Usability and Understanding of Individual Verifiability in the 2023 GI-Election

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

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

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

Abstract

Individual verifiability allow the voter to check that their vote left their voting device and arrived at the election server in the way they intended and therefore allows to detect possible vote manipulation by the voting device. In order for individual verifiability to be useful it is crucial that voters understand how and under which assumptions it work. We conducted an online user study to examine voter understanding and perceived usability of individual verifiability. The results hint at an insufficient understanding but attest good usability.

CCS Concepts

• **Human-centered computing** → **Human computer interaction (HCI)**.

Keywords

Individual Verifiability, Voter Perception, Voter Understanding, User Study, Online questionnaire

1 Introduction

Elections provide the foundations democracies and fair organizations are build upon. The way in which elections are held vastly differs based on several different factors such as the election format or the type of electorate. One promising way to hold election is remote electronic voting often described as online voting or internet voting. One major advantage of remote electronic voting lies in its promise of improving access to the election and therefore allowing for easier participation in basic democratic processes. Another benefit of remote electronic voting resolves from the comparably lower administrative costs for each cast vote compared to the in-person cast votes [11]. On the other hand, using an online channel for an election also inherits major challenges with regards to security and trustworthiness of the election. Contrary to in-person elections, a potential adversary does not need to have physical access to the ballot as the ballots are stored digitally on the ballot server. Consequently, adversaries could try to access the election server from basically anywhere on the world to breach vote secrecy or manipulate the cast votes or respectively the election result. To counter this, remote electronic voting systems need to implement measures to protect the election infrastructure and guarantee the integrity of the election. One possible approach is to provide voters with so-called individual verifiability, allowing to verify, that their vote was cast as intended, i.e. the vote leaves the voting device in the same way the voter intended. This approach was implemented in the 2023 election of the German association "Gesellschaft für Informatik" (= GI).

In order to examine German voters perception and understanding of this approach we conducted a user study with part of the GI electorate. Using the GI newsletter a call for participation was distributed, to which 23 people responded. Participants needed to answer open questions and multiple choice questions related to their perception of the purpose of individual verifiability using an online questionnaire. The results show, that only half of the participants displayed a general level of understanding but lacked precision in their response.

2 Background & Related Work

2.1 GI Elections

The GI holds yearly elections to elect their presidium and bi-yearly for their board. Since 2004 a secondary online channel in addition to the traditional postal channel was provided. From the voter perspective using this online channel was very similar to the general online shopping experience: voters logged into the system, selected their choice from a list and submitted it. Hence the used system could be described as a black box system, as it is needed to trust the voting system with regards to vote secrecy and integrity. In the 2019 election the GI integrated universal verifiability (= UV), allowing anyone to check whether the votes are tallied as recorded. For this researchers from Karlsruhe Institute of Technology (KIT) and University of Stuttgart developed UV tools that were since then integral part of the GI elections [3, 4].

For the recent 2023 election the GI election board decided to provide individual verifiability (= IV) to their voters, meaning that every voter, that cast their vote online, was able to verify that their vote was cast as intended. To allow for this, three developers ("KIT", "Famoser" & "University Stuttgart") and the voting system provider ("Polyas") developed independent tools to perform IV. The focus of this paper is based on these tools, which we henceforth refer to as "IV tools". In the 2023 election 2785 votes were cast, from which 2759 were cast online [1].

2.2 Individual Verifiability

There are many different definitions for IV. In the course of this paper we interpret it as followed: IV enables the voter to verify that

Mensch und Computer 2024 – Workshopband, Gesellschaft für Informatik e.V., 01.-04. September 2024, Karlsruhe, Germany

https://doi.org/10.18420/muc2024-mci-ws17-151

[1] For details we refer to https://gi.de/wahlen, Last accessed 4.06.24

their vote left the device used for voting in the way they intended it. The following three approaches for IV are most prominent.

The first approach is based on the concept of *audit-or-cast* and is often referred to as the *Benaloh challenge* [5]. In this approach the voter can audit their vote to verify the voting system works correctly. Afterwards, they need to re-vote as auditing leaves the initial vote invalid (for more details we refer to [6]).

The second approach is based on return codes and is currently used in various Swiss cantons for their elections [7]. Here voters receive a so-called code sheet via mail prior to the election. After casting their vote, the voting system generates a confirmation code, which the voter needs to compare to the corresponding code for their choice from the before received code sheet.

The third approach is called *cast-and-audit*. It in particular assumes the usage of secondary device to verify the cast vote. This approach is used in Estonian elections since 2013 [8] and was employed for the 2023 GI election. In the GI election, the voter was supposed to use a secondary device to access an independent IV tool. Once the vote was cast, the main voting application on the primary device displayed a QR code once the voter defined which IV tool to be used (A screenshot of this is attainable in the appendix in Figure 3).

This QR code contains the link to the corresponding IV tool, the voter ID and the randomness r used to encrypt the vote. The IV tool downloads the encrypted vote from the ballot server, checks which vote is encrypted in this ballot by using the randomness r and displays the vote to the voter.

2.3 Related Work

The amount of research on voter perception and understanding of the cast-and-audit approach is limited. There are a few studies that examine the usability and manipulation detection efficacy (e.g. [1, 9, 12–17] but to the best of our knowledge only one study examined voter perception and understanding of the third approach. In their study, researchers conducted semi-structured interviews to examine the understanding and perceived trustworthiness of Estonian i-voters [10]. They found that roughly half of their participants on a general level had a correct understanding of the IV process but no one was able to clearly describe the process or its security guarantees.

3 Methodology

3.1 Recruitment & Data Protection

Recruitment. Participants were recruited using the monthly GI newsletter. In this newsletter a short paragraph explained to the recipients that we are conducting a study to examine the perception and understanding of the newly implemented individual verifiability feature. It was made clear that participation is voluntary, no reimbursement will be awarded and that the results will be published (anonymously) in a scientific venue as well as in future edition of the GI newsletter.

Data Protection. At the beginning of the online survey participants were explained, that the data collected in the survey would only be stored on a server located in Germany and afterwards analysed by this research group. They were additionally told, that the collected data was not personalized and could not be traced back to them. Additionally, at the end of the survey we asked them, if they wanted to submit their answers or not. If they chose not to submit their answers, their recorded data was deleted automatically from the database.

3.2 Research Questions

We are mainly interested in the perception and understanding of IV. The term understanding, at least in our interpretation, encompasses both the general understanding of the functionality of IV as well as against which type of attack IV can protect. Consequently, we formulated the following research questions

RQ1: *How usable do GI voters perceive the newly added individual verifiability tools in the GI election?*

RQ2: *What do GI voters believe what purpose the individual verifiability tools serve in the GI election?*

RQ3: *What do GI voters believe against which type of attacks the individual verifiability tools can protect?*

3.3 Online Questionnaire

Figure 1 gives an overview of the different parts of the online questionnaire.

At the beginning participants were asked, if they detected the possibility of verifying their vote during the election. To aid their memory a screenshot of the final page of the election was displayed. This screenshot contained a brief explanation of the term IV and presented the four available IV tools (A screenshot of this website is displayed in the appendix in Figure 3). Participants responding in the affirmative were further questioned if they used one (or more) of the IV tools and if they abstained, why they chose to do so. Participants that performed IV were asked to select all the tools they used (again we provided screenshots of all of the tools' interfaces to aid memory) and why they chose this/these specific tool(s).

Participants were then asked to describe what they believe was the purpose of the IV tools in their own words. Afterwards they were asked the prior question again, but this time they needed to choose from a selection of multiple choice options. Participants were first asked to explain in their own words how IV tools can protect against different types of attacks, assuming the election observers are honest. Again, after that they were asked to select the correct options from a multiple choice list. Finally, participants were asked to rate IV using the system usability scale (= SUS)[2].

Regarding the multiple choice questions, the phrasing of the question and all of the potential choices were inspired by related work [10], discussed within the research team, including the decision which of the choices were to be categorized as correct and incorrect. All used questions are attainable in the appendix 6.

Lastly, participants were asked if they wanted to submit their prior given answers. If they restrained all their collected was automatically deleted from the database.

[2] SUS asks participants to rate a system or functionality based on ten predefined statements to which they need to express their level of agreement.

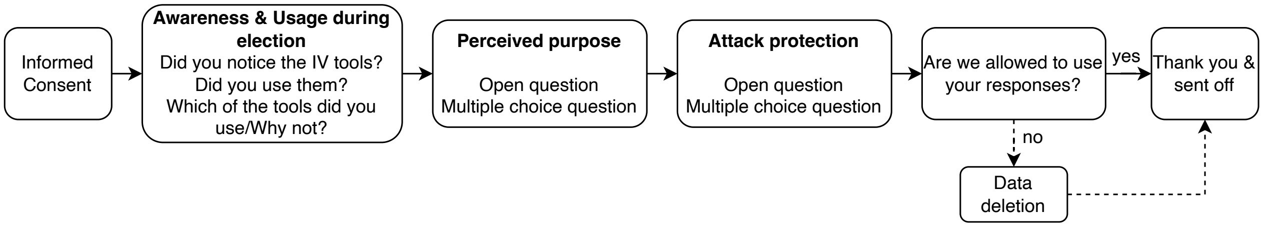


Figure 1: The different parts of the online questionnaire.

3.4 Data Analysis

The analysis of the responses to the two open questions was oriented on an inductive coding approach and done by two members of the research team. All responses were coded by two coders separately, based on a codebook provided by one of the coders after inspecting roughly 30% of the responses. The coded responses were than merged and checked for conflicts. After a short discussion all detected coding conflicts could be solved.

4 Results

4.1 Demographic and General Information

In total 23 participants completed the survey and submitted their answer for analysis. From these 23, 22 noticed during the election that they could perform IV. Three of these participants chose to not perform IV giving the following reasons (translated from German): (1) "I have sufficient trust in the GI", (2) "The election is not important enough to be manipulated" and (3) "If somebody can manipulate the voting system, they could also manipulate the verification tools". 12 participants could no longer remember, which of the tools they used. The ones that could still remember which tool they used were distributed over all four tools (KIT: 3; Famoser; 2; University Stuttgart: 1, Polyas: 1) and reasoned their decision with different explanations why they perceived their choice to be most trustworthy. As we did not collect any personal information, we can not give any details to their background apart from, that probably all of them have some sort of background in computer science (hence their membership with GI).

4.2 Usability of Individual Verifiability

To examine participants perception towards usability of IV we examined the SUS-score. Note, to assess the SUS-score of people that actually used the IV tools we excluded participants that stated, they did not detect that they could use the IV tools during the election and those that chose to not use them ($n = 4$). Overall the SUS scores indicate a "good" usability with a mean score of 75 ($sd = 22.43$) [2].
Fig. 2 gives an overview of the recorded SUS-Scores.

4.3 Purpose of the Individual Verifiabilty Tools

To asses the participants perception of the purpose we analyzed the responses to the respective open question and multiple choice question. We identified the following themes in the responses to the open question (Note, that some participants mentioned several of these themes):

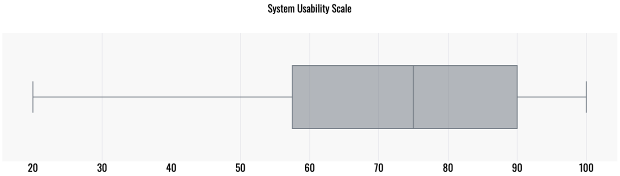


Figure 2: Box-plot of the recorded SUS-Scores.

- **Verify correct vote casting ($n = 7$)** *The purpose of the IV tools were described to verify, that the own vote was cast as intended.*
- **Enhance Trust ($n = 5$)** *Participants expressed that the feature was added to enhance voters' trust into the election.*
- **Verify correct vote counting ($n = 4$)** *The purpose of the IV tools were described to verify, that the own vote would be counted as it was cast.*
- **Manipulation prevention ($n = 3$)** *The participants explained in a very broad manner, that the goal of the IV tools is manipulation prevention.*
- **Error prevention ($n = 2$)** *The participants explained the purpose of the tools to prevent mistakes made by the voter (e.g. a misclick) or the voting system (e.g. transmission error).*
- **Verification by 3rd party ($n = 1$)** *The participant explained the purpose of the tools to be a verification by a third party not involved with the election.*
- **Safety & Security ($n = 1$)** *The participant very broadly stated the purpose to be for safety & security.*

From the 23 participants only seven were able to correctly answer the multiple choice question (see question 4 in the appendix 6).

4.4 Against which Type of Attack can the Individual Verifiability Tools protect?

To asses the participants perception of the IV tools' capabilities in protecting the voter against different types of attacks we analyzed the responses to the respective open question and multiple choice question. We identified the following themes in the responses to the open question (Note, that some participants mentioned several of these themes):

- **MITM = Man in the middle ($n = 10$)** *Participants explained that the usage of the IV tools would protect against a MITM-attack.*

- **Vote manipulation (*n* = 5)** *It was broadly stated, that the IV tools would protect against vote manipulation.*
- **No Idea (*n* = 4)** *Participants stated that they do not know the answer.*
- **Malicious voting device (*n* = 2)** *The participants stated, that the IV tools would help in detecting a malicious voting device potentially changing the vote.*
- **Vote deletion (*n* = 1)** *The purpose was explained to prevent the deletion of votes.*
- **Manipulation by election host (*n* = 1)** *It was explained, that the IV tools protect against a dishonest election host trying to manipulate the election.*

Only two participants were able to select the correct answers to the multiple choice question (see question 6 in the appendix 6), which is that the IV tools can protect the voter against (1) Polyas, (2) the GI, (3) the device used for checking the vote and (4) the device used to cast the vote, under the premise that the second device is honest, manipulating the vote without the voter noticing it.

5 Discussion

5.1 *RQ 1:* Usability

Overall the IV tools were perceived well and attributed a good usability as described in Sec. 4.2. In terms of measured usability the IV tools, that were in place for the GI elections achieved similar SUS scores as comparable to recent user studies also examining IV tools with a second device [9]. For example the study conducted by Hilt et. al [9] recorded a mean SUS score of 79 and the study by Marky et. al [14] a mean score of 85.

5.2 *RQ 2:* Purpose

Overall participants mentioned the idea that IV allows them to check their vote, but their responses did not hint at a complete understanding, indicated by their answers referring to verifying one's vote or describing it to be some sort of manipulation prevention. Less than a third of participants being able to describe the primary purpose was surprising, as we expected an electorate with interest in computer science (hence their membership in GI) to have a clearer understanding. On this regard it is important to mention, that many of the given explanations for the primary purpose of the IV tools were not necessarily wrong, but they remained too vague or incomplete to be classified as correct. As an example: five participants described to purpose of the tools to be enhancing trust in the election and one stated that they are for security and safety. While this is ultimately correct the answer lacked explanation and context, as the primary purpose of the tools is to allow the voter to verify that their vote was cast as intended. which can enhance trust in the election.

Another point that is important to briefly discuss is the fact, that the IV tools could also be used for a secondary purpose: After verifying one's vote, it was possible to download a so-called receipt of the ballot. This receipt could then be sent to the election organizer for them to perform universal verification using the tools introduced in the 2019 election [3, 4], to make sure that all ballots in the tally are valid. Hence the tools served a function in providing the receipts for universal verification but ultimately did not perform universal verification on their own, as this process was manually done by the election board. Consequently, the participants stating that the tools verify that the vote was count as cast, were not directly incorrect (as the tools played their part in this process), but again lacked precision. Interesting to highlight on this note is, that the GI introduced universal verifiability in 2019, at which time no tools for individual verifiability were available. Therefore participants could have known that the process of universal verifiability was already present in prior elections and is therefore to be separated from the IV tools. Ultimately the inaccuracy displayed in participants responses towards the purpose is understandable, as from a voters point of view the separation between UV and IV wrt. to the IV tools was not distinct.

5.3 *RQ 3:* Attack Protection

The lack of concrete understanding related to IV becomes more apparent when inspecting the responses to the questions related to potential attacks the IV tools can protect against. Only two participants were able to precisely state against which type of attack the IV tools protect (both in response to the open question as well as the multiple choice question): a malicious voting device. Similar to the prior topic of the purpose of the IV tools, five participants remained vague and described that the tools could help with manipulation prevention. The vast majority had the wrong impression or no idea at all, against which type of attack the IV tools can protect the voter.
Notably, ten participants stated that the IV tools would protect against a MITM attack which is not necessarily true: under the assumption that an attacker would be able to interfere during the transmission from the voting device to the election server it would also be possible for them to hijack the transmission from the second device accessing the election server to perform IV.

Compared to findings from a study conducted in Estonia the level of understanding is lower, which can be explained due to the fact, that Estonians use e-voting with a similar form of IV since 2013 [10]. Nonetheless, it is still remarkable, that even among an electorate with a background in computer science, the principles of the voting system in place seem to be not clear. This issue could potentially be addressed by providing more detailed information about the e-voting system in place by the election organizers. On the other hand, it remains uncertain, if the electorate would be even willing to engage with more extensive material, especially in the case of a low-stake election. Consequently, future research needs to examine how voters can be educated better about IV.

To summarize it can be noted, that the majority of participants had a general idea, that IV allows them to check their vote but less than a third of participants were able to clearly describe the purpose. The understanding of IV capabilities against attacks was clearly insufficient.

5.4 Limitations

The amount of participants and their background in computer science does not allow for generalization into the wider public. Nonetheless, as it was the first time IV was available for this election the findings are still interesting. The analysis of qualitative data is inherently interpretive as the researchers potentially could have introduced subjectivity to the findings. In order to minimize this the data was coded independently by two researchers.

6 Conclusion

We conducted an online user study with part of the electorate of GI. The objective of this user study was to examine the perception and understanding of voters wrt. to IV. Half of the participants displayed had a general idea, that IV allows them to check their vote, but were unable to precisely state the purpose of the IV tools. Moreover, when questioned about against which type of attack the IV tools can protect the voters, only two of 23 participants were able to give a precise and correct answer. These findings hint at an incomplete understanding of the purpose and functionality of the IV tools and raises the question, how this understanding can be improved.

References

[1] Claudia Z Acemyan, Philip Kortum, Michael D Byrne, and Dan S Wallach. 2014. 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 (2014), 26–56.

[2] Aaron Bangor, Philip T. Kortum, and James T. Miller. 2009. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies* 4, 3 (2009), 114–123. Publisher: Citeseer.

[3] Bernhard Beckert, Achim Brelle, Rüdiger Grimm, Nicolas Huber, Michael Kirsten, Ralf Küsters, Jörn Müller-Quade, Maximilian Noppel, Kai Reinhard, Jonas Schwab, Rebecca Schwerdt, Tomasz Truderung, Melanie Volkamer, and Cornelia Winter. 2019. GI Elections with POLYAS: a Road to End-to-End Verifiable Elections. In *Fourth International Joint Conference on Electronic Voting (E-Vote-ID 2019), 1-4 October 2019, Lochau / Bregenz, Austria - Proceedings. Ed.: M. Volkamer; B. Beckert.* Gesellschaft für Informatik (GI), Bregenz, 293–294.

[4] Bernhard Beckert, Jurlind Budurushi, Armin Grunwald, Robert Krimmer, Oksana Kulyk, Ralf Küsters, Andreas Mayer, Jörn Müller-Quade, Stephan Neumann, and Melanie Volkamer. 2021. *Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen.* Technical Report. Karlsruhe Institute of Technology (KIT). https://publikationen.bibliothek.kit.edu/1000137300

[5] Josh Benaloh. 1987. *Verifiable Secret-Ballot Elections.* Ph. D. Dissertation. Yale University. https://www.microsoft.com/en-us/research/publication/verifiable-secret-ballot-elections

[6] Josh Benaloh. 2006. Simple verifiable elections. In *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop* (Vancouver, B.C., Canada) *(EVT'06)*. USENIX Association, USA, 5.

[7] David Galindo, Sandra Guasch, and Jordi Puiggalí. 2015. 2015 Neuchâtel's Cast-as-Intended Verification Mechanism. In *E-Voting and Identity*, Rolf Haenni, Reto E. Koenig, and Douglas Wikström (Eds.). Springer International Publishing, Cham, 3–18.

[8] Sven Heiberg, Peeter Laud, and Jan Willemson. 2012. The Application of I-Voting for Estonian Parliamentary Elections of 2011. In *E-Voting and Identity*, Aggelos Kiayias and Helger Lipmaa (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 208–223.

[9] Tobias Hilt, Benjamin Berens, Tomasz Truderung, Margarita Udovychenko, Stephan Neumann, and Melanie Volkamer. 2024. Systematic User Evaluation of a Second Device based cast-as-intended verifiability Approach. In *Voting'24.* Springer, Cham. 46.23.01; LK 01.

[10] Tobias Hilt, Kati Sein, Tanel Mällo, Jan Willemson, and Melanie Volkamer. 2023. Voter Perception of Cast-as-Intended Verifiality in the Estonian I-Vote Protocol. In *E-Vote-ID 2023 (Lecture Notes in Informatics - Proceedings).* Gesellschaft für Informatik (GI), Bonn. 46.23.01; LK 01.

[11] Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Priit Vinkel, and Arne Koitmae. 2018. How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. In *Electronic Voting*, Robert Krimmer, Melanie Volkamer, Véronique Cortier, Rajeev Goré, Manik Hapsara, Uwe Serdült, and David Duenas-Cid (Eds.). Springer International Publishing, Cham, 117–131. https://doi.org/10.1007/978-3-030-00419-4_8

[12] Oksana Kulyk, Jan Henzel, Karen Renaud, and Melanie Volkamer. 2019. Comparing "Challenge-Based" and "Code-Based" Internet Voting Verification Implementations. In *Human-Computer Interaction – INTERACT 2019*, David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris (Eds.). Springer International Publishing, Cham, 519–538.

[13] Oksana Kulyk, Jonas Ludwig, Melanie Volkamer, Reto E. Koenig, and Philipp Locher. 2021. Usable Verifiable Secrecy-Preserving E-Voting. In *6th Joint International Conference on Electronic Voting, E-Vote-ID 2021, 5-8 October 2021. Ed.: R. Krimmer ; M. Volkamer.* University of Tartu Press, Tartu, 337 – 353. 46.23.01; LK 01.

[14] Karola Marky, Oksana Kulyk, and Melanie Volkamer. 2018. Comparative Usability Evaluation of Cast-as-Intended Verification Approaches in Internet Voting. In *SICHERHEIT 2018.* Gesellschaft für Informatik e.V., Bonn, 197–208. https://doi.org/10.18420/sicherheit2018_15

[15] Karola Marky, Verena Zimmermann, Markus Funk, Jörg Daubert, Kira Bleck, and Max Mühlhäuser. 2020. Improving the Usability and UX of the Swiss Internet Voting Interface. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20).* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376769

[16] Karola Marky, Marie-Laure Zollinger, Peter Roenne, Peter Y. A. Ryan, Tim Grube, and Kai Kunze. 2021. Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes. *ACM Trans. Comput.-Hum. Interact.* 28, 5, Article 30 (sep 2021), 36 pages. https://doi.org/10.1145/3459604

[17] Stephan Neumann, M. Maina Olembo, Karen Renaud, and Melanie Volkamer. 2014. Helios Verification: To Alleviate, or to Nominate: Is That the Question, or Shall we Have Both?. In *Electronic Government and the Information Systems Perspective*, Andrea Kő and Enrico Francesconi (Eds.). Springer International Publishing, Cham, 246–260.

Acknowledgments

This work was funded by the Topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and supported by KASTEL Security Research Labs, Karlsruhe.

A Appendix

A.1 Questions from the Online Questionnaire

In the following we present the questions asked in the online questionnaire (translated from German).

Question 1: Did you notice, that you could verify the correctness of your cast vote, i.e. perform individual verifiability?

- Yes
- No
- I don't remember

Question 2: Did you verify your vote?

- Yes
- No
- I don't remember

Question 3 (Understanding purpose): Please describe in your own words, what the purpose of this new added functionality is.

Question 4 (Understanding purpose): Additionally to the prior open question, we want to raise this question again but will provide you some response possibilities. Please select the response that you deem correct (multiple selection possible).
The new functionality was introduced, to allow me to check that ...

(1) ... all votes arrive in the digital ballot box as intended.
(2) ... my vote arrives in the digital ballot box as intended.
(3) ... all votes remain unchanged in the digital ballot box, as they were cast.
(4) ... my vote remains unchanged in the digital ballot box, as it was cast.
(5) ... all votes are tallied correct.
(6) ... my vote is tallied correct.

(7) None of the responses is correct.

Note: Response 2 is correct.

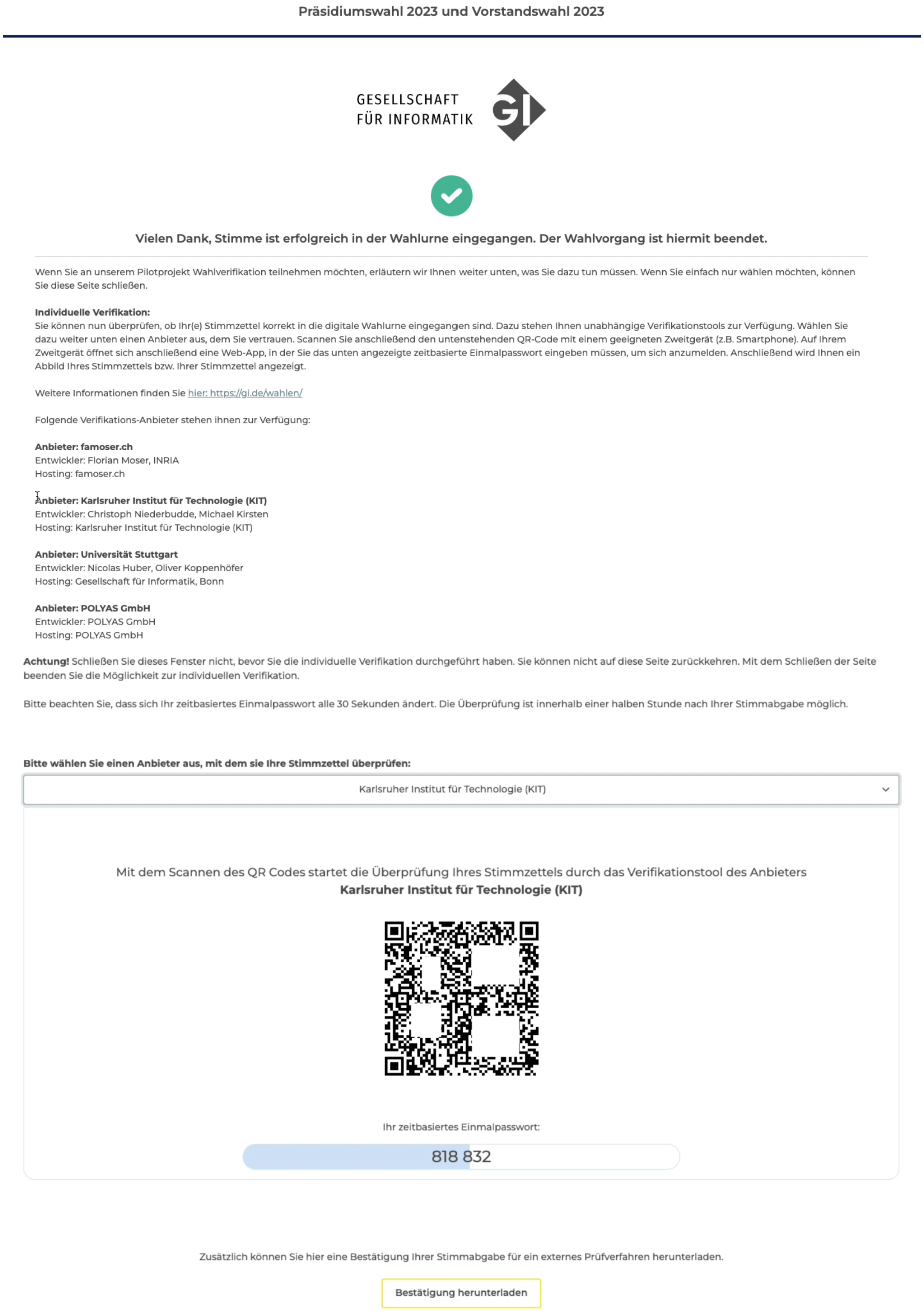
Question 5 (Understanding attack protection): Please describe in your own words, against which type of attack this functionality can protect.

Question 6 (Understanding attack protection): Please select all correct statements (multiple selection possible).
If I as a voter use the new functionality and under the premise that the election observer controlling the tally and the existence of all votes are trustworthy, it is ...

(1) ... not possible for Polyas to manipulate my vote unnoticed.
(2) ... not possible for the device used to cast my vote to manipulate my vote unnoticed, under the premise, that the second device used the check the vote is not manipulated as well.
(3) ... not possible for the GI to manipulate my vote unnoticed.
(4) ... not possible for the device used to cast my vote to manipulate my vote unnoticed.
(5) ... not possible for the device used to check my vote to manipulate my vote.
(6) ... None of the responses is correct.

Note: Responses 1, 2, 3 & 5 are correct.

A.2 Screenshots from the Voting System



Präsidiumswahl 2023 und Vorstandswahl 2023

GESELLSCHAFT FÜR INFORMATIK

✓

Vielen Dank, Stimme ist erfolgreich in der Wahlurne eingegangen. Der Wahlvorgang ist hiermit beendet.

Wenn Sie an unserem Pilotprojekt Wahlverifikation teilnehmen möchten, erläutern wir Ihnen weiter unten, was Sie dazu tun müssen. Wenn Sie einfach nur wählen möchten, können Sie diese Seite schließen.

Individuelle Verifikation:
Sie können nun überprüfen, ob Ihr(e) Stimmzettel korrekt in die digitale Wahlurne eingegangen sind. Dazu stehen Ihnen unabhängige Verifikationstools zur Verfügung. Wählen Sie dazu weiter unten einen Anbieter aus, dem Sie vertrauen. Scannen Sie anschließend den untenstehenden QR-Code mit einem geeigneten Zweitgerät (z.B. Smartphone). Auf Ihrem Zweitgerät öffnet sich anschließend eine Web-App, in der Sie das unten angezeigte zeitbasierte Einmalpasswort eingeben müssen, um sich anzumelden. Anschließend wird Ihnen ein Abbild Ihres Stimmzettels bzw. Ihrer Stimmzettel angezeigt.

Weitere Informationen finden Sie hier: https://gi.de/wahlen/

Folgende Verifikations-Anbieter stehen ihnen zur Verfügung:

Anbieter: famoser.ch
Entwickler: Florian Moser, INRIA
Hosting: famoser.ch

Anbieter: Karlsruher Institut für Technologie (KIT)
Entwickler: Christoph Niederbudde, Michael Kirsten
Hosting: Karlsruher Institut für Technologie (KIT)

Anbieter: Universität Stuttgart
Entwickler: Nicolas Huber, Oliver Koppenhöfer
Hosting: Gesellschaft für Informatik, Bonn

Anbieter: POLYAS GmbH
Entwickler: POLYAS GmbH
Hosting: POLYAS GmbH

Achtung! Schließen Sie dieses Fenster nicht, bevor Sie die individuelle Verifikation durchgeführt haben. Sie können nicht auf diese Seite zurückkehren. Mit dem Schließen der Seite beenden Sie die Möglichkeit zur individuellen Verifikation.

Bitte beachten Sie, dass sich Ihr zeitbasiertes Einmalpasswort alle 30 Sekunden ändert. Die Überprüfung ist innerhalb einer halben Stunde nach Ihrer Stimmabgabe möglich.

Bitte wählen Sie einen Anbieter aus, mit dem sie Ihre Stimmzettel überprüfen:

Karlsruher Institut für Technologie (KIT)

Mit dem Scannen des QR Codes startet die Überprüfung Ihres Stimmzettels durch das Verifikationstool des Anbieters
Karlsruher Institut für Technologie (KIT)

Ihr zeitbasiertes Einmalpasswort:

818 832

Zusätzlich können Sie hier eine Bestätigung Ihrer Stimmabgabe für ein externes Prüfverfahren herunterladen.

Bestätigung herunterladen

Figure 3: Final page of the voting system that allowed the selection of the IV tools, with KIT IV tool being selected.