Debrief on e-voting in Estonia

Is it worth to be constructive in a flawed policy debate?

28.12.2019 @36c3

Who am I?

Märt Põder // tramm@infoaed.ee // @tramm:matrix.org // +372 55643754

- Hacking stuff since 1990s, first plugged into FidoNet 2:490/222.33
- Board member/founder ISOC, Open Knowledge, Pirate Party, Wikimedia.
- Estobuntu etc developer, academic background philosophy/informatics.
- ID card software GNU/Linux source code packaging and campaign 2010.
- Hacked e-voting client application to cast a “spoiled vote” in 2015.
- Got on first pages of newspapers and involved in e-voting debates.
- Former member of government working group 2019 to make e-voting “verifiable, secure and transparent”.
- Declared report of working group a failure since no advancement in verifiability discussions.

Policy debate on e-voting in Estonia

- You can hardly find a critical voice on e-voting among technology experts.
- When introduced in 2005 it was compared to Skype (based in P2P protocol developed by Estonian engineers) and Estonia intended to become first country conducting national election online.
- Major political party opposing of e-voting was main voice of local Russians and also being centre-left was considered having Soviet flavour, which was despised by other political parties. Criticizing e-voting became an unpatriotic and non-progressive act.
- When got into government the same party started to support e-voting.
- In current government a new right-wing populist party in coalition with centre-left party started a work group to fulfill their election promise to find out what to do with e-voting (and maybe discontinue it).

Vicious circle among IT experts and legal experts

- Before introducing in 2005 two white papers were produced by academic researchers in 2001, setting requirements of verifiability, independent vote counting and open source code. These were ignored by project manager Tarvi Martens hired by electoral commission starting from 2003.
- The system was conceived ignoring research and 1990s style hackish solution with lots of NIH-syndrome involved was built. IT experts and startuppers share the feeling and have been satisfied with the e-voting system although proven unscalable and ignore criticisms as uninformed.
- Legal experts are blinded with explanations of IT experts and based on that produce legal reasoning to explain why Estonian e-voting is constitutional and near perfect as it is.
- This assures IT experts even more that it’s the rest of the world that is wrong.

Observing using end to end verifiable protocol

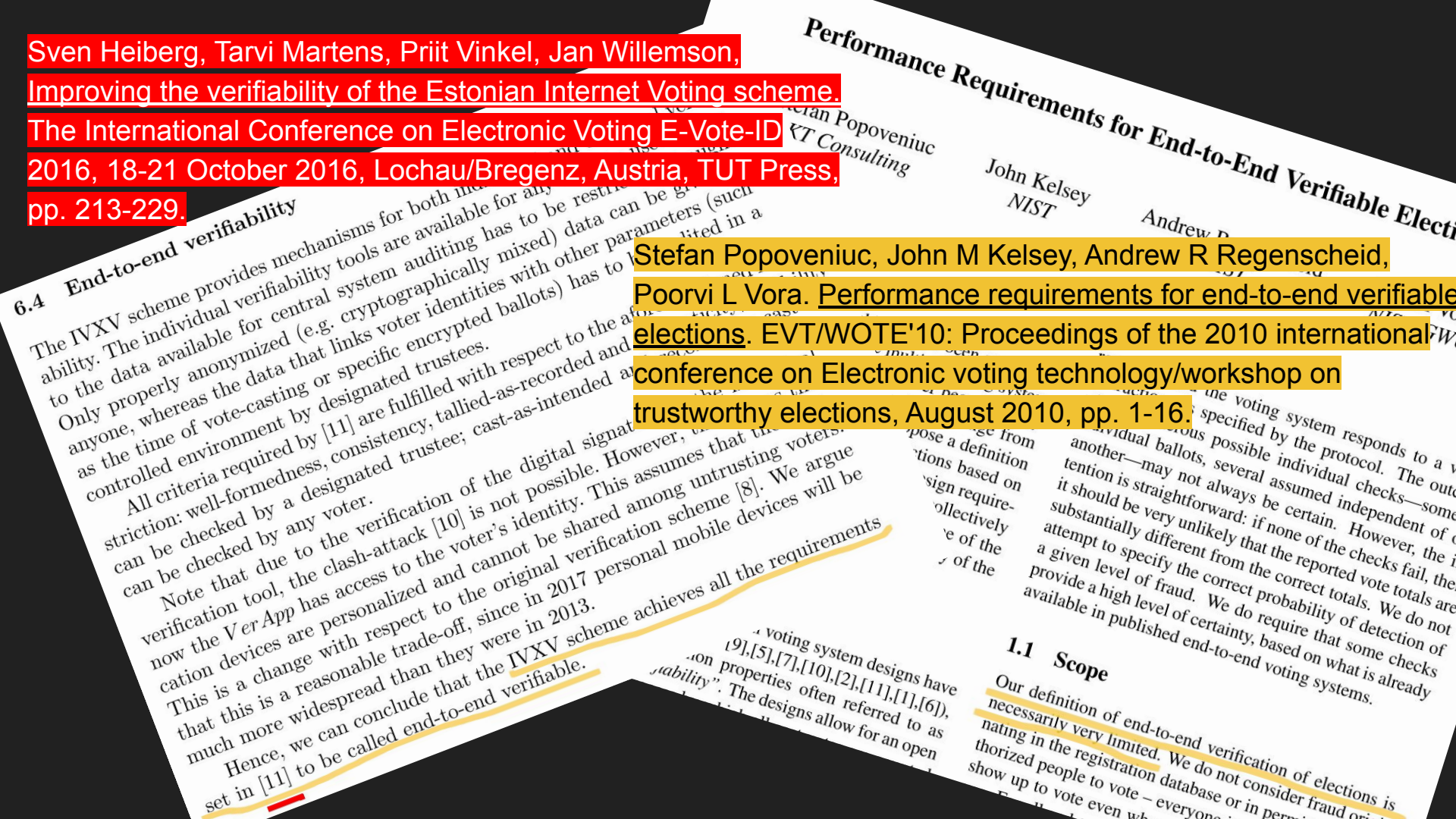
- End to end verifiability is a concept to transfer election principles of vote secrecy, public observability, one person one vote etc into digital environment.
- It is a game theoretical concept explaining how participants with different motivations would be observing/auditing/verifying that election was conducted correctly and that the results are correct.
- It’s usually realized using robust enough cryptographical models not depending on operator of e-voting to ensure observability joining motivations of voters, rivalling parties running in elections and public interest groups.
- Individual vote verifiability is for voters to verify if the vote was cast, stored and counted correctly.
- Universal verifiability is for interested voters and election observers to audit vote tallying so that there is a mathematical proof that all votes were counted and that they were counted correctly.

Estonian take on end to end verifiability

- Research paper by Helger Lipmaa and Oleg Mürk from 2001 required individual and universal verifiability from the system. System built in 2005 had no verification mechanisms whatsoever.
- In 2013 individual verifiability was introduced because OSCE/ODIHR recommendation mentioned e-vote application malware ignored by Estonian authorities up to constitutional court. Current verification solution allows voter to verify that the vote cast is stored in server up to 30 minutes after voting.
- In 2017 universal verifiability with mixnets was introduced, but its role in the process was not specified and was left “optional” in official explanation of the system and the process.
- The new white paper from 2016 by Jan Willemson, Tarvi Martens, Priit Vinkel and Sven Heiberg boasts that the system is “end to end verifiable”, but bases on a “very limited” definition from 2010.

Sven Heiberg, Tarvi Martens, Priit Vinkel, Jan Willemson, Improving the verifiability of the Estonian Internet Voting scheme. The International Conference on Electronic Voting E-Vote-ID 2016, 18-21 October 2016, Lochau/Bregenz, Austria, TUT Press, pp. 213-229.

Stefan Popoveniuc, John M Kelsey, Andrew R Regenscheid, Poorvi L Vora. Performance requirements for end-to-end verifiable elections. EVT/WOTE'10: Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, August 2010, pp. 1-16.



My personal quest for end to end verifiability

- In 2015 I wrote an article to biggest newspaper explaining “end to end verifiability” demanded by 2001 white paper, 2011 OSCE/ODIHR recommendation, 2014 Halderman lead independent group etc.
- In 2017 after reading new IVXV white paper I created a petition to make parliament discuss and take responsibility of electoral commission’s incompetence and snake-oil research used for verifiability of e-voting system.
- In 2019 I filed an election complaint to constitutional court which recognized that role of universal verifiability was not specified in the process and required to properly define it in relevant legal acts.
- In 2019 I filed a complaint to chancellor of justice Ülle Madise to assess if e-voting is compatible with constitutional rights and observability standards and got an non-answer that end to end verifiability is risky and not needed.

My 2017 petition to demand taking responsibility with e-voting from Estonian parliament, demanding correct definition of end to end verifiability and including public interest groups into discussion. Got 256 signatures of 1000 needed to send it to parliament.

Government workgroup on e-voting 2019

- Workgroup was gathered to find solutions to problems with “verifiability, security and transparency” of e-voting and I was invited to participate.
- As a result report was produced documenting 25 “spots of worry”, but workgroup composed mainly of current/former electoral commision members failed to recognize the need for any architectural changes.
- I supported fixing individual verifiability according to OSCE/ODIHR recommendation using control code known only to voter instead of QR-code system which leaks digitally signed and encrypted e-votes with a decryption key and extending the verification period up to counting of the votes.
- I proposed to review of the definition of end to end verifiability and make it follow the standard definition in scientific literature and the example of Switzerland where the requirements are clearly defined in national law.

Current individual verification is obstructing changes

- Individual vote verification is done by taking picture of QR code on computer screen generated by desktop voter application and using smartphone app to verify the vote.
- QR code contains vote UID and ElGamal ephemeral private key used to encrypt the vote. Encrypted vote is downloaded by any independent device using UID in 30 minutes, verification app decrypts the vote downloaded using the private key and shows the name and number of the candidate voted for.
- Obvious risk for voter coercion and vote secrecy of current verification mechanism make it impossible to extend verification period in order to make the e-voting follow the minimal requirements for end to end verifiability as stated in scientific literature or as defined in Swiss national law.
- Workgroup didn’t recognize any of the problems with QR code or definition of end to end verifiability nor did it recommend any architectural changes.

But leaking digitally signed votes is crazy enough

- OSCE/ODIHR election observers in their 2019 report noted that it's against Council of Europe standard on e-voting which Estonia is supposed to follow. Which means it's probably also against constitutional requirements.
- Digitally signed vote with decryption keys can be stored and used to not only show, but to legally prove the voter choice in eternal time after the election.
- Digitally signed electronic vote is even more hard evidence of the voter choice than photo of paper ballot in voting booth.
- You can sell your vote by voting in desktop application and sending QR code to interested buyer who "verifies" it using official smartphone app.
- You can scale electronic vote buying in darknet buying cryptograms accompanied with QR codes in masses and paying in cryptocurrency.
- You can provide scripts, tools and malware to outsource collection of the right votes with a promise to get paid for it.

Mom, look I’m in government coalition agreement!

- I explained the problem with QR code system revealing voter choice and leaking cryptograms in a meeting summoned by chancellor of justice, but in her written report she declared that vote secrecy is guaranteed. As a former electoral commission member she has written scientific articles on e-voting.
- Right-wing populist party in government quotes my statements on verifiability explaining their coalition agreement, but their minister failed to lead the work group to results. There is also second point in coalition agreement based on my constitutional court decision to specify the e-vote counting process in relevant legal acts. But this doesn’t guarantee meaningful discussion and the result might be the failure of 2017 kind, when electoral commission didn’t get the universal verifiability quite right.
- To take the debate to next level requires breaking the vicious circle among IT experts and legal experts in Estonia (see slide no 3).

Ülle Madise, Priit Vinkel. Constitutionality of Remote Internet Voting: The Estonian Perspective. Juridica International. International and National in Law: Development and Reciprocal Impact. January 2011, pp. 4-16.

Ülle Madise
Professor of Constitutional Law
University of Tartu

Priit Vinkel
Assistant, University of Tart
Advisor, Elections Departm
of the Chancellery of Riigik

Constitutionality of Rem
Internet Voting:

The Estonian Perspective

2.3. System architecture

The Estonian IT security experts in their security analysis[*14] published in 2003 and revised in 2010 declared that in a **practical sense** the Estonian I-voting system was secure enough for implementation. In absolutely secure systems, unexpected events are not possible. One may dream about such systems, but they can never be realised in practice. This applies particularly to I-voting systems. Considering the security level of personal computers, it is impossible to design I-voting systems that are absolutely secure for every user. The most important security goal of voting is not to affect the final results and not to abuse the constitutional principles. Single incidents with users are still important, but they do not have an influence on the final result. Moreover, small-scale incidents are acceptable even in traditional voting systems.[*15]

The part of I-voting in the whole process of organising elections is relatively small. The system uses information systems—the Population Register for the polling list, election information system of ...ittee (hereinafter referred to as the NEC) for the collection and publication of ... the infrastructure of Certification Centre Ltd. for check-

Forwarding

Being constructive in a flawed policy debate?

- I will continue explaining the goal of end to end verifiability to my Estonian colleagues despite it is hard topic in the middle of election legalese, technology, cryptography and constitutional requirements for democracy.
- Picture is worth 1000 words, so I am forking government workgroup report and stating the requirements in comprehensible manner with English translation, related progress bars etc based on CoE, OSCE/ODIHR recommendations and e-voting handbook, research papers and my own understanding of the topic as a veteran netizen.
- I intend to scale my debrief on e-voting in Estonia into netizen index of e-voting requirements that might be helpful for policy debates in other countries discussing, testing, piloting or introducing e-voting and maybe help to get rid of the example case of Estonia.

Debrief @e-vote About News Where is Putin? English

Status of e-voting in Estonia

All properties | Legal | Software | Auditability

Vote secrecy is ensured

Secrecy of vote is ensured throughout the process. Voter
elections are finished.

Individual vote verifiablity

Individual vote verification allows voter to make sure that her vote was cast, stored and counted correctly. Verification mechanism takes measures to ensure vote secrecy as much as possible.

Requirements for electronic voting booth are specified

Voting using personal computers in an uncontrolled environment is taken into account and proper legal safeguards are specified. Disclosing vulnerabilities is not outlawed by those legal prescriptions.

Universal verifiability of vote tallying is ensured

Universal verifiability of vote tally with proper mathematical proofs follows emergent best practices defined in scientific research in the field of cryptography and voting technology. Everybody is allowed to independently check if all eligible votes were counted and that they were counted correctly.

Publishing the source code

Source code is published in entirety with documentation to run it for testing. Publication uses proper free software license and there is no NDA needed.

Specifics of digital voting channel are taken into account

Specifics of digital technology are fully taken into account in legal acts setting the requirements for electronic voting. No wishful thinking basing e-voting on false analogy of paper ballots, e-banking or postal voting.

The system is digital democracy capable

Auditability is ensured by voters and election observers. The role of operator and need to place trust in it is minimized.

I will publish my own debriefing of e-voting forking government workgroup report from December 12. Will be published in first weeks of January 2020 at https://debriif.infoaed.ee/.

When will I publish and how to help?

- I plan to publish it in the very beginning of 2020. Based on Hugo static web generator, has full source code, is multilingual as well as easily forkable.
- I will be working on it here at 36c3 and you can help me discuss the requirements so they can be scalable or help with any other issues.
- I'd be happy to talk to activists having issues with e-voting.
- And of course I want everybody on board with my netizen index of requirements for e-voting.

Publication address: https://debriif.infoaed.ee/
Discuss: @evote-index:matrix.org
Contact me: @tramm:matrix.org // tramm@infoaed.ee

Thanks for listening and merry chaos!