Partial Verifiability in POLYAS for the GI Elections

M. Maina Olembo[1], Anna Kahlert[2], Stephan Neumann[1], and Melanie Volkamer[1]

[1]Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
Hochschulstraße 10
D-64289 Darmstadt
{firstname.lastname}@cased.de

[2]Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Pfannkuchstraße 1
D-34121 Kassel
a.kahlert@uni-kassel.de

Abstract: We discuss the use of POLYAS, an Internet voting system, in GI (German Society for Computer Scientists (Gesellschaft für Informatik e.V.)) elections before 2010, in 2010 and 2011, as well as in the future. We briefly describe how the system was extended in 2010 to provide partial verifiability and how the integrity of the GI election result was verified in the 2010 and 2011 elections. Information necessary for partial verifiability has so far only been made available to a small group of researchers. In the future it would be ideal to make such information available to the general public, or to GI members, in order to increase the level of verifiability. We highlight legal considerations accompanying these possibilities, including publishing more details about the election results, the requirement for secret elections, avoiding vote buying, and how to handle complaints. Motivated by legal constraints, we propose further improvements to the POLYAS system. Finally, we generalize our findings for any partially-verifiable Internet voting system.

1 Introduction

Internet voting systems for legally binding elections have predominantly been black-box systems, e.g., Estonia's federal elections [MM06] and the elections for the Austrian Federation of Students [KET10]. One needs to trust that these systems work as they should, which is not ideal for elections. The GI – German Society for Computer Scientists (Gesellschaft für Informatik e.V.) - has also used such a black-box Internet voting system, POLYAS, to conduct its elections since 2004. In 2010, modifications were proposed to introduce partial verifiability in POLYAS [OSV11]. While partial verifiability may not be considered optimal, the assurance it offers to voters is likely to increase their trust in election results. However, only a small group of researchers has been able to verify the processes for the GI elections in 2010 and 2011. Obviously, there is a need to

make partial verifiability available to the general public or at least to GI members. However, public verifiability requires publishing information that was previously kept secret. We address this from a legal point of view and provide recommendations for future GI elections.

Furthermore, we identify a flaw in [OSV11] that allows an attacker to coerce voters as a result of publishing information needed to partially verify the election process. We propose a technical improvement that significantly mitigates the risk of the outlined attack. While the addressed issues with respect to partial verifiability can be overcome by technical means, the handling of complaints remains an open problem. We therefore recommend partially implementing the proposal of [OSV11] for future GI elections. Our findings regarding the handling of complaints are generalized for any partially verifiable voting system.

In section 2 of this paper, we provide background information on the POLYAS voting system and its use in the GI 2010 and 2011 elections. Section 3 looks at challenges arising from making partial verifiability publicly available by publishing details of the election results. In section 4, we discuss the risk of vote selling, which is likely to occur when the general public can verify the processes as researchers did for the 2010 and 2011 elections. Section 5 focuses on our proposal addressing the publishing of hash chain information for the purpose of integrity with respect to the risk of coercion. Section 6 analyzes complaint handling, and we conclude in section 7 with a statement on these challenges and present future work.

2 Background

First, we provide our definitions for verifiability and then review the POLYAS system, discussing how partial verifiability is provided, and finally look at the application of partial verifiability in the GI 2010 and 2011 elections.

2.1 Verifiability

Verifiability can be categorized as *universal verifiability* and *individual verifiability*. We use the definitions given by [OSV11]. Individual verifiability focuses on the voter and enables him to verify that his vote has been properly prepared and sent to the voting server (cast as intended) as well as stored, unaltered, in the ballot box (stored as cast). Universal verifiability enables any interested party to verify the proper tallying of all votes stored in the ballot box.

2.2 The POLYAS Voting System

The various components of POLYAS are discussed in this section. We look at the protocol that runs during the voting phase including one special mechanism, the hash chain mechanism, and the post-voting phase of the protocol.

Components: POLYAS is made up of the electoral registry server (*ERS*), the validation server (*VS*), and the ballot box server (*BBS*). An off-line tallying component (*TC*) is used to tally votes (loaded in an encrypted state from *BBS*). A discussion on how these components work is presented in [RJ07] and [MR10]. In a GI election set-up, the *ERS* is administered by the GI at a computing center, while all other components are located at Micromata.

Voting Phase: A voter authenticates him- or herself at the election website using a personal voter ID and voting TAN (received via postal mail). These credentials are verified by the *ERS,* which forwards the TAN to the *VS.* The *VS* checks its database for this particular TAN and generates a random voting token (VT) if the TAN is valid and no VT has previously been generated for this voter. The *VS* then sends the voting token to the *BBS* and *ERS.* The *ERS* forwards the token back to the voter. The voter receives a ballot from the *BBS* and proceeds to mark the ballot for the desired candidates. This selection, along with the token VT, is sent to the *BBS* and the selection is stored for the final tallying only once the voter confirms his or her vote. The *BBS* informs the *ERS* that the voter corresponding to a particular VT has cast a vote. Then, the *ERS* and *BBS* delete the copy of the VT in order to maintain voter secrecy, and the *ERS* invalidates the voter ID to prevent double voting. The voter then receives confirmation of a successfully cast vote.

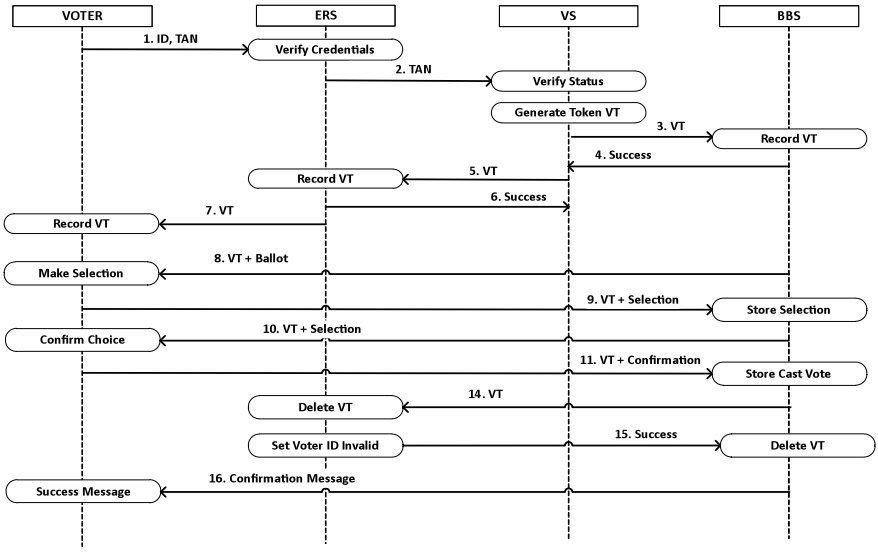

Fig. 1: A simplified view of the voting phase in POLYAS

Hash Chain: POLYAS uses a hash chain mechanism during the voting phase to enable integrity checks. Votes are encrypted once they are received, confirmed by the voter, and then stored in a randomized order in *BBS* in blocks of 30[1]. After receiving the first 30 votes, the *BBS* concatenates the encrypted votes, attaches an initial hash value in the first round, computes the hash using SHA-256, and signs the output using its private signature key. The output of the hash function and the signed version are sent to the *ERS* for storage. An acknowledgement message is sent back to the *BBS*. The next block of 30 votes is attached to this hashed output and SHA-256 is applied once again. This process is repeated for all available votes. If the last block of votes contains less than 30 votes, they are not included in the hash chain.

Post-voting Phase: At the end of the voting period, all encrypted votes are downloaded from the *BBS* and uploaded to the *TC*. The decryption key is input into the *TC* and all votes are decrypted and tallied.

This describes the original version of POLYAS, which does not provide any verifiability.

2.3 Partial Verifiability in POLYAS

A concept to enable partial verifiability in POLYAS was proposed in [OSV11]. A verifiability tool was developed and applied during the GI's 2010 elections and later extended to the GI's 2011 elections. The tool provides *universal verifiability* by taking the encrypted votes from the *BBS* and the decryption key as inputs, decrypting all the votes, and tallying them. The decryption key can be provided without violating secrecy of the vote, because there is no link between the encrypted vote and the corresponding voter. Assuming that the election results are published, the result obtained from the verifiability tool is compared to the result announced by the *TC*. This tool also facilitates partial *individual verifiability* through use of the hash chain. The encrypted votes and the initial hash value are required as inputs. The tool generates the hash chain information and compares the values obtained to those stored on the *ERS*. If there is any discrepancy, then manipulation can be detected. In this way, one can verify that after the hash value of a block is computed and sent to the *ERS*, votes in this corresponding block cannot be altered in the ballot box without detection, under the assumption that both the *ERS* and *BBS* do not collaborate. However, it must be noted that if a malicious *BBS* alters votes before they are stored in the ballot box and before the hash value is computed, then this would not be detected. Besides the verifiability tool, [OSV11] proposed that the *html* code be checked to verify that the vote has been cast as intended. Even with these extensions, POLYAS provides only partial verifiability as the process from receiving the vote and computing the corresponding hash value currently cannot be verified.

[1] The number of votes in a block is variable. The GI opted for 30 votes.

2.4 Application of the Verifiability Tool in the GI's 2010 and 2011 Elections

The GI holds elections once every year. In 2010, the election had a single race for the management board. There were nine eligible candidates and three positions to be filled. 3,193 voters participated via Internet voting and 51 voters by postal [2] voting. In 2011, the election had two races - for the presiding council and the management board. A voter could cast a "yes" or "no" vote for each candidate in the presiding council race and three votes in the management board race. In the 2011 election, 3,244 voters participated via Internet voting and 45 voters by postal voting.

The verifiability tool was used in the 2010 elections. After its extension to be used for two races, it was used for the 2011 elections. Both elections were successfully verified. For both of these elections, the GI opted not to make the information required to verify the election result publicly available. The interface specification which allowed implementation of the verifiability tool was only provided to researchers. Access to this information and the election data necessary to carry out verifiability required signing a non-disclosure agreement regarding the data provided and proprietary information on POLYAS.

In terms of verifiability, it would be ideal if this information was made available to all GI members or even to the general public. In addition, more information should be made available to further increase the level of verifiability. In the following sections, we discuss the legal and technical considerations for these extensions.

3 Publishing Complete Election Results

One consequence of enabling every GI member to verify his or her vote as described in section 2.4 is that voters could compute the number of selections per candidate, including the number of selections from Internet voters and those using the postal channel. This is possible because of the information available for verifiability and the published total result.

Until now, the GI only published the winning candidate's votes, preferring not to disclose the number of votes received by candidates who were not elected. Internet votes and postal votes are also not distinguished. In this section, we first consider legal requirements for publishing these details regarding the election results and discuss which body bears the responsibility of deciding whether to publish them or not.

[2] In this paper, postal voting also refers to voting by mail.

3.1 Is There a Legal Requirement to Publish Complete and Detailed Election Results?

In March 2009, the Federal Constitutional Court ruled that the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law - Grundgesetz - GG) requires that all essential steps in elections be subject to public examinability, unless other constitutional interests justify an exception [BVerG09]. Particular significance is attached here to the monitoring of the election act and to the ascertainment of the election result [BVerfG09].

However, private associations vested with legal capacity, like the GI, are allowed to regulate their elections and acclamations on their own [RGO09]. This is a result of the autonomy of association, a part of the constitutional principle of freedom of association (Article 9.1 GG) [El12]. As such, the association is free to regulate and formulate its affairs within the mandatory rules [Fl08]. This is regulated by law in § 25 of the Civil Code (Bürgerliches Gesetzbuch – BGB). § 40 BGB contains the right of the association to regulate their matters in articles of association according to their purposes [SSW10]. Therefore, the electoral principles (Article 38.1 in conjunction with Article 20.1 and 20.2 GG), which have to be observed at parliamentary elections, do not apply to associations' elections to the same degree, but the principles should fit with the autonomy of association [RGO09].

In matters associated with the proceedings of the GI elections, the autonomy of association of Article 9 GG is decisive. The legal arrangement of the electoral proceedings is delivered to the members of the association and can be specified by creating articles of association and subordinate electoral order in private autonomy [RGO09]. The GI availed itself of this opportunity by permitting electronic elections in § 3.5.4 of the articles of association and regulating particulars by implementing the Election Order (Ordnung der Wahlen und Abstimmungen - OWA) provision. Although § 3.5.4 of the OWA regulates the publication of the results, there are no rules about publishing the vote allocation, providing a listing of the results, and differentiating between postal votes and Internet votes.

Generally the elections of the management board and the presiding council are resolutions of the meeting of members according to § 32 BGB. However, the proclamation of a resolution of the meeting of members is not mandatory for the validity of a resolution [BGH75] [SSW10]. Even though it is stated in the articles of association that the organizer of the meeting of members, who is the returning officer, has to proclaim the resolutions of the meeting of members, this is generally considered just a regulatory action [SSW10].
As a result, an association, and in particular the GI, is neither compelled to publish detailed information about the election nor to distinguish between specific forms of elections when publishing the results; however, it is not forbidden. The remaining question therefore is to determine who can decide on publishing the election results. This is discussed in the following subsection.

3.2 Which GI Body is Allowed to Decide on Publishing Election Results?

The management board named in § 7.2 of the articles of association is the management board in terms of § 26 BGB and therefore the legal representative of the GI. This body is responsible for all of the GI's affairs that are not assigned to other bodies by the articles of association. The duties and authorities of the presiding council are mentioned in § 8.6 of the articles of association, including the decree about the implementing provisions like the OWA.

Since there is no regulation for publishing results, the GI could explain in the OWA to which extent election results are released to the public. The presiding council is responsible for modifying the OWA. Otherwise the management board is authorized to decide on the scale of the publication of electoral results because of the authority mentioned in § 7.2 of the articles of association. One could also decide to only provide access to GI members by publishing the results in the internal area of the GI web page.

4 Secret Elections and the Risk of Vote Selling

As it is generally possible to publish all relevant information for verifiability, in this section, we analyze whether the publication of the information required to verify future elections violates the secrecy of the vote.

4.1 Problem Description

In the GI elections, voters have multiple votes to cast and two races are held in parallel every second year. The risk of vote selling arises with such types of elections through the signature attack (also known as the "Italian attack"). In such an attack, a coercer [3] asks the voter to vote in an identifiable way for his preferred candidate. The voter would select the particular candidate and use the remaining votes to form a "signature" with his vote. Since the information to verify also enables a coercer to deduce all individual votes, he can confirm compliance with his instructions by searching through all the votes for the voter's "signature."

For the 2011 GI elections, given how POLYAS stores cast votes, there were 5,632 different possibilities to cast a vote.[4] This number of possibilities is obtained as follows: POLYAS stores the votes in the two ballots such that they can be linked to each other. The presiding council race had five candidates (a maximum of three could be selected), and another four candidates were available for the management board (for each candidate a "Yes" or "No" vote could be cast). An option for an invalid vote is provided on each ballot. POLYAS stores exactly what the voter selected, i.e., if in the first race the voter selected four candidates and the invalid option then this information was stored

[3] Coercer also refers to vote buyer.
[4] Note, only 3,244 votes were cast electronically.

exactly as selected. In the best case scenario, the coercer would ask a voter to vote for candidate *A* and create a signature along with this valid vote. The voter would then still have up to two selections to make out of four remaining candidates in the first race. In the second race, the voter votes either "Yes" or "No" for each option and whether or not to select the invalid option since the second vote can also be invalidated. This does not influence the first race and the vote for candidate *A*. The total number of possibilities for a unique signature is given by the equation below:

$$\#\,sig = \sum_{i=0}^{2}\binom{4}{i} \cdot \sum_{i=0}^{9}\binom{9}{i} = 5.632$$

In other words, 11 signatures from the first ballot times 512 signatures from the second ballot, with two being the maximum number of votes that remain in the first race for the voter to choose from, four is the total number of candidates the voter can now choose from in the first race, and nine is the number of vote options available in race two. Note, this attack was also possible with the postal voting approach used by the GI before Internet voting was introduced, when both votes were put in one envelope. GI members who were part of the tallying process and physically present at the GI headquarters in Bonn could search through all the votes to identify those which had the required signatures. As publishing the information to verify makes the data required for this attack more easily accessible, this attack would become much more attractive.

Similar to the discussion regarding publishing results, clarification is first needed on whether the GI's regulations require secret elections (this is not the case for all societies because members can also agree to non-secret elections).

4.2 Do GI Regulations Dictate Secret Elections?

Since associations are autonomous, they are allowed to form their own voting procedures as stated in Article 9.1 GG. The requirements for secret elections for associations differ from those for the elections of the Lower House of the German Federal Parliament (Bundestag) in virtue of Article 38.1 sentence 1 GG. If, however, an association opts for secret elections, the secrecy of individual voting decisions must be guaranteed [RGO09].

The GI Requirements for Internet-based Association Elections (*GI-Anforderungen an Internetbasierte Vereinswahlen*) [GI05], was adopted to the articles of association developed by a working committee of the GI's chairmanship. It declares that the secrecy of elections has to be ensured by mathematical methods and concepts of anonymity. This indicates that the principle of secrecy of elections is upheld by the GI and thus must be considered an election requirement.

According to the principle of the secrecy of elections under article 38.1, sentence 1, GG prescribes that the election procedure has to be carried out in such a way that the decision of the voter remains unknown [Sc09]. At the same time the secrecy of elections defends the freedom of election [Mo06]. The voter is protected from coercion and the candidate is safe from the postulations of 'his' voters.

Therefore, since the GI requires secret elections, the risk of vote selling based on the aforementioned signature attack is a problem for which a solution must be sought before making the verifiability information (as used in the elections in 2010 and 2011) publicly available.

4.3 Technical Solution Proposal

To mitigate the risk of the signature attack, we propose that the ballot be split into two ballots, one for each race, and stored in such a way that they can no longer be linked to each other. The number of possible signatures would be greatly reduced in the same scenario for the 2011 election in contrast to the scenario discussed above. There would only be 11 available signatures in the first race if the voter was coerced or sold his vote for candidate *A*. Note that in this approach, the second race cannot be used to create a signature as both votes will be stored independently and in such a way that they cannot be linked to each other. In the case where an adversary forces the voter to vote for candidate B in the second race, the coercer would only have twenty-seven possibilities to create signatures for valid votes:

$$\#\,sig = \sum_{i=0}^{3} \binom{3}{i} \cdot 2^i = 27$$

i.e., the voter can now choose up to three remaining candidates with a yes, no, or blank vote, thus there are three options. With this proposal, the adversary's number of possible signatures decreases significantly to 11 in the first race and 27 in the second race.

Another case, though not very attractive, is where the adversary forces the voter to cast an invalid vote (or buys an invalid vote). The number of possibilities to cast a vote for the second race [5] corresponds to 512, from which there are 431 invalid votes. To further improve the situation for this specific attack we propose that invalid votes are stored with no further information about the selected candidates, that is, there is no need to store further information from the ballot other than that the voter made an invalid vote selection. This proposal reduces the number of possibilities the adversary has available to demand invalid votes to one, thus the attack is no longer possible.

From a legal point of view, these technical solutions are an improvement as secret elections are further ensured. It remains to be seen if it is sufficient in the case of a judicial review.

[5] We focus on the second race as the problem is more obvious in this race.

5 Publishing Hash Chain Information

In the 2010 and 2011 elections, the hash chain information, which was stored on the *ERS,* was only provided at the end of the election. Thus, one needed to trust that the *ERS* and *BBS* did not collaborate to modify the ballot box (*BBS*) and the hash chain (*ERS*) accordingly. However, it would improve the level of verifiability if the hash chain information would be provided on a real-time basis on a public web page (*Bulletin Board - BB*), even if only accessible by GI members in the internal GI portal[6]. In this way, the members would be able to verify that no votes were modified after being included in the hash chain. As such, the assumption that the *ERS* and *BBS* do not collaborate would no longer hold because a modification of the database with the encrypted votes and the corresponding hash values would be detected as these values would not match with those on the BB. However, the idea of publishing this information immediately also has a drawback, which is discussed in the following subsection.

5.1 Problem Description

One drawback to providing the hash chain information on a real-time basis is the fact that a voter would know in which block his or her vote is stored as the voter could visit the BB before casting a vote, for example, for candidate *A*, and then observe that currently *x* hash values are published. He would then be able to tell a coercer that he voted for candidate *A* (as demanded by the coercer) and that his vote was stored in block *x+1*. The coercer would decrypt the votes at the end of the election and check on the votes in this specific block to verify the statement (again this is possible due to the verifiability discussed in sections 2.3 and 2.4).

In this scenario, a coercer only has to access the 30 votes in a given block while there would be 11 possibilities to cast a vote in the first race and 27 for the second race in total. Thus, the signature attack would again become more attractive if the hash chains are already being published during the election.

From a legal perspective, this is not acceptable in order to preserve secret elections. Therefore, we discuss possible improvements in the following subsection.

5.2 Technical Solution Proposals

To avoid disclosing this information, publishing the hash chain information could be delayed. A voter would then not know exactly which block contained his or her vote as several would be released simultaneously. However, this would decrease the level of verifiability because it provides a larger time frame within which votes could be manipulated without detection.

[6] This fact depends on the decision of section 3.2.

A second proposal is to split the ballot further, distributing the individual votes across the ballot box database and the hash chain. Rather than storing the votes from an individual voter together in the database and hash chain, these individual votes for specific candidates are randomly distributed and stored. Thus, individual ballots cannot be reconstructed from the database and the hash chain, however, it would still be possible to tally the votes per candidate and to verify, at the end of the election, that votes in the ballot box have not been changed after the hash chain was computed. A voter knowing which block his vote is stored in has nearly no knowledge that can be used by a coercer, and is thus prevented from selling his vote or being coerced.

Note, this also means that the honest voter who has not been coerced has less information. If he wants to verify whether his vote is in the corresponding block at the end of the election, he would not be able to reconstruct his vote. However, this is acceptable since the hash chain is used to detect manipulation in the database after the hash values are published, which was the main motivation for introducing hash chains. This possibility remains unaffected.

The measures of protection discussed in this section above are taken to avoid disclosing potentially sensitive information. As such, publishing hash chain information without delay but modifying how information is stored is acceptable from a legal point of view with respect to the secrecy of the election.

6 Complaints

Other than secrecy requirements for the election, there is a second challenge with respect to publishing hash chain information during the election, that is, how to handle complaints regarding the verifiable information.

6.1 Problem Description

A voter may check for the block number before casting his or her vote, and then complain that his or her vote was not included in that particular block, e.g., he selected candidate *A* while none of the votes in this block contains a vote for candidate *A*. Note, even though the voter does not know which is his vote, he can deduce that none of the votes contained the selection of candidate *A*. This situation is particularly difficult to handle as valid and invalid complaints cannot be distinguished. A dishonest voter may also attempt to make a falsified complaint, e.g., by selecting a block where no vote for candidate *A* is included and claiming that his vote is missing. Therefore, an approach is needed to handle complaints in order to allow immediate publication of the hash chain information. We first evaluate who has the burden of proof and then discuss what can be used as proof to file a complaint and how it would be handled in the judicial system.

6.2 Who Bears the Burden of Proof?

The judgment of the German Federal High Court of Justice states that every breach of mandatory law or articles of association causes the invalidity of adjudication. If the breach does not concern mandatory rules but procedural rules, which do not concern superordinate interests but rather the protection of individuals, the decision only becomes void if the voter protests against the decision [El12].

Relating to an action of an association against one of its members, the Federal Court of Justice has ruled that the association must prove the conformance of a decision with the articles of association, if the association wants to derive rights from an acclamation and if the member claims adverseness of the acclamation [BGH68]. Conversely, a member filing an action for a declaratory judgment and claiming the invalidity of an association election has to prove non-conformance with the articles of association. If someone claims the invalidity of a registered decision, the burden of proof generally rests on him [El12], [BGH68].

For the GI elections, this means that only breaches of mandatory rules of the articles of association or of the implementation rules cause invalidity of the election decision. It is up to the court of justice to determine this in particular cases. Every member of an association is allowed to file an action for a declaratory judgment in virtue of § 256 of the German Code of Civil Procedure (ZPO) against the association and thus assert the invalidity of an election. In this case, the member bears the burden of proof to show a defect. Therefore, members must have the possibility to control the election. Correspondingly, they are able to recognize election defects and submit these defects within the proper time period in order to push for legal action.

6.3 What Can Be Used and Accepted as Proof for Complaints?

The data that the POLYAS system itself currently provides for verifiability cannot be used as proof. However, voters could try to use technical aids to prove their claims, capturing voting actions using video or screenshots. If such a video would cover checking the block and then casting a vote, it can act as a proof, though it is not clear whether videos or screenshots have been manipulated. Voters may present witnesses to confirm their statement, but due to the possibility of manipulation, it can be assumed that the court is unlikely to admit this as proof.

Since a voter is not allowed to reveal his own voting decision in court as it violates the secrecy of elections [BVerwG76], it seems impossible that a court will admit the examination of a third person as a witness because this would mean further breach of secrecy. The voter could insist on appearing as a witness in person by arguing that there is no other chance to provide evidence that the system malfunctioned. It is not possible to judge on the voter's experiences and problem description as valid complaints can still not be distinguished from invalid ones, and the voter himself cannot prove his complaint. By refusing this evidence, the court would deprive the voter of his legal protection

[MüKo2012] [7], and by rejecting all complaints, as voters are not able to provide concrete evidence under the system, courts would not be able to further examine complaints that are indeed valid. To avoid the uncertain result of a legal proceeding, the association could establish an internal structure to scrutinize elections. However, for the moment, it cannot be recommended to publish the hash chain information during the election as no corresponding regulation for the GI exists.

7 Conclusion

In the recent past there has been an increase in the use of Internet voting systems. While ideally these systems would provide the user with the possibility to verify the election outcome, many of those used in practice are black-box systems. Voters therefore need to trust the systems. One example of a black-box Internet voting system is the POLYAS system, used in GI elections since 2004.

In 2011, the authors in [OSV11] proposed an improvement to POLYAS. Their suggestion was to publish the election results and the hash chain information to increase the level of verifiability, which is referred to as partial verifiability. In this paper we analysed the legal considerations for the GI elections using this version of POLYAS. This includes the need to publish election results for all candidates. We showed that this is not clearly regulated under the GI operating framework and that the presiding council is in charge of this. We then discussed whether publishing the information proposed in [OSV11] violates the secrecy of the vote. We showed that vote selling or coercion using the signature attack becomes more attractive. As this caused legal concerns, we proposed splitting the ballots in multiple race elections in order to maintain secret elections and enable partial verifiability for future GI elections.

Even though publishing election results is justifiable under the modifications made, publishing hash chain information during the election may still suffer from signature attacks. Therefore, we presented a randomization concept that allows one to bind the ballot box server to its content, ensuring integrity while at the same time significantly mitigating the risk of voter coercion.

However, as the handling of complaints turned out to be an open problem, we do not recommend publishing the hash chain information during the election. Therefore, it is recommended to clarify whether results per candidate can be published. If this is the case, then the improved extension for POLYAS should be applied for future GI elections without publishing the hash chain information during the election.

Recently, discussions with the POLYAS developers began regarding the corresponding problems and legal restrictions. For the future, we plan to closely collaborate to resolve these challenges. Future work will investigate how complaints can be handled and if such complaints are only a challenge to voting systems that provide partial verifiability

[7] Rejecting all complaints as voters are not able to prove their statement with this system would also mean that valid complaints will not be examined further. This needs to be discussed in future work.

or also to voting systems that provide end-to-end verifiability. A look at Civitas [CCM08] offers a potential solution. Since vote updating is enabled, a voter can update their vote, rather than raise a complaint, if they detect manipulation. Thereby, responsibility for the vote casting process rests with the voter.

Bibliography

[BGH68] Bundesgerichtshof. In: Neue Juristische Wochenschrift (NJW) 1968; pp. 543-545.

[BGH75] Bundesgerichtshof. In: Neue Juristische Wochenschrift (NJW) 1975; p. 2109.

[BVerfG09] Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 123; p. 39.(70) http://www.bundesverfassungsgericht.de/entscheidungen/rs20090303_2bvc000307en.html.

[BVerwG76] Bundesverwaltungsgericht. In: Neue Juristische Wochenschrift (NJW) 1976; pp. 259-260.

[CCM08] Clarkson, M.R.; Chong, S., Myers, A.C.: Civitas: Towards a Secure Voting System. In IEEE Symposium on Security and Privacy, 2008; pp. 354-368.

[CF85] Cohen, J.D.; Fischer, M.J.: A Robust and Verifiable Cryptographically Secure Election Scheme. In 26th Annual Symposium on Foundations of Computer Science, 1985; pp. 372-382.

[El12] Ellenberger, J. § 25. In: Palandt, O.: Bürgerliches Gesetzbuch – Kommentar, 71. Auflage, Verlag C.H. Beck, München 2012.

[Fl08] Fleck, W.: Die virtuelle Mitgliederversammlung im eingetragenen Verein. In: Deutsche Notar-Zeitschrift (DNotZ) 2008; pp. 245-258.

[GI05] Gesellschaft für Informatik: GI-Anforderungen an Internetbasierte Wahlen; 2005 http://www.gi.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf

[KET10] Krimmer, R.; Ehringfeld, A.; Traxl, M.: The Use of E-Voting in the Austrian Federation of Students Elections 2009. In (Krimmer, R., Grimm, R.): Electronic Voting 2010, Proceedings of the 4th Conference on Electronic Voting, LNI GI Series, Bonn, Germany, 2010; pp. 33 – 44.

[Ko12] Koch. § 18 Betriebsverfassungsgesetz; In: Erfurter Kommentar zum Arbeitsrecht, 12. Auflage, Verlag C.H. Beck, München, 2012.

[Mo06] Morlok, M., Art. 38. In: Dreier, H.: Grundgesetz – Kommentar, 2. Auflage, Mohr Siebeck Verlag, Tübingen, 2006.

[MM06] Madise, U.; Martens, T.: E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In (Krimmer, R.): Electronic Voting 2006, Proceedings of the 2nd International Workshop, LNI GI Series, Bonn, Germany, 2006; pp. 15 – 26.

[MR10] Menke, M.; Reinhard, K.: Compliance of POLYAS with the Common Criteria Protection Profile – A 2010 Outlook on Certified Remote Electronic Voting. In (Krimmer, R., Grimm, R.): Electronic Voting 2010, Proceedings of the 4th Conference on Electronic Voting, LNI GI Series, Bonn, Germany, 2010; pp. 109 – 118.

[MüKo12] Müller, H., § 107c. In: Münchener Kommentar zum Strafgesetzbuch, 2. Auflage, Verlag C.H. Beck, München 2012.

[OLGMü08] Oberlandesgericht München. In: Neue Zeitschrift für Gesellschaftsrecht (NGZ) 2008; pp. 351-353.

[OSV11] Olembo, M. M.; Schmidt, P.; Volkamer, M.: Introducing Verifiability in the POLYAS Remote Electronic Voting System. In: Proc. of the Sixth International Conference on Availability, Reliability and Security (ARES2011), Vienna, Austria, 2011; pp. 127 – 134.

[RGO09] Roßnagel, A.; Gitter, R.; Opitz-Talidou, Z.: Telemedienwahlen in Vereinen. In: MultiMedia und Recht (MMR) 2009; pp. 383-387.

[RJ07] Reinhard, K.; Jung, W.: Compliance of POLYAS with the BSI protection profile – Basic requirements for remote electronic voting systems. In (Alkasser, A; Volkamer, M.) E-Voting and Identity, 1st International Conference, (VOTE-ID 2007), Bochum, Germany. Lecture Notes in Computer Science, 2007; pp. 62 – 67.

[Sc09] Schreiber, W. § 1.: Bundeswahlgesetz – Kommentar, 8. Auflage, Carl Heymanns Verlag, Köln 2009.

[SSW10] Sauter, E.; Schweyer, G.; Waldner, W.: Der eingetragene Verein, 19. Auflage, Verlag C.H. Beck, München, 2010; Rn. 39a ff.