Nutiseadmetele? Brauserisse?

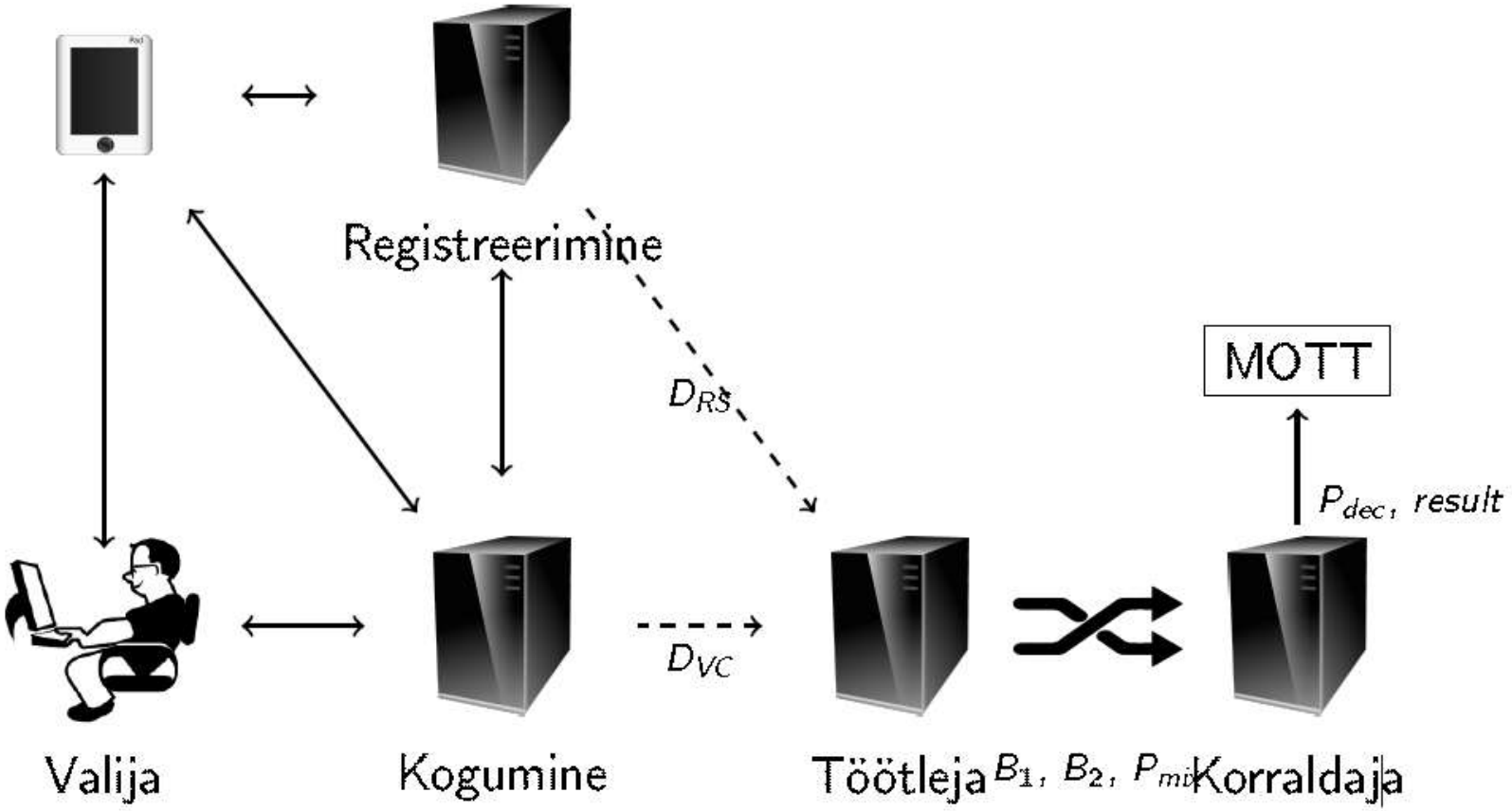
Sven Heiberg

sven@ivotingcentre.ee

Hääletamine brauseris, 2007

Hääletamine brauserita, 2009 - ...

Hääletamisprotokoll



Mida peab valijarakendus oskama?

- TLS ühenduse loomine ja usaldusväärsuse kontrollimine
- eID kasutamine (ID kaart, mID)
- Valiku krüpteerimine (juhuslikkus, ElGamal)
- Valiku signeerimine (SHA256, BDOC, XML, ZIP)
- Hääle verifitseerimine
  - RSA/ECC signatuuri verifitseerimine
  - OCSP vastuse verifitseerimine
  - PKIX ajatempli verifitseerimine
- QR-koodi genereerimine
- Samuti oluline evitamise turvalisus ja lihtsus

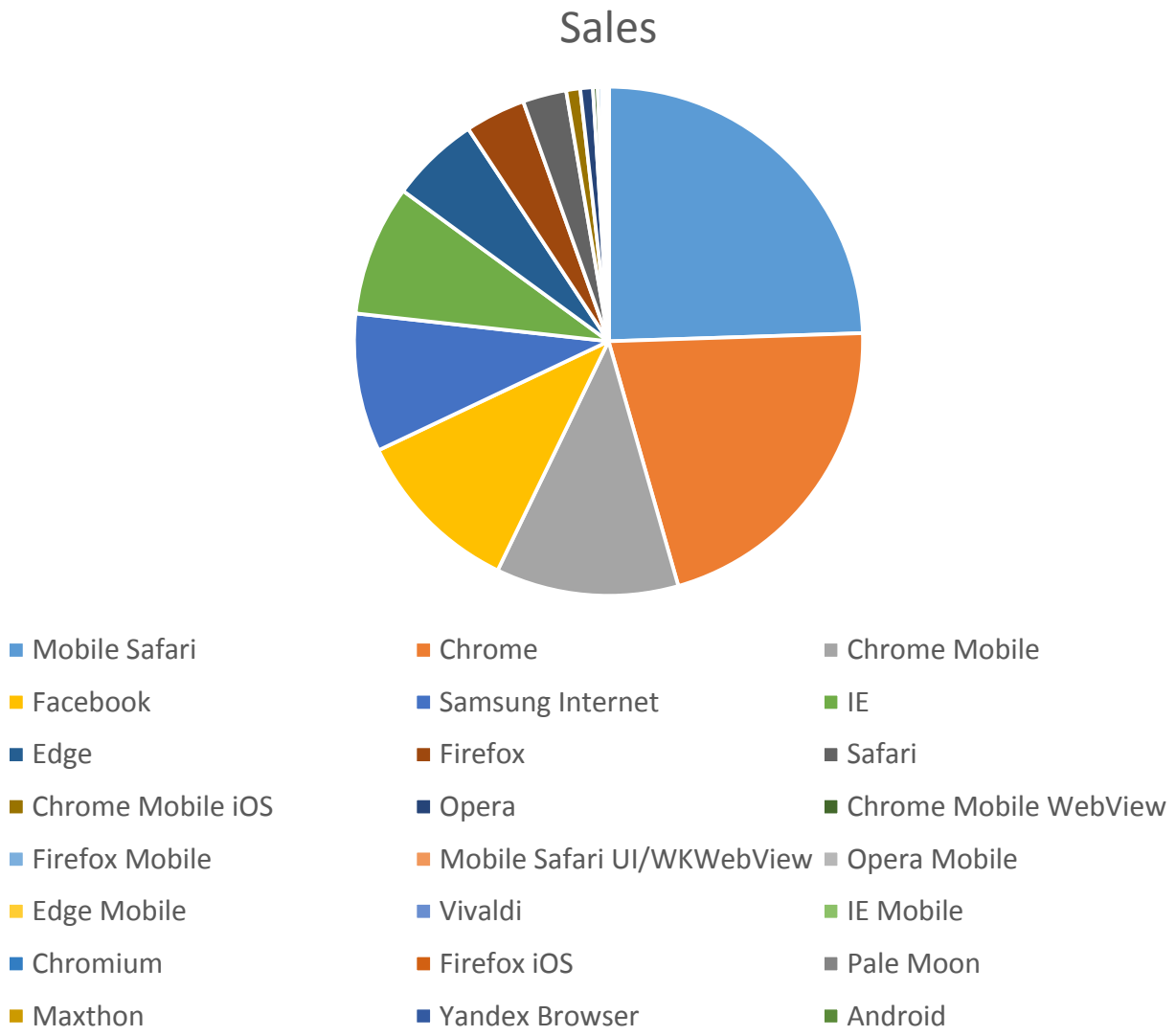
Nutiseadmed valimisel

App valijarakendusena?

- Kõik teemad on lahendatavad kui unustame ID-kaardi
- OS versioonide ühildamatuse tõttu tuleb süsteemsed teegid unustada (TLS ja muu krüpto)
- iOS ja Android vahel koodibaasi jagamine küsitav
- Evitamise turvalisus ja lihtsus?
  - Hääletamine algab marketist
  - iOS tsükkel tüsilik
  - Android võimaldab avatud lähtekoodi korral korratavaid builde
- Kuidas kontrollime?
  - Sama mehhanism, aga infovahetus? Platvormide sõltumatus?

Hääletamine brauseris, 2014 - ...

Brauserite jaotus 2018 ühtedel valimistel



Brauser valijarakendusena? Eestis?

- Taaskord teemad lahendatavad, kui unustame ID-kaardi
  - ID-kaardi toetamine siiski võimalik
- Siiski probleemid krüptoga
  - Usaldusväärsed teegid praktiliselt puuduvad
  - Kvaliteetne juhuslikkus?
  - XML/BDOC JavaScriptis?
  - Signatuuri verifitseerimine
  - OCSP vastuse verifitseerimine
  - PKIX ajatempli verifitseerimine
- JavaScript või TypeScript?
- Evitamise turvalisus ja lihtsus
  - Koodi terviklus?

Järeldused