Elektroonilise valimissüsteemi ja elektroonilise hääletamise töörühma 1. koosolek

Märt Põder, tramm@infoaed.ee, https://gafgaf.infoaed.ee, +372 55643754

E-hääletus on spetsiifiline süsteem, mille töökorra tagab esmalt selle arhitektuur ja alles seejärel vastavus turvastandarditele.

Süsteemi arhitektuuri kihid:

- Valimisõiguse põhimõtted: valimised on vabad, üldised, ühetaolised, otsesed, salajased ja vaadeldavad
- Süsteemi arhitektuur: TCP/IP protokollistik, ID-kaart ja selle taristu, avaliku võtme krüptograafia, anonümiseerimine, otsast lõpuni kontrollitavus (üksiku hääle kontroll, kokkulugemise kontroll), häälte talletamise server, ajatembeldusteenus, häälte kokkulugemise server jne
- Valminud tarkvara: HTTPS protokoll, serveriplatvormid, serverid ja nende tarkvara, hääletuse spetstarkvara, valijarakendus, nutitelefoni platvormid, hääle kontrollimise rakendus jne

Eesti süsteemi arhitektuur:

- 2001 Tanel Tammeti ja Helger Lipmaa veetud lähteuuringud, mis seadsid tingimuseks avatud lähtekoodi, sõltumatud käitajad ja otsast lõpuni kontrollitavuse
- 2003 viimast korda mainiti dokumentatsioonis otsast lõpuni kontrollitavuse aspekte
- 2005 avaliku võtme krüptograafia ja protsessiga tagatud hääle salajasus
- 2007 välisvaatlejad soovitavad parandada või e-hääletamise üldse lõpetada
- 2011 välisvaatlejad soovitavad rakendada otsast lõpuni kontrollitavust
- 2013 üksiku hääle kontroll kui otsast lõpuni kontrollitavuse komponent #1
- 2013 serveritarkvara lähtekoodi avalikustamine
- 2014 Haldermani töörühma kriitika ja soovitus rakendada otsast lõpuni kontrollitavust
- 2015 välisvaatlejad tunnustavad esimese sammu eest otsast lõpuni kontrollitavuse tagamisel
- 2017 miksimine ja kokkulugemise kontroll kui otsast lõpuni kontrollitavuse komponent #2
- 2019 komponendid on olemas, aga nende kooskõla ja eesmärk on küsitav, välisvaatlejate raport viibib

Küsimused:

- Kas aja jooksul süsteemi liidetud komponendid tagavad vastavuse valimisõiguse põhimõtetele?
- Kas ilma otsast lõpuni kontrollitavuse vajadust arvestamata loodud süsteemi arhitektuur, sh kasutajakogemuse disain võimaldab seda rakendada?
- Kas üksiku hääle kontroll 30-60 minutit pärast hääle andmist tagab otsast lõpuni kontrollitavuse?
- Kas üksiku hääle kontrollimisel näidatav kandidaadinimi ja -number on piiranguks kontrollitavuse laiendamisel?
- Kas ID-kaardiga allkirjastatud hääle edastamine on piiranguks kokkulugemise kontrolli avamisele kõigile vaatlejatele?
- Kas e-hääletuse puhul peaks kehtima vaadeldavusele kõrged nõudmised, sj kas vaatlemine peaks olema avatud kõigile ilma piiranguta ja kas lähteandmed, mille alusel vaadeldakse, peaks olema kõigile piiranguteta kättesaadavad?