Vote casting device with VV-SV-PAT for elections with complicated ballot papers

Melanie Volkamer, Jurlind Budurushi, Denise Demirel
SecUSo - Security, Usability and Society
Center for Advanced Security Research Darmstadt \ Technische Universität Darmstadt
Darmstadt, Germany
Email: Name.Surname@cased.de

***Abstract*—Some ballots such as those for local elections in Germany contain more than 500 candidates, allow for more than 70 votes and the system allows voters to perform cumulative voting, vote splitting and crossing out of candidates which results in huge ballot papers containing only one race. As none of the existing electronic voting systems seem to be feasible for this kind of election we propose a new approach in this paper. The main idea is to have a vote casting device that does not store votes but only prints a summary of the selection voters made at device. This printout is put into the ballot box. In addition, to the human readable summary, the so called Voter Verifiable Summary of the Vote Paper Audit Trail (VV-SV-PAT) contains a 2D barcode which makes it easier to properly enter votes into the counting software. In addition, we propose an improvement for the counting software. With this approach we aim to support the actual procedure of vote casting and tallying by an accurate use of technology while at the same time preserving, or even improving, verifiability and usability compared to the traditional system.**

***Keywords*-electronic voting, paper audit trail, verifiability**

I. Introduction

Elections vary greatly from country to country, but also within each country for different types of elections. Some have very simple ballots with two candidates or just a yes or no question, while other ballots like for local elections in Germany contain more than 500 candidates, allow for more than 70 votes and the system also allows voters to perform cumulative voting, vote splitting and crossing out of candidates which results in huge ballot papers (in Darmstadt in 2006 local elections about 27" x 35"). Manually tallying is very likely to be error prone and time intensive. The tallying for the local elections in Germany usually takes between four to six days. They have computer support for the counting and tallying where they enter vote by vote. Also vote casting is error prone as voters might accidently and without realizing spoil the vote. Consequently, electronic support could dramatically improve the situation for both voters and poll workers.

There exist many different types of electronic voting schemes and electronic voting systems in use. Some are for use in polling stations and still paper-based, such as punch card and optical scan systems. Other systems use voting machines such as mechanical lever machines or direct recording electronic voting machines (DREs) in the polling booth. Furthermore, there is the development of remote electronic voting protocols and systems. However, in a previous report [1], we show that neither one of the proposed voting protocols or schemes nor those electronic voting systems in use seems to be feasible for this kind of election, with highly complex and large ballot papers that have just one race on it.

The goal of this paper is to propose a concept for an electronic voting system that is feasible for elections with such large and complicated ballot papers. The main idea is to use vote casting devices instead of DREs which do not store votes but just print special voter verifiable paper audit trails (VVPATs), namely so called Voter Verifiable Summary of the Vote Paper Audit Trails (VV-SV-PATs) on a simple DIN-A4/letter format piece of paper. The summary of the vote contains the interpretation of the selections made on the vote casting device. Thus, it supports both the vote casting and the counting process. This approach is further improved by printing a 2D barcode on the VV-SV-PAT in order to simplify the counting process and by using a second monitor for the counting process in order to increase the transparency of the counting procedure.

We do not claim to provide an approach that is perfectly secure. While our approach provides a much higher level of verifiability and accuracy than the traditional paper based elections, both for vote casting and tallying, it does not yet fully solve the secrecy challenge that DREs have in common. A malicious DRE could track the order and time of cast votes while this information is later combined with the information of which voter casts his vote at which time. However, we believe that it is possible to find an adequate solution. In addition, the proposed scheme is not based on heavy cryptography which makes it easier for the public to understand and thus to trust this particular type of electronic voting system.

The structure of this paper is as follows. We first explain in Section II the local election in Hesse, Germany, and show its scale based on data from the 2006 election. We then show in the related work section (Section III) that existing voting schemes and systems are not applicable for elections like the local ones in Hesse. Section IV sketches the interface of the vote casting device. Afterwards, in Section V, we propose our own approach to adopt the vote casting device with a

This work has been published in the International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE), 2011. ISBN 978-1-4577-0951-7 DOI: http://dx.doi.org/10.1109/REVOTE.2011.6045910

Voter Verifiable Summary of the Vote on a Paper Audit Trail including a 2D barcode and how to use it to improve the tallying procedure. In Section VI we conduct a brief security and usability analysis of the proposed approach and compare it with the traditional paper based voting system. Finally, in Section VII, we conclude with suggestions for future work to further improve the proposed voting system.

II. Local elections in Hesse

The local election in Darmstadt, Hesse, combines the elections for the administrative body of towns, municipal and districts and is held for all citizens of one district at the same time. The ballot paper consists of several parties, identifiable by their name, abbreviation and number. Each party consists of several candidates, listed by their full name, an individual number (unique for a particular election), and the district he is living in. The candidates' names are ranked in a particular order specified by their party. The number of available seats determines the maximum number of candidates each party can nominate. Next to each party, there is one ballot checkbox to record the voter's preference while next to each candidate, there are three checkboxes (compare to Figure 1).

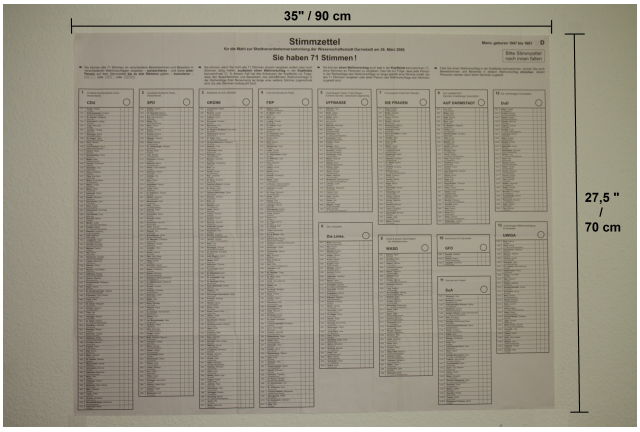

Figure 1. Ballot paper used in German local election

Before the polling station opens for vote casting, the ballot box is opened and the election authority and every voter can check that it is empty. Afterwards, the box is locked and is not permitted to be opened before the polling station closes.

Voters can select at most as many candidates as the number of available seats. Vote splitting, cumulative voting and crossing out of candidates is allowed. Correspondingly, voters have the following options to cast a valid vote:

1) They select n *candidates* while $n \leq$ number of seats. The voters can split their vote by casting votes for candidates of several parties on one ballot sheet. Cumulative voting is provided such that a voter can cast up to three votes for one candidate.
2) They select *one party* and may or may not cross out single candidates. In this case, the votes are distributed to candidates of this party during the counting process according to predefined rules while the order of the candidates on the ballot paper is very important. In this sequence, skipping those that are crossed out, the candidates each get a vote until the maximum number of votes is used or every candidate has three votes.
3) They select n *candidates and party* X while $n <$ number of seats and the selected candidates do not belong to party X. In this case, all remaining votes (the maximum number of votes minus number of votes cast for several candidates) will be distributed to all candidates of the party.[1]

Spoilt votes include breaking one of the three rules above as well as those with additional marks, writings, or paintings on it as well as empty ballots. The ballots are folded in the polling booth before being put into the ballot box outside the polling booth.

The tallying takes place partially in the polling station and partially at central venues which are open to the public, with every citizen having the right to observe the process. In the polling station, the poll workers only manually tally ballot papers where the voter cast his vote for only one party. All remaining ballot papers are taken to the state office and apportioned to several groups of three people who count these ballot papers using software. During this process one poll worker reads the markings aloud while another enters them in the software. This can be done by entering the position of the marked candidate or party or click on the associated entry on the displayed ballot. A third poll worker observes and controls the whole process. Every ballot paper is marked with the number of the associated digital ballot which offers the possibility to audit the correct transfer afterwards. Finally the election result of the digital ballot papers is counted automatically by the system. Both this result as well as the manually counted one is entered in a second software to tally the election outcome. The voting system is a party proportional one.

These decentralized results are reported to a central authority responsible for the whole state. Although the counting and tallying is (partially) computer supported, the definitive result is usually not known until after four days. To get an overview and a better understanding of the election, Table I provides some numbers from the local election of the city of Darmstadt in 2006.

III. Related Work

In this section we summarize the results of [1] showing that existing approaches seem not to be feasible for this type of election. Note, already in [1] we concentrate on electronic voting systems implemented for polling stations as these systems do not force a radical departure from the vote

[1]If $n =$ number of votes then the selection of party X will be ignored. If votes are assigned to candidates of party X then at least these votes are assigned to the selected candidates of party X.

Table I
LOCAL ELECTION OF DARMSTADT, HESSE, IN 2006 [2]

Number of cast votes	2,898,159
Number of invalid votes	1,383
Number of voters cast a vote	44,385
Number of eligible voters	101,666
Size of the ballot paper	90 cm x 70 cm / 35 " x 27½ "
Number of candidates	502 in 13 lists
Number of votes to cast	71

casting process that the voter is used to, and do not go along with new challenges of casting votes in private environments instead of in protected ones in the polling stations.

All systems which, in the current version, only offer homomorphic tallying, such as ThreeBallot [3], Scratch and Vote [4] and Bingo Voting [5] cannot be used because the context of the whole ballot paper has to be evaluated in the counting process to interpret each vote properly. The use of electronic voting systems like Prêt à Voter [6] and Scantegrity II [7], which offer the voter the possibility to verify the digital ballot by cryptographic means, have disadvantages regarding their usability. To print the candidate list with 500 candidates in arbitrary order, which is necessary for Prêt à Voter, and ask the voters to find their 71 candidates in this list makes it impossible to use such a system. Also Scantegrity II which offers the voter the possibility to note down confirmation codes for all marked candidates and parties is impractical for an election with 71 votes per voter. Scanning solutions are not feasible as it is very difficult to scan these huge paper ballots properly and the required scanner is very expensive while it can only be used for anything else than elections. Another solution is the Digital Voting Pen / DotVote system [8] which provides Voter Verifiable Paper Audit Trails by design. Besides a couple of smaller problems, the Digital Voting Pen is not feasible for the elections for the same reason as DREs with VVPATs namely because of the low level of verifiability and transparency (see also Subsection V-A for a more detailed explanation).

IV. INTERFACE FOR VOTE CASTING

Proposing electronic vote casting for such huge ballot papers results in interface challenges. There are two possibilities to 'get' the ballot on the screen by using either a very large screen that is able to show the whole ballot at once in the same format (as it was implemented when using the Nedap DREs) or an average monitor from office equipment (let's say 19"). While the first proposal requires dedicated and very expensive monitors, the second one may allow the usage of office monitors and even when buying new ones, these will be cheaper than the huge ones. In addition, the smaller ones are more flexible as the ballot might be larger or smaller for future elections if more parties apply or more parties propose the maximum number of candidates allowed to propose. Therefore, our proposal is to be based on an average office monitor of the size of 19"[2].

The interface has to be designed in a way that allows voters to make their selections as easy as in the traditional system. Computers other than papers provide additional possibilities to support voters which we propose to use: providing the interpretation of the ballot, changing font size, informing about invalid votes, audio support for blind people, undo and search functions. We currently distinguish between the following different interfaces and the corresponding process diagram is illustrated in Figure 2:

- a welcome page with some instructions similar to the one on the ballot paper.
- the main page where voters get the following information and possibilities to continue:
  - information that x out of y votes have been assigned and using which method(s). "x out of y votes" will be replace by "spoiled" with a corresponding explanation why it is spoilt;
  - names and shortcuts of all parties;
  - option to either select the party or candidates;
  - option to spoil the vote (invalid or empty ballot);
  - option to review the ballot;
  - option to search for canidates;
  - link to further information and help.
- the party list page where voters can assign votes to candidates or cross candidates out and where they can also select the party. It is possible to save this assignment or to reset it.
- the search page where voters can search for candidate's name, number, party, and district while party and districts are pull down menus. The search result is a list of candidates (including name, number, party, and district) that matches together with three checkboxes. There is also a button "cross out" assigned to each candidates. The voter can either save his selection or rest and go back to the main page. On this page the information " x out of y votes" is also displayed.
- the preview page that displays the summary of the voter's selection. This can either be accepted or modified by the voter.
- the confirmation page which displays again the summary of the vote and asks the voter to confirm. After the confirmation, the device is disabled and needs to be enabled by the poll workers before the next voter can start the vote casting process.

This is work in progress as the interfaces currently only exist on paper and are undertaking small usability tests to further improve it. While we focus on these huge ballot papers, we also have other types of elections in mind. For instance in Germany, the same device should also be feasable

[2]We also propose to turn the screen by 90 degree in order to get a similar shape to the printed paper audit trail.

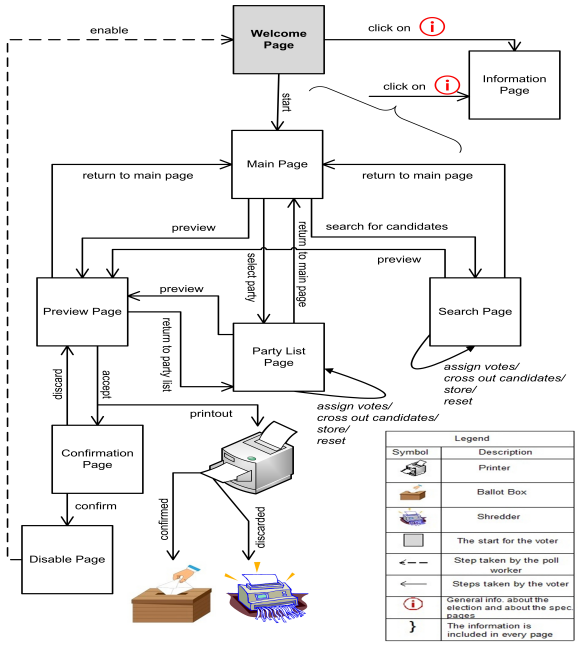

Figure 2. Process diagram

for other types of elections including the federal election with two races, one vote per race and usually less than twenty options per race.

V. Proposed Electronic Voting Solution

While the last section addresses the interface design to maximize the user support and in particular to decrease the likelihood that voters spoil a vote accidently and without realizing it, we propose in this section several extensions to the vote casting and tallying process to increase the level of verifiability while decreasing the vulnerability against privacy threats compared to common DREs.

A. Vote Casting Device instead of DRE

The general idea of a DRE would be that it stores the votes (hopefully in a random manner without timestamps) and at the end of the Election Day, the DRE tallies the votes and outputs the result. As this demands not only full trust in the device regarding the secrecy of the vote but also regarding the integrity of the election outcome, more and more DREs are equipped with so called Voter Verifiable Paper Audit Trails (VVPATs). The idea is that the DRE prints out the vote for the voter, the voter can check whether this contains his vote. Then, he confirms the vote at the DRE and puts the paper vote in the ballot box. Now, the DRE still outputs the result while in case of serious complaints it is possible to manually tally the votes. Even if this approach is used in some districts in the U.S. it decreases the level of verifiability compared to the traditional paper based system and would probably not comply with the public nature of elections required in the German constitutional court decision [9]. Therefore, at least for German elections, is seems to be plausible to require the tallying of all paper ballots before announcing the final and legal binding election result.

Therefore, we propose a device that does not outputs the result, and, correspondingly, does not store votes while it is only used to cast and print a vote. Therefore, we call the device not DRE any longer but vote casting device (VCD). This approach also increases the level of privacy as it is easier to ensure that the device does not record the order or time of cast votes.

In our approach, it is possible that the voter prints more than one paper ballot before he finally confirms. By doing so, even a manipulated device cannot break the secrecy of the vote as it does not know which one is put into the ballot box. This will probably be restricted to a number of print outs and then temporarily disabled. The VCD needs to be reenabled for a voter who printed more than the allowed number of votes before the voter can continue (enabling like it is required for every new voter). It might also be necessary to announce to the poll workers how many votes have been printed to make sure that the remaining ones (those that have not been put in the ballot box) are destroyed in order to ensure that a voter does not put two or more ballot papers in the ballot box. Note, the detailed process description is left for future work and it needs to be carefully designed to avoid accidental mistakes and to make it easy for voters and poll workers to properly follow the process.

B. VV-SV-PAT - Simple Version

A vote casting device will hardly be feasible to printout a VVPAT in the size of the original ballot as this would be too expensive and impractical. Reducing fonts to print it on an average Din-A4/letter size paper would not be readable anymore. Therefore, our proposal is to only print out the summary or the interpretation of the vote which we call Voter Verifiable Summary of the Vote Paper Audit Trail (VV-SV-PAT). The summary or interpretation must be represented in a way that from the printing sound it cannot be deduced whether someone spoiled a vote because this is just one line or seventy single candidates. Currently, we define a corresponding summary for all possible combinations of vote assignments in a way that no information about the content of the vote will be leaked by printing it. Note, the printed ballot paper is not individualized but looks the same when different voters make the same selections. The summary will also be displayed to the voter on the screen before he confirms and the corresponding paper trail will be printed. In addition, the challenge is to design the summary in a way that it is understandable for the voter.

Tallying the VV-SV-PAT is more efficient and less error prone than the tallying of the huge ballots in the traditional system. First of all, the ballot does not need to be unfolded several times but only once. Further, the whole huge ballot

does not need to be examined for marks or figures while only the information shown on the DIN-A4/letter paper needs to be entered to the software. This VV-SV-PAT makes it also easy and more efficient to check whether a particular vote has properly been entered into the software.

C. VV-SV-PAT with 2D Barcode

Although in the improved version with VV-SV-PAT the tallying process becomes easier, faster, and less error prone we can do better. In order to further improve the tallying processes, we propose to print 2D barcodes on the VV-SV-PAT in addition to the human readable summary of the vote (compare to Figure 3). These barcodes cover exactly the same information as displayed to the voter on the confirmation page and printed on the ballot paper above to the barcode. Correspondingly, the barcodes are not unique per ballot but are equal if the summary information is equal.

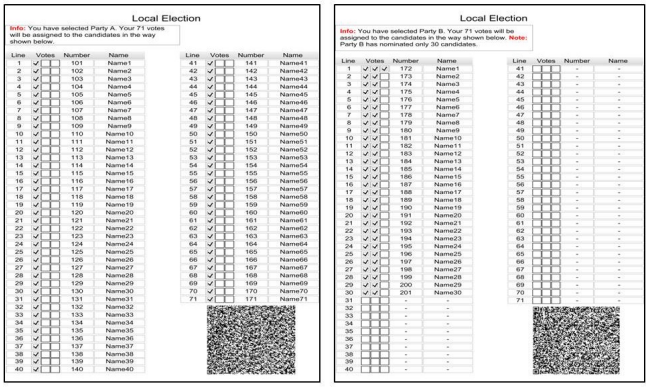

Figure 3. Examples of VV-SV-PATs with barcode

The voter only verifies the summary while he cannot verify the barcode without additional equipment. This might be acceptable as the barcode will be checked during the tallying process and as smart phones are nowadays able to interpret 2D barcodes.

In order to tally the votes, the poll workers scan the barcode, compare the summary displayed on the screen with the summary on the paper, confirm it and proceed. In order to compare this very efficiently, the paper summary has the following order: first the checkboxes, then the number of candidate, and afterwards the name of the candidate while the one displayed shows first the number of candidate and then the checkboxes. The poll workers can now easily put the paper next to the screen and compare as it is enough to compare the checkboxes and the numbers.

D. Improving Universal Verifiability

So far, we have improved the traditional system regarding many different properties. However, at the very end of the tallying process, there is still a black box outputting the final result based on the entered votes. To improve this situation we recommend using two monitors for the tallying process: One displaying the scanned summary and the other one the intermediate result (that is after entering the second vote already the sum of these two is displayed[3]). Thus, the poll worker or even any observer can check that the proper candidates got one more vote. In order to show the whole ballot on this one screen we propose to display only the candidate numbers and not the whole information provided on the ballot paper.

E. Handling Complaints in Polling Stations

Finally we want to address complaints in the polling station. The common problem of paper audit trails is that it is hard to distinguish complaints by trustworthy voters and an untrustworthy vote casting device from untrustworthy voters and a trustworthy device when someone leaves the polling booth telling the poll workers that the printout does not match to the screen. The problem is that by proving the difference the secrecy of the vote would be violated. In addition, as the voter can print multiple times, he may have changed the vote. The poll worker would see a screen that would not match to the printout even if the device is honest.

As the vote casting device is only used to cast and print, the voter could go to the device together with a poll worker and challenge the device by making selections, printout the ballot and compare it. This process should be as realistic as when someone would really cast a vote. If no difference between screen and paper audit trail occurs, the probability of using a manipulated device is very low. Thereby, it is possible to distinguish these two cases with a high probability.

VI. Analysis

In this section we analyze our proposal of using a vote casting device with VV-SV-PATs including the barcodes regarding verifiability, the secrecy of the vote, and usability issues. This is mainly done in terms of a comparison with the traditional paper based voting system with (partial) computer supported counting and tallying as described in Section II. We concentrate on verifiability, secrecy, and usability.

A. Verifiability

Verifiability can be split into three aspects: It should be possible to verify that the vote is *cast as intended*, *recorded as cast* and *tallied as recorded*.

In the traditional system *cast as intended* is somehow not necessary to be verified as the vote is cast on paper. With our proposed approach, it is also possible for the voter to verify that the vote is cast as intended by verifying the printed summary.

[3]Note, these intermediate results are computing during the tallying phase and do therefore not violate any legal regulations.

The step *recorded as cast* can neither in the traditional nor in our proposed system be verified by voters for their own vote. It is only possible to verify this for all cast votes. With both systems, voters or the public need to observe the ballot box and ensure that no one opens it to take out ballots or to modify them. In our proposal, it needs in addition to be observed that barcodes are scanned and interpreted properly during the counting phase. Similarly, in the traditional system it needs to be observed that votes are properly entered into the counting and tallying software. This observation is possible in both cases as the corresponding places are accessible for voters and the public. However, checking this process in the tallying phase is easier than with the proposed system than with the traditional one.

The traditional system does rarely provide a possibility to verify that all votes are *tallied as recorded*. After having entered all votes in the counting software and having confirmed that all votes have been properly entered, the software computes the result which is displayed a couple of seconds later. In the proposed approach, the counting software displays intermediate results after each entered vote.

In addition, the time required to tally is shorter with our approach than with the traditional one which increases the probability that a voter or the public are able to observe the whole process due to their time constraints. All this might not provide the maximum level of verifiability but at least a higher one than the traditional system does provide. The level of universal verifiability could be further increased for our proposed electronic voting system by using independent software to count the stored barcodes or by publishing them and thus enabling everyone to tally the result. Note, here, it needs to be trusted that this list of barcodes corresponds to the one scanned.

Verifiability of eligibility (only authorized votes are tallied) is also ensured in both approaches to the same extent. The voter or the public need to observe the ballot box in the polling station and ensure that no unauthorized votes are put into the ballot box.

B. Secrecy of the Vote

Our definition of the secrecy of the vote covers the aspect that it is not possible to link the voter to his vote as well as that voters cannot create any physical proof of the content of their cast vote (receipt-freeness).

In the traditional system the secrecy of the vote is ensured by the polling booth and the fact that the ballot paper is folded before cast into the ballot box. In our approach, one might argue that the vote casting device logs which vote was ”cast” at what time. If someone has access to this data and in addition would know who was in the polling station at what time then it would be possible to break the secrecy of the voter. The approach we proposed is to enable the voter to print more than one ballot with different votes on it. The device does not know which one the voter cast and can therefore not break the secrecy of the vote. For future work, we recommend to integrate mechanisms which further improve the situation, because we cannot assume everyone will print several votes and because this would actually take too much time if everyone prints a bunch of test ballots.

Both approaches are receipt-free. First of all they do not provide any data to the voter that he can take home. Second taking a picture from the paper ballot does not serve as receipt as it does not prove anything. The voter might have asked for a new ballot paper or might have printed another one after having taken the picture. Thus the cast vote and the one on the photo would be different.

C. Usability

We distinguish between usability issues for voters and for poll workers.

Voters' Usability: We define voter usability as comprising of ease of use, ease of understanding and accessibility. The criterion *ease of use* measures the facility with which voters can accurately cast their vote. Ideally, the process of casting a ballot should not take any significantly long period of time. Regarding the criterion *ease of understanding* it is necessary that a voter should fully understand how to fill out a ballot and cast it. In this respect, voters must understand how their vote is interpreted by the system and know if the vote is valid or not. This includes the verification process, which, according to [9], should be understandable for the average voter. Concerning *accessibility*, a voting system must be able to be used by all eligible voters. This includes voters with disabilities, who may face difficulties with conventional paper ballots.

As the interface is not yet developed and no user test has been conducted it is hard to say something about ease of use of our proposed approach. But the goal is to come up with an interface that is easy to use although the voter needs to take some steps on the screen as the whole ballot is not displayed at once (compare to Section IV and figure 2). In addition, we would recommend to provide a demonstration with the same interface on the internet and maybe also on public places to enable voters to practice casting a vote using our VCD.

Regarding the criterion ease of understand one can say that this does not hold for the traditional system because only few people fully understand it and more than 3.1% usually cast an invalid one[4]. As our approach provides feedback regarding the interpretation of selected candidates and parties and informs about invalid votes, the probability is very high that it is easier to understand even without having justified this by a user study.

In the traditional system blind people can only cast a vote in this type of election with assistance. The advantage of

[4]This is more than twice as much as for the German federal elections in 2005 and 2009.

having the VCD is that it could also provide audio output via earphones which would allow blind or visually impaired people to cast their vote independently and in private. Note, if it is possible to scan ballots also in the polling station and the scanner is equipped with an audio output the blind voters can also verify his vote without assistance. Another possibility it that the voter has a smart phone to take a picture of the barcode and an application that interprets the barcode and reads it to the voter.

Poll Workers' Usability: The tallying process should be easy to use and easy to understand. The later is closely related to *accuracy* as it ensures that the tallying is organized in way that it is not error prone but the votes are properly entered into the counting and tallying software. If a system is usable and easy to understand then the poll workers can proceed the counting *efficiently*.

Our approach performs regarding both categories - accuracy and efficiency - better than the traditional one. Obviously, the comparison of scanned summaries displayed on the monitor with the summaries on paper can be performed much faster than entering candidate by candidate for each huge ballot.

The usability statements are planned to be justified by user studies where both approaches are compared as soon as the interfaces are ready.

VII. Conclusion and Future Work

The main contribution of this paper is the proposal of a new voting system to overcome the challenges that elections with complicated ballots, like for local elections in Hesse, have to deal with. Our approach is based on a vote casting device instead of a DRE which is only used to support voters in selecting candidates and to print a summary of the vote, while it does not store any information. The printed paper contains the human readable summary and the same information coded in a barcode. This barcode is used to improve the counting process at the end of the Election Day. It only needs to be scanned, compared with the printout, and accepted. Furthermore, we proposed to use two monitors during the counting process to show both the scanned summary and the intermediate results which is updated after each accepted vote.

The analysis shows that our approach performs in almost all categories better than the traditional system. Secrecy is the only one where the system needs to be improved. Furthermore, the voting system itself might be strengthened by informing the voter when spoiling a vote, as more people might make use of all options to cast a vote and not just select one party to be sure not to spoil their vote. However, there is a lot of future work to research on before using this system in practice, including at least the following issues:

- implementing the corresponding interfaces after the current usability tests;
- conducting user studies of both the vote casting interface as well as the tallying software interfaces;
- conducting a field test using all three techniques (to justify the extra costs for the barcode scanner) to be able to compare the three systems with concrete numbers about error rates, time to cast a vote, and the tallying phase. Therefore, we hope to closely cooperate with the election authorities to get real data like percentage of invalid votes and percentage of people just selecting one candidate;
- improving the secrecy property; including avoiding side channels by any type of emissions from the vote casting device, the printer, or the audio channel for blind people;
- defining the processes in particular for enabling and disabling the vote casting device;
- providing adequate user guidelines for voters and poll workers;
- discussing the proposal with legal experts, in particular
  - whether the system meets the public nature and verifiability requirements demanded in the court decision [9],
  - whether using the particular summary is acceptable,
  - whether one should provide a scanner in the polling station for voters to verify that the barcode is properly build,
  - whether the assignment of unique numbers during the counting process (as it is done currently) is necessary and if yes integrate in the counting process,
  - which measure to further increase the level of the secrecy of the vote is acceptable,
  - how to handle VV-SV-PATs on which the voter put manually additional signs or drawings;
- integrating audio to enable voters with disabilities to cast their vote without assistance;
- finally one could try to even provide more verifiability by providing some data that voters can take home and remotely verify after the election whether their vote has properly been entered and tallied.

Acknowledgment

This paper has been developed within the project 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen - which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation). The authors would like to thank Richard Frankland for proof reading the paper.

References

[1] D. Demirel, R. Frankland, and M. Volkamer, "Readiness of various evoting systems for complex elections," Technische Universtität Darmstadt, Tech. Rep. TUD-CS-2011-0193, 2011.

[2] *Homepage publishing statistics, http://www.statistik-hessen.de/subweb/k2006/EG411000.htm [german], retrieved 20/4/2011*, Std.

[3] R. L. Rivest, "The threeballot voting system," Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Tech. Rep., Oct 2006.

[4] B. Adida and R. L. Rivest, "Scratch & vote: self-contained paper-based cryptographic voting," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29–40.

[5] J. Bohli, J. Müller-Quade, and S. Röhrich, "Bingo voting: Secure and coercion-free voting using a trusted random number generator," in *E-Voting and Identity*, ser. Lecture Notes in Computer Science, A. Alkassar and M. Volkamer, Eds. Springer Berlin / Heidelberg, 2007, vol. 4896, pp. 111–124.

[6] P. Y. Ryan and S. A. Schneider, "Prêt à voter with re-encryption mixes," in *Proceedings of the 11th European Symposium on Research in Computer Science (ESORIC'06)*. LNCS 4189, 2006, pp. 313 – 326.

[7] D. Chaum, R. T. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity II: end-to-end verifiability by voters of optical scan elections through confirmation codes," *IEEE Transactions on Information Forensics and Security*, vol. 4, p. 611–627, 2009, ACM ID: 1720423.

[8] M. Volkamer and R. Vogt, "New Generation of Voting Machines in Germany - The Hamburg Way to Verify Correctness," in *Proceedings of the Frontiers in Electronic Elections Workshop - FEE '06*, 2006.

[9] Bundesverfassungsgericht, *Judgment*, BVerfGE 123, 39 - 88, Std., March 2009. [Online]. Available: http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html