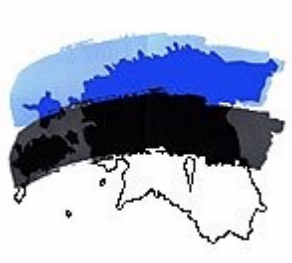
e-hääletamise süsteem IVXV



Tarvi Martens

Asjade seis 2015

- 10 aastat ja 8 hääletamist selja taga
- Uus süsteemi on valmis
- Eesmärgid uuendusele:
  - Ümberkirjutus
  - Paindlikum platvormivalik serveri poolele
  - Universaalsus
  - Otsast otsani verifitseeritavus

IVXV

hästi skaleeruv
otsast otsani verifitseeritav
e-hääletamise süsteem

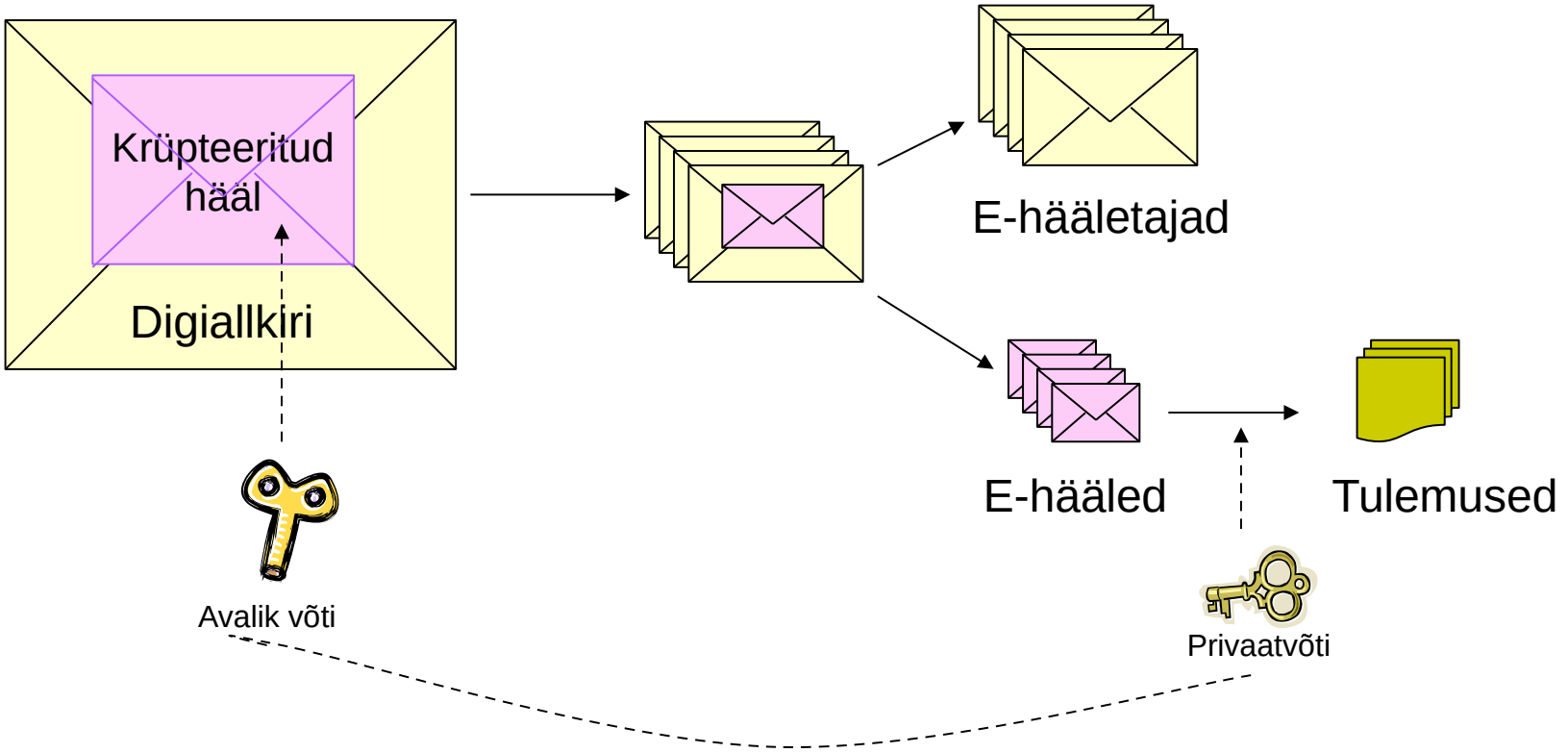
Otsast otsani (E2E) verifitseeritavus?

- Verifitseeritavus: protsessi sisendi ja väljundi sõltumatu kontrollimine
- Klassikaline E2E verifitseeritavus:

  „iga hääletaja saab veenduda, et tema konkreetne hääl läks arvesse“
- Aga kui on mitmekordne hääletamine?

  Hääletaja **ei tohi saada tõestada**, et tema konkreetne hääl läks arvesse
- E2E = salvestatud nagu kavatsetud + kokku loetud nagu salvestatud (1 hääl per hääletaja)

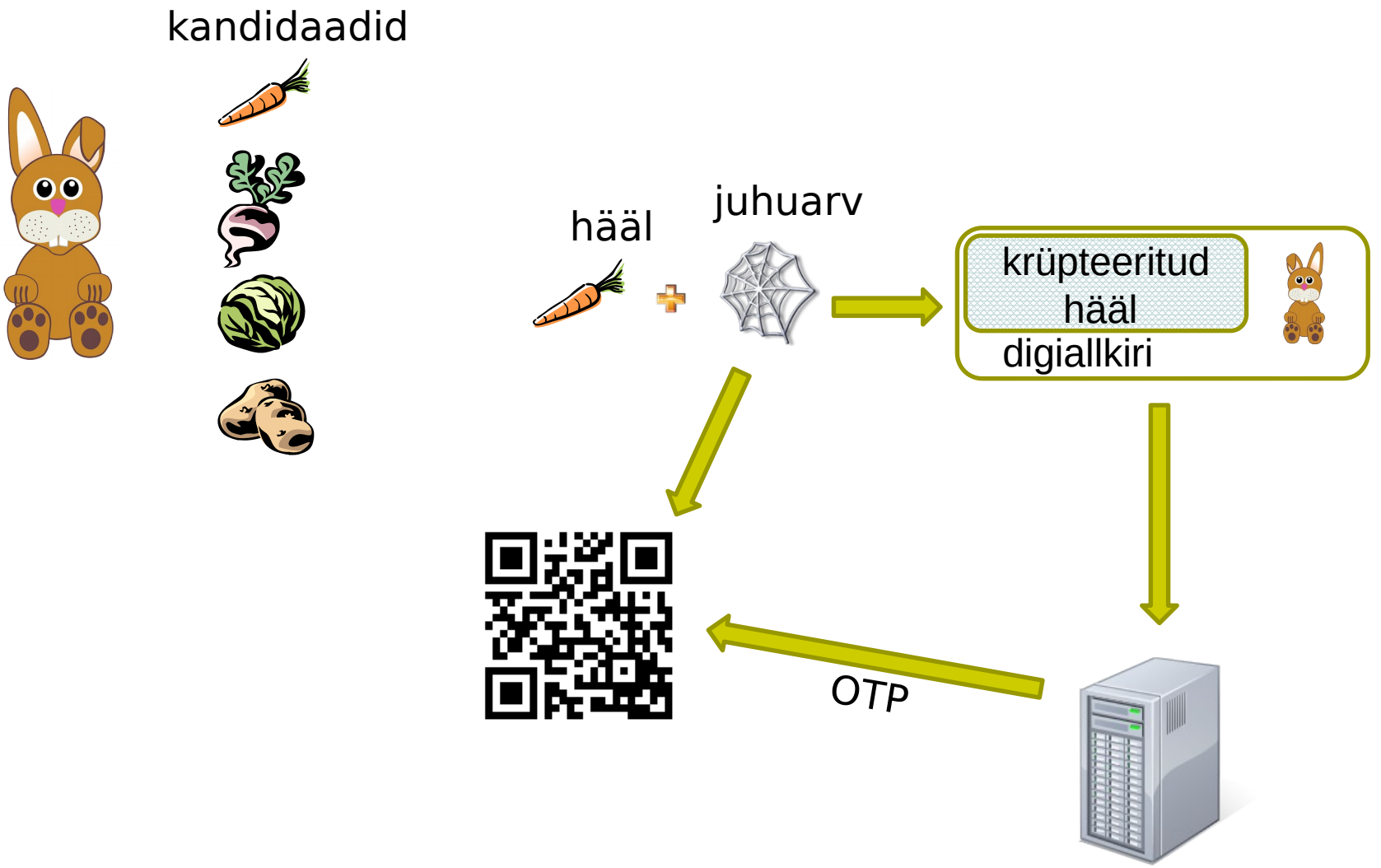
Ümbrikuskeem



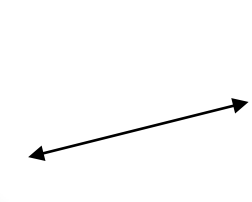
Salvestatud nagu kavatsetud

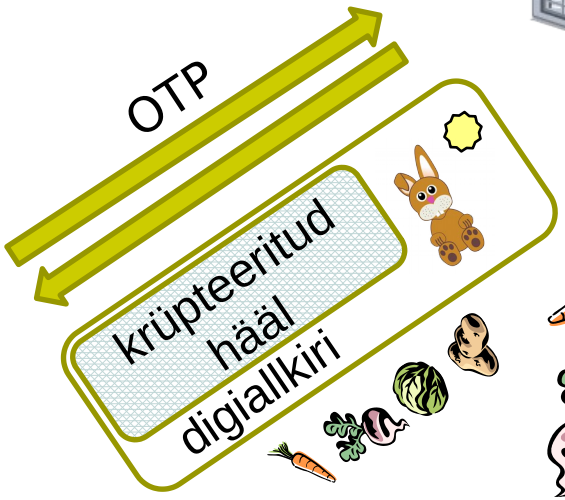
- Nutiseade, mis kontrollib arvuti abil antud hääle korrektsust
- Ammendav otsing kõigist võimalikest krüptogrammidest
  - Nutiseade teab krüpteermisel kasutatud juhuarvu
- Nutiseade verifitseerib ka allkirja
  - Ja seal sisalduvat ajatemplit

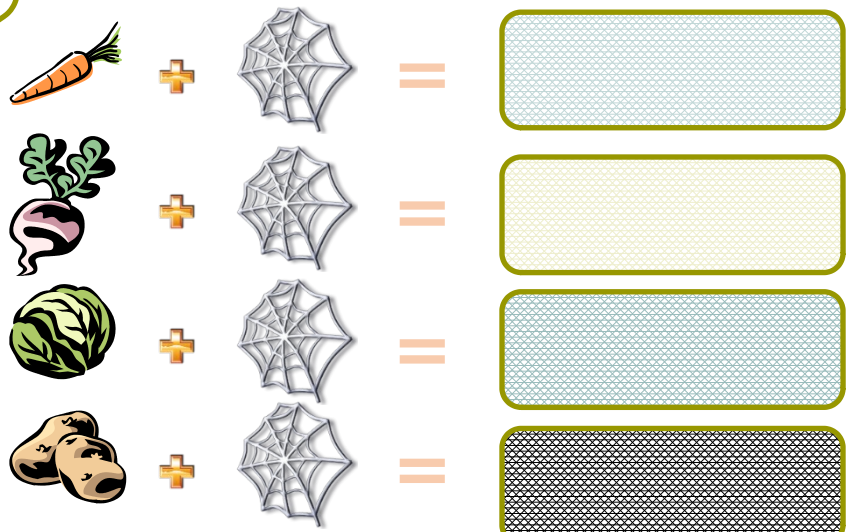
Valimine…


kandidaadid
hääl
juhuarv
krüpteeritud
hääl
digiallkiri
OTP

Verifitseerimine…



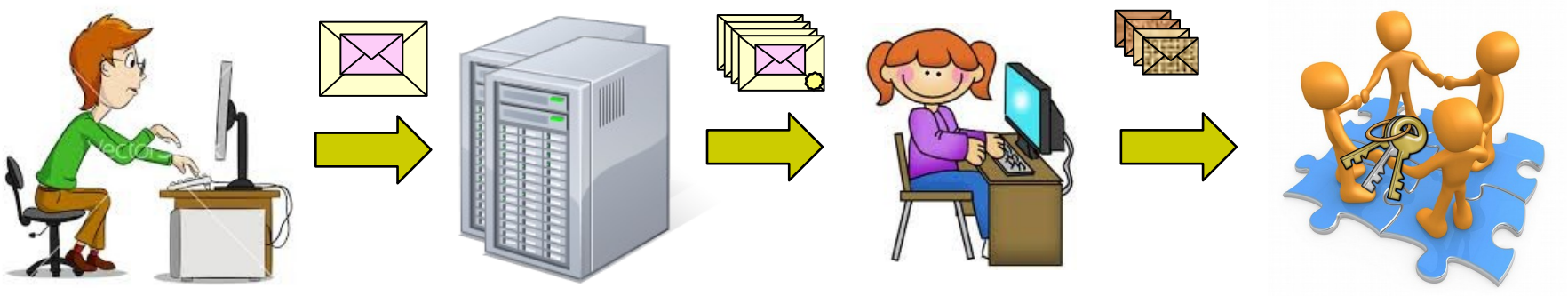




IVXV: Osapooled

- **Korraldaja** – valimiste korraldaja ja *Lugeja*
  - Defineerib valimised ja loeb hääled kokku
- **Hääletaja** – hääletab ja verifitseerib oma häält
- **Koguja** – kogub e-hääli (topeltümbrikuid)
- **Töötleja** – verifitseerib, anonümiseerib ja miksib e-hääli
- **Audiitor** – verifitseerib **andmeid**
- **muud** – ATO, STO, IdP, klienditugi jne

Osapooled



Hääletaja Koguja Töötleja Lugeja

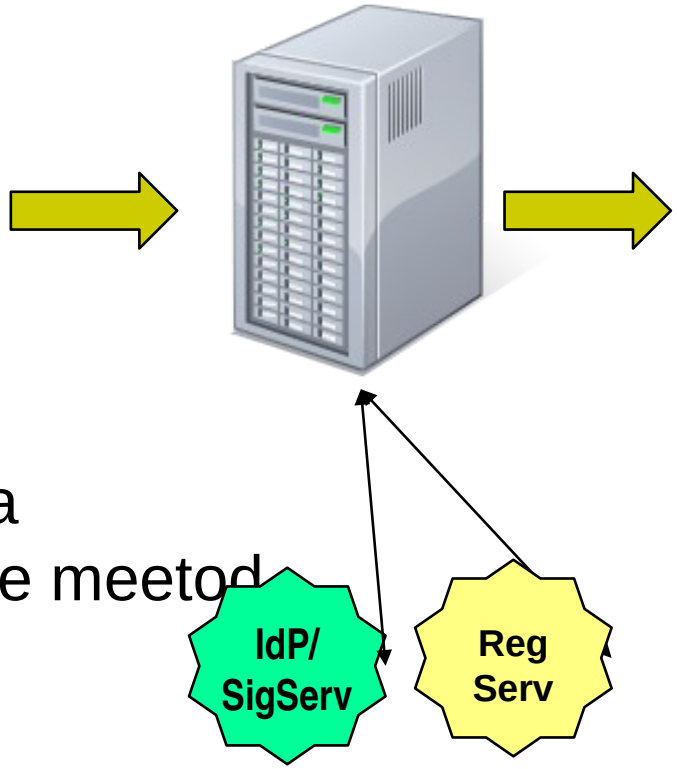
Korraldaja

- Paneb valimised püsti
  - Mida küsime, kes on kandidaadid?
  - Kes hääletavad?
  - Kas ja kuidas on kandidaadid jagatud ringkondade vahel?
  - Mis sorti krüptot ja võtmepikkusi kasutatakse hääle salastamiseks?
    - Genereerib võtmepaari – avaliku ja privaatvõtme
  - Millist hääletaja autentimist kasutatakse?
  - Millist digitaalallkirja süsteemi kasutatake?
- Loeb tulemused kokku

Koguja

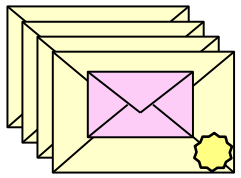
Sisend

- Hääletajad
- Kandidaadid
- Ringkonnad
- Avalik võti/ algoritm
- Autentimis- ja allkirjastamise meetod



Väljund

Topeltümbrikud – krüpteeritud ja allkirjastatud hääled



E-urni terviklus

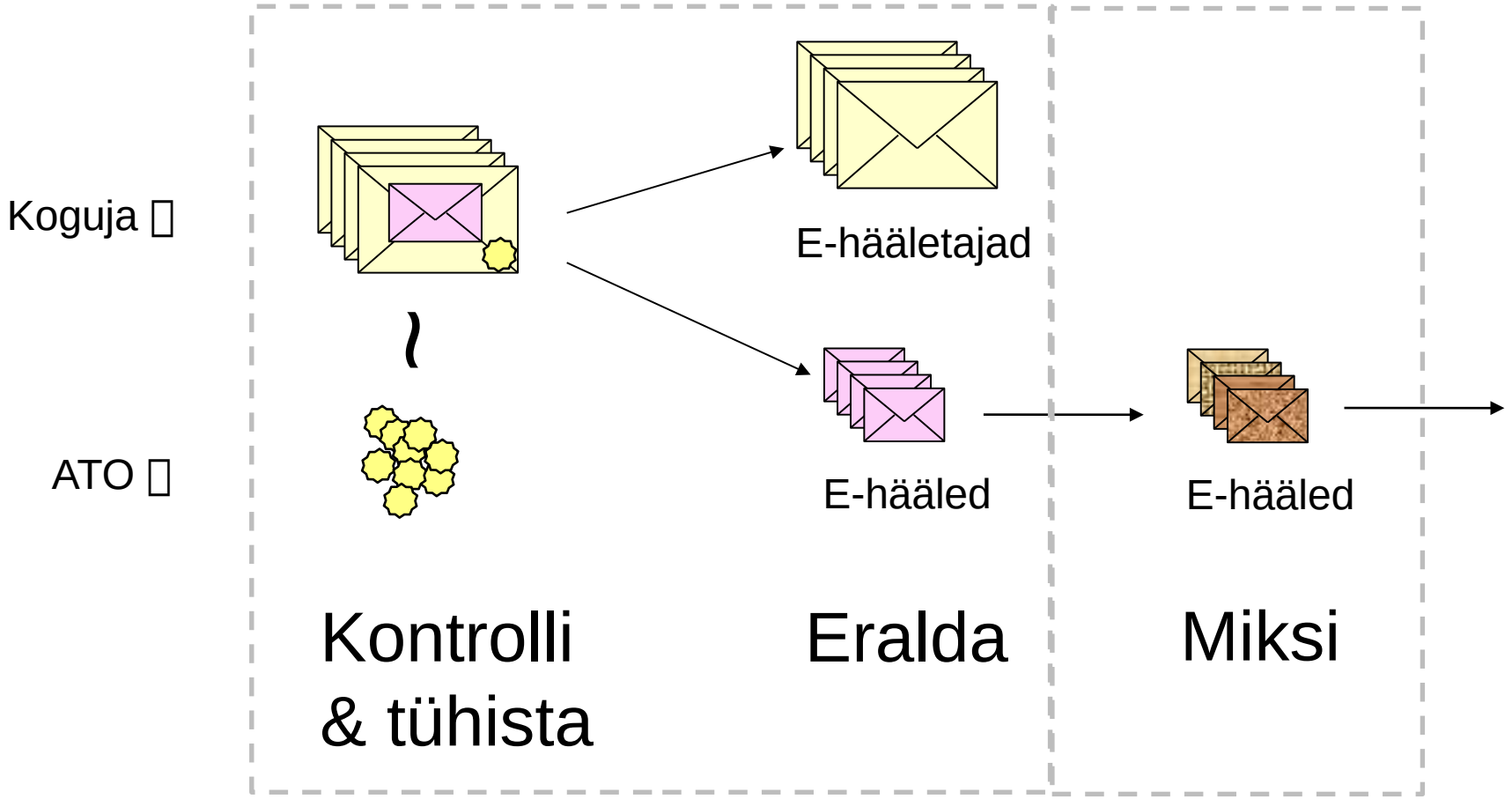
- Hääletaja on võimeline aru saama Koguja vigadest:
  - Pole nimekirjas, vale ringkond
  - Valed kandidaadid
  - Minu hääl ei verifitseeru

  Klienditeenindus peab olema ***läbipaistev***
- Hääli ei saa võltsida – digiallkiri peab vett
- Kas ikka kõik hääled anti üle?

Töötleja

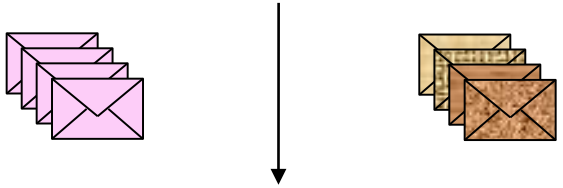
- Saab Kogujalt e-hääled
- Saab TSA käest kõik e-häältele väljastatud ajamärgendid
- Täielikkuse kontroll: iga ajamärgendi jaoks peab olema e-hääl
- Digiallkirjade verifitseerimine
- *Tühistamine*
- Ümbrikute lahutamine (anonümiseerimine)
- Miksimine

Töötleja ja miksija



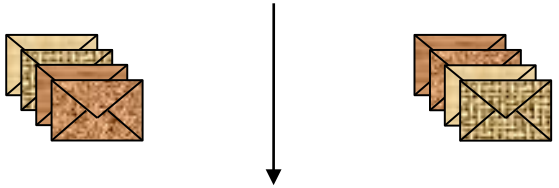
Miksimine

- **Ümberkrüpteerimine**

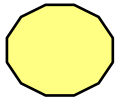


Vajab homomorfsete omadustega krüptosüsteemi (näiteks El Gamal)

- **Segamine**

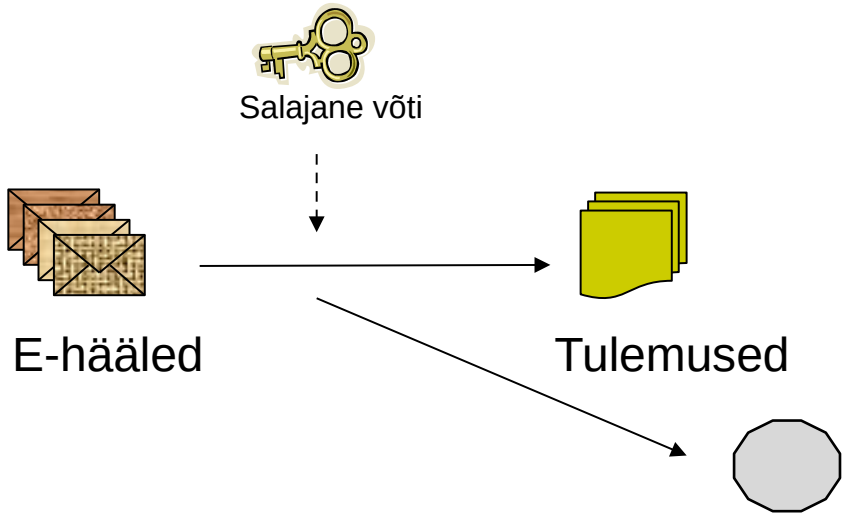


- **Väljastab korrektsustõestuse**



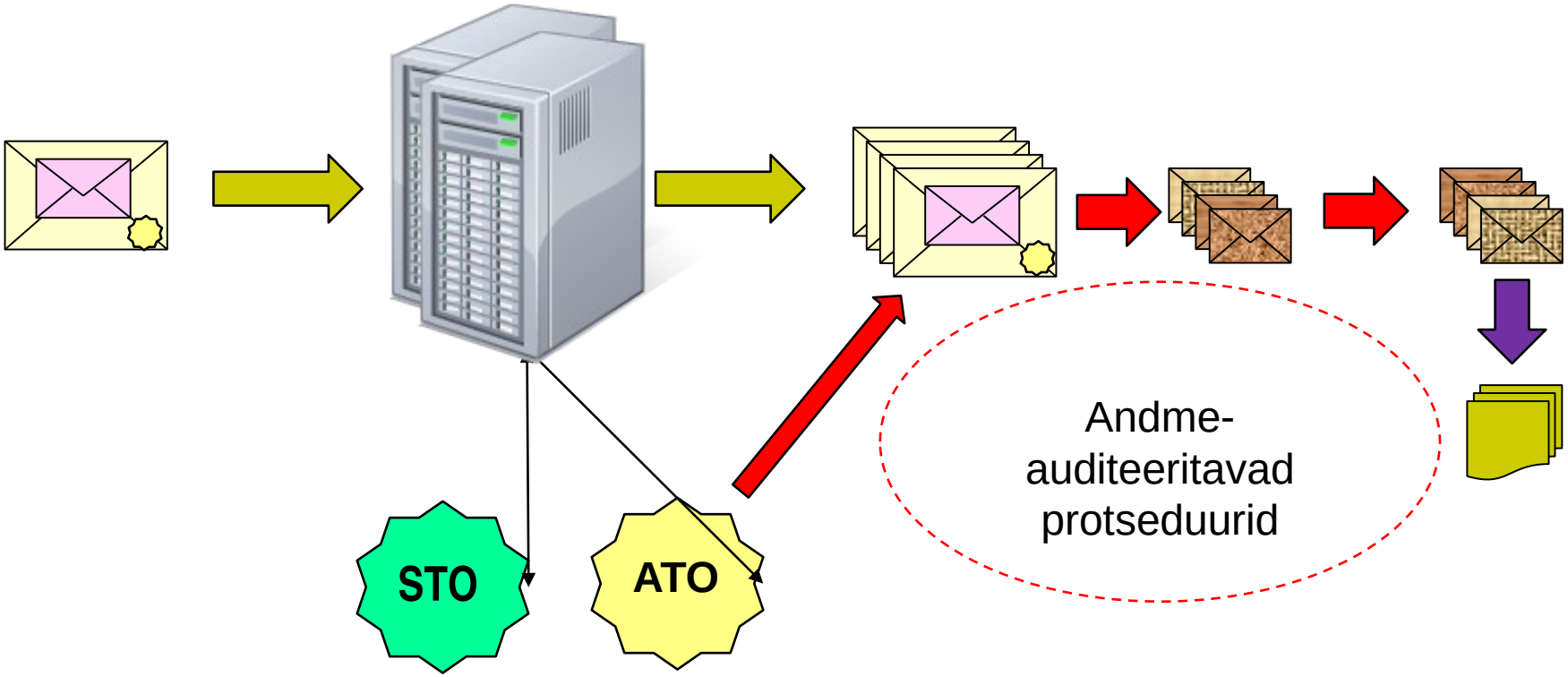
M-Tõend

Kokku lugemine



- Sisend ja väljund on avalik
- Homomorfne krüptosüsteem võimaldab väljastada korrektsustõestuse

Suur pilt



Audiitori/vaatleja tegevus

- Kõikide andmete terviklus ja autentsus
- Privaatvõtme kasutamine (protsess)
- Häälte verifitseerimine, komplekssuse kontroll, tühistamine, eraldamine – korda
- Häälte miksimine – kontrolli M-tõendi abil
- Häälte lugemine – kontrolli L-tõendi abil

Kontrollitavus

- Individuaalne kontrollitavus
  - Saab kontrollida ise tehtud tegevuse tulemit
- Universaalne kontrollitavus
  - „Kõik“ saavad kontrollida protsessi sisendit ja väljundit
  - Universaalselt kontrollitava asja võib teha valmis/edastada ebaturvalises keskkonnas!

Delegeeritud kontrollitavus

- *Osad* kontrollijad saavad teada millal kellegi viimane hääl anti
  - TSA, Koguja, Töötleja
  - Verifitseerijad (audiitor, vaatlejad)
- Need *osad* ei tohi seda teadmist kasutada ega levitada