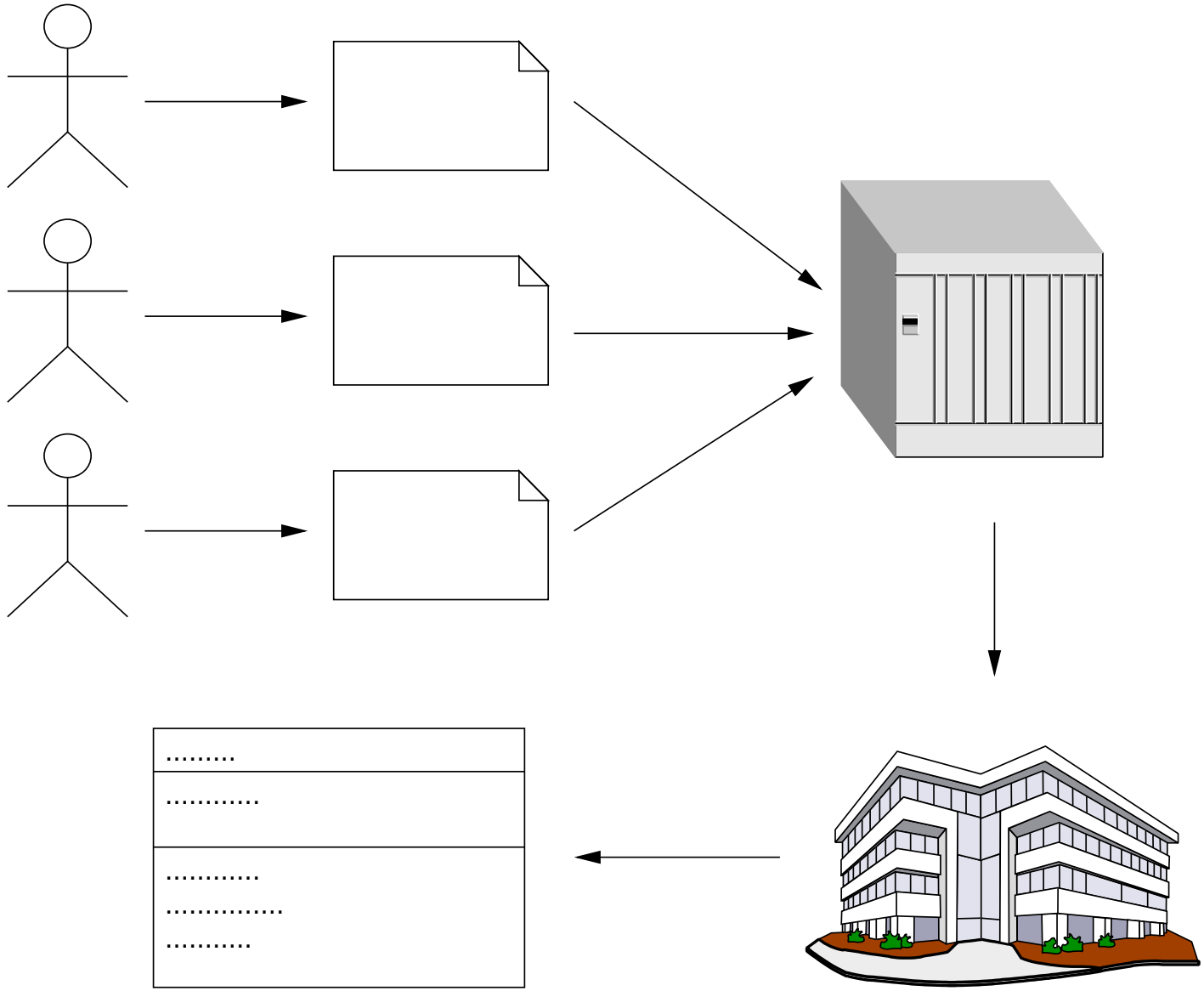
eValimised *vs* tValimised

Jan Willemson

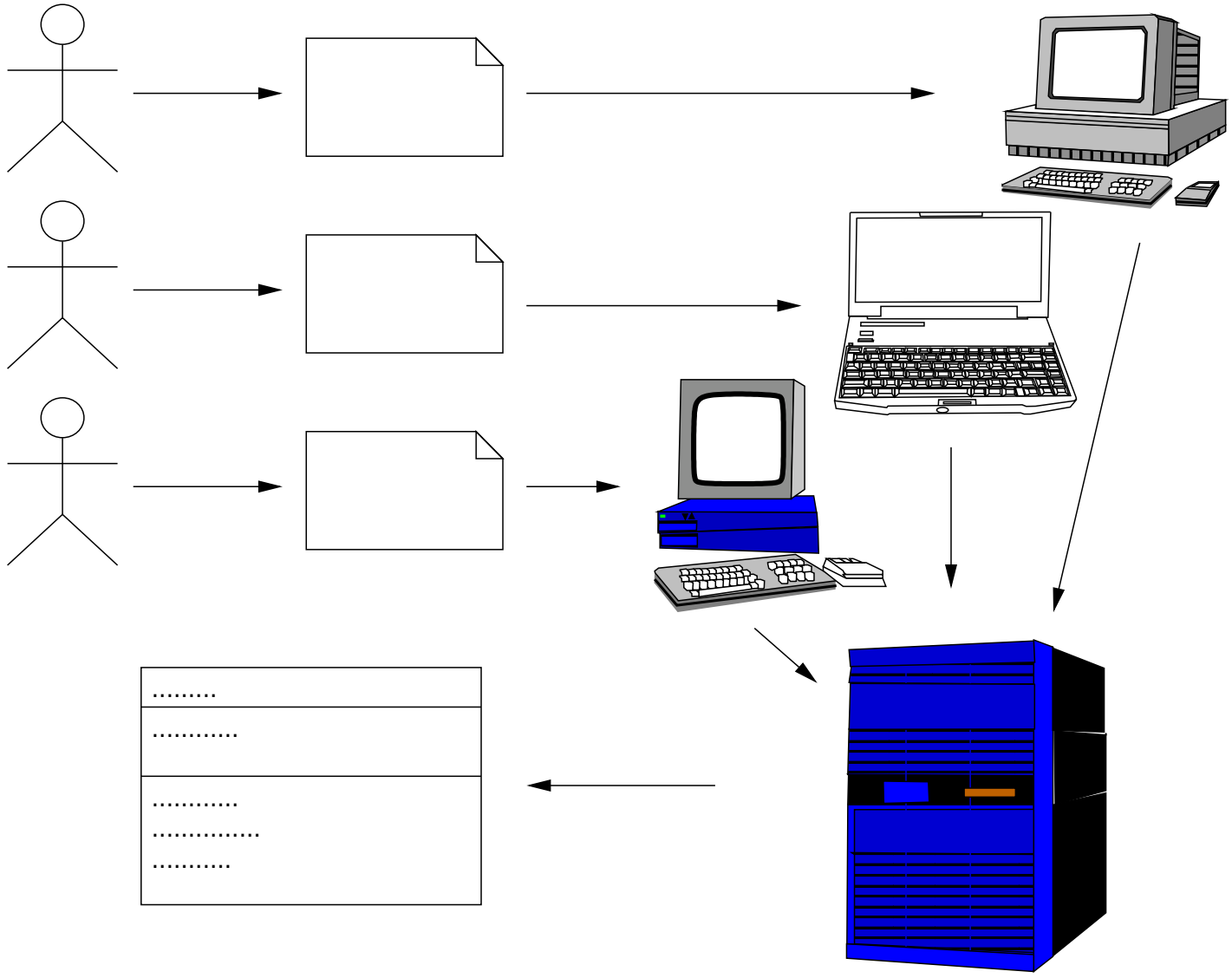
jan@cyber.ee

Cybernetica

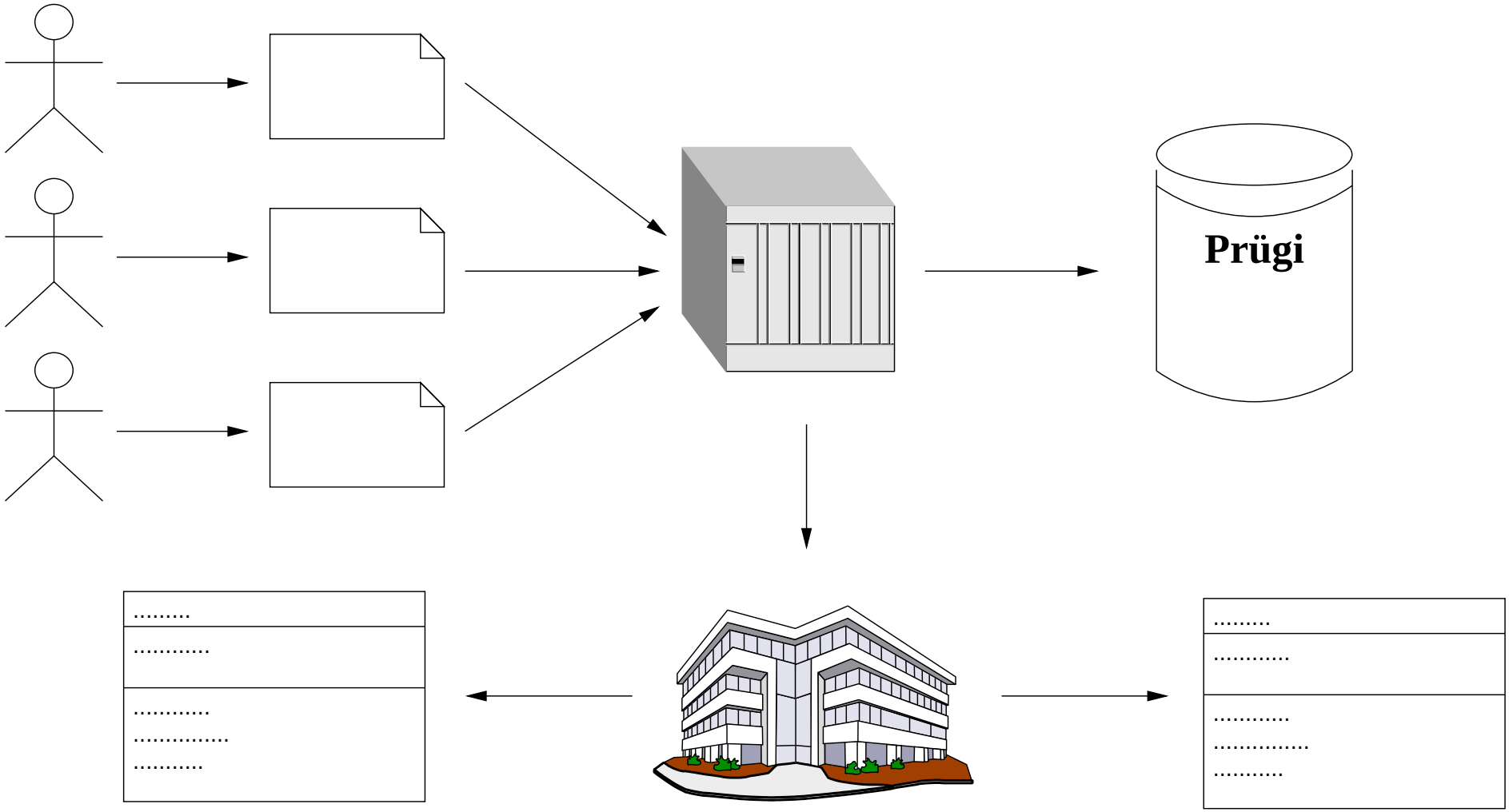
tValimised



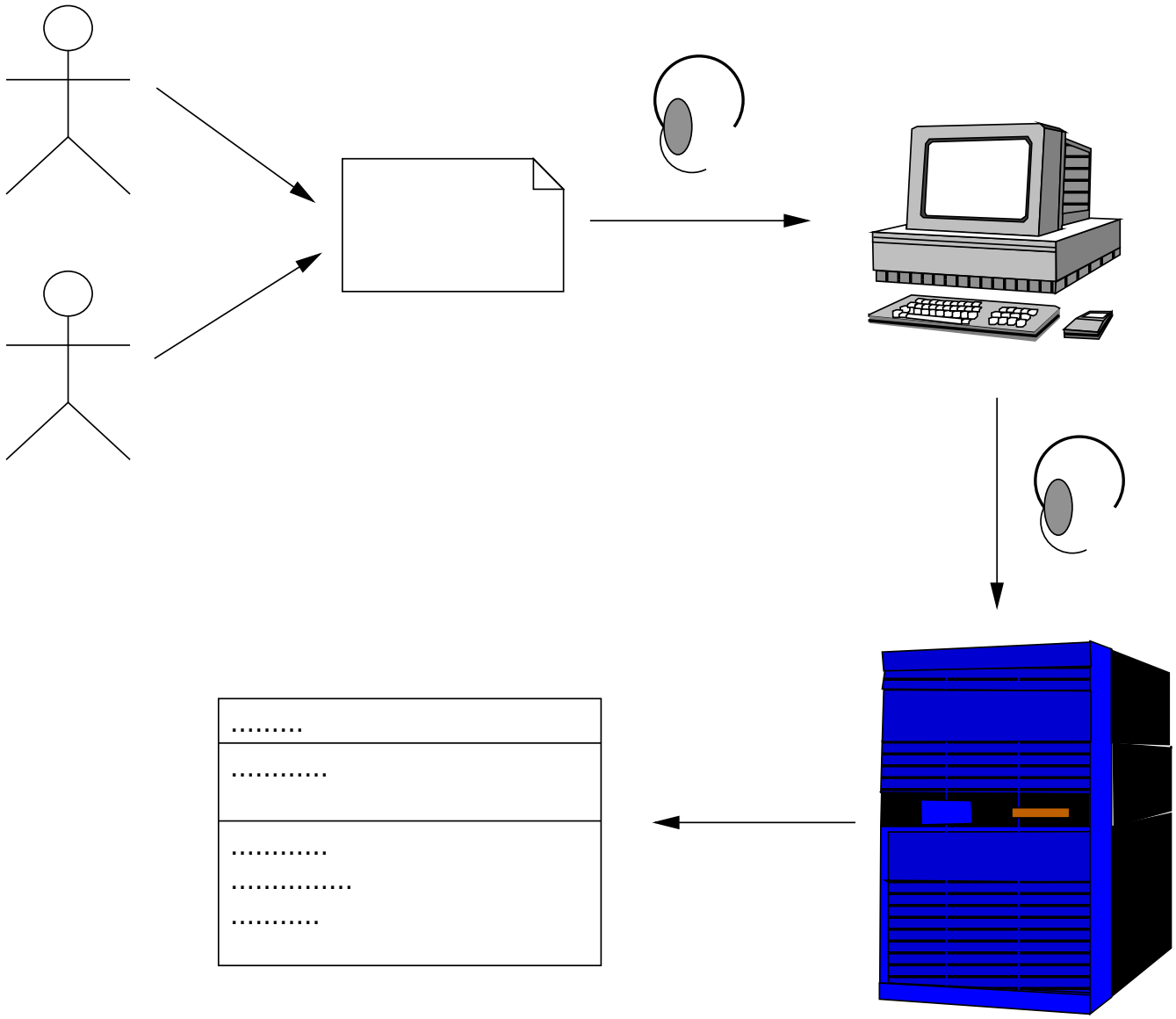
eValimised



t(e)Valimised – ohud



eValimised – ohud



Kas ohtude vastu saab?

- Kasutaja arvuti ründamise vastu ei anna eriti midagi teha

Kas ohtude vastu saab?

- Kasutaja arvuti ründamise vastu ei anna eriti midagi teha
- Samuti pole tegelikult võimalik tagada, et inimene ise oli see, kes hääletuse kinnituseks OK-nuppu vajutas

Kas ohtude vastu saab?

- Kasutaja arvuti ründamise vastu ei anna eriti midagi teha
- Samuti pole tegelikult võimalik tagada, et inimene ise oli see, kes hääletuse kinnituseks OK-nuppu vajutas
- Olukord on sarnane digitaalallkirjaga, mille korral me ei või 100% inimese enda osaluses kindlad olla; sellegipoolest inimene *vastutab* oma allkirja eest

Hääletamise salajasus

- Riigikogu Valimise seadus §1:

  (2) Riigikogu liikmete valimised on vabad, üldised, ühetaolised ja otsesed. Hääletamine on salajane.

Hääletamise salajasus

- Riigikogu Valimise seadus §1:

  (2) Riigikogu liikmete valimised on vabad, üldised, ühetaolised ja otsesed. Hääletamine on salajane.

- Elektroonilistel kommunikatsioonikanalitel (telefon, Internet) on pealtkuulamist raske välistada; pealtkuulatavus aga rikub salajasuse nõuet

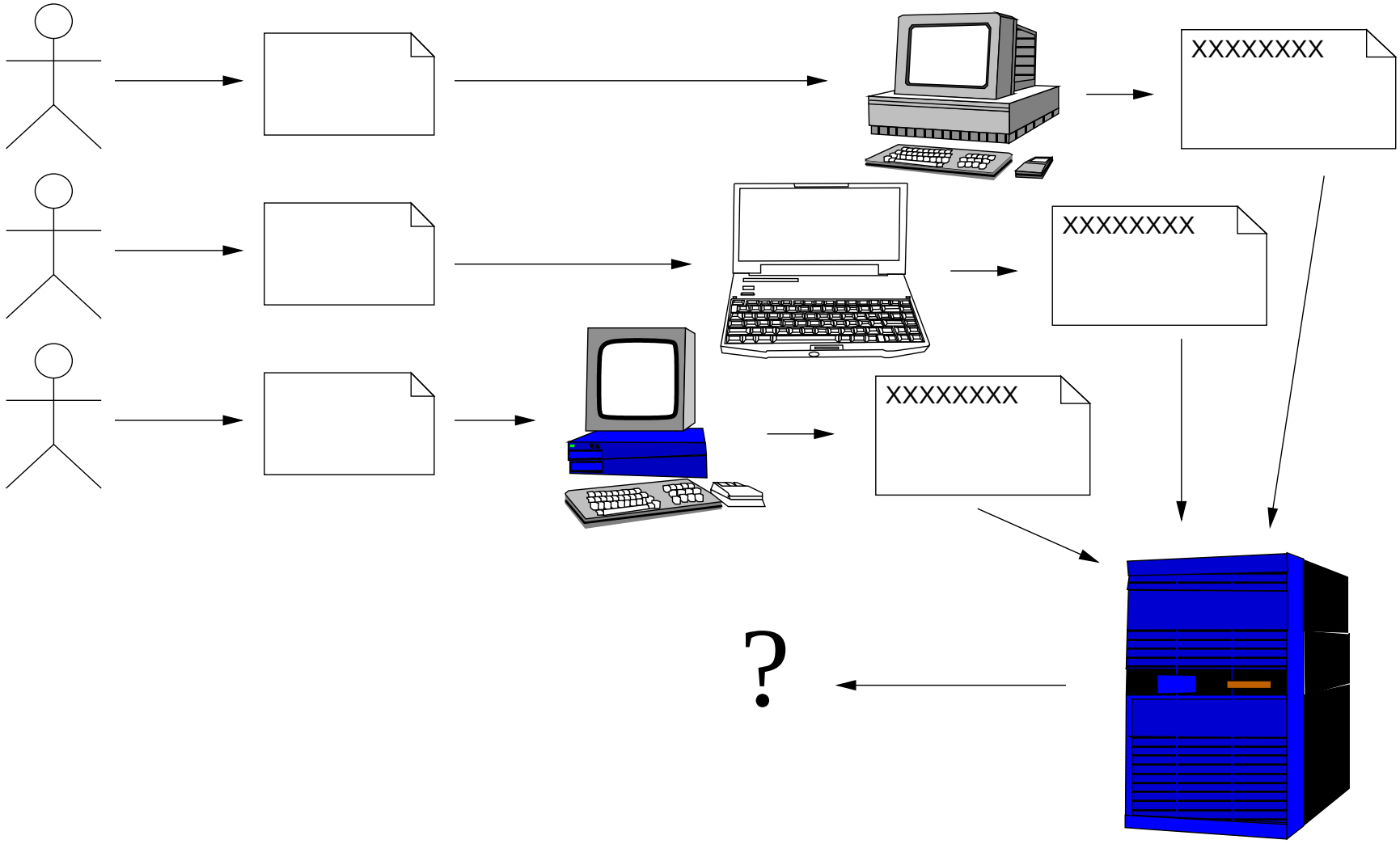
Hääletamise salajasus

- Riigikogu Valimise seadus §1:

  (2) Riigikogu liikmete valimised on vabad, üldised, ühetaolised ja otsesed. Hääletamine on salajane.

- Elektroonilistel kommunikatsioonikanalitel (telefon, Internet) on pealtkuulamist raske välistada; pealtkuulatavus aga rikub salajasuse nõuet
- Parim olemasolev lahendus on hääled kodeerida

Häälte krüptimine



Kuidas hääli kokku lugeda?

- Server võib kõigepealt dekrüptida hääled ja siis tulemused liita

Kuidas hääli kokku lugeda?

- Server võib kõigepealt dekrüptida hääled ja siis tulemused liita
  - Sel juhul saab server teada kõigi kodanike häälte väärtused

Kuidas hääli kokku lugeda?

- Server võib kõigepealt dekrüptida hääled ja siis tulemused liita
  - Sel juhul saab server teada kõigi kodanike häälte väärtused
- Server võib kõigepealt kombineerida krüptogrammid ja seejärel dekodeerida kombineeritud krüptogrammi

Kuidas hääli kokku lugeda?

- Server võib kõigepealt dekrüptida hääled ja siis tulemused liita
  - Sel juhul saab server teada kõigi kodanike häälte väärtused
- Server võib kõigepealt kombineerida krüptogrammid ja seejärel dekodeerida kombineeritud krüptogrammi
  - Sel juhul tuleb kuidagi eraldi kontrollida, et krüptogramm sisaldab korrektselt antud häält, aga mitte suvalisi bitte, sest vastasel korral ei tule krüptogrammide kombinatsioon korrektne. Selline kontroll on võimalik, aga nõuab väga spetsiifilist klienditarkvara

Kuidas hääli kokku lugeda?

- Server võib kõigepealt dekrüptida hääled ja siis tulemused liita
  - Sel juhul saab server teada kõigi kodanike häälte väärtused
- Server võib kõigepealt kombineerida krüptogrammid ja seejärel dekodeerida kombineeritud krüptogrammi
  - Sel juhul tuleb kuidagi eraldi kontrollida, et krüptogramm sisaldab korrektselt antud häält, aga mitte suvalisi bitte, sest vastasel korral ei tule krüptogrammide kombinatsioon korrektne. Selline kontroll on võimalik, aga nõuab väga spetsiifilist klienditarkvara
- Küsimus, kumb kurat on heledam, ootab poliitilist vastust

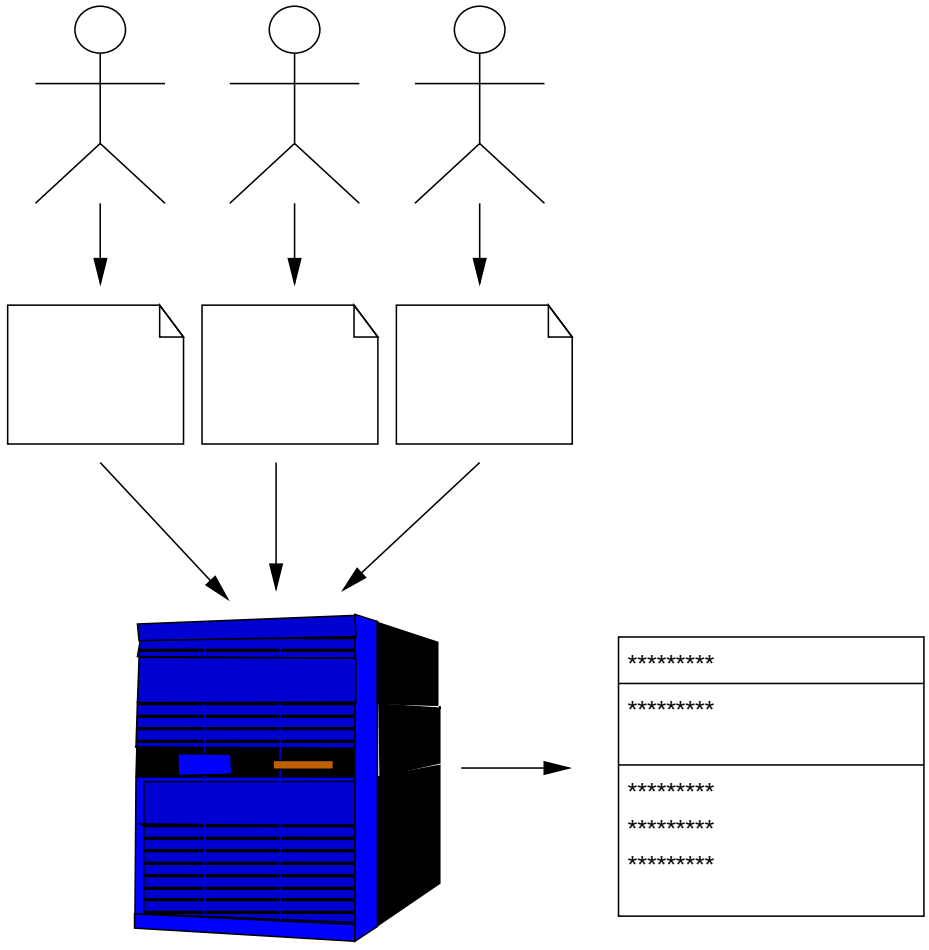
Server teab kõike

- Tegelikult osutub, et isegi juhul, kui server ei oska üksikhääli dekrüptida, suudab ta kõigi kodanike häälte väärtused teada saada

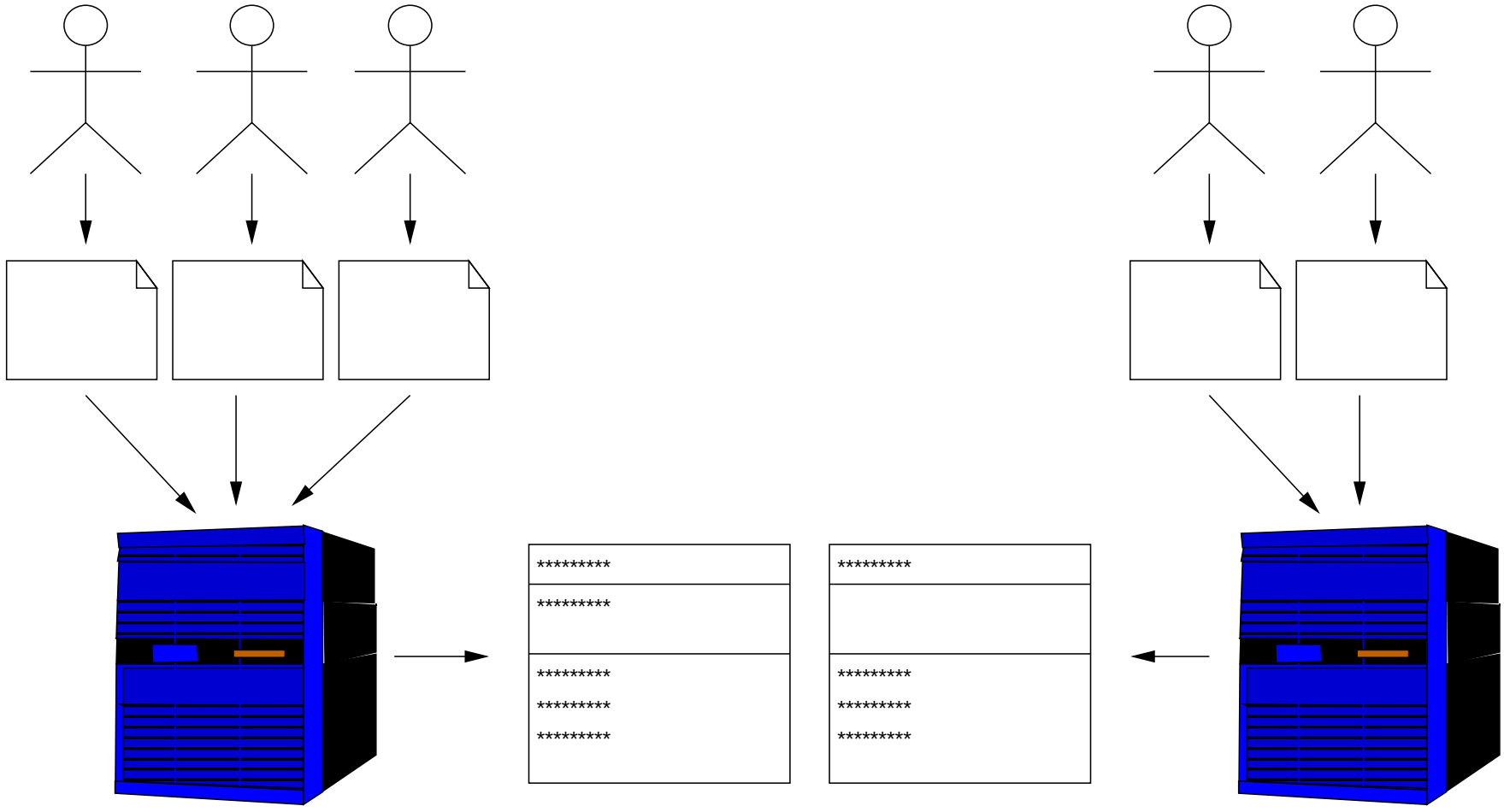
Server teab kõike

- Tegelikult osutub, et isegi juhul, kui server ei oska üksikhääli dekrüptida, suudab ta kõigi kodanike häälte väärtused teada saada
- Järelikult võib serverile häälte dekodeerimise võime ka anda, see ei muuda turvalisuse seisukohast midagi, sest serverit tuleb nagunii usaldada

Miks server kõike teab?



Miks server kõike teab?



e-häälte kopeeritavus

- Viimane rünne on võimalik tänu sellele, et e-hääli võib jälgi jätmata kopeerida ja neid hiljem edasi analüüsida; t-häälte korral niisugust probleemi ei esine

e-häälte kopeeritavus

- Viimane rünne on võimalik tänu sellele, et e-hääli võib jälgi jätmata kopeerida ja neid hiljem edasi analüüsida; t-häälte korral niisugust probleemi ei esine
- Me tahame, et häälte salajasus säiliks potentsiaalselt lõpmata kaua (nt et vältida hilisemaid repressioone) . . .

e-häälte kopeeritavus

- Viimane rünne on võimalik tänu sellele, et e-hääli võib jälgi jätmata kopeerida ja neid hiljem edasi analüüsida; t-häälte korral niisugust probleemi ei esine
- Me tahame, et häälte salajasus säiliks potentsiaalselt lõpmata kaua (nt et vältida hilisemaid repressioone) . . .
- . . . samas on krüptoalgoritmidel omadus aja jooksul nõrgeneda ja keegi ei garanteeri, et kuu aega pärast valimisi ei või suvaline osapool kõiki võrgust salvestatud hääli lahti murda

Kokkuvõtteks

- Digitaalinformatsioonil on võrreldes paberinformatsiooniga mitmeid mugavaid, aga ka mitmeid ebamugavaid omadusi

Kokkuvõtteks

- Digitaalinformatsioonil on võrreldes paberinformatsiooniga mitmeid mugavaid, aga ka mitmeid ebamugavaid omadusi
- Tänu sellele ei saa kõiki tavalistest valimistest tuttavaid teadmisi ja ootusi automaatselt e-valimistele üle kanda

Kokkuvõtteks

- Digitaalinformatsioonil on võrreldes paberinformatsiooniga mitmeid mugavaid, aga ka mitmeid ebamugavaid omadusi
- Tänu sellele ei saa kõiki tavalistest valimistest tuttavaid teadmisi ja ootusi automaatselt e-valimistele üle kanda
- Digitaalmaailmas võib ette tulla takistusi, mis füüsilises maailmas ei realiseeru

Kokkuvõtteks

- Digitaalinformatsioonil on võrreldes paberinformatsiooniga mitmeid mugavaid, aga ka mitmeid ebamugavaid omadusi
- Tänu sellele ei saa kõiki tavalistest valimistest tuttavaid teadmisi ja ootusi automaatselt e-valimistele üle kanda
- Digitaalmaailmas võib ette tulla takistusi, mis füüsilises maailmas ei realiseeru
- Keegi pole veel suutnud adekvaatselt hinnata, kas e-valimised ikka lahendavad rohkem probleeme kui nad neid tekitavad