# Multiple Casts in Online Voting: Analyzing Chances

Melanie Volkamer[1], Rüdiger Grimm[2]

[1]German Research Center for Artificial Intelligence (DFKI GmbH)
Stuhlsatzenhausweg 3
66123 Saarbrücken, Germany
volkamer@dfki.de

[2]Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz, Germany
grimm@uni-koblenz.de

**Abstract:** We analyze multiple casts as an easy and non-technical approach to overcome some of the open questions and risks of online voting. The mechanism of multiple casts can be added to almost all existing online voting systems. Nevertheless, there are also some disadvantages, for instance the validity of a timestamp, which are discussed in the paper as well.

## 1 Introduction

Multiple casts in online voting became popular by the Estonian's legal binding Local Government Council Election in autumn 2005. The voters had the possibility to cast several electronic ballots from different places and devices before the election day. Only the last one was counted. In addition, the voter could cast a paper ballot in the polling station on the election day. In case a voter cast a paper ballot, this paper ballot was counted and any of his electronic ballots was deleted. The Estonian government applied multiple casts in online voting to overcome the discussion about remote voting like voter coercion and ballot buying, because in Estonia postal voting is currently only allowed for citizens living abroad.

The Estonian approach caused a controversial discussion in the (e-)voting community. Nevertheless, multiple casts in online voting is not a new approach, it is not even specific for online voting. Multiple casts in voting are already applied in some countries, e.g. in most of the Scandinavian countries, in the traditional voting system to limit the risks of remote voting in general and to overcome the problem that remote voters are early voters and could not response to short-term political events otherwise. Other reasons are the transmission time and the missing receipt within postal voting. For

instance, in Sweden the voters have the possibility to cast their vote in the polling station even if they already applied remote voting (postal voting or voting in a post office). The ballot cast in the polling station is counted and the remote ballot is deleted. The disadvantage of the Swedish approach is the long period to count the postal ballots because the electoral staffs have first to verify whether the voter cast a ballot in the polling station. With paper ballots, this check cannot be done automatically but it would be possible within online voting.

Thus, some countries have already recognized the advantages of multiple casts in voting. Why do we not utilize these advantages for online voting in general? Is it possible? Are there any other advantages or disadvantages? Does it overcome existing problems and open questions of online voting? To get an answer to all these questions we analyze multiple casts in online voting. We start with an introduction of security requirements and threats to an online voting system in section 2 and identify the open problems specific for online voting in section 3. In section 4 we present different forms of multiple casts in online voting. The advantages will be discussed in section 5 and the disadvantages in section 6. Besides the disadvantages, we will explain in section 7 those mechanisms and techniques, which are necessary to apply multiple casts in online voting. In addition, we will analyze the application with the existing voting systems and approaches in section 8. Finally, we will conclude with a summery and a recommendation for the application of multiple casts in online voting.

## 2 Requirements and Threats of Online Voting Systems

The main principles of election laws are similar in all democracies. Democratic elections have to be at least *universal, equal, free* and *secret*. Starting from these basic principles, many researchers deduced technical requirements for an online voting system and organisational requirements for the application of online voting. The most popular system and protocol independent requirement catalogues are the Recommendations of the Council of Europe [CoE04] and the Catalogue of Requirements for "Online Voting Systems for Nonparliamentary Elections" of the Physikalisch-Technische Bundesanstalt [PTB04]. These are the main technical requirements to an online voting system:

Deduced from the *universal* principle the election system must ensure that no eligible voter is excluded from the election - $\mathbf{Req_u}$. This must also hold for any kind of server or client software breakdown as well as communication breakdown. In addition, no voter has the possibility to cast more than one ballot within such a break down (equal). To ensure the *equality* principle, no unauthorized person should be able to add, remove or alter votes undetected. This must hold during ballot casting - $\mathbf{Req_{e1}}$, ballot transmission - $\mathbf{Req_{e2}}$ and ballot storage - $\mathbf{Req_{e3}}$. The principle of *secret* elections demands that only the voter is aware of her voting decision. Nobody else is able to link the voter to her vote neither during nor after the election - $\mathbf{Req_{s1}}$. In addition, voters must be unable to prove their voting decisions - $\mathbf{Req_{s2}}$. There are two more requirements, which are less technical but more general. The principle of free elections requires that voters cast their ballot free of duress and without influence - $\mathbf{Req_f}$. In addition, the principle of equal elections requires that all voters can cast their ballots in the same way - $\mathbf{Req_{e4}}$.

An attacker has four attacking points either in order to *break the ballot secrecy* (violation of the secret and free election principle) or to *manipulate the election result* (violation of the equal, free and universal election principle):

***Observing a voter casting her ballot*** - The attacker could be next to the voter casting her ballot in order to observe the voters choice or to coerce her to vote in a specific way (e.g. imaginable in an old people's home) - $\mathbf{Threat_O}$. This is not an online voting specific attack but one for any remote voting system because the electoral office cannot ensure that voters cast their ballots in a free and secret environment. This is why postal voting is not allowed in many countries, and in some countries only as an exception.

***Manipulation of the voters' voting device*** - The attacker could also program malicious code and try to install it on the voter's PC. This code could read the voter's ID, and vote on his behalf - $\mathbf{Threat_{D1}}$, or change the voter's choice before sending it to the electoral server - $\mathbf{Threat_{D2}}$. Moreover, attacking the voter's PC is much more critical than the observation attack from above because now it is possible to manipulate or read several votes automatically. Of course, this attacker needed technical expertise.

***Manipulation or sniffing on the communication layer*** - The Internet is a public network so we cannot prevent an attacker to read or manipulate the connection between the voter and the electoral servers. The attacker can try to manipulate the election result by changing, adding or deleting ballot messages on the network - $\mathbf{Threat_M}$. He can also read and store messages in order to evaluate them - $\mathbf{Threat_S}$. The attacker could wait until someone will find a fast algorithm or faster PCs to decrypt the stored messages.

***Manipulation of the election servers*** - The election servers store beside other data both information, the voters' IDs and their votes. Thus, an attacker could try to get access to the election servers in order to get the corresponding data - $\mathbf{Threat_{E1}}$. He could also try to manipulate the servers - $\mathbf{Threat_{E2}}$.

| | $\mathbf{Req_u}$ | $\mathbf{Req_{e1}}$ | $\mathbf{Req_{e2}}$ | $\mathbf{Req_{e3}}$ | $\mathbf{Req_{s1}}$ | $\mathbf{Req_{s2}}$ | $\mathbf{Req_f}$ |
|---|---|---|---|---|---|---|---|
| $\mathbf{Threat_O}$ | | | | | x | x | x |
| $\mathbf{Threat_{D1}}$ | | | | | x | x | x |
| $\mathbf{Threat_{D2}}$ | x | x | | | | | |
| $\mathbf{Threat_M}$ | | | x | | | | |
| $\mathbf{Threat_S}$ | | | | | x | x | x |
| $\mathbf{Threat_{ES1}}$ | | | | | x | x | x |
| $\mathbf{Threat_{ES2}}$ | | | | x | | | |

Figure 1: Comparison Requirements - Threats

The table in Figure 1 illustrates which threat violates which security requirement.

## 3 Open Problems

Many different approaches exist to overcome the threats above and to meet the identified requirements. For an overview over different approaches, see e.g. [Lip05, Sch00]. Most requirements are fulfilled by the existing online voting systems but some unsolved

problems exist nevertheless. Some open problems can be identified by **deduction from the identified threats**. Others stem from **functional requirements**, and from **voting in advance**. These are discussed in the following.

***Problems deduced from the identified threats:*** Obviously, a remote online voting system does not overcome the observation problem - $\mathbf{Threat_O}$. As long as there is no technical or organizational approach to overcome this basic problem remote online voting will only be applied in parallel to postal voting - at least for important elections like parliamentary ones. The main technical challenge, which has not been solved yet, is the malicious code on the voter's PC - $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. There are some approaches like the assistance guidelines for the voters within the elections of the Gesellschaft für Informatik [Gi05], and the theoretical approach of Fischer and Zuser [FiZu05] where the voter does not enter the original vote but a scrambled one. The disadvantages of the existing approaches are organizational assumptions and usability. Thus, a convincing solution to this problem is still missing. Another unsolved problem is the temporary unlimited election secrecy against attackers sniffing on the internet - $\mathbf{Threat_S}$. In [VoKr06] the authors illustrate that the election secrecy is only ensured under corresponding cryptographic assumptions. However, if someone finds a fast algorithm or if he has enough computational power he will be able to link each voter to her vote. The only possibility known so far to enforce theoretical information security with respect to the election secrecy and with respect to attacker sniffing on the Internet is the application of a One-Time-Pad. However, this implies a very high organizational investment.

***Other open problems:*** One main problem in the context of online voting is to ensure that the voter can cast one and only one vote even when her local system, the communication system or the servers break down at any arbitrary step. This is a very important **functional requirement** in the context of online voting. It is hard to ensure this requirement because arbitrary things can happen, e.g. programming errors or an interruption of power supply or communication breakdowns. Another problem with respect to remote and especially postal voting is the **voting in advance**. In traditional postal voting without multiple casts, once the voter has cast her ballot, she cannot change her mind again for any reason, even if political events would cause her to do so. With online voting it is less a problem than within postal voting because the transmission time is much shorter. However, online voting would have problems to guarantee availability if everyone would cast the e-ballot on the Election Day, especially in the last few minutes before closing the election.

## 4 Forms of Multiple Casts in Online Voting

There are several possibilities to apply multiple casts in online voting which look similar on the first view. But from the organizational point of view they use different methods to ensure that multiple casts are counted only once even if voters use different channels: online voting, postal voting, and traditional voting in the polling station.

*(a)* The easiest form is to allow online voting exclusively, whereby voters can cast as many e-ballots as they want. *(b)*Within the second form, voters have to decide before the

election whether they want to use online voting or not. Here, a voter receives either a postal voting ballot or the electronic authentication tokens to access the online voting system. Thus, two different electoral registers exists: one for the traditional paper ballot voters and one for the e-voters. The e-voters can cast as many e-votes as they want and only the last one is counted. By doing so, it can be ensured easily that either an e-ballot or a paper ballot is counted.

*(c)* In the third variant, voters have the possibility to decide during the election time whether they want to apply online voting or not. After having cast an e-ballot the voter cannot cast a paper ballot anymore. But, she can cast as many e-ballots as she wants and the last one is counted. The possibility to apply online voting stops before the Election Day. An election register is printed for the Election Day, which lists all voters who did not cast an e-ballot. Listed voters are excluded from paper voting in the polling station. In addition, depending on the priority, either the e-ballot or the postal ballot has to be deleted to ensure that only one ballot per voter is counted. *(d)* Another possible form of multiple casts in online voting is an extension of (c). We allow voters to cast e-ballots also on the Election Day as long as they have not cast a paper ballot in the polling station. In this case, there is only one electoral register and we have to find a way to delete the e-ballots and/or the postal ballot. A more complicated form would be the following variant (d'): The voter can cast as many e-ballots as she wants, especially also on the Election Day and even *after* having cast a paper ballot. Here, the most favourite form of ballot casting (paper or e-ballot) has to be set up before the election, either uniformly for all voters, or even individually for every voter. For the calculation of the result, it must be possible to remove either the e-ballot or the paper ballot if someone cast ballots using both channels. In all cases it is important to delete the ballots without breaking or endangering the anonymity. Figure 2 illustrates the state machine of the described possibilities.

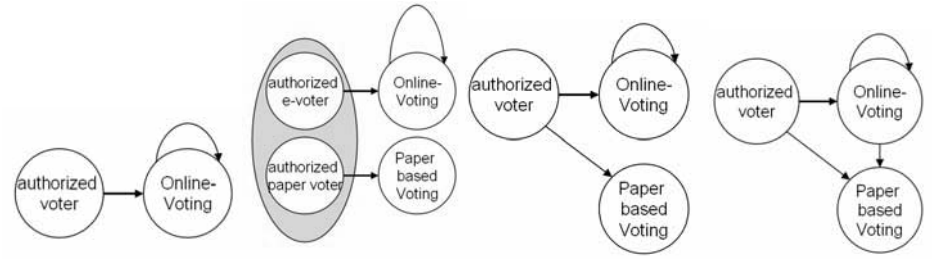


Figure 2: Forms of multiple casts in online voting

## 5 Advantages of Multiple Casts in Online Voting

Multiple casts in online voting provide a technical approach to overcome some of the open question especially the basic problems with respect to remote voting. The following advantages hold for all forms of multiple casts in online voting described above. First of all the principle of a free and secret ballot casting can be ensured also in the private sector - $\mathbf{Threat_O}$. Of course, an attacker can still observe and force the voter

to cast a ballot but the voter has the possibility to cast later on another ballot and to make another choice. So, it gets unattractive for an attacker to visit people in order to force them to cast a ballot. This is also true in old people's home because the attacker does not know whether someone else will go later on to the same old people's home and manipulate the voters to make another choice. Moreover, any voter who would like to change an unwanted vote could do so at any time. For the same reason, ballot buying gets unattractive[1].

Multiple casts in online voting can also be seen as an easy mechanism to ensure temporary unlimited election secrecy against an attacker sniffing on the Internet and trying to link identified voters to their votes after the election - $\mathbf{Threat_S}$. Strictly speaking, sniffing on the Internet becomes pointless for an attacker because in general he cannot know whether the last and counted ballot of a specific voter is in his memory of sniffed messages or not. The voter could have sent another ballot from another device and thereby over another path - a path on which the attacker is not sniffing. The sniffed encrypted ballots sent over the network become even less meaningful if the voting system allows an e-voter to substitute her e-ballot by a paper one - ***form (d)***. In the multiple casts form (d) an attacker can neither use the sniffed messages to break the election secrecy nor prove to someone else that the sniffed ballots represent valid votes of identified voters. Thus, the application of multiple casts in online voting makes the effort of sniffing and breaking encrypted ballots useless because attackers only get the counted ballots with a certain degree of (unknown) probability. Moreover they cannot use their knowledge to proof it to others.

Another advantage refers to manipulation attacks. When a voter would find out that she has malicious code on her PC during the election time, she is allowed to cast another ballot from an arbitrary PC or from special secure voting terminals or even on paper – $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. With multiple cast, manipulation attacks are only meaning full with respect to result manipulation. The information from the malicious code cannot be used to break the election secrecy because the voter could cast later on another ballot from another device.

There exist two more advantages of multiple cast in online voting. First, the **mal functionality problem** with respect to system or communication breakdowns can be mitigated. If a voter does not receive a receipt at the end of the voting protocol because some problems arose, there is no reason to worry, because the voter can restart the PC, the software and/or the communication and cast her ballot again to get the receipt and to be sure that the ballot is counted. Second, multiple casts in online voting would also overcome the **voting in advanced problem**. A voter can change her ballot at any time at least until the Election Day if some political events happen or the voter has other reasons to change her mind.

[1] This is only true, it the system does not have a receipt mechanism with a zero-knowledge proof. The proof would change for a resubmitted vote and thus the coercer or vote-buyer would notice the resubmission. This does also hold for the temporary unlimited election secrecy in the next paragraph.

## 6 Disadvantages of Multiple Casts in Online Voting

This new type of voting system with multiple casts does not only have advantages but also some disadvantages. The disadvantages are not specific for online voting in general but for multiple casts in online voting. The main issue of concern refers to the requirement $\mathbf{Req_{e4}}$ that all voters must have the same chances to cast the ballot. *Form (a)* of multiple casts in online voting fulfils this requirement because only online voting is allowed. However, this form can only be applied if every voter has the possibility to cast a ballot (otherwise the universal election principle would be violated). The other proposed forms of multiple casts in online voting - *(b)-(d)* - do not comply with requirement $\mathbf{Req_{e4}}$. Here, the e-voters have the possibility to cast several votes and change their decision while people who are not able or do not have a PC and thus must apply the paper-based election, have only the possibility to cast one ballot. This is especially problematic with respect to the postal voters because they have to cast their vote some days in advance. Moreover, e-voters can get a receipt about the storage of their vote in the electronic ballot box but postal voters do not receive such a receipt. They are discriminated compared to the e-voters with respect to the equality principle.

Currently, at the end of the election most of the systems provide a consistency check. They compare the number of announced voters in the electronic voters register who finished their voting process with the number of votes stored in the ballot box server. This check helps to increase the trust in the system. With multiple casts in online voting, this check is much less meaningful. The voter could announce the vote several times to the electronic electoral register, which would label the voter after the first completed voting process. So, we do not get any statement about the multiple votes cast later on. This unveils another disadvantage of all forms of multiple casts in online voting: It is difficult to verify whether the one vote which is counted is indeed the vote the voter wants to be counted.

Some more disadvantages refer to social aspects: with multiple casts in online voting, we run the risk to loose the seriousness and the value of elections. It becomes similar to a game or some silly polls in the Internet or on TV. Closely related to this is the problem that some critical or unconfident voters could be unsettled which of their votes is actually counted. In addition, with multiple casts in online voting there might arise confusion with election forecasts. While in practise election forecasts are an important part of the election, they must be clearly separated from them.

## 7 Additional Mechanisms and Techniques

The existing systems have to be extended in order to apply multiple casts in online voting. Several auxiliary mechanisms are necessary and some new techniques have to be developed or have to be taken over from other applications. For example, it has to be ensured that the last cast ballot is the one that is stored and not e.g. the last ballot received at the ballot box. A challenging problem is the deletion of obsolescent ballots. The related function must either delete the e-ballots or destroy the paper ballots in order to allow multiple channel voting as described as ***forms (b), (c)*** and ***(d)***. Another important mechanism is the *timestamp* mechanism for the ballot messages. This becomes

necessary because multiple casts open the door to a new form of replay attacks. An attacker could send an older ballot again in order to manipulate the result. Reliable timestamps can only be provided by a trusted timeserver. The clock of the voter's PC would not suffice, because it is easy to manipulate it. Using the incoming time of a ballot at the ballot box server does not work either, because the ballot message could be withheld by an attacker and forwarded later. Thus, we need a possibility to uniquely assign a ballot message to the time when it was really cast by the voter.

The possibility to cast multiple ballots has to be integrated in the online voting system. There are two possibilities to implement this function. Either the voter's right to vote is checked in the electoral register each time she wants to cast a ballot or it is only verified the first time. In the latter case, the voter would receive an anonymous authentication token, which she uses each time she wants to cast a ballot during the election. Here, the voter needs to have a secure portable memory to store this token. Otherwise, she does not have the possibility to cast the ballot from arbitrary PCs. This could be a smart card, for instance. The problem is that the voter is excluded from casting ballots if this memory gets lost, stolen, or broken. In addition, high security requirements like integrity and confidentiality have to be ensured by the chosen memory otherwise the token could be read out. Therefore, the cheaper, easier and more user-friendly way is the first form: to run through the whole voting process each time again. This mechanism has to be implemented in all proposed forms of multiple casts in online voting.

In some forms of multiple casts in online voting, we have to integrate an additional and very critical mechanism. In ***forms (c)*** and ***(d)*** where the voter can cast both e-ballots and paper ballots the functionality to remove either the paper ballots or the e-ballots has to be implemented. There must be a link either between the e-ballot and the voter or between the paper ballot and the voter, or the voter must be able to remove one of them. This link must be possible without the violation of the secrecy principle (unlinkability forever). At least for the paper ballot election in the polling station the introduction of a link between voter and ballot would downgrade the anonymity compared to the traditional elections in the polling station. In particular for the e-ballots a technical solution must exist which does not violate the election secrecy. There must be a technical means to find the old e-ballot of the voter in the electronic ballot box in order to delete it and to store the new one. A possible solution is provided in [VoRV06].

In addition, the algorithm to replace the old ballot of a specific voter in the electronic ballot box by a new one must be fast. If the algorithm is too slow, the voter has to wait undue until she receives a receipt. ***form (d)*** of multiple casts in online voting requires two additional mechanisms: After the voter cast a paper ballot, the e-ballot has to be deleted and it must be ensured that the voter cannot cast an authorized e-ballot later on. Another mechanism should be implemented in each multiple cast form for online voting: *the wilful abstention from voting after having cast e-ballots*. This means: a voter who has already cast an e-ballot should be able to decide explicitly not to vote at all and thus her already cast ballot to be deleted and not counted. Thereby two things must be done: The ballot has to be secured in the ballot box and a corresponding flag in the voters' register has to be set.

## 8 Realization of Multiple Cast in Online Voting

There are three types of online voting approaches to overcome the anonymity problem: (1) preliminary voter authentication with subsequent anonymous tokens or pseudonyms, (2) blind signatures and (3) homomorphic encryption. In this chapter, we have a closer look whether multiple casts in online voting can be applied to all of these approaches and which are the respective protocol extensions or new assumptions.

Preliminary voter authentication means, that first the voter sends a request with personal data to the electoral register. This register generates an anonymous token and sends it back to the voter. Second, the voter sends her ballot together with the token to the electronic ballot box. The authentication of the cast ballot is checked by the eligibility of the token. Here it is quite easy to apply multiple casts in online voting because the electoral register just sends the same random token to the voter when she wants to announce a new vote. The ballot box can identify all ballots from one voter by the anonymous token. The difference to the implementation now is that the tokens cannot be deleted after having completed one voting procedure because they are needed for the multiple votes as well. Thus, the anonymity is more endangered and thus the servers have to be better protected. Another variant of preliminary voter authentication is pseudonymous voting. Here the application of multiple casts would be easier with less danger for the anonymity. But, generally, pseudonyms are harder to administrate.

Voting protocols with blind signature are based on Chaum's blind signature algorithm. Blind signatures allow to sign a vote or other data without revealing the content. There are two possibilities to apply this technology to voting protocols: firstly, the voters register blinds the ballot; alternatively, the voters register signs a blinded random token chosen by the voter. The latter one works perfectly with multiple casts in online voting. The random token is sent together with the ballot. Thus, the token can be used to identify all votes from one voter. The first approach to let the voters register blindly sign ballots does also work: currently the voter receives blinded ballots from the voters register for all possible choices. At present, the voter can only choose one of it and send it to the ballot box. With the same mechanism the ballot box now verifies that the voter only sends one of the signed ballots, the ballot box can identify the old ballot of a voter to remove this with the new one in multiple casts in online voting. Here, the application of multiple casts in online voting provides the same anonymity as online voting without multiple casts.

Voting protocols based on homomorphic encryption can also be extended quite easily because the link between an encrypted ballot and the voter is given and can even be proved. Thus, it is easy to replace an old ballot by a new one on the so-called bulletin board.

## 9 Conclusion

We have illustrated these open problems of online voting: observation within remote voting, manipulation of the voter's PC, the temporary unlimited election secrecy against sniffing on the network, the mal functionality with respect to system and communication breakdowns, and the voting in advance problems. Multiple casts in online voting overcomes some of these problems, namely obviously the remote problem, the voting in advance and the mal functionality problem. The manipulation of the PC is still a possibility for the attacker to manipulate the election result but not to break the election secrecy.

Beyond technology and organizational issues, we should also consider the voters themselves. Security increases only if the voters take the opportunity to cast several votes. Indeed, most of the voters will not do so. In Estonia, they counted 364 of 9681 repeated e-ballots and 30 of them cancelled e-ballots by casting a paper ballot on the Election Day. Therefore, it might be a nice, technically easy but only theoretical solution, which does not overcome the problems in practice. We should also take into account that changing electoral laws in order to allow online voting is not easy in general but it will be harder to allow multiple casts in online voting because multiple casts in voting is not in use in most of the countries. Moreover, there are also disadvantages like the integration of a trusted timeserver, the violation of the equal election with some forms of multiple casts in online voting, and the new mechanisms, which might be critical with respect to the election secrecy. We have identified some open research questions in this context, which have to be solved first.

## References


[CoE04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation rec(2004)11 adopted by the committee of ministers of the council of europe and explanatory memorandum. Council of Europe, Straburg, 2004.

[FiZu05] Gerald Fischer and Wolfgang Zuser. The Vote Scrambling Algorithm. Schweighofer E., Augeneder, S., Liebwald, D., Menzel, T. - Boorbergverlag, 2005.

[Gi05] GI Gesellschaft f¨ur Informatik e.V. Election 2005 Assistance guidlines. http://www.gi-ev.de/wahlen2005/ retrieved on 15-2-2006, 2005.

[Lip05] Helger Lipmaa. Electronic voting. http://www.cs.ut.ee/ lipmaa/crypto/link/protocols/voting.php retrieved on 15-2-2005.

[PTB04] Physikalisch-Technische Bundesanstalt Braunscheig PTB and Berlin. Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements. http://www.berlin.ptb.de/8/85/LB8 5 2004 1AnfKat.pdf retrieved on 15-2-2005, 8.5.2004.

[Sch00] Schlifni M. Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democrac. Dissertation Technische Universität Wien, 2000.

[VoKr06] Melanie Volkamer and Robert Krimmer. Secrecy forever? analysis of anonymity in internet-based voting protocols. In (not yet publish conference in April 2006), editor, The First International Conference on Availability, Reliability and Security; The International Dependability Conference Bridging Theory and Practice, 2006.

[VoRV05] Melanie Volkamer, Walter Reinhard, and Roland Vogt. Fuse - ein Internetwahlsystem für zeitlich unbegrenzte geheime Betriebsratswahlen. Sicherheit 2006 ”Sicherheit - Schutz und Zuverlässigkeit”, 22 February 2006.