THE IMPACT OF THE COUNCIL OF EUROPE RECOMMENDATION CM/REC (2017)5 ON EVOTING PROTOCOLS

Domenica Bagnato[1]

DOI: 10.24989/ocg.v335.4

Abstract
Evoting systems are defined by the protocol system employed and two such protocols are the Envelope and Token protocols. On the 14 June 2017, the Council of Europe passed its recommendations for evoting systems for elections and referendums, which define requirements for the core functioning of an evoting system. This paper assesses these two main protocols and assesses their viability in context of the Recommendations.

1. Introduction

This paper analyses two key e-voting system protocols, namely the Envelope and Token protocols, and assesses their viability in regards to the Council of Europe's Recommendation CM/Rec(2017)5[2].

On the 14 June 2017 the "Recommendation CM/Rec(2017)5[2] of the Committee of Ministers to Member States on standards for e-voting" and the two addenda containing an explanatory memorandum [10] and guidelines [11] were passed. This superseded Recommendation 2004(11) on the same topic [1]. For such purposes the major concern is the evoting protocol itself, which is the method applied that defines the systems core functioning and includes the cryptographic methodology of the system. This paper focuses on the main improvements of 2017(5) as compared to 2004(11), which arguably lie in the areas of (i) verifiability; and (ii) strong protection of voting secrecy.

2. Framework of Analysis

There is no such thing as an information system and/or cryptographic system that can provide perfect security in all dimensions at this stage. The question really is for us: (i) to identify the security dimensions; and (ii) to determine the extent of the security provided by a system in these dimensions; in order to assess the e-voting system as a whole, according to the Recommendations CM/Rec(2017)5 of the Council of Europe. It is important to distinguish between which security safeguards are organisational measures, that is a result of human effort at the time of the election, and which are technical, that is a result of system programming that functions independently from human work effort at the time of an election. This paper is primarily concerned with the technical aspects of the e-voting system and to the extent to which the e-voting system can provide

[1] Domenica Bagnato, Hierodiction Software GmbH. Email: domenica.bagnato@hierodiction.com

safeguards independently of organisational measures, for organisational measures in themselves can be manipulated and hence are a risk to security. For clarity, organisational measures would include the transporting of the ballot box data file from one location to another by the election committee. This in itself could provide a risk to security as the file may be corrupted.

In the following, only those standards, abbreviated SD, of CM/Rec (2017)5 have been selected that directly relate to the core functioning of an evoting system namely, its protocol. Standards unrelated to the evoting protocol,[2] pertaining for example to organisational issues, are not the focus of this paper.

In assessing the evoting protocols according to the Standards, six basic criteria (A-F) and their dimensions have been defined, namely:

(A) Equal suffrage includes:

(i) The unique identification of voters (SD 7);

(ii) Access granted only to authenticated voters (SD 8);

(iii) Only appropriate number of votes per voter are stored in the electronic ballot box (SD 9);

(iv) Only appropriate number of votes per voter are included in the final count (SD 9).

Note that (i) and (ii) are generic properties that are independent from the evoting protocol.

(B) Individual Verifiability includes:

(i) Verification by the voter that the voters' intention is accurately represented by the vote and that the "sealed vote" has entered the ballot box without being altered. (SD 15);

(ii) Voter confirmation that the vote has been cast successfully (SD 16).

(C) General Verifiability includes:

(i) Sound evidence, be provided, "that each authentic vote is accurately included in the … election results" and be independently verifiable from the evoting system (SD 17);

(ii) Sound evidence, be provided that "only eligible voters' votes have been included in the … election results" and be independently verifiable from the evoting system (SD 18);

(D) Secret suffrage includes:

(i) Ensuring the secrecy of previous voting choices made by the voter before issuing his or her final vote. (SD 25);

[2] An example for this would be Standard 16: The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed. This standard certainly relates to verifiability, but does not concern the eVoting protocol, rather it is an issue of user interface design independent from the eVoting protocol itself.

(ii) Anonymity of votes, notably that the unsealed vote and the voter cannot be linked during counting. (SD 26);

(iii) Ensuring "that the secrecy of the vote be respected at all stages of the voting procedure." (SD 19).

(E) No premature disclosure of election results:

(i) Secrecy of the number of votes for any voting option is to be maintained until after the closure of the electronic ballot box. (SD 24).

(F) Anti-coercion:

(i) Not providing the voter with proof of the content of a vote cast "for use by third parties." (SD 23).

3. Enveloping Protocols

Enveloping is an example of a protocol family, where anonymization takes place after the vote was added to the ballot box. Let us first look at how the Envelope scheme, so named because of its similarity to ordinary postal voting procedures, basically works. Enveloping has been widely implemented, probably because of its intuitive appeal due to its emulation of postal voting, and as an example we will take a look at the Estonian e-Voting system [5][7], which has been implemented in elections in Estonia since 2005 [5, p. 4][3, p. 83].

3.1. General Overview

The envelope evoting process can be split into three stages:

3.1.1. Casting a Vote

The voter downloads a voting client application and uses it to identify himself, via his ID-Card by entering in the PIN associated with his authentication key, to the VFS[3], which verifies the voter's eligibility to vote, in order to receive the list of candidates, based on the voter's constituency, for whom he is eligible to vote [5, p. 7][7, p. 705][3, p. 87]. The voter's vote and the random number generated, r, supplied by the e-voting client is encrypted using the public key of the election committee, and this creates the inner envelope [5, p. 7][7, p. 705]. The voter then confirms his vote by digitally signing the inner envelope creating a second layer known as the outer envelope [5, p. 7]. The outer envelope containing the inner envelope is sent to the server and it returns a QR-code, which enables the voter to verify and/or change his vote a maximum of three times for up to 30 minutes after casting his initial vote [7, p. 706].

3.1.2. Verification

To verify and/or to change the vote, the voter scans in the QR-code using a different device from which he initially voted and the smart device sends the code to the VFS, which passes it on to the

[3] Vote Forwarding Server (VFS) is the only server that is publically accessible. "It verifies voter eligibility, and acts as an intermediary to the back end vote storage server, which is not accessible from the Internet." [7, p. 705]

VSS[4]. From the session code, the VSS identifies the vote stored in the system and sends it back via the VFS. The encrypted vote only as well as a list of all the possible candidates are received by the smart device. It encrypts all the possible combinations for the candidates with the original public key used to encrypt the vote and compares it with the voters' intended choice. If there is a match the candidate is displayed. The voter also has the option to change the vote [7, p. 706].

The e-voting system stores the voting envelopes on the VSS until it is time to count the votes. [7, p. 705]

3.1.3. Counting

At this time, the outer envelope, which contains the voter's digital signature, and the inner envelope, consisting of the vote encrypted by the public key, are separated as seen in the figure below. The anonymous encrypted votes are stored on a DVD and transferred to a separate machine that decrypts and counts the votes. [7, p.706].

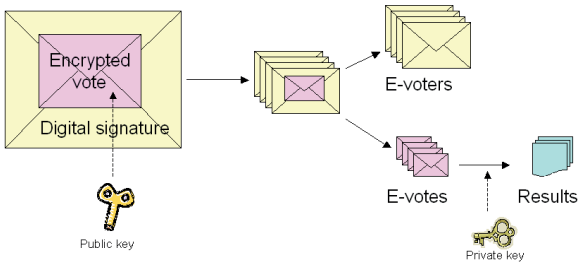

Figure 1. Envelope evoting system [6, p. 10, fig. 2]

3.2. Envelope Protocol in the Light of CM/Rec(2017)

Using the envelope system as defined by the literature, it is possible for the voter to accurately verify his vote and to verify that the sealed vote has entered the electronic ballot box (VSS) without being altered and since all interactions are logged[5] manipulation should be detectable fulfilling the requirements of SD 15.

However, during the verification stage of the voting process, it is questionable as to whether the system is able to compute large scale and complex voting possibilities using such devices as a smartphone [7, p. 706] in order to compare the voter's intention to all possible votes to find a match, because this could equate to thousands of combinations. For example, we have an election with preference voting, enabling the voter to select from 10 parties and 10 candidates per party, for preference voting, from which voters may select 3 from the party they voted for. This would be a typical scheme, for instance, in an Austrian national or European Parliament elections. For each party, there are n! / (n-k)! k! = 10! / 7!3! = 120 combinations of preference votes and for all 10 parties, 1200 combinations. If voters are not limited to the candidates of the party they voted for in

[4] Vote Storage Server "(VSS) is a backend server that stores signed encrypted votes during the online voting period. Upon receiving a vote from the VFS, it confirms that the vote is formatted correctly and verifies the voter's digital signature." [7, p. 705]
[5] Log Server "is an internal logging and monitoring platform that collects events and statistics from the VFS and VSS." [7, p. 705]

their preference votes, the number of combinations increases to over 160,000, whose RSA-encrypted inner envelope has to be computed. This requires considerable computing power and memory, on the device and may create a non-negligible data load.

Moreover, the envelope protocol is not able to provide any evidence that authentic votes from only eligible voters are accurately included in the respective election results and to verify this by means that are independent from the e-voting system as required by SD 17 and SD 18 of the recommendations. Once voting has ceased and the votes are to be counted, the inner and outer envelopes are split. The inner envelopes that contain only the encrypted votes are then burnt on a DVD and decrypted and counted on a separate server. It is at this point, where there is true anonymity in terms of who voted for whom. There is no way at this stage to check that the voter's vote has been included in the election results, for there is no connection between the voter and the vote itself and no way to ascertain that connection without using the original e-voting server containing the original file where the inner and outer envelopes where still bound. In this way, the recommendations have not and cannot be fulfilled using the envelope protocol. Furthermore, the files with the inner envelope could be swapped during transportation from one server to another, and hence the election manipulated. There would be no way to detect manipulation without using the original e-voting server nor to check if any one individual vote had been included in the election results. It is because the inner envelopes are completely anonymous, that make the votes unverifiable. An independent recount is also not possible without compromising anonymity. SD 18, that is to provide "sound evidence" that the eligible voters' votes has been included in the final result, is also not possible for the same reasons. This protocol can only provide verification that the vote has entered the ballot box (VSS), not if it has been included in the final tally. There is no end-to-end relationship that is, voter to tally, of any form.

It should be noted that in contrast to SD 15, SD 17 and 18 only provide a vague passive voice recommendation: "The e-voting system shall provide sound evidence …" instead of as in SD 15 demanding that "The voter shall be able to verify that …". Hence, one may argue that only SD 15, which is limited to requiring verifiability that the vote accurately reached the ballot box, is subject to verification by the voter, whereas the more far reaching criteria SD 17 and SD 18 which require verifiability that the eligible voters' authentic votes are included in the final tally only require unspecified "sound evidence" of verifiability. However, the only way to reproduce the tallying procedure is to take SD 15 voter-verifiable ballot box and subject it to a recount by an independent authority. This however, as we will see below (4.4. Secret suffrage), may seriously compromise voter secrecy.

4. Token-based Protocols

4.1. General Overview[6]

The token protocol is a two-staged process. The first stage is to attain a valid, signed Voting Card, which allows the voter to at any stage during the voting period to cast a vote. The second stage is to vote via an electronic ballot sheet using the Voting Card attained in the first stage, as the only means of authentication, which is the deciding factor in making the voter, anonymous.

[6] For a detailed description of the token protocol see, Prosser & Müller-Török [9]

4.1.1. Stage 1

The voter first identifies himself to the election system. This can be done by any current means of identification. The voter client generates a very large random number as token and submits it to the election system for a blind signature. The blind signature gives an authentic signature on the token, nevertheless the server never sees the token it signs.[7] In everyday terms this could be seen as signature of a document in a sealed envelope lined with carbon paper. The signor signs on the sealed envelope without ever seeing the content of the envelope. Nevertheless, it is an authentic signature that is imprinted on the sealed document via the carbon paper.[8]

The same process can be repeated with one (or several) election observers, eg. an OSCE or Council of Europe Server System, each adding another signature to the voting card, so all observers sign the original token. At the end of the first stage, the voter has a voting card VC=[t, t^d] validly signed by the election system (and possibly observers VC=[t, t^d,t^δ] with their asymmetric keys (ε,δ,μ)).

If several constituencies have to be served, the server maintains a key pair (e,d,m) per constituency and the constituency C is added to the VC = [t, $t^{d(C)}$,t^δ, C].

A meaningful implementation of the protocol will of course enable symmetric (password-based) encryption of the VC, for instance with AES [9] to prevent possible misuse of the voting card. This of course also means that if the voter forgets the password for encrypting the VC, the vote is lost.

4.1.2. Voting

During the voting stage the voter sends in his Voting Card (VC) via a web site or app using his VC as the only means of identification. After successfully checking whether the VC has already been used and whether the signature/s of the election system (possibly specific to the constituency indicated) and observer/s are correct, the ballot box server returns the ballot sheet, which is then filled in by the voter.

The voting client cryptographically concatenates the VC and ballot in a way that the link cannot be broken afterwards and submits this as the vote. If an election system allows multiple (replacement) votes, the voter may use his VC multiple times. Each time the new vote replaces the existing vote/s already submitted under the same token.

4.1.3. Counting

The votes in the ballot box are already anonymous, and are only validated by a correctly signed VC to which they are concatenated. Counting therefore involves the following steps:

---

[7] The election system has an asymmetric key pair (e,d,m, the paper uses standard notation for public key cryptography, for an introduction see [9]), of which after successful identification it sends back the public key (e,m) to the voter's client system. The client system (typically a Java applet or app) generates two very large random numbers, r (which will serve as a "pad") and t (the token). It computes $x=r^e.t$, which it sends to the server, which due to the padding does not "see" the t it is supposed to sign. The server sends back x^d. The client "extracts" the signed token by computing $x^d/r = t^d$. This calculation can easily be shown by expanding x: $(r^e.t)^d/r = (r^e)^d.t^d/r = t^d$. The client then concatenates the voting card VC = [t, t^d]. Note: All calculations are of course done modulo m, the modulus of the election system's key pair (e,d,m). For ease of exposition the modulus has been omitted.

[8] Consider r^e to be the carbon paper.

(i) Validating the concatenation of VC and ballot sheet;

(ii) Checking the signatures of election system and observer/s on the VC according to their public keys (e,m) and that the token was used only once; and

(iii) Checking the ballot[9] and including it in the tally.

4.2. Independent Recount

Since the ballot box does not contain any data that identifies the voter it can be disseminated to other authorities for an independent recount without compromising voting secrecy. Literally, *anybody* may perform the above steps, once the ballot box has been made available.

4.3. Individual Verifiability

The ballot box line items, that is the VC and ballot, may also be published on a web site, possibly segmented into constituencies. Each voter can then individually check that his vote entered the tally correctly by searching the web page for his token, t. The same list also enables to check the validity of the token signature/s t^d, t^δ and the concatenation with the ballot. Since the token is used by the voter, he does not compromise voting secrecy in checking his vote.

This list therefore combines individual verifiability by the voter and collective verification of the entire result. The system indeed offers a much higher degree of transparency of the result than conventional voting procedures.

5. The Protocols in context

5.1. Equal Suffrage

Dimension (i) and (ii), that of: the unique identification of voters; and the granting of access to only authenticated voters, corresponding to SD 7 and SD 8 respectively, are standard building blocks of any evoting system and are independent of the evoting protocols' functionality. Ensuring that only the appropriate number of votes per voter are stored in the ballot box and included in the final count, SD 9, dimensions (iii) and (iv), applies to elections, where replacement votes are a requirement, opposed to a referendum. Both the envelope and the token protocols are able to accommodate for this functionality providing the last of the replacement votes are reliably selected for the tally.

5.2. Individual Verifiability

Verification that the voter's intention is accurately represented by the vote and the sealed vote has entered the ballot box without being altered, dimension (i) and confirmation to the voter that the vote has been cast successfully, dimension (ii), corresponding to SD 15 and 16 respectively, ensure

[9] Checking the ballot includes checking that the voter has submitted a vote. It may be a requirement by the election law that the electronic media allows voters to submit an invalid vote, whether by mistake or as an intentionally invalid vote, in order to treat paper and electronic voting in an equal way. SD 13 of the Recommendations states that "the e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options." [2]

verifiability only in the voting stage of the election process, but does not ensure verifiability for an individual voter that his or her vote has been included in the election results. Hence a third dimension is necessary, namely that an individual voter can verify that his or her vote has been included in the final election results. Please note that according to the SD 15, and 16 individual verifiability only extends to the ballot box but does not include the final tally and therefore any misdemeanour between the vote entering the ballot box and computation of the final tally would not be covered by the recommendations and represents a breech in voting security. General verifiability, however, covered by SD 17 and 18, do encompass the final election results, but not verifiability for an individual voter, therefore a voter' right to check that his or her vote has been accurately included in the final election results is not ensured by the recommendations as shown below in Figure 2.

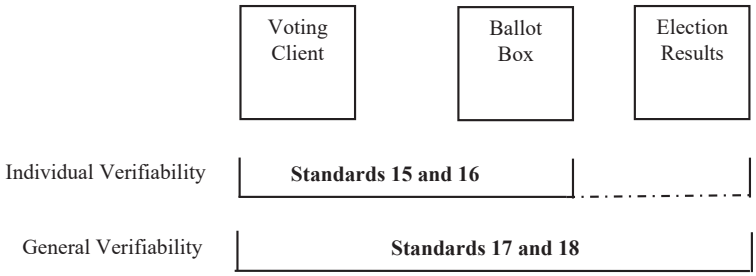

Figure 2. Standards and their verifiability

The token protocol enables the voter to verify that his or her sealed vote has been accurately entered into the ballot box and additionally, enables the voter to check that his or her vote has been included in the election results, while maintaining voter secrecy at all stages of the election process. The envelope protocol, however, is unable to allow an individual voter to check that his or her vote has been included in the final results.

5.3. General Verifiability

In the token protocol general verifiability is achieved by publishing a list of the tokens, their blindly issued digital signature by the election authority and by the observer/s, if observers are used in the election or referendum, the vote and the concatenation information between the authenticated token and the vote and therefore there is a complete audit trail which enables the following verifications:

a. Each token entered the tally once;

b. Each token is properly authenticated by the election authority and, if used, by the observers;

c. Each vote is concatenated with a valid token;

d. The vote count published by the election authority can be reproduced with this published list and therefore be verified; and
e. Comparison between the number of authenticated tokens and the number of tokens issued by the election authority and the observer/s ensures that no tokens/votes have been suppressed.

The Envelope protocol, however, does not enable publication of the ballot box data because this would mean to compromise voting secrecy for the entire electorate. If, on the other hand, only the

individual votes are published, it is not possible to verify whether these votes represent a "legitimate" voters' decision. Therefore, "verification" using the envelope protocol is to simply count a list of published votes, without being able to individually identify votes from one another and hence does not represent a complete audit trail, which is needed to "provide sound evidence", SD 17 and 18, that free suffrage has been ensured.

5.4. Secret suffrage

SD 25 requires that replacement votes be identified in the ballot box. In the envelope protocol the identifying property is the voter ID, which remains linked to his or her vote stored in the ballot box. It is not until counting that the Voter ID is stripped away, leaving only the vote itself. However, this creates a security breech because votes could easily be inserted and there would be no way to discern corrupt votes from authentic votes. In the token protocol the identifying factor is the anonymised yet authenticated token. SD 25 and SD 26 are fulfilled by the envelope protocol system, however at the cost of compromising voter secrecy, because the Voter ID is intrinsically linked to the vote. Relating to the protocol itself, it cannot be said that the envelope protocol fulfils SD 19, that is that the protocol ensures voting secrecy at all stages. The entire protection of voting secrecy relies on the fact that nobody possesses the votes containing the outer and inner envelope as they are stored in the ballot box, and the private key of the election committee. So voter secrecy hinges on organisational security measures. The token protocol, however, does ensure voting secrecy at all stages of the voting procedure in accordance with SD 19 and fulfils SD 25 and 26.

5.5. No premature disclosure of results

SD 19 and 26 using the envelope protocol cannot possibly be fulfilled. The ballot box for each vote contains the following information: Voter ID, digital signature of the voter and the ballot. Voting secrecy in these protocols is achieved by "separating" the voter information from the ballot. Although this may work fine in the physical world where once a ballot sheet is taken out of a paper envelope, it is not in the paper envelope anymore because the physical ballot sheet exists only once, but this is not necessarily true in the digital world. In the digital world systems are backuped regularly. There are tape backups, backup buffer files, mirrored databases and virtualised server structures, all to ensure the integrity of the data and the operation of the system. It cannot be guaranteed that the data in the ballot box exists just once at any one time without compromising basic computer system functionality.

In the case of the envelope protocol, is true that the vote is encrypted with a private key of the election committee, which is applied to the ballot only after the separation, however, if the ballot box in its original state, and the private key of the election committee, are brought together, voting secrecy can be compromised for the entire electorate in an automated way. This is also the reason why independent and external recounts are highly problematic, because they would require to hand over the ballot box and the private election key to a third party. It is hence, impossible to implement SD 17 and 18 without severely compromising SD 19, 25 and 26. These two groups of standards for envelope protocol are mutually exclusive. The token protocol, however, do not have these pitfalls as the ballot is already anonymised at the very point in the time it enters the ballot box and that is why the ballot box can be easily handed over to third parties and/or published.

5.6. Anti-coercion

Anti-coercion is a general issue with every form of distance voting including postal voting. It could be said that there is no form of distance voting generally that can fulfil this requirement. There is a clear goal antinomy between any form of individual verifiability and the requirements of SD 23, namely not providing the voter with proof of a vote cast. This is outside the control of the protocol design capabilities. A legislator enabling remote voting, whether on paper or digitally, must be aware that voter coercion, such as family voting and vote buying and the like, is impossible to avoid. There are many ways one can provide proof to third parties of a vote cast and this can be as simple as video taping a vote being cast with a mobile phone. There must be a point where voters take responsibility for their right to free suffrage and if there is a problem, to take action to report it. We can programme secure systems to as far as possible protect voters rights to free suffrage but the public itself must ultimately embrace that right.

6. Conclusion

CM/Rec (2017)5 effectively creates a watershed between voting protocols, depending on whether anonymization happens before or after the vote is submitted to the electronic ballot box. Envelope protocols are good examples for anonymization after that point and it remains doubtful whether given the requirements of CM/Rec (2017)5 they are still viable for they cannot fulfil the requirements of the council of Europe. Token-based protocols have the potential of anonymization before the submission of the vote, which means the ballot box is subject to external verification without compromising voter secrecy.

7. References

[1] Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

[2] Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

[3] MAATEN, E., Towards remote e-voting: Estonian case in A. Prosser and R. Krimmer (eds), Electronic Voting in Europe – Technology, Law, Politics and Society, GI-Edition, Lecture Notes in Informatics, p. 83-90.

[4] https://www.valimised.ee/sites/default/files/uploads/eng/Verification_of_I-Votes.pdf

[5] https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf

[6] https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf

[7] SPRINGALL, D., FINKENAUER, T., DURUMERIC, Z., KITCAT, J., HURSTI, H., MACALPINE, M., HALDERMAN, J. A., Security Analysis of the Estonian Internet Voting System https://jhalderm.com/pub/papers/ivoting-ccs14.pdf,

[8] https://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf

[9] PROSSER. A., MÜLLER-TÖRÖK, R., E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess, in Wirtschaftsinformatik 44 (2002) 6, p. 545 – 556.

[10] Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, download from https://search.coe.int/cm/Pages /result_details.aspx?ObjectID=090000168071bc84

[11] Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, download from https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b