DOI 10.5817/MUJLT2020-2-6

COUNCIL OF EUROPE RECOMMENDATION CM/REC(2017)5 AND E-VOTING PROTOCOL DESIGN

by

ROBERT MÜLLER-TÖRÖK[*], DOMENICA BAGNATO[**], ALEXANDER PROSSER[***]

The Corona pandemic has created a push towards digitization in a number of fields, not least in the public sector including democratic processes. This of course includes an increased interest in e-voting via the Internet. The Council of Europe has a long-standing history of work in the field including two Recommendations – (2004)11 and (2017)5 – which have become the de facto yardstick against which every e-voting system is measured. Rec(2017)5 builds on a decade of experience with e-voting and particularly strengthens two concepts important in any electronic voting system: Voting secrecy and auditability/verifiability. This has distinct implications for the design of e-voting protocols.

The aim of this paper is to analyse the impact on what arguably are the most popular voting protocol families, envelope and token protocols. How does the modified Recommendation impact on the viability of protocols and protocol design? The paper first presents the Council of Europe Recommendation and the technical issues it addresses. Then a model is introduced to assess a voting protocol against the Recommendation; a typical envelope and a token protocol are assessed in view of the model and finally the two assessments are compared including policy recommendations for a path to e-voting implementation.

[*] mueller-toeroek@hs-ludwigsburg.de, University of Public Administration and Finance Ludwigsburg, Germany.

[**] domenica.bagnato@hierodiction.com, Hierodiction Software GmbH, Austria.

[***] alexander.prosser@wu.ac.at, Vienna University of Economics and Business Administration, Austria.

KEY WORDS
Council of Europe, Envelope Protocol, e-Voting, Token Protocol, Voting Principles

1. THE COUNCIL OF EUROPE AND ITS E-VOTING RECOMMENDATIONS

On the 30th of September 2004, the *Council of Europe* passed the *Recommendation for electronic voting, Rec(2004)11*[1]. It was the first attempt to define requirements for e-voting systems, which also includes remote voting and voting machines. Some points listed in the recommendation would prove to be irrelevant to the practical implementation for e-voting systems as they were of rather general nature equally concerning all voting channels and methods.[2] Yet it was the landmark attempt to define the legal, operational and technical standards an e-voting system has to follow (Appendices I–III). *The Explanatory Memorandum to Appendix III* on the technical standards was couched in *Common Criteria (CC)* terminology; CC is a global standard for the security evaluation and certification of IT systems.[3] Clear reference to CC terminology and structure indicates that the *Council of Europe* intended the Recommendation to become the basis for e-voting system certification.

Building on a decade of practical experience of e-voting, *CM/Rec(2017)5*[4] provides an update that equally applies to voting machines and remote (typically internet) voting. This paper uniquely focusses on the latter. It has to be noted that there is no such thing as "e-voting", but that there are many systems in place, which also follow vastly different protocols and algorithms. It also has to be understood that the correct and meaningful

---

1 Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, 30 September 2004. Available from: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf [Accessed 16 June 2020].

2 Example includes, *"Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting"*, ibid, Appendix I, A. 2.; *"E-voting systems shall prevent any voter from casting a vote by more than one voting channel"*, ibid, A.6.; *"The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting"* , ibid, Appendix III, 12.

3 Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC(2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May.

4 Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM/Rec(2017)5), p. 2. Available from: https://rm.coe.int/0900001680726f6f [Accessed 17 April 2019].

software implementation of the protocol has to be considered as well.[5] This paper focusses on the *protocol design* (not the intricacies of software implementation) of e-voting systems in view of the Recommendation.

After the release of the 2004 Recommendation several e-voting projects in European countries failed, including Austria,[6] United Kingdom[7] and Finland,[8] which led to a general feeling that more stringent recommendations were needed. The main issues surrounding the failed elections could be summarised as a lack of reproducibility, audibility, general verifiability, transparency, and voter secrecy. In the Austrian student elections 2009, the election committee was unable to perform its duties because electronic election data had been destroyed and there was no means to verify the election results. In Finland, electronic votes went missing, which clearly indicates a lack of audibility. In the UK, votes were manually edited in clear text to fit into the counting application[9] and the election committee could not follow the procedures for opening the ballot box and counting the votes. Furthermore, undocumented data transfers during an ongoing election were observed.[10] These and similar events clearly necessitated a new and more stringent Recommendation.

On the 14th of June 2017, the *Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting* and an explanatory memorandum[11] and guidelines[12] were passed. We hold that

---

5 Prosser, A. and Müller-Török, R. (2009) E-Voting: Lessons Learnt. In: Kaplan, B. and Aktan, D. (eds.). *International Conference on eGovernment and eGovernance*, Ankara, pp. 265–280.

6 Constitutional Court. (2011) V 85-96/11-15, 13 December.

7 Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

8 Karhumäki, J. and Meskanen, T. (2008) *Audit Report on Pilot Electronic Voting in Municipal Elections*. University of Turku, Turku.

9 Actica Consulting. (2007) *Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0019/16192/Actica_Rushmoor_27248-20137__E__N__S__W__.pdf [Accessed 31 May 2018].

10 Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

11 Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM(2017)50-add1 final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168071bc84 [Accessed 17 April 2019].

12 Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, 14 June 2017 (CM(2017)50-add2final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726c0b [Accessed 17 April 2019].

the Recommendation, for the most part, streamlines requirements for e-voting in the context of the practical application of an e-voting system, particularly in the field of voter secrecy as well as (individual and collective) verifiability.

2. COMPARATIVE ANALYSIS OF REC(2004)11 AND CM/REC(2017)5

The relevant recommendations that relate to the technical core functioning of e-voting are found in Appendix I, standards 1–26 of CM/Rec(2017)5. First and foremost, the document has been streamlined with the number of standards being reduced from 112 to 49. Below are a number of standards that were added to or expanded in CM/Rec(2017)5 as compared to the 2004 recommendation.

1) Defining the way in which voting information is to be presented. In terms of the user interface, this recommendation is crucial. Official voting information is to be presented in an equal way across voting channels [CM/Rec(2017)5, 5][13]. This may lead to unexpected results: Catering, for instance, for persons with disabilities, such as the visually impaired, by supporting a screen reader would mean that the way information is presented needs to be changed to make it accessible and this breaches CM/Rec(2017)5, 5. Furthermore, an e-voting system cannot reasonably be seen to maintain voter secrecy under these conditions and hence poses a security breach.
2) The voter registry and its requirements for e-voting is not controlled by the e-voting system, hence Rec(2004)11, 2 was rightfully omitted. CM/Rec(2017)5 expanded its requirements to enforce that the system authenticate a person as having the right to vote [CM/Rec(2017)5, 8] before accessing the e-voting system. This was indirectly addressed by Rec(2004)11, 80 and 94 but has been reworded to specifically apply to the voter.
3) The function of an electronic ballot box differs considerably to that of the physical ballot box in traditional voting. The electronic ballot box stores votes cast, including redundant votes created

[13] In the following, CM/Rec(2017)5, x refers to Standard x of the Recommendation. The same applies to Rec(2004)11. In accordance with *Council of Europe* practice we equally use CM/Rec and Rec.

through the voter's right to cast a vote up to an arbitrary number of times. During the vote-counting stage, the system sorts the votes discarding redundant votes and counts only the last vote cast per voter, irrespective of how many times a voter voted and includes only that last vote in the final election results [CM/Rec(2017)5, 9].

4) The e-voting system is required to alert the voter if he or she attempts to cast an invalid vote, giving the voter the option to cast a valid vote [CM/Rec(2017)5, 14]. This however means that "paper voters" and electronic voters are not treated the same way, as such an alert does not exist for postal or paper-based presence voting.
5) A requirement that presents itself in the 2017 recommendations is the need for collective verifiability in that each vote is accurately included in the election results and it must be verifiable independently from the e-voting system [CM/Rec(2017)5, 17 and 18].
6) The voter shall be able to verify that his or her intention is accurately represented in the vote [individual verifiability, CM/Rec(2017)5, 15]. Please note that individual verifiability reaches until the vote enters the ballot box and general verifiability reaches until the election result.
7) E-voting system stores only personal information that is necessary to conduct the election [CM/Rec(2017)5, 20]. Depending on the protocol, very little personal information is needed, because the system only needs to identify the user as having the right to vote, possibly assign a constituency (if any) and record that the user has voted at least once.
8) The recommendation on the confidentiality of the voter's register has been expanded slightly to allow for accessibility by authorised parties [compare Rec(2004)11, 78 and CM/Rec(2017)5, 22].
9) The 2004 recommendation did not take into account the possibility for a voter to vote several times and so the 2017 recommendations has included this requirement. It asks that

"E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected"

in CM/Rec(2017)5, 25. However, here the standard does not accurately correspond to the technical functioning of an e-voting system for no vote/choice is erased by the system, if it is to be secure and auditable. The previous choices are not included in the final election results but they are stored in the ballot box and nobody has the right to erase or change a vote cast at any stage of the election process for this would be a clear breach of security, cf. CM/Rec(2017)5, 24.

The essence of the improvements can be summarised by verifiability, Standards 15, 17, 18 and a strengthening of voting secrecy, Standards 19, 20, 25 and – most prominently – 26, with some emphasis on usability, recommendations 5 and 14.

3. HOW TO MEASURE AN E-VOTING SYSTEM'S VIABILITY

An e-voting system is defined by the protocol it implements. The protocol is the basis for its core functionality and determines to what extent the system will be able to fulfil the requirements of CM/Rec(2017)5. The first step is to define the dimensions and then to assess the extent to which an e-voting protocol fulfils the dimensional requirements. Using the recommendation of the *Council of Europe*, CM/Rec(2017)5, the following dimensions can be distinguished:[14]

A. Equal suffrage:

   1. The unique identification of voters [CM/Rec(2017)5, 7];
   2. Access granted only to authenticated voters [CM/Rec(2017)5, 8];
   3. Only the appropriate number of votes per voter are stored in the electronic ballot box [CM/Rec(2017)5, 9].

B. Individual verifiability includes:

   1. 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 [CM/Rec(2017)5, 15];

[14] This section builds upon the general modelling method introduced in Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

2. Voter confirmation that the vote has been cast successfully [CM/Rec(2017)5, 16].

C. General verifiability includes:

1. Sound evidence must be provided, *"that each authentic vote is accurately included in the* [...] *results"* and be independently verifiable from the e-voting system [CM/Rec(2017)5, 17];
2. Sound evidence must be provided that *"only eligible voters' votes have been included in the* [...] *result"* and be independently verifiable from the e-voting system [CM/Rec(2017)5, 18].

It should be noted that B and C cover protection against manipulation,[15] however distinguishes between the type of verification following the systematisation in CM/Rec(2017)5.

D. Secret suffrage includes:

1. Ensuring the secrecy of previous voting choices made by the voter before issuing his or her final vote [CM/Rec(2017) 5, 25];
2. Anonymity of votes, notably that the unsealed vote and the voter cannot be linked during counting. [CM/Rec(2017)5, 26];
3. Ensuring *"that the secrecy of the vote be respected at all stages of the voting procedure"* [CM/Rec(2017)5, 19].

E. Anti-coercion:

1. Not providing the voter with proof of the content of a vote cast *"for use by third parties"* [CM/Rec(2017)5, 23].

F. No premature disclosure of election results:

1. Secrecy of the number of votes for any voting option is to be maintained until after the closure of the electronic ballot box. [CM/Rec(2017)5, 24].

[15] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

Each of these dimensions may be protected by purely organisational or by technical means. The former means separation of control, data access restrictions in an application, usage of certified personnel, legal provisions etc. Organisational protection ultimately relies on people playing by the book; it relies on the fact that not a single individual or coalition of individuals may break the security of the system. Technical protection typically means cryptographic security that cannot be broken by any coalition of actors.[16] Therefore, the level up to which each of the above dimensions A–F is protected by technical means indicates a security frontier for an e-voting system.

It has to be understood that at some stage, organisational protection must be employed, there can be no 100 % technical security. However, the question is, when the organisational safeguards are needed. Two dimensions appear to be relevant in this context; both concern a violation of Dimensions A–F above (in a generalised way referred to as "violation" below):

1. How many votes may be violated by organisational means?

    a. The entire election (as far as conducted electronically);
    b. The content of one (virtual) ballot box, i.e. a ward;
    c. A single vote.

2. Who can violate successfully?

    a. A single person in whatever capacity ("hot" candidates would be a system administrator or members of the election committee);
    b. A coalition of persons without the voter, e.g. the election committee in its entirety;
    c. A coalition including the voter/s concerned.

Let us assign levels 1 to 3 to combinations of the two violation dimensions in as far as the e-voting system does not provide *technical* protection (for which organisational protection must apply). We operate

[16] Here we disregard the fact that over time key lengths may become obsolete and may be broken. This risk may be minimised by using cryptographic keys with a sufficiently large "buffer time" until their length becomes obsolete.

under the assumption that there is one (logical) electronic ballot box per ward, which is controlled by one election committee.

	How many votes?			
		Entire ward	Single vote	No vote
How many actors?	Single actor	1	1	3
	Coalition w/o v.	1	2	3
	Coalition /w v.[17]	2	2	3

Table 1: Levels of manipulation that the technical safeguards of the e-voting system allow

"Violation" in this context means the undetected (hence successful) and directed violation of any of the Dimensions A–F. *Detected* violation of a dimension does not count as violation in the above systematization as it may entail an enormous backlash including repetition of the election but does *not* imply the successful violation of the dimension and the underlying election principle. To assign a value to the dimension, the first line in *Table 1* (single actor) is analysed. If a single actor can violate the dimension for the ward or a single vote, a value of 1 is assigned to the dimension and the analysis of the dimension stops; otherwise ("no vote" in line one), line two (coalition of actors without a voter, e.g. the election committee or a subset thereof) is analysed the same way; if it also yields "no vote", line three is analysed. An example: Assume that Dimension D (voting secrecy) is completely (technically) protected against single actor violation and that a coalition without the voter can violate the dimension for the entire ward: Line one yields a value of 3, hence line two is analysed, which yields a value of 1 for the dimension and the analysis stops. This procedure is repeated for all dimensions. Summarising, *Figure 1* presents a model for mapping the resulting security frontier following a systematisation proposed by *Prosser*.[18] There are Dimensions A to F and values of 1 to 3 in each dimension.

Remark: The interested reader is invited to insert his or her own classification in the above systematisation. The model is also flexible enough to include additional or fewer dimensions or to provide for a finer distinction, for instance with a defined subgroup of votes cast in a ward

[17] Meaning with all the respective voter/s concerned.

[18] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2), pp. 171–184.

as additional level of compromising votes. The values in *Table 1* represent our take of the severity of violations and will be suitable for the following discussion of the two protocol families.

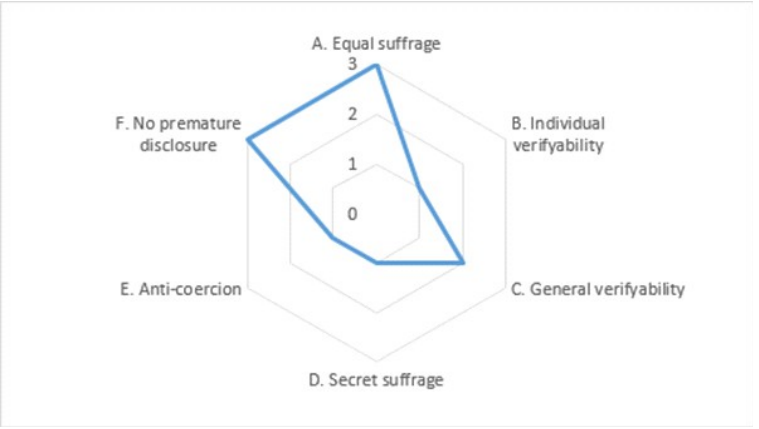

Figure 1: Model of the aims of an e-voting system – hypothetical example

The hypothetical system depicted in *Figure 1* provides high protection of equal suffrage, for instance by using a citizen card for voter identification and cryptographic protection for the data link between voter and constituency assignment. Individual verifiability is on a low level, for instance, a single person could fool voters into believing that their vote reached the ballot box correctly, where in fact it was altered. General verifiability is on a medium level, for instance the election committee of a ward could collude to provide a false audit trail for the correctness of the result of their ward with respect to an individual vote. Protection of voting secrecy is minimal, again a single person could break it for a ward. Anti-coercion protection is equally minimal, vote buying by a single person would effectively be possible. Premature disclosure of results however, has the highest protection level.

We hold that this model is (i) useful to quickly map the abilities of a voting protocol in view of the requirements set out in CM/Rec(2017)5 and (ii) flexible enough to be adapted and/or refined to more specific needs in this regard, for instance selection of an e-voting system in a tendering procedure.

4. TRADE-OFFS

4.1. INDIVIDUAL VERIFIABILITY AND WAYS TO DETER VOTE BUYING

The CM/Rec(2017)5, 19, recommends the secrecy of the vote be respected at all stages of the voting procedure. However, this presents a conflict with CM/Rec(2017)5, 15, which requires that the voter be able to verify the vote and verify that the vote has entered the ballot box without alteration. Finally, CM/Rec(2017)5, 23 contrasts in that

> *"An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties".*

It becomes evident that these requirements create two goal conflicts, that of individual verifiability versus anti-coercion and individual verifiability versus secret suffrage. These conflicts have been realised very early on.[19] It should be understood that individual verifiability may create conflicts in terms of voting secrecy, for in order to verify the vote cast, the voter would need to receive confirmation of the actual vote cast to validate its correctness; this could be checked by a third party buying the vote or coercing the voter. However, this equally applies to postal voting.[20]

However, on a very general level, it is not possible to stop voters from recording in some format their vote; this also applies to polling booth voting as well. The moment a voter has the ability to check the authenticity of a vote, voter secrecy is compromised paving the way for voter coercion. Voter buying relies on proof in some format that the vote cast is the vote that was bought. In this light, measures could be taken in terms of system procedures that would question the authenticity of the vote recorded for use by third parties, by allowing only the ability to verify a vote when having the option to change it. So, one could never be sure if the verification recorded by the voter for use by third parties was the final vote actually cast or not.

The *Explanatory Memorandum to CM/Rec(2017)5* in relation to Standard 23 of the recommendation outlines concerns where voter secrecy could be

---

[19] Cf. Cohen, J. and Fischer, M. (1985) A robust and verifiable cryptographically secure election scheme. In: *26th Symposium on the Foundations of Computer Science*, October 21–23, IEEE, pp. 373–382.

[20] Müller-Török, R. (2019) The Principles Established by the Recommendation CM/Rec(2017)5 on Standards for E-Voting Applied to Other Channels of Remote Voting. *Masaryk University Journal of Law and Technology*, 13 (1), pp. 3–26.

compromised. From this list, compromised voting secrecy could be summarised:

1. Through some form of remote access to computers via the internet such as a computer virus to collect and record voter transactions;
2. The voter physically breaches voter secrecy by using some means to create a copy of the vote and distribute it.

It is very difficult to control every aspect of remote voting particularly internet connected computers and although the ability to disable printing and print screen functionalities, erasing user interaction through input and output devices such as keyboards, mice and screens, can be realised. Ultimately it is up to the voters to take responsibility for the security of their computers and in doing so voter secrecy. The same applies to postal voting, where the ballot should perhaps also not be filled in in public.

It must be understood that if one can see the vote, one can record the vote and the voting process via devices that are not physically connected to the voting device, such as photographing the screen and video recording the entire procedure. The same applies to paper-based voting, whereby, for instance, in Austria it is perfectly legal to take a photo of one's own vote and post it on social media.[21] At this stage, it is not possible to prevent this from happening, but to focus on defining e-voting procedures making vote buying or coercion more difficult. Here some technical suggestions we find useful from an implementation perspective:

1. Deter photographing and printing of votes, enable multiple vote casting

   Enable multiple voting, something that is impossible to realise in postal voting procedures. Furthermore, in voting multiple times, there should be no indication on the screen of the voting device as to how many times the voter has voted. Even if the voter took a photo of the screen or even a screen shot and printed it out to validate his vote, the information displayed should not give the viewer any indication as to whether the vote displayed is

[21] Pichler, G. (2019) Darf man seinen ausgefüllten Wahlzettel auf Instagram teilen? *Der Standard*, 25 May. [online] Available from: https://www.derstandard.at/story/2000103646954/darf-man-seinen-ausgefuellten-wahlzettel-auf-instagram-teilen [Accessed 16 June 2020].

the final vote cast. This would at least provide doubt as to the authenticity of the final vote shown to a third party.

2. Deter recording the voting process

   When recording the entire process via video camera for example, restrictions can be set requiring that before changing a vote, the voter must wait a certain number of hours before being allowed to change the vote, making the recording process difficult and tedious at best and the authenticity of the proof provided by the voter would still be questionable.

3. Deter bulk voting

   Restrictions could be placed on how many voters can access the voter registry and/or actually vote from any one computer or device. This could be done by recording the (physical) MAC address of the PC or device, separate from any identification information of the person voting. This would deter people from buying the right to vote on behalf of voters by having bought the identification needed to register and then voting for a group of people from any one PC. Also, this would be a huge improvement as compared to postal voting.[22]

4.2. SECRET SUFFRAGE VS. EQUAL SUFFRAGE

A system perfectly gauged to protect equal suffrage can be built but it would completely denigrate voting secrecy. An example would be the Austrian electronic citizens' initiative system, where supporters of a citizens' initiative sign with their electronic signature cards.[23] In contrast to hand-written signatures, these signatures can be reliably verified. Voter secrecy is not an issue here, as it is a citizens' initiative.

[22] Cf. the horrendous number of bulk voting cases documented in the U.K., cf. White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library, and a recent case in Germany, cf. Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhöring*. [press release] 15 October. Available from: https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php [accessed 2 November 2018], all involving bulk postal voting.

[23] Stein, R. and Wenda, G. (2014) Das Zentrale Wählerregister – Ein skalierbares Instrument zur Bürgerbeteiligung mit 1:1-Verifikation. In: Plodereder, E., Grunske, L., Ull, D. and Schneider, E. (eds.). *44. Jahrestagung der Gesellschaft für Informatik.* INFORMATIK 2014, 22–26. September, Bonn, pp. 1427−1436. [online] Available from: https://subs.emis.de/LNI/Proceedings/Proceedings232/1427.pdf [Accessed 16 June 2020].

The essence of every e-voting protocol is to balance secrecy and reliable identification, which are clear trade-offs there.[24]

In the following sections, two voting protocol families are discussed with a view to the Recommendation and the security model in *Figure 1*. They can be distinguished by one "watershed" property, that is when the anonymization of the vote takes place – before or after the vote is put in the electronic ballot box.

5. ENVELOPING PROTOCOLS

Enveloping protocols have been widely implemented, probably because of their intuitive appeal due to the emulation of postal voting, and as an example we will take a look at the Estonian e-voting system,[25] which has been implemented in elections in Estonia since 2005.[26]

It should also be noted that the authors of CM/Rec(2017)5 due to some wording appear to have had an envelope protocol in mind when drafting the new recommendation, cf. for example Standard 15:

> *"The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box* […]*)"*;
>
> Standard 26:
>
> *"*[…] *in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter* […]*)"*;
>
> or Standard 45:
>
> *"Votes and voter information shall be kept sealed until the counting process commences"*.

[24] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics, pp. 83–90.

[25] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020] and Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J.A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[26] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics, pp. 83–90.

This is arguably due to the fact that enveloping protocols are comparatively easy to implement and have dominated the first wave of e-voting systems.

The envelope e-voting process can be split into three stages:

5.1. CASTING A VOTE

The voter authenticates him- or herself *vis à vis* the voting application using an eID. This is not part of the e-voting protocol proper.

The voter selects option/s on the ballot. The voting client selects a large random number *r* and constructs a pad from it, *pad(r)*.[27] The voter's vote and *pad(r)*, together as a "package", are encrypted using the public key of the election committee, and this creates the inner envelope.[28, 29] The voter then confirms his vote by digitally signing the inner envelope with his or her eID (digital signature card) creating a second layer known as the outer envelope.[30] The outer envelope containing the inner envelope is sent to the server and the voting client shows a QR-code containing the voter ID and *r*, 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.[31]

5.2. INDIVIDUAL VERIFICATION

To verify and/or to change the vote, the voter scans in the QR-code (that is his voter ID and random *r*) using a different device (typically a smart phone) from which he initially voted and the smart device sends the voter

---

[27] That is to ensure that even if two votes vote for the same option/s, they look different in encoded state.

[28] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin, p. 7. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[29] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 705. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[30] Cf. State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin, p. 7. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[31] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 706. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

ID to the electronic ballot box. From the ID, the ballot box identifies the vote stored in the system and sends it back. The encrypted vote as well as a list of all the possible voting options (parties, candidates or options at a referendum) are received by the smart device, which encrypts all the possible combinations for the options and the *pad(r)* with the original public key used to encrypt the vote and compares it with the voters' intended choice. If there is a match the option is displayed. This mechanism is used to verify what is in the encrypted inner envelope.[32]

5.3. COUNTING

First the digital signature in the outer envelope and whether the voter has already cast a vote are checked. Then outer and inner envelope are "separated" and the encrypted votes of the inner envelope are stored on a DVD and transferred to a separate machine that decrypts the vote using the private key of the election committee. Finally, the decrypted votes are counted.[33] *Figure 2* schematically depicts this process.

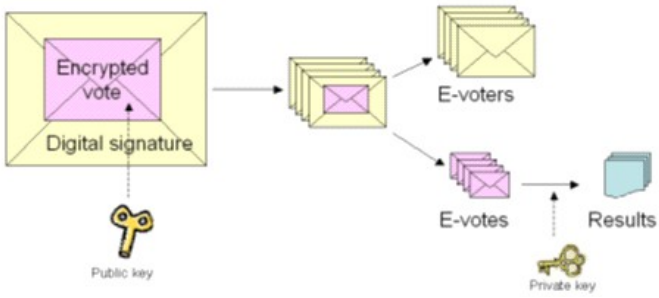

Figure 2: Envelope e-voting system[34]

[32] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

[33] Cf. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM, p. 706. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[34] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010, p. 10, Figure 2. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

5.4. THE ENVELOPE PROTOCOL AND CM/REC(2017)5

Figure 3 depicts the enveloping protocol assessment according to the model in *Table 1* and *Figure 1*:

Equal suffrage is protected if an eID is used to authenticate voters. Thereby it is readily possibly to prevent voters from illegally casting multiple votes. This ID also determines the constituency for which the vote may be cast.

Individual verifiability is implemented in a rather roundabout way with the QR code and it should be clear that in the case of complex voting schemes with a large number of preferential votes, this mechanism does not scale well.[35] However, voters may check whether the vote reached the ballot box correctly; they may not check whether the vote stays there and enters the result correctly, which however is not required by CM/Rec(2017)5, 15! Therefore, the protocol gets a full score here.

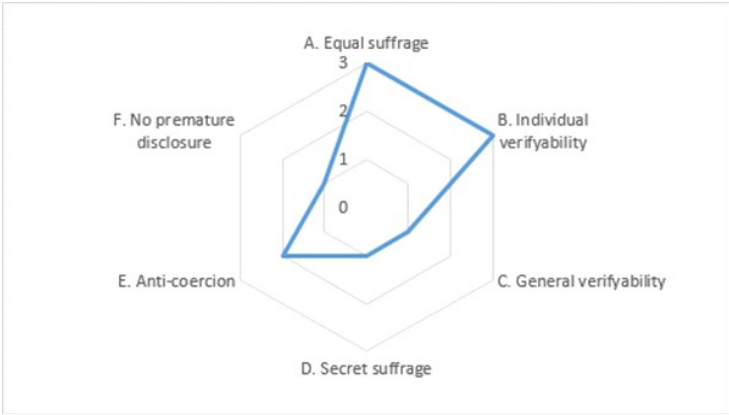

Figure 3: Enveloping protocol

General verifiability however cannot be guaranteed. The big weakness of this protocol family is that the ballot box contains the information how a voter voted (whereby the "how" is encrypted with the public key of the election committee). If the private key of the election committee and the ballot box with the votes containing the outer envelope were ever to be brought together, one could find out how every single voter voted. This could be done by a single person, e.g. a fraudulent administrator,

[35] Cf. Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC (2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May, pp. 59–69.

or a coalition without the voter, most notably a collusive election committee. This is also the reason why an independent recount is simply not possible:

- It would either mean to pass the ballot box plus private key of the election committee to an independent authority hoping that this authority does not misuse this information, or
- It would mean that the independent authority to conduct the recount gets the unsealed votes, which could also be manufactured by the election committee, part thereof or a fraudulent administrator (i.e. a single actor).

For the same reason, voting secrecy can only be guaranteed as long as the ballot box and the private key of the election committee are not joined. This has to be ascertained by organisational means. Therefore, Dimensions "general verifiability" and "secret suffrage" get the lowest score possible.

Anti-coercion is generally difficult to guarantee in remote voting procedures, electronic or paper-based, as discussed above. However, the QR code solution enables a coercer or vote buyer to check the "correct" vote. However, this is only possible for a single vote each time and involves cooperation by the voter, hence value 2 in *Figure 3*.

Premature disclosure of the ballot can be controlled to some extent by the application of the private key of the election committee, if a protocol of key decomposition is followed, where each election committee member holds a part of the key which is then assembled.[36, 37] Otherwise a single actor could apply the private key to "open" the ballots of the entire ward. However, in both cases the lowest value in *Table 1* applies.

6. TOKEN-BASED PROTOCOLS

A token protocol implements a two-staged process. The first stage is to attain a valid, signed voting card (token), which allows the voter to cast a vote at any stage during the voting period. The second stage is to vote via

[36] Cf. Blakley, R. (1979) Safeguarding cryptographic keys. In: IEEE (eds.). *International Workshop on Managing Requirements Knowledge (MARK)*, New York, 4–7 June, pp. 313–317.

[37] Cf. Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. (2004) Implementation of Quorum--Based Decisions in an Election Committee. In: Traunmüller, R. (ed.). *Proceedings of DEXA/EGOV 2004*, Lecture Notes in Computer Science LNCS 3183, Springer, Berlin, pp. 122–127.

an electronic ballot sheet using the token attained in the first stage. In the following the protocol presented in *Prosser and Müller-Török* (2002) is taken as a reference.[38]

6.1. CREATION OF THE TOKEN

The voter first identifies himself to the election system. This can be done by any current means of identification; in the context of political elections an eID would typically be used. The voting application then generates a very large random number as token *t* and submits it to the election system for a blind signature.[39] The blind signature gives an authentic signature on the token, nevertheless the server never sees the token it signs. In the physical world this would correspond to inserting a document to be signed into a carbon paper-lined envelope and sealing the envelope. The signor signs on the envelope and the signature imprints itself onto the document – there is an authentic signature by the signor, who nevertheless never sees what he signed. Blind signatures achieve this in the world of cryptography. However, in contrast to the physical envelope, the cryptographic "seal" cannot the broken. The election administration uses an asymmetric key pair (e.g. following the *RSA protocol*) of (e, d, m) with *e* being the external/public, *d* the domestic/private key and *m* the modulus.[40] The voter now has a voting card VC=[t, t^d].

The same process can be repeated with an election observer using a second RSA key pair (ε, δ, μ) adding another signature to the voting card. At the end of the first stage, the voter possesses a token validly signed by the election system and by the observer VC=[t, t^d, t^δ]. 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]. Of course, also several election observers could be used and the respective blind signatures concatenated in the token. To prevent misuse of the token

---

[38] Prosser, A. and Müller-Török, R. (2002) E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik*, 44 (6), pp. 545–556.

[39] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24 (2), pp. 84–86.

[40] RSA signatures/encryption are done in a residue class ring modulo a very large number. Hence, a key "pair" always consists of private key, public key and modulus. For an introduction, we would recommend to directly go back to the classic [see Rivest, R. L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2)]. Please note that a blind signature according to *Chaum* (Ibid) is always executed on the full text not a hash of the full text as done in open (standard digital) signatures.

it can be saved symmetrically (=password) encrypted on the local file system, for instance using AES.[41]

6.2. VOTING

VC is the only means of identification the voter uses when casting a vote. Hence, anonymization happens before the vote is inserted in the ballot box. The ballot box (server) checks the voter authentication in VC by checking the digital signature/s (t, t^d) and, if used, (t, t^δ), by applying the public keys of the election authority e[42] and the observer ε. Also, the ballot box verifies whether the token *t* has already been used. After verification the voter gets the ballot sheet of the respective constituency. The ballot sheet is filled in and inextricably linked to the VC, for instance via a hash or other concatenation methods. The entire vote is then encrypted with the public key of the election committee and submitted to the ballot box.

6.3. 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:[43]

1. Decrypting the ballots with the private key of the election committee;
2. Validating the concatenation of VC and ballot sheet;
3. Checking that the token was used only once;
4. Checking the signatures of election system and observer/s on the VC according to their public keys;
5. Checking the validity of the ballot and including it in the tally.

Since the electronic ballot box does not contain any information on the voter, it can be transferred to a third party for an independent recount. Moreover, the election authority could publish VCs and votes in a table (e.g. on a web site per ward) to enable verification containing

---

[41] National Institute of Standards and Technology. (2001) *Federal Information Processing Standards Publication 197*, ADVANCED ENCRYPTION STANDARD (AES). [online] Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 16 June 2020].

[42] Note that a voter cannot fraudulently modify the constituency as then the public key *e* of the new (modified) constituency would not work anymore.

[43] Prosser, A (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy,* 8 (2), pp. 171–184.

the authenticated voting card, the filled-in ballot sheet and the concatenation hash linking both as shown in *Table 2*.

$VC_1 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_1$	$Hash_1$
$VC_2 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_2$	$Hash_2$
$VC_3 = [t, t^{d(C)}, t^{\delta}, C]$	$Ballot_3$	$Hash_3$
...	...	...

Table 2: Publication of votes in a token protocol

6.4. THE TOKEN PROTOCOL AND CM/REC(2017)5

Figure 4 shows the degree to which the dimensions from the Recommendation are fulfilled.

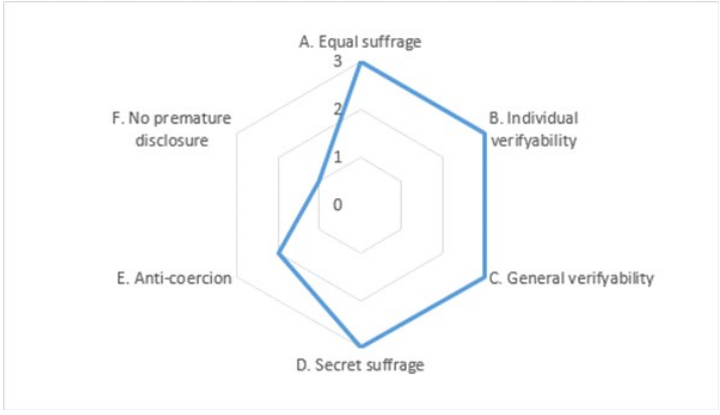

Figure 4: Token protocol score

If an eID or similar means of authentication is used, respect for the principle of equal suffrage is fulfilled; the discussion is the same as with the enveloping protocol.

The degree of individual verifiability of token systems indeed does not only fulfil the requirements of CM/Rec(2017)5, it goes way beyond. To see that consider *Table 2* and *Figure 5*. CM/Rec(2017)5 requires general verifiability as an "end-to-end" solution right to the election result. Individual verifiability, however, is only required until the ballot box, not the end result.[44] With a token protocol however, as votes are already anonymous when they reach the ballot box, the very content of the ballot box could be published on a website, probably organised by the ward

[44] Maybe having an envelope protocol type in mind, where such end-to-end individual verifiability would indeed be unthinkable.

to enable easier access by the voters. For each vote in the ballot box, VC, vote and concatenation information is published as depicted in *Table 2*. The voter can now readily access the web site and search for his or her token and verify, whether it entered the tally correctly. This can be done without compromising voting secrecy only using the token as a means of identifying the vote.[45] In this context token protocols reach a degree of individual verifiability that is not only higher than that of postal voting, but also than that of conventional polling station voting.

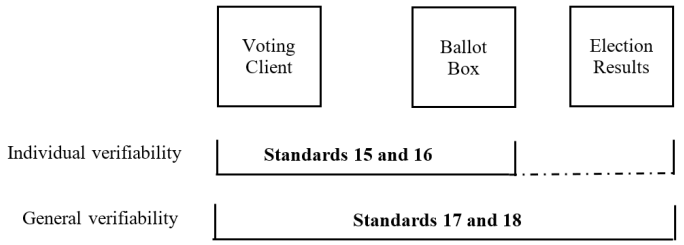

Figure 5: Individual vs. general verifiability in Rec(2017)5

In this list of published votes, individual verifiability is the "row-wise check" each individual voter can perform. General verifiability would be the "column-wise check" verifying all votes in the ward published with the following verification steps:

a. Each token entered the tally once;
b. Each token is properly authenticated by the election authority and, if used, by the observer/s;
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;
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 or inserted.

In contrast to envelope procedures an independent recount is possible because publishing the ballot box does not contain the information how voters voted and hence does not compromise voting secrecy. Every

[45] This could be offered in a "pure" function using *Ctrl+F* search for one's token on the web site and/or with a more amenable search functionality.

organisation interested and "civil society" in general may do that with a comparatively modest cryptographic toolset being necessary. Of course, open source tools for independent recounts can also be expected to emerge. In both verifiability dimensions the score is hence 3.

Secret suffrage is protected by the fact that nowhere in the server landscape of the election system the information how a voter voted is stored. The basis of authentication is the token signed by the election authority and the observer/s. No organisational means are necessary to protect secrecy. The only time, when the system "sees" voter information and token in the same transaction, the token is cryptographically (therefore technically, not organisationally) protected by the blind signature algorithm. The token is authentically signed without the signor ever seeing the token. That is also the reason why the ballot box as well as the private key of the election committee can be passed on after the election without compromising voting secrecy.

Anti-coercion is only moderately protected as with any remote voting scheme. However, the token may be used several times to cast a vote depending on the legal framework of the election. Each vote cast upon the token supplants the older one/s cast upon the same token. This may make vote buying and coercion more onerous than in postal voting procedures, where the paper-based election material may be used just once. The argument concerning protection against premature disclosure works the same way as with envelope protocols, a value of 1 is assigned.

7. CONCLUSION

This paper discussed the effects on the updated *Council of Europe Recommendation (2017)5* on e-voting protocol viability focussing on envelope and token protocols. A multi-dimensional model was advanced to systematically map the abilities of an e-voting protocol against the core requirements (dimensions) of CM/Rec(2017)5. A capabilities frontier was defined depending on how far technical safeguards protect each of the dimensions; beyond that only organisational safeguards apply. The paper then proceeded to present a typical envelope and a typical token protocol mapping it against the multi-dimensional model showing that there are considerable differences between the two protocol families in achieving the requirements of CM/Rec(2017)5.

The main weakness of enveloping is the complete absence of general verifiability and the necessity to keep the private key of the election committee and the ballot box apart, as both together enable to break voting secrecy on a large scale. The token protocol protects voting secrecy technically and enables a very high degree of individual and general verifiability, with individual verifiability exceeding the requirements of CM/Rec(2017)5.

As shown in the paper, the question of whether anonymization occurs before or after the insertion in the ballot box, is a true watershed between e-voting protocols. This question decides about the quality of individual verification, the possibility of a meaningful independent recount and the technical (not organisational) protection of voting secrecy. The authors hold that CM/Rec(2017)5 accentuates this watershed. In this regard the CM/Rec(2017)5 can be considered a seminal piece of work by the *Council of Europe* towards reliable e-voting.

LIST OF REFERENCES

[1] Actica Consulting. (2007) *Technical Evaluation of Rushmoor Borough Council e-voting Pilot 2007*. [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0019/16192/Actica_Rushmoor_27248-20137__E__N__S__W__.pdf [Accessed 31 May 2018].

[2] Actica Consulting. (2007) *Summary of Technical Assessments of May 2007 e-voting Pilots.* [online] Available from: http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0018/16191/Actica_Summary_27244-20136__E__N__S__W__.pdf [Accessed 31 May 2018].

[3] Bagnato, D. (2019) The impact of the Council of Europe Recommendation CM/REC (2017)5 on eVoting protocols. In: Nemeslaki, A., Prosser, A., Scola, D., Szadeczky, T. (eds.). *Central and Eastern European eDem and eGov Days 2019*, Budapest, 2–3 May.

[4] Blakley, G.R. (1979) Safeguarding cryptographic keys. In: IEEE (eds.). *International Workshop on Managing Requirements Knowledge (MARK)*, New York, 4–7 June.

[5] Cohen, J. and Fischer, M. (1985) A robust and verifiable cryptographically secure election scheme. In: *26th Symposium on the Foundations of Computer Science*, October 21–23, IEEE.

[6] Common Criteria. (2014) *Common Criteria Recognition Arrangement, Common Criteria for Information Technology Security Evaluation*, Version 3.1R5, Parts 1 to 3. Available from: https://www.commoncriteriaportal.org/cc/ [Accessed 16 June 2020].

[7] Constitutional Court. (2011) V 85-96/11-15, 13 December.

[8] Estonian National Electoral Committee. (2010) *E-Voting System – General Overview*, Tallin, 2005–2010. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/General_Description_E-Voting_2010.pdf [Accessed 16 June 2020].

[9] Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM(2017)50-add1 final) Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168071bc84 [Accessed 17 April 2019].

[10] Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting, 14 June 2017(CM(2017)50-add2final). Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726c0b [Accessed 17 April 2019].

[11] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24 (2).

[12] Karhumäki, J. and Meskanen, T. (2008) *Audit Report on Pilot Electronic Voting in Municipal Elections.* University of Turku, Turku.

[13] Landgericht Regensburg. (2018) *Strafverfahren wegen Verdachts der Wahlmanipulation in Geiselhöring*. [press release] 15 October. Available from: https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/regensburg/presse/2018/7.php [Accessed 2 November 2018].

[14] Maaten, E. (2004) Towards remote e-voting: Estonian case. In: Prosser, A. and Krimmer, R. (eds.). *Electronic Voting in Europe – Technology, Law, Politics and Society*, GI-Edition, Lecture Notes in Informatics.

[15] Müller-Török, R. (2019) The Principles Established by the Recommendation CM/Rec (2017)5 on Standards for E-Voting Applied to Other Channels of Remote Voting. *Masaryk University Journal of Law and Technology*, 13 (1).

[16] National Institute of Standards and Technology. (2001) *Federal Information Processing Standards Publication 197*, ADVANCED ENCRYPTION STANDARD (AES). [online] Available from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [Accessed 16 June 2020].

[17] Pichler, G. (2019) Darf man seinen ausgefüllten Wahlzettel auf Instagram teilen? *Der Standard*, 25 May. [online] Available from: https://www.derstandard.at/story/2000103646954/darf-man-seinen-ausgefuellten-wahlzettel-auf-instagram-teilen [Accessed 16 June 2020].

[18] Prosser, A. (2014) Transparency in eVoting – Lessons learnt. *Transforming Government: People, Process and Policy*, 8 (2).

[19] Prosser, A. and Müller-Török, R. (2009) E-Voting: Lessons Learnt. In: Kaplan, B. and Aktan, D. (eds.). *International Conference on eGovernment and eGovernance*, Ankara.

[20] Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. (2004) Implementation of Quorum--Based Decisions in an Election Committee. In: Traunmüller, R. (ed.). *Proceedings of DEXA/EGOV 2004*, Lecture Notes in Computer Science LNCS 3183, Springer, Berlin.

[21] Prosser. A. and Müller-Török R. (2002) E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik*, 44 (6).

[22] Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting, 14 June 2017 (CM/Rec(2017)5). Available from: https://rm.coe.int/0900001680726f6f [Accessed 17 April 2019].

[23] Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, 30 September 2004. Available from: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf [Accessed 16 June 2020].

[24] Rivest, R. L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2).

[25] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J. A. (2014) Security Analysis of the Estonian Internet Voting System. In: *CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ACM. [online] Available from: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 16 June 2020].

[26] State Electoral Office of Estonia. (2017) *General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia*, Document: IVXV-ÜK-1.0, Tallin. [online] Available from: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [Accessed 16 June 2020].

[27] Stein, R. and Wenda, G. (2014) Das Zentrale Wählerregister – Ein skalierbares Instrument zur Bürgerbeteiligung mit 1:1-Verifikation. In: Plodereder, E., Grunske, L., Ull, D. and Schneider, E. (eds.). *44. Jahrestagung der Gesellschaft für Informatik.* INFORMATIK 2014, 22–26 September, Bonn. [online] Available from: https://subs.emis.de/LNI/Proceedings/Proceedings232/1427.pdf [Accessed 16 June 2020].

[28] White, I. and Coleman, Ch. (2011) *Postal Voting & Electoral Fraud*, SN/PC/3667, House of Commons Library.