

Implementing and evaluating a software-independent voting system for polling station elections

Jurlind Budurushi, Roman Jöris and Melanie Volkamer

TU Darmstadt / CASED

Abstract

In 2009 the German Federal Constitutional Court introduced the principle of “public nature of elections” [1]. This principle requires that when using electronic voting systems it must be possible for the citizen to verify the essential steps in the election process and in the ascertainment of the results reliably and without special expert knowledge. Unfortunately, none of the existing systems complies with this principle. As a result, the use of electronic voting systems in Germany for parliamentary elections has stopped. Nevertheless, electronic voting systems are necessary and would improve the situation, especially for elections with complex ballots and voting rules, for example some local elections in Germany or parliamentary elections in Belgium and Luxembourg. The concept proposed by Volkamer et al. [2] was analyzed by a legal expert and evaluated to comply with the German legal requirements for local elections in the state of Hesse [3]. In this paper we specify and concretize processes that were left open in the concept, and implement a prototype. We evaluated this prototype in a user study that was conducted alongside the university elections at the Technische Universität Darmstadt in June 2013. The results of the study show that most of the participants were satisfied with the prototype and would support its use for the upcoming university elections. We also report some lessons learned.

Keywords: electronic voting system, software-independence, polling station elections, implementation, evaluation, user study

1. Introduction

Electronic voting continues to be a topic of interest with widespread use in different contexts and countries. While countries like U.S., Estonia, Norway,

Switzerland, and Finland use electronic voting for legally-binding elections, others such as the Netherlands and Germany have stopped their use, due to legal requirements.

Germany seems to have the strictest legal requirements with respect to the use of electronic voting systems in legally-binding elections. Electronic voting systems have to comply with the principle of “public nature of elections”, which was introduced by the Federal Constitutional Court of Germany in 2009 [1]. Hence, when using an electronic voting system, it must be possible for the citizen to verify the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge. This holds true for federal, state and local elections in Germany. The use of electronic voting systems in Germany is especially necessary for local elections with complex ballots and voting rules, for example local elections in Hesse. To the best of our knowledge, the concept introduced by Volkamer et al. [2] is the only one that has been analyzed by a legal expert with respect to, and evaluated to comply with, the German legal requirements for local elections in Hesse [3].¹ However, before this concept can be used in such elections, a number of processes need to be concretized, specified and implemented.

Volkamer et al. [2] proposed the printing of multiple paper ballots in the vote casting process, but this was not concretized. Hence, we concretized the vote casting process by comparing advantages and disadvantages of multiple versus single printouts. From a concept level the following processes need to be specified:

- Enabling/disabling the voting device.
- Preventing permanent storage of votes.
- Ensuring physical security.

Afterwards, we implemented a prototype, in order to evaluate the electronic voting system and to improve our technical approaches. To enable the use

¹As [3] is in German, we provide here a short summary: 1) Voters can verify their printouts without any specialist knowledge and without relying on the system’s integrity. Independent of the QR-Code, the human-readable part is determinative. 2) The system enables a fully manual counting, similar to the traditional one. 3) The system strengthens the principle of “public nature of elections”, because voters better understand the impact of their selections, and the tallying process might be faster than in traditional system.

of the prototype in user studies, we also developed adequate user guidelines/procedures for voters and poll workers. Furthermore, we conducted a user study alongside university elections at the Technische Universität Darmstadt in June 2013. The focus of the user study was to evaluate the voting phase, while an implementation and evaluation of the tallying phase is left for future work.

2. Concept: EasyVote

The EasyVote concept proposed by Volkamer et al. [2] mainly addresses challenges in elections with complex ballots and voting rules, e.g., some local elections in Germany or parliamentary elections in Belgium and Luxembourg. However, this concept is applicable to any type of elections. The novelty of EasyVote is that it combines the advantages of the traditional paper-based system and those of an electronic voting system. Furthermore, according to the definitions of Rivest et al. [4] EasyVote is software-independent.

Voting phase. The voter first identifies herself to the poll workers, similar to traditional paper-based elections. Afterwards, the voter enters the voting booth and uses the electronic voting device to prepare the ballot by selecting candidates. When the voter confirms the selected candidates, the electronic voting device starts the printing process and at the same time deletes all electronic data, i.e. all voter’s selections.² The printout, which contains voter’s selections, consists of two parts: a human-readable and a machine-readable (a QR-Code) part.³ The voter verifies that the human-readable part contains the candidates selected on the electronic voting device. Finally, the voter folds the printout, leaves the voting booth and deposits the printout into the ballot box. The components used in the vote casting process, are shown on the left side of Figure 1.

Tallying phase. Similar to the traditional paper-based system, poll workers first open the sealed ballot box, and verify that the number of printouts (paper ballots) matches the number of voters in the electoral register. Afterwards, the poll workers start counting, by scanning each single printout. Thus, they scan the QR-Code and verify that its content, shown on a moni-

²At this point in time, data are deleted from the vote casting software, i.e. on the software level.

³The machine-readable part, which contains the exact information as the human-readable part, enables an automatic tallying of the printouts.

tor, matches the human-readable part of the printout. The scanned printout is added to the intermediate result, shown on a second monitor, when the poll workers have verified and confirmed its content. Additional components used in the tallying process, are displayed on the right side of Figure 1.

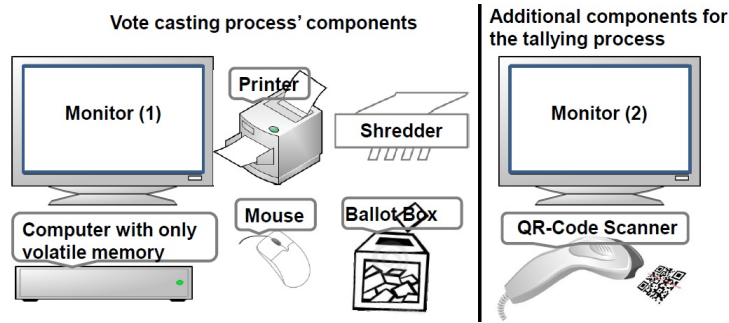


Figure 1: EasyVote components.

3. Concretizing the vote casting process

Volkamer et al. [2] propose to enable voters to print several printouts (paper ballots) in the vote casting process. The main motivation for enabling multiple printouts is to ensure secrecy w.r.t. a malicious voting device that would store the sequential order of cast votes. This approach also enables the voter to become familiar with the system. However, when concretizing this approach a number of challenges and disadvantages arise. The major challenge of this approach is ensuring that each voter casts only one vote (only one printout is deposited into the ballot box). This challenge can be addressed by a number of different techniques: Voters can be provided an envelope which they deposit into the ballot box. Multiple printouts in an envelope makes that vote invalid. Another technique is that poll workers stamp the backside of the printout, before the voter deposits it into the ballot box. A very exotic technique is by using accurate weighing scales. Thus, the voter would place the folded printout(s) on the weighing scale before depositing it/them into the ballot box. However, poll workers would identify if more than one folded printout is placed on the weighing scale, because independent of the amount of ink on printouts, the weight of a single printout is relatively constant. A fourth technique is to provide poll workers with a counter that displays the exact number of printed printouts

during a single vote casting process. Thereby, poll workers are required to verify that the voter cast only one printout and secretly destroys the rest.

All these techniques either increase costs or the organizational effort towards poll workers. Stamping the backside of printouts as previously agreed with an attacker might lead to voter coercion or vote selling. Furthermore, by using the fourth technique different attacks such as chain voting [5] or voter coercion are still possible. For instance, the attacker can either leave a printout in the voting booth or take one out and give it to the voter. Then, the attacker needs to observe that the voter spends a specific time in the voting booth.⁴ These attacks might be prevented by using the fourth technique, however destroying printouts secretly and verifying the exact number of destroyed printouts seem to be two contradicting actions.

In contrast, enabling only a single printout in the vote casting process prevents all attacks mentioned above. However, a challenge of this approach is that voters can not become “very” familiar with the system during the vote casting process. Nevertheless, this challenge can be addressed by providing voters with an online prototype before the actual elections. Another challenge is that a malicious voting device which stores the sequential order of cast votes might violate vote secrecy. However, from a legal perspective this challenge also applies when multiple printouts are allowed. In case of multiple printouts a malicious voting devices can link a voter with her vote with a non-negligibly higher probability than from the final election result. Based on this comparison we recommend to change the EasyVote from multiple to single printouts. Table 1 summarizes the advantages and disadvantages of both approaches.

	<i>Challenges</i>	<i>Possible attacks</i>
<i>Multiple</i>	yes	yes
<i>Single</i>	no	no

Table 1: Advantages and disadvantages of multiple versus single printout.

4. Enabling/disabling the voting device

While specifying the process for enabling/disabling the voting device, we also consider the results of section 3. In that case the process should ensure

⁴The time interval which is too short to start the printing process.

that voters can only print a single printout (paper ballot) in the vote casting process.

The simplest and most secure approach that ensures the printing of a single printout in the vote casting process, is to automatically *disable* the voting device when the printing process starts. Thus, for all following *enabling approaches* we assume that the voting device is disabled when the printing process starts. The voting device can be enabled by using *a token*, e.g. a smart card as in [6] or in Avante Vote-Trakker. This approach increases costs, because the token should be configurable, i.e. to re-enable the voting device with the same token, the token needs to be re-configured. Furthermore, readers are necessary. Another approach is to implement *a timer* that automatically enables the voting device after it has been disabled. This approach increases the organizational effort for poll workers, as they have to make sure that voters leave the voting booth, before the voting device is re-enabled. A third approach is to enable the voting device *manually by poll workers*, like most DRE systems. However, this increases the organizational effort for the poll workers. The voting device can also be enabled *remotely by poll workers using an enabling device*. The enabling device, similar to the Nedap voting machines, is connected via cable to the voting device. This device can be simple and cheap, as it only needs to show the current state of the voting device (enabled/disabled) and the interface should only allow to send an enabling signal to the voting device, for example a single button. The last combines the advantages of all previous approaches, therefore we recommend to use this approach to enable the voting device.

5. Preventing permanent storage of votes and ensuring physical security

EasyVote [2] requires that electronic votes are not stored permanently. However, a practical approach that meets this requirement has not yet been specified. In this section we propose a practical approach that meets this requirement from a hardware level perspective. In order to ensure that votes are not stored permanently, we introduce the following requirements:

1. The voting device shall consist only of volatile memory, such that when the power supply is removed all data are irrevocably lost.⁵

⁵With voting device we refer to all components in the vote casting process.

2. The voting device shall not contain any integrated or external network interface controller.
3. The voting device shall provide only the following input/output sockets:
 - (a) An input/output socket for the monitor.
 - (b) An input/output socket for the printer.
 - (c) An input/output socket for uploading the voting software into memory.
 - (d) An input/output socket for the enabling device.

To provide a high guarantee that the voting device meets these requirements, we recommend the following five-step approach: 1) Observing the hardware development process. 2) Certifying/Evaluating the voting system. 3) Verifying that the certified system will be used. 4) Performing random plausibility-checks. 5) Performing random reverse-engineering of systems after the elections.

Note that we assume that other technical/organizational requirements, e.g. verifying the integrity of the voting software, preventing the installation of hidden cameras in the voting booth, are met.

Ensuring physical security. To ensure physical security the voting device and the printer should be placed inside securely closed cases, such that unauthorized physical access is prevented. Further, only the user interface, i.e. screen and printer output tray can be accessed in the voting booth, while the processing unit of the voting device and printer are accessed only from the outside of the booth in a way that anyone in the polling station can monitor it during the election. Furthermore, all cables should be visually accessible to the poll workers and fixed to the ground.

6. The EasyVote prototype

In this section we describe the implemented EasyVote prototype, which includes voter instructions and guidelines/protocols for poll workers.

6.1. Implementation

For the implementation of the prototype we considered all recommendations made in the sections 3, 4 and 5. The voting software was implemented in the Java programming language. The voting device consisted of an integrated touch screen (type: elo touch system) and a computer (Motherboard MS-6535 VER:2; CPU Pentium 4, 2.40 GHz; 512 DDR-SDRAM and a CD-ROM). The hard disk and the Ethernet network interface controller were

removed. The printer was a Kyocera FS 1300D. We created a live CD that included the operating system (Porteus V2.0-i486), a Java run time environment (jre-7u11-i586-1.jre), the voting software, the drivers for the printer, touchscreen and the enabling device. The enabling device, shown in Figure 2, included an ATmega 8[7] microcontroller from Amtel for the controlling.

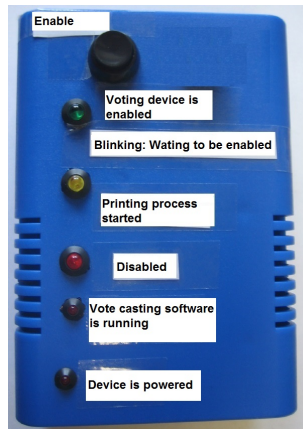


Figure 2: The enabling/disabling device. (English translation)

6.2. Instructions for voters

Usually in real elections voters are informed about the voting system through the media, e.g. news or advertising, or in the election notification and polling station. Even though EasyVote is software-independent, there is no doubt that election integrity is only ensured if voters verify their printouts. This holds true for all software-independent voting systems that provide voter verifiable paper audit trails (VV-PATs). Current research show that voters are not very likely to verify the VV-PATs [8], [9], [10] and [11]. Therefore, in the user study we integrated voter verifiability instructions, which we have developed by Budurushi et. al [12]. The verifiability instructions and their integration in the vote casting process are presented in Figure 3. Additionally and based on the verifiability instructions, we developed a poster that depicts all steps in the vote casting process, refer to Figure 4. Finally, we also developed a video that animates the vote casting process.⁶

⁶To watch the video visit the following link: <http://tinyurl.com/lhj5no7>.

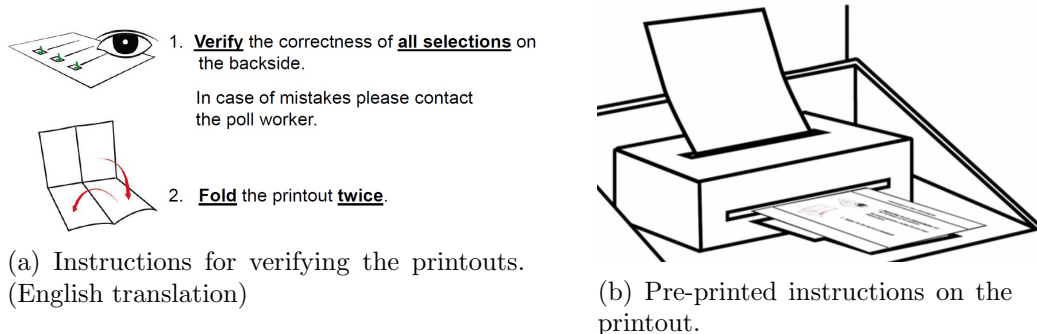


Figure 3: Verifiability instructions and their integration.

6.3. Guidelines and protocols for poll workers

In real elections poll workers are trained and instructed about the election, i.e. the voting system in use. Therefore, we developed corresponding guidelines and protocols, in order to provide poll workers with necessary information.

Guidelines. We developed the follow guidelines: *General*, *Repeating of Vote Casting Process*, *Wrong Printout*, *Exceptional Cases and Solutions*, and *Tallying*.

The *General* guideline provide poll workers with instructions regarding data privacy protection, voter identification, enabling/disabling the voting device and the vote casting process. The *Repeating of Vote Casting Process* guideline instructs poll workers in case a voter wants to repeat the vote casting process, e.g. when the voter wants to cast a different vote (printout) from the one already printed. The *Wrong Printout* guideline provides instructions when voters complain that the printout does not match their intention, i.e. what they selected on the voting device. This guideline includes a two-step approach: In the first step, the poll worker and the voter enter the voting booth together and try to cast (print) a test vote (printout). In case no problems are identified, the voter is left alone in the voting booth to repeat the process in secret. In case the voter complains again that the printout does not contain the selections made on the voting device, the voter is given a sealed envelope that contains all possible pre-printed printouts. Then, the voter is asked to enter the voting booth, select and cast the appropriate

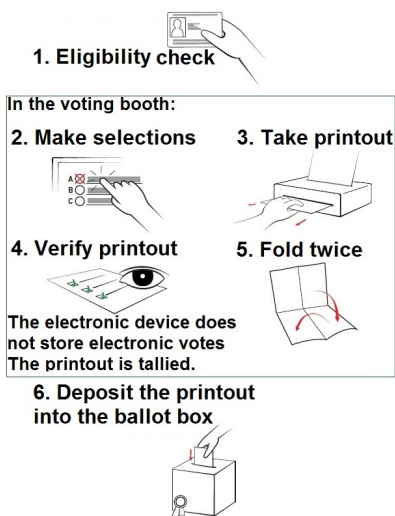


Figure 4: Steps of the vote casting process. (English translation)

printout, and secretly destroy the rest.⁷ The *Exceptional Cases and Solutions* guideline provide poll workers with instructions to follow and contact persons, in case the voting device crashes or the printer does not work, or there is a power failure. Last but not least, the *Tallying* guideline included a poster that depicted all steps in the tallying process, refer to Figure 5.

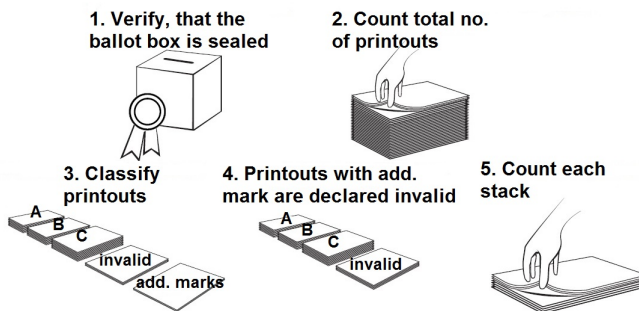


Figure 5: Steps of the tallying process. (English translation)

Protocols. All protocols required at least two poll workers to record information, thus enforcing the so called four-eyes principle. Except for the

⁷Note that the second step is only feasible for “simple” elections. For elections with complex ballots and voting rules, voters are required to lodge a formal complaint.

General guideline, we developed for all other guidelines a corresponding protocol. The following protocols were developed: *Preparation of the live CD*, *Election Start*, *Devices and Materials*, *End of Election*, *Electoral Register*, *Filling Printouts and Changing Cartridges*, *Complaints*, *Present Poll Workers*, *Tallying* and *Miscellaneous*.

We only describe the first four protocols, as all others are self-explanatory through their naming. The *Preparation of the live CD* protocol consists of all steps that are necessary to create a live CD. This includes all specific information regarding software (operating system, OpenSSL, disc burning software etc.), and hardware (computer, USB etc.) type and version used. Additionally the SHA-1 hash value of the live CD should be computed and recorded into the protocol. Furthermore, the process of creating a second original live CD should be platform-independent.⁸ The SHA-1 value of the second live CD is computed, compared with the SHA-1 hash value of the first live CD, and recorded into the protocol. This process, which is best-practice in the field of computer forensics, ensures the integrity of the content of the live CD, as everyone in possession of the original voting software is able to create an identical live CD. Note that the live CD was created, the day before election day in a public process. We had announced it a month before via our website, and invited people via E-Mail, especially the legal department of our university. However, only a PhD student of the chemistry department who had no relationship with our research group was present. In the *Election Start* protocol poll workers were required to verify and record that all documents (guidelines/protocols), devices and materials were provided. Further, the poll workers should verify that the ballot box is empty, seal it and record this into the protocol. Finally, when setting up the voting device poll workers should compute and verify that the SHA-1 hash value of the live CD matches the value recorded in *Preparation of the live CD* protocol, and record the computed value into the protocol. The most important part of the *Devices and Materials* required the poll workers to perform a plausibility-check w.r.t. volatile memory and network access. Thereby, poll workers should visually control that no hard disk and no network interface controller (e.g. WLAN, Ethernet) were installed. Further, poll workers sent a printing job to the printer and at the same time removed the power. After

⁸Note that this process enables to detect technical problems or a malicious system during the creation process of the first original live CD.

reconnecting the power the printer should not execute the printing job sent before. Poll workers had to record these plausibility-checks into the protocol.⁹ This protocol also required poll workers to verify and record that all necessary devices (e.g. printer) and materials (e.g. printouts) were provided. The *End of Election* protocol required poll workers to verify that all protocols were completed and signed. The number of voters in the electoral register should be recorded into the protocol. Poll workers should also verify and record that the ballot box is still sealed. Finally, the polling station should be disassembled and all devices, materials etc. should be transported to the lab of our research group.

7. Evaluation of the prototype

In this section report the results and lessons learned from the user study that. The general goal of the user study was to evaluate the prototype from a technical and practical perspective. We were also interested in the opinion of the participants regarding the concept (EasyVote) and electronic voting in general.

7.1. Pre-tests

In order to identify any technical issues and to improve the process in the vote casting phase, we conducted a number of pre-tests in the lab of our research group. In the pre-tests participated 10 members. This includes members of our research group and members of the “Cryptography and Computer Algebra” research group at the Technische Universität Darmstadt. From a technical perspective no problems were identified in the pre-tests. Nevertheless, we got valuable feedback regarding the process in the vote casting phase. This feedback mainly addressed the process of introducing participants with the goals of the user study and the steps in the vote casting software. We considered this feedback in the user study.

7.2. Experimental design and procedure

The user study took place alongside the day university elections at the Technische Universität Darmstadt in June 2013. Our polling station was next to the polling stations of the university elections. For the user study

⁹Note that due to time and funding restrictions, for the user study we performed only plausibility-checks.

we designed a simple test election. In the test election participants voted by expressing their satisfaction regarding their supervisor. For expressing the satisfaction we used a five-point Likert scale (always satisfied - mostly satisfied - sometimes yes sometimes no - rarely satisfied - never satisfied). In order to cover as many participants as possible, the range consisted of seven different types of supervisors in our university: the orientation phase tutor (for freshers), mentor, bachelor thesis supervisor, master thesis supervisor, PhD thesis supervisor, superior (for employees), and the president (for professors). The interfaces of the test elections are presented in Figure 6.

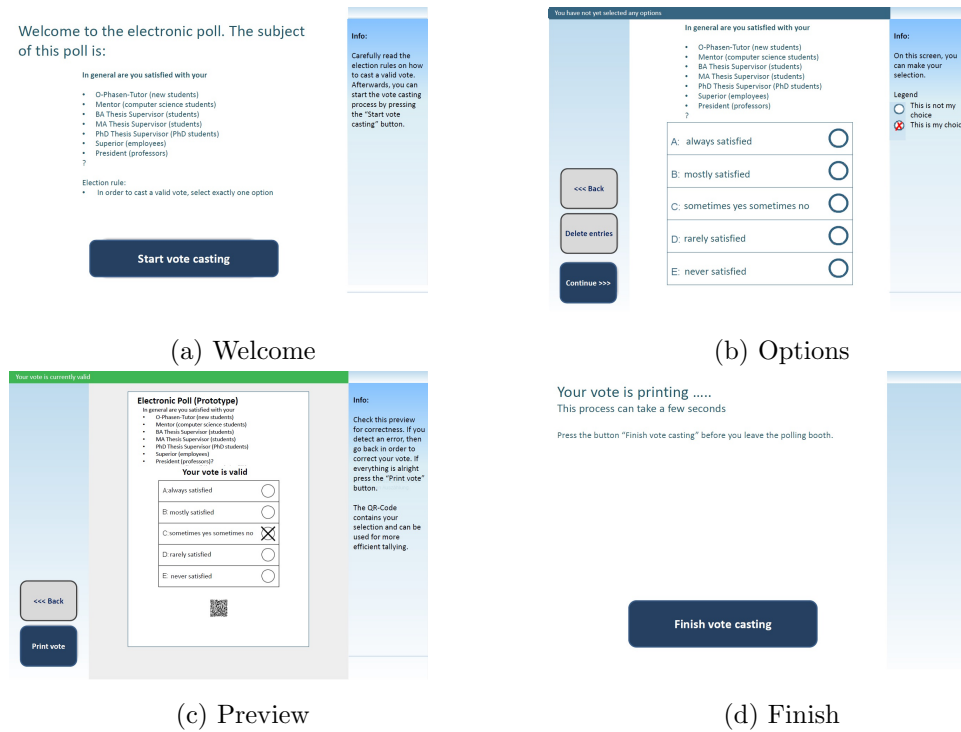


Figure 6: Interfaces for the test election. (English translation)

The test election proceeded as follows: Each participant had to pass through four sequential phases: First, the participant was provided with oral explanation about the goals and the procedure of the entire experiment. Afterwards, the participant was explicitly introduced to the vote casting process. The different steps were explained using the vote casting poster, refer to Figure 4 in section 6.2. Thereby, the participant was told that by selecting only one of the given options, she cast a valid vote, otherwise no

selection or more than one selections would invalidate her vote. According to [13, §1, Rn. 23], the principle of the free suffrage contains the right to cast invalid votes. Thus, the voting software should support voters to not spoil their votes unintentionally, but also enable them to cast an invalid vote.¹⁰ In the next phase after the identification, the participant entered the voting booth, made her selections and deposited the printout into the ballot box. Finally, the participant could fill in the online post-questionnaire either next to our polling station or from any other preferred location.

7.3. Post-questionnaire

The post-questionnaire measured the following statements by using a five-points Likert scale (strongly disagree - rather does not apply - neither nor - rather agree - strongly agree) (English translation):

- “Please briefly tell us your impression of the electronic voting system that you have just used. Feel free to suggest any improvements”.
- “In the next university elections I would like to use the electronic voting system I just used”.
- “I would like to cast my vote electronically in the next university’s elections”.
- “I think that vote secrecy might be violated by the use of the QR-Code.”

In addition the post-questionnaire collected some demographic data (gender, age, and education).

7.4. Setup

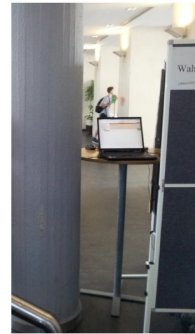
The polling station consisted of three different areas: the poll workers’, the post-questionnaire, and the voting booth area. The poll workers’ area, is presented in Figure 7(a). The post-questionnaire area, which was outside of the polling booth is presented in Figure 7(b). The poster used to explain participants the vote casting steps is presented in Figure 7(c). Finally, Figure 7(d) presents the voting booth area. Furthermore, voters and poll workers

¹⁰We are aware that this depends from the corresponding election regulations of each country.

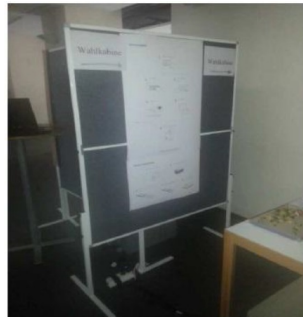
were provided with the guidelines and protocols introduced in section 6.2 and 6.3. Note that we used all materials (devices, guidelines, protocols etc.) several times, because the university elections lasted four days.



(a) Poll workers' area



(b) The post-questionnaire area.



(c) The vote casting poster.



(d) Inside the voting booth.

Figure 7: The setup of the polling station.

7.5. Recruiting and sample

The participants were recruited verbally, directly after having cast their vote for the university elections. One of the three poll workers stood in front of the poll workers' area and asked people to take part in the experiment. No payment was provided to the participants. The experiment had 421 participants that cast a vote, but only 198 of them (135 male, 63 female) between the age of 18 - 59 years filled in the online post-questionnaire. Thus, in the results we consider only 198 participants. The sample consisted of students of different departments (e.g. sociology, psychology, mathematics

etc.) and employees (e.g. secretaries, care takers, administrative technical staff etc.) of our university.

7.6. Ethical considerations

Ethical requirements for research involving human respondents are provided by an ethics commission at the university. These were met, e.g. as all participants were told before participating in the experiment that data was stored anonymously and served only for the purpose of the experiment.

7.7. Results

The analysis of the statement “Please briefly tell us your impression of the electronic voting system that you have just used. Feel free to suggest any improvements” shows that most of the participants were satisfied with the prototype, especially with the EasyVote concept. A detailed analysis of this statement looks as follows: Only 166 out of 198 gave valuable answers. The 32 questionnaires that were not useful contained responses such as (English translation): “No time”, “hmmm”, “bla” etc. 81 out of the 166 participants had a positive impression of the system (English translation): “It seems to be a very practical solution. I am convinced that such a system will be used in the future.”; “The system was easy to use and intuitive”; “Very good, a hybrid system is better than a fully electronic one”, “After a short familiarization phase, the system appears clear and simple. It could be very convenient for the concerns regarding university elections.”. 26 of 166 participants did not understand the advantages of the electronic voting system compared to the traditional paper-based system. They were mostly surprised why a printout was needed if they are voting electronically. Some participants also had difficulties using the prototype. Here are some of the reasons: 15 participants complained that the printing process is too slow; seven participants complained that the touchscreen did not react very fast; three participants were confused that the button leading to the next step was on the left side of the interface; three participants had not perceived that there was a preview screen; two participants would have preferred a bigger status bar informing them about the validity of their vote; one participant was confused with the last screen and thought something went wrong; one participant would have preferred a bigger platform for folding the printout. Participants gave also valuable feedback w.r.t. the information provided to the participants and the public in general and regarding organizational processes: Eight participants would have liked more information about the system (about the QR-Code,

system interconnection, processing of the data); two participants suggested that we should have had more advertising and should have not set up our polling station into a small corner; One participant suggested that back-up printouts (empty paper ballots) are important in case of failure. Further, two participants criticized the prototype as not matured and that it provides too much information. Finally, only 14 participants do not support the use of electronic voting in general because of secrecy concerns.

Table 2 summarizes participants’ opinion regarding the statement “In the next university elections I would like to use the electronic voting system I just used”, while Table 3 regarding “I would like to cast my vote electronically in the next university’s elections”.

<i>Likert rating</i>	<i>No. of participants</i>	<i>%</i>
strongly disagree	22	11,1
rather does not apply	31	15,7
neither nor	46	23,2
rather agree	73	36,9
strongly agree	26	13,1

Table 2: Using EasyVote in the upcoming university elections.

<i>Likert rating</i>	<i>No. of participants</i>	<i>%</i>
strongly disagree	24	12,1
rather does not apply	26	13,1
neither nor	49	24,7
rather agree	63	31,8
strongly agree	36	18,2

Table 3: Support regarding e-voting in general.

The result regarding the statement “I think that vote secrecy might be violated by the use of the QR-Code.” show that 39.9% of the participants have concerns regarding vote secrecy due to the use of QR-Code. This confirms the findings of Llewellyn et al. [14]. We conclude that in general participants (voters) seem to have secrecy concerns when encoded information is on the printouts.

7.8. Lessons Learned

During the user study we identified a number of lessons learned: First, it is important to clearly communicate the advantages of the electronic voting system compared to the traditional paper-based system or any other known system to the participants. Second, the printing process should be faster, in order to not confuse voters during the vote casting process. The same also holds true for the touch screen. We need to review the process for creating two original live CDs from independent platforms, which would have the same hash value. This process did not succeed in the user study, thus we created only copies of the one original live CD. Further, participants shall be provided with sufficient information regarding the operation and all components of the system. It is also important that participants are clearly informed about the steps of the vote casting process, as poll workers identified a number of deviations. These deviations are summarized in Table 4.

	<i>No. of participants</i>
<i>Printout left in the voting booth</i>	16 out of 421
<i>“Finish vote casting” not clicked</i>	20 out of 421
<i>Printout not folded</i>	14 out of 421

Table 4: Deviations during vote casting process.

In order to prevent confusion and long queues, poll workers should be provided with clear instructions about the enabling device. It is also very important to provide participants with the adequate amount of information. Finally, we note that we did not have any technical or organizational issues during the user study, and everything worked flawlessly.

8. Conclusion and Future Work

In this paper report on an implementation and evaluation of a first prototype based on the EasyVote voting system [2]. The results of the evaluation are very positive regarding EasyVote and e-voting in general. Thus, 73.2% of 198 participants would support the use of EasyVote in upcoming university elections, while 74.7% of the 198 participants support e-voting in general.

The results also provide a number of interesting research questions for the future. Thus, for future work, we plan to design a user study to address voters’ secrecy concerns when using encoded information on printouts. In

addition we will have the poll workers evaluate the system, guidelines and protocols, as due to time constraints we were not able to do so. Further, we plan to analyze if it is technically possible to create two original live CDs independent from the platform. We are going implement and evaluate a prototype for complex ballots and voting rules, e.g. local elections in Hesse, while considering all lessons learned. However, this also includes open issues, like content on the printout, designing the user study, and providing adequate interfaces (including colors). As parties are generally associated to colors, these colors must be excluded in the design of interfaces. Afterwards, we plan to address organizational and technical measures that prevent information leakage through electro-magnetic radiations and power consumption.

Acknowledgements. 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). We would like to thank everyone who supported us, especially our student assistants Kristoffer Braun, Markus Hau and Philipp Rack, and those who participated in the user study.

References

- [1] Federal Constitutional Court of Germany: Entscheidungen des Bundesverfassungsgerichts(BVerfGE), BVerfGE 123, 39 - 88, http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html, (last accessed 17.01.2014) (March 2009).
- [2] M. Volkamer, J. Budurushi, D. Demirel, Vote casting device with VV-SV-PAT for elections with complicated ballot papers, in: REVOTE11, 2011, pp. 1–8.
- [3] M. Henning, M. Volkamer, J. Budurushi, Elektronische kandidatenauswahl und automatisierte stimmermittlung am beispiel hessischer kommunalwahlen, DÖV (20) (2012) 789–796, https://www.secuso.cased.de/fileadmin/user_upload/Group_SECUSO/EasyVote/Video/RechtlicheBewertung.pdf, (in German, last accessed 17.01.2014).
- [4] R. L. Rivest, J. P. Wack, On the notion of “software independence” in voting systems, <http://people.csail.mit.edu/rivest/>

- RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf, (last accessed 17.01.2014) (2006).
- [5] D. W. Jones, Chain voting, in: Workshop on Developing an Analysis of Threats to Voting Systems, National Institute of Standards and Technology, 2005.
 - [6] C. Vegas, The New Belgian E-voting System, in: EVOTE12, 2012, pp. 199–211.
 - [7] Atmel, 8-bit Atmel with 8KBytes InSystem Programmable Flash – Datasheet, rev.2486aaavr02/2013 Edition.
 - [8] S. B. Cohen, Auditing Technology for Electronic Voting Machines, master thesis, MIT, Media Lab. (2005).
 - [9] T. Selker, A. Pandolfo, A methodology for testing voting systems, JUS 2 (2006) 7–21.
 - [10] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, P. L. Francia, B. B. Bederson, F. Conrad, M. Traugott, The promise and pitfalls of electronic voting: results from a usability field test, http://www.capc.umd.edu/rpts/Promise_and_Pitfalls_of_Electronic_Voting.pdf, (last accessed 17.01.2014) (2005).
 - [11] A Study of Vote Verification Technology Conducted for the Maryland State Board of Elections Part II: Usability Study, <http://www.capc.umd.edu/rpts/MarylandReport\%202-13-06.pdf>, (last accessed 17.01.2014) (2006).
 - [12] J. Budurushi, M. Woide, M. Volkamer, Introducing precautionary behavior by temporal diversion of voter attention from casting to verifying their vote, in: Workshop on Usable Security (USEC), 2014.
 - [13] W. Schreiber, Bundeswahlgesetz Kommentar, Carl Heymanns Verlag (March 2009).
 - [14] M. Llewellyn, S. Schneider, Z. Xia, C. Culnane, J. Heather, P. Y. Ryan, S. Srinivasan, Testing voters’ understanding of a security mechanism used in verifiable voting, JETS 1 (1) (2013) 53–61.