Development and Expert Evaluation of an Informative Video Concerning Verifiable Internet Voting

Tobias Hilt[1](✉), Florian Moser[2], Philipp Matheis[1], and Melanie Volkamer[1]

[1] SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany
{tobias.hilt,philipp.matheis,melanie.volkamer}@kit.edu
[2] Université de Lorraine, CNRS, Inria, LORIA, 54000 Nancy, France
florian.moser@inria.fr

Abstract. As digitalization advances, online elections are becoming increasingly prevalent. State-of-the-art internet voting systems implement verifiability, which allows to observe the election result to be correct, while safeguarding the secrecy of the election. However, the continued use of unverifiable 'black-box' systems suggests that election organizers may be unaware of the security challenges in internet voting and the mitigation strategies that have been developed.

To address this gap, we developed an informative video on the topic for election organizers who are non-experts in internet voting. To ensure that the simplifications made for our target audience do not lead to misunderstandings, 19 German-speaking internet voting experts evaluated the video. Based on their feedback, we consider improvements to the video to enhance its correctness, clarity, and completeness. Further, developing the video and then performing the expert evaluation provided valuable experiences and lessons learned we want to share with similar endeavours trying to simplify complex topics for non-expert audiences.

Keywords: Online Elections · Verifiable Internet Voting · Informational Video · Expert Evaluation

1 Introduction

Elections are increasingly held digitally, as can be, for example, observed for national elections in Estonia [8] or Switzerland [4]. In contrast to these examples, however, online elections often rely on so-called "black-box" systems, where the integrity and confidentiality of the voting process are entirely in the hands of a single system with no details public about its internal workings [17].

Using a black-box system presents risks, as potential manipulations or neglect of vote secrecy cannot be (dis)proven by an independent party. An attacker could, for example, compromise the election server from a remote location, altering votes undetected or breaching vote secrecy, which has been shown to be feasible [25]. This in turn may undermine trust in the electoral process and therefore

D. Duenas-Cid et al. (Eds.): E-Vote-ID 2025, LNCS 16028, pp. 107–123, 2026.
https://doi.org/10.1007/978-3-032-05036-6_7

in democracy itself, as voters did not receive any concrete assurance that their votes are accurately recorded and counted and that their choices remain secret. Moreover, unsatisfied voters or malicious actors might claim electoral fraud, and neither the election organizers nor the system providers would be able to conclusively disprove such allegations.

To mitigate this risk, there are approaches that enable voters to verify that their votes have been cast as intended. In addition, election observers may verify that all cast votes are tallied correctly, notably while safeguarding vote secrecy. These approaches still require trust in some part of the system, but clearly disclose where this trust is required. This allows the election organizer to make an informed decision whether a given system is appropriate in their election context. Such systems are well-known in the academic literature (e.g., [2]), and some have also been developed by industry and are in active use (e.g., [9,21]).

The continued use of "black-box" systems [17] implies that many election organizers are not fully aware of the risks of internet voting, and at the same time, not aware of the different available approaches that aim to fix these issues. Lastly, they are likely unaware that there is no single perfect solution, but rather all approaches include trade-offs, and the election organizers must make an informed decision which approach is appropriate in their election setting.

Our Contribution. To introduce election organizers to internet voting, we developed an informational video on the subject. This video not only highlights the security challenges of internet voting, but also explains possible solutions for mitigating risks using a concrete internet voting system as a running example. It also communicates the open nature of the challenge, with each solution approach delivering their unique advantages, disadvantages and trust assumptions.

As we aim at a non-expert audience, and through the inherent limits of content transferable in a medium-length video, it is crucial to explain the topic in a simplified manner. However, simplification must not lead to incorrect statements, as this would risk misinforming the election organizers. Therefore, we evaluated the video with 19 German-speaking internet voting experts.

In this work, we document both the video and its evaluation results, but also the approach used. By documenting and evaluating the approach, we hope to support similar projects where an informational video aimed at a non-expert audience explains a complex topic in a simplified, but nonetheless correct, manner. By the production and evaluation of the video itself, we hope to contribute meaningfully to the secure advancement of electronic voting, particularly in German-speaking countries. The main contributions of this work are therefore:

- Development of a video about risks of internet voting, and approaches to mitigate that risk, popularized for non-expert election organizers.
- Evaluation of the correctness of this video by 19 German-speaking internet voting experts and the derivation of improvements to enhance the clarity.
- Documentation of the methodology used to develop a popularized video on a complex topic and the evaluation of the said video by experts.
- Lessons learned about the development and evaluation process and recommendations for future work.

2 Related Work

Previous work has already explored how e-voting systems can be made comprehensible to a broader audience, including potential voters and election organizers.

Some studies implicitly explain the characteristics of e-voting systems to their study participants. For example, Kulyk et al. investigated user interactions with successive versions of a voting system [13]. Although the primary goal was to assess usability and security trade-offs, participants gained an implicit understanding of these features, through their interactions and short explanations of the differences. Furthermore, studies on verifiability (e.g., [11,22,23]) use manipulated voting systems to help participants understand verification properties, although the primary focus is again not on education.

Further, some work also explicitly explains characteristics of e-voting systems, but again usually focuses on a concrete system or a concrete aspect of e-voting systems. Examples include research from Storer et al., which used videotaped material in a lab study to explain the mCESG voting system used in the UK [20], and Llewellyn et al., which provided oral explanations and illustrated figures to explain the “split mechanism” of the Prêt-à-Voter voting system [15]. Research by Gharadaghy and Volkamer offers detailed descriptions of various verifiability forms in e-voting systems using illustrated figures and text [5], while Schürmann et al. report on the use of e-learning modules and videos to improve the cybersecurity awareness of election organizers in the context of the 2019 European Parliament elections [19]. Moreover, short explanatory videos on concrete instances of e-voting systems produced by industry exist, e.g. about the system by Swiss Post[1] which is in use in Switzerland.

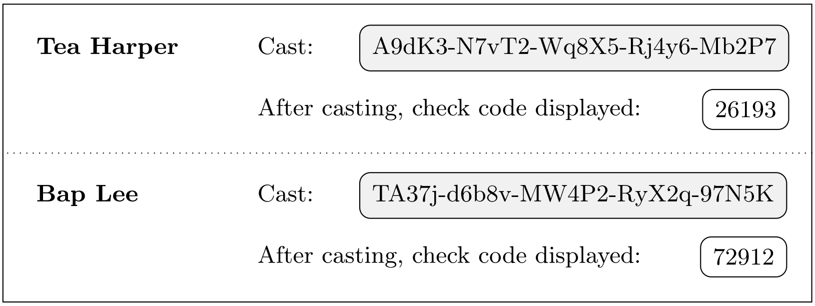
Our work extends upon these contributions by presenting a more holistic view of the security challenges of and potential solutions to mitigate risks in internet voting in general, focusing less on specific characteristics and concrete systems. While we also use a concrete system as a running example, we do not go into great detail on how it works. Instead, the video focuses on the general concepts which transform well to other systems.

3 Distributed Code Voting with Confirmation Codes

Here, we detail the voting system we took as a basis for the video. It is similar to existing proposals (e.g., [1,6]), while it remains unproven, which is however sufficient for our purposes.

Setup Phase. In the setup phase, the distributed servers agree on an encryption key ek with a distributed decryption key (in spite the fact that decryption requires the involvement of all servers). The election encryption key ek is sent to the printer. For each voter, the printer then selects for each candidate c a random voting code v_c and, per server i, a random partial confirmation code r_c^i.

[1] https://www.youtube.com/watch?v=j4X5iyIKhGg, last accessed 27.06.2025.



Tea Harper	Cast:	A9dK3-N7vT2-Wq8X5-Rj4y6-Mb2P7
	After casting, check code displayed:	26193
Bap Lee	Cast:	TA37j-d6b8v-MW4P2-RyX2q-97N5K
	After casting, check code displayed:	72912

Fig. 1. Code sheet for a two-candidate election.

The printer then responds to each server i for each candidate c with an encryption of the candidate $e_c = enc(ek, c)$, a hash of the voting code $hash(v_c)$, as well as the respective partial confirmation code r_c^i. Furthermore, the printer prints the personal vote sheet of the voter, which for each candidate c lists the corresponding voting code v_c, as well as the aggregation of all partial confirmation codes of that candidate $r_c = aggr(\forall i.r_c^i)$.

Voting Phase. When the voting period starts, the voter receives their personal code sheet (see fig. 1). On their voting device (e.g., laptop or phone), the voter opens the voting interface (e.g., webpage or app), and enters the voting code v_c of the preferred candidate c as printed on the code sheet. This voting code v_c is sent to the servers, which confirm to each other using digital signatures that this is the first valid vote of that voter. Then, each server marks the corresponding encryption e_c ready for tally and responds with the corresponding partial confirmation code r_c^i. The partial confirmation codes are aggregated, and the resulting confirmation code $r_c = aggr(\forall i.r_c^i)$ is displayed to the voter. The voter then checks whether the displayed confirmation code r_c matches the confirmation code as printed on the code sheet, or otherwise complains to the authorities.

Tally Phase. After the voting phase, each server has a ciphertext for each voter who cast their vote, and corresponding signatures from all other servers. They collectively perform a verifiable shuffle (e.g., [24]), which transforms the ciphertext to destroy the link to the casting voter, while provably not altering its content. Afterwards, the servers collectively decrypt the list of transformed ciphertext, and then count the votes.

Informal Security Statement. Assuming the printer, the channel from the printer to the voter, and one of the servers are honest (but notably not the voter's device), this protocol guards the secrecy and the integrity of the votes. Intuitively, the voting code hides the selected candidate to achieve secrecy, and the confirmation code ensures that all servers have received the authenticated unmodified vote to achieve integrity. Finally, the verifiable shuffle and distributed decryption guard the properties in the tally phase. Notably, some of the steps are verifiable by independent third parties (e.g., the proofs output by the verifiable shuffle).

4 Methodology

As described in Sect. 2, to the best of our knowledge, there are no existing endeavours that present a holistic view of the risks and the mitigation approaches to a non-expert audience. We therefore document in this section in detail how we approached the project, and the reasoning behind it. In Sect. 6, we discuss the strengths and weaknesses of this chosen approach.

Our approach is based on the principles of design science [10]. The primary objective is to inform election organizers about the security challenges associated with conducting elections online, outline existing methods to mitigate risks, and highlight the remaining issues. The main artifact we developed through this approach is an informational video created through iterative refinement. In line with the design science methodology, we then subjected the artifact to an evaluation. Section 4.1 and Sect. 4.2 provide further details on these components.

4.1 Video

We chose video as our medium because studies indicate that videos can efficiently communicate complex information by combining visual and auditory elements [18]. In addition, we decided to keep it at a length of ten minutes, which is within the recommended duration for informational videos [16].

Defining the Story Structure. The structure and story of the video will be highlighted shortly, but for a thorough inspection, we refer the interested reader to the video with English subtitles and translated script[2]. Based on previous experiences made while consulting election organizers on this topic, we decided that the overall theme of the video should follow an exploratory approach.

The story opens by motivating internet voting through parallels with other digitized services, such as online banking or appointment scheduling. It then highlights essential election requirements, such as fairness, vote secrecy, and vote integrity, alongside associated challenges and common misconceptions. Particular emphasis is placed on the significant security risks posed by voters using untrusted personal devices, given the numerous potential vulnerabilities across device types, operating systems, applications, and browsers (see Fig. 2).

After that, we present a proposal for an e-voting system that addresses these challenges and discuss its (dis)advantages. The technical details described in Sect. 3 are not part of the video, instead, the approach is explained more visually and in easier-to-understand terms (see Fig. 3).

The video further explains that alternative e-voting approaches exist, each potentially addressing certain challenges of the proposed system but introducing

[2] https://secuso.org/2025-07-E-Voting-Explanation-Video/.

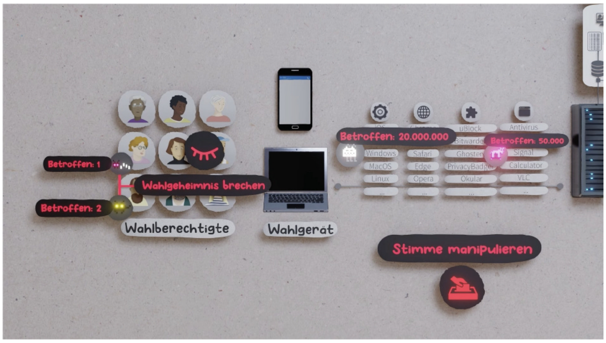


Fig. 2. The video visualizes the diversity of devices and software in use, which altogether pose a large attack surface. Malware might therefore be able to infiltrate some of these systems, and then break vote secrecy or manipulate the vote.

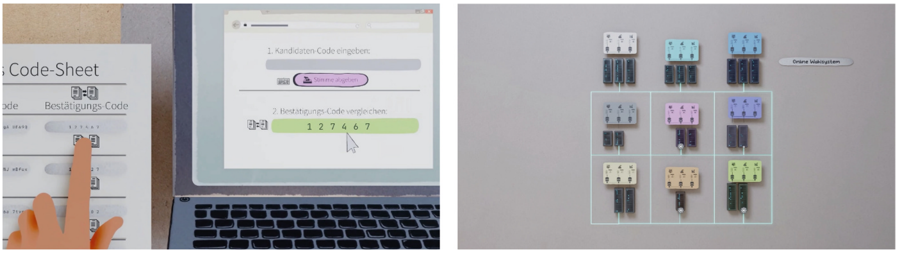


Fig. 3. The video explains how a voter verifies their confirmation codes, and how the servers communicate with each other to implement a digital “four-eyes principle”.

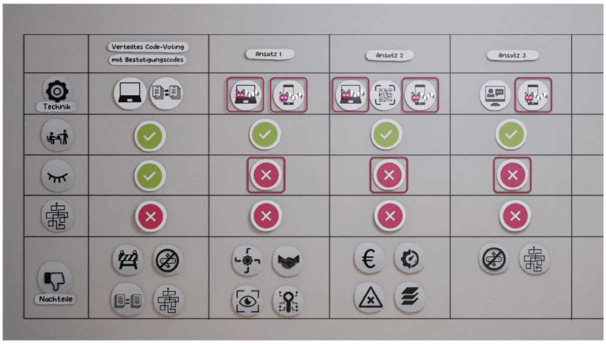


Fig. 4. The video uses a table to illustrate how different approaches exist, with each having individual characteristics and (dis)advantages. Notably, we discovered in the expert evaluation that the visualisation of this comparison is confusing, which we discuss in Sect. 5, and will improve in the next version of the video.

new issues or performing worse in other aspects. It emphasizes the need for continued research, as a single, perfect solution that resolves all challenges without creating new ones does not yet exist (see Fig. 4).

Finally, the story concludes that many open questions remain, for example, whether such a complex system would be fully trusted by voters.

Choosing a Voting System. Unfortunately, there is no clear default choice for which voting system to present: State-of-the-art systems are diverse in both the mechanism they employ, as well as the trust assumption they rely upon for their security (e.g., see [17]). To inform the election organizers accurately while at the same time respecting the limits of our medium, we needed a highly secure voting system while keeping its complexity in terms of mechanisms and trust assumptions to a minimum.

The approach we have chosen to present employs voting codes with confirmation codes, paired with distributed servers. This results in a secure voting system that needs only weak trust assumptions, notably none in the voting device or a single server. To cast a vote, a single interaction with the server is sufficient, and the computations and voter tasks are straightforward. Overall, our setting is derived from what is enforced by Swiss legislation for their national elections [3], and the system is similar to recent proposals employing code voting in the Swiss setting [1,6]. The system is described in detail in Sect. 3.

Producing the Video. In the beginning, the interdisciplinary research team, consisting of members with a background in cryptography and human factors, and the production team discussed a rough initial concept. This initial concept resulted in a draft of the textual script written by the interdisciplinary research team that was iteratively refined with the production team. After reaching a consensus on the final version of the textual script, the script was recorded. Subsequently, the production team developed a visual script based on the textual script. This visual script outlined in detail how the topic would be presented visually. Similar to the development of the textual script, the visual script underwent iterative revisions with input from the entire development team until a consensus was reached.

Finally, the production team proceeded to produce the video using the visual script and the recording of the textual script. The production phase was also followed by an iterative feedback process, with multiple iterations of the video produced until all parties were satisfied with the final result.

4.2 Expert Evaluation

Our intended target audience is election organizers who are in charge of important decisions such as whether an online channel will be offered for an election. However, through the limits in time and complexity that can be conveyed through our chosen short-video approach (see Sect. 4.1), we needed to simplify the topic. To avoid the risk that this simplification introduced inaccuracies, we chose to perform an expert evaluation first, to guarantee the correctness of the simplified content.

Reaching Out to Experts. We reached out to 18 German-speaking internet voting experts directly via email. Additionally, we contacted the email distributor for internet voting offered by the Federal Office for Information Security (BSI[3]). We believe that the selection considered most internet voting experts in the research community who understand German.

The invitation mail contained the following questions:

- Is the subject matter presented in the video presented correctly according to your understanding?
- Are there any aspects of the video that are misrepresented or could be misleading?
- What did you (not) like about the video?

With the invitation email we offered a two-week period to respond. Experts could participate by simply answering the email or by filling out the anonymous online questionnaire (linked in the invitation email). A reminder email was sent one week later to encourage participation. In total, we have received 19 answers.

Analysing the Responses. The responses we received were forwarded to a different member of the research team who merged and randomized the responses to ensure anonymity and avoid bias in the analysis. The feedback analysis then broke down the experts' responses into their statements which were categorized into three categories by two members of the research team:

- *Issues to Address* contained all the comments in which experts identified potential inaccuracies or misleading aspects of the video. This category highlighted areas that require further review or clarification.
- *Suggestions* captured recommendations for changes that did not necessarily point to inaccuracies but offered ideas for improvements, such as adjustments in content or presentation.
- *General Feedback* included comments on what experts liked or disliked about the video, reflecting their personal preferences and biases. In particular, remarks about inaccuracies were excluded from this category.

Any disagreements on understanding and categorization were resolved through brief discussions among research team members. Subsequently, the *Issues to Address* category was further analysed by two team members. They sub-categorized the feedback into three specific areas: *Correctness*, *Completeness*, and *Clarity*. For each aspect under *Correctness*, the team discussed internally to determine agreement with feedback or different points of view, with these points detailed in Sect. 5.2. Feedback about *Completeness* and *Clarity* was also carefully reviewed and decisions were made on whether and how to address these points in a future revised version of the video.

[3] https://www.bsi.bund.de/DE/Home, Last accessed on 24.01.2025.

5 Expert Evaluation

In this Section, we present the analysis to our expert evaluation as described in Sect. 4. We start with the results collected in Sect. 5.1, which we discuss in Sect. 5.2. Finally, the limitations of this analysis are presented in Sect. 5.3.

5.1 Results

We received responses from a total of 19 experts. In general, the experts indicate that they enjoy the video, and often give useful suggestions to improve the video further. Nine experts note minor issues, while they express none of the issues as critical. In this evaluation, we focus on statements that we classify as "Issues to address". We received 29 statements in this category which were sub-categorized into nine statements concerning *Correctness*, 11 concerning *Clarity*, and nine concerning *Completeness* (see Table 1). Given the substantial number of responses, we focus on a representative subset of the feedback that encompasses the most significant themes.

Table 1. Number of statements that were classified as "Issues to address".

Category	
Correctness	9
Clarity	11
Completeness	9

Correctness. Some of the statements are related to the potential manipulation of votes by the servers, proposing attacks against the presented internet voting system:

- **Expert 4:** As long as only ONE provider is honest [...] and if a majority (not all) providers manipulate together, then they can enforce their (manipulated) ballots as the true ones [and decide] against the honest providers by majority vote. Or not?
- **Expert 12:** With regard to protection against manipulation, tallied-as-cast [...] is not covered at all, is it?

Other statements are related to authentication:

- **Expert 5:** The fact that the nPA [the German electronic identity card] is not used for general applications or services does not prevent it from being used for voting, does it?
- **Expert 5:** The person voting must still identify themselves to the election server, otherwise anyone can send any code and use brute force to cast the correct vote, which is why the statement that the identity of the person voting is not known by malware is not true.

Additionally, one expert's statement is related to costs; **Expert 18** "would not generally agree that specific voting devices are generally too complex and expensive", responding critically to a statement made in the video that argues that dedicated voting devices delivered to each voter are impractical due to the complexity and cost of such a solution.

Clarity. Most of the responses categorized into the *Clarity* category are related to the phrasing used in the video and often contain alternative phrasings proposed by the experts. Two different experts mention that the phrase "mathematical proof" might be misleading. For example, **Expert 3** writes that "When checking the verification codes, I would not speak of "mathematical proof", but rather of a strong indication that the vote must have arrived correctly."

Two experts highlight clarity issues related to the approach:

- **Expert 1:** It is claimed that [...] the vote would be counted later if only at least one of the participants in the online voting system works correctly. This is ultimately not wrong, but misleading, because, in fact, as soon as the participants in the online voting system no longer agree, 'the election is canceled' and no counting takes place. The system as such is therefore not robust.
- **Expert 19:** The candidate code is incredibly long and complicated. Or could you not use much shorter codes?

Completeness. With regards to *Completeness*, experts mentioned that we could add different aspects to the video to have a more holistic view. Four of the proposed additions are listed below:

- **Expert 11:** Not wrong or misleading, but one aspect was missing: denial of service.
- **Expert 12:** It should also be mentioned that the postal service provider must be trusted throughout the entire scenario.
- **Expert 19:** The voting machine must also be trusted in this approach to voting secrecy. A manipulated device could simply display: "Enter the name of your candidate".
- **Expert 19:** If you are already proposing approaches "without protection of voting secrecy" (as you call it) you must also mention the Swiss approach [...].

5.2 Discussion

We now discuss all the expert responses mentioned in Sect. 5.1, and give an outlook on how this may be addressed in the next version of the video.

Correctness. Given the fully-defined system we presented in Sect. 3, we observe that a single honest server is sufficient to guarantee the true cast ballots are tallied, and prevent even a majority of dishonest servers from proposing manipulated ballots. The reason is that the servers confirm to each other using digital signatures that some incoming vote is the first valid vote of that voter. Only if this agreement is successful will the servers then produce the return code. This aspect was not mentioned in the video to reduce the amount of concepts explained, but we will consider including it in the next version, possibly with a suitable simplification.

Responding to the feedback related to the authentication process, we agree that the nPA could, in principle, be used to authenticate electronic ballots, similar to how the eID is used in Estonia to authenticate [9], and we could mention this in the video. However, we note that the nPA is as of yet not broadly used in Germany [14]. Responding to the second feedback related to authentication, which suggests that the voting codes alone are insufficient to authenticate an eligible voter, we note that the voting codes visualized in the video are designed to hold more than 128bit of randomness[4]. This is considered to be secure against random guessing by current standards[5]. We plan to address this in a future version of the video by explicitly stating that the codes are chosen sufficiently long that they cannot be guessed. What we also have to acknowledge is that the phrasing at this point in the video is not very clear about identification, and indeed, as the expert noted, the casting voter can be identified: for example by malware on the voter's device, or by an implementation which may as a hardening measure require the voters to additionally login[6]. However, the secrecy of the votes is still ensured, as the voting code does not reveal the voter's choice, and the tally phase makes sure the encryptions related to the voter's choice are separated from the casting voter before decryption (see Sect. 3).

Regarding costs, we agree that it is hard to make absolute statements concerning which approaches are more expensive than others, as costs depend on several factors, such as the size of the electorate or the frequency of elections. As this is also not the core point of the video, instead of discussing the cost of different voting modalities (e.g., using the Estonian example [12]), we plan to address

[4] We chose the alphabet A_{57} from [7], which holds 5.83 bit per character. Each voting code is 25 characters long, hence each holds 145.75 bits of information. The "spare" bits may be used for other purposes, e.g. validation or error correction.

[5] NIST considers 128bits secure until 2030 and beyond, see https://www.keylength.com/en/4/, last accessed 24.01.2025.

[6] This may help to defend against denial of service attempts, which flood a server with many (invalid) requests, until they are overwhelmed and can no longer respond.

this in a future version of the video by choosing a more open formulation, or not mentioning this point at all.

Clarity. It was suggested to avoid using the term "mathematical proof", but instead "strong indication", when describing the verification of the confirmation codes. Indeed, in a scientific publication, one would not use "mathematical proof", as this implies an absolute (true) result, whereas in the proposed system, even if the verification of the confirmation code is successful, the voting code may not reach the tally: For example, the adversary might have prevented the voting code from reaching the servers and guessed the confirmation code. However, this can be made very unlikely (to the extent of practical impossibility) by proper configuration of the system, for example, a sufficient length of the confirmation codes. In a future version of the video, we will strive for an alternative wording that finds a better balance between transporting the desired meaning intuitively, while also being factually correct.

We agree with the expert arguing that "the vote would be counted later if only at least one of the participants in the internet voting system works correctly [...] [is] misleading", as indeed in the design chosen, the election could be forced to be canceled by a single dishonest server, by it simply refusing to participate in the generation of confirmation codes or the decryption in the tally phase[7]. This phrase intended to focus on the strong security guarantees, mentally prefixed with "if the confirmation code is correct, and the election is tallied, then [...]". The next version of the video will communicate this more appropriately.

We further agree with the expert that the voting codes are very long. However, in our running example voting system, the voting codes also serve as the authentication mechanism, and therefore need to be sufficiently long to be hard to guess for the adversary. We could instead separate authentication from the voting codes and, by this, reach very short voting codes in the length of the number of candidates (a single digit would be sufficient for up to 10 candidates), as proposed in [1]. We will reevaluate in the next version of the video whether we can present an approach using shorter voting codes, or whether these suggestions are less appropriate for our purposes, which are strongly focused on simplicity of presentation.[8]

Completeness. Some experts notice that not all trust assumptions are explicitly stated in the video. Although a letter is stated to be delivered to the voter, it is not mentioned that this assumes the postal service to be honest. In a similar spirit, the video does not mention that voters are only protected if they use the voting system as intended (even if a malicious component tries to convince

[7] While such active dishonest behaviour is likely attributable, if the adversary does not fear or care about the consequences, it might still manifest.

[8] For example, mapping the fundamental ideal of [1] to our proposal would require the voter to enter two values, concretely one long authentication secret and one short voting code. This might substantially increase the textual and visual burden of the casting procedure in our informational video.

the voter to break protocol). Another expert mentions that relevant context to internet voting is omitted, specifically a discussion of denial of service attacks. While the video can not discuss all aspects of internet voting, due to its target audience and limited duration, we may reevaluate the relative importance of e.g. fully and precisely stating our trust model versus other mentioned aspects of internet voting.

When the video discusses the advantages and disadvantages of the presented voting system, a table visualizes potential trade-offs to other approaches. Based on the feedback received, we realize that the table visually (wrongly) transports the meaning that we compare to other actual approaches. However, our only goal was to argue that, overall, other valid approaches with different trade-offs exist, which we intend to visualize better in a future version of the video.

5.3 Limitations

This study has several limitations that should be acknowledged.

- Feedback from the experts may not fully address the practical concerns and informational needs of the intended audience – election organizers. We explicitly chose to evaluate the video with experts before sharing it with election organizers to identify any remaining errors in accuracy.
- The feedback from the experts is qualitative, relying primarily on descriptive assessments rather than quantitative metrics. This limits the possibility of generalizing the findings and their respective importance.
- The video is currently produced in German and was reviewed exclusively by German-speaking experts. This language limitation means that the video's applicability and usefulness have not yet been tested with experts from different linguistic backgrounds.
- The system presented in the video is not in active use. Rather, it has been chosen because of its simplistic design, which is useful for our didactic purposes. However, as such, the video may not fully capture the complexities and challenges of actual deployed verifiable internet voting systems.

6 Approach Evaluation & Future Work Recommendations

As described in Sect. 4, the approach applied in this study was based on design science principles, primarily because to the best of our knowledge, there is no comparable and documented endeavour. To support future projects that aim to simplify highly complex topics (which may have significant consequences if communicated incorrectly) to non-expert audiences, we are sharing our insights from this approach alongside the recommendations for future work.

Overall, the adopted approach was successful, as evidenced by the overwhelmingly positive response received for the artifact, and the actionable feedback to improve the video further. We reflect here on the crucial aspects of the approach and discuss possible improvements.

Establish a Clear Basis Before Simplification: At the outset, it was invested in clearly establishing what exact (real-world and therefore complex) scenario would serve as the foundation for the project. Having this well-defined base was crucial during the various stages of simplification. It allowed us to continuously refer back to the original scenario and assess whether the simplifications remained valid. This proved particularly beneficial in ensuring that the integrity of the simplified scenario was maintained throughout the project.

Embrace Interdisciplinary Collaboration: The interdisciplinary nature of our team was invaluable. By integrating insights from different fields, we were able to simplify complex details without sacrificing accuracy. Concretely, having both experts from cryptography and human factors involved, allowed us to balance necessary detail with understandability. The general success of this collaborative approach was reflected in the expert feedback, which did not highlight any major flaws in the simplifications.

Be Aware of Challenges in Phrasing: Throughout development, and during expert evaluations, we encountered the significant challenge of finding universally acceptable phrasing. To address this, we involved the video production team, who were non-experts, from the outset. Their input was invaluable in flagging phrases and concepts that the cryptography and human-factors experts assumed were self-evident but were not clear to a broader audience. Despite numerous iterations and alternative proposals, the e-voting experts we consulted continued to suggest revisions, underscoring how difficult it is to find phrasing that resonates across diverse perspectives and backgrounds.

Seek Early Expert Review for Textual Script: A key lesson we have learned is the importance of obtaining expert feedback on the video script *prior* to the production of the visuals. Much of the feedback we received was related to the textual content, rather than the visualizations. This suggests that involving experts earlier in the process could resolve potential issues before the time-consuming visual production begins. However, we note that some visuals also lead to actionable feedback from the experts: Concretely, the comparison table of voting systems was misunderstood to compare to concrete systems, instead of the intended meaning to highlight more generally that all approaches have advantages and disadvantages. This indicates that expert feedback and potential revisions after visual production cannot be fully avoided.

7 Conclusion

We produced an informative video through interdisciplinary collaboration, aimed at informing election organizers about the security challenges associated with conducting elections online, outlining existing methods to mitigate risks, and highlighting the remaining issues. We chose a short video as our medium and devoted considerable effort to simplifying and condensing the complex topic. To ensure the factual correctness of the video, we sought feedback from German-speaking internet voting experts. The feedback is overall positive, and no major issues identified, while it is very helpful to refine the video further. With the final, to be produced, version of this video we hope to contribute to the further advancement of secure internet voting, especially in Germany.

We find that establishing a clear basis before simplification, which can be consulted when developing the presentation of the topic, helps to keep the simplifications accurate and consistent. Further, useful for the simplification is especially interdisciplinary collaboration, which enables one to continuously balance details with understandability. However, this can not fully resolve the challenges of phrasing, which seem to be best addressed by including a large number of reviewers of diverse backgrounds in the project. Finally, besides expert review of the final result, expert review of the textual script can uncover most of the areas for improvement before the time-consuming production of the visuals begins. By sharing these insights, we hope to offer guidance and a starting point for similar endeavours trying to simplify a complex topic for a non-expert audience, without the simplification jeopardizing the correctness of the explanations.

Acknowledgement. This work was supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs. Further, this work benefited from funding managed by the French National Research Agency under the France 2030 program with the reference ANR-22-PECY-0006. Finally, we would also like to thank MotionEnsemble (Lena Schall, Alexander Lehmann) for their valuable support in producing the video and helping to refine its content.

References

1. Cortier, V., Debant, A., Moser, F.: Code voting: when simplicity meets security. In: Computer Security – ESORICS 2024, pp. 410–429. Springer, Cham (2024)
2. Cortier, V., Gaudry, P., Glondu, S.: Belenios: a simple private and verifiable electronic voting system, pp. 214–238. Springer, Cham (2019)
3. Federal Chancellery: Federal chancellery ordinance on electronic voting (2013). https://www.fedlex.admin.ch/eli/cc/2022/336/en
4. Germann, M., Serdült, U.: Internet voting and turnout: evidence from Switzerland. Elect. Stud. **47**, 1–12 (2017)
5. Gharadaghy, R., Volkamer, M.: Verifiability in electronic voting - explanations for non security experts. In: Krimmer, R., Grimm, R. (eds.) Electronic Voting 2010. LNI, vol. P-167, pp. 151–162. GI (2010)
6. Haenni, R., Koenig, R.E., Locher, P.: Private internet voting on untrusted voting devices. In: Financial Cryptography and Data Security. FC 2023 International Workshops, pp. 47–62. Springer, Cham (2024)
7. Haenni, R., Koenig, R.E., Locher, P., Dubuis, E.: CHVote protocol specification. Cryptology ePrint Archive, Paper 2017/325 (2017). https://eprint.iacr.org/2017/325
8. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), pp. 1–8 (2014)

9. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: International Conference on Electronic Voting (EVOTE) (2014)
10. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**(1), 75–105 (2004)
11. Hilt, T., Berens, B., Truderung, T., Udovychenko, M., Neumann, S., Volkamer, M.: Systematic user evaluation of a second device based cast-as-intended verifiability approach. In: Voting'24. Springer (2024)
12. Krimmer, R., Duenas-Cid, D., Krivonosova, I., Vinkel, P., Koitmae, A.: How much does an e-vote cost? Cost comparison per vote in multichannel elections in Estonia. In: Electronic Voting, pp. 117–131. Springer, Cham (2018)
13. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: How much usability can you sacrifice for security? IEEE Secur. Priv. **15**(3), 24–29 (2017)
14. Liesbrock, P., Sneiders, E.: Assessing poor adoption of the Eid in Germany. In: Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Colla, V. (eds.) Information Systems and Technologies, pp. 292–301. Springer, Cham (2024)
15. Llewellyn, M., et al.: Testing voters' understanding of a security mechanism used in verifiable voting. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). USENIX Association (2013)
16. Manasrah, A., Masoud, M., Jaradat, Y.: Short videos, or long videos? A study on the ideal video length in online learning. In: 2021 International Conference on Information Technology (ICIT), pp. 366–370 (2021)
17. Moser, F., Kirsten, M., Dörre, F.: SoK: mechanisms used in practice for verifiable internet voting. In: 9th International Joint Conference on Electronic Voting (E-Vote-ID 2024). LNI, Gesellschaft für Informatik (2024)
18. Noetel, M., et al.: Video improves learning in higher education: a systematic review. Rev. Educ. Res. **91**(2), 204–236 (2021)
19. Schürmann, C., Jensen, L.H., Sigbjörnsdóttir, R.M.: Effective cybersecurity awareness training for election officials. In: Electronic Voting, pp. 196–212. Springer, Cham (2020)
20. Storer, T., Little, L., Duncan, I.: An exploratory study of voter attitudes towards a pollsterless remote voting system. In: IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings, pp. 77–86. Citeseer (2006)
21. Swiss Post Ltd.: Swiss post voting system – system specification (version 1.4.1), Technical report, Swiss Post Ltd. (2024)
22. Thürwächter, P.T., Volkamer, M., Kulyk, O.: Individual verifiability with return codes: manipulation detection efficacy. In: Electronic Voting, pp. 139–156. Springer, Cham (2022)
23. Volkamer, M., Kulyk, O., Ludwig, J., Fuhrberg, N.: Increasing security without decreasing usability: a comparison of various verifiable voting systems. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), pp. 233–252. USENIX Association (2022)
24. Wikström, D.: A universally composable mix-net. In: Theory of Cryptography, pp. 317–335. Springer, Berlin, Heidelberg (2004)
25. Wolchok, S., Wustrow, E., Isabel, D., Halderman, J.A.: Attacking the Washington, D.C. internet voting system. In: Financial Cryptography and Data Security, pp. 114–128. Springer, Berlin, Heidelberg (2012)