

Security Assets in E-Voting

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

Institute for Information Processing, Information Business and Process Management
Department Production Management

Vienna University of Economics and Business Administration
A-1200 Vienna, AUSTRIA

[Alexander.Prosser | Robert.Kofler | Robert.Krimmer | Martin.Unger}@wu-wien.ac.at

Abstract: As discussed in the literature [PrMü01; Rub04; Phi02] e-voting faces a lot of threats. The purpose of this paper is to give a systematically ordered overview of attacks against e-voting and to show one solution to the issues. The challenge is to provide identification and anonymity at the same time and to exclude the possibility of fraudulent manipulations by the server administration, the voter, and any third party.

1 Protocol Issues

1.1 Two-Stage Versus One-Stage Voting Protocols

In a fundamental contribution, Nurmi et al. [NSS91] identified two building blocks in an electronic voting system: (i) Voter identification and registration for e-voting and (ii) vote casting. These steps can be provided in one Internet session (one-step protocol); but here the identification may be used to trace the identity of the vote via the IP address or temporary files. This issue is avoided by a two-stage procedure, which strictly separates voter identification and vote-casting. But the advantage comes at a price, as the result of successful identification (voting token) has to be stored at the voter to be used later to cast a vote. Figures 1a and 1b provide an overview of the two stages.

Registration phase:

The voter applies for a voting token. The system performs a check of his credentials and a check for multiple application. If this is his first attempt, the voter will receive a voting token which he can use anonymously to cast a vote later. If not, the system performs a restart procedure, which always issues the same token to the applicant, which is stored in the database of the registration service.

At the end of the process, the voter checks the authenticity and integrity of the token and stores it either on a smart card or on another media, e.g. a USB token.

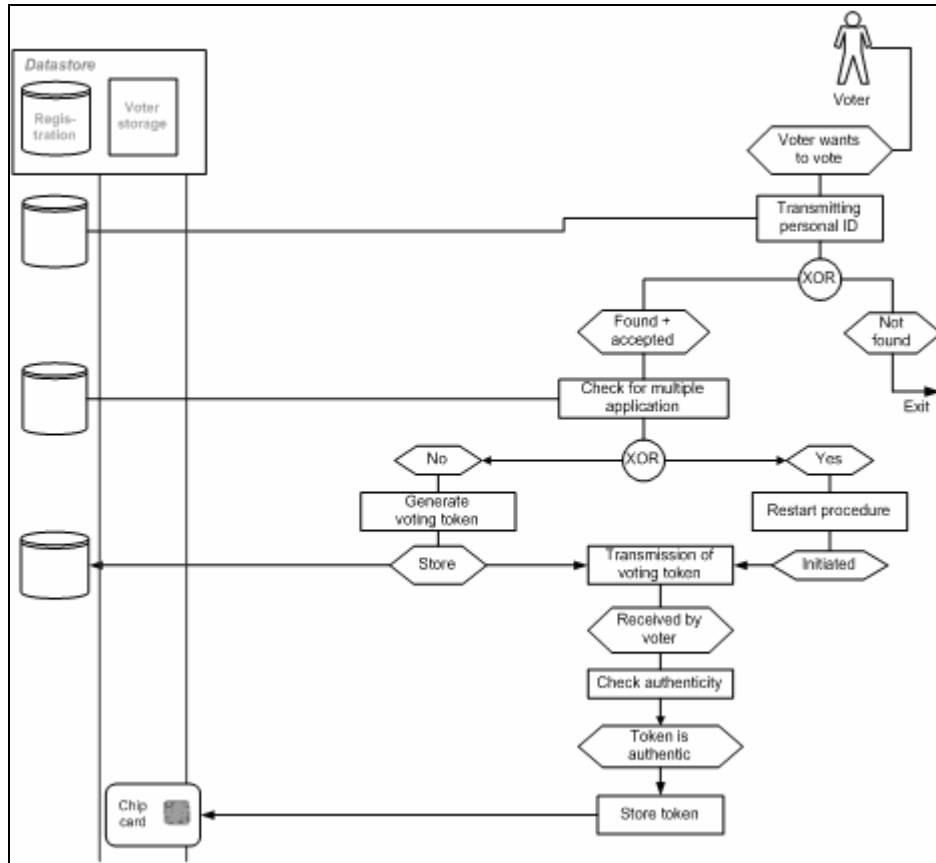


Figure 1a: Registration phase

Voting phase:

The voting application reads the voting token from the storage device and sends it to the ballot box system, which verifies its authenticity and checks for duplicates. If the checks are successful, the voter will receive a ballot sheet, which must be protected against manipulation. The voter fills in the ballot sheet and casts a vote. There is a precaution mechanism that challenges the voter before the vote is actually cast to prevent precipitate or “junk” votes.

Finally the voter receives a confirmation that the vote has been cast successfully.

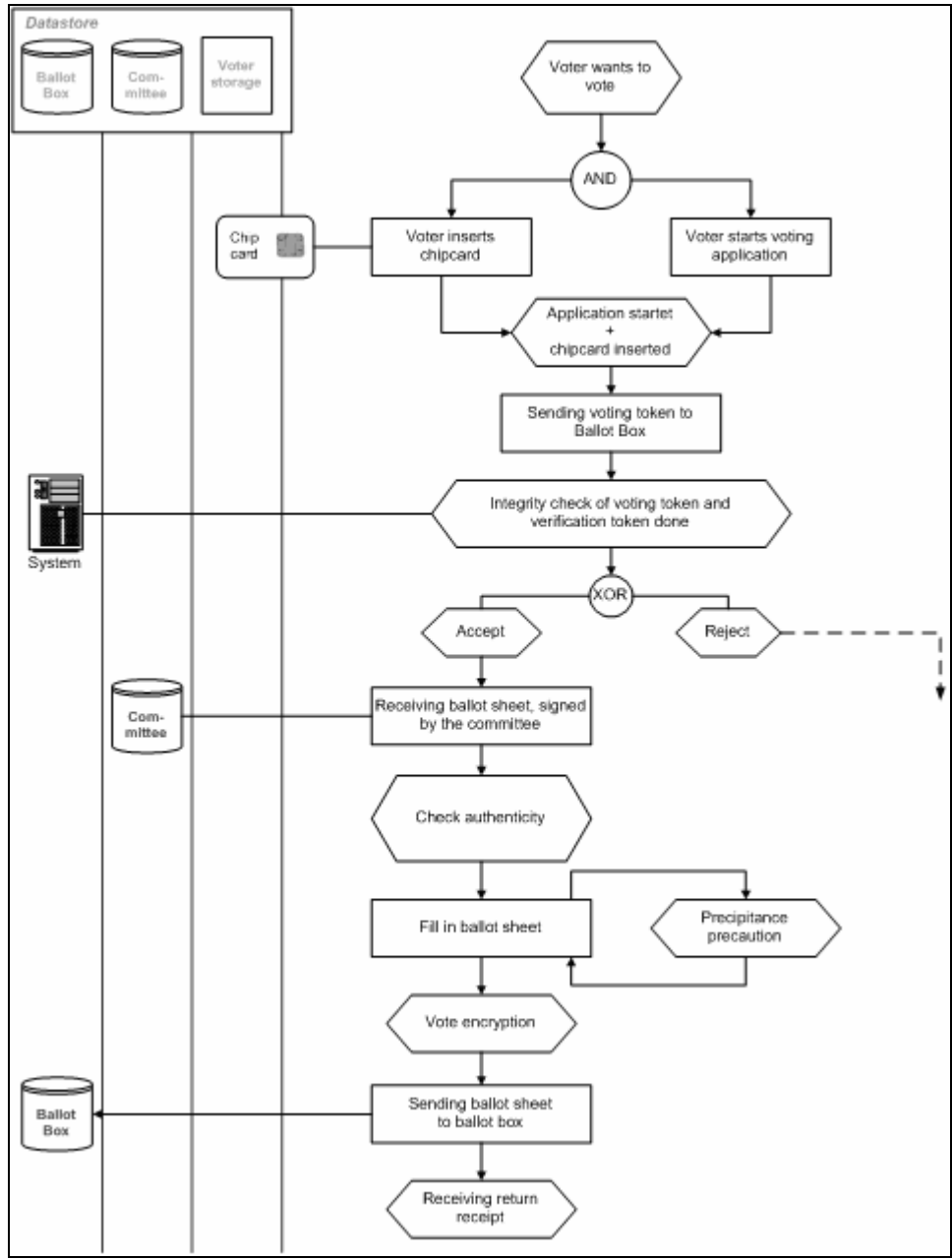


Figure 1b: Voting phase

Eventually, there may also be also a facility for the voter to check whether his vote was counted correctly and entered the tally.

1.2 Threat Scenarios

1.2.1 Threats during Registration

Beginning with the initiation of the process there must be a possibility to verify the authenticity of the voter's application and/or visited webpage [FFW99]. The next step is the application for the selected election (there can be more than one election at the same time). When the user transmits his personal ID or related information, it must be protected from modification, re-send attacks, content sniffing (the fact whether somebody is going to vote should remain private) and all forms of faked identities. The voter's identification and assignment to a constituency must be established beyond doubt and must be protected from manipulation by the voter as well as by the system administration.

Also the constituency the voter belongs to should be protected from manipulation (eg., a voter "re-registers" himself to another constituency, where he perceives that the vote would probably have a higher marginal value). This is particularly an issue in two-stage voting protocols, as the token issued on registration must be used anonymously and hence, has to include the constituency information, so that the vote can be assigned correctly, even though the voter will not be identified at the voting stage.

On the voting server side, it must be assured that multiple (malicious) applications from one person can be handled. The Server administrator must not be able to change a voter's constituency without detection; also selective denial of service to registrants by the administration must be prevented. In addition, the administration must not be able to create fake voting tokens or to-kens on behalf of people, who did not register.

Furthermore the administrator must not delete records from the registration database unrecognized. An audit trail must be producible that links every voting token issued to an eligible voter, showing that every voter also had the opportunity to obtain a voting token but once.

When the voting token is received by the client, some integrity checks should be done before the token is stored on a secure media or if no secure media is available we need equivalent methods to prevent others from using it (eg, a third person, Trojan, virus or other malign application).

1.2.2 Threats during the Voting Phase

Authenticity, validity and integrity of a voting token must be assured, at the same time, the token must be usable in a completely anonymous way. The voter uses the token to apply for a ballot sheet. It has to be assured that the ballot sheet is not modified during transmission by a man in the middle or by the administrator of the ballot box - therefore the voter needs some guarantee that this is the correct ballot sheet he applied for. Duplicate use of voting tokens has to be prevented.

Also, it has to be assured that ballot sheets cannot be manipulated by the server administration and are delivered to the voter authentically. When the voting software renders and displays the ballot sheet, it should use a secure viewer so that no virus or Trojan horse application can neither change the ballot sheet, nor forward the voter's choice to a third party. As the content of the vote should be kept secret even from the election system administration until the ballot box is opened, the vote should also be encrypted in a way that the administration cannot read or manipulate the vote.

The ballot box server environment must prevent the administration from denying access, deleting, inserting or modifying ballot sheets and it must prevent multiple usages of voting tokens. In a two-stage protocol the administrator must not be able to separate the voting token from the ballot sheet. And most importantly, voter anonymity must be guaranteed vis-à-vis the election administration as well as any third party.

The last step in the voting process is a return receipt which shows the voter that his ballot sheet was received. However, no proof must be possible, how a voter voted, as this would enable vote buying and pressured votes. On request, an audit trail must be produced linking the token used and the fact that a ballot sheet was obtained and stored. This audit trail must not corrupt anonymity, but it has to be manipulation-proof, also by the election administration. This also serves as a defence against unfounded objections and complaints from voters, candidates or third parties maintaining irregularities in the voting process in order to sabotage or discredit the election.

1.2.3 Levels of Security

In the discussion of e-voting security, one has to distinguish between organizational and technical security. Precautions are organizational, if they rely on the behaviour of agents and their compliance to rules. Examples would be

- Information stored on two server systems, which, once joined, would corrupt anonymity; the server administrators are obliged (possibly under oath) not to communicate data.
- Servers locked into a safe room to prevent tampering.
- A witness, who (digitally or on paper) signs that a certain document was filled in at a certain time and in a certain place.

Technical precautions provide a technical guarantee against defined manipulations or threats; it does not rely on any agent's compliance with proper procedures. Examples would be

- Cryptographic encoding of ballot sheets to prevent their manipulation by the server administration.
- A blind signature [Chau82] or ANDOS [BCR87] procedure to prevent the tracing of voting tokens.

It should be noted that technical security cannot be absolute – at some stage organizational security has to come in. Digital signature cards, for example, provide an extremely high level of technical security; however, when the card is issued,

organizational precautions against manipulations are necessary to prevent, for example, the card PIN entered by the card holder from being recorded and later to be used in conjunction with the stolen signature card. Hence, the decisive question is, at which level technical security ends and where reliance on organizational measures starts. The following section provides a model to assess this issue in the field of e-voting.

2 Six Aspects of E-Voting Security

Six aspects can be identified in e-voting security to be fulfilled either by organizational or technical/algorithmic arrangements. The degree to which an e-voting system relies on technical security constitutes the essential quality parameter of such a system [IPI01].

The aspects are: (i) Permanent voter anonymity, (ii) voter identification and ascertainment of eligibility, (iii) resistance against all forms of manipulation (third party, voter or administration staff), (iv) prevention of vote buying, (v) a complete audit trail for authorities and voters, (vi) prevention of sabotage and attempts to discredit the election. Figure 2 summarizes these dimensions defining a 4 point scale for each dimension (from within: (1) slight to no protection, (2) corruptible with medium determination, (3) high degree of protection, (4) virtually unbreakable). For each dimension, the model defines how far technical safeguards apply (the line joining the dimensions). Beyond this level, organizational safeguards may apply. However, it remains to be ascertained from case to case, whether organizational protection is viable.

Some of the above goals are in clear antinomy. An e-voting system, for example, designed to perfectly meet requirements (ii) to (vi) cannot technically guarantee voter anonymity (see Figure 2). In this case, organizational safeguards would have to be provided.

On the other hand a system, designed to meet the requirement of anonymity only (“naive anonymity”) would neglect the other goals and would have to provide purely organizational safe-guards (Figure 3).

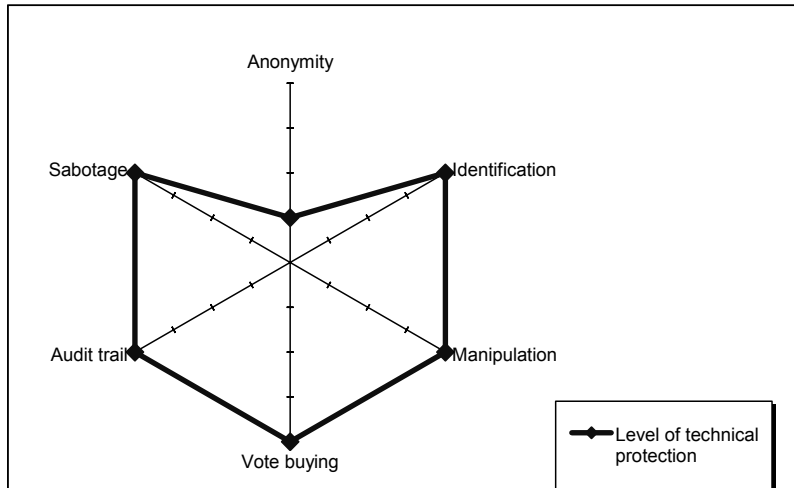


Figure 2: Fully auditable system, resistant against sabotage and manipulation

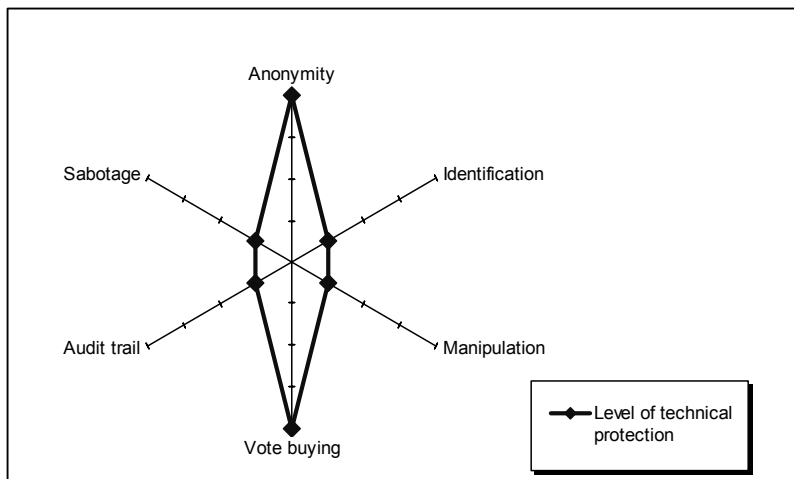


Figure 3: "Naively" anonymous system

The question arises, whether a voting protocol can be defined that combines technical safe-guards for voter anonymity as well as identification and reproducibility.

3 The Protocol of e-voting.at

The participating parties are (i) the voter, (ii) the registration authority maintaining the voter register, (iii) the electronic ballot box, (iv) a third party, such as a trust centre or the Privacy Protection Committee.

Registration:

1. The registrator has one signature key pair (e, d) per constituency c ; each trust centre participating in the election has its (ε, δ) .
2. The voter sends his voter ID to the registrator, which after checking the voter's eligibility answers with c and the appropriate e . The voter also polls the trust centre for ε .
3. The voter creates random tokens t and τ preparing them for a blind RSA signature $(b(t), b(\tau))$. c , $b(t)$ and a standard text applying for a signed e-voting token is sent to the registrator, which after checking the credentials again blindly signs and returns $d(b(t))$. The voter removes the blinding layer and obtains $d(t)$.
4. The voter obtains $\delta(\tau)$ in a similar way from the trust centre.

Storage:

The voter stores $t, d(t), \tau, \delta(\tau), c$ on a secure media (for the role of smart cards in e-voting, cf. [PKKU04]).

Voting:

1. Prior to the election, the members of the election committee form RSA key pairs (k, k') and make their respective encryption keys k' known to the ballot box server.
2. On election day, the voter sends $t, d(t), \tau, \delta(\tau), c$ to the ballot box server, which knows all relevant e and ε .
3. If the ballot box can authenticate the tokens for the constituency indicated and if they have not already been used, it returns an empty ballot sheet BS and the relevant k' .
4. The voter codes the filled-in BS with k' and untamperably links the tokens to this $k'(BS)$. The ballot box once again checks the tokens and stores the ballot.
5. The ballot box issues a receipt, which does not contain any information on the vote cast.

After the election finished, the members of the election committee reveal their secret decryption key k and the ballot sheets are decrypted. The above protocol as currently implemented does not enable majority decisions by the election committee, or enables the replacement of an election committee member who had an accident, lost his key, wants to sabotage the election etc. A solution for quorum-based decisions is provided in [PKKU04a].

4 Threats and Security

Let us analyze the security aspects identified in Figures 2 and 3:

Anonymity

Since the token is issued with a blind signature it cannot be traced back to the user. On election day, the voter uses the token as means of authentication only. The only means of intercepting the token and to corrupt anonymity is the voter's PC. This can be ruled out, if the decisive parts of the voting protocol (such as the resolution of the blind signature provided by the registration server) are performed in the secure environment of a smart card (eg., a signature card).

Identification

Authenticity can be provided by signing the application for a voting token using a digital signature card. If this is also a citizen card (in Austria cf. [HoKa04]), the voter can also be identified. Authenticity on election day is only provided by the voting token. If this token is not stored in the secure environment of a PIN protected area on a smart card, the token has to be password-protected.

Manipulation

Manipulation by a third party can happen in transmission or on the voter's PC. The former is prevented by standard encryption, such as SSL/TLS (IETF RFC 2246), the latter by again performing the decisive protocol elements in a secure and tamper-proof environment.

Manipulation by the administration can affect:

- (i) The issue of fake tokens, which is prevented by the second authority, whose token is needed to cast a vote as well.
- (ii) The manipulation of votes, which is prevented by encryption of the ballot sheet with the keys of the members of the election committee.
- (iii) The insertion of votes, which is prevented by the same mechanism as (i) and by the fact that the token is re-submitted and inextricably linked to the filled-in ballot sheet when it is submitted.
- (iv) The deletion of votes can be prevented when the tokens are published for which a vote was cast and voters are provided with a signed conformation by the ballot box server that a vote has been cast for this token.

Vote Buying

The voter is given a receipt without any reference to the actual vote cast. This would also be impossible, as the vote submitted to the ballot box server is coded with the election committee keys.

Audit Trail

The audit trail is two-fold corresponding to the two-stage protocol: (i) it is reproducible, which member of the electorate sent in a signed application to vote electronically and

whether she received a token; (ii) which token was sent in to obtain a ballot sheet and which vote was cast for the respective token. Of course, the link between (i) and (ii) is not reproducible; this is the essence of a two-stage protocol. (iii) Each signed application must contain a corresponding one from a second authority.

Sabotage

Since there is a complete audit trail, assertions of irregularities can be dealt with satisfactorily.

The protocol described in this paper has been implemented and used in two test elections parallel to the Student Union election in 2003 [PKK03] and the Austrian Federal Presidential election in 2004 [PKKU04b].

References

- [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, pp. 234-238
- [Chau82] Chaum, D.: Blind Signatures for Untraceable Payments in: Chaum, D., Rivest, R.L., Sherman A.T. (eds): Advances in Cryptology, Proceedings of Crypto 82, pp. 199-203
- [HoKa04] Hollosi, A., Karlinger, G.: Einführung in die österreichische Bürgerkarte; Bundeskanzleramt, Stabsstelle IKT-Strategie des Bundes, Technik und Standards, Vienna, 2004, <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html> (10.6.2004)
- [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)
- [FFW99] Feghhi, J., Feghhi, J., Williams, P.: Digital Certificates – Applied Internet Security; Addison-Wesley, Reading, 1999
- [NSS91] Nurmi, H., Salomaa, A., Santeau, L.: Secret ballot elections in computer networks; Computers and Security 36 (10), 1991, pp. 553-560
- [Phi02] Philippson M.: Internetwahlen – Demokratische Wahlen über das Internet; Informatik Spektrum 25(2) 2002, pp. 138-150
- [PKK03] Prosser, A., Kofler, R., Krimmer, R.: Deploying Electronic Democracy for Public Corporations. In: Traunmüller, R. (ed.): Electronic Government, LNCS 2739(2003), pp. 234-239
- [PKKU04] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Annual Hawaii International Conference on System Sciences (CD-ROM), Computer Society Press, 2004
- [PKKU04a] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: Implementation of Quorum-based Decisions in an Election Committee; to appear in Traunmüller, R. (ed.) E-Government; Lecture Notes in Computer Science, Springer, 2004
- [PKKU04b] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: e-Voting Wahltest zur Bundespräsidentenschaftswahl 2004, Arbeitsbericht zum Tätigkeitsfeld Wirtschaftsinformatik, Informationsverarbeitung und Informationswirtschaft 01/2004, Wirtschaftsuniversität Wien, 2004
- [PrMü01] Prosser, A., Müller-Török, R.: Electronic Voting via the Internet; Int. Conf. on Enterprise Information Systems ICEIS 2001, Setúbal, pp. 1061-1066
- [Rub04] Rubin, A.: Security Considerations for Remote Electronic Voting over the Internet <http://avirubin.com/e-voting.security.pdf> (23.5.2004)