E-hääletamise usaldusväärsuse infotehnoloogiline tagamine

Jaak Tepandi

TTÜ professor
Infosüsteemide sertifitseeritud audiitor

Millest räägime

- **E-hääletamine ja usaldusväärsus**
  - võimalused - usaldusväärsus - kõige hullem?
- **Mida peame arvesse võtma?**
  - organisatsioon - IT süsteem - etapid
- **Usaldusväärsuse tagamisest**
  - teemad - tarkvara - osalejad
- **Materjale**
  - e-valimised - standardid ja normid - kogemused

E-hääletamine - võimalused

Võimalused:

- **Inimeste osaluse suurenemine, demokraatia areng**
- **Inimeste osavõtt, kellel on raskusi osaleda muul moel**
- **Rohkem valimisi: Kohalikud probleemid / spetsiifilised küsimused – kiiremini ja efektiivsemalt**
- **Tegelikkus: küsitlused Interneti jne kaudu populaarsed**
- **Perspektiivis valimiste maksumuse vähendamine**
- **Prognoos: Internet varsti infokanalina TVst ees**

Tulemus: kasvav huvi e-hääletamise vastu kogu maailmas

(IT) süsteemi usaldusväärsus

- (Funktsionaalsus) - "Teeb seda, mida vaja"
- Turvalisus (käideldavus, konfidentsiaalsus, terviklus) - "Ei tee seda, mida pole vaja +…"
- Töökindlus, ohutus - "Teeb vajalikku piisavalt tihti, ohtlikku piisavalt harva"
- Hooldatavus - "See toimub ka tulevikus / ilma meieta"

Kõige hullem?

(E-)hääletamise olulisemad välditavad tulemused:

- **Tulemuste ebakorrektsus või ebausaldusväärsus, mida ei suudeta õigeaegselt avastada**
- **Hääle salajasuse rikkumine**
- **Hääletamise katkemine / tühistamine**

- **E-hääletamise probleemid avastatakse õigeaegselt?**
- **Hääletaja ei saa e-hääletada?**
- **E-hääletamine on (esialgu) lisakulu? Jne**

…Arutelud ja diskussioonid väga vajalikud

Mitte vaid e-hääletamine

Kus?

- **Transport, tööstus, meditsiin, (aatomi)elektrijaamad...**
- **Kui vaja nii tegevust kui ka tegevusloogikat**

Kuidas? Meetodid, vahendid, standardid, kogemus

- **(riski)analüüsiks**
- **kavandamiseks**
- **realiseerimiseks**
- **(riski)halduseks**

Millest räägime

- **E-hääletamine ja usaldusväärsus**
- **Mida peame arvesse võtma?**
  - organisatsioon - IT süsteem - etapid
- **Usaldusväärsuse tagamine**
- **Materjale**

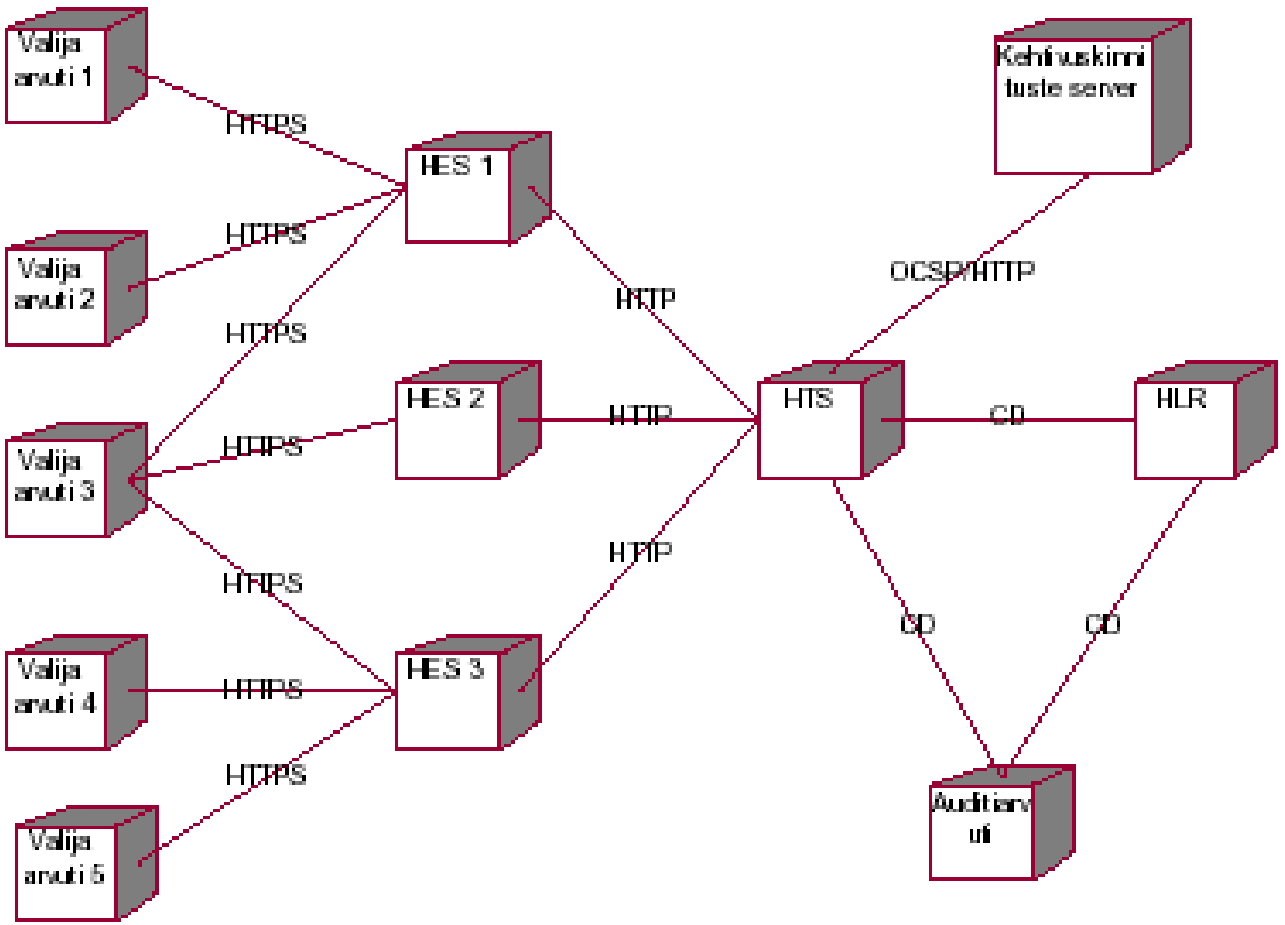
Organisatsioon - eripära

- Osa aega on aktiivne ja osa aega deaktiveeritud
- Mitmed osapooled
- Personal põhilise osa ajast tegev muude ülesannetega
- Peab vastama väga kõrgetele turvanõudmistele
- Osaliselt virtuaalne, piiritletud e-hääletamise regulatsioonide ning juhenditega
- Määratleda minimaalne e-hääletamise süsteemi organisatsioon ning selle komponendid

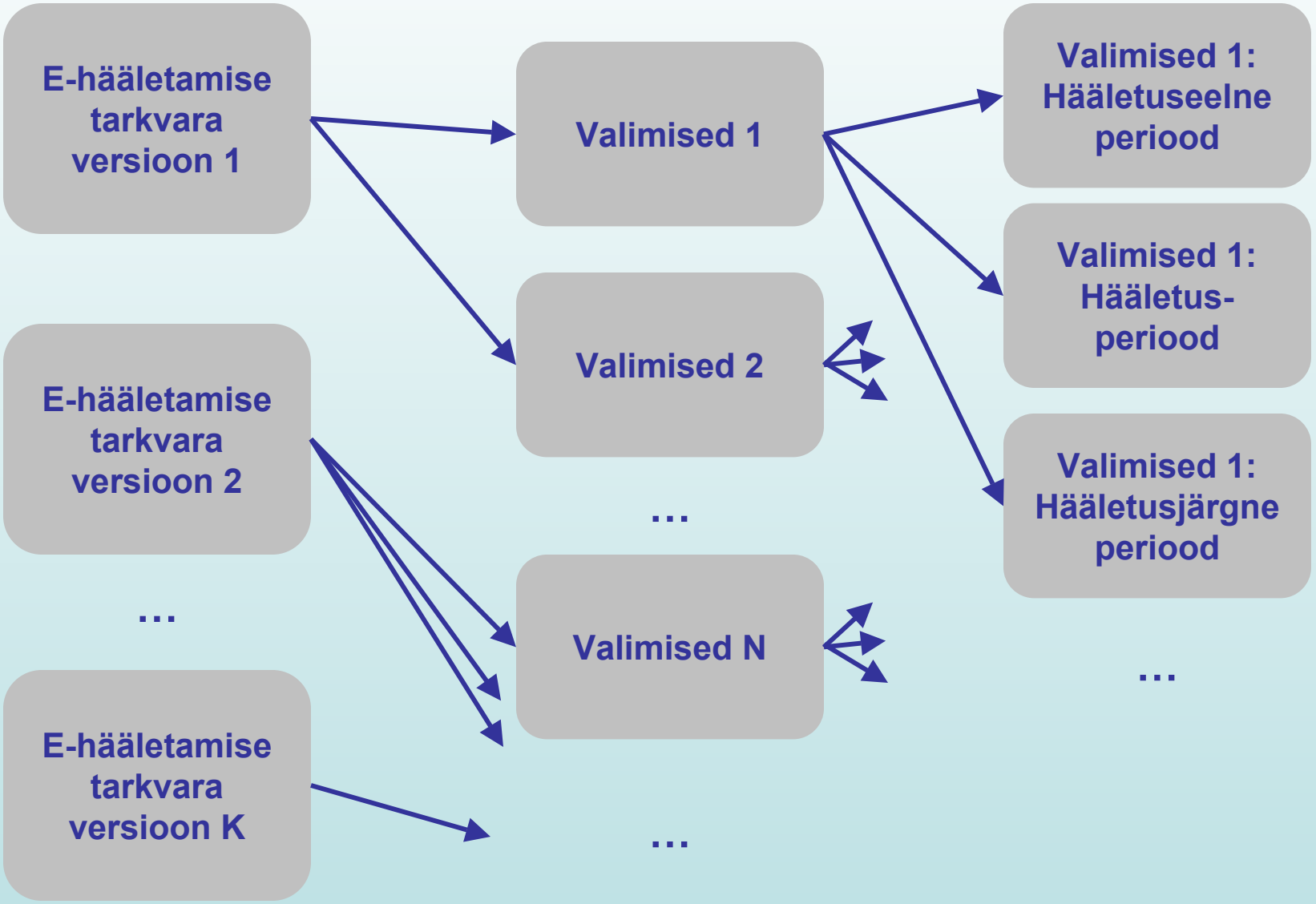
Organisatsioon - osalejaid (näide)

- Valijad
- Vabariigi Valimiskomisjon, maakonna / valla / linna valimiskomisjonid, jaoskonnakomisjonid
- Riigikogu Kantselei valimiste osakond
- E-hääletamise tarkvara arendaja, riistvara tarnija
- Häälteedastamis- ja häältetalletamisserverite majutaja
- Sertifitseerimisteenuse osutaja
- Rahvastikuregistri vastutav töötleja
- Riigi Infosüsteemide Arenduskeskus
- Hääletuseelse tehnilise eelekspertiisi, hääletusaegse auditi, hääletusjärgse auditi tegijad, …

E-hääletamise IT süsteem (näide)



Etapid



Millest räägime

- **E-hääletamine ja usaldusväärsus**
- **Mida peame arvesse võtma?**
- **Usaldusväärsuse tagamine**
  - teemad - tarkvara - osalejad
- **Materjale**

Turbehalduse teemad

Kogu süsteemi kaitstakse, sealhulgas

- **organisatsioon**
- **personal**
- **hooned ja ruumid**
- **riist- ja tarkvara**
- **võrgud**

Usaldusväärsus tarkvara tasemel (1)

Vasturääkivad nõudmised:

- **Range konfidentsiaalsus**
- **Hääletamise protsessi auditeeritavus**

Põhimõtteid:

- **ID kaardi kasutamine**
- **Avaliku võtme krüptograafia kasutamine**
- **"Ümbrikuskeem"**
- **Kriitilised tegevused nõuavad mitmeid osapooli**
- **…**

Turbe põhimõtteid: tarkvara

- Tarkvara algversioon on tuvastatud ja verifitseeritud
- Muudatusi hallatakse konfiguratsioonihalduse korra kohaselt (iga hetke konfiguratsioon on tuvastatud ja verifitseeritud)
- Süsteemi kaitstakse

Turbe põhimõtteid: organisatsioonid

- Kriitilistele seadmetele ja informatsioonile tuleb anda juurdepääs ainult tõendatud tööalase teadmisvajaduse alusel ja keelata juurdepääs kõigil teistel
- Kriitiliste seadmete ja informatsiooni kaitse peab olema rakendatud sõltumatult nende asukohast
- Kriitilisi protseduure tuleb täita vähemalt kahe töötaja koostöös. Neid töötajaid tuleb perioodiliselt roteerida. Selliste protsesside täitmisest peab jääma auditeeritav jälg.

Valija keskkond

- **Hooldatud, teadlik valija - > usaldusväärne**
- **Otseselt mitte hallatav**
- **Saab jälgida ründeid**
- **Saab teavitada**
- **Olulised võimalused:**
  - uuesti hääletada
  - vajadusel e-hääletamine katkestada (valijad saavad hääletada muul viisil)

Millest räägime

- **E-hääletamine ja usaldusväärsus**
- **Mida peame arvesse võtma?**
- **Usaldusväärsuse tagamine**
- **Materjale**
  - e-valimised - standardid ja normid - kogemused

Eesti e-valimiste materjale

- Süsteemi eelanalüüs, turbe analüüs, Riigikogu Kantselei korrad, muud üldised materjalid
- Tehnilised nõudmised, infoturbe poliitika, ametijuhendid jm - e-hääletamise haldus
- Lõppkasutaja, süsteemiülema, operaatorite jne juhendid
- Tarkvara projektdokumentatsioon
- Vabariigi Valimiskomisjon. Elektrooniline hääletamine. Materjalid aadressilt http://www.vvk.ee/elektr/index.html

Standardeid ja norme

- Infosüsteemide kolmeastmelise etalonturbe süsteem (ISKE-metoodika), www.ria.ee
- EVS-ISO/IEC 17799:2003. Infotehnoloogia. Infoturbe halduse menetluskoodeks, www.evs.ee/
- *Governance, Control and Audit for Information and Related Technology (COBIT)*. Infosüsteemide auditi ja juhtimise fond, www.isaca.org/
- EVS-ISO/IEC TR 13335. Infotehnoloogia. Infoturbe halduse suunised. Osad 1 kuni 5, www.evs.ee/
- …

Kogemusi kogu maailmast

- **Paljudes riikides**
- **Euroopa Liit: CYBERVOTE, scytl jt**
  - Scytl's Pnyx.DRE - Frontiers in Electronic Elections conference in Milan on September 16, 2005 (IST)
- **E-hääletamise analüüse ja materjale mujalt maailmast**
- **Infoturbe materjalid**
- **…**

Kokkuvõte: E-hääletamise usaldusväärsuse infotehnoloogiline tagamine

E-hääletamine - nagu iga uus asi - loob uusi **võimalusi** ja toob kaasa **riske**, mida tuleb arutada ja hallata

IT riskide haldamine on osa üldisest riskihaldusest, selleks on **rahvusvahelised metoodikad ja standardid**

Võetakse arvesse e-hääletamise **organisatsiooni** ja **IT süsteemi** kõigil **etappidel**

Kogu süsteemi kaitstakse, sealhulgas organisatsioone, personali, hooneid ja ruume, riist- ja tarkvara, võrke

Nagu ka **tavahääletamise** puhul jäävad **jääkriskid**, mida tuleb aktsepteerida

E-hääletamise süsteemid ja nende turve **arenevad kogu maailmas**, sealhulgas Eestis

Tänan!