Implementing and Evaluating the Usability of Reliable Voter Complaints in E2E Verifiable Remote Electronic Voting

Tobias Hilt
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
tobias.hilt@kit.edu

Christian Mack
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
christian.mack@kit.edu

Philipp Matheis
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
philipp.matheis@kit.edu

Benjamin Berens
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
benjamin.berens@kit.edu

Tobias Länge
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
tobias.laenge@kit.edu

Rolf Haenni
Bern University of Applied Sciences
EVG, ICE
Bern, Switzerland
rolf.haenni@bfh.ch

Reto E. Koenig
Bern University of Applied Sciences
EVG, ICE
Bern, Switzerland
reto.koenig@bfh.ch

Philipp Locher
Bern University of Applied Sciences
EVG, ICE
Bern, Switzerland
philipp.locher@bfh.ch

Melanie Volkamer
Karlsruhe Institute of Technology
SECUSO
Karlsruhe, Germany
melanie.volkamer@kit.edu

***Abstract*—End-to-end (E2E) verifiable remote electronic voting is often discussed as an alternative to postal voting for voters living abroad. Such systems require voters to verify that their vote is recorded as intended and to complain if this is not the case. The challenge with voters living abroad is to provide them with a usable, reliable online channel to file their complaints. The contributions of our paper are: (1) Proposal of such a reliable mechanism for a well-established voting scheme including the adoption of voting material to support it. (2) Evaluation of the proposal's effect on the usability (i.e. effectiveness, efficiency, and satisfaction of the voting process) and the manipulation detection rate on the voting scheme. (3) Evaluation of the effectiveness of the complaint filing mechanism. The study comprised two phases in which 150 participants cast their votes over the internet after receiving the voting material by postal mail. The first phase focused on the usability and the second one (being deceptive) simulated a manipulation, examining the manipulation detection rate and the effectiveness of the complaint filing mechanism. Our results show a significant improvement in efficiency, without any negative impact on other usability dimensions or participants' ability to detect manipulations. Among those who detected the manipulation in the second phase, 73% used the complaint filing mechanism correctly, while the rest would have filed a complaint to the attacker who had manipulated their vote in the first place. We conclude that the proposed reliable complaint channel can and should be integrated into E2E verifiable remote voting systems and outline ways to help more voters use it effectively.**

***Index Terms*—Reliable Complaints, E2E Verifiability, Remote Electronic Voting, Return-Code Approach**

1. Introduction

End-to-end (E2E) verifiability is a prerequisite for remote electronic voting systems. E2E verifiability enables voters to independently verify that their vote is recorded as intended (individual verifiability) and it enables the public to independently verify that all recorded votes are properly tallied (universal verifiability). The focus of this paper is on individual verifiability. Here, voters are required to take corresponding verification steps in order to detect manipulations, i.e., in case either their device or the voting system is dishonest and withdraws or alters their vote. However, voters must not only be able to detect manipulations, but also be able to reliably file complaints to electoral authorities. In practise, we see two types of mechanisms for complaint filing: The first type of mechanisms requires voters to physically visit a location to ensure their complaint reaches the authorities. The second type requires voters to send emails (and expects to receive a confirmation email) or call the authorities. Both of them come with several drawbacks: The physical one undermines the convenience of online voting, particularly disadvantaging voters residing abroad who cannot easily go to the embassy or diplomatic missions. For the second type of mechanisms, the issue is that a compromised device would simulate this process, reassuring the voter with a fake confirmation email, while in the background suppressing the complaint. Thus, they rely on the assumption that the device used to file the complaint is trustworthy, which is not in line with the notion of being an E2E verifiable system (in which it should be possible to detect if a device is manipulating votes).

The manipulation detection capabilities of individual

verifiability approaches have been extensively evaluated in user studies (e.g., [1]–[8]). However, we are not aware of any prior research explicitly focusing on the development and/or evaluation of mechanisms for reliable remote complaints. Note, manipulation detection rate was measured in various ways, e.g., by clicking a button in the interface [3], to call or write an email to the study instructor in case of remote studies [7] or to talk to the study instructor in case of a lab study [4]. None used a mechanism to reliably file a complaint remotely.

To address this gap, we introduce a novel complaint filing mechanism for E2E verifiable voting schemes consisting of a dedicated so called *complaint code* and a corresponding *complaint return code* sent via postal mail which is sent together with the actual voting material. Both codes are generated in a distributed way and the printing service as well as the postal service are considered trustworthy. Note, we are aware that this might be debatable in some countries, however, this assumption already exists in several E2E verifiable voting schemes and in particular the one we focus on for this paper.

We selected the return-code based approach for individual verifiability (referred to here as *Vote & Confirm*) as a baseline which we extend with the complaint filing mechanism for the following reasons: This approach naturally involves voter interaction with multiple verification codes, and previous studies (e.g., [3], [4] indicated that this approach has superior usability and manipulation detection effectiveness. We extend both the general approach of the return-code based approach (the extension is referred to here as *Cancelable Vote & Go*) and a variation of it which is used in some cantons in Switzerland (the extension to the Swiss version is referred to here as *Cancelable Vote & Confirm*).

In addition to proposing the complaint filing mechanisms and describing how to apply it to the return-code based approach for individual verifiability, we evaluate both – the *Cancelable Vote & Go* and *Cancelable Vote & Confirm*– against the baseline (*Vote & Confirm*) regarding usability and manipulation detection rate. Furthermore, we evaluate the proposed complaint filing mechanism. We conducted a deceptive, two phase, between-subjects user study with 150 participants. Phase 1 focussed on the usability and served as deception (participants were asked to provide feedback to improve the system), while Phase 2 simulated a manipulation (to measure manipulation detection and to evaluate the complaint filing behaviour).

Our findings reveal no significant differences w.r.t. *effectiveness* and *satisfaction* between the three approaches, however participants from the *Cancelable Vote & Go* approach were significantly faster than participants from the other two approaches. The manipulation detection also did not differ significantly. Furthermore, 73% of our participants that detected the manipulation were able to successfully file a complaint with our proposal, i.e., in particular they did not file their complaint with the simulated attacker.

We conclude that the proposed complaint filing mechanism does not negatively affect usability while allowing to remotely file complaints in a reliable and verifiable manner. We, therefore, recommend that the proposed complaint filing mechanism can and should be integrated into E2E remote voting systems. Without such a mechanism, it is not possible to remotely file complaints which defeats the purpose of E2E verifiability. Moreover, based on our results we propose to reduce the complexity of both the Swiss extension of the return-code based approach as well as it's research proposal, because the additional steps of confirmation and finalisation code did not improve manipulation detection rates while at the same time leading to a worse efficiency.

Research Contributions: There are at least the following three contributions:

1) **A novel complaint filing mechanism:** We propose a mechanism that allows voters to reliably file complaints without needing physical presence or trust in potentially compromised devices. Although evaluated within the return-code based approach, this mechanism is universally applicable to all E2E verifiable voting schemes.
2) **Empirical evaluation of its effect on usability and manipulation detection rate:** Through a between-subjects user study (N=150), we evaluate the impact of our proposed complaint filing mechanism on system usability and manipulation detection capabilities. There is no negative effect.
3) **Empirical evaluation of the proposals effectiveness:** In Phase 2 of the user study, we simulated a manipulation in order to evaluate whether participants can properly use the proposed mechanism. Based on our results, we identify future research directions to further improve the effectiveness.

2. Related Work

This section provides an overview of prior work that informs and motivates our research. We first examine how filing complaints of irregularities is handled in actual elections using verifiable remote electronic voting systems. We show that current procedures lack a reliable mechanism for filing complaints remotely (Subsection 2.1). We then present empirical studies researching the usability and manipulation-detection rates of E2E verifiable voting systems (Subsections 2.2 and 2.3). These studies form the methodological foundation for our study design.

2.1. Filing Complaints in Practice

In this subsection, we report on mechanisms for filing complaints from actual elections using verifiable voting systems.

In Switzerland, voters are instructed that "If the codes displayed do not match the ones from the code sheet, the vote casting process must be aborted and the responsible canton must be contacted" [9]. In the canton of St. Gallen, e.g., this means calling a phone number or sending an email [10], which leaves voters vulnerable if their device is controlled by an attacker. In Estonia, voters who suspect a problem are told they can simply cast a new vote (as vote-updating is implemented in the system), as "The voter who finds that they could not vote freely or that they do not trust their computer can vote again" [11]. If "something is really wrong," [11] voters are directed to contact the police. While we could not find more information on how, we assume they should visit the police in-person because

a phone call could be intercepted (without noticing) by a compromised device. In the German social elections, only a generic email address was provided for filing complaints about irregularities [12].

Across all these examples, complaint filing mechanisms depend on insecure, attacker-visible channels, offer no confirmation, and fail to provide a reliable remote process.

There is one exception: The German Association for Computer Science allowed voters to revoke their vote in case of irregularities. To do so, they were asked to email their revocation request to the authorities. In case the authorities receive it (because the device is not manipulated), the online vote was cancelled and new voting material via postal mail was sent to these voters [13]. If these voters who filed a complaint via email then received new voting material via postal mail, they would know that their complaint reached the authorities. However, this mechanism expects enough time to send postal voting material to the voter and to send the vote back in time. This might be difficult for voters living abroad. In particular it takes some time until voters know that their complaint was successful. Therefore, we do not consider this approach as adequate for voters living abroad.

Summary: There is no reliable mechanism used in practise to remotely file complaints, which is an actual issue for elections offering a (verifiable) remote voting channel for voters living abroad.

2.2. Usability Studies of Different Types of Individual Verifiability Approaches

End-to-end (E2E) verifiability means that the entire election process, including all its steps, can be verified independently of the system provider [14]. This includes individual verifiability, meaning voters can verify that their vote is stored as intended. Different types of individual verifiability have been proposed and studied from a usability point of view: The *Audit-or-Cast* approach as introduced in [15] allows voters to decide, after the system has encrypted the selected candidates, whether to *challenge* this ciphertext (have it opened and checked) or to *cast* it. User studies have shown that this approach is difficult to understand and less usable than the other approaches [4], [16], [17].

The *return-code based* approach as e.g. discussed in [18]–[20] provides each voter with individual return codes (delivered over an out-of-band channel such as postal mail) that correspond to their available selections. After the vote is cast from the device, the system displays the return codes matching the submitted vote; the voter compares these on-screen codes with the pre-distributed reference sheet. Most of the studies evaluating the usability of individual verifiability approaches focus on this approach, see e.g. [2]–[7], [21].

Tracking-code approaches, as e.g. discussed in [22]–[24] assign each voter a unique tracking code that is either generated by the system or created by the voter themselves. This tracking code is stored together with the encrypted ballot. After tallying, all ballots are published alongside their tracking codes on a public bulletin board. Its usability has rarely been studied, e.g. in [3], as the privacy guarantees of these approaches are smaller compared to the guarantees of other approaches.

Cast-then-audit is discussed in [14], [25]–[27] and the general idea is that after casting an encrypted vote, the voting system presents cryptographic verification data which enables reconstructing a human-readable representation. While this approach is used in the Estonian elections (see, e.g., [25], [27]), its usability is only studied in [1].

Summary: The different usability studies show that the usability for almost all implementations of these approaches is excellent (see Table 3 in [6]).

2.3. Deceptive User Studies Measuring the Manipulation Detection Rate

Research on individual verifiability has often investigated voters' ability to detect manipulations, i.e., the effectiveness of the individual verifiability approach in place. Corresponding studies were deceptive as participants were made believe it is about the overall usability but in fact they were asked to use a system with a simulated manipulation and the research question was how reliably participants detect the manipulation in place.

The majority of the research in this area is focused on return-code based approaches (e.g. [2]–[7]). There is only limited research on the cast-then-audit approach (e.g. [1], [3]), the tracking-code approach (e.g. [3], [8]) and the cast-or-audit approach (e.g. [3]).

Two main categories of manipulations are typically distinguished: In a *vote tampering* manipulation, the attacker only changes the vote while voters would be able to detect this manipulation in case they verify their vote. In a *verification prevention* manipulation, attackers (depending on the system) change or delete the actual vote and they manipulate the user interface (UI) in a way that the voters do not get any option to verify, but a message telling them, that vote casting and verification was successful.

Summary: Research has shown that the verification prevention manipulation is much more difficult for voters to detect, compared to the vote altering manipulation (see e.g. [1]). The return-code based approaches reach higher manipulation detection rates compared do the other approaches, in particular for vote tampering in one study 100% was achieved [2].
Therefore, the return-code based approach is most promising while more research is still needed regarding the verification prevention manipulation type. This is why we decided to focus on the return-code based approach and the verification prevention manipulation in our research.

3. Proposed Complaint Filing Mechanism

The goal of this section is to explain our proposal. It is based on the variation of the return-code based approach as implemented in the Swiss voting system. Therefore, we first provide some background information about the return-code based approach in general as well as the Swiss extension of it. We then present our proposal and explain how it could be integrated.

3.1. Background

As explained in the related work section, in return-code based approaches, each voter receives individual

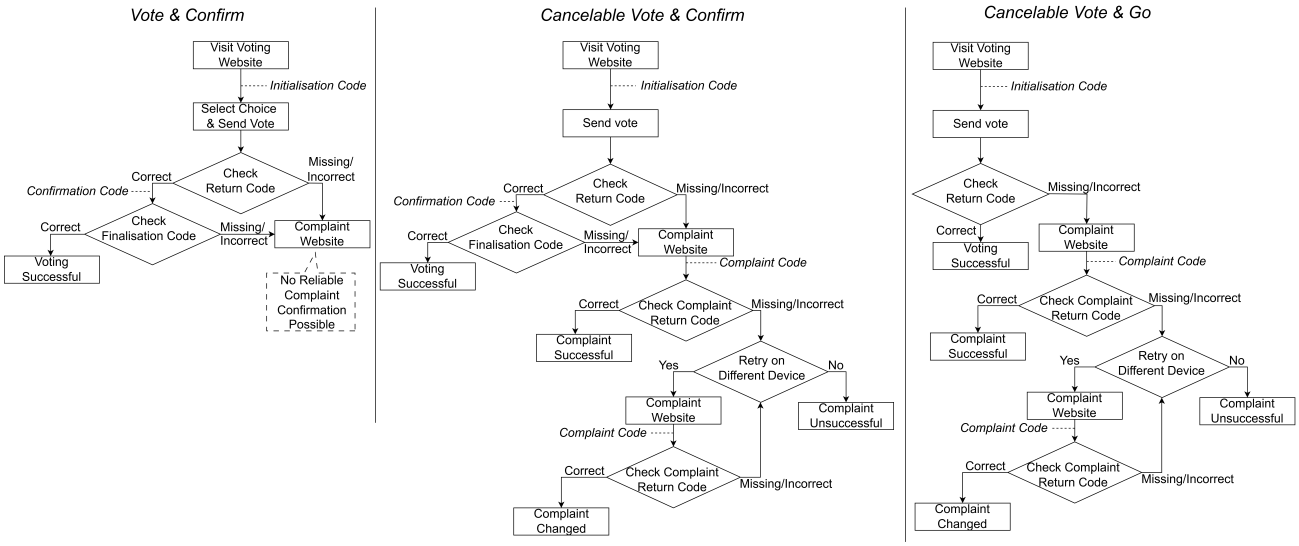

Figure 1. Overview of the steps voters perform in the three approaches. The left diagram illustrates the baseline *Vote & Confirm*, representing the return-code based approach as implemented in Switzerland. The middle diagram (*Cancelable Vote & Confirm*) extends this baseline with a reliable complaint filing mechanism. The right diagram (*Cancelable Vote & Go*) simplifies the process by replacing the confirmation and finalisation steps with the complaint filing mechanism, reducing voter interactions in the normal case. Dashed lines represent the voter needing to submit information they received prior to the election trough a secure channel.

code sheets (delivered over an out-of-band channel such as postal mail) containing return codes that correspond to their available selections. After vote selection, the encrypted vote is sent to the voting infrastructure, a return code per selection is displayed and the voter is asked to verify that these codes match the ones on their code sheet. The security of the return-code based approach relies on the distributed generation (across independent servers) of individual return codes for each voter and every possible choice. During the election, all participating independent servers generate the return code for an incoming vote only if they unanimously agree on the vote's content. Consequently, if at least one honest server participates, no return code can be produced for a different selection. Voters are required to check the return code and file a complaint if it does not match their selection. In Switzerland, a variation

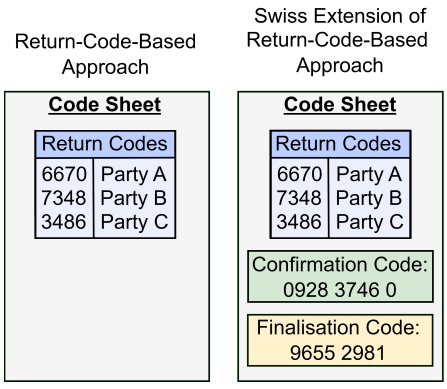

Figure 2. Code Sheets voters receive for a return-code based election (left) and the Swiss extension of the return-code based approach (right).

of this approach is currently implemented by law [28], [29]. In particular, the above steps are extended by two additional steps using the same procedure as described for return-code based approach: voters must actively confirm the correctness of the received return code using a unique confirmation code from their code sheet, which is then validated with a finalisation code which again is only sent if all servers agree. This results in two additional codes on their code sheet. [30] The difference in code sheets is illustrated in Figure 2. Note, this extension to the original idea is meant to encourage voters to verify their return codes before the voting process is finalized, as they can withhold the confirmation code if the displayed return code appears incorrect. The idea is that in such a case one can still vote on paper (if paper channels are available). Note, this extension comes with at least one drawback: Voters may 'forget' to confirm, resulting in their vote not being tallied. Moreover, the addition of these two codes represent another manipulation possibility, as an attacker, aiming to drop votes (for a certain party or in general) could suppress the confirmation code, rendering the vote invalid. We refer to this approach as *Vote & Confirm*.

However, the general concept as well as the Swiss extension of it lack a dedicated and reliable mechanism for filing complaints remotely (see Subsection 2.1).

3.2. General Idea

We propose to use the logic of the confirmation and finalisation codes and the corresponding cryptographic protocol for reliable complaint filing. Voters would receive as part of their code sheet two additional codes: a *complaint code* (similar to the confirmation code) as well as *complaint return code* (similar to the finalisation code). Thus, if a voter detects an issue, such as a changed vote or another manipulation attempt, they can use their complaint code to file a complaint. If they receive the complaint return code that matches their code sheet, the voter knows that their complaint was filed successfully, as the code's high entropy prevents guessing or forgery (as it is the case for the finalisation code). If an incorrect or missing complaint return code is displayed, the complaint was compromised and the voters have probably filed their

complaint with the attacker and need to retry – most likely with a different device or check that they are connected to the proper complaint filing infrastructure. Consequently, the infrastructure for filing a complaint should be distinct from the voting infrastructure itself and hosted on different servers, so that filing complaints is still possible even when the voting system itself may be compromised.

This idea can be integrated in any E2E verifiable voting system with a distributed back-end, and as such in particular to the general return-code based approach (we refer to its extension as *Cancelable Vote & Go*) as well as in the Swiss extension (we refer to its extension as *Cancelable Vote & Confirm*). An overview of the steps voters must perform in these approaches is presented in Figure 1.[1]

3.3. Integration into the Return Code Approach

Two prior works, [5] and [2], proposed and evaluated usability improvements to the Swiss voting system as well as the voting material including the code sheet. We decided to base our research on the voting material from Kulyk et al. [5] for the following reasons: they also investigated the verification prevention manipulation (which we focus on in our research). Moreover, the study design of Marky et al. [3] had some methodological flaws, as participants needed to indicate within the voting system itself and on the same device if they detected a manipulation, which could be intercepted by an attacker having control over the voting device or the voting system.

As there was no dedicated complaint filing mechanism in Kulyk et al. [5], we extended the voting material accordingly for the two proposals *Cancelable Vote & Go* (see Figure 19) and *Cancelable Vote & Confirm* (see Figure 16). We also introduced small improvements to the code sheet to enhance clarity, which are described in more detail in the Appendix C.

As neither of the two prior studies published the election invitation letters they used, we adopted the invitation letter by Hilt et al. [1], originally designed for a cast-then-audit approach, and adapted its content to match the characteristics of the return-code based approach. The invitation letter includes textual cues shown to motivate voters to verify their vote (i.e., to check the return code) [32]. All three participant groups received identical invitation letters, except that the URLs and group name varied according to the group (see figure in Appendix C).

The interfaces for the voting system used in all three approaches of this study were derived from the Swiss Post demo system, which was publicly available as of November 2024, allowing potential voters to familiarize themselves with it.

We provide demonstration videos of the interfaces for each of the three approaches.[2] showing how to cast a vote and how to file a complaint. Please note, the study was conducted in German. For accessibility, we translated the interface texts from German to English. All materials used in the study are also attainable in the appendix.

1. Since the submission to EuroS&P a publication describing the technical details of this general idea has been published by Haenni et al. [31].

2. Overview of all videos on the voting and complaint filing process: https://secuso.org/2026-03-24_EuroSP_Reliable_Voter_Complaints/Videos/, last accessed: 25.03.2025

4. Methodology

This section describes the methodology of our study. We begin by presenting the research questions and their connection to our research contributions, followed by an explanation of the simulated manipulation and a detailed description of the study procedure. The section concludes with ethical considerations and a description of our data collection and analysis methods.

4.1. Research Questions & Study Groups

In very short, *Cancelable Vote & Confirm* extends the baseline *Vote & Confirm* approach by offering voters a reliable way to file a complaint and *Cancelable Vote & Go* shortens the voting process but offers a reliable way to file a complaint. However, it is unclear whether the integration of this mechanism affects usability or the voters' ability to detect manipulation attempts. To investigate these potential effects, addressing our research contribution 2 - empirical evaluation of its effect on usability and manipulation detection rate, we formulate the following research questions:

$\mathbf{RQ1}_{Usability}$: Do the three approaches differ in the usability of the vote-casting process?

- $\mathbf{RQ1.1}_{Effectiveness}$: Do participants of the three approaches differ in their ability to successfully cast a vote?
- $\mathbf{RQ1.2}_{Efficiency}$: Do participants of the three approaches differ in their required time to successfully cast a vote?
- $\mathbf{RQ1.3}_{Satisfaction}$: Do participants of the three approaches differ in their perceived satisfaction with the vote-casting process, as measured by the System Usability Scale (SUS)?

$\mathbf{RQ2}_{Detection}$: Do participants of the three approaches differ in their ability to detect manipulations?

Beyond usability and manipulation detection, we aim to closely examine the complaint filing mechanism itself. Specifically, we investigate whether voters can effectively use them and how they can be further improved. By effectively use we mean are they able to successfully file a complaint once they detect a manipulation. To address our research contribution 3 - empirical evaluation of the proposals effectiveness, we pose our third research question:

$\mathbf{RQ3}_{Complaint}$: Can voters effectively use the proposed complaint filing mechanism?

4.2. Manipulation

In order to answer $\mathbf{RQ2}_{Detection}$ and $\mathbf{RQ3}_{Complaint}$, we simulate a verification prevention manipulation (see also Section 2.3) as, in past studies, this one was more challenging for participants to detect compared to the vote tampering one [1]. Such an attack could be conducted by either a manipulated voting system or by a manipulated vote casting device. For our study we focus on a manipulated vote casting device, as this is the more powerful

attack and is also more relevant w.r.t. filing complaints. Correspondingly, we assume that the attacker has full control of the voter's cote casting device.

The manipulation was implemented as follows: Once voters cast their vote, instead of receiving the expected return code for the selected party, a success message was displayed informing that the return code was automatically checked and a vote for the voter's intended choice was recorded. The selected party was also displayed again.

For participants using the *Vote & Confirm* and *Cancelable Vote & Confirm* approaches, the attacker would aim to trick the voter into providing their confirmation code, allowing the attacker to confirm the manipulated vote. Note, in order for a (changed) ballot to be tallied it needs to be confirmed with the confirmation code. Correspondingly, the return code was replaced by the following text:

> "We have checked your verification code for you, and it matches the vote you cast. Please verify if the party displayed above corresponds to your chosen party. If the displayed party does not match the one you selected, please report this immediately using the "File Complaint" button below. If the displayed party matches the one you selected, enter the confirmation code so that your vote is counted in the tally."

Below this text, the interface asked to enter the confirmation code as on the authentic system. For the corresponding screenshots, we refer the reader to Appendix D.

To investigate $\mathbf{RQ3}_{Complaint}$ we assumed that an attacker controlling the voter's vote casting device would also attempt to prevent voters who detect a manipulation from successfully filing a complaint. This was simulated in the following way: Once the complaint filing website was requested, it was checked whether the request was sent from a device used for vote casting[3]. If this was the case, they were redirected to a deceptive complaint filing website, visually indistinguishable from the official complaint filing website mentioned in the voting material. Similarly, it asks voters to enter their Complaint Code.

For participants using the *Cancelable Vote & Go* approach, the attacker merely sought to suppress any complaint and reassure the voter that no issue existed, as this approach does not require explicit vote confirmation. In the *Cancelable Vote & Go* approach, the deceptive complaint filing website displayed the following message (once the complaint code was entered):

> "Thank you for filing your complaint! We have reviewed your filed complaint, as well as the vote currently recorded for you, and fortunately, we did not find any issues. No further actions are required from you. Should you have any further questions, please contact us via email at: [anonymised]"

As explained before, for participants using the *Cancelable Vote & Confirm* approach, an attacker would make sure that voters provide their confirmation code. Therefore the text on this page was slightly different:

> "Thank you for filing your complaint! We have reviewed your filed complaint, as well as the vote currently recorded for you, and fortunately, we did not find any issues. Please return to the voting website now and complete the vote submission by entering the confirmation code. Should you have any further questions, please contact us via email at: [anonymised]"

For the corresponding screenshots, we refer the reader to Appendix E.

Voters can detect that they have opened the deceptive complaint filing website by noticing the missing complaint return code. Note, the attacker can not provide the correct complaint return code, because the complaint is not filed. To successfully file a complaint participants needed to use another device than the one they used for vote casting. Figure 3 illustrates how the simulated manipulation was implemented.

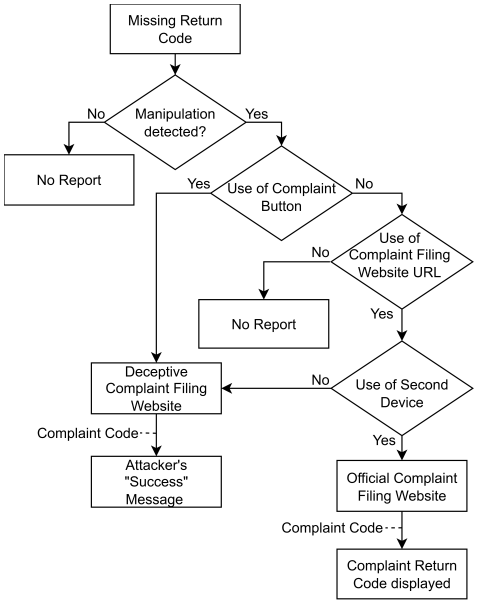

Figure 3. Overview of the simulated manipulation. Voters can get misled by the attacker's complaint button which leads to a deceptive complaint filing website. They receive a fake success message after sending their complaint code to the attacker. The same happens when the URL to the complaint filing website is entered on the device used for vote casting.

4.3. Study Procedure

The study was conducted over a period of nine weeks and consisted of three consecutive phases: Phase 1, an intermediate phase, and Phase 2. Each phase lasted approximately three weeks. Participants were randomly assigned to one of three approaches (i.e., *Vote & Confirm*, *Cancelable Vote & Confirm*, or *Cancelable Vote & Go*). They used the same approach during the entire study and were told to evaluate and provide feedback on the usability. We simulated a European Parliament Election as the actual election for the European Parliament happened earlier this year.

Phase 1 and Phase 2 followed the same structure: participants received a study package by postal mail, cast their vote online, and subsequently completed an online questionnaire. After completing the online questionnaire, they were provided with a unique payment code. The intermediate phase was used to make some changes to the UI of the voting systems.

Each postal package consisted of three colour-coded envelopes and an overview sheet (see figure in the Ap-

3. We do not distinguish between the following two scenarios because we assume the attacker controls the voter's device to cast their vote: (1) Participants clicking on the "File Complaint" button in the main voting interface after vote casting. (2) Participants typing in the URL on the device used for vote casting.

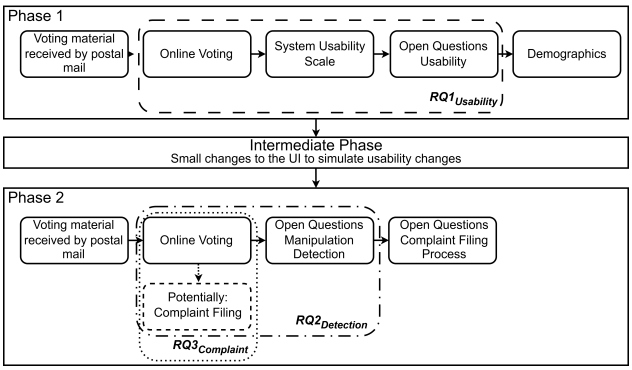

Figure 4. Study procedure: The three phases of the study participants took part in and their relation to the posed research questions. For research question 1 *Usability* results of the SUS and open questions after the voting process in Phase 1 are used. Research question 2 *Detection* deals with the results of the voting process in Phase 2 and the subsequent open questions. Research question 3 *Complaint* looks at the voting process in Phase 2 and the potential complaints.

pendix A.1) describing the order of steps participants needed to follow in this phase. The white envelope included general study instructions and the participant's role card, specifying their voter ID and a fictitious voting preference to preserve vote secrecy. The green envelope[4] represented the official election material, i.e. an election invitation letter and a step-by-step voting guide with the participant's individual codes. The red envelope contained a short link to the online questionnaire.

All materials used in the study are provided in Appendix A. An overview of the entire procedure is shown in Figure 4 including which parts are used to answer which research question. Next, we describe each phase in detail.

Phase 1. Participants were asked to follow the procedure according to the overview document (see figure in Appendix A.1), i.e. reading the materials, participating in the election, and immediately afterwards filling out the online questionnaire. This questionnaire contained the System Usability Scale (SUS) [33] questions for quantitative usability assessment[5], open questions assessing what participants (dis)liked about the system and if they have further remarks, which were added to upkeep the cover story of the study being a two-phase usability study that would integrate user feedback. The survey of Phase 1 ended with collecting participants' demographic data (age and gender).

After submitting the questionnaire, participants were informed that Phase 2 would begin three weeks later, supposedly to allow time to implement the "usability improvements" based on their feedback. Finally, participants received a unique payment code which also signalled to the provider that the finished Phase 1 successfully [6].

Intermediate Phase. The intermediate phase between Phase 1 and Phase 2 served to maintain the cover story that the voting systems were being revised based on their feedback. To support this narrative without introducing new confounding factors, only minor visual adjustments were made to the user interfaces, i.e. changes to colour schemes. Importantly, no changes to the voting process itself were introduced.

Phase 2. In Phase 2, we simulated a manipulation (as described in Subsection 4.2), i.e. simulated participants casting a vote from a device which the attacker controls. Participants received a new package via postal mail and were asked to follow the procedures according to the overview document. Immediately after completing the voting process, and potentially filing a complaint, participants filled out the second online questionnaire. Following the approach of Hilt et al. [1], this questionnaire first asked whether participants had noticed anything unusual during the voting process and, if so, to describe it in free text. Participants who reported noticing irregularities were then asked whether and how they had filed a complaint, or, if they had not done so, to explain their reasoning. Afterwards, participants were fully debriefed (for more information see Section 4.5). Participants then received their payment code.

4.4. Pre-Study

Before the main study, we conducted a small pre-study with acquaintances to verify the technical setup and clarity of instructions. Two participants per system took part, resulting in six participants in total. The goal was to identify potential flaws in the study procedure, voting interfaces, or study instructions. No major issues were observed. Minor adjustments were made to improve visual consistency and the wording of study instructions before the main study commenced. Please note, the documents in the appendix and the interfaces from the videos are those from the actual study.

4.5. Recruitment, Ethical Considerations & Data Protection

Participants were recruited through a professional service provider specialised in assembling representative samples for user studies in Germany.

Eligible participants were required to be at least 18 years old, fluent in German, and to possess access to at least two Internet-capable devices (ideally a computer or laptop and a smartphone or tablet). Note, this was necessary for our simulated manipulation as complaints to be successful needed to be filed from a device distinct from the voting device (see Section 4.2). To avoid bias, individuals with prior experience in user studies related to remote online voting or electronic voting were excluded.

Participants received a reimbursement of 50 € for completing both study phases. While this amount exceeds the local hourly minimum wage, it was determined in consultation with the recruitment provider to ensure sufficient motivation, reliability, and representativeness of the sample, as the study spanned an extended period and required participants to return for Phase 2. Participants who completed only Phase 1 received 20 €.

4. This envelope contains the information a voter would receive in an actual election.

5. We used the translated German version of the SUS [34].

6. Participants who successfully finished Phase 1 but did not finish Phase 2 received a partial reimbursement, as described in Section 4.5

The study was reviewed and approved by the ethics committee of our institution. It was announced to the participants as a two-phase usability study intended to gather and implement user feedback on an online voting system. Thus, in particular, we did not mention the simulated manipulation in Phase 2 during recruitment and not in the study information. This deception was necessary to avoid priming participants to actively search for manipulations, which could have biased the results. Participants were fully debriefed in Phase 2. Here, the true purpose of the study and the nature of the manipulation were explained in detail, including how the manipulation could be detected. The full text is attainable in the Appendix A.5.

All data were collected and processed in accordance with institutional data protection policies and the EU General Data Protection Regulation (GDPR). The external recruitment provider had access to participants' postal addresses and real identities for study coordination; this provider did not receive any study data. We prepared the envelopes per study group and phase with pseudonyms as voter ID. We did not receive and/or store sensitive or personally identifying data. Survey responses were pseudonymised and stored on servers located in Germany, and system interaction logs contained only pseudonymous identifiers. No IP addresses were recorded. Survey responses were obtained through SoSci Survey [7]

The provider handled the informed consent prior to participation. Participants provided written informed consent (see in the Appendix A.4).

4.6. Data Collection

Data collection combined server-side logging of system interactions with SoSci Survey. Both data sources were pseudonymised and linked via participants' voter ID, from their role card.

Interaction data were logged during each voting session to reconstruct participants' user journey and assess effectiveness and efficiency. For each participant, every event representing one step in the voting process was recorded alongside their voter ID, timestamp and browser fingerprint. [8]

Browser fingerprint was used to determine whether the device used for vote casting differed from the device used to file a complaint, allowing us to infer whether participants changed devices between these actions (see Section 4.2. This method was chosen as the most privacy-preserving option available, as it did not involve cookies, local storage, or persistent identifiers. We acknowledge that fingerprinting provides only approximate identification and may result in occasional collisions or false negatives.

If a participant filed a complaint through the official complaint filing website, the content of the complaint, along with the provided complaint code (where applicable), was captured and linked to their study ID.

7. SoSci Survey is fully GDPR-compliant and hosted on servers located in Germany. https://www.soscisurvey.de/, last accessed 18.11.2025.

8. For browser fingerprinting the *FingerprintJS* library (v4.5.0) was used. Source code available at https://github.com/fingerprintjs/fingerprintjs, last accessed 13.11.2025

4.7. Data Analysis

Data Cleaning. In total 192 participants were recruited for Phase 1 with the goal of having at least 50 participants from each approach finishing Phase 1 and Phase 2. Only participants that successfully finished Phase 1 were contacted to participate in Phase 2. The final sample comprised n=150 participants: *Vote & Confirm* (n=50), *Cancelable Vote & Confirm* (n=52), and *Cancelable Vote & Go* (n=48). Outliers for voting-task duration and SUS scores were removed using the 1.5×IQR rule within each condition (n=8). One additional case was excluded because the participant could not reach the research team via phone, and five participants were excluded for not completing phase 2 questionnaire directly after using the voting system, but several hours later.

Usability. Usability (effectiveness, efficiency, satisfaction) was analysed statistically. Effectiveness was examined by the participants ability to successfully cast a vote. Efficiency was examined by the completion time needed to successfully cast a vote from visiting the voting website to the display of the return code (for *Cancelable Vote & Go*) or the finalisation code (for *Vote & Confirm* and *Cancelable Vote & Confirm*). Satisfaction was assessed with SUS scale. Important to mention, we only analysed these metrics for the not-manipulated trial in Phase 1.

Participants "usability feedback" from Phase 1, which was collected as part of the cover story, was also inspected by two independent coder to identify potential flaws that would need fixing before Phase 2. [9]

Manipulation Detection Rate. Detection was defined as either (a) explicitly describing the manipulation in the post-task questionnaire (e.g., noting that the return code was missing) or (b) attempting to file a complaint containing a reference to the manipulation, regardless of whether the complaint was successfully submitted. Two independent coders classified all open-text responses as *detected* (= 0) or *not detected* (= 1). Disagreements were resolved through discussion until full consensus was reached. The resulting binary list was analysed statistically.

Effectiveness of Complaint Filing. As filing a complaint presupposes that the manipulation was detected, only those participants who had identified the manipulation were included in the following analysis. Similar to the manipulation detection classification process all open-texts submitted with the complaint were classified by two independent coders. Disagreements were resolved through discussion until full consensus was reached. To capture different aspects of complaint filing behaviour, we predefined several metrics:

- *Filed to attacker* includes participants who initially filed a complaint using the deceptive complaint button within the manipulated voting interface or by visiting the complaint filing website with the same

9. No critical issues were noted that would need to be fixed for Phase 2.

device used for voting, which resulted in their report being intercepted.

- *Changed complaint* captures those who first submitted a complaint to the attacker but subsequently repeated the process via the official channel, likely after noticing the missing complaint return code.
- *Successful complaint* refers to participants who filed their complaint through the legitimate reporting channel using a different device and received the correct complaint return code, providing cryptographic proof of successful submission.

5. Results

Our results are structured as follows. We begin by presenting demographic information about our participants. We then report the findings for our three research questions, addressing usability ($\mathbf{RQ1}_{Usability}$), manipulation detection ($\mathbf{RQ2}_{Detection}$), and complaint filing ($\mathbf{RQ3}_{Complaint}$). Finally, we summarise further findings identified during the analysis.

5.1. Demographics

From our 150 participants, 64 identified as male, 85 as female and one preferred not to disclose their gender. The distribution across age groups and gender was very evenly across the systems, as shown in Table 1.

TABLE 1. AGE DISTRIBUTION BY SYSTEM, WITH GENDER SPLIT (M/F/D).

Age bin	Vote & Confirm	Cancelable Vote & Confirm	Cancelable Vote & Go
18–30	3/6/1	7/5/0	7/7/0
31–40	6/6/0	5/7/0	2/4/0
41–50	6/5/0	6/3/0	8/4/0
51–60	3/6/0	4/7/0	5/6/0
61+	4/4/0	5/3/0	3/2/0

5.2. Usability

Answering $\mathbf{RQ1}_{Usability}$ we analysed usability across three dimensions: effectiveness, efficiency, and satisfaction.

Effectiveness. All participants across all three approaches successfully cast a vote, indicating that the systems were equally effective in supporting task completion. Accordingly, no significant differences were found. Consequently, no between-group differences exist, and statistical testing was not conducted due to the absence of variance.

Efficiency. Completion time differed significantly between the three approaches. Figure 5 visualizes the distribution of task durations across the three approaches.

Participants using *Vote & Confirm* required on average 107.88 s ($SD = 38.90$) to cast their vote, those using *Cancelable Vote & Confirm* 104.05 s ($SD = 42.09$), and those using *Cancelable Vote & Go* 37.82 s ($SD = 16.95$).

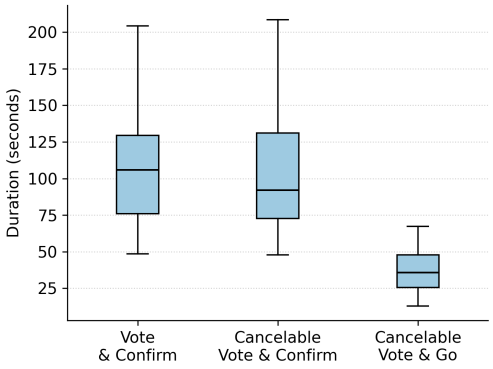

Figure 5. Distribution of task duration for the vote-casting process across the three approaches.

As the data did not meet the assumptions of normality and homogeneity of variances, a Kruskal–Wallis test was used, which indicated a significant effect of system type on task duration ($H = 80.43$, $p < .001$). Post-hoc Mann–Whitney U tests with Holm correction revealed that *Cancelable Vote & Go* was significantly faster than both *Vote & Confirm* ($U = 2096.0$, $p < .001$) and *Cancelable Vote & Confirm* ($U = 2129.0$, $p < .001$), while no significant difference was found between *Vote & Confirm* and *Cancelable Vote & Confirm* ($U = 1268.0$, $p = .509$).

Satisfaction. The archived SUS scores indicate excellent usability according to [33] for all three approaches: *Vote & Confirm* achieved a mean score of 87.15 ($SD = 11.61$), *Cancelable Vote & Confirm* 81.3 ($SD = 16.95$), and *Cancelable Vote & Go* 85.26 ($SD = 11.86$). Figure 6 shows the distribution of SUS scores across the three approaches. As the data did not meet the assumptions of normality and homogeneity of variances, a Kruskal–Wallis test was used, which found no significant differences between the approaches ($H = 2.26$, $p = .323$). These excellent SUS scores are in line with prior related work on the return-code based approach, which is usually perceived as very usable (e.g., [3], [6]).

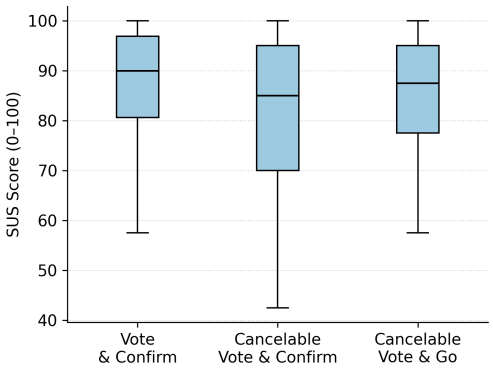

Figure 6. Distribution of System Usability Scale (SUS) scores across the three approaches. All approaches achieved excellent usability ratings, and no significant differences were observed.

Takeaway: The findings for $\mathbf{RQ1}_{Usability}$ *show that*

the three voting approaches do not differ in effectiveness ($\mathbf{RQ1.1}_{Effectiveness}$*) or in satisfaction (*$\mathbf{RQ1.3}_{Satisfaction}$*), but they do differ in efficiency (*$\mathbf{RQ1.2}_{Efficiency}$*) - Cancelable Vote & Go is faster than both Vote & Confirm and Cancelable Vote & Confirm (the latter two do not differ from each other).*

5.3. Manipulation Detection

We examined whether the three approaches differed in participants' ability to detect manipulations, answering $\mathbf{RQ2}_{Detection}$.

Detection rates were 36% $(18/50)$ for *Vote & Confirm*, 44% $(23/52)$ for *Cancelable Vote & Confirm*, and 54% $(26/48)$ for *Cancelable Vote & Go*. A chi-square test of independence revealed no significant differences between the three groups ($\chi^2(2, N{=}150) = 3.28$, $p = .194$). We further tested if demographic information had an effect on detection capabilities but found no effect, neither based on age ($p = 0.227$) or gender ($p = 0.69$).

Takeaway: Regarding $\mathbf{RQ2}_{Detection}$*, the analysis consistently shows comparable results across all groups, indicating the absence of a group effect for manipulation detection.*

5.4. Reliably Filing a Complaint

To answer $\mathbf{RQ3}_{Complaint}$, we analysed participants' ability to reliably file a complaint only for the two approaches that implemented the proposed mechanism, *Cancelable Vote & Confirm* and *Cancelable Vote & Go*. In *Vote & Confirm*, participants could attempt to report an issue, but they did not receive a verifiable confirmation, and these data are therefore excluded from this analysis.

For the *Cancelable Vote & Confirm* approach 22 out of 23 people that detected the manipulation tried to file a complaint (95.65%) , while in the *Cancelable Vote & Go* approach all 26 out of the 26 participants that detected the manipulation tried to file a complaint (100%). Figure 7 gives an overview of participants complaint filing behaviour.

Seven in *Cancelable Vote & Confirm* and eleven in *Cancelable Vote & Go* filed a successful complaint on their first attempt, i.e., they visited the complaint filing website with a different device and submitted their complaint code. In both, (*Cancelable Vote & Confirm*) and (*Cancelable Vote & Go*), a majority of 15 participants first filed an unsuccessful complaint, from which nine for *Cancelable Vote & Confirm* and eight for *Cancelable Vote & Go* noticed the missing complaint return code, changed their device and filed another, successful, complaint with their second device. In total, six people in *Cancelable Vote & Confirm* and seven *Cancelable Vote & Go* were unable to successfully file a complaint (both 27% of all the people within their specific group that tried to file a complaint). Notably, all six people from *Cancelable Vote & Confirm* that did not change devices to file a second complaint were likely convinced by the attackers message. All six consequently returned to the voting system and confirmed their ballot with their confirmation code. The one person from *Cancelable Vote & Confirm* who detected the manipulation but did not try to file a complaint answered in the survey, that they noticed the missing return code but the existence of the input field for the confirmation code distracted them mentally. The participants that successfully filed a complaint explained in the survey, that they changed devices as the instructions specifically instructed them to do so.

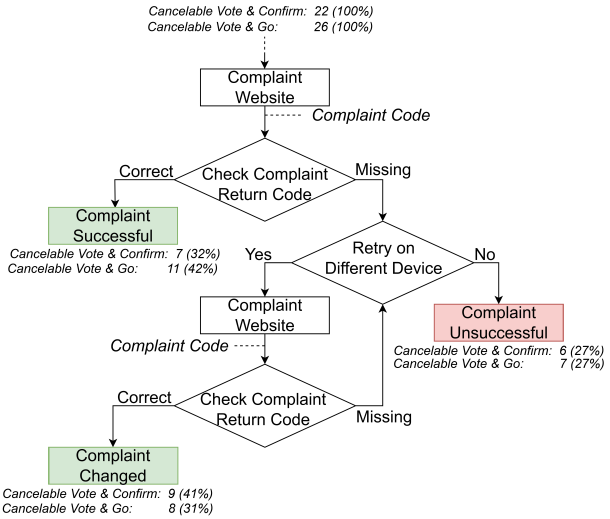

Figure 7. Overview over participants complaint filing behaviour. "Complaint unsuccessful" is highlighted in red, as the attacker reaches their goal in this case - in the case of *Cancelable Vote & Confirm* all six participants returned to the voting system and submitted their confirmation code, whereas in *Cancelable Vote & Go* the attacker successfully suppressed their complaint. To assess the number of total complaints filed successfully, one has to summarise the values of "Complaint successful" and "Complaint changed", both highlighted in green.

In total though 73% $(16/22;\ 19/26)$ of participants of both approaches that detected the manipulation eventually filed a complaint successfully.

Takeaway: With respect to $\mathbf{RQ3}_{Complaint}$*, the findings indicate that the majority of participants who detected the manipulation were able to file a complaint successfully, showing that the proposed complaint-filing mechanism can be used effectively.*

5.5. Further Findings

First, we present some findings on the complaint filing behaviour of participants from *Vote & Confirm*. We then present some insights for all approaches learned from inspecting the participants responses to the open questions regarding "usability feedback" asked as part of the cover story in Phase 1.

In *Vote & Confirm*, although participants lacked a verifiable reporting mechanism, 88.9% of participants that detected the manipulation $(16/18)$ still attempted to file a complaint. However, only 37.5% $(6/16)$ submitted their complaint with a second device and the remaining ten participants were deceived by the deceptive complaint filing website that no issue exists, that they can confirm their vote and they actually provided the confirmation code on the voting website.

The open feedback revealed that participants perceived the usability of all the approaches (*Vote & Confirm*, *Cancelable Vote & Confirm* & *Cancelable Vote & Go*)

very positively. They especially highlighted the simplicity of the interfaces and the easy to understand and follow code sheets. The reaction to the usage of (several) codes were mixed though: while some participants perceived the codes as contributing to a greater sense of security, others mentioned them as a source of additional effort and potential confusion. Participants suggested offering different ways of authenticating, for example using an e-ID[10]. They recommended adding a clear finalisation page at the end, consisting only of a short thank you message, to signal to voters that they can safely close the window and thus provide a clear sense of closure. They further proposed expanding the explanation of why the codes exist, why they should be checked, and what types of issues can be detected with them. In addition, some participants suggested providing an explanatory video on how the system works before it needs to be used, as well as offering a test platform with dummy data that everyone can have a look and practise in advance.

6. Discussion

The discussion is organised around the central insights emerging from our study. We first analyse how effectively voters were able to file complaints when supported by the proposed mechanism. We then consider the usability and manipulation-detection results and how they differ between approaches. Building on these observations, we examine the broader conceptual implications of verification-flow complexity. We conclude by outlining recommendations for the design of remote electronic voting systems (specifically return-code based approaches, but also in general), followed by limitations of our work and directions for future research.

6.1. Effectiveness of Complaint Filing Mechanism

Our findings indicate that the proposed mechanism to reliably file complaints helps voters to successfully file a complaint once they detect a manipulation. Across all systems, most participants who attempted to file a complaint were initially deceived by the attacker-controlled complaint button embedded in the manipulated interface, underscoring the strength of UI-based attacks when the voting device is compromised. However, the majority of participants from *Cancelable Vote & Confirm* $(9/15)$ and *Cancelable Vote & Go* $(8/15)$ recovered after this initial failure. They recognised the absence of the complaint return code and followed the instructions from the code sheet to switch devices and file another complaint. In total 73% of participants who detected the manipulation from both approaches with the mechanism for reliably filing complaints (*Cancelable Vote & Confirm* and *Cancelable Vote & Go*), were able to successfully file a complaint, compared to only 37.5% $(6/16)$ from the approach without this mechanism (*Vote & Confirm*). Participants explicitly referred to the postal voting material when describing their decisions, noting that it instructed them to distrust on-screen information and use a separate device for complaint filing. This demonstrates that clear instructions paired with a dedicated complaint filing channel, distinct from the voting system itself, can mitigate the effects of attacker-controlled interfaces. It also highlights the importance of clearly signalling to voters that the postal voting material takes precedence over any on-screen messages, which is crucial under a threat model where the attacker controls the voting device.

10. In Germany, a digital ID function is available, which can be used to authenticate citizens online: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/online-ausweisen/online-ausweisen-node.html, Last accessed: 20.11.2025

6.2. Usability and Manipulation Detection

The integration of this mechanism does not negatively impact the usability as all three usability metrics (effectiveness, efficiency and satisfaction) do not differ between *Vote & Confirm* and *Cancelable Vote & Confirm*. However, comparing all three approaches, participants from *Cancelable Vote & Go* were significantly faster, likely because it removes intermediate confirmation code entry and finalisation code checking, while not differentiating w.r.t. effectiveness and satisfaction. This demonstrates that streamlining the flow can meaningfully reduce voter effort without compromising user satisfaction or task success. Manipulation detection rates did not differ significantly, even though differences could be observed: *Cancelable Vote & Go* achieved the highest detection rate (54%), followed by *Cancelable Vote & Confirm* (44%) and *Vote & Confirm* (36%). Although no statistical significance could be detected, this trend suggests that removing complexity, i.e., by removing the confirmation code and finalisation code step, may increase participants ability to detect missing return codes.

6.3. The Cost of Complexity

This observation runs counter to the intention behind the Swiss extension: rather than enhancing voters' attentiveness, the additional confirmation and finalisation steps appear to divert attention away from the return code. In our study, participants using *Cancelable Vote & Go*, which omits these extra steps, detected manipulations most frequently. A plausible explanation is that some participants in *Vote & Confirm* and *Cancelable Vote & Confirm* expected the missing return code to appear at a later stage of the process. Since the return code check in those systems occurs mid-process and is followed by additional system-provided codes, a missing return code may not be interpreted as the final outcome. By contrast, *Cancelable Vote & Go* deliberately positions the return code check as the final system-provided action, leaving no plausible interpretation that a missing code might still appear later. This clearer end-state likely reduced ambiguity and may have contributed to the numerically higher detection rate observed in *Cancelable Vote & Go*. The different end-states reflect the underlying conceptual distinctions between the approaches. *Vote & Confirm*, based on the Swiss extension, and *Cancelable Vote & Confirm*, which adds the proposed complaint filing mechanism, treat correctness of the return code as something that must be explicitly confirmed by the voter. This explicit confirmation produces a finalisation code which is expected to be checked – but cannot itself be confirmed by an additional step without creating an infinite confirmation loop. As a

result, voters are asked to confirm one system-provided code (the return code) but merely inspect another (the finalisation code), adding procedural complexity without resolving the structural limitation of the process ending with a system-provided code. Instead of requiring mid-process confirmations, the proposed mechanism equips voters to reliably file complaints when an anomaly is detected. This design reduces cognitive load, removes ambiguous transitional steps, and creates a clear and interpretable endpoint. These properties likely contributed to the higher (though non-significant) detection rate observed in *Cancelable Vote & Go* and highlight the advantages of simplifying the verification process rather than layering additional confirmation codes.

6.4. Recommendations

Taken together, these findings suggest that future work on the return-code based approach, as well as its deployment in Switzerland, should reconsider the "extra round" of confirmation and finalisation codes. Rather than improving security, these additional steps appear to increase cognitive load and introduce ambiguity about when the verification process is actually complete. Removing these steps could not only support higher detection rates but also reduce the risk that voters inadvertently fail to submit the confirmation code and thereby render their ballot invalid – particularly if they assume that the process ends after the display of the (correct) return codes. Moreover, removing this extra round shortens the overall task duration of the vote-casting process, which voters are likely to appreciate. Instead, integrating the proposed mechanism for reliably filing complaints may offer a more effective pathway to strengthening individual verifiability. Our findings show that voters can successfully use this mechanism even under a strong threat model in which the attacker fully controls the voting device. Clear instructions paired with an independent complaint channel allow voters to act on anomalies without needing to navigate complex multi-step confirmation procedures. These insights should inform both future refinements of return-code based approaches and ongoing national deployments. Moreover, since our results show that integrating the proposed complaint mechanism does not negatively impact usability or manipulation detection, while providing clear security benefits by enabling voters to reliably file complaints remotely, this mechanism should be incorporated into all remote electronic voting systems that already use a distributed back end.

6.5. Limitations

As with any controlled study, our work is subject to several limitations that must be taken into account when interpreting the findings. First, the study was conducted in a simulated election environment without real political stakes. Participants did not face the personal, emotional, or societal consequences that may accompany real elections, and their motivation to detect or report anomalies may therefore differ from behaviour in an actual voting context.

Participants were also specifically instructed to read all the materials carefully before casting their vote, which may not happen in an actual election.

We assume the existence of a trustworthy postal channel, voter adherence to the intended protocol and voters having access to at least two devices, which limits the applicability of the proposed mechanism (and internet voting in general) for elections where these assumptions are not met.

Our sample was recruited through a service provider specialised in recruiting participants for user studies, which introduces the typical self-selection biases. Although we ensured a balanced distribution across age and gender, panel participants may differ from the general population in digital experience, motivation, or attentiveness. The generalisability of the results to all eligible voters should therefore be treated with caution.

Another limitation concerns how we identified whether participants changed devices when filing a complaint. We relied on browser fingerprinting techniques that, while deliberately privacy-preserving, cannot guarantee perfect accuracy. More invasive approaches such as cookie-based device tracking would have provided more precise measurements but were intentionally avoided to protect participants' privacy. As a result, some device switches may have been misclassified.

Our design choice for the codesheet including explicit warning and red highlighting might represent another limitation. While this design supports the external validity of the study, as in real elections as well, voters can not be assumed to instinctively react appropriately to irregularities without guidance, hence strong visual cues are needed. However, this design choice may have influenced the perception of and trust into the voting system itself, which should be investigated in future work.

6.6. Future Work

Future work should further explore how to reduce the burden of interacting with different kinds of codes without compromising security. Several participants suggested using QR codes to replace manual entry of the initialisation or confirmation codes. While QR-based submission could meaningfully improve usability, integrating QR codes into a return-code based approach requires careful redesign. Scanning QR codes from the physical code sheet risks leaking return codes to a compromised device fully under the attackers control, which would render manipulations undetectable. Prior work by Thürwächter et al. [7] already examined the integration of QR codes for the submission of all codes into the return-code based approach utilizing code voting. They found that the manipulation detection rate could be improved but did not examine the effect on usability. Future work should investigate how the integration of QR codes affects the usability.

While we tested this complaint filing approach for the return-code based approach, as it represents a minimal extension to existing functionalities within this approach, its applicability is not limited to the return-code based approach. Future work should investigate both the effectiveness of the complaint filing approach as well as its effect on usability in other approaches for individual verifiability.

Alternative authentication methods were also proposed by participants, including ID–password combinations or the use of national e-IDs. Such approaches may reduce

friction and increase accessibility, but they introduce different trust and deployment considerations. In particular, adoption of e-ID systems is currently low in many countries, and authentication performed entirely on the compromised voting device may not meaningfully change the attacker model. Future work should therefore examine how alternative authentication methods can be integrated into return-code based approaches.

A number of participants further noted that the terminology used throughout the system (several different values all being referred to as "codes") was confusing. We intentionally refrained from modifying terminology in this study, as doing so between Phase 1 and Phase 2 could have affected participants' ability to detect manipulations. Future work should explore alternative terminology or design representations for the various codes and examine whether such changes improve usability or manipulation detection.

Another direction concerns attacker objectives. Our study focused on a targeted manipulation in which the attacker aims to change a vote to a specific alternative option. In this scenario, the attacker needs to convince voter from *Vote & Confirm* and *Cancelable Vote & Confirm* to submit their confirmation code in order for the vote to be successfully cast. However, attackers who simply wish to drop votes for a specific candidate do not require the confirmation code and instead only need to suppress any subsequent complaint. In such a scenario the attackers goal would align across all three systems, as the attacker would only need to suppress filed complaints. Consequently, the manipulation detection rates in such a scenario may differ from our results. Future research should therefore examine how different attacker objectives, such as changing votes or dropping votes, interact with the structure of each approach and how attacker success rates vary across these scenarios.

Finally, the proposed complaint mechanism was originally designed to support voters residing abroad who may not be able to physically visit consular offices to file complaints. However, the mechanism may equally benefit domestic voters by reducing effort and increasing accessibility. At the same time, making complaint filing too easy could introduce new challenges: some voters may file complaints inadvertently or without understanding their severity, and malicious actors could intentionally file false complaints to undermine public trust. Future work should therefore examine how to balance accessibility with appropriate friction to ensure that complaints remain meaningful and that the mechanism is not misused.

7. Conclusion

We proposed a mechanism that allows voters to remotely file a reliable complaint, building on principles introduced in the Swiss extension of the return-code based approach, which can be integrated in every remote verifiable electronic voting system that already operates on a distributed back end.

In our user evaluation, we investigated how voters interact with three variants of the return-code based approach for remote electronic voting system under a strong threat model in which the attacker controls the vote casting device. Our results demonstrate that integrating a dedicated mechanism for reliably filing complaints does not decrease usability or voters' ability to detect manipulations. Participants were able to follow the instructions from the postal voting material, switch devices, and file a correct complaint even after initially being deceived by an attacker-controlled interface. Importantly, this mechanism offers these security benefits without negatively affecting usability or manipulation detection.

Our findings also highlight that the additional confirmation round currently used in the Swiss extension of the return-code based approach adds complexity without clear benefit. The confirmation and finalisation code steps increased task duration and, descriptively, reduced manipulation detection. Moreover, this extra round creates the risk that voters may believe the process is complete after the return code is shown and unintentionally fail to submit the confirmation code, rendering their vote invalid. For both applied deployments and future research, our results therefore indicate that the confirmation round should be removed in favour of simpler flows that reduce cognitive load and provide a clearer end-state to voters, as proposed in *Cancelable Vote & Go*.

Taken together, these insights suggest a concrete path forward for the design of secure and usable remote electronic voting systems: provide voters with a trustworthy, attacker-independent channel for filing complaints, and avoid unnecessary confirmation steps that complicate the process without improving verifiability. For any remote electronic voting systems, both in practice and in research, that already operates on a distributed back end, the proposed complaint mechanism can be integrated with comparatively little effort. We therefore recommend its adoption in all such systems, and encourage future research on the return-code based approach to return to the conceptual foundations of the approach rather than adhering to the more complex Swiss variant solely because it is deployed in practice.

Acknowledgements

This work was supported by funding from the project "Engineering Secure Systems" of the Helmholtz Association (HGF) [subtopic 46.23.01 Methods for Engineering Secure Systems], KASTEL Security Research Lab and "armasuisse Science and Technology" (project number AR-CYD-C-031).

References

[1] T. Hilt, B. Berens, T. Truderung, M. Udovychenko, S. Neumann, and M. Volkamer, "Systematic User Evaluation of a Second Device Based Cast-as-Intended Verifiability Approach," in *Financial Cryptography and Data Security. FC 2024 International Workshops*. Berlin, Heidelberg: Springer, Nov. 2024, pp. 33–49. [Online]. Available: https://doi.org/10.1007/978-3-031-69231-4_3

[2] K. Marky, V. Zimmermann, M. Funk, J. Daubert, K. Bleck, and M. Mühlhäuser, "Improving the Usability and UX of the Swiss Internet Voting Interface," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 1–13. [Online]. Available: https://dl.acm.org/doi/10.1145/3313831.3376769

[3] K. Marky, M.-L. Zollinger, P. Roenne, P. Y. A. Ryan, T. Grube, and K. Kunze, "Investigating usability and user experience of individually verifiable internet voting schemes," *ACM Trans. Comput.-Hum. Interact.*, vol. 28, no. 5, Sep. 2021. [Online]. Available: https://doi.org/10.1145/3459604

[4] O. Kulyk, J. Henzel, K. Renaud, and M. Volkamer, "Comparing "Challenge-Based" and "Code-Based" Internet Voting Verification Implementations," in *Human-Computer Interaction – INTERACT 2019*. Cham: Springer International Publishing, 2019, pp. 519–538.

[5] O. Kulyk, M. Volkamer, M. Müller, and K. Renaud, "Towards improving the efficacy of code-based verification in internet voting," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 291–309.

[6] M. Volkamer, O. Kulyk, J. Ludwig, and N. Fuhrberg, "Increasing security without decreasing usability: A comparison of various verifiable voting systems," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 233–252. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/volkamer

[7] P. T. Thürwächter, M. Volkamer, and O. Kulyk, "Individual Verifiability with Return Codes: Manipulation Detection Efficacy," in *Electronic Voting*. Cham: Springer International Publishing, 2022, pp. 139–156.

[8] C. Nissen, O. Kulyk, M. Volkamer, L. E. Fredrich, and H. Hermansen, "Tracking code-based verification - design and evaluation," in *E-Vote-ID 2024*. Bonn: Gesellschaft für Informatik, 2024, pp. 85–100.

[9] Website with information about e-voting in swiss cantons. Last accessed 13.11.2025. [Online]. Available: https://www.evoting-info.ch/sicherheit/einfache-tipps-fuer-mehr-sicherheit

[10] Website with information about e-voting of swiss canton st. gallen. Last accessed 13.11.2025. [Online]. Available: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html

[11] Website of valimised about internet voting fact check. Last accessed 13.11.2025. [Online]. Available: https://www.valimised.ee/en/internet-voting/i-voting-fact-check-myth-and-reality

[12] Website of tk about social elections 2023. Last accessed 13.11.2025. [Online]. Available: https://www.tk.de/techniker/unternehmensseiten/unternehmen/sozialwahl-2023/waehlen-sie-jetzt-online-2119940

[13] Website of gi. Last accessed 13.11.2025. [Online]. Available: https://gi.de/wahlen

[14] F. Moser, J. Müller, V. Cortier, A. Debant, P. Gaudry, A. Goetschmann, R. Küsters, and M. Volkamer, "A Study of Mechanisms for End-to-End Verifiable Online Voting," *BSI*, 2024, last accessed 14.11.2025. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Cryptography/End-to-End-Verifiable_Online-Voting.pdf

[15] J. Benaloh, "Simple verifiable elections," in *2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 06)*. Vancouver, B.C.: USENIX Association, Aug. 2006. [Online]. Available: https://www.usenix.org/conference/evt-06/simple-verifiable-elections

[16] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II," *USENIX Journal of Election Technology and Systems (JETS)*, pp. 26–56, 2014. [Online]. Available: https://www.usenix.org/jets/issues/0203/acemyan

[17] K. Marky, O. Kulyk, K. Renaud, and M. Volkamer, "What Did I Really Vote For? On the Usability of Verifiable E-Voting Schemes," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–13. [Online]. Available: https://dl.acm.org/doi/10.1145/3173574.3173750

[18] D. Galindo, S. Guasch, and J. Puiggalí, "2015 Neuchâtel's Cast-as-Intended Verification Mechanism," in *Proceedings of the 5th International Conference on E-Voting and Identity - Volume 9269*, ser. VoteID 2015. Berlin, Heidelberg: Springer, Sep. 2015, pp. 3–18. [Online]. Available: https://doi.org/10.1007/978-3-319-22270-7_1

[19] R. Haenni, R. E. Koenig, P. Locher, and E. Dubuis, "CHVote protocol specification," Cryptology ePrint Archive, Paper 2017/325, 2017. [Online]. Available: https://eprint.iacr.org/2017/325

[20] R. Haenni, R. Koenig, P. Locher, and E. Dubuis, "CHVote System Specification," Oct. 2017. [Online]. Available: https://www.bfh.ch/dam/jcr:a22d95f9-e935-4475-a12b-a3b7656c8093/Formale%20Spezifikation%20Genf.pdf

[21] O. Kulyk, S. Neumann, J. Budurushi, and M. Volkamer, "Nothing Comes for Free: How Much Usability Can You Sacrifice for Security?" *IEEE Security & Privacy*, vol. 15, no. 3, pp. 24–29, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7945211

[22] A. Damodaran, S. Rastikian, P. B. Rønne, and P. Y. A. Ryan, "Hyperion: Transparent End-to-End Verifiable Voting with Coercion Mitigation," 2024, publication info: Preprint. [Online]. Available: https://eprint.iacr.org/2024/1182

[23] P. Y. A. Ryan, P. B. Roenne, and V. Iovino, "Selene: Voting with Transparent Verifiability and Coercion-Mitigation," 2015. [Online]. Available: https://eprint.iacr.org/2015/1105

[24] V. Distler, M.-L. Zollinger, C. Lallemand, P. B. Roenne, P. Y. A. Ryan, and V. Koenig, "Security - Visible, Yet Unseen?" in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–13. [Online]. Available: https://dl.acm.org/doi/10.1145/3290605.3300835

[25] S. Heiberg and J. Willemson, "Verifiable internet voting in Estonia," in *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, Oct. 2014, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/7001135

[26] O. Pereira, "Individual Verifiability and Revoting in the Estonian Internet Voting System," 2021, publication info: Preprint. MINOR revision. [Online]. Available: https://eprint.iacr.org/2021/1098

[27] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. Scottsdale Arizona USA: ACM, Nov. 2014, pp. 703–715. [Online]. Available: https://dl.acm.org/doi/10.1145/2660267.2660315

[28] *Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) vom 1. Juli 2022*. Die Schweizerische Bundeskanzlei (BK), 2022.

[29] *Technische und administrative Anforderungen an die elektronischen Stimmabgabe (Version 2.0)*. Die Schweizerische Bundeskanzlei (BK), 2018.

[30] R. Haenni, R. E. Koenig, P. Locher, and E. Dubuis, "CHVote protocol specification – version 4.2," *IACR Cryptology ePrint Archive*, vol. 2017/325, 2024.

[31] R. Haenni, R. E. Koenig, and P. Locher, "Private online voting on untrusted devices without confirmations," in *Voting'26, FC 2026 International Workshops*, K. Marky and C. C. Drăgan, Eds., St. Kitts, 2023.

[32] M. M. Olembo, K. Renaud, S. Bartsch, and M. Volkamer, "Voter, What Message Will Motivate You To Verify Your Vote?" in *Proceedings 2014 Workshop on Usable Security*. San Diego, CA: Internet Society, 2014. [Online]. Available: https://www.ndss-symposium.org/ndss2014/workshop-usable-security-usec-2014-programme/voter-what-message-will-motivate-you-verify-your-vote

[33] J. Brooke, "SUS: A quick and dirty usability scale," *Usability Eval. Ind.*, no. 189, 1995.

[34] B. Rummel, "System usability scale (translated into german)," 04 2013.

Appendix A.
Study Material

A.1. Overview Figure

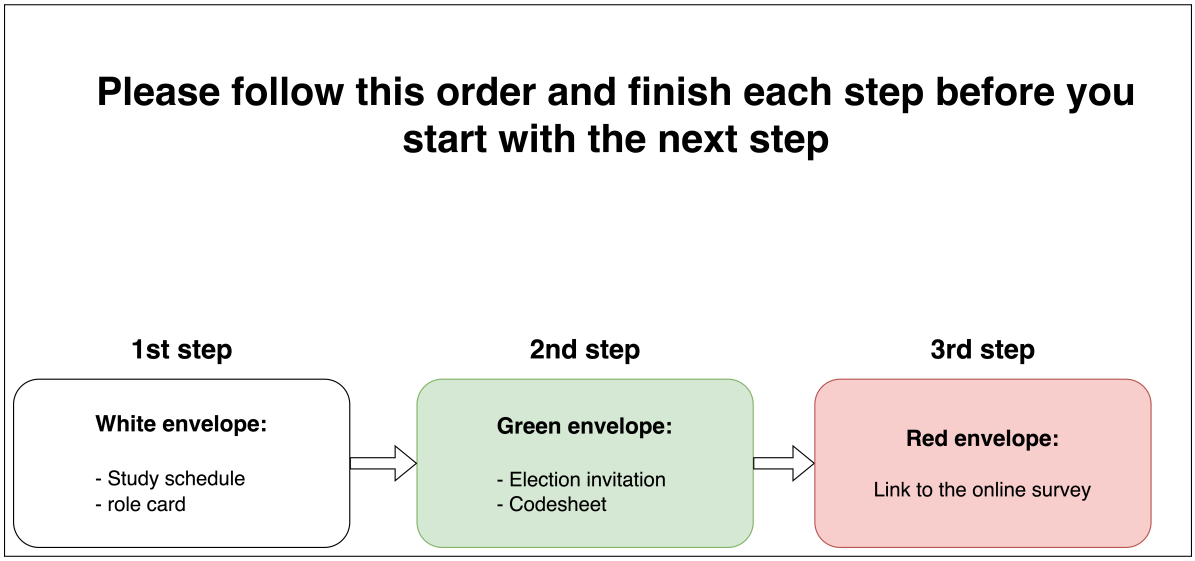

Figure 8. Overview figure participants received with their study material informing them about the schedule of the study. (Texts translated to English for reader's convenience; original texts were in German)

A.2. Role Card

Role Card

Imagine your name is Chris Musterperson, you were born in 1980, and you live in Germany. Your voter ID is:

RHKBD

As you have learned from the news, the European Parliament election is currently taking place.

You have decided to participate in this election. You informed yourself thoroughly beforehand and decided to cast your vote for the following party:

Christlich Demokratische Union Deutschlands (CDU)

Since this year, for the first time, there is the option to cast your vote online, you have decided to try out this new possibility yourself and submit your vote online. To do so, you previously requested the voting materials, which you have now received (see green envelope).

Figure 9. An example of a role card participants received for the study. The role card describe the persona one has to take for the study, their assigned voter ID and the party one has to select to protect their real vote secrecy. (Texts translated to English for reader's convenience; original texts were in German)

A.3. Study Invitation

Study Procedure – Please Read First!

Dear study participant,

Thank you very much for taking part in the study "Investigation of the Usability of a New Online Voting System"! You are currently in **Phase 2** of the study. Phase 2 runs from **28 November 2024 to 13 December 2024**.

Please read this study procedure carefully before reviewing the other documents.

Based on the feedback we received in Phase 1 of the study, we have revised the appearance of the online voting system. The functionality and basic process, however, remain the same. The goal of this phase is to evaluate whether the changes have improved the usability of the online voting system. **As in Phase 1, you will evaluate the voting system "hb".** Accordingly, the suffix "hb" will appear more frequently in your voting documents. When typing URLs, please pay close attention not to forget this suffix, so that you can successfully participate in the study.

The election you will conduct is once again a simulation of the European Election.

To protect the secrecy of the vote, you will again take on a role in the user study and cast a predetermined vote in this role. You will find more information about this on the enclosed role card.

You will again be asked to answer questions in the online questionnaire. Your answers will be stored by SoSciSurvey on servers located in Germany and later analyzed by [anonymized]. The collected information is not personalized and cannot be traced back to you.

Even after the revision, if something is unclear or not obvious when using the online voting system, this is not your fault but rather due to insufficient usability of the online voting system. Providing such feedback through the online questionnaire is very important for the further development of the system.

In this study, we again want to collect your assessment of the usability of the online voting system. **Therefore, we ask you to conduct the voting process and complete the online questionnaire directly one after the other.**

Figure 10. Front page of the study invitation. This was part of the instructions in the white envelope. We provide only the version for phase 2 here as they are nearly identical. They only differ in the phase number and voting period. (Texts translated to English for reader's convenience; original texts were in German)

Phase 2 proceeds as follows:

Step 1: After reading this document, please read your **role card**.

Step 2: Then open the **green envelope** containing your voting materials.

1. Read the **election invitation** carefully.

2. Then read the **codesheet** carefully.

3. Then carry out the voting process.

Step 3: After completing the voting process, open the **red envelope**.

1. Access the **online questionnaire**.

2. Enter your Voter ID from your **role card** and complete the online questionnaire.

3. At the end of the online questionnaire, you will receive a link to a website by Custom Interactions and a personal confirmation code for participating in the online questionnaire. Enter this code on the linked website.

The steps of this phase and the documents you will need are shown in the enclosed diagram.

If you have any questions regarding the study procedure, please send them to eu-wahl-support@institution.org.

Figure 11. Back page of the study invitation. (Texts translated to English for reader's convenience; original texts were in German)

A.4. Informed Consent

A.4.1. Phase 1. Dear participant,

Thank you for taking part in the online questionnaire for the first phase of our study on the evaluation of the usability of an online voting system. Your feedback is highly valuable to us.

Completing the questionnaire will take approximately 10–15 minutes. In this survey, we will ask you about the usability of the online voting system you have just used, including any suggestions for improvement. The responses you provide via SoSciSurvey are stored on servers located in Germany and will later be analysed by the research team conducting this study. All collected data are anonymised and cannot be traced back to you. Further details can be found in the data protection information.

By selecting the option "I have read the information sheet and consent to participate in the study and to the associated processing of my data." you confirm your informed consent to take part in this study.

A.4.2. Phase 2. Dear participant,

Thank you for taking part in the online questionnaire for the second phase of our study on the evaluation of the usability of an online voting system. Your feedback is highly valuable to us.

Completing the online questionnaire will take approximately 10–15 minutes. In this questionnaire, we will ask you about the usability of the online voting system you have just used, including any suggestions for improvement. The responses you provide via SoSciSurvey are stored on servers located in Germany and will later be analysed by the research team responsible for this study. All collected data are anonymised and cannot be traced back to you. Further details can be found in the data protection information.

By selecting the option "I have read the information sheet and consent to participate in the study and to the associated processing of my data." you confirm your informed consent to take part in this study.

A.5. Debriefing

Debriefing on the Actual Purpose of the Study

We would like to begin by informing you that, during the voting process in the second phase, an inconsistency occurred which was deliberately introduced by us. This was done to **simulate the manipulation of the voting device**. In other words, we replicated a scenario in which the device you used to cast your vote altered your vote in the background. (Your personal device was of course not manipulated; this behaviour was simulated solely through modifications to our voting system.)

An important aspect of the usability of **online voting systems** is the ability for voters to **reliably verify whether their vote has been recorded correctly**. Such systems also enable manipulations to be reliably detected. The voting system used in this study confirms the receipt of your vote using a unique return code (see Step 5.1 in the code sheet). If the return code displayed in the online system matches the code printed on your code sheet, you can be confident that your vote has been correctly recorded. If no return code is displayed online, or if the return code does not match the one on your card, this may indicate manipulation.

In this study, **the manipulation was simulated in such a way that no return code was shown to you**. Instead, you were presented with a message on the website claiming that the return codes had been checked automatically. In place of the return code, the system displayed the party you had selected. **A compromised voting device** could determine your actual choice but **would not know which return code on your code sheet corresponds to that choice**. For this reason, **voter code sheets are delivered by postal mail** rather than online: this prevents a manipulated device from learning the return codes and using this information to carry out a more effective deception.

If you noticed this manipulation, you were able to report the issue using the information on the code sheet and a **second device** that was not used for the online vote. After visiting the reporting website linked on the code sheet, the voter must enter the problem code printed there. The reporting page acknowledges receipt of the problem code with a corresponding problem-confirmation code. This provides the voter with proof that the problem has been successfully reported, and that election officials will subsequently investigate it. If the device used for reporting is also compromised and blocks the report, no confirmation code would be shown. If the reporting device does not display a confirmation code after the problem code is entered, the voter can be certain that this device is also manipulated. In such a case, the voter should switch to another device and submit the report again. Assuming that every voter has access to at least one uncompromised device (e.g., belonging to friends or family), the reporting of manipulations can be carried out reliably. In a real election, the election authorities would be able to investigate the issue and take appropriate action.

An additional "File Complaint" button was displayed in the online voting system. In our simulated attack scenario, a manipulated voting device may deliberately offer such a button in the hope that the voter will use it instead of following the official instructions on the code sheet. If the voter clicks this button, they may either be redirected to a manipulated reporting website or the true reporting process may be blocked by the compromised device. In both cases, the voter would not receive a problem-confirmation code, which is an indication that the device is acting dishonestly. The voter should then switch to a different device and report the problem again.

Please note that we did not inform you about the simulated manipulation at the start of the study, as this would have influenced your natural behaviour. Had we warned you beforehand, you might have actively looked for inconsistencies, which would have distorted the results. For methodological reasons, we also could not implement all feedback that was

submitted, as the systems needed to remain comparable to those used in Phase 1. (For example, the suggestion to use a QR code for logging into the voting system could not be implemented — both for methodological and for security reasons.)

The aim of this study was not to test you, but to test the system. If the inconsistency went unnoticed, this reflects insufficient usability in the online voting system, not a failure on the part of participants.

At present, we cannot say whether an online voting system will actually be used in the next European election. The European election was chosen for this study because it is conducted nationwide and generally affects a large number of people. It is also not predetermined who would send the letters containing the voting materials. For the purposes of this study, we assumed that this would be handled by the Federal Returning Officer, as this detail is not relevant to the study's results.

Appendix B. Voting Material

B.1. Documents used in the study

We made all documents used in the study publicly available to allow future work to build upon the materials employed in this study. All documents from the study (in German) and a translated version (in English) are attainable here: https://secuso.org/2026-03-24_EuroSP_Reliable_Voter_Complaints/

B.2. Video from the Voter's Point of View

Several videos from the voter's point of view for all three approaches are attainable here: https://secuso.org/2026-03-24_EuroSP_Reliable_Voter_Complaints/Videos

Here, you can find videos (1) showing the normal vote casting process, (2) how the vote casting process differed under the simulated manipulation and (3) how to file a complaint.

B.3. Election Invitation

Chris Sampleperson
Sample street 1
Sample city 12345

26 November 2024

Dear Sample Person,

You have applied to receive documents for online voting in the upcoming 2024 European Parliamentary Election. We would like to provide you with these documents in this message. Below is a summary of the voting rules:

- You have exactly one vote for one party.
- You may also explicitly mark your ballot as invalid.
- If you have not yet encrypted and transmitted your vote, you can cancel and restart the online voting process at any time.
- If you notice any inconsistencies with one of the codes to be checked, please report them using the information on your codesheet.
- You can cast your vote between 28 November 2024 and 13 December 2024.

To ensure the security of your online-cast vote, the online voting system uses various types of codes. At different stages of the voting process, you will need to enter codes from your personalized codesheet into the online system, as well as compare return codes displayed there with those on your codesheet. The codesheet enclosed with this letter will guide you step by step through the entire voting process.

If the return codes match, you can be sure that your vote was correctly received by the election server. This allows manipulation attempts to be detected, similar to how independent election observers uncover such issues in traditional in-person elections.

If the codes do not match or no codes are displayed in the online system, you must immediately stop the voting process and report the problem using the information provided on your codesheet. **Please note that the information and instructions in this letter and on your codesheet always take precedence over all information and instructions displayed in the online voting system.**

In case any technical difficulties or questions arise during the election, you can contact us by email (eu-wahl-support@institution.org), via our help page (https://help.anonymized.de), or by telephone (0721 anonymized).

Figure 12. Front page of the election invitation. This was part of the voting instructions in the green envelope. We provide only the version for phase 2 here as they are nearly identical. They only differ in the phase number, voting period and URL. (Texts translated to English for reader's convenience; original texts were in German)

By checking and, if necessary, reporting issues, you make an important contribution to the security and integrity of the online election. Voters who want to protect democracy should verify the correctness of their vote using the return codes and report any problems.

Please read all steps on the codesheet carefully and then cast your vote.

Kind regards,

The Federal Returning Officer

In case any technical difficulties or questions arise during the election, you can contact us by email (eu-wahl-support@institution.org), via our help page (https://help.anonymized.de), or by telephone (0721 anonymized).

Figure 13. Back page of the election invitation.. (Texts translated to English for reader's convenience; original texts were in German)

B.4. Code Sheets

Vote & Confirm.

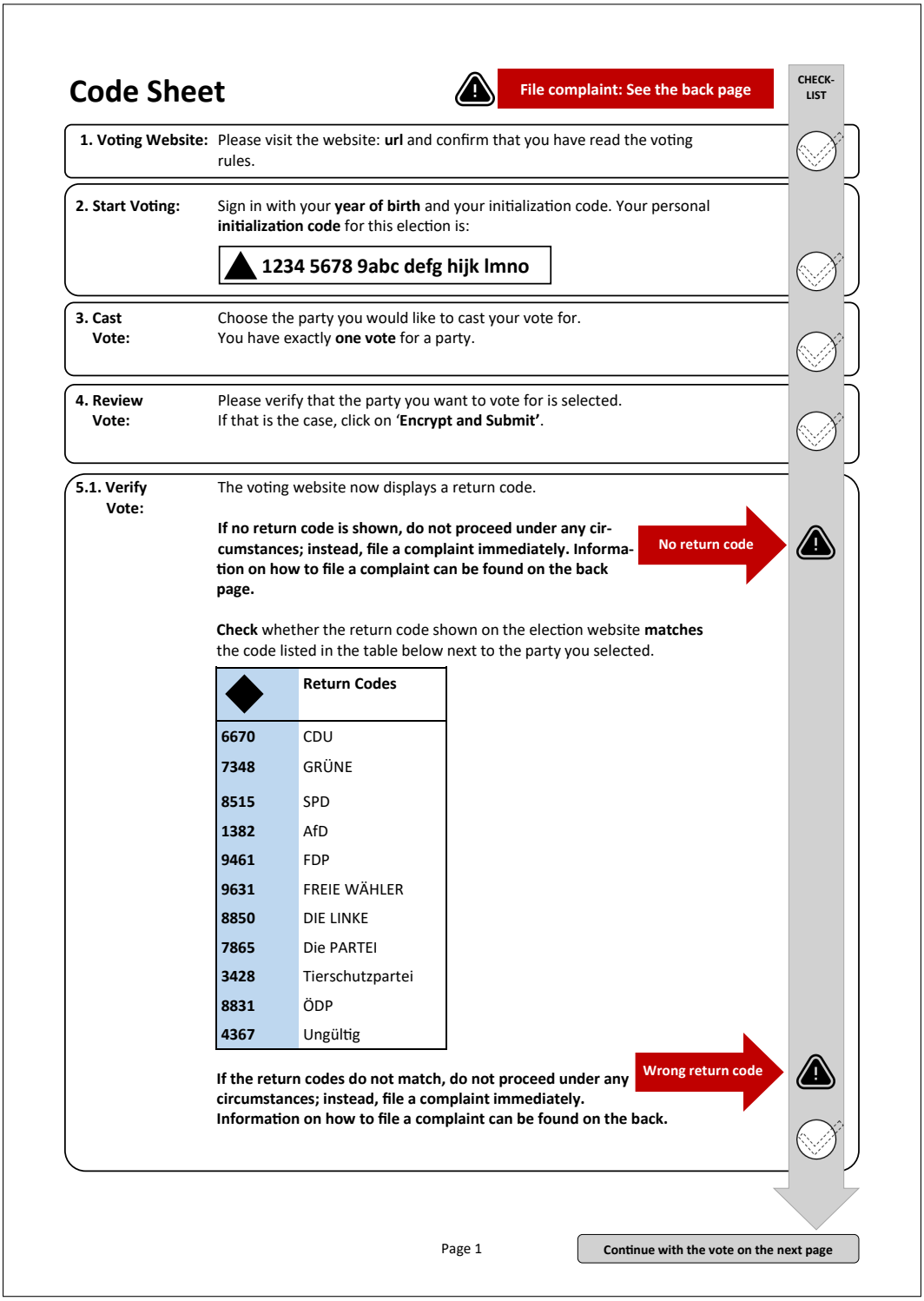

Figure 14. Code Sheet for *Vote & Confirm* approach. Page 1. (Texts translated to English for reader's convenience; original texts were in German)

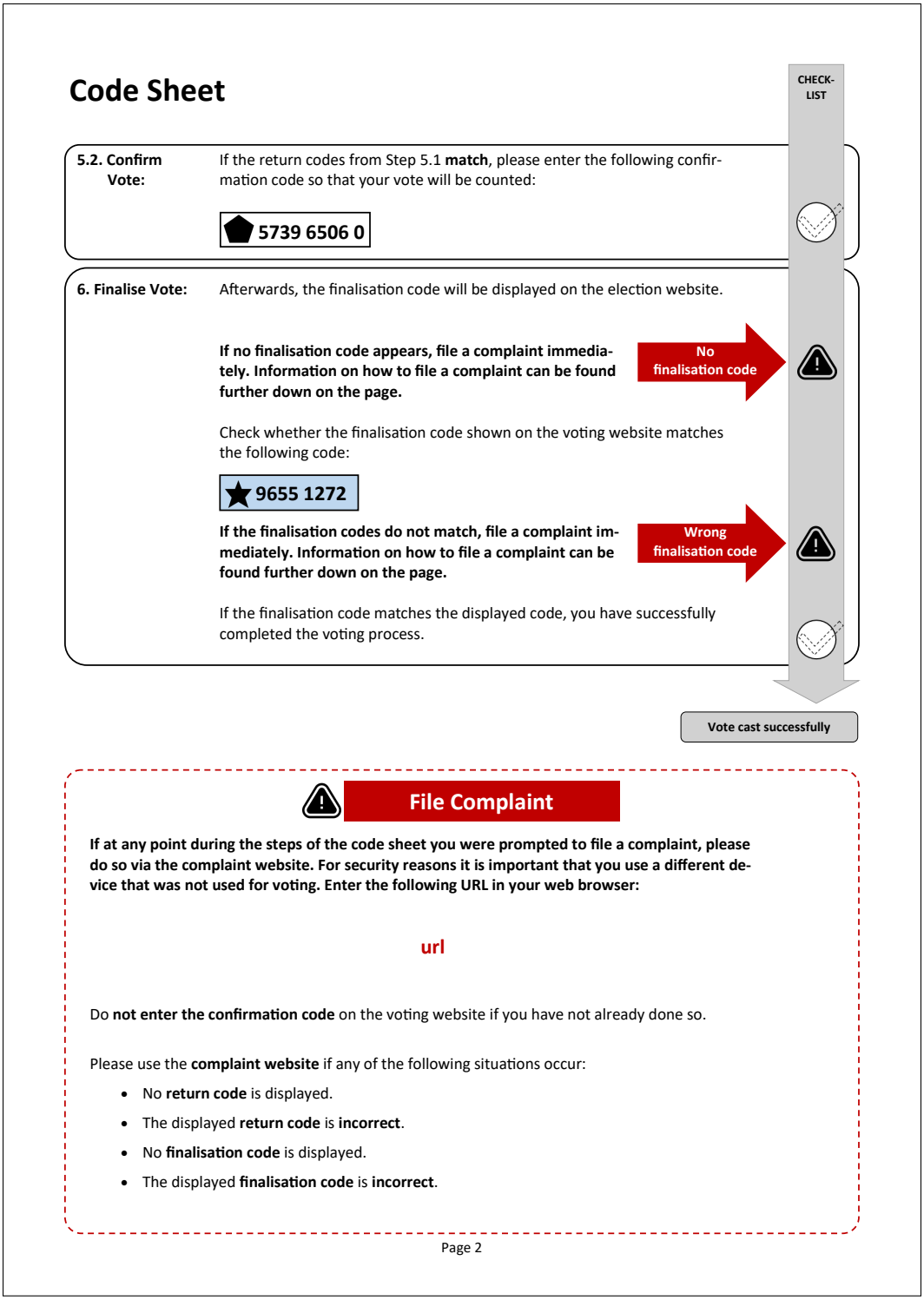

Figure 15. Code Sheet for *Vote & Confirm* approach. Page 2. (Texts translated to English for reader's convenience; original texts were in German)

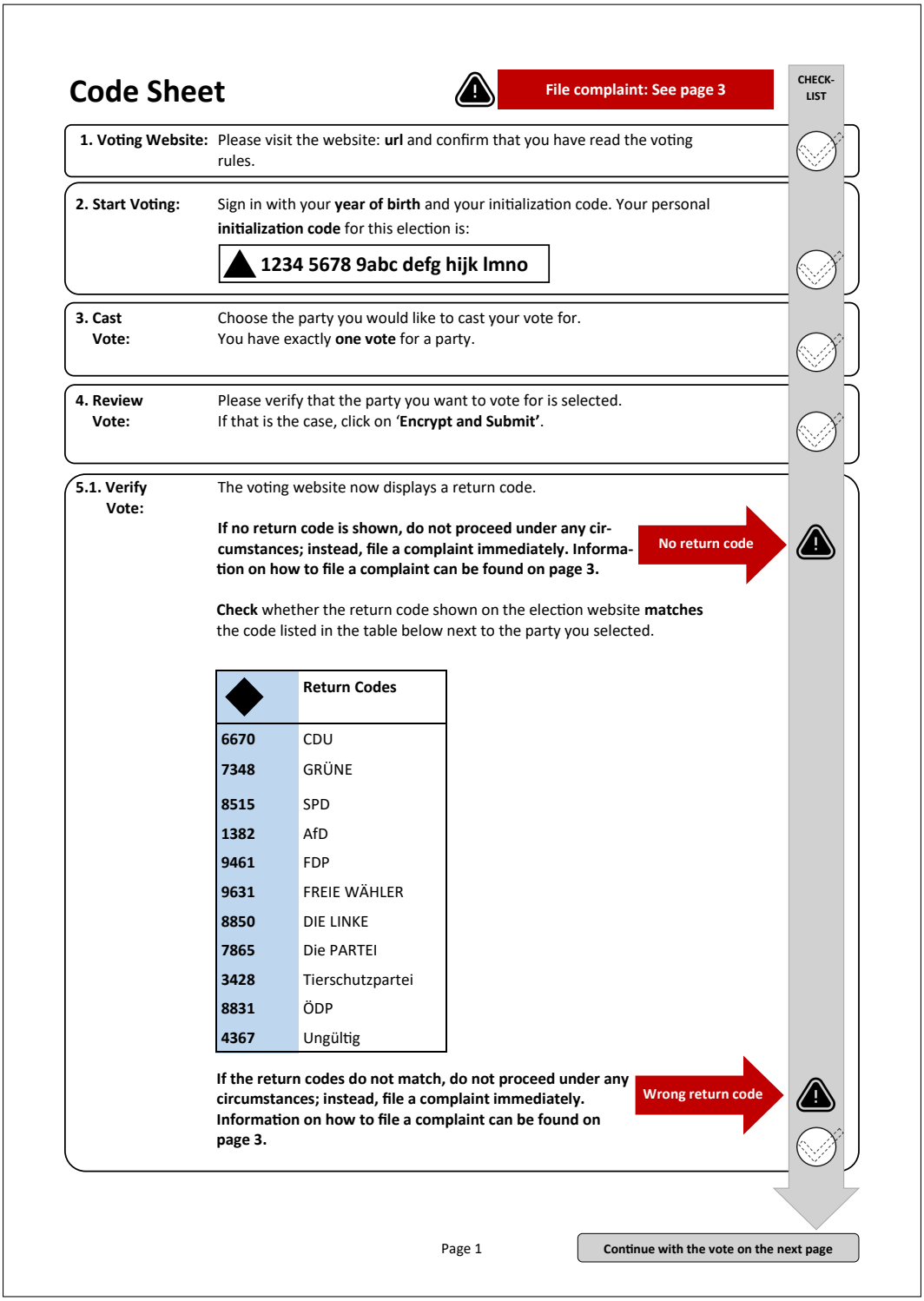

Figure 16. Code Sheet for *Cancelable Vote & Confirm* approach. Page 1. (Texts translated to English for reader's convenience; original texts were in German)

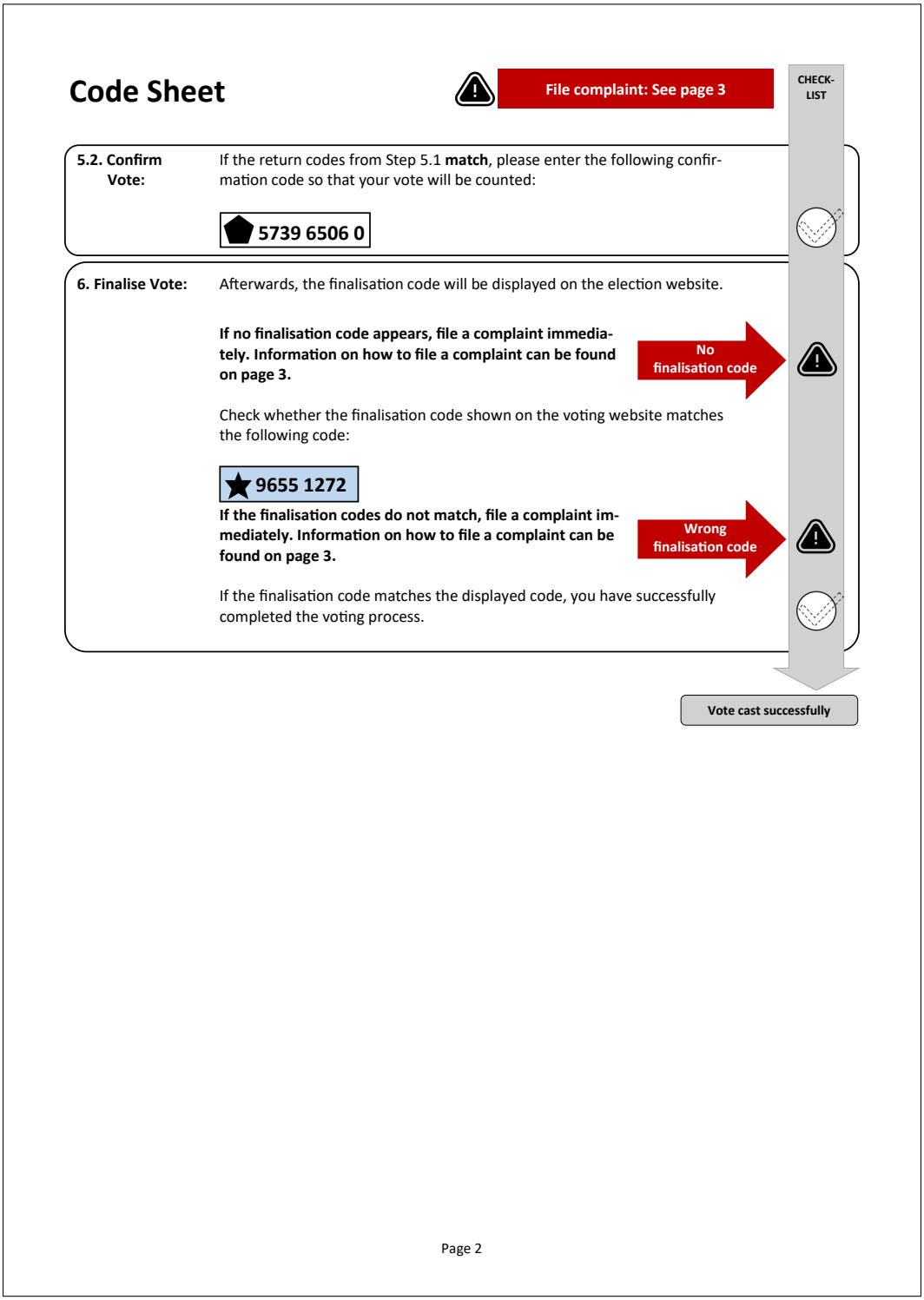

Figure 17. Code Sheet for *Cancelable Vote & Confirm* approach. Page 2. (Texts translated to English for reader's convenience; original texts were in German)

Code Sheet

File Complaint

If at any point during the steps of the code sheet you were prompted to file a complaint, please do so via the complaint website. For security reasons it is important that you use a different device that was not used for voting. Enter the following URL in your web browser:

url

Do **not enter the confirmation code** on the voting website if you have not already done so.

Please use the **complaint website** if any of the following situations occur:

- No **return code** is displayed.
- The displayed **return code** is **incorrect**.
- No **finalisation code** is displayed.
- The displayed **finalisation code** is **incorrect**.

Enter the following **complaint code** on the reporting website:

abcd efgh ijkl mno1 2345 6789

Check whether the displayed complaint return code **matches** the following code:

7653 8871

If no code is displayed or the two codes do not match, it may be because you used the same device that was also used for voting. Please switch to a different device and file a complaint again.

If the two codes match, you have successfully filed a complaint.
You now have a guarantee that the issue will be investigated diligently by the official authorities.

Figure 18. Code Sheet for *Cancelable Vote & Confirm* approach. Page 3. (Texts translated to English for reader's convenience; original texts were in German)

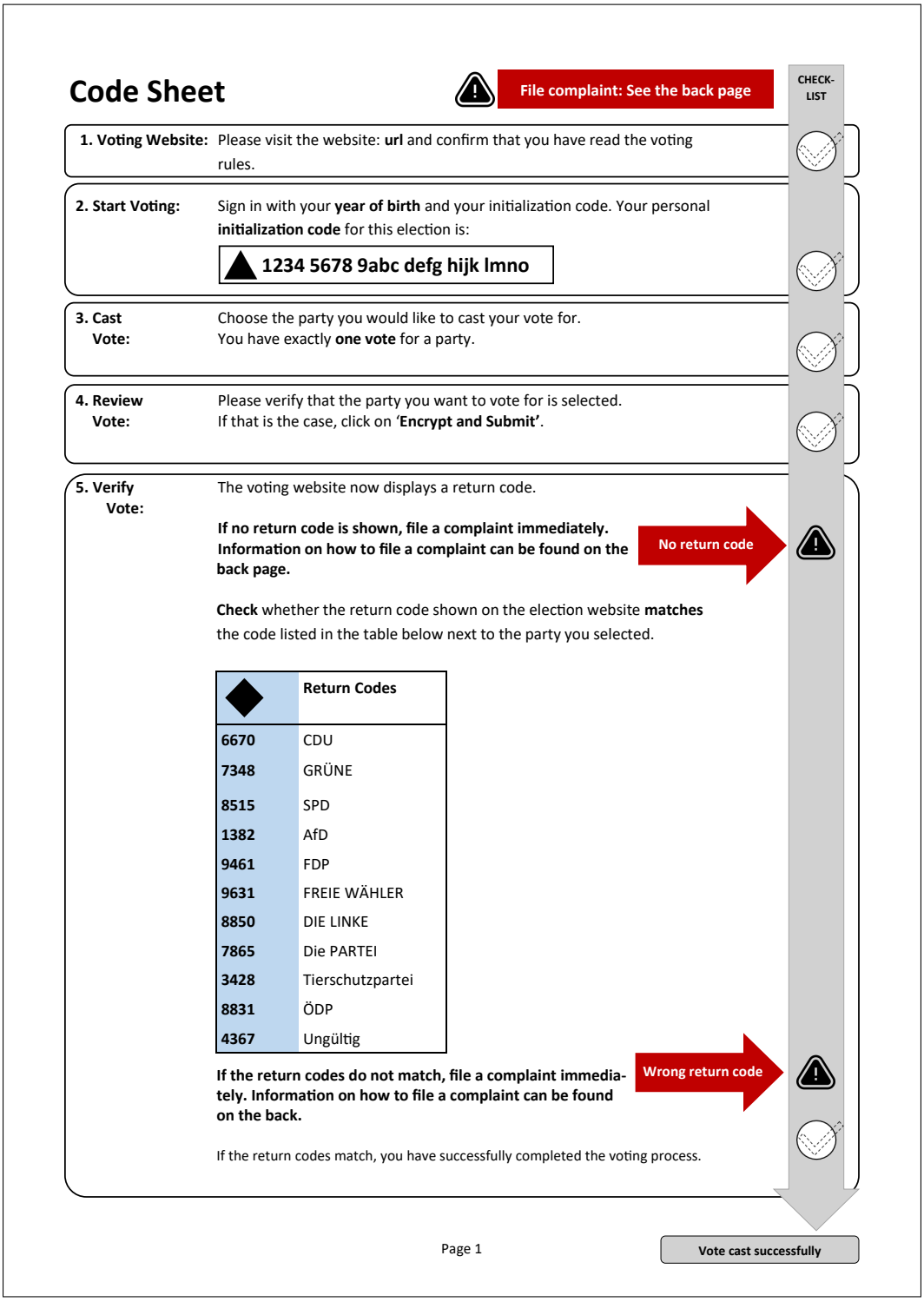

Figure 19. Code Sheet for *Cancelable Vote & Go* approach. Page 1. (Texts translated to English for reader's convenience; original texts were in German)

Code Sheet

File Complaint

If at any point during the steps of the code sheet you were prompted to file a complaint, please do so via the complaint website. For security reasons it is important that you use a different device that was not used for voting. Enter the following URL in your web browser:

url

Please use the **complaint website** if any of the following situations occur:

- No **return code** is displayed.
- The displayed **return code** is **incorrect**.

Enter the following **complaint code** on the reporting website:

abcd efgh ijkl mno1 2345 6789

Check whether the displayed complaint return code **matches** the following code:

7653 8871

If no code is displayed or the two codes do not match, it may be because you used the same device that was also used for voting. Please switch to a different device and file a complaint again.

If the two codes match, you have successfully filed a complaint.
You now have a guarantee that the issue will be investigated diligently by the official authorities.

Figure 20. Code Sheet for *Cancelable Vote & Go* approach. Page 2. (Texts translated to English for reader's convenience; original texts were in German)

Appendix C.
Code Sheet from Kulyk et al.

We made the following changes to the code sheet from Kulyk et al. to further enhance clarity and integrate the proposed mechanism for reliably filing complaints:

- **Symbols:** Because our dedicated complaint filing website was intended to be the primary channel for reporting issues, we removed the original phone icon and accompanying "Support" label. Instead, we used a warning triangle, which also appears at the top of the code sheet together with the instruction: "File Complaint: See back page."
- **Titles:** We revised the titles of the individual steps so that each one explicitly corresponds to a specific action the voter performs while casting their vote, thereby improving the step-by-step guidance.
- **Voter checks:** We rephrased the voter checks to make them more explicit. For example, in step five we changed the original instruction "If not, contact support immediately" to: "If no return code is shown, file a complaint immediately. Information on how to file a complaint can be found on the back page."
- **Complaint filing mechanism:** We extended the code sheet with information explaining how and under which circumstances voters should file a complaint (see Figure 18).

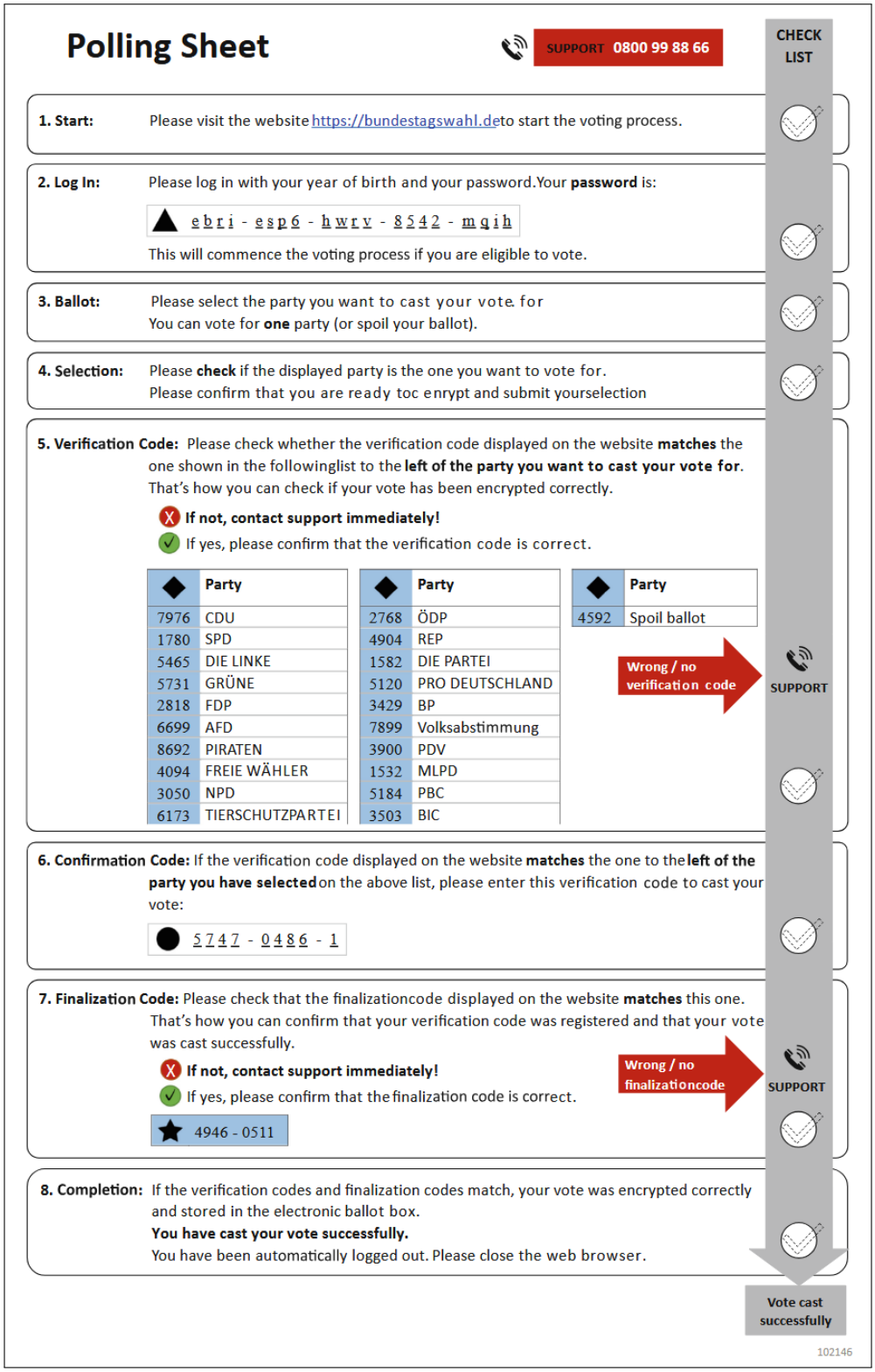

Figure 21. Code Sheet Kulyk et al. used in their study, which we built upon.

Appendix D.
Manipulated Interfaces

D.1. *Vote & Confirm*

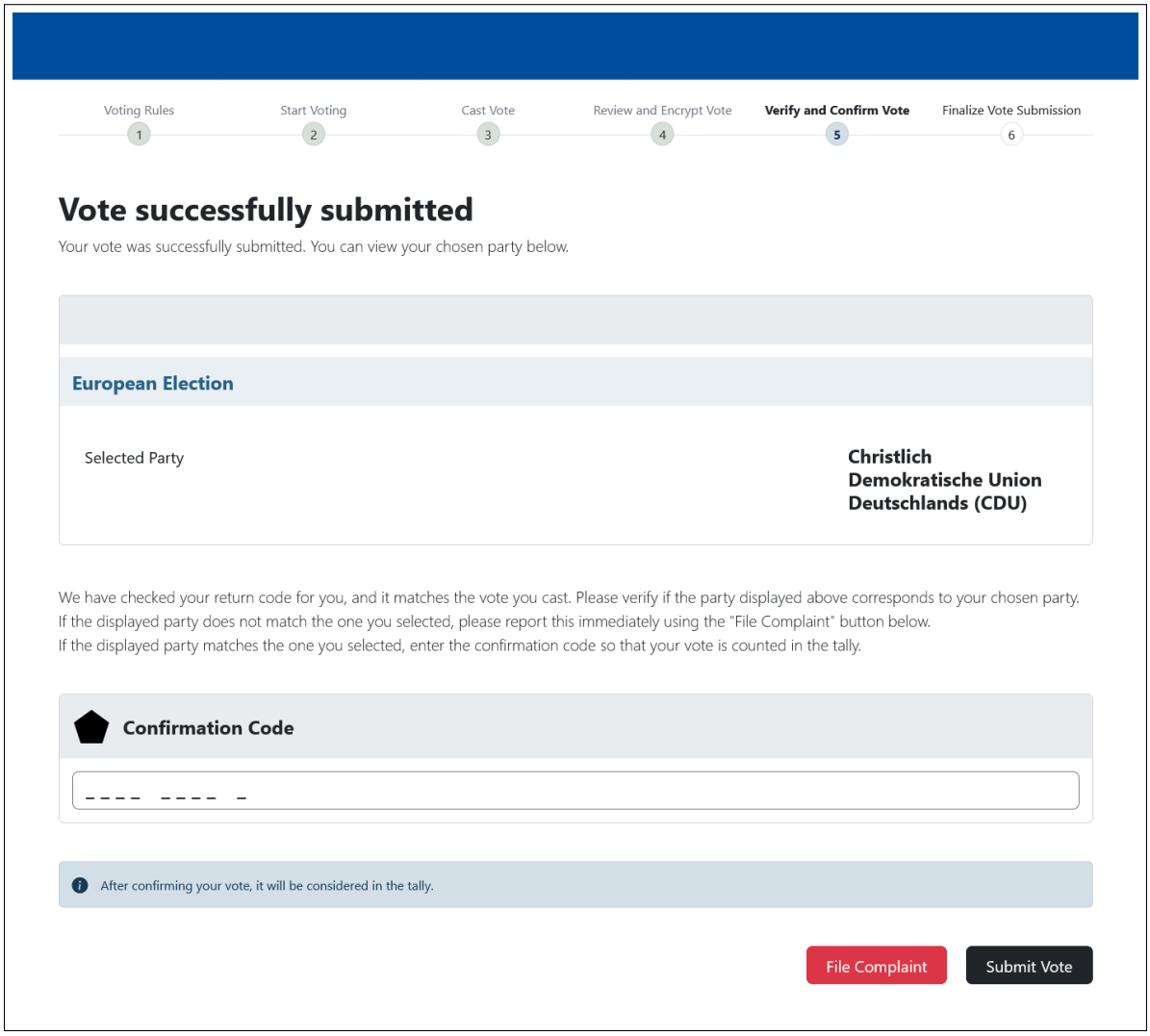

Figure 22. *Vote & Confirm*: Manipulation during confirmation step. Instead of showing the return code the text states that the vote was automatically verified and the voter should only report a problem in case the selected party does not match. Additionally the report button is manipulated and would bring the voter to a manipulated complaint page where the complaint would be intercepted. (Website translated into English for reader's convenience; original texts were in German)

D.2. *Cancelable Vote & Go*

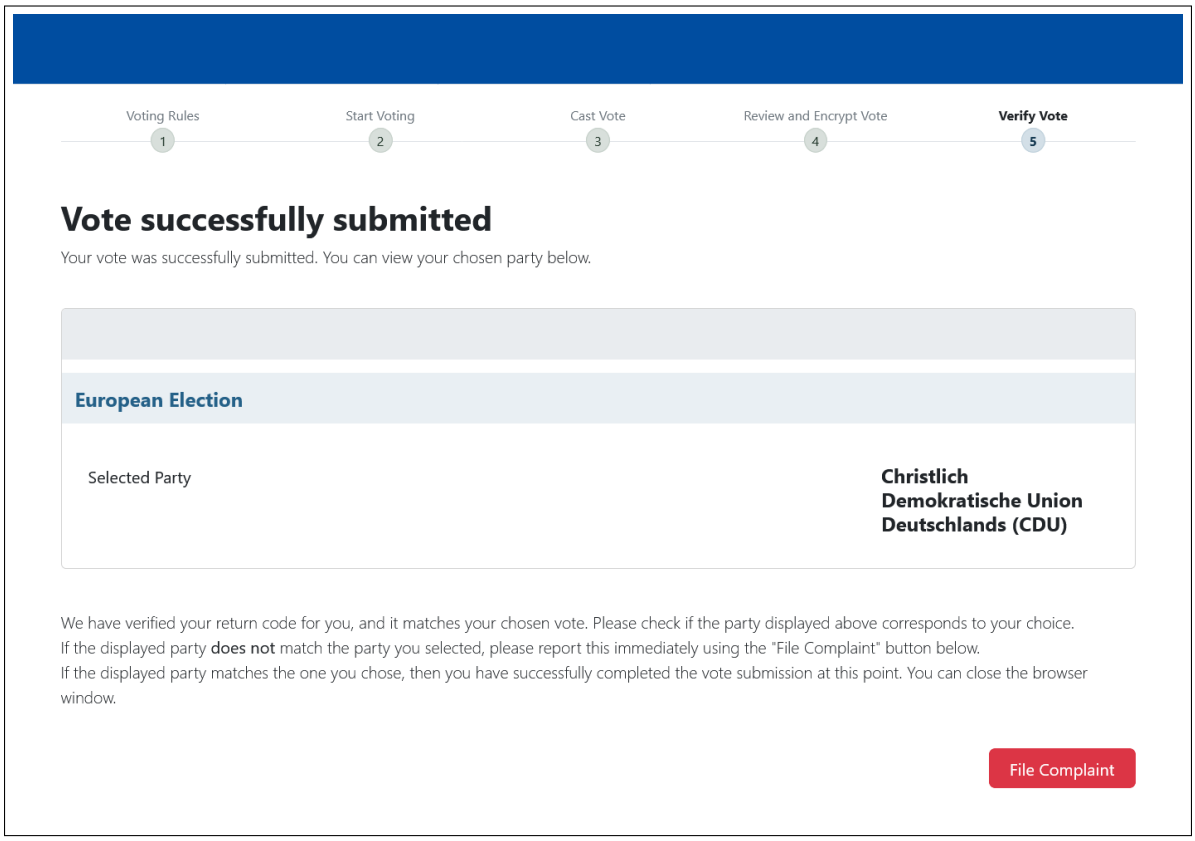

Figure 23. *Cancelable Vote & Go*: Manipulation during confirmation step. Instead of showing the return code the text states that the vote was automatically verified and the voter should only report a problem in case the selected party does not match. Additionally the report button is manipulated and would bring the voter to a manipulated complaint page where the complaint would be intercepted. (Website translated into English for reader's convenience; original texts were in German)

D.3. *Cancelable Vote & Confirm*

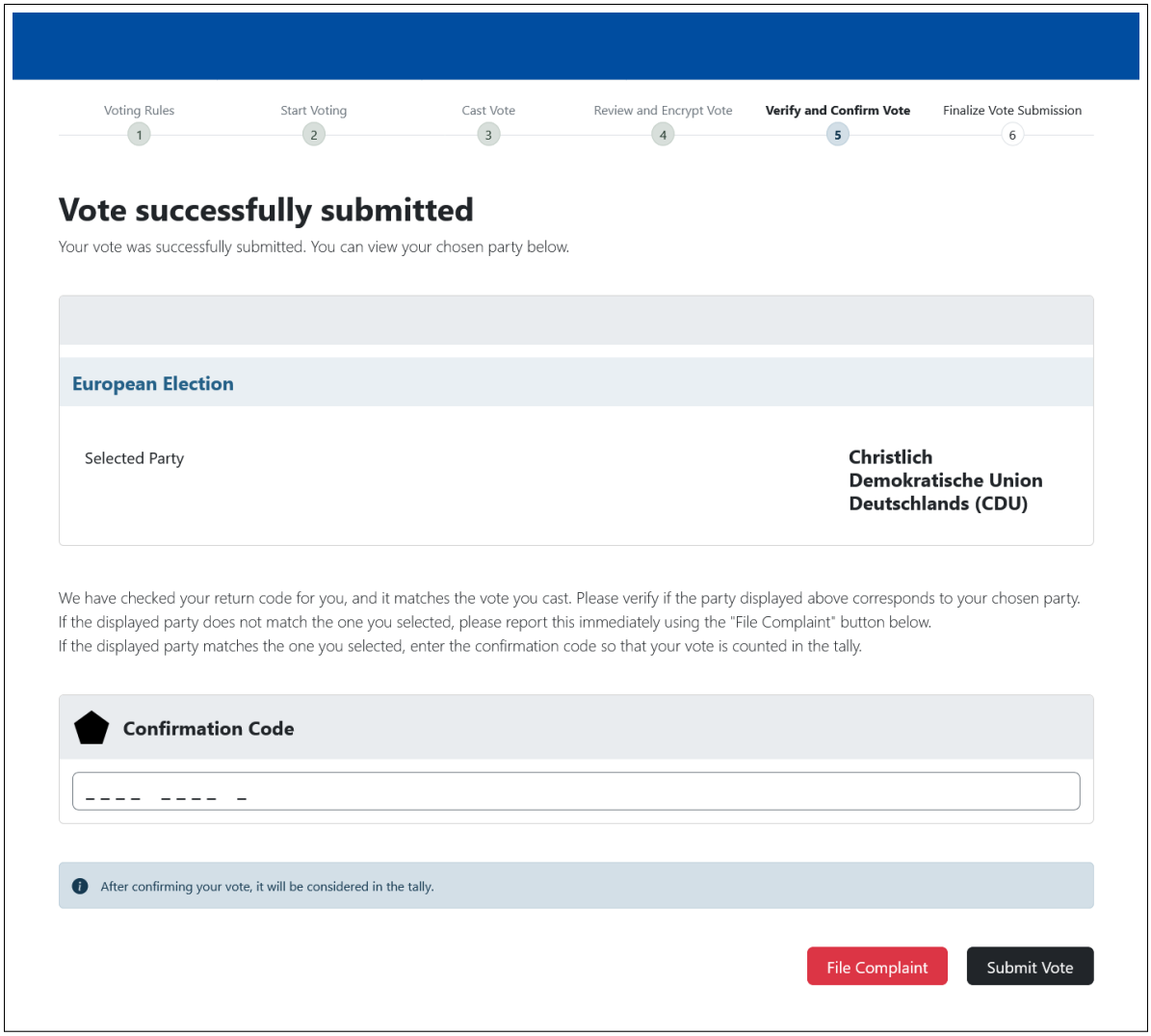

Figure 24. *Cancelable Vote & Confirm*: Manipulation during confirmation step. Instead of showing the return code the text states that the vote was automatically verified and the voter should only report a problem in case the selected party does not match. Additionally the report button is manipulated and would bring the voter to a manipulated complaint page where the complaint would be intercepted. (Website translated into English for reader's convenience; original texts were in German)

Appendix E.
Manipulated Complaint Filing

E.1. *Vote & Confirm*

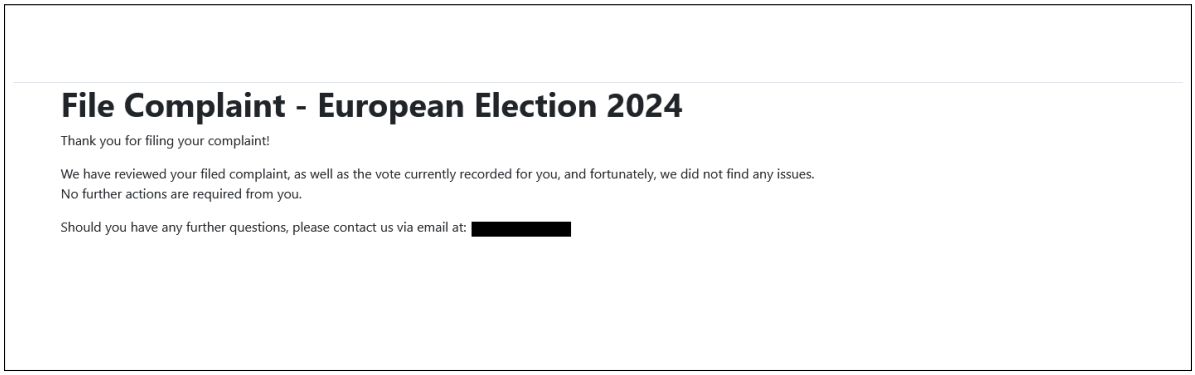

Figure 25. *Vote & Confirm*: Manipulation of complaint filing. (Website translated into English for reader's convenience; original texts were in German)

E.2. *Cancelable Vote & Go*

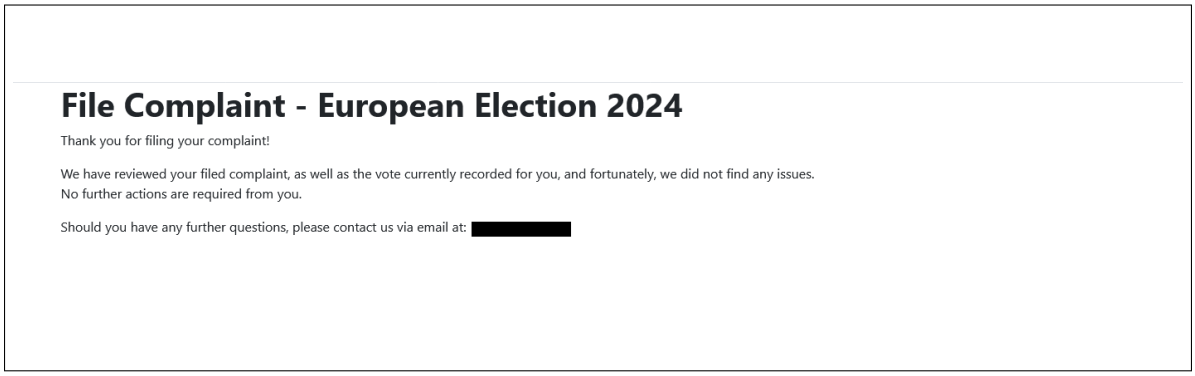

Figure 26. *Cancelable Vote & Go*: Manipulation of complaint filing. (Website translated into English for reader's convenience; original texts were in German)

E.3. *Cancelable Vote & Confirm*

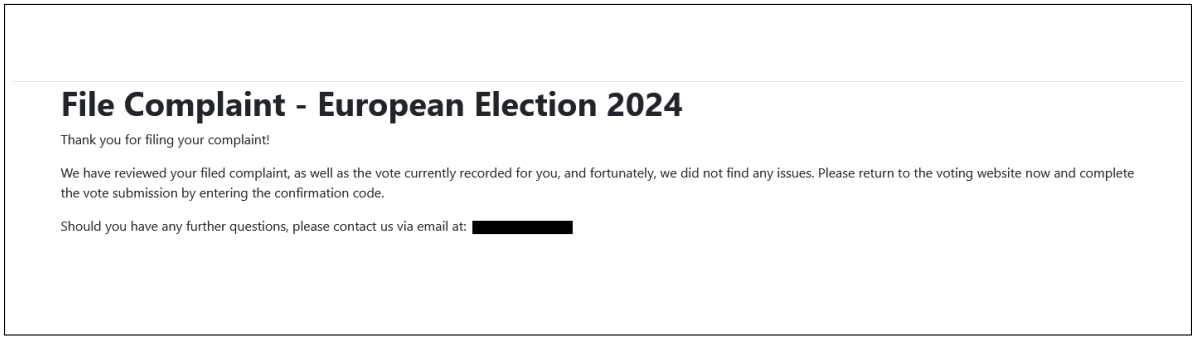

Figure 27. *Cancelable Vote & Confirm*: Manipulation of complaint filing. (Website translated into English for reader's convenience; original texts were in German)