securityandtrust.lu

Studying Boardroom E-Voting Schemes: Usability and Trust

Dalia Khader, SnT, University of Luxembourg

Rod McCall, SnT, University of Luxembourg

Jose Miguel Lopez, University of Luxembourg

Revised Edition, February 2014

ISBN 978-2-87971-119-5/

Technical Report TR-SnT-2013-3

Studying Boardroom E-Voting Schemes: Usability and Trust

Prepared by: Dalia Khader, Rod McCall, Jose Miguel Lopez

Summary.

This technical report presents initial results of an ongoing research on Usability and Trust in Boardroom E-voting Systems. OpenVote, an implementation of one of the existing boardroom e-voting schemes, is used as our case study.

The primary contributions of this report are:

- A usability and trust study of the first version of the OpenVote System.
- The development of a questionnaire relating to usability and trust within boardroom e-voting systems.
- An overview of a revised version of OpenVote.

Correction

The first edition of this report contained an error in the way the overall system usability score was calculated. This resulted in the overall SUS score for both versions of Openvote being significantly lower. This revised version of the technical report has corrected this error.

Table of Contents

1. Introduction

The following technical report presents the results of a study designed to identify usability and trust issues within a boardroom e-voting system. The study used SUS [13] as a basic questionnaire to rate the overall usability of the system, it was complemented by some open ended questions which were designed to capture the users' feels about the system. From this a set of core issues relating to security, privacy and trust were identified and a questionnaire developed. The questionnaire was then used within a second study. The results of the second studied will be published separately.

The report begins with a background to the area, an overview of the first version of a system known as OpenVote followed by results from the study and an overview of the questionnaire. The second part of the report summarizes a revised version of OpenVote while the appendix contains the questionnaire

2. Background

Voting is the democratic process of making a decision among publicly known options based on the mast majorities' opinion. Electronic voting (E-voting) is a wide ranging term that implies a computer was used at one point of the voting process.

E-voting systems proposed so far can be categorized as follows:

- **Centralized vs. Decentralized Voting:** E-voting systems that are centralized depend on election administrations to run the system, such as ballot generators, tallying authorities, ballot distributers, etc, [1][2][3]. Centralized schemes are typically designed for large scale elections and rely upon stronger trust assumptions to enable scalability, usability and robustness. On the other hand, decentralized systems have no election administration and all entities in the system have the exact same role. All entities equally can vote and tally without the help of any central authority (or group of authorities). Decentralized systems are typically designed for small scale elections with a focus on security with minimal trust assumptions [4][5][6][7]. They are proposed for boardroom elections were using a centralized system is overkill. Boardroom elections are designed to resemble a hands-up scenario where the voters have to be present in one room at the same time. A chairman asks the question and the votes are collected by counting the number of people who have their hands-up as a sign of agreeing with the decision compared to the number of people who did not raise their hands as a sign of appausing the decision. The main difference between using a hands-up voting scheme over using an electronic boardroom voting scheme is the latter reserves confidentiality of the vote. Scenario 1 illustrates it's usage.

- **Supervised vs. Remote Voting:** There are two types of e-voting systems: Systems that are supervised physically by independent electoral official and/or governmental representatives [1][8], where the voters still need to go to a polling station to submit their votes. Alternatively, the systems can be remote where the vote is submitted from a personal computer, or mobile phone via the internet also known as i-voting[3][2]. Regarding the supervised voting they can be end-to-end electronic where voting and tallying are electronic. They can have the frontend electronic via using machines like punchcards and lever machines while tallying remains manual. They can also be a mixture of paper based and electronic where the voter still uses a paper ballot that carries certain digital information that will be used in tallying.

> *A company, which has several shareholders, wants to make a decision on whether to close a deal with a private business owned by one of them. To avoid disputes the shareholders meet each other to decide according to the majorities' opinion. However, the different shareholders may not want to disclose their opinion and may prefer it to remain confidential.*

Scenario 1 Boardroom Elections

2.1 On the Security of E-Voting Schemes

Paper-based voting schemes gained their properties from the physical constraints of the real-world. For example, voters will mark their ballot in isolation inside a voting booth within a supervised polling station and they would drop it into a locked ballot box. This will ensure confidentiality of the vote, and furthermore will guarantee that no voter was influenced by an external entity when submitting their votes. Moreover, the opening of the sealed boxes and the counting can be done under official observers from the public which gives an assurance of correctness, transparency and verifiability.

E-voting systems try replicating these properties in the digital world. The confidentiality of the vote is the major concern when designing an e-voting scheme and the best way to achieve confidentiality in the digital world is to use encryption schemes. Nevertheless, using encrypted votes makes it challenging to verify the procedure of the election. Adida categorizes verifiability into three types [9]:

1. Individually verifying that a vote is casted as intended, recorded as casted and counted as recorded.
2. Universal verifiability of the tallying being correct.
3. Verifying eligibility of voters.

Different solutions were proposed in the literature for achieving verifiability. The most famous technique used a vote receipt and a public bulletin board [3] [1] [2] where each voter receives a receipt when submitting their vote, that receipt has enough information to check that the tallying authority received their votes by looking them up in the bulletin board. However, these receipts do not reveal the actual votes.

In boardroom voting schemes the votes are also encrypted. The other security properties are derived from the cryptographic properties of the protocol and are summarized as follows [4]:

1. Self-tallying: At the end of the protocol, voters and observers can tally the election result from public information that got broadcasted.
2. Fairness: Nobody has access to partial results before the deadline.
3. Dispute-freeness: A scheme is dispute free if all voters and any third party can verify that the protocol was run correctly and that each voter acted according to the rules of the protocol.
4. No trusted authority is needed to guarantee its security.

2.2 On the Usability and Trust of E-voting Schemes

E-Voting Scheme/Paper	Usability	Trust	Methodology
Remote Scheme: Helios [10]	yes	No	cognitive walkthrough approach [11]
Supervised and Verifiable: Prêt a Voter [12]	yes	yes	SUS [13] and Modified UTAUT [14][1]
Compare : Frontend designs USA elections [15][16]	yes	No	Expert Reviews, Close Observation-video, Field Study,
Several paper ballot designs [17]	yes	No	SUS [13]
Compare: 2paper forms, punch card, lever machine [18]	yes	No	SUS[13]
Ballot Design [19][20]	yes	Limited	Analysis of unrecorded votes and the effect of ballot designs.
Supervised and Verifiable: Prêt a Voter [21]	no	Limited	Designed a game related to Prêt a Voter style ballots

Table 1 E-Voting Usability and Trust Studies

Table 1, summarizes the literature found in “Usability and/or Trust of E-voting Systems”. Note that most studies focused on “usability of the system” and used well known techniques such as cognitive walkthrough, SUS, and UTAUT. On the other hand, studies of “trust in the system” were limited. The authors of [19][20] focused on studying the effect of ballot designs on

[1] We could not find the modified UTAUT online

unrecorded votes which probably would affect trust in the system. In [21] focused on an end to end verifiable scheme: Prêt a Voter. In that scheme the ballot design has an effect on both privacy and verifiability. In [21] a game was designed to evaluate the understanding of the participants to the motivation behind such a ballot design.

3. OpenVote Version [I]

3.1 System Overview

The implementation provided in this document is based on the following voting protocols:

- Veto [5]: This protocol is used to build an election in which every voter has the right either to "veto" the election or not.
- Referendum [6]: By using this protocol one can build an election in which the participants have to decide between two possible options, which are normally "yes" or "no". At the end of the election every participant can tally the election.
- Multicandidate [6]: This protocol is used to build an election in which the participants have to vote for one of **n** possible candidates. At the end of the election, every participant counts the votes for each candidate. Every vote has the same weight.

All three protocols are based on a cryptographic concept referred to as multiparty computation described in Description 1. All known multi-party computations used in e-voting have at least two rounds. In the first round the voters share with each other enough information to setup the system. The second round is when participants broadcast an encryption of their votes. The information in the first round together with the information in the second round are computed in such a way that no one can decrypt the individuals' votes and everyone can compute the final result of the election. In other words, confidentiality of vote, fairness, dispute freeness, and self tallying are the security properties achieved.

A multi-party computation is a cryptographic protocol that enables several parties to compute a specific functionality (e.g. voting) over a set of inputs where each element of the set belongs to one of the parties. The protocol ensures that the inputs (e.g. votes) remain confidential to their owners while it guarantees that the output is known to all (e.g. results). The protocol assumes that no trusted third party exists.

Description 1 Multi-Party Computation

3.2 The Implementation of OpenVote Version [I].

The protocols mentioned above assume the existence of a fully connected network and authenticated (but not secret) channels between every participant. However, in the implementation, we eliminate the need of the fully connected network by introducing a server which is built under the “honest but curious” assumption. This assumption implies that the server will broadcast information it receives honestly but may try to break the privacy of the voters. The use of the server does not compromise any of the security properties previously described; this is true even if the server is curious.

In our implementation (Figure 1), the server is also responsible for creating the elections; nevertheless it is not authorized to participate in one.

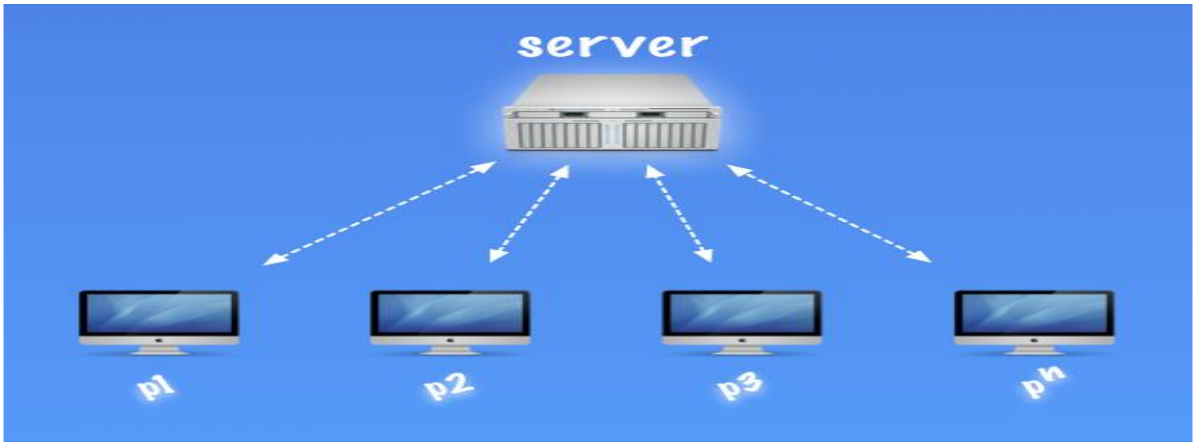


Figure 1 Client - Server Diagram with n voters connected to the server

For the implementation we used:

- Programming language: Python v2.7.3
- Graphical library: PyQt v4.4.10
- Cryptographic library: pyCrypto v2.6
- Experiment testing: Windows operating system

The following diagram (Figure 2) shows the interaction between the participants and the server from the implementation’s point of view.

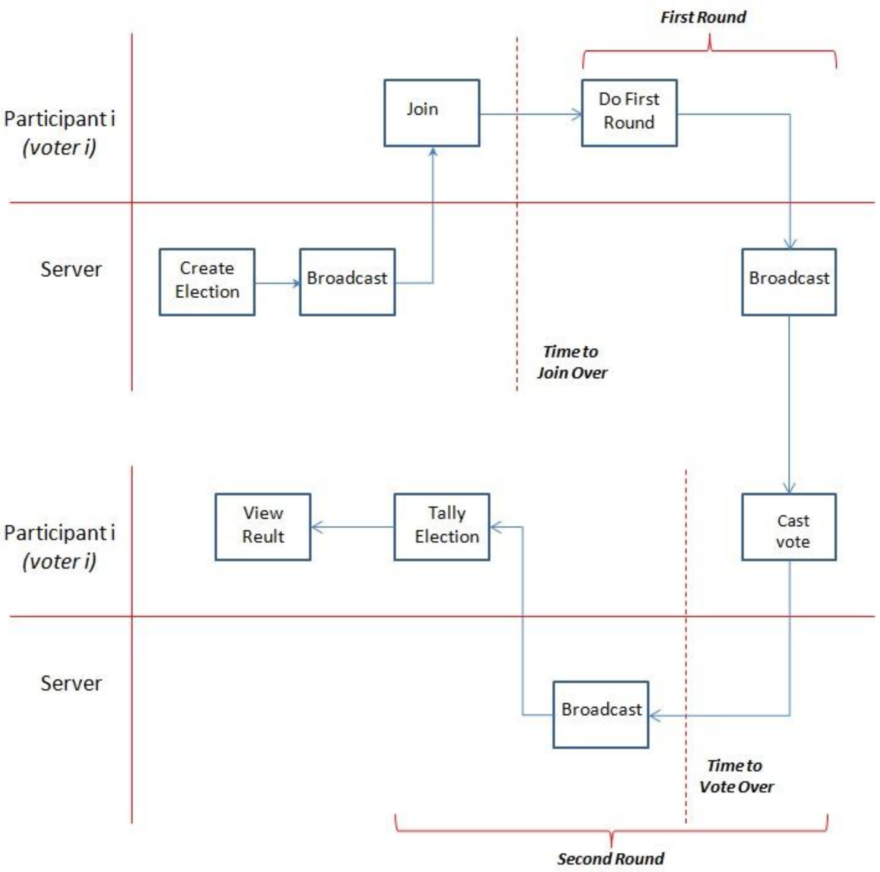


Figure 2 Procedure of the Election

Now we describe the actions needed for a participant who is using the application.

1. Login to the system: The user inputs his credentials and logins to the server (Figure 3).

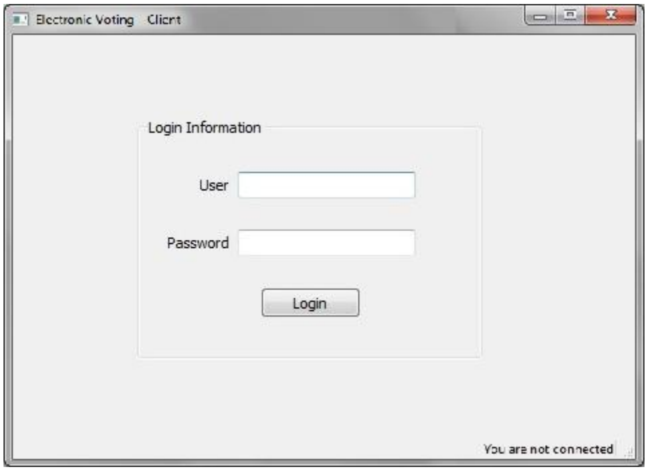
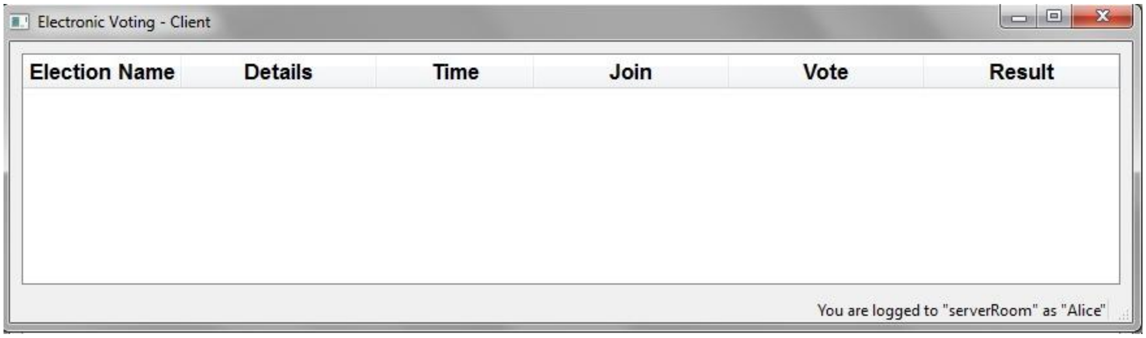


Figure 3 Login

2. Wait for upcoming elections: The participant is logged and waits for upcoming elections (Figure 4).


Electronic Voting - Client

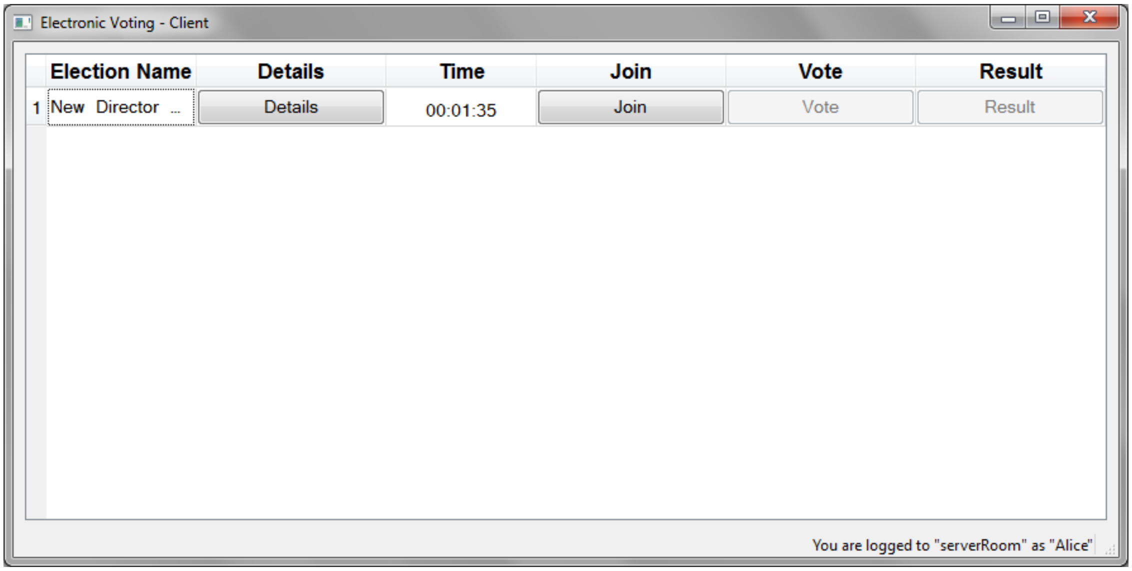
Election Name	Details	Time	Join	Vote	Result

You are logged to "serverRoom" as "Alice"

Figure 4 Participant logged in to the server

3. Decide whether to join or not the election: Once an election has been created, the participant can read the information related to the election and decide whether he wants to participate on the election or not (Figure 5).

   We introduce the term “Remaining Time to Join” which is the time given to the participants to join a certain election. Once this time is over, the participants execute the first round of the protocol.


Electronic Voting - Client

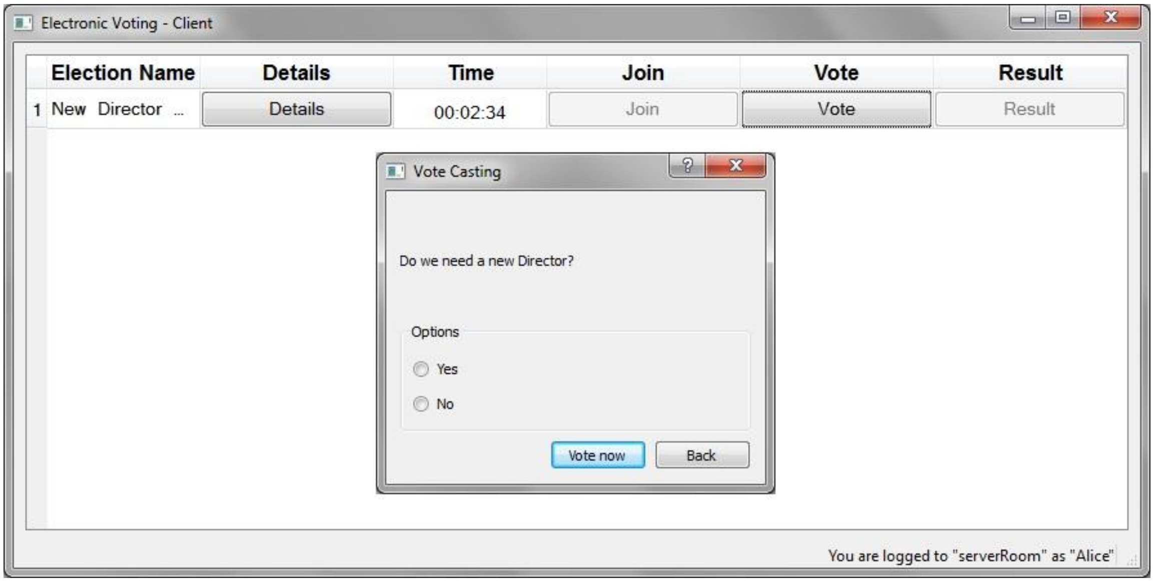
	Election Name	Details	Time	Join	Vote	Result
1	New Director ...	Details	00:01:35	Join	Vote	Result

You are logged to "serverRoom" as "Alice"

Figure 5 join the election

4. Cast the vote: Only the participants who joined an election are able to cast their vote.

   We introduce the term "Remaining Time to Vote" which is the time given to the participants to cast its vote. Once this time is over, the participants execute the second round of the protocol and the election finishes (see Figure 6).



	Election Name	Details	Time	Join	Vote	Result
1	New Director ...	Details	00:02:34	Join	Vote	Result

Do we need a new Director?

Options

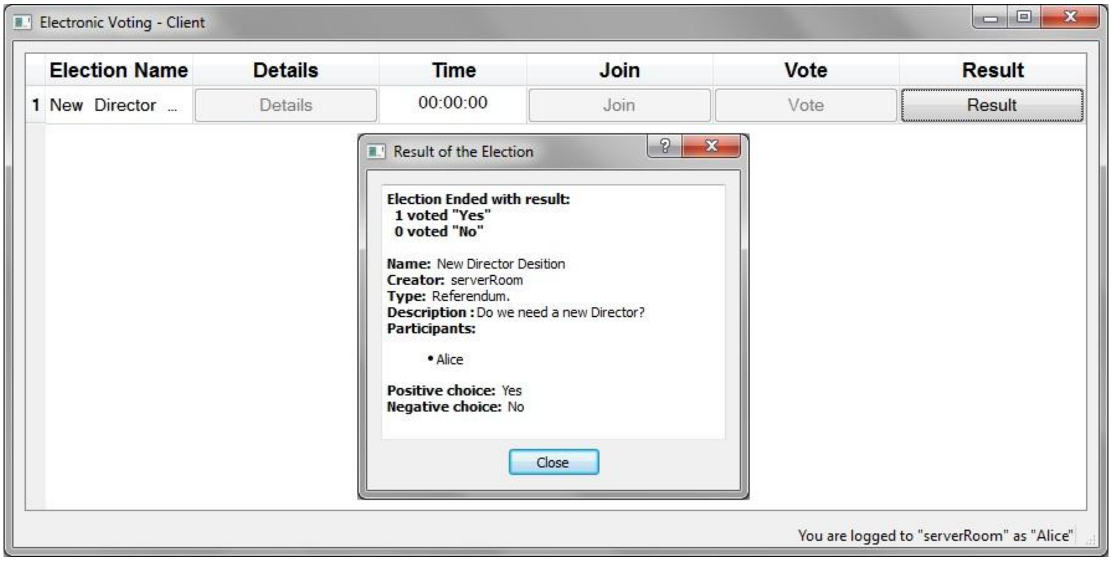
○ Yes

○ No

You are logged to "serverRoom" as "Alice"

Figure 6 cast the vote

5. Get the result: Once the election has finished, every participant who voted, can get the result of the election by clicking on the "Result" button (Figure 7).



	Election Name	Details	Time	Join	Vote	Result
1	New Director ...	Details	00:00:00	Join	Vote	Result

Election Ended with result:
1 voted "Yes"
0 voted "No"

Name: New Director Desition
Creator: serverRoom
Type: Referendum.
Description : Do we need a new Director?
Participants:

- Alice

Positive choice: Yes
Negative choice: No

You are logged to "serverRoom" as "Alice"

Figure 7 Result of the Election

4. Exploratory Study

4.1Overview of the Study

Our study took place within the context of a workshop on e-voting that was arranged at the university. The primary reason for doing this was so that those already with experience of e-voting platforms could provide feedback. This meant that the overall study could only take place within free time e.g. lunch or coffee breaks. The latter constrained our study to a maximum duration of 20 minutes, including the completion of all questionnaires. This had the disadvantage of it being a relatively short period of time but also in the case of the system we are testing is also quite relevant as the actual act of voting does not and should not take too long and also within the particular context the system should be as walk-up and use as possible without actual training or supervision. For example it would generally be considered unacceptable for an election official to stand over a voter and provide assistance.

Our study was primarily intended to assess the usability of the system in order to make further improvements; to assess whether the underlying voting protocol can be understood by users; and to start exploring aspects of trust around the system. Related to the latter point is how usability and trust affect one another and how trust may vary in accordance with the types of election undertaken.

4.2 Scenarios

Two scenarios were developed which were designed to explore different use cases. One scenario consisted of a single election while the second scenario consisted of two elections. There is no major difference in the tasks except that there are two elections in the second scenario, which requires a decision on which election to vote in first.

The first scenario asked people to login to the system (using an ID they were provided with) followed by asking them to vote on the location of the next workshop. This required them to both join and vote. We chose this particular election as it is relevant as well as important but not critical. After completion of the task they were asked to answer the following questions:

(i) At the end of the vote, how many people had voted?
(ii) What was the final result of the election?
(iii) Who is the creator of this election?

In order to encourage them to explore more of the interface they were asked to write down who else had voted in the election along with a guess as to how that person voted. This scenario can be thought of as the underlying learning task as it familiarizes users with the basics of the system.

The second scenario asked the participants to join and vote in two elections. One to decide on who to hire for a particular job and the other is on whether they believe e-voting should be used in a presidential election. These two scenarios were chosen as they represent more important decisions and theoretically would require voters to be more concerned in the trustworthy and secure nature of the system. Also while the act of joining and voting remains similar having two simultaneous elections makes the interface marginally more complex and introduces the possibility for usability problems to be experienced by end users. At the end of this vote they were asked three questions: (a) Have you managed to Join both? (b) Have you managed to Vote in both? (c) Did you think the time allocated for each is enough or too much?

The participants were asked to only view one scenario at a time and to indicate when they had completed their tasks. Only once all participants had completed the first scenario was the second one activated.

4.3 Questionnaire

We chose the SUS questionnaire [13] as the basis for the underlying usability test as it has also been used for testing more traditional voting methods [18]. Also as the system should be walk-up and use we were very interested in how quickly people perceived they could learn it and whether people would use it frequently. Both these issues are specifically addressed in the SUS questionnaire. SUS consists of 10 questions where participants are asked to respond on a five point likert scale, a list of the questions can be found in Table 2. A strongly agree is given a score of 5, and a strongly disagree a score of 1. The method itself focuses on overall themes of usability and does not encourage users to identify specific problems or other issues. Scoring was carried out based on the scheme proposed by [13].

	Item
1	I think that I would like to use this system frequently
2	I found the system unnecessarily complex
3	I thought the system was easy to use
4	I think that I would need the support of a technical person to be able to use this system
5	I found the various functions in this system were well integrated
6	I thought there was too much inconsistency in this system
7	I would imagine that most people would learn to use this system very quickly
8	I found the system very difficult to use
9	I felt very confident using the system
10	I needed to learn a lot of things before I could get going with this system

Table 2 the SUS Questionnaire

The second part of the questionnaire consisted of three sets of questions relating to: (a) Trust (b) Specific usability problems (c) Reasons they would not use the system.

For the trust questions were predominantly interested in exploring under what election conditions someone would use such a system. Our belief yet to be fully validated in our work is that such a system will be preferred under certain contexts. We explored this by asking people to respond on a likert scale as to what type of elections they would use such a system for example choosing: (a) A birthday present (b) A professional appointment (c) A local representative (d) Your next president.

In order to explore usability and trust we then asked the participants to list up to five aspects that are not user friendly and five other reasons they would not use such a system. In both cases they were informed that an answer was not required.

Data from the usability and trust questions were analyzed by two evaluators. After the first round of coding the data a meeting was held along with the system developer to discuss and agree on the topics identified. During phase two the comments were then placed into the mutually agreed groupings by one evaluator, although it remained open to them to adjust the groupings if required. Once this phase was completed the two evaluators agreed on the final groupings of the items (these can now be found in the results section). This approach ensured consistency as to how individual comments were coded as well as a method of agreeing on common themes.

4.4 Participants

A total of 28 participants took part, the ages ranged from 24 to 60. We had 11 participants who were also attending the parallel workshop on e-voting and their backgrounds ranged from cryptography to software engineering. Additionally, we had administration staff, PhD students and other researchers from our centre who worked on unrelated projects. In total data from 24 participants was analyzed (15 male and 9 female), we had to discard some people (4) as during one session the network connection failed causing the system to stop working.

4.5 Procedure

The study was administered in the following way: the evaluator provided an overview to the participants; the participants completed the informed consent form and their profile. They were then given scenario one to complete and asked to complete the scenario questions. After they had completed the scenario questions the second scenario would begin. On completion of the second scenario they complete the scenario questions. At the end they were asked to complete the questionnaire and then debriefed.

As the voting platform is intended to be used without prior training or much assistance from election officials participants were informed that they could not ask for assistance unless they experienced significant problems. Also as the voting concept is designed to support privacy they were told they should not confer during the study.

As votes involve groups of people we took the view that we should test the system with a small number of simultaneous users. Therefore all tests were conducted with 3-4 voters (we had limited available hardware) and one person acting as the election supervisor. The latter person only triggered the relevant scenarios when asked to do so and did not assume any other role or act out any particular aspects. In addition at least one evaluator was on hand to observe the study and took notes of any relevant events which occurred.

The procedure was extensively tested to conform not only to the 20 minute limit but also to remove obvious causes of problems, for example excessive waits during the election procedure or to improve the questionnaire. During this testing phase we managed to reduce the running time from 45 to 20 minutes.

4.6 Scenario Data

In the first scenario the time given to join the election was one minute and to vote another minute. Among the 24 participants 2 did not manage to join on time. In the second scenario we had two elections running at the same time, each of which was 45 seconds to join and another 45 seconds to vote. Two participants left the answers for this part empty. Three participants did not manage to join in time both elections; another participant joined in time but did not manage to vote in time. Three participants even though they joined and voted for both elections they thought time was tight. This leaves 15 participants out of 24 who joined both elections, voted in both elections and felt time was enough.

5. Results

5.1 Questionnaire – SUS (usability)

The SUS questionnaire has a predefined formula for assessing whether a system is usable. OpenVote [I] scored a mean of 61.45 (out of 100). The individual scores for each question are presented in Figure 8 and Figure 9. We should highlight that the overall SUS rating of 61.45 should be taken as the indication of how user friendly the system is and not individual questions, however the separate items are merely reported here to provide a greater insight as to areas of possible problem or concern.

In both Figure 8 and Figure 9 the higher the score the more the respondents agrees with the statement, so for example a high score in Figure 8 should be considered a positive reply whereas in Figure 9 it should be considered negative. It should be noted that the standard deviations for each item ranged from 0.82 to 1.2. In the following report “means” provide a starting point and should be read in conjunction with the “median” scores. Additionally we assume that a score of 2.5-3.5 +/- for the mean scores is in the neutral response category. Table 8 indicates that most participants were neutral to positive towards the OpenVote system, as most scores were in the 2.5 to 3.5 range. However, users indicated that they would be able to learn to use OpenVote quickly. The lowest mean score related to confidence in using the system, however again this was still within the neutral category. For the negative scores respondents disagreed with most of the statements (I.e. mean scores of <2.5).

The SUS score was approximately what was expected within the study, although when comparing it with data from [18] it scores slightly lower. Recall [18] compared lever and punchcard voting machines as well as paper methods such as arrow and bubble. Having said that, the sample populations of our studies and the studies in [18] are different. The work of [18] took place in the US where voters are more familiar with the systems used, where as in this study the group was from various countries and they were in general not familiar with the approach being used.

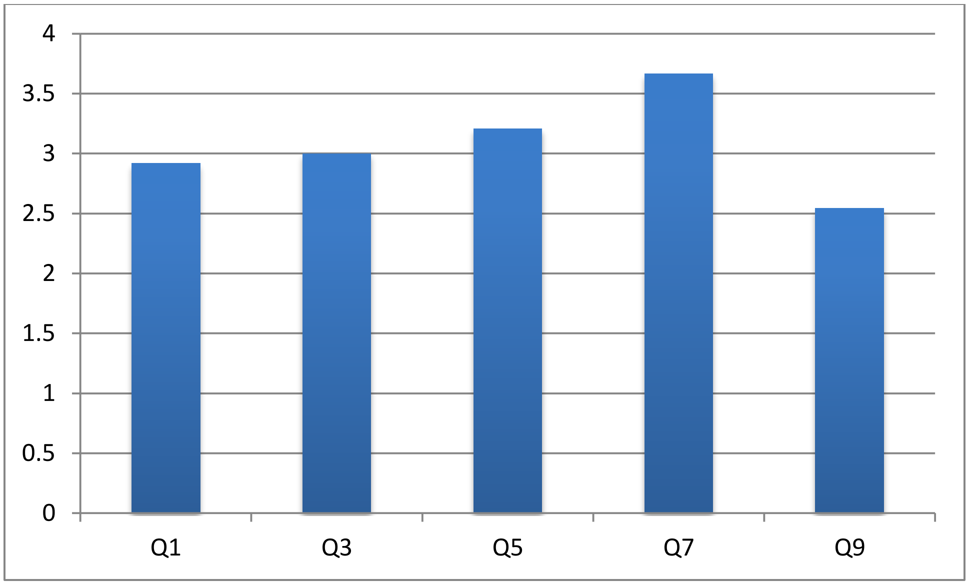


Figure 8 Average score for positive statements from the SUS Questionnaire.

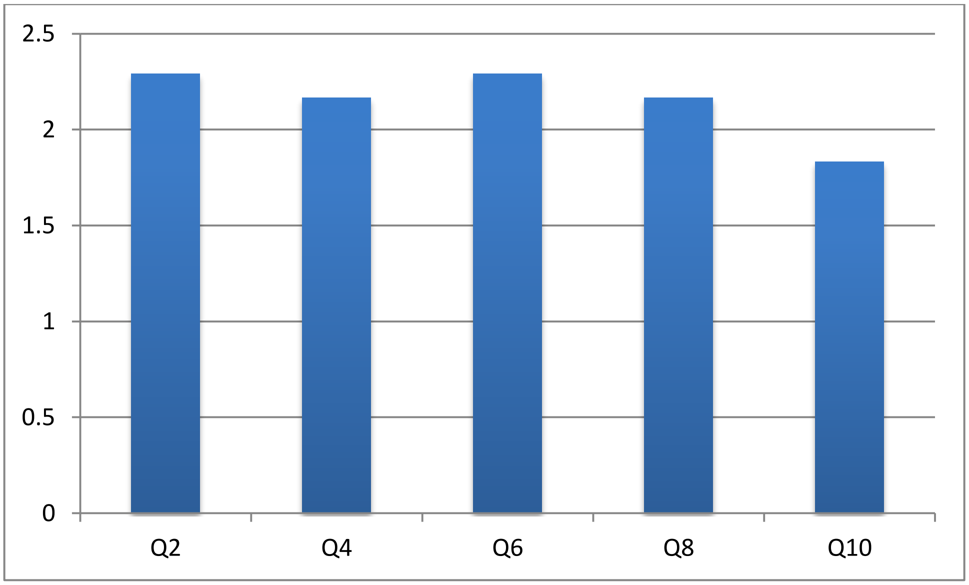


Figure 9 Average score for negative statements in the SUS questionnaire.

5.2 Usability issues

Topic	Issues	Total Instances /
Popups Dialogues	Design Too much scrolling & Information Displayed	10
Layout and Fonts	Layout/Size of buttons, Fonts too small	8
Training	System requires user training	4
Feedback	When joining election, and Generally in system	10

Table 3 Summary of basic usability issues identified

In total 63 comments relating to usability were identified from a total of 66 made under the usability question, we had to discard 3 comments as they were either positive statements or not relevant to usability. Based on our data analysis and discussions the following main categories of data were uncovered: user interface, procedure, usability & training and miscellaneous. As noted in the following section there are relationships between the different groups, for example there is a strong relationship between the use of a timer (on a usability level) and the overall procedure used to vote. Also the issue of feedback when joining an election is also related to the overall election procedure.

As can be seen from the Table 3 there are set of basic usability problems ranging from the dialogue boxes containing too much information through to poor layout and feedback when users undertake certain actions. These issues were highlighted by a number of people as outlined below:

> *"I have to scroll in the results window" (Participant, A30)*
>
> *"Too many message boxes" (Participant, A32)*
>
> *"I would like bigger buttons" (Participant, A8)*
>
> *"No acknowledgement after joining" (Participant, A19 & A24)*

Only a small number of comments indicated that users should receive training in order to use the system.

Topic	Issues	Total Instances
Timer Display	Display Procedure to take part	15
Overall voting procedure	Overall procedure Displaying of information relative to status	7
Presentation of information and functions	No graphical overview or results	3

Table 4 Summary of procedural usability issues identified

Problems relating to the timer used for the join and voting phases were the most remarked upon issue in the study (see Table 4 and comments below). Related to this was the overall procedure involved in voting also confused users. The presentation issues were grouped with this category as they related to seeing the results at the end of the election, however they are also related to presentational and usability issues.

In total issues relating to the timer and voting procedure accounted for over 33% of the total usability issues registered against the OpenVote platform.

> *“Red clock ticking” (Participant, A30)*
>
> *“No status information related to counter” (Participant, A27)*
>
> *“Not Clear What timer means” (Participant, A26)*
>
> *“Countdown not clear at start what it is needed for” (Participant, A20)*
>
> *“Which sequence you have to use -> steps” (Participants , A31)*
>
> *“Software should guide user “ (participant, A32)*
>
> *“No indication of when vote will arrive” (Participant, A19*)

Other issues

A total of six other issues were identified these ranged from the slowness of the system, through to anonymity issues and technical aspects.

5.3 Questionnaire – trust

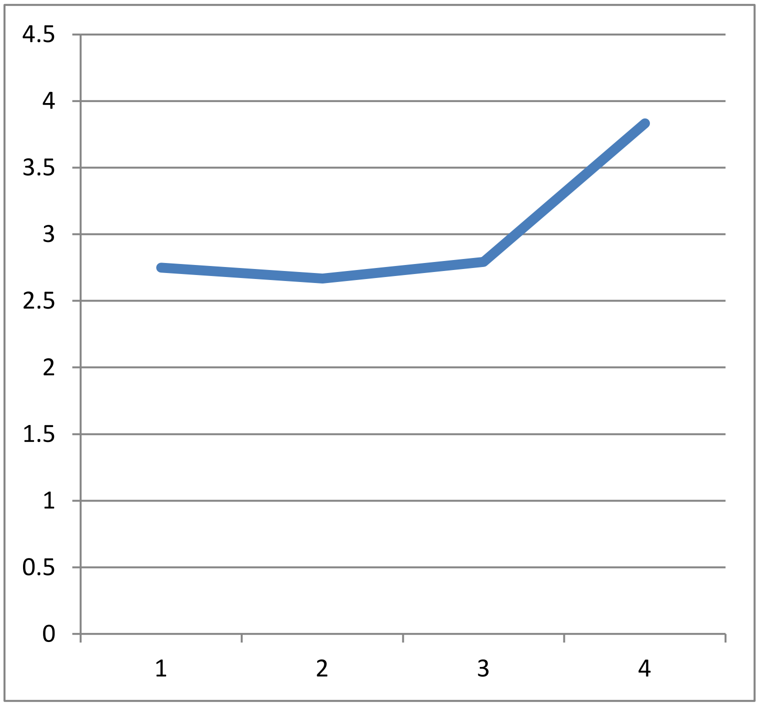


Figure 10 Mean ratings for the trust questions, the higher the score the less they agree with that option.

The questions on trust provided an insight into under what type of election conditions people would use such a system (Figure 10). In general people were neutral to positive when asked if they would use it for (1) deciding on a birthday present (mean=2.75/median=2.5), (2) a professional appointment (mean=2.66/median=2) or (3) local representative (mean=2.79/median=2). However, the participants indicated they would not use it for (4) choosing their next president (mean=3.83/median=4). The median scores point to a slightly more positive tendency for most of the questions with the exception of the last one where the score is more negative. Again though the standard deviations for each question were in the range of 1.22 to 1.67 and indicate that the results should be treated with some caution.

5.4 Other issues

In the questionnaire we asked the participant the following: "Ignoring usability issues please list *up to* five reasons why you would NOT USE such a system, if there are none, do not list any." This free response section was designed to capture their main concerns.

The participants have left 53 comments altogether, 3 of which were related to the timer display and the button layout. Based on our data analysis and discussions the non-usability issues can be categorized as follows: Transparency & Accountability, Privacy, Trusting Technology and Entities involved, Verifiability and finally User Context.

Topic	Issues	Total Instances
Trusting Technology	These were issues related to trusting the hardware, software or Network	4
Trusting Entities	Trusting the election official and other voters	6
Transparency and Accountability	Wanting to understand the infrastructure and security behind the system	15

Table 5 Trust issues identified in free responses

As seen in the above table trust issues varied in the system. Some participants had problem with trusting the entities involved and/or technology used. We highlight a few of the comments regarding that:

“Machine will learn my vote” (Participant A9)

“Voting Software is run on a potentially compromised machine” (Participant A19)

“Lack of confidence on election managing authority” (Participant A33)

“Legitimacy of other voters not sure” (Participant A22)

Topic	Issues	Total Instances
Privacy	Vote confidentiality	5
Verifiability	Vote been counted, Tallying is correct	8

Table 6 Privacy and Verifiability issues in the free responses section.

Other participants felt that they need to know more about the infrastructure and security measures used in the system before trusting it. Examples:

“I need to find more about the infrastructure and security” (Participant A25)

“No information about how data is encrypted/protected” (Participants A19, A9)

“If I don’t understand it, I won’t use it” (Participant A31)

“How do I identify responsibility in case something goes wrong” (Participant A6)

Security issues highlighted can be divided into privacy and verifiability as shown in Table 6.

“Not confident with Confidentiality of Vote” (Participant A13)

“No proof that my vote has been counted correctly” (Participant A19, A30, A21)

“Unclear which measures ensures that my vote has been counted as intended” (Participant A27)

“Can’t See tallying process” (Participant A7)

Finally user context was one of the main concerns of the participants (see Table 7).

Topic	Issues	Total Instances
Used Context	Mentioning elections they would use it for	4
Passed Experience	User Perception ideas on voting and e-voting	2
Complexity	Guidelines, training, education, etc	5

Table 7 Additional Free From Responses

“Not Presidential Elections” (Participant A12, A21)

“Fear of Change” (Participant A21)

“Not as straight forward as usual voting” (Participant A14)

“Unnecessary Complex” (Participant A22)

“Requires Prior Guidelines” (Participant A14)

The non-usability issues can be summarized into three main categories: trust, security and user Context.

6. Discussion

We will not concentrate on the basic usability issues such as font sizes or scrolling as these can be changed comparatively easily. Instead what is far more relevant for the current study and future work are issues relating to conceptual models related aspects of the voting method, its associated procedure and aspects of verifiability and trust.

The results point to the participants finding it difficult to understand the steps involved in using the system and related to that the use of the timers. This was indicated within the raw comments provided as well as the data relating to scenario completion. For example many participants did not like the idea of or understand why they needed to wait to join or to vote in an election. However, this is a key part of the cryptographic protocol that is used within the system. Moreover, some participants did not like the fact that the time was as a countdown and was alerting. Therefore a challenging aspect of developing a boardroom voting system is to present the two “waiting periods” in such a way that the users can understand the reason why or to redesign the system so that one or both of these phases is no longer as apparent to the user. However, it is worth pointing out that the short time given to the users may be a result of the particular scenario and that during the pilot phase longer time periods were deemed as also being a problem.

Related to the time issue was the overall understanding of the electoral procedure. This was highlighted within the raw usability comments but also to some extent within the other issues section. For example, they found the flow of actions confusing and lack of feedback or status information also compounded this problem. They also pointed to a need for training or guidance in order to make the steps involved clearer. This also may explain the non-completion of some scenarios by end users. It is important to note that unlike other computer systems which may rely on social help (e.g. from others who can stand over first time users) voting systems such as the one here should be walk-up and use ***without the need*** for someone to watch over and assist the voter.

Data from the other issues comments points to the participants preferring a more transparent system where they would be more aware of what was going on behind the scenes; this may be due to the nature of the user base which was largely drawn from the e-voting community.

A key part of the proposed system was the lack of a central server or election authority and the concept of self-tallying between voters; the main aim being to reduce the possibility for corruption. Indeed this is a key part of the underlying protocol. This desirable aim seems to conflict with the conceptual view of the system held by the participants, who continued to view the system as having a central point where they did not trust the server or its administrator. It should be pointed out that we did not inform the participants beforehand of the architecture of the system and this in part may explain the confusion. This was deliberate as we were seeking to identify further issues to be addressed. However, the findings point to the need either to explain in advance how such a system operates (behind the scenes) or to understand that voters still perceive there will central voting authority or server (even if there is not one). This requires further investigation as it clearly has an impact on the perceived trust of the system. For example it could be that there is a need to provide a publically acceptable way of verifying and tallying the votes that makes it clear that the vote has been cast, was received as intended and been counted correctly.

Participants trust in voting systems is essential for public confidence but as we found trust is relative to the underlying context of use. This was reflected in the trust questionnaire section that such a system was acceptable for use in low importance elections but not for presidential elections. This is no doubted related to many factors from the underlying protocol, its implementation in OpenVote through to the underlying verifiability and transparency issues. The precise link between these aspects again requires further consideration but is certainly a key element in deciding what voting system to use within a given context.

7. Designing the Questionnaires

Given the outcome of our experiments we designed the questionnaires provided in the appendices. Our primary focus within the questionnaire was to capture the users' perception of trust related issues, although we also included usability questions which are relevant to e-voting in general. We tried where possible to make the questionnaire usable out with the specific OpenVote context from which it was devised so that it can possibly be validated when used with other systems. The questionnaire uses a set of five point likert scales coupled with a selection of yes/no questions, multiple choice answers and free form responses.

The first part of the questionnaire focuses on issues relating to the vote cast by the individual ranging from whether it was counted correctly through to whether they have confidence in the anonymity of their vote and also in the verification process. As SUS only provides a very general overview of usability we felt that the method lacked clarity with respect to specific voting related phases, e.g. joining and election, voting, counting the ballots (tallying) and verification. Therefore a set of questions relating to these areas was included. We further enhanced the questionnaire by adding in usability related questions relating to the number of steps involved and their sequence. A question on verification was also added and additionally we asked them how they had verified their vote. We were also interested in seeing under what used context they would consider using such a system, for this a set of questions were asked relating to whether they would use such a system within a range of different votes. Our primary interest here was to see confidence in use of the system across domains. As this is early work we acknowledge that the proposed domains should probably be changed for other voting systems or in other studies. Finally the questionnaire asks people to provide the five features/aspects they like or disliked most followed by a request for 30 words (about anything relating to the experience).

8. OpenVote Version [II]

8.1 System Overview

The implementation provided in this document is based on (Khader, et al., 2011) voting protocol which is a multiparty computation (See description 1). This means that the protocols have to be executed in two rounds as in OpenVote [I]. The protocol can also have extra rounds of recovery in case one of the voters drops out before submitting their votes to the rest of the group. In our implementation we allow the recovery round to take place when we have more than 50% of the participants have submitted their votes.

8.2 Implementation of OpenVote Version [II]

We present an implementation of the voting protocol provided by (Khader, et al., 2011). The network implementation is similar to it in OpenVote [II]. OpenVote [II] is designed as a wizard to be run per election. The wizard has the following workflow:

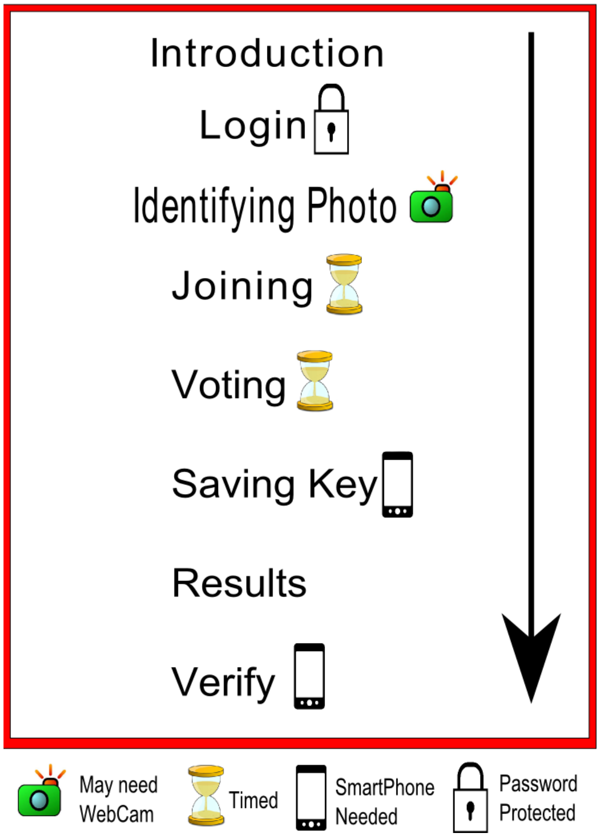


Figure 11. OpenVote flow

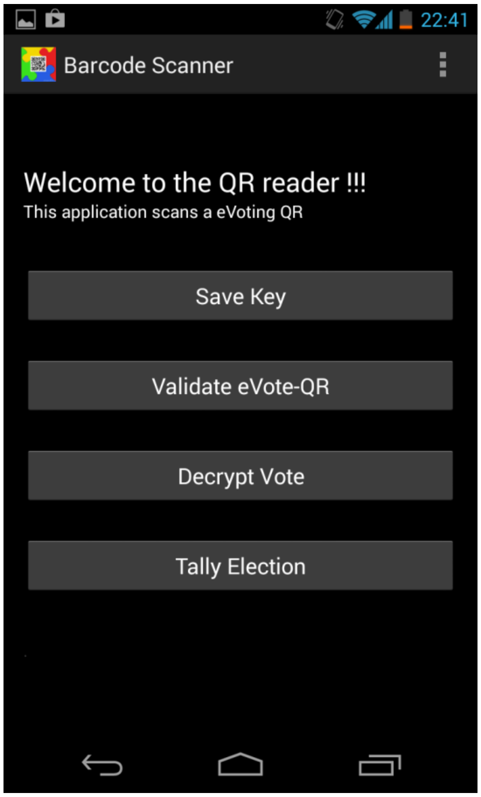
Additionally to the wizard interface, we also developed an android application with the aim of increasing the trust of the user in our system. We name this application “Barcode Scanner”. A user who is suspicious about system could use his smart phone and our android application to:

- Verify the integrity and confidentiality of his vote
- Verify his vote was counted
- Tally the election

We describe the functionalities of the Barcode Scanner application:

- Save secret-key: Reads a QR code containing the secret-key of the participant. This is used later on to allow the participant to decrypt his own vote.
- Validate e-Vote: Reads a QR code and verifies that it contains a valid “Open Vote” vote.
- Decryption of Vote: When the user has voted, he is given his vote in a QR code format. If he has saved his secret-key, he can use it to decrypt his vote and verify it was casted as intended.
- Tally Election: The participant tallies the election by scanning (all together at the same time) the votes of the participants presented as QR codes.

Next figure shows the main menu of the Barcode Scanner application.



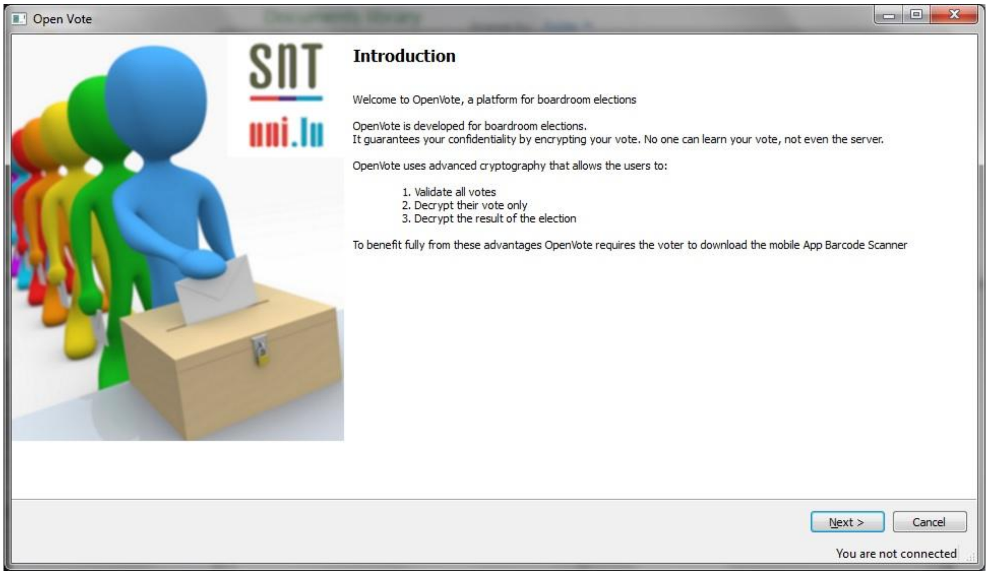
Welcome to the QR reader !!!

This application scans a eVoting QR

Figure 12. Barcode Scanner menu

Now we describe the most important actions needed for a participant who is using the OpenVote application, during execution of this wizard the participant is required to use his smart phone containing the Barcode Scanner app.

1. The participant gets an introduction about OpenVote.



Introduction

Welcome to OpenVote, a platform for boardroom elections

OpenVote is developed for boardroom elections.
It guarantees your confidentiality by encrypting your vote. No one can learn your vote, not even the server.

OpenVote uses advanced cryptography that allows the users to:

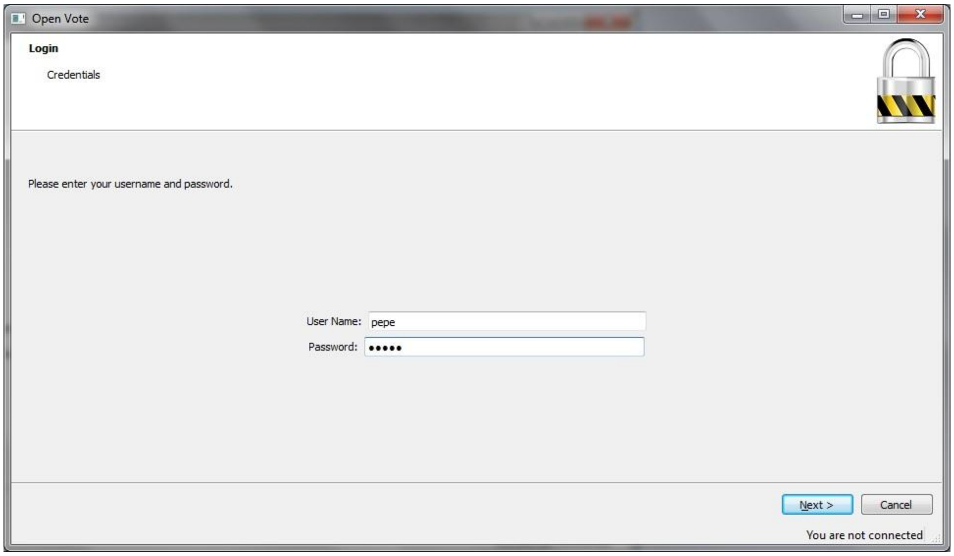
1. Validate all votes
2. Decrypt their vote only
3. Decrypt the result of the election

To benefit fully from these advantages OpenVote requires the voter to download the mobile App Barcode Scanner

You are not connected

Figure 13. OpenVote - Introduction page

2. The participant inputs his credentials to login.



Login

Credentials

Please enter your username and password.

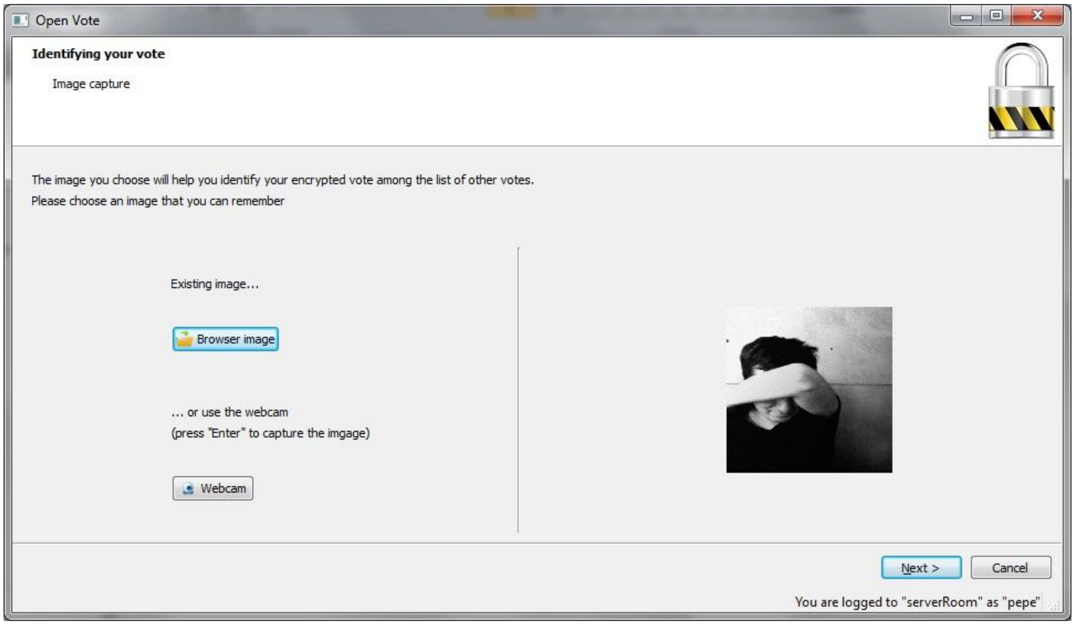
User Name: pepe

Password: •••••

You are not connected

Figure 14 Login Page

3. The participant has to either browse for an image or use the webcam to take a picture. This image will be used to identify ones vote among the list of votes when the results are announced.



Identifying your vote

Image capture

The image you choose will help you identify your encrypted vote among the list of other votes.
Please choose an image that you can remember

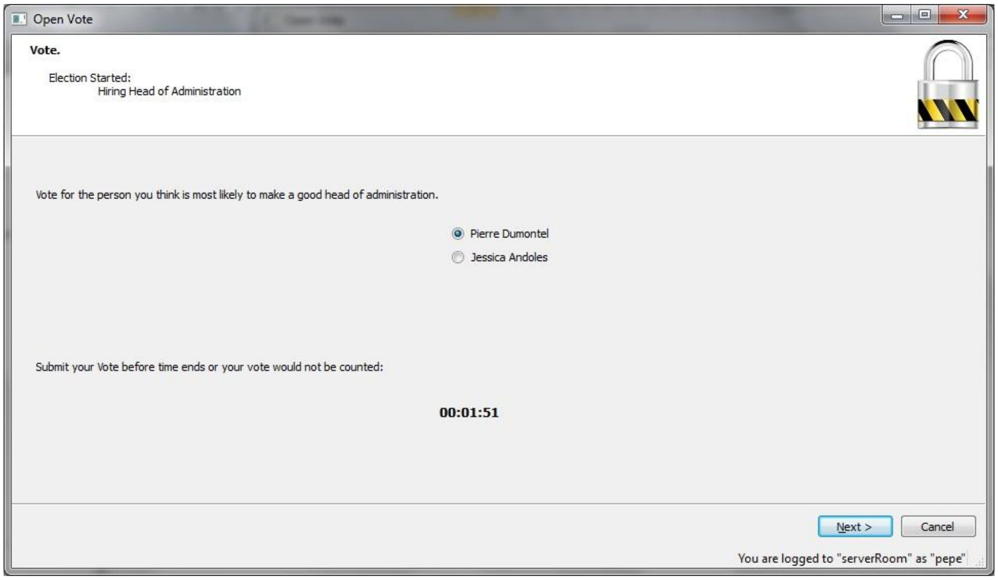
Existing image...

... or use the webcam
(press "Enter" to capture the imgage)

You are logged to "serverRoom" as "pepe"

Figure 15. OpenVote - upload image

4. The participant is given a time period to decide whether he wants to join the election or not (first round of the voting protocol). If the participant joins the election, he needs to wait until the time to join is over to continue the wizard. If the participant does not join the election, he is not required to do any further actions and the application finishes.
5. Once the time to join is over, the participants who joined the election are given second period of time to submit cast their vote (second round of the protocol).



Vote.

Election Started:
Hiring Head of Administration

Vote for the person you think is most likely to make a good head of administration.

● Pierre Dumontel
○ Jessica Andoles

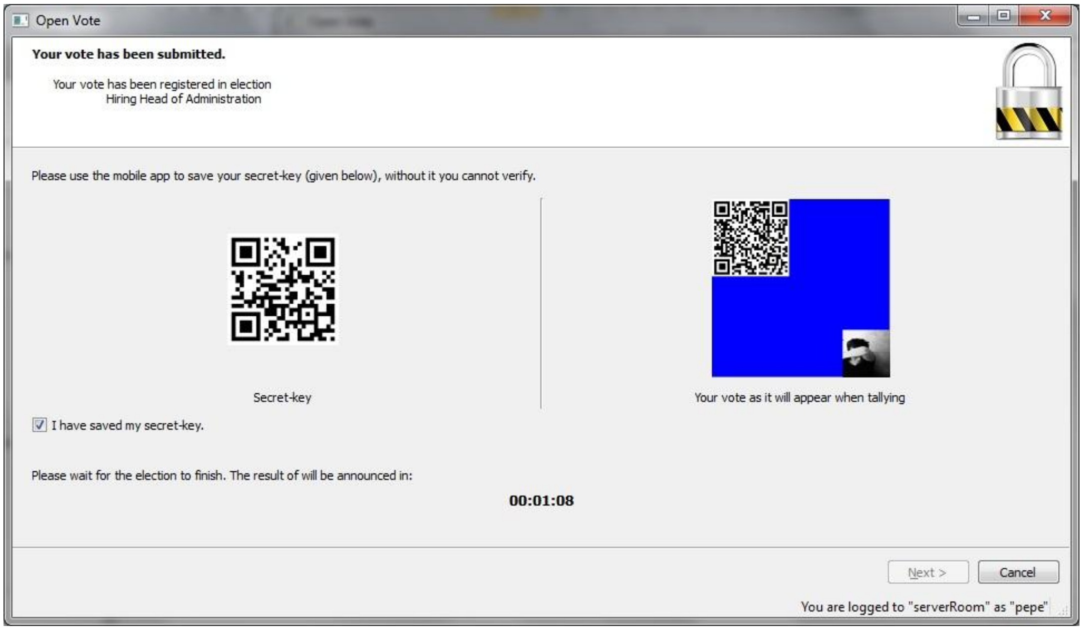
Submit your Vote before time ends or your vote would not be counted:

00:01:51

You are logged to "serverRoom" as "pepe"

Figure 16. OpenVote- vote submission

6. Once the participant has submitted his vote, he is given the following:
   a) A QR code as a secret-key to decrypt his vote. He needs to use his smart phone and "Barcode Scanner" application to scan it and save it.
   b) A graphical representation of his vote. This is how the vote of the participant is publicly displayed when the results are announced. This image contains the picture the participant uploaded in step 3 and a QR code containing his encrypted vote. Once he has saved his secret-key, he could the "Barcode Scanner" application to decrypt his vote and verify it was casted as intended.



Your vote has been submitted.

Your vote has been registered in election
Hiring Head of Administration

Please use the mobile app to save your secret-key (given below), without it you cannot verify.

Secret-key

Your vote as it will appear when tallying

☑ I have saved my secret-key.

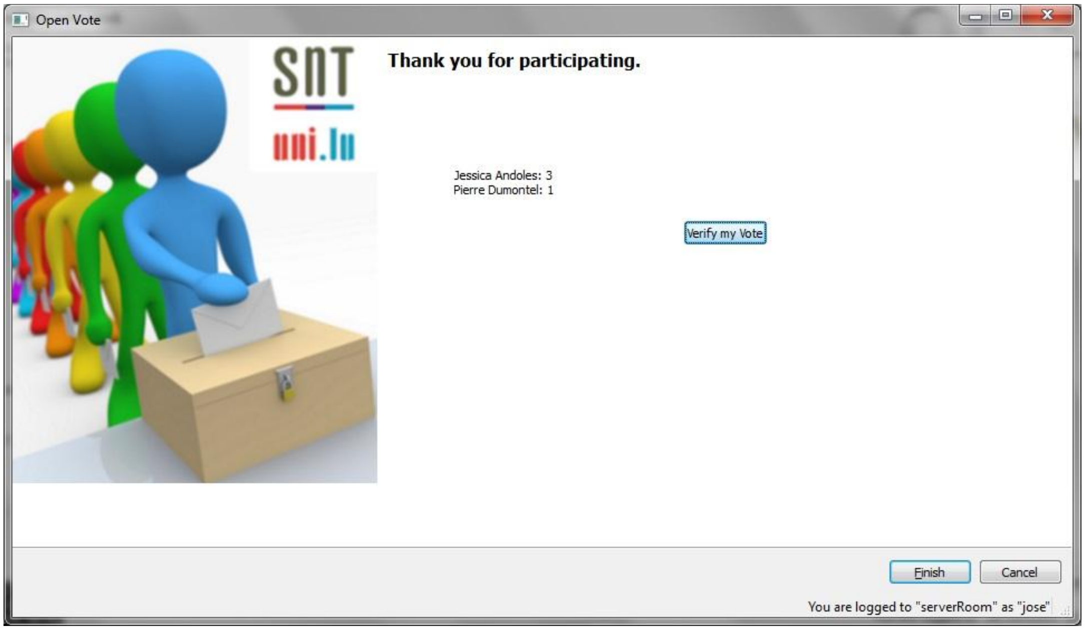
Please wait for the election to finish. The result of will be announced in:

00:01:08

You are logged to "serverRoom" as "pepe"

Figure 17. OpenVote - secret key and vote as QR codes

7. When the time to vote passes, the results are announced as text on the screen of every participant.



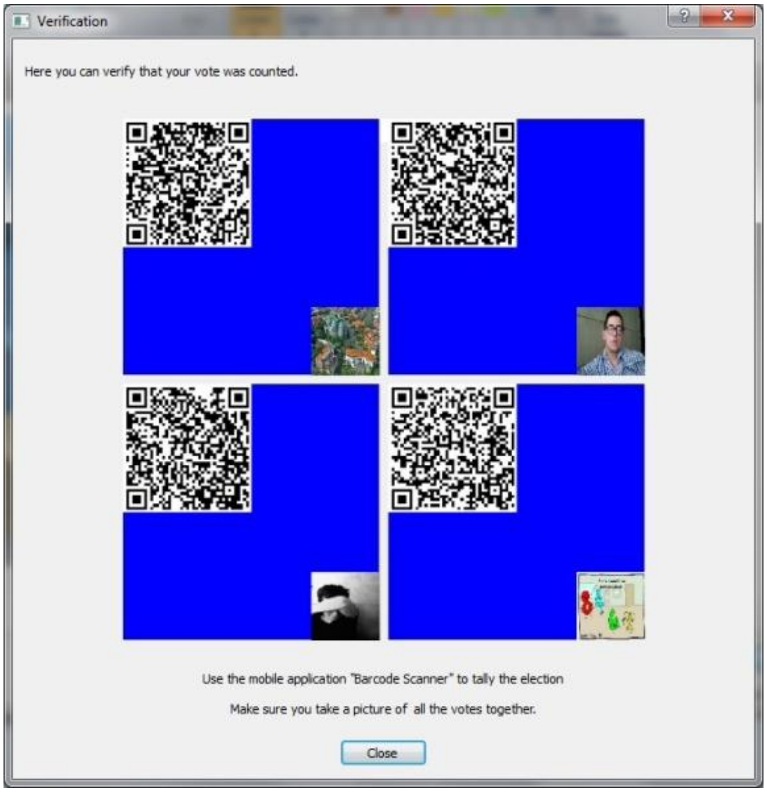
Thank you for participating.

Jessica Andoles: 3
Pierre Dumontel: 1

You are logged to "serverRoom" as "jose"

Figure 18. OpenVote - result of election

8. Additionally, when the results are announced, the votes of every participant are put together and displayed on a projected screen in the room (so every user sees the same image) The same picture is displayed on the screen of every participant.



Verification

Here you can verify that your vote was counted.

Use the mobile application "Barcode Scanner" to tally the election

Make sure you take a picture of all the votes together.

Figure 19. OpenVote – votes together

A participant can use this graphical representation of the votes and the "Barcode Scanner" application to decrypt his vote, verify the correctness of every vote and finally tally the election.

9. Real Study

We conduct the real study on 32 participants in total after having run pilot studies over 11 participants. The study was a comparison study between OpenVote Version [II] and Paper Based Elections**.**

The details of this study and the overall results will be published in a separate paper. This technical report presents the SUS results only.

9.1 SUS RESULTS

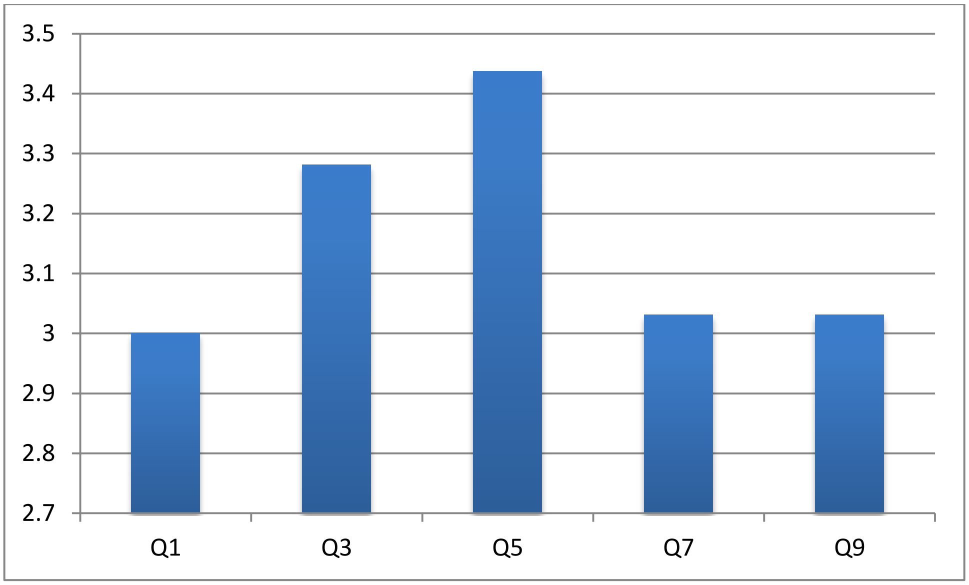


Figure 20 SUS Results for Positive Statements

The results in Figure 20 point to users generally being neutral (mean score 2.5<3.5) towards OpenVote [II] when presented with the SUS positive statements. The same situation applies to negative statements, although interestingly they disagreed when asked if they needed to learn a lot before they could use the system. Overall the second version of OpenVote scored an average of 57.1875 which is marginally less than the first version.

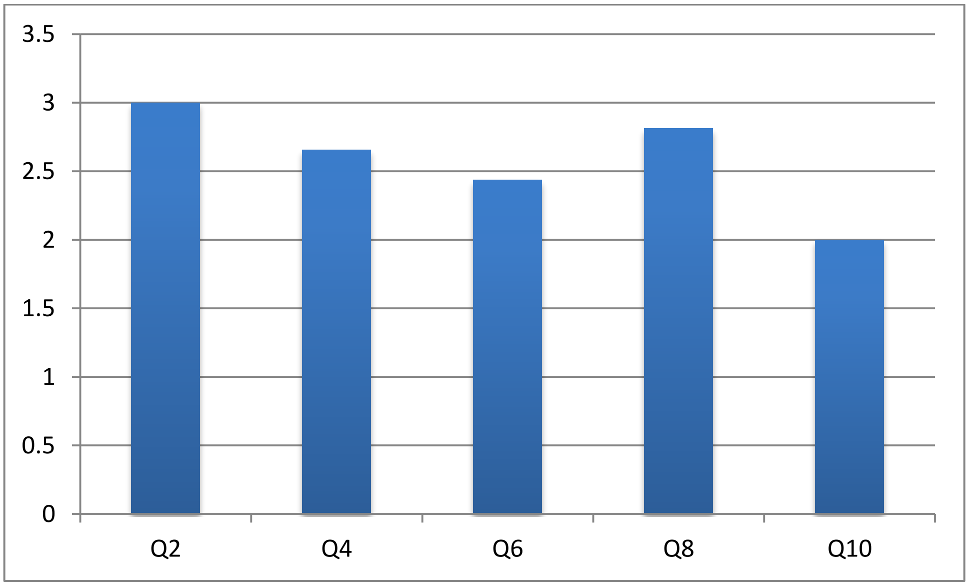


Figure 21 SUS Negative Statements

10. Conclusion

In conclusion we have presented study of usability and trust of a boardroom voting system. Our primary objectives were to improve the existing system and to uncover areas which require further examination. Findings of the Exploratory Study can be summarized as follows:

- The flow of the election procedure and how easy this is for voters to understand is very important
- Voters require a clear explanation of how the underlying system works or they will lack trust in the system or alternatively interfaces should be designed in such a way as to alley these fears.
- There seems to be a perception of their always being a trusted server or election official; even when there is none. This again undermines confidence in the system.
- Compelling voters to join an election within a specified time is not a good option
- Trust is a relatively transient concept and the perceived level of trust varies with the proposed election type e.g. relatively minor through to ones of national importance.

Our study presents resulted in a new version of OpenVote and in a general questionnaire that can be used in evaluating any verifiable voting scheme. The findings of our second study are to be published in a second paper; however we summarize the results of the SUS of OpenVote [II].

Acknowledgement

Special thanks to Dr. Lancrenon and Prof Ryan, for their support. Furthermore, we would like to thank all the participants involved in the experiments conducted.

Bibliography

[1] P. Y. Ryan, "A variant of the chaum voting scheme.," Technical Report, Newcastle, 2004.

[2] P. Y. Ryan and V. Teague, "Pretty Good Democracy," Security Protocols XVII, 2008.

[3] B. Adida, "Helios: web-based open-audit voting," San Jose, CA, USA, 2008.

[4] J. Groth., "Efficient maximal privacy in boardroom voting and anonymous broadcast," in *FC*, 2004.

[5] F. Hao and P. Zielinski, "A 2-Round Anonymous Veto Protocol," SPW Cambridge, 2006.

[6] D. Khader, B. Smyth, P. Y. A. Ryan and F. Hao, "A Fair and Robust Voting System by Broadcast.," Evote, 2011.

[7] A. Kiayias and M. Yung, "Self-tallying elections and perfect ballot secrecy.," PKC, 2002.

[8] P. Y. A. Ryan and S. A. Schneider, "Prêt à Voter with Re-encryption Mixes," ESORICS, 2006.

[9] B. Adida, Advances in cryptographic voting systems, PhD ed., MIT: Thesis, 2006.

[10] F. Karayumak, M. M. Olembo, M. Kauer and M. Volkamer, "Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System," USENIX, 2011.

[11] D. Stone, J. Caroline, W. Mark and M. Shailey, User Interface Design and Evaluation (Interactive Technologies), 1 ed., Morgan Kaufmann , 2005.

[12] W. Marco, B. Regina, P. Philippe, L. David, L. Kieran, R. Peter, A. Eugenio and S. Lorenzo, "Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter," ICEGOV, 2009.

[13] J. Brooke, "SUS: A quick and dirty usability scale," 1996.

[14] V. Viswanath, G. M. Michael, B. D. Gordon and D. D. Fred, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly ,* vol. 27, no. 3, pp. 425-478 , 2003.

[15] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson and R. G. Niemi, "Electronic Voting System Usability Issues," CHI Proceedings of the SIGCHI conference on Human factors in computing systems, 2003.

[16] P. S. Herrnson, O. G. Abbe, P. L. Francia, B. B. Bederson, B. Lee, R. M. Sherman, F. Conrad, R. G. Niemi and M. Traugott, "Early Appraisals of Electronic Voting," *Social Science Computer Review,* vol. 23, no. 3, pp. 274-292 , 2005.

[17] S. P. Everett, M. D. Byrne and K. K. Greene, "Measuring The Usability of Paper Ballots: Efficiency, Effectiveness and Satisfaction.," 2547–2551, 2006.

[18] D. B. Michael, K. G. Kristen and P. E. Sarah, "Usability of voting systems: Baseline data for paper, punch cards, and lever machines," 2007.

[19] D. Kimball and M. Kropth, "Ballot Design and Unrecorded Votes on Paper-Based Ballots," *Public Opinion Quarterly,* vol. 77, no. 2, 2013.

[20] D. C. KIMBALL and M. KROPF, "BALLOT DESIGN AND UNRECORDED VOTES ON PAPER-BASED BALLOTS," Vol. 69 4, 2005.

[21] L. Morgan, S. Steve, X. Zhe, C. Chris, H. James, R. Peter Y.A. and S. Shriramkrishnan, "Testing Voters' Understanding of a Security Mechanism Used in Verifiable Voting," *JETS,* vol. 1, no. 1, 2013.

[22] F. Hao, P. Y. A. Ryan and a. P. Zielinski, "Anonymous voting by two-round public discussion.," *Journal of Information Security,* vol. 4, no. (2), pp. 62-67, 2010.

Appendix

Paper Based Questionnaire

1. I am confident my vote has been counted as cast.

Strongly Agree				Strongly Disagree

2. I am confident that the other voters do not know how I voted unless we voted the same way.

Strongly Agree				Strongly Disagree

3. I am confident that all votes cast by all voters have been counted correctly.

Strongly Agree				Strongly Disagree

4. I am confident that the person placing the votes on the wall is unaware of how I voted

Strongly Agree				Strongly Disagree

5. I found the process of joining an election easy.

Strongly Agree				Strongly Disagree

6. I found the process of voting in an election easy.

Strongly Agree				Strongly Disagree

7. I found the process of finding out the election result (tallying) easy.

Strongly Agree				Strongly Disagree

8. I found the process of verifying *if my vote* was counted correctly easy.

Strongly Agree				Strongly Disagree

9. The sequence of steps involved (joining, voting, tallying and verifying) was logical

a.YES
b. N0

10. Have you verified (checked) your vote on the board?

a.YES
b. N0

Why?……………………………………………………………………….

11. In relation to the sequence of steps involved I felt that there were:

a. Too many steps involved
b. Too few steps involved
c. The right number of steps involved

12. Assume you are a member of parliament, please indicate your view on the following statement: “I would use Paper Based to vote on a new law”

Strongly Agree				Strongly Disagree

13. You are on a committee who decides to give a national award e.g. actor of the year. Please indicate your view on the following statement: “I would use Paper Based voting to vote for actor of the year”

Strongly Agree				Strongly Disagree

14. You are on the board of directors for a company and have to decide on an important business decision e.g. hiring more staff. Please indicate your view on the following statement: “I would use Paper Based Voting to make a business decision”

Strongly Agree				Strongly Disagree

- Please list the five aspects you most liked about Paper-Based Voting:
- Please list the five features you liked least about Paper-Based Voting:
- Using no more than around 30 words please write down anything about your experience of using Paper-Based Voting

OpenVote Questionnaire

1. I think that I would like to use OpenVote frequently

Strongly Agree				Strongly Disagree

2. I found OpenVote unnecessarily complex

Strongly Agree				Strongly Disagree

3. I thought OpenVote was easy to use

Strongly Agree				Strongly Disagree

4. I think that I would need the support of a technical person to be able to use OpenVote

Strongly Agree				Strongly Disagree

5. I found the various functions in OpenVote were well integrated

Strongly Agree				Strongly Disagree

6. I thought there was too much inconsistency in OpenVote

Strongly Agree				Strongly Disagree

7. I would imagine that most people would learn to use OpenVote very quickly

Strongly Agree				Strongly Disagree

8. I found OpenVote very cumbersome to use

Strongly Agree				Strongly Disagree

9. I felt very confident using OpenVote

Strongly Agree				Strongly Disagree

10. I needed to learn a lot of things before I could get going with OpenVote

Strongly Agree				Strongly Disagree

11. I am confident my vote has been counted as cast.

Strongly Agree				Strongly Disagree

12. I am confident that the other voters do not know how I voted unless we all voted the same way.

Strongly Agree				Strongly Disagree

13. I am confident that all votes cast by all voters have been counted correctly.

Strongly Agree				Strongly Disagree

14. I am confident that the system is unaware of how I voted.

Strongly Agree				Strongly Disagree

15. I found the process of joining an election easy.

Strongly Agree				Strongly Disagree

16. I found the process of voting in an election easy.

Strongly Agree				Strongly Disagree

17. I found the process of finding out the election result (tallying) easy.

Strongly Agree				Strongly Disagree

18. I found the process of verifying *if my vote* was counted correctly easy.

Strongly Agree				Strongly Disagree

19. The sequence of steps involved (joining, voting, tallying and verifying) was logical (please circle):
    a.YES
    b. N0

20. Have you used the projected screen for either verification, validation or tallying (counting):
    a. YES
    b. N0

    Why?……………………………………………………………………

21. In relation to the sequence of steps involved I felt that there were (please circle):
    a. Too many steps involved
    b. Too few steps involved
    c. The right number of steps involved

22. Assume you are a member of parliament, please indicate your view on the following statement: “I would use OpenVote to vote on a new law”

Strongly Agree				Strongly Disagree

23. You are on a committee who decides to give a national award e.g. actor of the year. Please indicate your view on the following statement: “I would use OpenVote to vote for actor of the year”

Strongly Agree				Strongly Disagree

24. You are on the board of directors for a company and have to decide on an important business decision e.g. hiring more staff. Please indicate your view on the following statement: “I would use OpenVote to vote on a business decision”

Strongly Agree				Strongly Disagree

- Please list up to five aspects you most liked about OpenVote:
- Please list up to five features you liked least about the OpenVote:
- Using around 30 words please write down anything about your experience of using OpenVote