E-hääletamise kesksüsteem

Sven Heiberg
Tallinn

11.07.2013

CYBERNETICA

Elektroonilise hääletamise kesksüsteem

- Elektroonilise hääletamise kesksüsteem on valimiste, kui suurema süsteemi komponent.
- Elektroonilise hääletamise kesksüsteemi vastutusala on:
  - Valija autentimine ning ringkonnale vastava kandidaatide nimekirja väljastamine
  - Digitaalselt allkirjastatud hääle vastu võtmine, verifitseerimine ning talletamine
  - Hääle kontrollimise võimaldamine
  - Elektroonilise hääletamise tulemuse arvutamine talletatud häälte põhjal.
- Süsteem ei tegele kandidaatide registreerimisega, paberhääletamisega, valimistulemuse arvutamisega, hääletamistulemuse visualiseerimisega etc.

Kesksüsteem ajas

- Seadistusperiood
  - Tarkvara paigaldamine ja seadistamine
  - Valijate, kandidaatide ja ringkondade seadistamine
- Hääletamisperiood
  - Kandidaatide nimekirjade väljastamine
  - Häälte vastu võtmine ja talletamine
  - Valijate nimekirjade uuendamine
  - Kontrollprotokolli rakendamine
- Tühistamisperiood
  - E-hääletanute nimekirja koostamine
  - Tühistus/ennistusnimekirjade rakendamine
- Lugemisperiood
  - Häälte anonümiseerimine
  - Anonümiseeritud häälte lugemine
- Lõpetamine

CYBERNETICA

Arhitektuur

- Valija komponendid
  - Valijarakendus
  - Kontrollrakendus
- Kesksüsteemi komponendid
  - HES – Häälteedastusserver
  - HTS – Häältetalletusserver
  - HLR – Häältelugemisrakendus
- Auditikomponendid
  - Logianalüüs, tervikluse kontroll
- Võtmehaldus HSM abil
- Sisendandmed
  - Kandidaatide nimekiri
  - Valijate nimekiri
  - Jaoskondade/ringkondade nimekiri
  - Hääled
- Tulemus
  - E-hääletanute nimekiri
  - Hääletamistulemus

CYBERNETICA

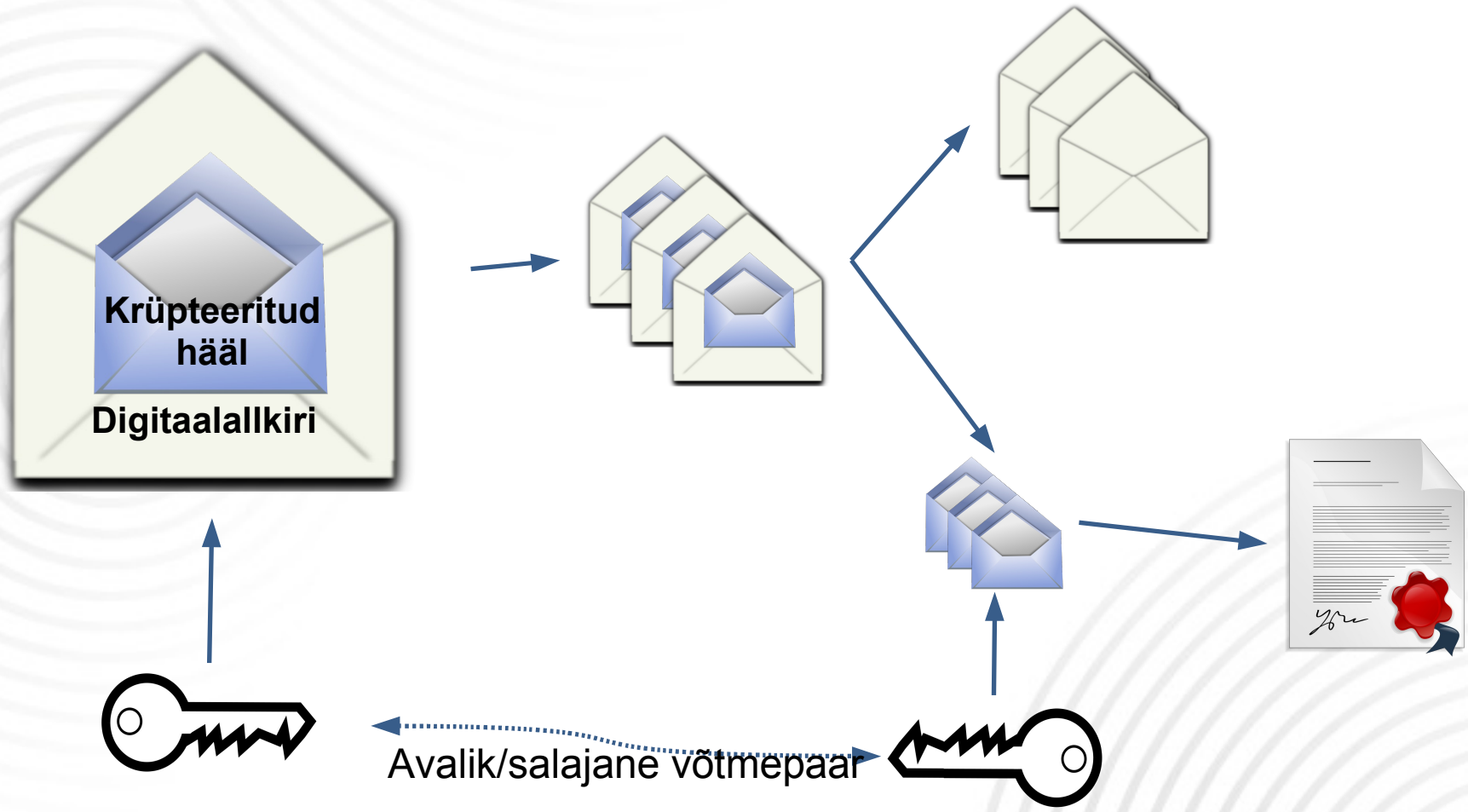
Hääletamine

(1): ID-kaardiga autentimine

(2): Kandidaatide nimekiri

(3): $Sig_V(Enc_S(Rnd,Vote))$

Hääle salajasus



CYBERNETICA

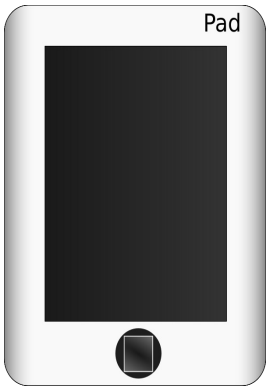
Laiendatud protokoll kontrollitavusega

(1):ID-kaardiga autentimine

(2): Kandidaatide nimekiri, OTP

(3): $Sig_V(Enc_S(Rnd,Vote))$

(4): Rnd, OTP



(5): OTP

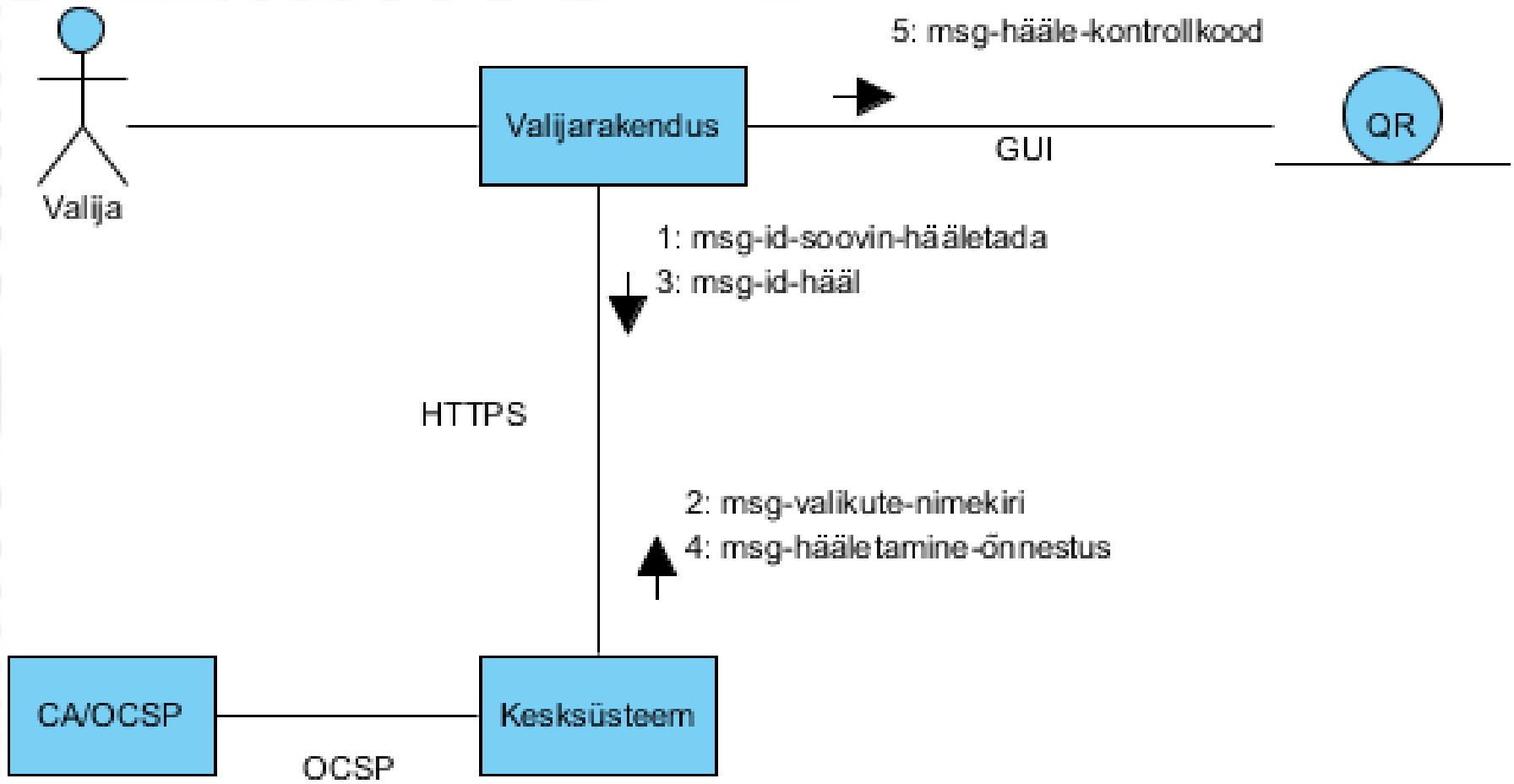
(6): $Sig_S(Sig_V(Enc_S(Rnd,Vote)))$ Kandidaatide nimekiri

CYBERNETICA

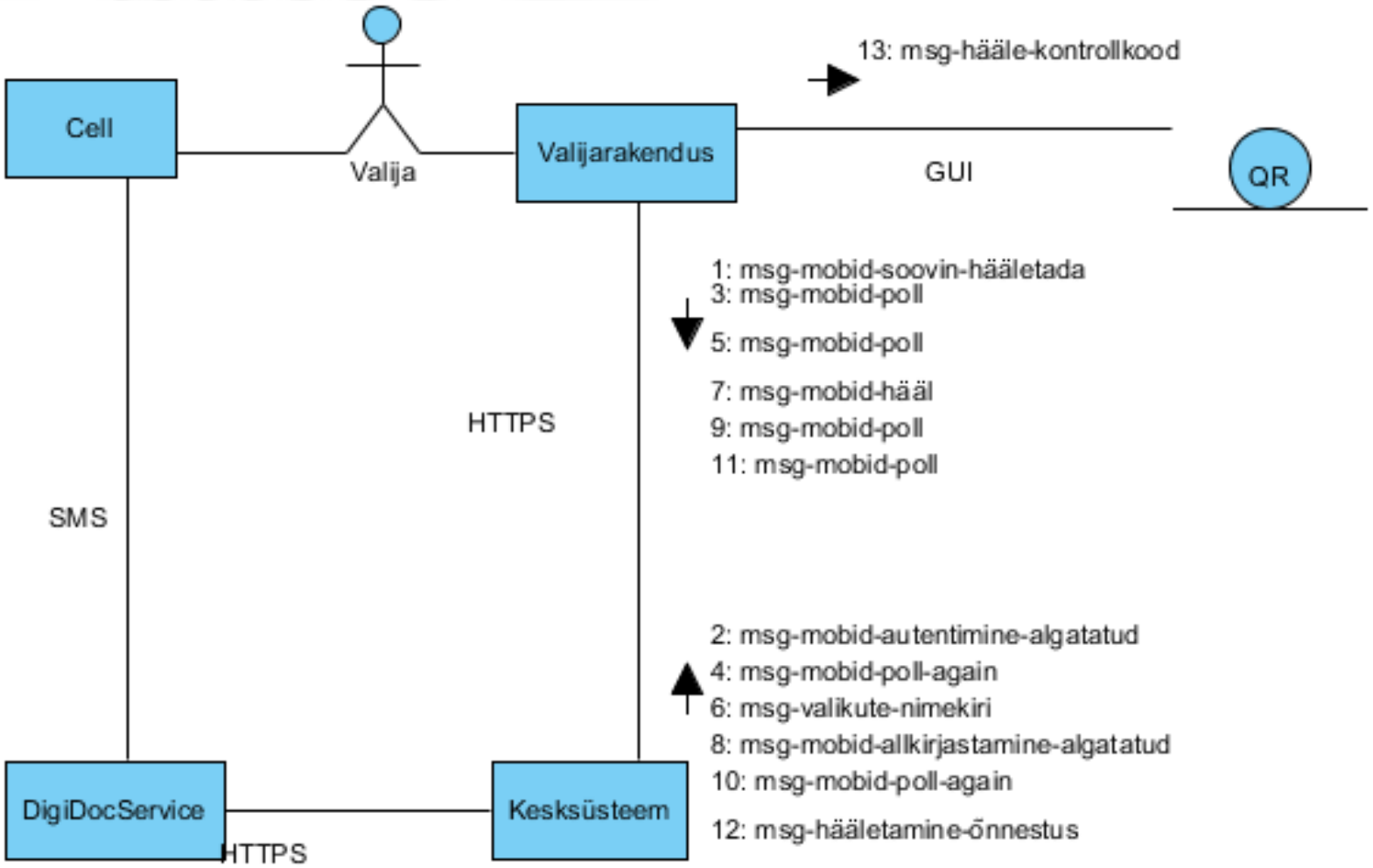
Protokollistik

- Ülddokument
  - Hääle vorming, jaoskonnad/ringkonnad, ühised andmed
- Hääletamisprotokoll
  - ID-kaart, Mobiil-ID
- Kontrollprotokoll
- Siseprotokollid
  - Sisendnimekirjade vorming, hääletamistulemus

Hääletamine ID-kaardiga



Hääletamine Mobiil-ID'ga



Hääle olekud

Hääl läbib oma eluea jooksul kesksüsteemis erinevad olekud:

LOG1: vastvõetud hääled kujul: *aeg, hash(hääl), ringkond, valimisjaoskond, IK*

LOG2: tühistatud hääled kujul: *aeg, hash(hääl), ringkond, valimisjaoskond, IK, põhjus*

LOG3: lugemisesse läinud hääled kujul: *aeg, hash(hääl), ringkond, valimisjaoskond, IK*

LOG4: kehtetud sedelid – vale kandidaadi nr. kujul: *aeg, hash(hääl), ringkond*

LOG5: arvestatud hääled kujul: *aeg, hash(hääl), ringkond*

Auditikomponendi kontrollida peale häälte lugemist

Lähtekood

- Debian Wheezy
- Python, C++
- CGI liidesed
- Ühiskomponendid
- Allkirjakomponent
- Administraatori komponent
- HES
- HTS
- HLR

Küsimused? sven.heiberg@cyber.ee

CYBERNETICA