Voter Perception of Cast-as-Intended Verifiability in the Estonian I-Vote Protocol

Tobias Hilt[1] Kati Sein[2] Tanel Mällo[3] Jan Willemson [4] Melanie Volkamer[5]

Abstract: The internet voting protocol deployed at Estonian political elections was enhanced by cast-as-intended vote verifyability mechanism in 2013 to reveal manipulations of the vote casting device by using a second device (most likely a mobile device as it needs to be euqipped with a camera). This paper studies voters' perception and comprehension of this mobile-device-based cast-as-intended verifiability mechanism. We conducted semi-structured interviews with 13 eligible voters who have cast an electronic vote at least once since the availability of this mechanism. While most participants were in favor of having the option to verify available, , most were not aware of the main purpose to verify. Instead, they, for instance, thought it was designed to check that they had not made a mistake while selecting a candidate or to verify one's vote was tallied as intended. Thus, our findings highlight the need for improved communication on cast-as-intended verifiability in order to enable informed decisions whether to verify or not.

Keywords: Cast-as-intended verifiability; Online voting; Voter perception; comprehension; Interviews

1 Introduction

With the escalating global population, the costs and complexities associated with traditional elections have intensified [HS14]. While certain advancements in this domain have yielded positive outcomes, there exist adverse consequences resulting from the malevolent activities of individuals or groups aiming to disrupt elections conducted through online platforms [Gi19, HT15]. Adversaries may possess the capability to manipulate individual vote casting devices such as laptops or smartphones, as well as the online voting platform or parts of it, thereby enabling the replacement or elimination of votes – without voters or anyone noticing it.

One possibility to address this issue would be giving the voter an option to check that his/her vote was tallied the way he/she intended to (sometimes also called *end-to-end* (E2E) verifiability). Such a proof is difficult as a strong proof of vote integrity, might be used in coercive scenarios and for vote selling. While several research proposals for E2E secrecy ensuring verifiability exist, in practice, i.e. for real elections, weaker forms are offered to

[1] Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany tobias.hilt@kit.edu
[2] Cybernetica AS, Narva mnt 20, Tartu, Estonia kati.sein@cyber.ee
[3] Cybernetica AS, Narva mnt 20, Tartu, Estonia tanel.mallo@cyber.ee
[4] Cybernetica AS, Narva mnt 20, Tartu, Estonia jan.willemson@cyber.ee
[5] Karlsruhe Institut for Technology, AIfB, Kaiserstr. 89, 76131 Karlsruhe, Germany melanie.volkamer@kit.edu

voters, e.g. voters can verify that their vote reached the vote collection server in an unaltered way (called *cast–as-intended* verifiability).

A form of cast-as-intended verifiability has been implemented in the Estonian voting system since 2013 [HW14]. Its aim is to reveal manipulations of the vote casting device with a second (mobile) device while assuming that not both devices are manipulated.

For any cast-as-intended verifiability mechanism to deliver its promise, it relies on three key assumptions: (1) voters indeed perform the verifiability steps, (2) they notice if their vote has not been cast as intended, and (3) they report the observed disturbance. All three assumptions have been challenged by user studies while the focus was on cast-as-intended verifiability mechanisms different from the one used in Estonia [Ac14, Ka11b, Ma18, WH09]. These studies have revealed that the complexity and unfamiliarity of the corresponding steps can easily prevent voters from performing the necessary steps correctly, or at all. Even if the voters observe some issues, they are not likely to report them, as they may believe that verifying was not possible due to their own mistakes as they have a wrong comprehension of the purpose of verifying their vote [Vo22, TVK22].

Ten years after the introduction of cast-as-intended verifiability in Estonia, we wanted to study voters' perception and comprehension of it. To do so, we opted for a qualitative approach – in contrast to most of the recent related studies on other voting systems which predominantly use quantitative research methods. This choice was influenced by two considerations: First, Estonia stands out for having actually applied an electronic voting system providing cast-as-intended verifiability. Therefore it is possible to gain insights into the perceptions and comprehension of individuals who have used the e-voting system in real life. Second, since this study is a pioneering endeavor in exploring the perception and comprehension of Estonian voters, a qualitative approach is deemed more effective in providing in-depth insights compared to a quantitative one.

The paper is structured as follows. We discuss our work in light of related work in Sect. 2, followed by some background information about Estonian elections and a short description of the https://www.overleaf.com/project/649d876efde0a1310a0f47f2Estonia online voting system in Sect. 3. We present our research questions in Sect. 4 and describe our used methodology in the following Sect. 5. Our results are presented in Sect. 6. Sect. 7 provides several points of discussion, and finally, conclusions are drawn and directions for future work are presented in Sect. 8.

2 Related work

Three distinct methodologies for the realization of cast-as-intended verifiability in electronic voting systems have gained traction.

The first methodology utilizes return codes, is currently employed in Switzerland and is advocated by sources such as Galindo et al. [GGP15]. Here, the voters are provided with a sheet of codes via postal mail prior to the election. Once the vote is cast, a confirmation code is generated which the voter must cross-verify with the codes listed on the sheet received earlier.

The second methodology encompasses the Benaloh challenge, also referred to as the verify-or-cast approach, which is to be employed before the vote is cast [Be06].

The third methodology, exemplified by its implementation in Estonia since 2013, entails the use of an ancillary device for vote verification [HW14]. This involves the use of an autonomous verification tool that accesses the random seed used in vote encryption, and is able to decrypt the vote in a separate mobile device.

The first two methodologies, namely the Benaloh challenge and the return code approach, have been the subject of usability studies and suggestions for enhancements in usability have been posited [WH09, Ka11b, Ka11a, Ne14, Ac14, Ac15b, Ac15a, Ma18, Ma19, Ku20, Ma20, Ku21, Ku21, TVK22]. Additionally, a study juxtaposing both methodologies was undertaken [Ku19].

Scholarly attention has also been paid to the third methodology. Notably, Marky et al. [MKV18] conducted an investigative study employing a cognitive walk-through technique across the three methodologies. Though this did not encompass a user study, it involved the identification of presumptions regarding voter behavior as posited by the different systems, and used these assumptions as a benchmark for comparison. The return code methodology emerged superior, requiring the least amount of assumptions in terms of the number of assumptions necessitated. However, the authors did not study users perception of any of the systems but only concluded that a system with less assumptions on voters' behavior may have advantages in terms of motivating voters to verify and have them making less mistakes.

A user study that assessed all three methodologies concerning their efficacy was conducted [Ma21]. This study concluded that the return code methodology fared the best, while the Benaloh challenge came in second. Thus, the focus was only on being able to detect manipulations. Furthermore, it is important to note that the study had certain methodological limitations, including the fact that participants had to rely on the voting system they suspected to be manipulated to report any perceived manipulations.

3 Background Information

According to the Estonian constitution, parliamentary elections take place on the first Sunday of March once every four years. In practice, this is the day of polling site in-person paper voting.

Estonian legislation allows for more than ten alternative ways of submitting a vote. In recent years, Internet voting has become the most popular channel. Alternative vote casting methods (including Internet voting) are mostly utilized during the advance voting period which spans over approximately one week before the election Sunday. In 2023, for example, Internet voting was possible from February 27th until March 4th (with March 5th being the election Sunday).

In order to cast an electronic vote, the voter first has to download the voting application (available for Windows, macOS and Linux) from the election organizer's website. Once this software is installed and started, voters authenticate themselves by using their state-issued electronic ID. Afterwards, the list of candidates corresponding to the electoral district of the voter is displayed. Once voters make their choice, the selected candidate is then encrypted. The voter signs the corresponding cyphertext with the voter's electronic ID.

As the voter's device is not necessarily trustworthy and can attempt to change the vote (e.g. as a result of a malware attack), the voter can ensure the integrity of the vote by verifying it, within 30 minutes after casting the vote. This cast-as-intended verifiability enables the voter to query the voting server for the vote associated with their signature. Note that verifying the vote later than 30 minutes after casting is disabled to limit coercion attacks.

It was decided that one cannot rely on the (potentially malicious!) voting device, in 2013 the Internet voting system was adopted to provide cast-as-intended verifiability. Since 2013 voters can verify the integrity of their vote using a second smart device install a corresponding app. During the cast-as-intended verifiability step, the randomness used to encrypt voters' candidate as well as a unique vote reference is transferred from the voting application on the vote casting device to the app on the second device via a QR-code (see Fig. 1)[6].

The cast-as-intended verifiability application queries the voting server based on the vote reference, downloads the signed and encrypted vote, and verifies this information by mainly taking the following steps: First, it checks the signature. After this check passes successfully, the application checks which candidate encrypted with the randomness provided in the QR Code matches the cyphertext (encrypted vote) which was received from the server. This candidate is display on the screen of the mobile device. Voters then need to check whether the displayed candidate is the one they intended to cast (see Figure 2).

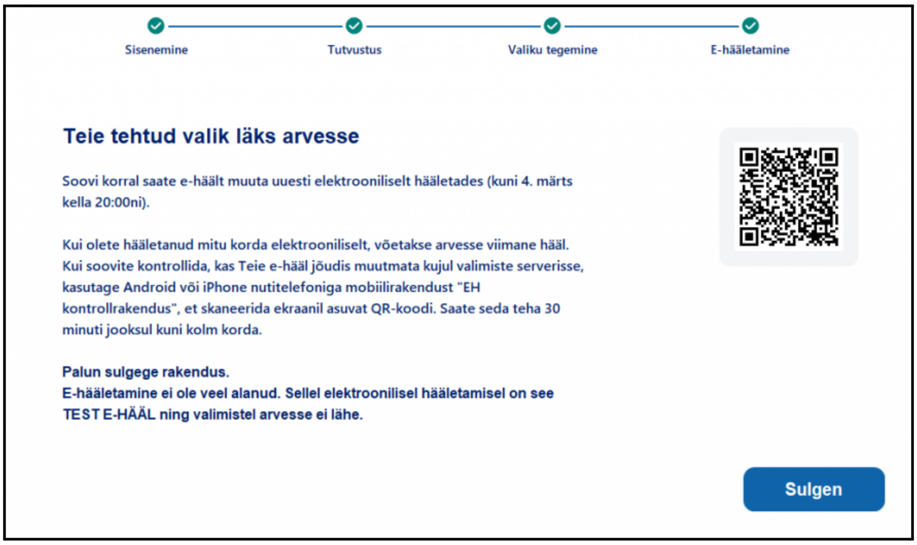
A more elaborate description of the Estonian Internet voting and protocol of the cast-as-intended verifiability mechanism is described by Ehin et al. [Eh22].

4 Research Questions

In this study, we aimed to examine how i-voters in Estonia perceive and comprehend the step of cast-as-intended verifiability.

There is a regular survey conducted in Estonia after every election event covering about 1000 respondents [ES21]. We were able to access the survey results of 2023, and it turns

[6] https://www.valimised.ee/en/internet-voting/guidelines/checking-i-vote, last accessed 12 September 2023



Teie tehtud valik läks arvesse

Soovi korral saate e-häält muuta uuesti elektrooniliselt hääletades (kuni 4. märts kella 20:00ni).

Kui olete hääletanud mitu korda elektrooniliselt, võetakse arvesse viimane hääl. Kui soovite kontrollida, kas Teie e-hääl jõudis muutmata kujul valimiste serverisse, kasutage Android või iPhone nutitelefoniga mobiilirakendust "EH kontrollrakendus", et skaneerida ekraanil asuvat QR-koodi. Saate seda teha 30 minuti jooksul kuni kolm korda.

Palun sulgege rakendus.
E-hääletamine ei ole veel alanud. Sellel elektroonilisel hääletamisel on see TEST E-HÄÄL ning valimistel arvesse ei lähe.

Fig. 1: The last page of the Estonian voting application displaying the QR code for vote verification. The text reads: "**Your choice has been taken into account.** If you want, you can change your e-vote by voting electronically again (until March 4th, 20:00). If you have voted electronically several times, the last vote will be counted. If you want to make sure that your vote reached the election server in an unaltered form, use the app called "EH kontrollrakendus" on an Android or iPhone smartphone, and scan the QR-code from the screen. You can do this for the duration of 30 minutes up to three times. **Please close the application. E-voting has not started yet. Right now this is a TEST E-VOTE and will not be counted at the real elections.**"

out that, according to this survey, 50% of the electorate is aware of the cast-as-intended verifiability option[7]. Among the i-voters the respective percentage was 68.3, and among the paper voters it was 41.8. Still, only 5.5% of the i-votes were actually verified.[8] A natural question arises, *why do i-voters not verify their vote?*

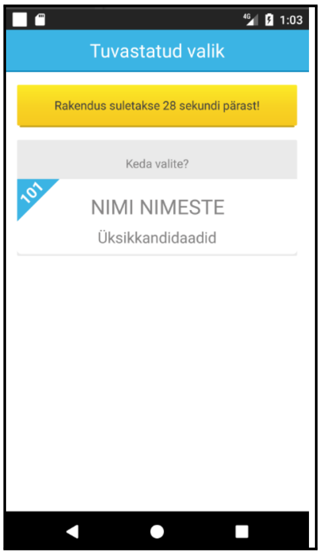
Our working hypothesis is that the electorate is not aware of the rationale behind cast-as-intended verifiability. Therefore, we try to answer the following research question:

RQ1: [Comprehension] What do Estonian i-voters think is the purpose of cast-as-intended verifiability?

In 2020, Solvak studied the usage patterns of Estonian i-vote verifiers based on the voting log data and how these affect voter confidence towards the integrity of the election [So20].

[7] The question, we consider is: "Kas Te teate, et 2023. aasta valimistel sai valija oma interneti teel antud häält kontrollida?"which can be translated to: "Do you know that during 2023 elections it was possible for a voter to verify his/her Internet vote?"

[8] https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-haaletamise-statistika, last accessed 07 July 2023



1:03

Tuvastatud valik

Rakendus suletakse 28 sekundi pärast!

Keda valite?

101

NIMI NIMESTE

Üksikkandidaadid

Fig. 2: Final screen of the cast-as-intended verifiability app. The text reads: "Identified choice. The application will be closed in 28 seconds. Whom did you choose? 101, Nimi Nimeste, Individual candidate"

However, the predefined multiple choice format of the questionnaire did not allow to dig deeper into the confidence building mechanisms. Thus, we extended the current study by setting the second research question.

RQ2: [Perception] How does the presence of cast-as-intended verifiability impact the perceived trustworthiness of the i-voting system?

5 Methodology

5.1 Recruitment

We required our study participants to meet one criterion: having cast an i-vote in Estonian elections at least once since 2013 (i.e. since the year cast-as-intended verifiability was introduced in Estonia). Participants were recruited through various channels: We made announcements to colleagues, friends, fellow Estonian researchers, and students of Tartu University. We also placed paper advertisements in public areas in Tartu city and its vicinity, and published advertisements on both LinkedIn and in the print version of Maaleht,[9] an Estonian weekly newspaper with readership among rural and elder Estonians. We also

[9] https://maaleht.delfi.ee, last accessed 07 July 2023

encouraged participants to disseminate the invitation among their acquaintances. It is important to note that no monetary or other forms of compensation were provided to participants.

Although in Estonia individuals aged 16 and above are eligible to vote in local municipal elections, no individuals under 18 volunteered for the study, so no parental consent was necessary.

5.2 Interview Procedure

We developed a semi-structured interview protocol to conduct the interviews. However, to facilitate clarity, participants were permitted to ask questions, which occasionally led to slight deviations in the interview process. Note, given the multilingual composition of the research team and the local execution of the study in Estonia, two language versions of materials were developed: First, study materials were developed and discussed in English. Later, the Estonian members of the research team translated it into Estonian.

We conducted one pilot interview in English to allow the entire research team to observe and identify areas for improvement. We identified some improvements in terms of wordings used in the interview protocol and altered it accordingly, e.g., changing the terminology from "check" to "verify" to accurately describe the process of verifying one's vote. The final interview protocol is available online[10]. The main interviews were conducted in Estonian by the same interviewer. The interview procedure is illustrated in Fig. 3 and the individual parts are briefly explained below.

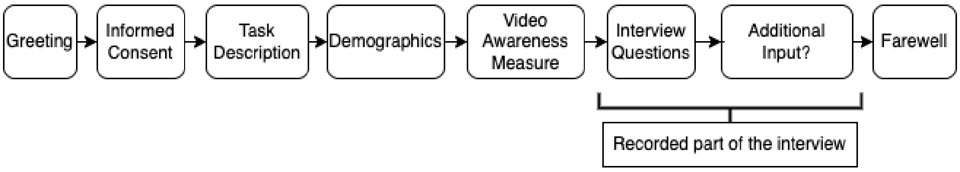


Fig. 3: Flowchart describing the various parts of the interview.

Informed consent & Task Description. If the participant had contacted the researchers via e-mail, the informed consent form was sent to them before the interview took place, detailing the scope of the research and the rights of the participants. The actual interview started with informing the participants of the nature of the research, their role in it and their rights. The participants were encouraged to ask questions if they had any.

In particular, participants ware asked for permission to audio record the interview. The commencement and conclusion of the recording were explicitly confirmed with the participant.

[10] https://secuso.aifb.kit.edu/downloads/documents/Interview_Guide.pdf, Last accessed 12 September 2023

Demographics. Participants were asked to specify their preferred gender and select the age ranges they fall into, with the options being 16-29, 30-39, 40-49, 50-59, 60-69, 70-79, and 80+.

Video Awareness Measure. Next, all participants watched a five-minutes video[11] to establish a common knowledge foundation. The video depicted a voter's perspective in a fictitious election, consisting of casting a vote and verifying this vote with a separate device and a corresponding app. The narrator of the video explained the process in real time in Estonian.

Interview Questions. At this point, the participants were informed that the recording was started. The interview questions encompassed both open-ended and multiple-choice formats. The interview consisted of 12 main questions, with several of them having detailed sub-questions to delve into specific nuances of the topic. For instance, a question concerning an imaginary scenario in which the voter detects that their vote was not cast-as-intended was used to examine the participants theoretical behavior in such a scenario. Therefore we asked them how they would react emotionally, what they would themselves do and what they would expect officials to do in such a situation. The complete interview guide is available online[12].

After an interviewee was asked how important they considered that the majority of voters verified their votes (Q7), they were explained the actual purpose and functionality of the cast-as-intended verifiability mechanism and why it was added to the Estonian i-voting system. Afterwards, some more questions were asked.

Once the participants answered all interview questions, they were offered the possibility to add information or opinions in case they felt something has remained without attention; or ask clarification questions from the interviewer. Then the recording was stopped and they were thanked for their help.

5.3 Data Analysis

The data from the interviews was processed and analyzed through a systematic approach. The recordings were transcribed using Kaldi Offline Transcriber for the Estonian language[13]. The outputs of the transcriber were edited by the interviewer to correct any speech recognition

[11] Version without voice but English subtitles of what was spoken on the video shown to the participants https://secuso.aifb.kit.edu/downloads/Videos/i-vote_Estonia2023_ENG_sub.mp4, last accessed 12 September 2023

[12] English version of the guide: https://secuso.aifb.kit.edu/downloads/documents/Interview_Guide.pdf, last accessed 12 September 2023

[13] https://koodivaramu.eesti.ee/taltechnlp/kaldi-offline-transcriber/-/tree/master, last accessed 05 July 2023

mistakes and achieve intelligible verbatim transcription. An inductive coding approach was adopted for the analysis [Sa09, Th06]. Initially, each of the two coders individually reviewed four out of the thirteen interviews and devised codes to encapsulate the content. Following this, there was a group discussion within the research team. It was discerned that reviewing four interviews was insufficient to capture the entirety of the data, prompting the coders to analyze four additional interviews individually.

Separate codes were created for each question to maintain clarity and structure. The term "codebook" henceforth encompasses all these individual sets of codes. Following the analysis of the additional interviews, the coders convened to discuss their findings, culminating in the creation of an initial codebook encompassing all identified codes along with their definitions and criteria for application.

This initial codebook was then reviewed, discussed, and ratified by the entire research team. Subsequently, both coders independently re-applied this finalized codebook to all thirteen interviews. The coded data of both coders was then compared to determine discrepancies. The coders engaged in discussions to resolve these disagreements, primarily by clarifying any misunderstandings. The link to the final codebook is available online[14]

Once an agreement was reached on the final version of the applied codes, the data was analyzed using the software MaxQDA[15], which facilitated the computation of the intercoder reliability coefficient Kappa, as outlined by Brennan and Prediger [BP81]. This process led to a substantial improvement in intercoder agreement, as measured by Brennan and Prediger's Kappa, which increased from an initial value of k=0.91 to a final value of k=0.99 (as calculated across all interview questions), indicating near-perfect inter-rater agreement.

For the current analysis, the answers to the following questions were used. Q3, Q6, and Q7 were analyzed to answer RQ1, while Q9 and Q5 contributed to answering RQ2. The raw data collected as a result of the interviews actually allows to provide more insights. These insights will be covered in an upcoming extended version of the paper.

6 Results

In this section, we delve into the results obtained through the corresponding questions of the interview. For better readability, we summarize the process of performing cast-as-intended verifiability by using a dedicated app to verify one's vote, as described in Sect. 3, in the following subsections by the term *verifiability step*. The section is structured along the research questions, while we start with some descriptive information about our participants.

[14] https://secuso.aifb.kit.edu/downloads/documents/Codebooks.pdf, Last accessed 12 September 2023
[15] https://www.maxqda.com, last accessed 07 July 2023

6.1 Interview Participants

The interviews engaged a total of 13 participants, from which three identified as male and ten as female. There was a considerable diversity in the age range of the participants, as detailed in Tab. 1.

Age range	16-29	30-39	40-49	50-59	60-69	70-79	80+
Number of participants	2	4	3	1	1	1	1

Tab. 1: Age range of participants

The interviews were thorough, with an average duration of 43 minutes per session, culminating in a total of 563 minutes of recorded content that was transcribed for analysis. Only two individuals had actually undertaken the step of verifying their vote in any of the elections since 2013. One of them succeeded and another one failed because of incomplete comprehension of the process (scanning the QR-code with an incorrect app).

6.2 Comprehension of the Cast-as-Intended Verifiability Mechanism

Various different interpretations were given in replies to the question about the purpose of the verifiability step (Q3): The interpretation from 12 out of 13 participants was related to various doubts and concerns associated with the voting process. These doubts included voter's own performance during the voting process (e.g., a misclick while selecting the candidate), the voting-specific infrastructure ("system error") as well as malfunctioning of infrastructure that is not specific to voting (e.g., incidental problems with the Internet connection).

Some answers were very abstract and, thus, leave room for interpretation: "[Verifying that] the vote has reached the server" was mentioned by seven participants. While this can be considered as partially correct comprehension of the mechanism, it leaves room for interpretation as it does not specify which potential problems are addressed and which server they had in mind (e.g. also the one tallying the votes which would then not be correct).

Two participants described the purpose of the verifiability step as detecting vote tampering but did not specify at which device (or maybe while send to the server) this could take place.

In addition, seven participants mentioned providing satisfaction for the voter's need for proof and confidence, e.g. one of them sad that the verifiability step as such is specifically addressed to "people who like checking things". Two participants expressed that the verifiability step cannot detect anything important and is only there to provide artificial confidence. Notably, we observed that nobody mentioned the possibility that the source of vote tampering could be the device used to cast the vote – the voter's own computer which is the main purpose why the verifiability step was introduced in 2013.

In addition to the open-ended question (Q3), we use a multiple choice question to study participants comprehension of the verifiability step (Q6). Note, among the six choices presented[16] only one was correct and the interviewees were informed that there is at least one correct answer.

We observed 12 out of 13 participants correctly identifying the correct answer ("My vote reached the vote collector server the way I intended to."), however, four of them additionally picked a wrong one ("My vote is correctly tallied.") and one declared that they cannot decide about the other two options about one's individual vote.

Thus, seven out of thirteen participants demonstrated correct comprehension of the cast-as-intended verifiability mechanism when providing them a list of choices with one being the correct one.

The one participant, who did not select the proper choice, picked the option "My vote is correctly tallied.", clearly indicating that more is expected from the verifiability step as it actually does provide.

In addition, we observed the participants perceiving the importance of verification differently, by asking them how important they deem the verifiability step to be taken by all i-voters (Q7).

Seven participants did not regard it crucial that voters verify their vote, two viewed it as somewhat important while four interviewees assessed it as very important. The reasons mentioned by those who considered it as very important justified it with statements like"fast detection of issues", "demonstration of security of i-voting" or "increasing voter confidence".

Those considering it as not important mentioned that it does not have an effect on the election results, and that the presence of verification option induces doubt. Two interviewees also expressed that the Estonian e-Government system is sufficiently secure even without the verifiability step.

One interviewee said that verifiability step is, in addition to failing to address the correctness of tallying, a waste of resources – electricity and time of voters and system developers – and as such should rather be avoided.

In addition, several participants emphasized that the verifiability step should not be a universal requirement for all voters since many might not possess a smart device to complete it.

[16] Note, the choices were presented in a random order.

6.3 Perception - Impact of the Cast-as-Intended Verifiability Mechanism on Perceived Trustworthiness

Answering RQ2, one has to consider, that participants were explained the real purpose of the verifiability during the interview, as described in Sect. 5.2.
When questioned what a person with malicious intend could do if i-voters do not perform the verifiability step (Q3b), the interviewees expressed different comprehension. Six participants felt that the absence of the verifiability step would not necessarily make the system more vulnerable to malicious exploitation. The reasoning behind this belief was diverse, with three participants expressing faith in the inherent security of the system even without the verifiability step, and one surmising that an adversary with the capacity to compromise the voting system could equally circumvent the verifiability mechanism. It was also once stated, that ‘ì-voting is logged and tempering would be detected using logs”. Additionally, one didn’t reason their decision, that an attacker could not do anything. While two interviewees expressed uncertainty, in total five interviewees stated potential malicious actions or exploits that could happen, if the verifiability step is not in place. Three interviewees believed that their vote could be tampered, without disclosing how exactly or at which point (e.g. on which device) this could take place. Vague expressions by two participants were captured using the codes “wider attack surface” and “voter coercion”. Important to mention is also, that four interviewees explicitly stated already earlier (Q3a), that the verifiability has no effect and especially does not increase trust for people who already mistrust the government or technology. E.g. one of the participants stated that “person who has doubt in the system would not have belief in scanning the/a QR code”. This again shows a wrong comprehension of the actual purpose of the verifiability step.
Presented with a hypothetical scenario in which the displayed vote (on the second device) would differ from the one they cast (on the vote casting device), they were asked what they would think and how they would feel in such a scenario (Q5a). Eight interviewees suspected technical error to be reason of the discrepancy between the vote they cast and the one they verified. The remaining five interviewees expressed suspicion and concerns, with two respondents suspecting system tampering and one suspecting bystanders. Eight participants also expressed doubt in their own performance and four that they would experience immediate negative feelings.

The participants were educated about the real purpose of the verifiability step before they were asked about the trustworthiness of the voting process (Q9b). Eight participants deemed the voting system more trustworthy with the verifiability step in place and four viewed the impact negligible[17]. Five interviewees expressed that the “additional control” enhances the credibility of the voting system. One interviewee addressed this enhanced credibility directly to the second device. Additionally, two interviewees reasoned, that the verifiability step is endorsed by security experts, which makes it trustworthy. When asked whether they would prefer a voting system with or without the verifiability step (Q9a), one participants expressed indifference and the rest of the participants expressing preference

[17] Note that in one of the interviews, we didn’t receive an answer to this question.

for a system with the verifiability step. Reasons for this preference that were mentioned at least once were the following: “increases trust”, “reduces scepticism”, “increases security”, “detection of technical errors”, “malware protection” and “preference for personal control”. The interviewee expressing indifference reasoned, that for them they would prefer the verifiability step to be available later in the election, such as shortly before tallying or a few days after the results have been announced[18].

7 Discussion

Our participants displayed a diverse comprehension by verbalizing what could be detected by performing the cast-as-intended verifiability step while all being very abstract, several misconceptions could be identified. In particular none of the participants noticed that the main purpose of the studied verifiability step is to enable voters to detect if their voting device is malicious (and changes their vote before encrypting it), given their second device is not malicious. When presented with multiple choices to describe the purpose of the verifiability step, nearly all participants were able to detect the correct choice. Important to highlight here is, that nearly half of them also picked an additional, wrong option or stated they were unsure about their decision. The fact, that nearly all were able to detect the correct option may be due to nature of the multiple choice question asked: six possible answers were given but only three distinct purposes were stated[19], each having slight differences regarding the amount of votes under examination (my personal vote or all votes). By inspecting the choices one could deduct the obvious wrong answers and be left with fewer choices. This realization combined with the finding that nearly half of the participants also selected additional wrong options supports the conclusion, that the voters clearly lack comprehension of the real purpose of the verifiability step. Consequently, it is not surprising that only about a third of participants stated that the verifiability step is very important to be taken by all or most of the voters. Although nobody explicitly stated that they have changed their opinion after being exposed to education about the actual purpose of the verifiability step, nearly all expressed a preference of a voting system with the verifiability step in place and that such a system would be more trustworthy. This contrasts their prior assessment that somebody with malicious intent could do nothing in a voting system without the verifiability step. It shows that our participants themselves didn’t had the right comprehension of the purpose of the verifiability step and therefore most likely regarded it as not essential. After being educated about the real purpose they seemed to attribute the verifiability step more importance and credibility, which could lead to a higher trustworthiness.

One important thing to mention is that several participants expressed high trust in the Estonian e-Government in general. It can be argued, that these people attribute less importance to the verifiability step itself because they trust the complete voting system with the verifiability step being part of it.

[18] Note, this would be End-to-end verifiability.

[19] (1) Vote(s) reached vote collector server, (2) vote(s) are not altered on collector server until tallying and (3) vote(s) are correctly tallied.

Preference for the availability to verify their vote shortly before tallying or after the election results has been announced was also mentioned. One of the reasons why some participants deemed the verifiability step unimportant was also that performing the step has no effect on the election result. This shows the insufficient comprehension of the purpose of the verifiability step once again, as these participants refer to end-to-end verifiability and not individual verifiability.

7.1 Limitations

This research is subject to several limitations that should be considered while interpreting the findings. Firstly, the study's sample size, consisting of 13 participants, is small and therefore can not be considered as representative of the entire electorate in Estonia.

There is a possibility of self-selection bias, as participants voluntarily chose to be part of the study. The absence of monetary compensation could have deterred certain demographics from participating, further contributing to self-selection bias.

Another limitation is language and cultural factors, as the study was conducted in Estonian. Non-Estonian speaking residents who are eligible to vote were not represented in this study.

Thus, with a more representative sample even more misconceptions may occurred than those identified in our research.

Temporally, the study was conducted close to 2023 parliamentary elections, which could mean that the responses might have been influenced by the electoral atmosphere or recent political events, thus not reflecting long-term attitudes and comprehension.

Lastly, the qualitative nature of data collected through semi-structured interviews and its subsequent interpretation by the researchers could introduce subjectivity into the findings. The analysis of qualitative data is inherently interpretive, and the semi-structured format of interviews may have led to variations in the data collected.

8 Conclusion

The primary objective of this study was to examine voter perception and comprehension towards cast-as-intended verifiability in the Estonian online elections.

Our interviews revealed that several have noticed that there is something one can check, a number of misconception about the provided cast-as-intended mechanism as well as skepticism and diverse viewpoints concerning the criticality of the verification process (several did not view it as an essential component).

In conclusion, while being aware or at least not surprised about the option to check something, there is a need for explaining the purpose of the verifiability step. Currently, it is likely that voters cannot make an informed decision whether to verify or not due to their lack of comprehension of the purpose. The same holds for their perception whether or not the verifiability step increase the security or trustworthiness of the overall system. Currently, it is not surprising that some voters do not consider this step as necessary due to their lack of comprehension of its purpose.

Thus, we conclude that policymakers and election authorities should contemplate broader information campaigns to ensure that voters not only notice that their is something to check but also understand its purpose; thus basically enable them to make an informed decision whether or not to verify.

Such campaigns should be carefully prepared to avoid causing distrust when starting explaining what the purpose is (but also what it is not for). We also recommend to accompany such information campaigns with research to study the impact on perception and comprehension, i.e. comparing it before and after the campaigns.

Acknowledgements

This paper has received funding from the Estonian Research Council under the grant number PRG920, from the project "Engineering Secure Systems" of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems], and by KASTEL Security Research Lab.

Bibliography

[Ac14] Acemyan, Claudia Z; Kortum, Philip; Byrne, Michael D; Wallach, Dan S: Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. The USENIX Journal of Election Technology and Systems, 2(3):26–56, 2014.

[Ac15a] Acemyan, Claudia Z; Kortum, Philip; Byrne, Michael D; Wallach, Dan S: From error to error: Why voters could not cast a ballot and verify their vote with Helios, Prêt à Voter, and Scantegrity II. USENIX Journal of Election Technology and Systems, 3(2):1–19, 2015. Publisher: USENIX.

[Ac15b] Acemyan, Claudia Z.; Kortum, Philip; Byrne, Michael D.; Wallach, Dan S.: Users' Mental Models for Three End-to-End Voting Systems: Helios, Prêt à Voter, and Scantegrity II. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, pp. 463–474, 2015.

[Be06] Benaloh, Josh: Simple Verifiable Elections. Electronic Voting Technology Workshop, EVT '06, 2006. Place: Berkeley, CA, USA Publisher: USENIX Association.

[BP81] Brennan, Robert L.; Prediger, Dale J.: Coefficient Kappa: Some Uses, Misuses, and Alternatives. Educational and Psychological Measurement, 41(3):687–699, 1981.

[Eh22] Ehin, Piret; Solvak, Mihkel; Willemson, Jan; Vinkel, Priit: Internet voting in Estonia 2005-2019: Evidence from eleven elections. Gov. Inf. Q., 39(4):101718, 2022.

[ES21] Ehin, Piret; Solvak, Mihkel: Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005–2019. In: International Joint Conference on Electronic Voting. Springer, pp. 75–90, 2021.

[GGP15] Galindo, David; Guasch, Sandra; Puiggali, Jordi: Neuchâtel's Cast-as-Intended Verification Mechanism. In: International Conference on E-Voting and Identity (VOTE-ID). Springer, pp. 3–18, 2015.

[Gi19] Giles, Martin: , US elections are still far too vulnerable to attack - at every level, 2019.

[HS14] Harada, Masataka; Smith, Daniel M: You have to pay to play: Candidate and party responses to the high cost of elections in Japan. Electoral Studies, 36:51–64, 2014. Publisher: Elsevier.

[HT15] Halderman, J Alex; Teague, Vanessa: The New South Wales iVote system: Security failures and verification flaws in a live online election. In: International Conference on E-voting and Identity, September 2-4. Springer, pp. 35–53, 2015.

[HW14] Heiberg, Sven; Willemson, Jan: Verifiable internet voting in Estonia. In (Krimmer, Robert; Volkamer, Melanie, eds): 6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014, Lochau / Bregenz, Austria, October 29-31, 2014. IEEE, pp. 1–8, 2014.

[Ka11a] Karayumak, Fatih; Kauer, Michaela; Olembo, M. Maina; Volk, Tobias; Volkamer, Melanie: User Study of the Improved Helios Voting System Interfaces. In: 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST). IEEE, pp. 37–44, 2011.

[Ka11b] Karayumak, Fatih; Olembo, Maina M.; Kauer, Michaela; Volkamer, Melanie: Usability Analysis of Helios-An Open Source Verifiable Remote Electronic Voting System. In: EVT/WOTE. USENIX, 2011.

[Ku19] Kulyk, Oksana; Henzel, Jan; Renaud, Karen; Volkamer, Melanie: Comparing "Challenge-Based" and "Code-Based" Internet Voting Verification Implementations. In: IFIP Conference on Human-Computer Interaction. Springer, pp. 519–538, 2019.

[Ku20] Kulyk, Oksana; Volkamer, Melanie; Müller, Monika; Renaud, Karen: Towards Improving the Efficacy of Code-Based Verification in Internet Voting. In: VOTING. Springer, 2020.

[Ku21] Kulyk, Oksana; Ludwig, Jonas; Volkamer, Melanie; Koenig, Reto E.; Locher, Philipp: Usable Verifiable Secrecy-Preserving E-Voting. In: 6th International Joint Conference on Electronic Voting (E-Vote-ID). University of Tartu Press, 2021.

[Ma18] Marky, Karola; Kulyk, Oksana; Renaud, Karen; Volkamer, Melanie: What Did I Really Vote For? In: ACM CHI. p. 176, 2018.

[Ma19] Marky, Karola; Schmitz, Martin; Lange, Felix; Mühlhäuser, Max: Usability of Code Voting Modalities. In: ACM CHI. 2019.

[Ma20] Marky, Karola; Zimmermann, Verena; Funk, Markus; Daubert, Jörg; Bleck, Kira; Mühlhäuser, Max: Improving the Usability and UX of the Swiss Internet Voting Interface. In: ACM CHI. 2020.

[Ma21] Marky, Karola; Zollinger, Marie-Laure; Roenne, Peter; Ryan, Peter YA; Grube, Tim; Kunze, Kai: Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes. ACM Trans. Comput.-Hum. Interact, 28(5), 2021.

[MKV18] Marky, Karola; Kulyk, Oksana; Volkamer, Melanie: Comparative Usability Evaluation of Cast-as-Intended Verification Approaches in Internet Voting. In: SICHERHEIT. Gesellschaft für Informatik, 2018.

[Ne14] Neumann, Stephan; Olembo, Maina M.; Renaud, Karen; Volkamer, Melanie: Helios Verification: To Alleviate, or to Nominate: Is That the Question, or Shall we Have Both? In: International Conference on Electronic Government and the Information Systems Perspective. Springer, pp. 246–260, 2014.

[Sa09] Saldaña, Johnny: The coding manual for qualitative researchers. Sage, 2009. OCLC: ocn233937452.

[So20] Solvak, Mihkel: Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In (Krimmer, Robert; Volkamer, Melanie; Beckert, Bernhard; Küsters, Ralf; Kulyk, Oksana; Duenas-Cid, David; Solvak, Mikhel, eds): Electronic Voting - 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6-9, 2020, Proceedings. volume 12455 of Lecture Notes in Computer Science. Springer, pp. 213–228, 2020.

[Th06] Thomas, David R.: A General Inductive Approach for Analyzing Qualitative Evaluation Data. American Journal of Evaluation, 27(2):237–246, 2006.

[TVK22] Thürwächter, Paul Tim; Volkamer, Melanie; Kulyk, Oksana: Individual Verifiability with Return Codes: Manipulation Detection Efficacy. In: 7th International Conference on Electronic Voting (E-Vote-ID). volume 13553. Springer LNCS, p. 139–156, 2022.

[Vo22] Volkamer, Melanie; Kulyk, Oksana; Ludwig, Jonas; Fuhrberg, Niklas: Increasing security without decreasing usability: Comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, Boston, MA, August 2022.

[WH09] Weber, Janna-Lynn; Hengartner, Urs: , Usability Study of the Open Audit Voting System Helios, 2009.