Dubious security practices in e-voting schemes
Between tech and legal standards

Tamara Finogina, Adrià Rodríguez-Pérez, and Jordi Puiggalí

Scytl Election Technologies, S.L.U., 08021, Barcelona, Spain
{tamara.finogina, adria.rodriguez, jordi.puiggali}@scytl.com

Abstract. Remote electronic voting has been around for a few decades now. However, some legal uncertainty regarding its uses remains. In this paper, we would like to highlight and discuss several techniques used in e-voting which may not be fully compliant with the law. We analyze several e-voting practices that rely on the addition of dummy ballots and show how they conflict with legal standards. Specifically, we focus on cases where dummy ballots are required for: better performance, testing, participation privacy, or preventing coercion. We argue that these practices may raise issues with the standards of authenticity and eligibility, as well as with the principle "one voter, one vote". Our research aims to offer a better understanding of how legal principles can be interpreted to ensure the legality of technological proposals in e-voting.

1 Introduction

Electronic voting is not a novel idea. It has been a topic of intense research for a few decades and has a history of successfully performing legally-binding elections [10,15,29]. Yet, the ambiguity in some legal aspects remains up to this day [9,18,30]. While it is true that the electoral procedure is, indeed, underspecified for electronic voting, some legal principles are channel-agnostic.

In this paper, we would like to highlight the problematic nature of including dummy ballots in the ballot box, commonly employed by e-voting schemes for fighting correction, optimizing tally, and testing. More specifically, we look into the casting of test votes in some Canadian municipalities, the optimization of some e-voting mix-nets, participatory privacy as suggested in the Helios-null scheme, and coercion-resistance mechanisms proposed in Selene II.

Through the paper, we focus only on basic requirements that are not likely to change in the future: equal suffrage, eligibility, and authentication. While it is true that the law might change, we look at legal principles that are likely to stay stable over time. It is important that electronic voting systems are designed with legal principles and requirements in mind instead of designing systems first and then trying to fit them into preexisting regulations.

With this work, we aim to encourage the consideration of electoral requirements in the early stages of e-voting solution development to facilitate its use in practice. We hope that it will help to re-evaluate the merit of some decisions and, perhaps, lead to better e-voting scheme designs.

Paper structure: In section 2, we briefly explain different scenarios leading to dummy votes addition to the ballot box. Then, in section 3, we recall general and national legal standards and discuss possible conflicts. After that, in section 4, we propose some recommendations and conclude our paper in section 5.

2 Addition of dummy ballot to the ballot box

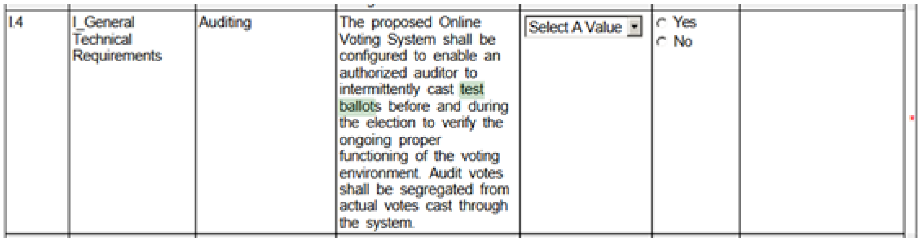
In traditional elections, it is illegal to insert ballots of non-eligible voters (including empty or invalid ones) into a ballot box (i.e., ballot box stuffing) [6]. Yet many e-voting schemes add dummy votes to the ballot box for various reasons. By dummy votes, we mean any ballot that is stored in the ballot box during the election but not included in the election result: e.g., vote containing encryption of zero, vote used for testing the system, votes pre-added to the ballot box, etc.

Usually, the goal of the dummy ballot addition is to hide that a voter voted or re-voted, facilitate the optimizations of cryptographic schemes (e.g., Mixing), enhance privacy, or perform an election audit. Typically, e-voting schemes claim that such votes are easily detectable and thus are in line with electoral principles and requirements. However, it is not as simple as it might appear.

In this section, we briefly explain how exactly different e-voting schemes utilize dummy ballots.

2.1 System audit during the election

Casting audit ballots during the election is a functionality required by some Election Management Bodies on their requirements when searching for an Internet voting solution (e.g. Figure 1). Examples are some of the Ontario Municipalities in Canada, such as the City of Markham [25] and the City of Vaughan [26]. In both cases, they request the possibility for auditors to cast test/audit ballots before and during the election to verify the proper behavior of the system. The audit ballots must be segregated from valid ones to avoid their (audit ones) inclusion in the election results. Additionally, the system should provide reports for both audit and regular ballots to allow auditors to check if the audit vote's content corresponds to the intended one, thus ensuring the accuracy of the system.



I.4	I_General Technical Requirements	Auditing	The proposed Online Voting System shall be configured to enable an authorized auditor to intermittently cast test ballots before and during the election to verify the ongoing proper functioning of the voting environment. Audit votes shall be segregated from actual votes cast through the system.	Select A Value ▾	○ Yes ○ No	

Fig. 1. Extract from audit ballot requirement on City of Markham RFP.

The main idea behind audit ballots is that the voting system provides special voting credentials for auditors that allow them to cast audit votes in the same voting system used by voters during the election period. That way, audit votes are not only cast in the same environment used by the voters but also stored in the same ballot box. Therefore, if there is something not properly implemented in the voting system or the voting system misbehaves, this could be detected by the auditors during the voting (e.g., there are missing or incorrect voting options) or counting (the contents of the audit votes are not the same as the ones cast by the auditors) phases. It is relevant in this requirement that the system is exactly the same one used in production used by the voters. Therefore, standard practices in IT systems such as: using pre-production environments to avoid testing in production are not valid in this case.

To allow audit ballots, auditors need at least one credential for casting an audit vote. However, it also is required that these audit votes must be distinguishable from the valid ones to avoid compromising election integrity (i.e., altering the election results). That means audit votes should include some information or mark that will allow to isolate them from the counting process. For this purpose, we can distinguish two different approaches: one is to permit identifying votes in the ballot box at any time of the election (i.e., during the voting process), and the other is to do the same but in the counting process only.

If votes are identifiable at any time (for instance, if they have a tag in the envelope [1] or correspond to the auditor credential), anybody can distinguish them at any step of the voting process. While this provides complete transparency on the type of vote, it limits the audit capabilities mainly to errors in the election configuration or on the behavior of the voting system. For example, an auditor who wishes to detect attacks focused on manipulating the election cannot do so since the attacker can identify the audit votes and hide attacks. For this reason, the alternative approach is to keep secret the mechanism that identifies audit votes from the valid ones during the voting process.

Mechanisms that hide the difference between audit and regular votes until the counting process is over require the audit votes to look like any other vote cast by any eligible voter. Therefore, attackers cannot identify an audit credential from a valid one nor detect a tag specific to auditors.

Using audit ballots implies the following requirements from an election management point of view:

- Provide audit credentials to auditors: to allow them to cast audit votes as if they were valid voters;
- Traceability of cast votes: to avoid that audit votes are not included with the valid ones on the final count.

In addition to distinguishing valid voters from the auditors, we also need to identify which ballot has been cast by these auditors. When auditors are not anonymous, we can easily group the votes with the same audit tag (e.g., with the same identifier in the envelope). When the auditor's identity must remain secret, we cannot use the audit tags; however, we still can rely on the link between cast votes and the credential used to cast them. Standard practice is to encrypt votes before sending them, so we should keep the link to this encrypted vote (envelope) instead of the contents (vote). This approach is similar to postal voting, where the envelope with a vote is inside a second envelope which contains the voter's identity.

However, this traceability requirement should be global, even for valid voters. Therefore, it becomes of paramount importance that Internet voting systems anonymize the encrypted votes (e.g., homomorphic tally or Mixing) before proceeding with decryption and counting.

[1] The envelope tag is an identifier concatenated to the encrypted vote that makes it different from the valid ones, like having an envelope with a specific color for audit votes.

2.2 Mix-net optimizations

The verifiable shuffle is one of the most used anonymization techniques in the tally phase. It allows breaking the correlation between voter identities and decrypted ballots; while simultaneously providing assurance that no vote was modified, omitted, or inserted. Among all verifiable shuffle proposals, the most efficient and famous are Bayer-Groth [3] and Terelius-Wikström [24] proofs.

However, generating and verifying the shuffling proof can be time-consuming, plus it requires a significant amount of memory. Consider the verification of the shuffle proofs for $N = 100000$ ElGamal ciphertexts done by four mix-nodes[2]. Verifying[3] a single Terelius-Wikström shuffle proof requires approximately $9N$ exponentiation, while a single Bayer-Groth proof needs $4N$ [11]. Assuming one modular exponentiation on 3072-bits integers takes about 9 milliseconds, we can estimate verification to roughly take 9 and 4 hours. In terms of poof size, the optimized Byer-Groth proof is by a factor of 50 more compact than Terelius-Wikström proof [3]. Therefore, in practice, implementations aim to optimize the shuffle part.

For example, a Bayer-Groth proof is more compact when the number of messages N is closer to a square [3]. Technically, the proof works for any matrix shape and, in general, has a sub-linear communication complexity. However, the minimal communication complexity $\mathcal{O}(\sqrt{N})$ can be achieved only if we can arrange messages into a square matrix $N = n \times m$ with $m = n$.

Another optimization, applicable to both Bayer-Groth and Terelius-Wikström proofs, was proposed in [24]. The idea is to significantly speed up the proof generation process by splitting it into online and offline phases [31]. In the offline phase, the prover computes a commitment to a permutation matrix and proves it is constructed correctly. It is a costly process, but it can be pre-computed. In the online phase, the prover demonstrates that the committed permutation matrix has been indeed used in the shuffle. The optimization makes the online part several times faster by shifting some of the heavy computations to the offline one. For example, optimized in that manner, Terelius-Wikström proof would have similar to Bayer-Groth proof performance.

The bottleneck, however, is the fact that the number of votes cast in an election is unknown in advance. Even the best statistic does not allow

[2] The example is taken from [11]

[3] To generate the proof, Terelius-Wikström requires $8N$ exponentiations and Bayer-Groth needs $2N \log m$, where $N = m \times n$ [11].

us to foresee how many votes will reach the tally phase. Therefore the practical use of mix-net optimizations is not that straightforward. Some propose to do the pre-computation for a fixed pre-selected number N and then, when finally only X ballots arrived to the mixnet, add $N - X$ trivial messages $(1, 1)$ [12] (e.g., encryption of 1 with randomness 0) to get N ciphertexts and enable the optimization. The justification for adding dummy votes is that they are easy to detect and remove from the final tally.

2.3 Participation privacy

In some cases, the dummy ballots are cast during the voting phase to hide whether a particular voter voted or re-voted. The expectation is that the coercer cannot attribute ballots to a particular voter; hence it cannot tell whether the voter changed the vote or even participated in the election at all.

For example, in the Helios-null scheme [16], the real votes are masked by the null votes cast by posting proxies and other voters. The idea is that anyone may add encryption of 1 to any voter's raw, and voters can update their votes. The addition of dummy null votes creates a constant flow that confuses the coercer. As a result, the scheme provides participation privacy.

To ensure that ballots arrive at unpredictable intervals, Helios-null requires another entity, a posting proxy, to submit multiple null votes on behalf of each voter at random times. Those null votes are indistinguishable from real ones and accepted as valid by the ballot box. For preventing vote modification, each ballot includes disjunctive proof showing that it is either an encryption of 1 or was cast by an eligible voter.

At the end of the election, the final ciphertext of each voter is a product of votes corresponding to the voter. Since the null votes are all encryptions of 1, only the non-null votes influence the tally. If some voters abstained, their resulting ciphertexts are encryption of 1.

2.4 Fighting coercion

Another idea for providing coercion-resistance was proposed in Selene II [23], which enhances the original Selene scheme. Selene relies on assigning tracking numbers to votes for enabling cast-as-intended verification. The voters cast their votes without knowing their tracking numbers just yet. Then all votes are shuffled, decrypted, and published along with corresponding tracking numbers. For performing verification, each voter should return, and receive the tracking number shares from all Tellers. After that, the voter uses a private key to recover the corresponding tracking number and locate the decrypted vote. In case of coercion, the voter can fake the tracker and point it to any other line in the public ballot box. Because the shares are sent without any proof of origin, the coercer cannot distinguish between real and fake tracker.

The drawback of Selene is that a coerced voter might have the misfortune of choosing the coercer's tracking number. Alternatively, the coercer might falsely claim that it was his tracker. In both cases, the voter might not be confident enough to insist and hide disobedience.

Selene II addresses this issue by providing each voter with a set of personalized fake trackers and fake votes that the voter can use to trick the coercer. The bulletin board will now contain one extra vote per candidate per voter. On the one hand, it assures voters that their fake tracker will not be claimed by someone else. On the other hand, those dummy ballots should be removed before announcing the final tally.

In a nutshell, the idea of the Selene II tracking collision fix is to start an election with a ballot box already containing fake votes related to fake trackers (i.e., the ballot box is not empty). Before the election begins, each candidate already has one vote from each eligible voter. In a sense, each voter votes once for every candidate and twice for the intended selection. Though, the pre-added votes come from authorities rather than the eligible voters. After mixing and decryption, the ballot box contains a mix of real and pre-added ballots, and no one can tell them apart. However, since each candidate received the same number of additional votes, one can easily reconstruct the final tally.

3 Discussion

3.1 (International) standards for e-voting and how to observe them

It is important to evaluate these practices against international standards for democratic elections. In this regard, the techniques describe may need to comply with the principle of equal suffrage.

International standards for e-voting Equal suffrage is a fundamental principle of democratic elections. For example, art. 21 the Universal Declaration of Human Rights (UDHR) states that "[t]he will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures" (emphasis added) [27]. Similarly, art. 25 of the International Convention on Civic and Political Rights (ICCPR) states that "Every citizen shall have the right and the opportunity, [. . .] (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors" (emphasis added) [28].

Comment no. 25 by the Human Rights Committee further develops the requirements in art. 25 ICCPR [13]. When it comes to equal suffrage, it states that "[t]he principle of one person, one vote, must apply, and within the framework of each State's electoral system, the vote of one elector should be equal to the vote of another" [13, §21]. In Europe, the European Commission for Democracy through Law (Venice Commission) has also developed standards from electoral principles. According to the Venice Commission, equal suffrage entails equal voting rights, meaning that "each voter has in principle one vote; where the electoral system provides voters with more than one vote, each voter has the same number of votes" [6]. In a similar fashion, paragraph 7.3 of the Copenhagen Document also says that participating States will provide "equal suffrage to adult citizens" [1].

When it comes to (remote) electronic voting, the only international reference is the Council of Europe's recommendation on e-voting: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. The understanding of equal suffrage in the Recommendation is based on the Venice Commission's Code of Good Practice in electoral matters [4, §14]. It is summarized as "each voter has the same number of votes, each vote has the same weight and equality of opportunity has to be ensured" [4, §14]. The Recommendation identifies five standards regarding this principal [19, §5-9]:

5 All official voting information shall be presented in an equal way, within and across voting channels.

6 Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.

7 Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

8 The e-voting system shall only grant a user access after authenticating him/her as a person with the right to vote.

9 The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

The Explanatory Memorandum to the Recommendation further details these provisions. When it comes to authentication (standard 8), it reads that “[i]n cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter” (emphasis added) [4, §43]. Therefore, standard 9 can be linked to eligibility requirements. Eligibility is not defined in standard 9, but standard 18 in the Recommendation reads that “[t]he system shall provide sound evidence that only eligible voters’ votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system” (emphasis added) [19, §18]. Here, the Explanatory Memorandum also provides some additional information. It states that “[v]oters and third parties should be able to check that only eligible voters’ votes are included in the election result” (emphasis added) [4, §62]. In this regard, a vote is defined as “the expression of the choice of voting option” [19] (and by casting a vote it is understood “entering the vote in the ballot box” [19])

The Explanatory memorandum further develops the standard of “one person, one vote” (standard 9) as well. It sets that “[a]ll votes cast by either electronic or non-electronic voting channels are counted. It should be ensured that only eligible voters’ votes are included in the election results” [4, §44]. Regarding the later standard, the Guidelines also provide some additional information. According to the Guidelines, “multiple votes are considered as an attempt to cast more votes than a particular voter is permitted. This risk might arise, for instance, if the voter tries to cast multiple votes him or herself or if another person tries to use the voter’s identity in order to vote, in the voter’s name, after he or she has voted” [5, §9.c].

Interestingly, the Recommendation does not preclude the possibility of multiple voting. Multiple voting has been introduced in several countries in order to mitigate coercion concerns in uncontrolled environments. The first country to introduce multiple voting was Estonia. In Estonia it is possible to cast several votes online and only the last one counts. Likewise, a voter can decide to cancel any online votes cast under duress by going to a polling station and voting in person. Since the last local elections, a voter can even cancel their e-vote by voting on election day (something that was not possible before). Other cases where multiple voting has been introduced are Norway [2], and the Åland Islands in Finland [14].

In this regard, the Guidelines on the implementation of the provisions of the Recommendation [5] foresee two different scenarios with multiple voting. In the first scenario, "a voter is allowed to cast an electronic vote multiple times" [5, §9.a]. In the second, "a voter is allowed to cast a vote by more than one voting channel" [5, §9.b]. In both scenarios, is understood that multiple voting can be introduced "as a countermeasure to voter coercion, which remains possible when voting takes place outside a controlled environment" [5, §9.a-9.b].

Equal suffrage in national e-voting regulations

Switzerland: The Annex to the Federal Chancellery Ordinance explicitly states that votes stored in the ballot box must be properly cast:

"If the vote has been cast in conformity with the system, the system stores the vote in the electronic ballot box and informs the voter that the vote has been cast successfully. Votes not cast in conformity with the system are not stored in the electronic ballot box. [...]" [7, 2.6.3]. Later it is also clarified what "cast in conformity with the system means: "A vote is deemed to be cast in conformity with the system only if the client-sided authentication measure used corresponds to a server-sided authentication measure that was adopted and "assigned" to a voter in the preparatory phase of the ballot. The proof must therefore include confirmation that no unallocated authentication certificates for casting votes have been issued. In addition, during preparation for the ballot, the control components or the auditors must have been given corresponding data as the basis for making a comparison. The auditors must ascertain that the number of authentication certificates corresponds to the (official) number of authorised voters."[7, 4.4.6]

Estonia. Estonia is one of the countries where it is possible to cast multiple votes electronically, and even cancel any online vote by voting on paper during the advanced voting period or on election day.

Notwithstanding, there were discussions about the legality of multiple voting. On 12 July 2005, after the Riigikogu adopted the Local Government Election Act, the President of the Republic of Estonia turned to the Supreme Court to declare it unconstitutional. The President referred "in the reasons for his decision to contradictions with the principle of uniformity of local government councils elections stipulated in subsection

256 of the Constitution" [17, p. 19]. However, "[t]he Constitutional Review Chamber of the supreme Court refused to satisfy the application of the President of the Republic", who pursuant to the Constitution was obliged to proclaim the Act [17, p. 20]. The Supreme Court of Estonia justified the constitutionality of e-voting and of multiple voting ruling that "Despite the repeated electronic voting a voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. A vote given by electronic means shall be counted as one vote and from the point of view of voting results this vote is in no manner more influential that the votes given by voters using other voting channel" [22].

However, this is not a breach of the principle "one voter, one vote". Legal provisions in Estonia are clear when it comes to ensure the principle of "one voter, one vote". In this regard, art. 48.7 of the Riigikogu elections act states which is the valid vote that should be taken into account when voters have cast more than one ballot: the last vote cast by electronic means [21, 48.7(1)], or any ballot cast on paper, since these take precedence over votes cast electronically [21, 48.7(4)]. Even more interesting, section (5) of this article clearly sets that "If a voter has voted several times outside the voting district of his or her residence, and using electronic means, all envelopes with ballot papers of the voter as well as the vote cast using electronic means shall not be taken into account."

How to observe new voting technologies? One of the limitations of the Recommendation is that it does not specify how compliance with the standards can be ascertained. In this regard, it is more useful to investigate the OSCE/ODIHR's methodologies for the observation of new voting technologies. The methodologies of the OSCE/ODIHR do not set standards as such, but rather "focus on identifying good practices or formalizing procedures. They do not aim at providing an evoting regulation and most of them are domain specific focusing on the needs of election officials, observers and so on."[8, p. 112] Although the OSCE/ODIHR's methodologies are based on the Copenhagen document, we have already seen that it does also include the principle of equal suffrage. More specifically, and according to the Handbook for the Observation of New Voting Technologies, "one of the aspects of the principle of equality is that no voter will be able to cast more votes than another, [. . .] This means that NVT systems must prevent any person from casting more votes than is established by law and must prevent any votes from being subtracted from the system" [20, §10]. For the OSCE/ODIHR, what can be assessed to evaluate compliance with secret suffrage are: “What steps are taken to ensure that the electronic memory does not contain any votes prior to the start of voting? Is this verifiable?”[20, 58]

As it is the case for the Council of Europe’s Recommendation, these provisions do not prevent the casting of multiple votes. In this regard, it is acknowledged that “[s]ome Internet voting systems allow voters to cast their vote more than once, with the condition that only the last cast vote counts. This helps to reduce the risk of voter coercion and vote buying. Consequently, it must be possible to verify that no violations of the principle of equality have taken place” [20, 10].

3.2 Dubious practices

Therefore, some of the techniques described may not either comply with the standards of authentication; with the standards of eligibility; or with none of them. In what follows we analyze the different practices against these two standards:

Issues with authentication and eligibility For example, mix-net optimizations as suggested by [12] require adding trivial messages to the ballot box. Regardless of the value of these messages, they can clearly be understood as votes cast into the ballot box based on the definitions in the Recommendation. However, the wording of standards 9 and 18 in the Recommendation establish that “only eligible voters’ votes have been included in the respective final result” (emphasis added). Since the proposal only adds these votes during the mixing phase, the practice would be compliant as long as they are removed from the final results. The question is therefore how to ensure that those votes are dully deleted before the count.

In Selene II, several votes are cast for all candidates by a non-eligible entity as well. In fact, here the ballot box is not empty at the beginning of the election. The votes are stored in the ballot box until the actual decryption. It is only then that the election authority can subtract the extra votes for all candidates and reveal the actual election result. Therefore, the issue here is what is understood by “final result”. Since the output of the decryption is not yet final, it is possible to argue that this system still complies with the international standards.

However, it is evident that this proposal does not satisfy the requirement by the Swiss and Estonian legislation on the validity of votes cast, and neither will they comply with the OSCE/ODIHR’s criteria that no votes should be cast prior to the start of voting.

Issues with the principle "one voter, one vote" In the proposal for participation privacy, voters can cast dummy votes on behalf of other votes. This practice seems to breach the standard of "one voter, one vote". Furthermore, and in contrast to multiple voting, here it is not the voter themselves who cast the extra votes to cancel out any vote cast under duress.

Furthermore, the posting proxies also cast votes on behalf of the actual voters. This fact means that not only are more than one vote per voter cast, but that some of these votes are actually cast by proxies who are not eligible in the election. Therefore, their role breaches the two standards that we have identified.

Issues with both principles The proposal to cast audit impacts both standards. On the one hand, having audit credentials translates into additional voters being added to the electoral roll of the election since it is necessary to add auditor credentials. On the other hand, it is possible that an auditor is registered several times as different voters in case they want to make multiple tests or test different contents in the same election.

If it is not necessary to keep the audit credentials secret, the system and the parties involved can be aware of which votes are cast by auditors. However, this could limit the ability to detect attacks. Therefore, the main impact is when the auditors must be indistinguishable from regular voters since auditors should be registered as (fake) eligible ones. The list of the additional audit voters and their related auditors must be kept secret until the voting process ends. Afterward, the list must be made public to allow to distinguish between valid voters and audit ones to isolate audit votes in the counting process and provide real participation statistics.

An alternative to casting audit votes is to allow voters to participate in the validation of their votes cast. That implies adding Individual Verifiability capabilities (cast-as-intended and counted-as-cast) to the voting system. Therefore, it is not necessary to generate audit credentials for auditors or isolate audit votes from valid ones in the ballot box. So it is less intrusive from the vote casting and counting point of view. However, individual verifiability is not a traditional process and therefore, generates other conflicts from the election legislation point of view that must be also evaluated.

4 Recommendations

As a general recommendation, we advise storing in the ballot box only votes cast by eligible voters. This approach would be the most in line with all legal regulations. Moreover, it would prevent the spread of misconceptions regarding e-voting security, which commonly arise in cases of temporal addition of ballots to the ballot box. The general public often remarks that adding values to the ballot box (even if temporary) feels insecure.

Also, the addition of any values (no matter how temporary) unavoidably complicates the tally and audit processes as more ballots should be reviewed and/or anonymized. For example, Selene II would require shuffling significantly more ballots than any other system in similar settings, which would slow down the tallying.

In the case of audit ballots, the separation of audit and valid votes in a ballot box must happen before executing the anonymization and counting. We can do this through a reconciliation process (also known as cleansing) that uses the secret list of audit voters (revealed at the counting phase) to segregate the votes cast from these voters from the valid ones. The list of valid ones is sent through the anonymization and counting process to have the results. The audit votes should be decrypted directly to allow auditors to check if the cast votes indeed contain their selected voting options. In turn, it must be also audited that none of the ballots is included in the final tally

As for the mix-net optimizations, we recommend disabling precomputations and focusing on other optimization techniques.

5 Conclusion

In this paper, we analyzed several e-voting practices that rely on the addition of dummy ballots and showed how they conflict with legal standards, namely: authentication, eligibility, and the principle “one voter, one vote”. In our analysis, we considered both international e-voting standards and national regulations. More specifically, we look into the casting of test votes in some Canadian municipalities, the optimization of some e-voting mix-nets, participatory privacy as suggested in the Helios-null scheme, and coercion-resistance mechanisms proposed in Selene II. We have concluded that such practices do not comply with the OSCE/ODIHR criteria or Swiss and Estonian legislations. We also provided some general recommendations that would be in line with regulations. We hope that our observations and recommendations will facilitate the implementation of electoral requirements in the early stages of e-voting solution development to facilitate its use in practice.

References

1. *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE*, Copenhagen, June 1990. Organization for Security and Co-operation in Europe.
2. Jordi Barrat, Michel Chevalier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. Internet voting and individual verifiability: the norwegian return codes. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, pages 35–45, Bonn, 2012. Gesellschaft für Informatik e.V.
3. Stephanie Bayer and Jens Groth. Efficient zero-knowledge argument for correctness of a shuffle. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 263–280, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
4. Council of Europe. 2.3 Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) a. Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Committee of Ministers.
5. Council of Europe. 2.3 Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) b. Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. Committee of Ministers.
6. Council of Europe (Venice Commission). *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report.* Council of Europe, Strasbourg, 2002.
7. Die Schweizerische Bundeskanzlei (BK). Annex to the FCh Ordinance of 13 December 2013 on Electronic Voting (OEV, SR 161.116). Technical and administrative requirements for electronic vote casting.
8. Ardita Driza Maurer. Ten years council of europe rec(2004)11: Lessons learned and outlook. In Robert Krimmer and Melanie Volkamer, editors, *Proceedings of Electronic Voting 2014 (EVOTE2014)*, pages 111–117, Tallinn, 2014. TUT Press.
9. Ardita Driza Maurer. Legality, separation of powers, stability of electoral law: The impact of new voting technologies. *Electoral Expert Review*, 01 2016.
10. J. Paul Gibson, Robert Krimmer, Vanessa Teague, and Julia Pomares. A review of e-voting: the past, present and future. *Annals of Telecommunications*, 71, 06 2016.
11. Rolf Haenni and Philipp Locher. Performance of shuffling: Taking it to the limits. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers*, page 369–385, Berlin, Heidelberg, 2020. Springer-Verlag.
12. Thomas Haines, Olivier Pereira, and Vanessa Teague. Report on the swiss post e-voting system. March 2022.
13. UN Human Rights Committee (HRC). Ccpr general comment no. 25: Article 25 (participation in public affairs and the right to vote), the right to par-

ticipate in public affairs, voting rights and the right of equal access to public service. UN General Assembly, 1996. `https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf`.

14. Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Radu Antonio Serrano, Marlon Freire, and Casper Wrede. Nordic pioneers: facing the first use of internet voting in the Åland islands (parliamentary elections 2019). SocArXiv 5zr2e, Center for Open Science, 2019.
15. Robert Krimmer, Stefan Triessnig, and Melanie Volkamer. The development of remote e-voting around the world: A review of roads and directions. In Ammar Alkassar and Melanie Volkamer, editors, *E-Voting and Identity*, pages 1–15, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
16. Oksana Kulyk, Vanessa Teague, and Melanie Volkamer. Extending helios towards private eligibility verifiability. volume 9269, September 2015.
17. Ülle Madise, Priit Vinkel, and Epp Maaten. Internet voting at the elections of local government councils on october 2005 : Report, 01 2006.
18. Sutton Meagher. When personal computers are transformed into ballot boxes: How internet elections in estonia comply with the united nations international covenant on civil and political rights. *American University International Law Review*, 23, 2007.
19. Council of Europe. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Committee of Ministers.
20. OSCE Office for Democratic Institutions and Human Rights (ODIHR). *Handbook for the Observation of New Voting Technologies (NVT)*. November 2013.
21. Riigikogu. Riigikogu Election Act.
22. Riigikogu. SUPREME COURT OF ESTONIA. Constitutional judgment 3-4-1-13-05. JUDGMENT OF THE CONSTITUTIONAL REVIEW CHAMBER OF THE SUPREME COURT.
23. Peter Ryan, Peter Rønne, and Vincenzo Iovino. Selene: Voting with transparent verifiability and coercion-mitigation. volume 9604, pages 176–192, February 2016.
24. Björn Terelius and Douglas Wikström. Proofs of restricted shuffles. In Daniel J. Bernstein and Tanja Lange, editors, *Progress in Cryptology – AFRICACRYPT 2010*, pages 100–113, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
25. THE CORPORATION OF THE CITY OF MARKHAM. RFP 079-R-21. Municipal Election (2022) – Supply and Implementation of an Online Voting System with Support and Services.
26. THE CORPORATION OF THE CITY OF VAUGHAN. RFP21-269. Provision of Internet voting services for the 2022 Municipal Election.
27. United Nations. *Universal Declaration of Human Rights.* December 1948.
28. United Nations (General Assembly). International covenant on civil and political rights. *Treaty Series*, 999:171, December 1966.
29. Carlos Vegas and Jordi Barrat. Overview of current state of e-voting worldwide. In Feng Hao and Peter Y. A. Ryan, editors, *Real-World Electronic Voting. Design, Analysis and Deployment.*, pages 51–75, New York, USA, 2016. Auerbach Publications.
30. Priit Vinkel. *Remote Electronic Voting in Estonia: Legality, Impact and Confidence.* PhD thesis, 08 2015.
31. Douglas Wikström. A commitment-consistent proof of a shuffle. In *Proceedings of the 14th Australasian Conference on Information Security and Privacy*, ACISP '09, page 407–421, Berlin, Heidelberg, 2009. Springer-Verlag.