German voters' attitudes towards voting online with a verifiable system

Oksana Kulyk[1], Melanie Volkamer[2], Niklas Fuhrberg[2], Benjamin Berens[2], and Robert Krimmer[3][0000−0002−0873−539X]

[1] IT University of Copenhagen, Denmark
okku@itu.dk
[2] Karlsruhe Institute of Technology, Germany
{name.surname}@kit.edu
[3] Johan Skytte Institute of Political Studies, University of Tartu, Ülikooli 18, 51003, Tartu, Estonia
robert.krimmer@ut.ee

Abstract. A representative study came to the conclusion that more than 63% of German voters would have like to cast their vote for the federal election in 2021 online. In this paper, we aimed to investigate why Germans might be in favour or against online voting, conducting a online survey. We furthermore aimed to study the reactions of people being in favor of online voting if confronted with a verifiable remote voting system, as well as with interventions aimed at communicating that it is important to follow all the steps to verify. Our findings show that the the majority of our participants were generally willing to vote online. Convenience emerged as the most popular reason for voting online. The reaction to the verifiable remote voting system was diverse, from our participants being irritated from the complexity, to very positive reactions due to high security level. Nonetheless, the majority of the participants did not change their willingness to vote online after seeing the proposed system. the different interventions had no effect. Furthermore, the majority agreed on the importance of verifiability being in place.

Keywords: user study · verifiable Internet voting · trust

1 Introduction

Internet voting is in the middle of societal discussions again, given the ongoing push towards digitalisation of the society and the COVID-19 pandemic that poses risks with traditional polling-place voting. Especially in Germany, in the context of recent federal elections, internet voting is being widely discussed, with political parties using online voting systems for internal elections[4], and the Federal Office of Information Security issuing guidelines on how to securely conduct elections using online voting for the next so called social elections organized by the health

[4] https://archiv.cdu.de/artikel/1-digitaler-parteitag-der-cdu-so-funktionierten-die-abstimmungen (Oct 30 2021)

insurance agencies (being the third largest election in Germany)[5]. Some months before the German federal elections in 2021, a nation-wide survey has shown that 63% of Germans would like to cast their vote for the federal elections online[6].

Given that the majority of voters is in favor of e-voting, in this work we aim to gain insights into what exactly are the reasons why people are willing or not willing to vote online. As we expected that most participants have either no experience with online voting or only with black box voting systems (i.e. systems not providing any means to verify that the vote as tallied as cast), we were also interested in their reaction when being confronted with a verifiable voting system. As both the voting procedure and the security guarantees of verifiable voting systems differ from black box voting systems, we aimed to investigate how voters' attitude is affected when gaining some insights into how the voting procedure would look like, and what are the steps they can perform to verify that their vote is not manipulated. We decided to use the idea of return codes as it is implemented in the Swiss voting system for various reasons: e.g. the steps to verify are more integrated in vote casting than it is is the case e.g. in Helios [4]; it has been used in Switzerland for actual elections, and past research has improved its usability and has shown that it is usable [17]. Furthermore, we were interested the effect of different interventions explaining in a more or less alarming way that it is important to carefully take all the steps described in the received voting material. This last research question is motivated by the fact that past research has concluded that it is important to motivate voters to verify as well as to explain the importance for the overall security of the system [17]. In particular, we are interested whether such interventions have a negative impact on trust.

To answer all these research questions, we conducted an online survey with 548 participants. Our findings show that the the majority (62%) of our participants were generally willing to vote online, which aligns with the nation-wide study, indicating the representativeness of our sample. Convenience emerged as the most popular reason for being in favor of voting online and security concerns and potential for manipulation are the most popular reasons for being against it. 18% changed their attitudes from positive to either neutral or against online voting once confronted with the verifiable voting system. Interestingly, we could not measure a significant difference between different interventions neither wrt. general attitude towards online voting nor trust in the proposed system. We discuss all our findings and deduce future research directions as well as lessons learned for actual elections.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03162/BSI-TR-03162.pdf (Oct 30 2021)

[6] https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-sprechen-sich-fuer-Online-Wahlen-aus (Oct 30 2021)

2 Related Work

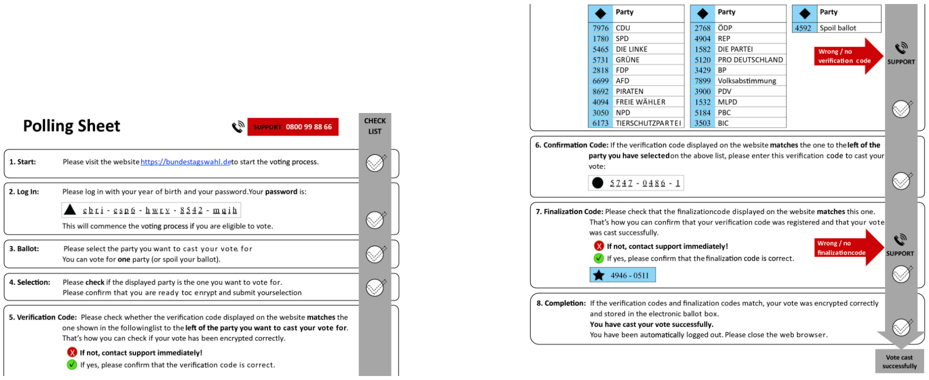
Studies – e.g. [16, 23–27, 30, 39] – have shown that several human related factors should be considered when developing and introducing a verifiable electronic voting system. Other research has evaluated the usability of verifiable electronic voting systems, e.g. [1–3, 5, 7, 10–14, 17–20, 22, 28, 35, 36]. Several report serious usability issues (incl. that participants have difficulties with detecting manipulations if the adversary manages to tamper with the flow of the verification process) as well as misperceptions. For instance, Distler et al. [10] report that their participants felt less secure after having verified than before. In [7], the authors report a high score of verification efficacy, probably because of the system was developed using a human-cantered security approach. Other base for this work is the research conducted by Marky et al. [21] on the usability of code voting in general. [14] also evaluated the usability and acceptance of code voting and code-based verification. According to this work, a system with the highest security assurance was more accepted by the voters, even if the usability of this system was rated worse compared to less secure systems.

Internet voting as a technology is perceived to be highly disruptive and as such has the potential to change the electoral process as a whole. Studies investigating the take-up of such technologies, have focused on the adoption of the technology in a given context [29], the end-user [9, 34], or the relationship between society and technology. Early adoption of Internet voting has been largely connected to technical competence and experience [33]. Similar patterns were found for the use of verifiability when voting online [32]. Nonetheless, due to their disruptive nature, introducing new technologies in elections can lead to perceived lack of legitimacy which leads to lack of trust and acceptance [6].

3 Background

In this section we describe the approach used in Switzerland to provide voters a mean to verify that their vote as neither manipulated by their own device they use to cast their vote nor by one voting server once received. This approach is one instantiation of so called code-based verifiable voting systems. These approaches issue voters with a unique *polling sheet*, delivered via postal mail. This sheet provides the website address voters can use to cast their votes, instructions, and one or more codes to verify the correct processing of their vote. In this work, we use a variant based on a voting system used in Swiss elections [31], with the polling sheet and user interface modifications developed by Kulyk et al. [17]. While there also exist improvements from [22], we decided to go for the Kulyk et al. [17] because it was evaluated with respect to more attack types than the proposal by Marky et al. [22].

The polling sheet of [17, 22, 31] provides three types of codes: check, confirmation *and* finalization code. In order to cast their vote, the voter first has to identify themselves by entering their password, which is provided on the polling sheet. After selecting the party to vote for and reviewing the choice, the voter is provided on the screen a check code and is asked to check that the displayed check code corresponds to the personalised one on their polling sheet. If the codes match, the voter then has to provide the confirmation code. Otherwise, they are instructed to report the mismatch to the election authorities, using the number on the polling sheet. The voter is informed that once they enter and submit the confirmation code, the vote is considered cast and that they are not allowed to cast a vote via postal or in the polling stations anymore. Once entered the confirmation code, the page with the finalization code is displayed. The purpose of the finalization code is to reassure the voter that the voting system has indeed cast their vote as intended, and giving the voter the possibility to confirm that the code displayed is matching their choice. The corresponding polling sheet is displayed in Fig. 1.



Polling Sheet ☎ SUPPORT 0800 99 88 66

1. Start: Please visit the website https://bundestagswahl.deto start the voting process.

2. Log In: Please log in with your year of birth and your password.Your **password** is:

▲ cbri - csp6 - hwrv - 8542 - mqih

This will commence the voting process if you are eligible to vote.

3. Ballot: Please select the party you want to cast your vote for
You can vote for **one** party (or spoil your ballot).

4. Selection: Please **check** if the displayed party is the one you want to vote for.
Please confirm that you are ready toc enrypt and submit yourselection

5. Verification Code: Please check whether the verification code displayed on the website **matches** the one shown in the followinglist to the **left of the party you want to cast your vote for**.
That's how you can check if your vote has been encrypted correctly.

☒ **If not, contact support immediately!**

✓ If yes, please confirm that the verification code is correct.

◆	Party	◆	Party	◆	Party
7976	CDU	2768	ÖDP	4592	Spoil ballot
1780	SPD	4904	REP		
5465	DIE LINKE	1582	DIE PARTEI		
5731	GRÜNE	5120	PRO DEUTSCHLAND		
2818	FDP	3429	BP		
6699	AFD	7899	Volksabstimmung		
8692	PIRATEN	3900	PDV		
4094	FREIE WÄHLER	1532	MLPD		
3050	NPD	5184	PBC		
6173	TIERSCHUTZPARTEI	3503	BIC		

6. Confirmation Code: If the verification code displayed on the website **matches** the one to the**left of the party you have selected**on the above list, please enter this verification code to cast your vote:

● 5747 - 0486 - 1

7. Finalization Code: Please check that the finalizationcode displayed on the website **matches** this one.
That's how you can confirm that your verification code was registered and that your vote was cast successfully.

☒ **If not, contact support immediately!**

✓ If yes, please confirm that the finalization code is correct.

★ 4946 - 0511

8. Completion: If the verification codes and finalization codes match, your vote was encrypted correctly and stored in the electronic ballot box.
You have cast your vote successfully.
You have been automatically logged out. Please close the web browser.

(a) Polling Sheet Top Part

(b) Polling Sheet Bottom Part

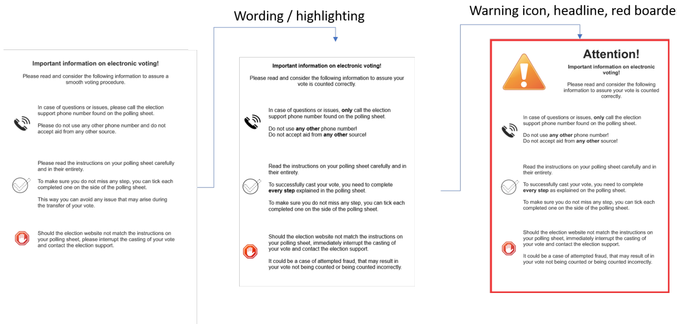
Fig. 1: Polling Sheet

4 Methodology

Here we are describing the selected approach for this research.

4.1 Designing the Interventions

Several researchers have noticed a lack of voter's motivation to actually verify as well as misconceptions regarding which information to trust and which not to trust. For the verifiability approach making use of codes it is important (1) that voters only follow all the instructions on their polling sheet, (2) that they call the election organizers in case the instructions on the webpage are different, and (3) that they dial the number provided on the polling sheet (and not a number provided on the webpage). This information was provided in an additional document which we call intervention. We designed three different interventions. These are more or less alarming (see Fig. 2 which also indicates the main differences). The motivation to have three is the following: Being more alarming makes it more likely that voters read and apply it. However, it may cause more distrust in the voting system as warning icons are often recognized as something negative [37].


Wording / highlighting
Warning icon, headline, red boarder

Important information on electronic voting!

Please read and consider the following information to assure a smooth voting procedure.

In case of questions or issues, please call the election support phone number found on the polling sheet.

Please do not use any other phone number and do not accept aid from any other source.

Please read the instructions on your polling sheet carefully and in their entirety.

To make sure you do not miss any step, you can tick each completed one on the side of the polling sheet.

This way you can avoid any issue that may arise during the transfer of your vote.

Should the election website not match the instructions on your polling sheet, please interrupt the casting of your vote and contact the election support.

Important information on electronic voting!

Please read and consider the following information to assure your vote is counted correctly.

In case of questions or issues, **only** call the election support phone number found on the polling sheet.

Do not use **any other** phone number!
Do not accept aid from **any other** source!

Read the instructions on your polling sheet carefully and in their entirety.

To successfully cast your vote, you need to complete **every step** explained in the polling sheet.

To make sure you do not miss any step, you can tick each completed one on the side of the polling sheet.

Should the election website not match the instructions on your polling sheet, immediately interrupt the casting of your vote and contact the election support.

It could be a case of attempted fraud, that may result in your vote not being counted or being counted incorrectly.

Attention!

Important information on electronic voting!

Please read and consider the following information to assure your vote is counted correctly.

In case of questions or issues, **only** call the election support phone number found on the polling sheet.

Do not use **any other** phone number!
Do not accept aid from **any other** source!

Read the instructions on your polling sheet carefully and in their entirety.

To successfully cast your vote, you need to complete **every step** as explained on the polling sheet.

To make sure you do not miss any step, you can tick each completed one on the side of the polling sheet.

Should the election website not match the instructions on your polling sheet, immediately interrupt the casting of your vote and contact the election support.

It could be a case of attempted fraud, that may result of in your vote not being counted or being counted incorrectly.

Fig. 2: Interventions: IN-L (low alarming), IN-M, and IN-H (high alarming)

4.2 Research Questions and Hypotheses

We study the topic using both a quantitative and a qualitative approach with two sets of research questions. For the qualitative part, we have posed three research questions.

RQ1: What are reasons for participants being in favour, neutral, or against casting their vote over the Internet for federal elections?

RQ2: What are reasons for participants being in favour, neutral, or against using the introduced system to cast their vote over the Internet for federal elections – while focusing on those who are in general in favor of online voting.

RQ3: What is users feedback on the voting system and the interventions?

Following this qualitative approach, we investigate the effect of being exposed to a particular *verifiable system on people's attitudes towards online voting*, including the effect of three different interventions, using a quantitative approach. We define and test the following hypotheses for those participants who – in general – like to cast their vote online for federal elections:

H1 There is a difference in terms how *willing* participants are to use the proposed system to vote online, depending on the intervention.
H2 There is a difference in terms of overall *trust* in the system, depending on the intervention.
H3 There is a difference in terms of *perceived usefulness of verifiability*, depending on the intervention.

4.3 Study Procedure

The study is structured in the following phases (see also Fig. 3): 'Welcome & Informed content', question on 'Taking part in 2021 federal elections', question on 'Voting online if possible for 2021 federal election', 'introduction of voting system with and without interventions', 'attention check', question on 'Voting wit this system for 2021 federal election', questions on 'general trust, importance of verifiability', 'comments' to the voting system and if applicable to the intervention, and 'demographics, thanks and reimbursement'.

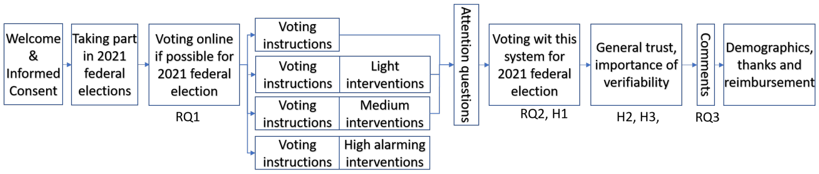

Welcome & Informed Consent
Taking part in 2021 federal elections
Voting online if possible for 2021 federal election
RQ1
Voting instructions
Voting instructions
Light interventions
Voting instructions
Medium interventions
Voting instructions
High alarming interventions
Attention questions
Voting wit this system for 2021 federal election
RQ2, H1
General trust, importance of verifiability
H2, H3,
Comments
RQ3
Demographics, thanks and reimbursement

Fig. 3: Study design

For 'general trust, importance of verifiability', we used questions, adapted from a questionnaire introduced in [38][7]. The questions are provided in Fig. 5. The changes that we made included (1) changing the scale from 6-point to 5-point in order to make it more consistent with the rest of our questionnaire, (2) adapting the questions about the voting and the process to verify in order to account for differences between the voting system for which the questionnaire has originally been developed and the system that we evaluate, (3) adapting and expanding the questions about beliefs regarding the possibility of election manipulation to account for different verifiability aspects. Note, items 1–7 are used to evaluate H2 on general trust and items 8 and 9 to evaluate H3 on perceived usefulness of verifiability.

4.4 Recruitment and Ethics

We recruited the participants using the Clickworker platform. We did so one week before the federal election in Germany took place. Participants were paid €1,6 for their participation which was estimated to take 10 minutes (based on conducted pretests), which corresponds to an hourly fee above the minimal wage in Germany. In order to ensure quality of the collected data, we introduced attention checks in the questionnaire, of which the participants were informed at the beginning of the survey. While there is no mandatory ethical review process at the authors' institutions, we took care to ensure that no harm is being done to the participants, asking for their informed consent and providing them with the information about the purpose of the study, the fact that their participation is anonymous, and that they can decide at any time to stop participating.

[7] The original questions were translated to German (using back-&-forward translation).

5 Results

We denote "CG" as the control group, i.e. the participants who did not see an interventions, and we denote "IN-L", "IN-M" and "IN-H" the group with low alarming, medium alarming, and high alarming intervention (see Section 4.1) correspondingly. For the analysis of hypotheses H1-H3 we conduct statistical tests (using R package "stats"). For the analysis of research questions RQ1–RQ2 we conduct open coding of participants' open-ended answers using the following procedure: (1) one author developed an initial code book out of 20% of the answers. (2) Afterwards the code book was discussed with a second author and adopted to the code book used for the next step. (3) Two authors coded another 20%. (4) This assignment was discussed while only minor adoptions to the assignment as well as to the code book were necessary. (5) One author coded all answers. Note, the coding was done in German and afterwards translated.

5.1 Demographics

There were 548 participants[8], of them 339 men, 207 women and 2 non-binary persons. The most common age group was 30 to 34 years old with 96 participants, followed by 35 to 39 years old (79 participants); among the rest of the participants, 119 were between 18 and 30 and 254 were above 40 years old. Note, 21 were above 65 years old. Looking at the educational level: 33 finished high-school, 80 completed an apprenticeship, 47 had an entrance qualification for a university of applied sciences, 135 had an university entrance qualification, 253 had an university or university of applied science degree. About their current employment: 1 was a schoolchild, 5 were in a apprenticeship, 60 were students, 295 are employees, 19 were civil servants, 105 were self-employed, 30 were unemployed and 31 answered others mostly retired persons or stayed at home (2 did not answer the question).

5.2 General attitudes towards online voting (RQ1)

Overall, 62% of participants (343 out of 548) selected either 1 or 2 on a 5-point scale, with 1 indicating "strong agreement" with the statement that they would vote online in the upcoming federal election if it were possible (before seeing the proposed voting system and interventions)[9].We conduct a qualitative analysis of open-ended answers to the question in which participants were asked to explain their statement whether or not they would vote online if possible. We decided to have two code books. One for the answers of those having stated that they are in favor (i.e. 1 or 2) and one for the answers of those being against online voting (i.e. 4 and 5). Both code books were combined for the answers of those having answered neutrally (i.e. 3 on the scale from 1 to 5). The frequency of codes for

[8] Participants who failed attention checks or answered that they have no intention at all to vote in the upcoming election have been excluded.

[9] This percentage matches the Bitkom survey result (see Section 1).

both code books is provided on Table 1. The following codes have been identified from answers of participants being *against online voting*:

- Security concerns: Participants either mentioned general security concerns or data protection concerns. Sometimes they just used the term 'security concern' or that they believe that online voting is insecure.
- Manipulation: Participants state that election can be manipulated, individual votes or the entire result can be changed with online voting. Participants talked about manipulations/ changes, mentioned hackers or cyber attacks, or about the ease to sell votes as it cannot be checked who cast the vote.
- Lack of trust: Participants stated in general that they do not trust in the government to properly set up such a system or are afraid that such a system is properly implemented, i.e. error free.
- Lack of transparency: Participants stated that they think the process or the system (or even both) would not be transparent, i.e. e.g. it is unclear what happens to their vote, how it works, or whether it is working as expected.
- Vote privacy: Participants mentioned risks in regards to free, secret, and anonymous elections; including mentioning risks on voting while being observed.
- Ritual: Participant stated that it is an important, formal, or well-established act of casting their vote on paper or of going to the polling station on this one Sunday (maybe combining it with a walk or with meeting people). Other stated that they simply prefer to cast their vote on paper.
- Being clearly against online voting: Participants did not see a need for a change or stated that they are against online-voting.
- Being uncertain: Participants were uncertain, i.e. they made a decision in one way or the other but do not have a strong opinion; most likely because they have not yet thought a lot about it or they would need more information in order to decide. Several added this in addition to another statement while two just sad that they are uncertain.
- Others: This code is used for nonsense answers as well as answers that did not appear more than twice: e.g. a statement of one participant that the effort for online voting is much to high.

The following codes have been identified from answers of participants being in *favour of online voting*:

- Timely: Participants stated that it is timely to have online voting or to digitalise elections (as one of the governmental services) or participants stated that they are in favor of having all services and processes being digitized.
- Convenience: Participants mentioned that online voting is more convenient because they save time or effort; or that they can decide when and where they can cast their vote. Furthermore this code covers answers related to statements like: it is (more) easy, (more) convenient, (more) comfortable etc. than the available paper based channels.

- Reliable delivery: Participants stated that compared to postal voting the delivery is much faster; i.e. less issues for people living abroad and no need to cast votes remotely several days / weeks before the actual election day.
- More secure: Participants stated that online voting systems are more difficult to manipulate; or that they can be easier protected against manipulations.
- Environment-friendly: Participants mentioned that this is better for our environment as it safes paper and air pollution (no driving to polling stations).
- Advantages for the state: Participants mentioned one or more reasons related to organizing the election: e.g. less poll workers, costs are reduced, counting is faster. Increasing voter turn out is also one aspect of this code.
- COVID-19 related: Participants mentioned something pandemic related.
- Security concerns: Same as in the previous code book.
- Others: This code is used for nonsense answers as well as answers that did not appear more than twice, e.g. no queues before the polling station.

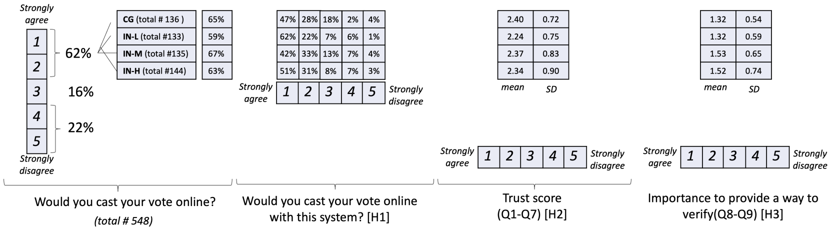
	# mentions		# mentions
convenience	270 (25)	security concerns	46 (37)
security concerns	73 (37)	manipulation	45 (9)
advantages for the state	37 (0)	ritual	19 (7)
timely	32 (1)	lack of trust	14 (5)
environment-friendly	23 (2)	being uncertain	13 (29)
COVID-19-related	22 (0)	lack of transparency	11 (7)
better security	19 (0)	other	9 (6)
other	14 (6)	being clearly against	4 (0)
reliable delivery	6 (0)	vote privacy	3 (7)

Table 1: Code frequency for reasons in favor (left) or against (right) online voting – in parantheses indicate the frequency from participants with a neutral attitude.

5.3 Attitudes towards using the verifiable voting (H1-H3, RQ2)

Out of the participants who initially had a positive willingness to vote online, 63% of them (216 out of 343) did not change their willingness after seeing the proposed system. Among the remaining 127 participants, 15 (4%) were more willing to vote online (changing their response from 2 to 1 on a 5-point scale), 40 (12%) were less willing to vote online but still positive (changing their response from 1 to 2), 41 (12%) changed their response to "neutral" (selecting option 3) and 19 (6%) changed their response to "negative" (selecting either option 4 or 5). Fig. 4 shows the distribution of responses after seeing the proposed verifiable system. There was no significant difference between the intervention types (ANOVA, $F = 1.697$, $p = 0.167$), hence, *H1 cannot be confirmed.*

For the evaluation of H2, a general trust score was computed from the questionnaire items 1-7. Note, the scores for the last three questions (i.e. questions



CG (total # 136)	65%
IN-L (total #133)	59%
IN-M (total #135)	67%
IN-H (total #144)	63%

1	2	3	4	5
47%	28%	18%	2%	4%
62%	22%	7%	6%	1%
42%	33%	13%	7%	4%
51%	31%	8%	7%	3%

mean	SD
2.40	0.72
2.24	0.75
2.37	0.83
2.34	0.90

mean	SD
1.32	0.54
1.32	0.59
1.53	0.65
1.52	0.74

Fig. 4: Descriptive results for Hypotheses H1-H3.

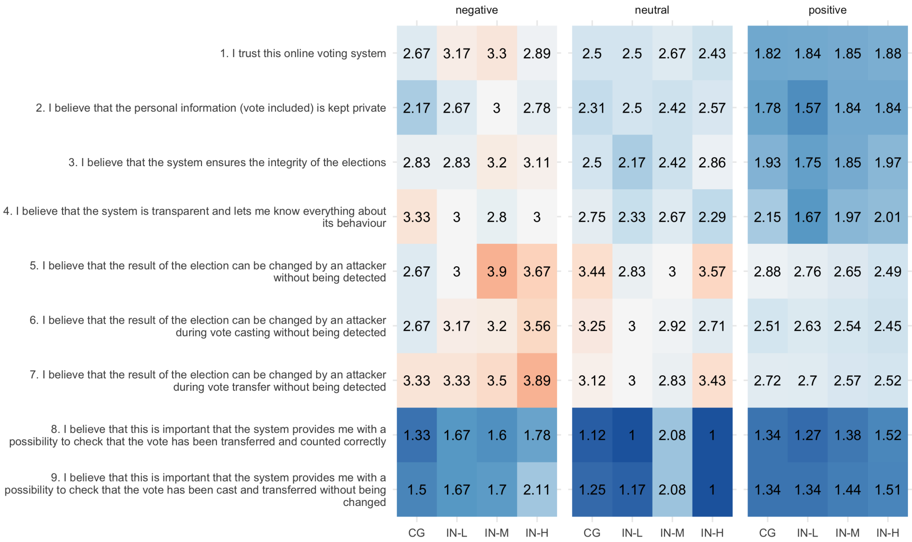
where agreement indicated belief that an undetected manipulation of the election result is possible) were *reversed*. Fig. 4 shows the average resulting scores for all groups. There was no significant difference in the trust scores between the intervention types (ANOVA, $F = 0.646$, $p = .586$), hence, *H2 cannot be confirmed.*

For the evaluation of H3, we computed an average score for the answers to questions 8-9 (i.e. the questions that specifically asked about the usefulness of verifiability). Fig. 4 shows the average resulting scores for all groups. There was no significant difference between the intervention types (ANOVA, $F = 2.0611$, $p = .105$), hence, *H3 cannot be confirmed.*

Figure 5 shows the average scores for each one of the questions by intervention type and the willingness to vote online after seeing the corresponding intervention. Overall, the usefulness of the verifiability was perceived to be high, regardless of the intervention type or the willingness to vote online after seeing the intervention.

In order to answer *RQ2, that is, to better understand the participants' attitudes towards the proposed system and specific interventions*, we analyzed the statements in which they explain their responses. We derived the following codes while the code frequency is provided in Table 2:

- Only system independent advantages: Participants justified their decision by mentioning general advantages they see for online voting. The mentioned advantages are similar to those coded for RQ1.
- System easy to use: Participants stated that the proposed system seems straight forward or that it is easy to cast a vote or more generally to use it.
- Just too complex: Participants only mentioning that the proposed system is e.g. (too) complex, (too) cumbersome, (too) confusing), and (too) error-prone. This code also contains statements of participants being afraid to make a mistake when casting a vote with this system.
- Just more secure: Participants only mentioning that they would use the system as it seems secure. Some particular saying that this is due to the additional steps to verify their vote.
- Complex but system independent advantages: Participants mentioning that the system is complex but they also state that they still see one ore more advantages of online voting – in general.
- Complex but secure: Participants mentioning that the system is complex but they also say that this makes it (more) secure.



	negative				neutral				positive			
	CG	IN-L	IN-M	IN-H	CG	IN-L	IN-M	IN-H	CG	IN-L	IN-M	IN-H
1. I trust this online voting system	2.67	3.17	3.3	2.89	2.5	2.5	2.67	2.43	1.82	1.84	1.85	1.88
2. I believe that the personal information (vote included) is kept private	2.17	2.67	3	2.78	2.31	2.5	2.42	2.57	1.78	1.57	1.84	1.84
3. I believe that the system ensures the integrity of the elections	2.83	2.83	3.2	3.11	2.5	2.17	2.42	2.86	1.93	1.75	1.85	1.97
4. I believe that the system is transparent and lets me know everything about its behaviour	3.33	3	2.8	3	2.75	2.33	2.67	2.29	2.15	1.67	1.97	2.01
5. I believe that the result of the election can be changed by an attacker without being detected	2.67	3	3.9	3.67	3.44	2.83	3	3.57	2.88	2.76	2.65	2.49
6. I believe that the result of the election can be changed by an attacker during vote casting without being detected	2.67	3.17	3.2	3.56	3.25	3	2.92	2.71	2.51	2.63	2.54	2.45
7. I believe that the result of the election can be changed by an attacker during vote transfer without being detected	3.33	3.33	3.5	3.89	3.12	3	2.83	3.43	2.72	2.7	2.57	2.52
8. I believe that this is important that the system provides me with a possibility to check that the vote has been transferred and counted correctly	1.33	1.67	1.6	1.78	1.12	1	2.08	1	1.34	1.27	1.38	1.52
9. I believe that this is important that the system provides me with a possibility to check that the vote has been cast and transferred without being changed	1.5	1.67	1.7	2.11	1.25	1.17	2.08	1	1.34	1.34	1.44	1.51

Fig. 5: Average responses after having seen the verifiable system (scale 1 to 5). Lower scores indicate stronger agreement with the statement, except for questions 5-7 where the scores are reversed.

- Being uncertain: Participants were uncertain, i.e. they made a decision in one way or the other but do not have a strong opinion; most likely because they have not yet though a lot about it or they would need more information in order to decide, e.g. regarding security properties.
- Paper-based is easier: Participants state that they prefer to vote on paper
- Not timely: Participants stated that it does look old-fashion or that the voting system should be all digital, in order to be timely.
- Others: This code is used for nonsense answers as well as answers that did not appear more than twice (overall groups).

5.4 Feedback on the system and the interventions (RQ3)

We received the following feedback to the verifiable voting system or more precisely to the *polling sheet*: Some participants were requesting more information (e.g. regarding the security features or how to cast an invalid vote). Furthermore, we received the feedback that the amount of codes should be removed to simplify the vote casting process. Related to this aspect, some were recommending to explain why it is so complicated. Interestingly, some recommended to use a different approach to authenticate voters, i.e. using the German federal electronic ID card or 'video-ident' which is used for other sensitive services in Germany. We also received feedback that the process should be more close to what is used in the banking context: e.g. the codes should come in different letters and not

	CG	IN-L	IN-M	IN-H	Overall
(+) system-independent advantages	32	36	34	31	133
(+) system easy to use	13	6	12	11	42
(+) more secure	9	13	17	26	65
(+) complex but with system independent advantages	6	6	2	2	16
(+) complex but secure	2	4	2	3	11
(-) too complex	16	11	15	7	49
(-) paper voting is easier	4	5	4	3	16
(-) security concerns	5	2	4	3	14
(-) not timely	1	2	0	2	5
being uncertain	0	1	1	2	4
other	14	5	9	6	34

Table 2: Code frequency for reasons being in favor (or not) of the proposed system

in one letter, two-factor-authentication for submitting the actual vote. Finally, we received feedback on the language and the design of the polling card, e.g. to simplify the language including concrete proposals such as talking about 'numbers' instead of 'codes' and 'help' instead of 'support' and to improve the design e.g. by putting not all content on one page but using several pages.

Regarding the *interventions*, we received the following general feedback: The design of the intervention should be more aligned with the general voting information and the polling sheet. Several provided feedback to simplify the language (e.g. use the term 'help' instead of 'support'), use a more friendly language, and improve the design (e.g. provide more pictures and highlight important terms). Some were requesting more information (e.g. regarding the security, whom to contact in case of questions, why this is so complicated and why it is important to only trust the paper and not what is displayed on the screen, that it is important to cast the vote unobserved, and what to do in case one loses the Internet connection while voting). Many actually noticed that it would be important to also have the telephone number of the support on the intervention and not just on the polling card. Furthermore, several participants in the IN-H group stated that the intervention is deterrent, too negative, and worrying. Related to this, some stated that they feel like they have done something wrong or must be careful to not make mistakes. Correspondingly, a more subtle design was recommended.

6 Discussion and Conclusion

Overall, convenience was mentioned as the most popular reason for online voting (by 270 of 343 participants). However, even among people who were generally willing to vote online, 73 voiced security concerns. Furthermore, security concerns and manipulations were mentioned as the most popular reason against online voting by the people who were not willing to vote online (in total 91 of 120 participants). For those being neutral regarding online voting, security concerns was also the most mentioned reason. It looks like participants currently value convenience over security (e.g. either implicitly trusting the government to take proper measures against security risks, or considering such risks to be low) – although we talked particularly about German federal elections (and not e.g. some elections or polls in very small groups or local societies). We got the impression, that many consider it as easy as online banking and online shopping – while in particular for online banking they may have forgotten how many steps were necessary to start using it.

Only 6% changed their opinion and stated that they would not want to use the proposed system to cast their vote for the 2021 federal election (12% changed to neutral). Given the open text answers as well as the answers to the seven questions on trust this is kind of surprising as several more complained about the complexity of the vote casting process and/or were not certain how much they can trust the system to detect manipulations. It may be explained as the most prominent reason in favor of still using it were system independent advantages of online voting in general, thus again convenience was rated over security.

Thus, future work should investigate on the one hand why many rate convenience over security as well as on explaining why from a security point of view it needs to be more complicated as voters may expect it to be. The good news from [8] is that it is likely that voters will accept additional steps if they understand why it is necessary. Such additional explanations may also convince some of those being against online voting if they understand which security guarantees the system provides.

Interestingly, several participants compared the (security) mechanisms in place with those they know from other context – in particular from the online banking context. Correspondingly, they e.g. did not like that all codes came with one letter and that authentication happens through a password. As future work it should be investigated whether it is either possible to align verifiable voting systems more with processes voters may know from other contexts or to explain why it is different but still secure when developing information material.

We found that most participants – even being against or neutral to the proposed system and even without having seen any interventions – are clearly in favor of having the possibility to verify their vote. While for federal elections, this is a clear requirement[10], as future work we want to investigate whether people would also see this as an important property for other elections and polls. Note, in Germany so far, we have only seen the use of blackbox voting systems. Thus, if voters would require verifiable voting systems this would help to convince election management boards to change to verifiable systems. Furthermore, the fact that participants see a need for verifiable systems should support the investigations in explaining the need for voting systems being more complex than expected.

We found no significant difference between the three intervention groups. The interventions do not seem to change their mind regarding their willingness to use the system, their trust in the system nor their attitude towards the importance of

[10] https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html (Oct 30 2021)

verifiability. Thus, we would recommend to use the high-alarming intervention in a user study to evaluate its effect while evaluating the effectiveness wrt. detecting manipulations as it was studied e.g. in [17, 22]. Furthermore, we want to study the trust score further as a measure instrument which ideally can be applied to various systems – also to compare the trust scores between systems. Additional insights on how to design assurances to increase the voters' trust in verifiable systems – e.g. by including explanations on how the verification process works in the proposed system – can be adapted from research on related fields, such as studying assurances in privacy notices [15].

We conclude that the harm of extra interventions – even very alarming ones – is very limited and should be used to increase the likelihood that voters verify. Furthermore, it is important to address voters' expectations – in particular the one that online voting is more convenient than paper based voting channels. This includes to explain that in order to provide verifiability, systems cannot be as easy as they may wanted it to be.

7 Acknowledgment

This work was supported by funding of the Helmholtz Association (HGF) through the POF subtopic 46.23.01 called 'Methods for Engineering Secure Systems'.

References

1. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. The USENIX Journal of Election Technology and Systems **2**(3), 26–56 (2014)
2. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: From error to error: Why voters could not cast a ballot and verify their vote with Helios, Prêt à Voter, and Scantegrity II. USENIX Journal of Election Technology and Systems **3**(2), 1–19 (2015)
3. Acemyan, C.Z., Kortum, P., Byrne, M.D., Wallach, D.S.: Summative Usability Assessments of STAR-Vote: A Cryptographically Secure e2e Voting System That Has Been Empirically Proven to Be Easy to Use. Human Factors pp. 1–24 (2018)
4. Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX Security Symposium. vol. 17, pp. 335–348. USENIX Association (2008)
5. Bär, M., Henrich, C., Müller-Quade, J., Röhrich, S., Stüber, C.: Real world experiences with bingo voting and a comparison of usability. In: EVT/WOTE (2008)
6. Blanchard, N.K., Selker, T.: Improving voting technology is hard: the trust-legitimacy-participation loop and related problems. In: Proceedings of the 8th Workshop on Socio-Technical Aspects in Security and Trust. pp. 1–8 (2018)
7. Budurushi, J., Renaud, K., Volkamer, M., Woide, M.: An investigation into the usability of electronic voting systems for complex elections. Annals of Telecommunications **71**(7-8), 309–322 (2016)
8. Budurushi, J., Volkamer, M., Kulyk, O., Neumann, S.: Nothing comes for free: How much usability can you sacrifice for security? IEEE Security & Privacy Special Issue on Electronic Voting (2017)

9. Davis, F.D.: A technology acceptance model for empirically testing new end-user information systems: Theory and results. Ph.D. thesis, MIT (1985)
10. Distler, V., Zollinger, M.L., Lallemand, C., Roenne, P., Ryan, P., Koenig, V.: Security–visible, yet unseen? how displaying security mechanisms impacts user experience and perceived security. In: ACM CHI. pp. 605:1–605:13 (2019)
11. Fuglerud, K.S., Røssvoll, T.H.: An evaluation of web-based voting usability and accessibility. Universal Access in the Information Society **11**(4), 359–373 (2012)
12. Gjøsteen, K., Lund, A.S.: An experiment on the security of the norwegian electronic voting protocol. Annals of Telecommunications **71**(7-8), 299–307 (2016)
13. Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability Analysis of Helios-An Open Source Verifiable Remote Electronic Voting System. In: EVT/WOTE. USENIX (2011)
14. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M.: Nothing comes for free: How much usability can you sacrifice for security? IEEE Security & Privacy **15**(3), 24–29 (2017)
15. Kulyk, O., Renaud, K.: "i need to know i'm safe and protected and will check": users want cues to signal data custodians' trustworthiness. In: 2021 Workshop on Human Centric Software Engineering and Cyber Security (2021)
16. Kulyk, O., Volkamer, M.: Usability is not Enough: Lessons Learned from Human Factors in Security - Research for Verifiability. E-Vote-ID pp. 66–81 (2018)
17. Kulyk, O., Volkamer, M., Müller, M., Renaud, K.: Towards improving the efficacy of code-based verification in internet voting. In: VOTING. Springer (2020)
18. MacNamara, D., Gibson, P., Oakley, K.: A preliminary study on a DualVote and Prêt à Voter hybrid system. In: CeDEM. p. 77 (2012)
19. MacNamara, D., Scully, T., Gibson, P.: Dualvote addressing usability and verifiability issues in electronic voting systems (2011)
20. Marky, K., Kulyk, O., Renaud, K., Volkamer, M.: What Did I Really Vote For? In: ACM CHI. p. 176 (2018)
21. Marky, K., Schmitz, M., Lange, F., Mühlhäuser, M.: Usability of Code Voting Modalities. In: Proceedings of CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts),May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA 7 Pages. (2019). https://doi.org/10.1145/3290607.3312971
22. Marky, K., Zollinger, M.L., Roenne, P., Ryan, P.Y., Grube, T., Kunze, K.: Investigating usability and user experience of individually verifiable internet voting schemes. ACM Trans. Comput.-Hum. Interact **28**(5) (2021)
23. Neumann, S., Olembo, M.M., Renaud, K., Volkamer, M.: Helios Verification: To Alleviate, or to Nominate: Is That the Question, or Shall we Have Both? In: International Conference on Electronic Government and the Information Systems Perspective. pp. 246–260. Springer (2014)
24. Olembo, M.M., Renaud, K., Bartsch, S., Volkamer, M.: Voter, what message will motivate you to verify your vote. In: USEC. Internet Society (2014)
25. Olembo, M., Volkamer, M.: E-Voting System Usability: Lessons for Interface Design, User Studies, and Usability Criteria, pp. 172–201. Information science reference (2013). https://doi.org/10.4018/978-1-4666-3640-8.ch011
26. Olembo, M.M., Bartsch, S., Volkamer, M.: Mental Models of Verifiability in Voting. In: E-Voting and Identity. pp. 142–155. Springer (2013)
27. Olembo, M.M., Volkamer, M.: A study to identify trusted verifying institutes in germany. Tech. rep., Technical University Darmstadt (2014), technical Report
28. Oostveen, A.M., Van den Besselaar, P.: Users' experiences with e-voting: A comparative case study. Journal of Electronic Governance **2**(4) (2009)

29. Rogers, E.M.: Diffusion of innovations. NY: Free Press (2003)
30. Schneider, S., Llewellyn, M., Culnane, C., Heather, J., Srinivasan, S., Xia, Z.: Focus group views on prêt à voter 1.0. In: REVOTE,. pp. 56–65. IEEE (2011)
31. Serdult, U., Germann, M., Mendez, F., Portenier, A., Wellig, C.: Fifteen Years of Internet Voting in Switzerland . In: ICEDEG. pp. 126–132. IEEE (2015)
32. Solvak, M.: Does vote verification work: usage and impact of confidence building technology in internet voting. In: International Joint Conference on Electronic Voting. pp. 213–228. Springer (2020)
33. Vassil, K., Solvak, M., Vinkel, P., Trechsel, A.H., Alvarez, R.M.: The diffusion of internet voting. usage patterns of internet voting in estonia between 2005 and 2015. Government Information Quarterly **33**(3), 453–459 (2016)
34. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: Toward a unified view. MIS quarterly pp. 425–478 (2003)
35. Weber, J., Hengartner, U.: Usability study of the open audit voting system Helios. urlhttp://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf (2009)
36. Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., Alberdi, E., Strigini, L.: Assessing the Usability of Open Verifiable E-Voting Systems: a Trial with the System Prêt à Voter. In: ICE-GOV. pp. 281–296 (2009)
37. Wu, M., Miller, R.C., Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks? In: ACM: CHI. pp. 601–610 (2006)
38. Zollinger, M.L.: From Secure to Usable and Verifiable Voting Schemes. Ph.D. thesis, University of Luxembourg, Esch-sur-Alzette, Luxembourg (2020)
39. Zollinger, M.L., Estaji, E., Ryan, P.Y., Marky, K.: “just for the sake of transparency”: Exploring voter mental models of verifiability. In: International Joint Conference on Electronic Voting. pp. 155–170. Springer (2021)