Citizen Register (Zentrales Melderegister). This number is included in the digital certificate of the signature card, thus providing a unique link between the digital certificate, the entry in the voter register and the real person. For a report on the implementation progress, refer to [19].

5. References

[1] R. Müller and A. Prosser, "The economic effects of the transition of the U.S. federal procurement to Electronic Commerce," *CEMS Business Review (2)*, pp. 295-308, 1998.

[2] A. Prosser and R. Müller, "Öffentliche Beschaffung mittels Electronic Commerce," *Wirtschaftsinformatik*, vol. 99, pp. 256-266, 1999.

[3] E-Procurement, *http://simap.eu.int* (as per 2002-03-15).

[4] Report on the National Workshop on Internet Voting, *http://www.internetpolicy.org/research/e_voting_report.pdf* (as per 2002-03-15).

[5] W. Dujmovits, *Auslandsösterreicherwahlrecht und Briefwahl*. Wien: Verlag Österreich, 2000.

[6] H. Nurmi, A. Salomaa, and L. Santean, "Secret Ballot Elections in Computer Networks," *Computers and Security 36 (10)*, pp. 553-560, 1991.

[7] Vote Here Gold, *http://www.soundcode.com/voteheregold.html* (as per 2002-05-25).

[8] J. Feghhi, J. Feghhi, and P. Williams, *Digital Signatures - Aplied Internet Security*. Reading: Addisson-Wesley, 1999.

[9] E. A. Fisch and G. B. White, *Secure Computers and Networks - Analysis, Design, and Implementation*. Boca Raton: CRC Press, 2000.

[10] EU Student Vote, *http://www.eusv.org* (as per 2002-05-25).

[11] Wahl zum Jugendgemeinderat Fellbach, *http://www.fellbach.de/wahlen* (as per 2001-11-20).

[12] Glossar zur Wahl 1999, *http://www.parlament.ch/dL/D/Wahlen/Wahlen99/Glossar_A_Z_d.htm* (as per 2002-05-25).

[13] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," presented at Advances in Cryptology - AUSCRYPT92, Berlin, 1993.

[14] Sensus e-Voting system, *http://lorrie.cranor.org/voting/sensus* (as per 2002-05-23).

[15] Forschungsgruppe Internetwahlen, *http://www.internetwahlen.de* (as per 2002-05-23).

[16] Pressearchiv Forschungsgruppe Internetwahlen, *http://www.internetwahlen.de/internetwahlen/archiv2/archiv2.html* (as per 2002-05-23).

[17] A. Prosser and R. Müller-Török, "Electronic Voting via the Internet," presented at International Conference on Enterprise Information Systems ICEIS2001, Setùbal, 2001.

[18] H.-R. Hansen and G. Neumann, *Wirtschaftsinformatik 1*, 8 ed. Stuttgart: UTB, Lucius & Lucius, 2001.

[19] A. Prosser, R. Kofler, and R. Krimmer, "Implementing an Internet-based Voting System for Public Elections - Project Experience," *submitted to ICEIS 2003*.