

PSEUDONÜÜMITSEREMOONIA

Hääletustunnuste jagaja on eeldab vaikimisi viimase Ubuntu või Debiani kasutamist. Tegu on eksperimendiga e-hääletuse lävepakuküsitluse korraldamiseks Euroopa Parlamendi valimistel ning tseremoonia peamine eesmärk on tagada lävepakuküsitluse korrapärane toimumine vastavalt algselt seatud eesmärgile. Kuigi küsitlusele ei kehti samad nõuded, mis valimistele, siiski püütakse tagada samade või sarnaste põhimõtete järgimist, mida peab järgima valimiste korraldamisel.

1. Riistvara valik

Hetkel on korraldaja poolt valikus MSI Bravo 15 C7V sülearvuti. Viimane Ubuntu läheb sellel tööle ilma eriseadistusi vajamata.

2. Opsüsteemi valik

Ilmselt kõlbavad ka viimased Debianid, aga Ubuntu võib olla lihtsam eri riistvarale paigaldada. Viimane Ubuntu on Ubuntu 24.04 LTS “Noble Numbat”. Ubuntu autentsuses veendumiseks genereeritakse vähemalt opsüsteemi tõmmise räsi ja võrreldakse seda Ubuntu lehel avaldatud allkirjastatud räsiga.

```
wget https://releases.ubuntu.com/noble/ubuntu-24.04-desktop-amd64.iso
sha256sum ubuntu-24.04-desktop-amd64.iso
wget https://releases.ubuntu.com/noble/SHA256SUMS
wget https://releases.ubuntu.com/noble/SHA256SUMS.gpg
gpg --keyid-format long --keyserver hkps://keyserver.ubuntu.com --recv-keys 0x46181433FBB7545
gpg --keyid-format long --list-keys --with-fingerprint 0x46181433FBB75451 0xD94AA3F0EFE21092
gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
sha256sum ubuntu-24.04-desktop-amd64.iso
```

3. Opsüsteemi paigaldamine

Paigaldatakse Ubuntu tavapärasel viisil, määrates juurkasutaja ja parooli. Pärast Ubuntu paigaldamist eeldatakse, et ollakse turvalises süsteemis, ühendutakse Internetiga ja tehakse kõike tavapärase Ubuntu kasutamise hea prakтика raames. Kui logitakse Ubuntu sisse, pannakse esimese asjana käima videosalvestus.

4. Tarkvara paigaldamine

```
sudo apt install git
git clone https://github.com/infoaed/pseudovote-euro24.git
sudo apt install python3-m2crypto python3-pyasn1 python3-pycryptodome python3-progressbar py
```

5. Valijate nimekirja ja sertide paigaldamine

Valijate nimekiri on tekstifail `voterlist.txt` ja sertifikaadid on JSON-vormingus failid nimetatud malli järgi `01234567890.json`, mis on kataloogis `res`. Paigaldatakse mälupulgalt, räsid dokumenteeritakse.

6. Pseudonüümide looja käivitamine

Enne pseudonüümide looja käivitamist peab olema olemas kataloog `con`, kuhu paigutatakse krüptitud hääletustunnused.

`./ceremony.py`

Pseudonüümide karantiinitud nimekirja krüptimise faasis sisestatakse järjest isikukood, kelle ID-kaardi jaoks nimekiri krüptitakse. Nimekiri paigutatakse krüptitud konteinerisse, sj iga järgnev konteiner paigutatakse uue isikukoodi jaoks krüptimisel uude konteinerisse. Nii saab konteinerit avada ainult kõigi adressaatide nõusolekul ja koostöös.

Väljundiks on:

- Krüptitud pseudonüümid kataloogis `con`, nimetatud malli järgi `01234567890.cd`.
- Pseudonüümide räside nimekiri failis `pseudonuumide_rasid.txt`.
- Karantioneeritud pseudonüümide nimekiri krüptitud failis `karantiin_01234567890.cd`.

7. Loodud failide räside dokumenteerimine

Kõigi loodud failide räsid dokumenteeritakse.

```
cd con
ls | xargs sha256sum
```

8. Karantiinitud nimekirja allkirjastamine

Valimiskomisjoni liikmed allkirjastavad dokumenteeritud räsid ja pseudonüümide karantioneeritud nimekirja koos kokkuleppega seda mitte enne valimiste lõppu avada.

Käesolevaga lubavad allkirjutanud mitte avada karantioneeritud pseudonüümide nimekirja enne h

Pseudonüümide räside nimekirjaga, valijate nimekirjaga ja sertifikaatidega võib tutvuda kohapeal, aga neid eraldi ei avaldata.

9. Valimiskomisjon kinnitab tulemuse

Hääletusperioodi lõpul loeb valimiskomisjon hääled avalikult teadetetahvliolt kokku ja annab teada tulemuse. Sama võivad teha ka kõik teised soovijad, vaidlused lahendatakse võimalusel koostöös valimiskomisjoniga.