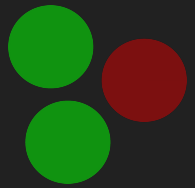

Pseudovote

https://pseudovote.net/

Kõigile auditeeritav salajane hääletus, kus läbiviija tagab usalduse minimalismiga

Märt Põder <tramm@infoaed.ee>

4. aprill 2023

Osapooled ja nende rollid

- Valijad, kelle rivaliteet on piisavalt intensiivne, et nõuda vastastikust kontrolli, aga mitte nii halvaloomuline, et tooks kaasa keerulised tehnilised ründed valimissüsteemi, nt meilikanalite ja/või teadetetahvli enda vastu
- Kolmeliikmeline või suurem valimiskomisjon, mis viib end süsteemiga kurssi ja teeb jooksvalt otsuseid
- Sõltumatu, garanteeritult usaldusväärne ja valijatele hästi ligipääsetav kanal valijatunnuste jagamiseks, prototüübis e-mail
- Neutraalne, sõltumatu ja tehniliselt usaldusväärne teadetetahvli pidaja, kes tagab häälte vastuvõtmise tehnilise stabiilsuse, tõrjub elementaarsed ründed
- Kuni mõnituhat osalejat, kelle puhul häälte ostu/müügi oht pole nii tugev, et peaks rakendama täiendavaid meetmeid kviitungivabaks hääletuseks

Pseudonüümse hääletuse üldskeem

- Valimiskomisjon tõendab, et jagab igale osalejale lihtsa ühekordselt kasutatava pseudonüümi, kuid ei jäta meelde valijatunnuse seost isikuga
- Tunnused loositakse välja juhuslikkuse alusel, kasutades minimalistlikku tarkvara, nt 100-realist Pythoni skripti, mis võimalikult paljudele loetav
- Hääletusel osalejad annavad hääle avalikul teadetetahvlil pseudonüümselt ja nähes reaalajas teiste pseudonüümsete valijate sissetulevaid hääli
- Hääletusperioodi lõpul kuvab skript jagatud pseudonüümide nimekirja, mille alusel eemaldatakse häälte hulgast nimekirjaväliste pseudonüümide kirjed, st “kehtetud sedelid”, ning loetakse kokku nimekirjas olnud valijate hääled
- Kõik osalejad võivad pseudonüümide nimekirja alusel teadetetahvlil toodud hääli töödelda ning veenduda hääletustulemuste korrektsuses

Hääletussüsteemi põhiomadused

- Valijad anonüümitakse võimalikult varases faasis
- Usaldus pole süsteemi automaatselt eeldatud omadus, valimiskomisjon peab usalduse tagamiseks reaalset tööd tegema
- Pseudonüümide jaotamine on turvamudelis kriitilise tähtsusega tegevus
- Pseudonüümide äraarvamise vältimiseks valitakse iga kord uus sõnastik
- Pseudonüümide korrektset jaotamist tõendab valimiskomisjon protseduuri lihtsuse, loetava lähtekoodi ja üldtunnustatud komponentide kasutamisega
- Teadetetahvli pidaja usaldusväärsust kontrollivad kõik valijad hääletamise käigus oma hääle edastamisega teadetetahvlile
- Hääletustulemuse saab kindlaks teha igaüks, autoriteetse tulemuse kuulutab välja valimiskomisjon


Salajane hääletus Internetis – on see võimalik?

Tüüpilised kasutusjuhud

- Mõnesaja kuni mõne tuhande liikmega ühingute üldkoosolekud, sj hääletamine füüsilistel üldkoosolekutel nutiseadmega
- Virtuaalsed üldkoosolekud 2020 maikuus vastu võetud seadusemuudatuste valguses, mis lihtsustasid koosolekute protokollimist, kuid seadsid kahtluse alla salajase hääletuse lubatavuse
- Seaduse mõttes rangelt võttes lubatav vaid salajane hääletus täismahus koosolekutel, mis sisaldab kõigi osalejate reaalajas audio-/videosilda
- Prototüübis realiseeritud integratsioonis Jitsi videokonverentsi tarkvaraga https://jitsi.eesti.ee/, mis logib koosoleku käigu ja osalejate nimekirja automaatselt, et hõlbustada protokolli esitamist ja kvoorumi tõendamist

Paigutus e-hääletuse raamistike seas

Lihtsaim avalikul teadetetahvlil põhinev otsast lõpuni kontrollitav hääletussüsteem krüptograafilise hääletuse klassikute Benaloh jt vaimus nende 2015 aasta artiklist:

> *Proovigem niisiis nutikamat lähenemist: valimiste korraldaja määrab igale valijale pseudonüümi. Kui valija annab hääle, paneb valimiste korraldaja teadetetahvlile üles hääle koos pseudonüümiga. Ka nii saab iga valija isiklikult kontrollida, et tema hääl on toodud ära tema pseudonüümi juures. See kaitseb teatud määral hääle salajasust (mõned valijad võivad kogemata või nimelt oma pseudonüümi avalikustada), kuid sellega on siiski probleeme -- näiteks ei ole välistatud valijasund ja korraldaja võib petta nii, et omistab sama pseudonüümi valijatele, kes võiksid hääletada ühtemoodi.*