# Usaldatavuse uuringud

## Tehnoloogia vaade

**Ahto Buldas ja Märt Saarepera**

# Taust ja kava

Kas, millal ja milleks saab (arvuti) süsteeme usaldada?

Näiteks:

- Kas m-valimine on piisavalt usaldatav?
- Kas ID-kaart on piisavalt usaldatav (“turvaline”)?

Kas plokiaheltehnoloogia tagab süsteemide absoluutse usaldatavuse?

**Ettekande kava**:

Osa 1: Süsteemide vea- ja ründekindlus

Osa 2: Väliselt auditeeritavad süsteemid ja plokiahelad

# Osa 1:
# Süsteemide vea- ja ründekindlus

# Andmetöötlus arvutis

Arvutusülesanne -> Algoritm -> Programm -> Programmi täitmine

**Praktilised piirangud**:

Arvutusülesannetel on keerukus: kõik ülesanded ei tarvitse olla tänastele arvutitele jõukohased

Arvutites kui masinates tuleb arvestada vigadega (rikked, tõrked): vigu ei ole võimalik kunagi täielikult välistada

Saab ainult küsida: Kui töökindel arvuti on? Kui kaua ta on võimeline vigadeta töötama mingis keskkonnas?

# Vigade liigid

Juhuslikud keskkonnast tulenevad vead

Süstemaatilised vead: juhuslik viga programmis või aparatuuris

Ründetegevusest tulenevad vead: ründaja muudab tahtlikult andmeid, programmi või aparatuuri

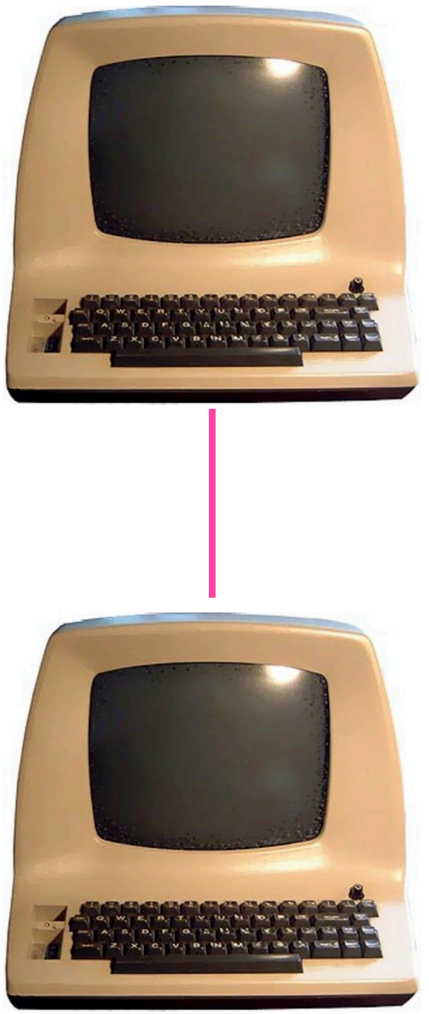
# Arvutivõrgud ja sidevead

Süsteemi spetsifikatsioon -> Protokoll -> Protsessid -> Protokolli teostamine arvutivõrguna

Juhuslikud sidekanalist tulenevad vead

Süstemaatilised vead: viga protokollis, näiteks tekib tupik (*deadlock*)

Ründetegevusest tulenevad vead: ründaja muudab edastatavaid andmeid või loeb konfidentsiaalseid andmeid



# Veahalduse strateegia

Vältimine -> Avastamine -> Parandamine

**Veahalduse etapid**:

- Vea vältimine: kvaliteetsemad materjalid, paremad sidekanalid, ründekindlamad krüpteerimisalgoritmid jne. Vigu ei saa kunagi täielikult vältida
- Vea avastamine: veaavastusmeetmed on süsteemi osa
- Vea parandamine: süsteemi taaste (automaatne või mitte). Eeldab vea avastatavust.

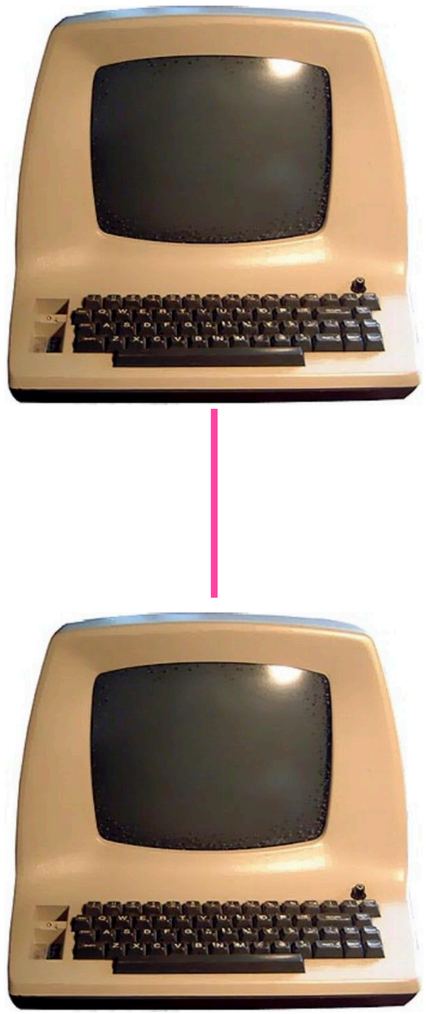
# Süsteemi Spetsifikatsioon

Funktsionaalsed nõuded: mida süsteem peab tegema

Mittefunktsionaalsed nõuded:

- Jõudlus ja sidevajadused
- Veakindlus
- Ründekindlus

Süsteemi teostus peab sisaldama veahaaldust



# Süsteem + Organisatsioon

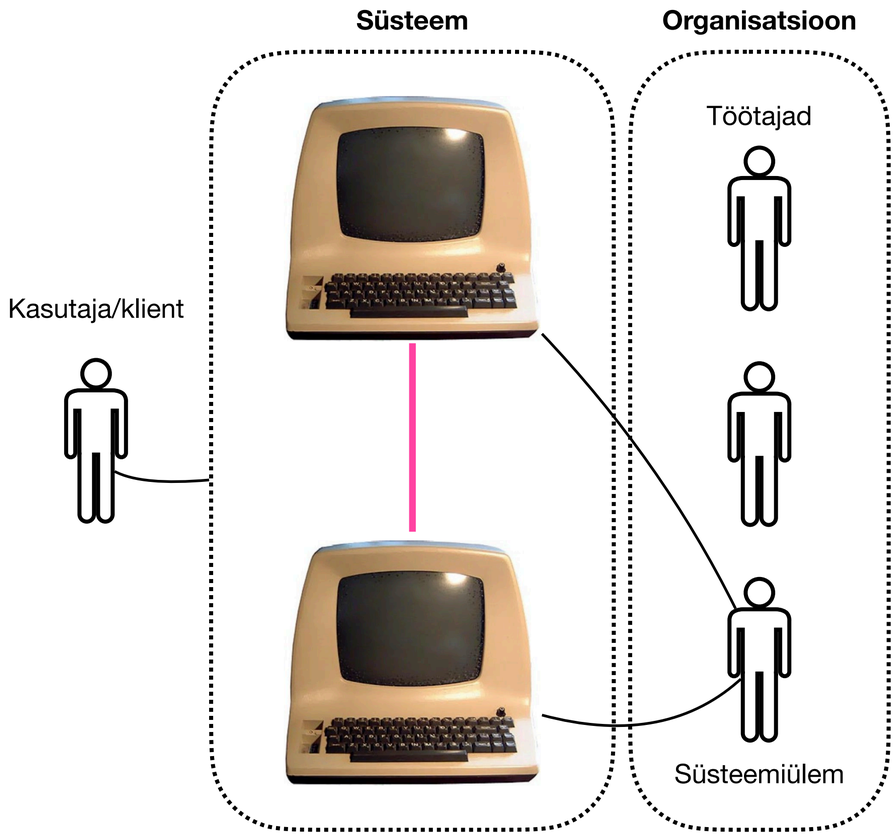
Spetsifikatsioon peab arvestama ka organisatsiooniga:

- Inimvead
- Siseohud

Süsteemi olemasolust tulenev eeldatav kasu peab ületama süsteemi vigadest tuleneva eeldatava kahju

Seega, iga uue süsteemi kasutuselevõtt eeldab:

- süsteemist tuleneva kasu hindamist
- süsteemi vigadest (sh rünnetest) tuleneva kahju hindamist



# Süsteemi ründekindlus

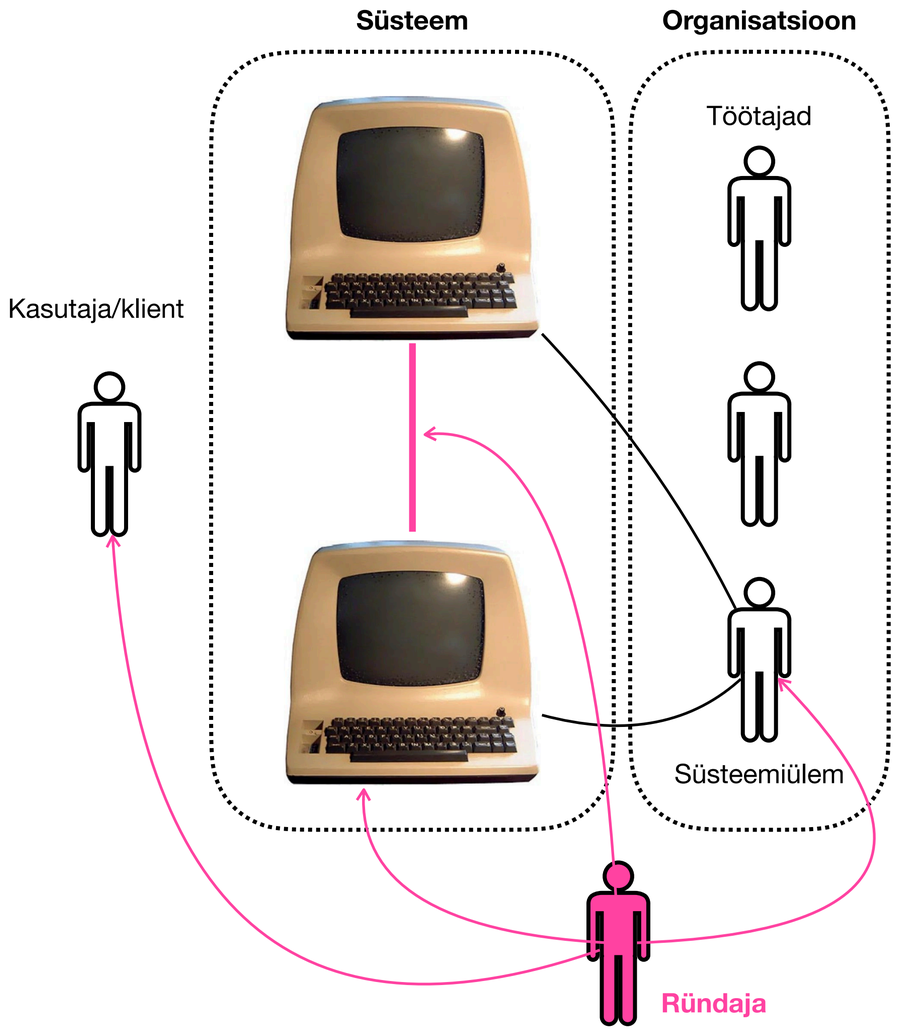
Süsteemi (ja organisatsiooni) võime taluda ründeid

Rünne = projekt, millel on:

- maksumus (arvutusprotsessi kulud, suhtluskulud)
- õnnestumise tõenäosus
- toimumise tõepära (sõltub ründaja tahtest)

**Ründaja motivatsioon**:

- kasu saamine (majanduslikult motiveeritud ründed)
- kahju tekitamine (näiteks militaarründed)



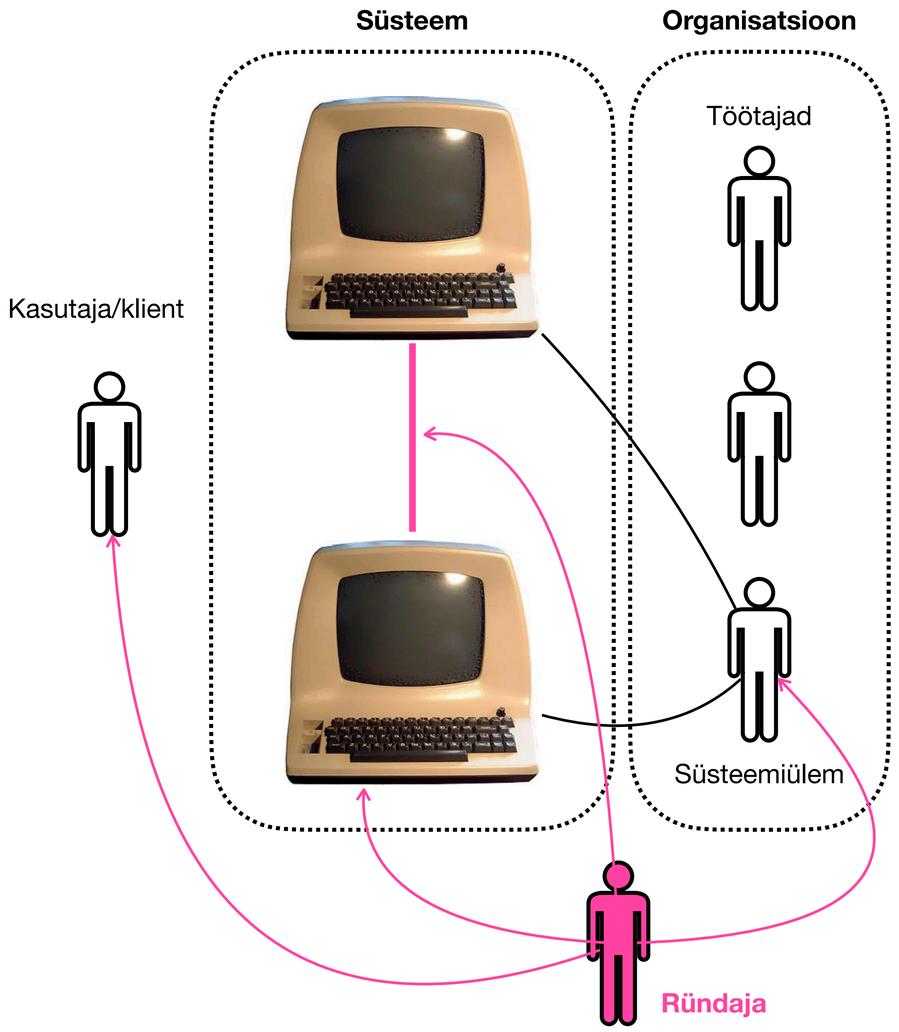
# Süsteemi ründekindlus

**Ründekindluse tagamine/analüüs**:

1. Tõepäraste rünnete loendi fikseerimine
2. Iga ründe kui projekti hindamine
3. Otsus — aktsepteerimine/süsteemi muutmine

**Ründekindluse astmed**:

- Kommertsturve — ründed on ründajale majanduslikult kahjulikud
- Strateegiline turve — tõepäraste rünnete õnnestumise tõenäosus on piisavalt väike



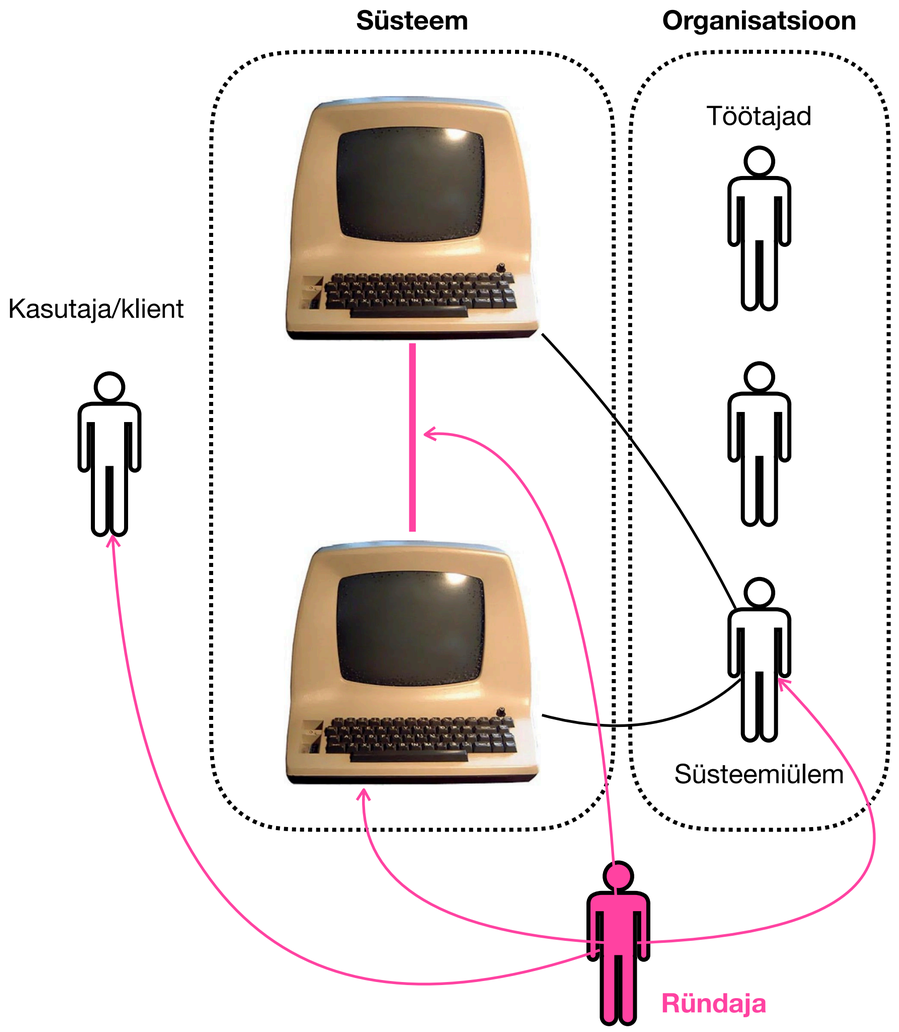
# Süsteemi ründekindlus

**Praktilised piirangud**:

- Tõepäraste rünnete nimistu ei tarvitse olla täielik
- Ründaja motivatsiooni põhineb ainult mudelil
- Rünnete toimumist ei saa kunagi täielikult välistada
- Rünnete mittetoimumine (kui olukord — nn. “turvalisus”) ei ole vaadeldav nähtus

**Kokkuvõte**:

- Süsteemi aktsepteerimise otsus põhineb alati vaid teadaoleval informatsioonil ja süsteemi mudelil
- Mida parem mudel, seda väiksem on ründekahju



# Vea- ja Ründekindla Süsteemi Loomine

Algne spetsifikatsioon: sisaldab vea- ja ründekindluse nõudeid

Tehniline ja organisatsiooniline spetsifikatsioon

Vea- ja ründekindluse analüüs

Tellija otsus: põhineb analüüsil

Süsteemi teostus

# Osa 2:
# Väliselt auditeeritavad süsteemid ja plokiahelad

# Perimeetriturvalisusega süsteem

Süsteemi töö põhineb reeglitel: tehingukorraldused muudavad ettenähtud viisil süsteemi olekut

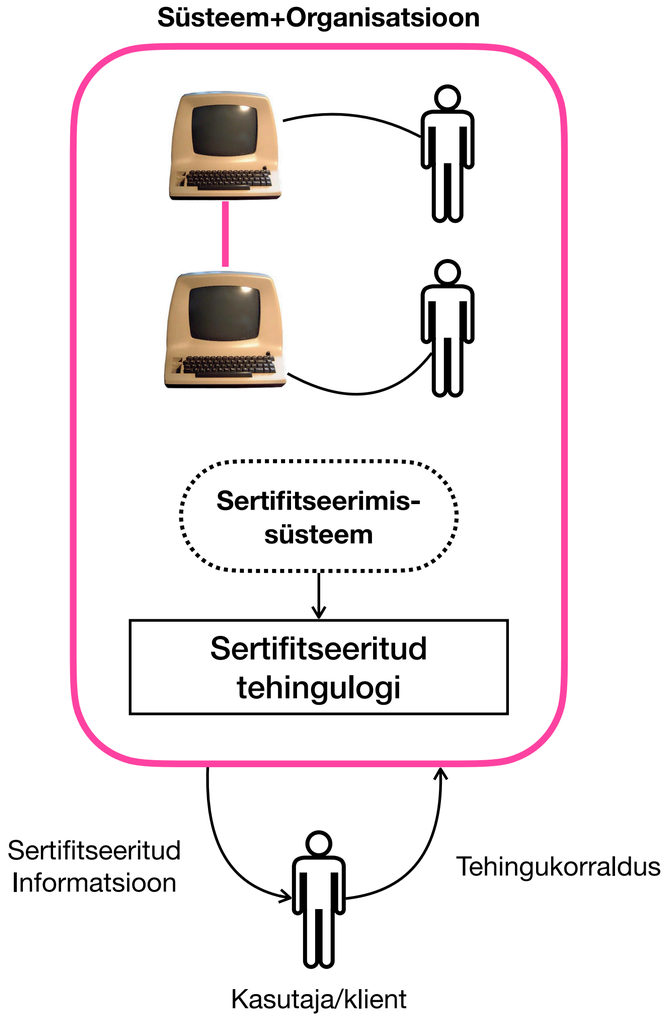
Süsteem salvestab täieliku tehingulogi

Süsteem sertifitseerib regulaarselt tehingulogi suheldes sisemise sertifitseerimissüsteemiga

Tehingukorraldusetel on kasutajate allkirjad

Sertifitseeritud tehingulogi abil ei saa täielikult veenduda, et süsteem on seni korrektselt töötanud

Siseründed ei tarvitse olla tuvastatavad



# Väliselt auditeeritav süsteem

Süsteemi töö põhineb reeglitel: tehingukorraldused muudavad ettenähtud viisil süsteemi olekut

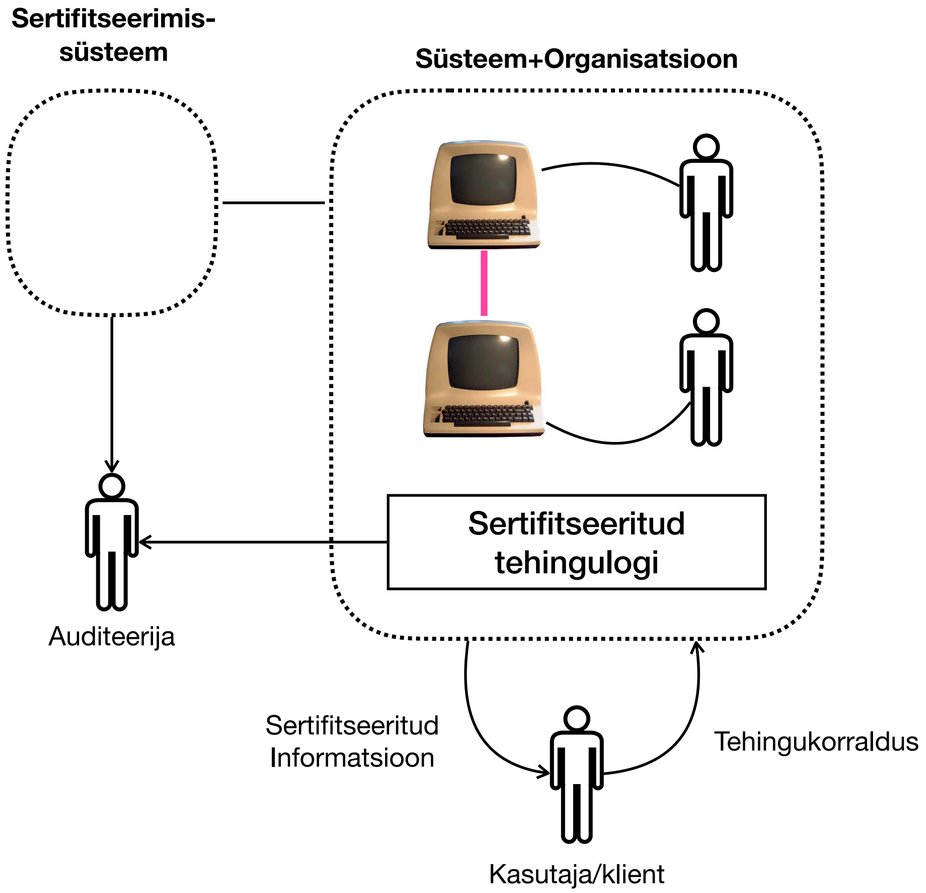
Süsteem salvestab täieliku tehingulogi

Süsteem sertifitseerib regulaarselt tehingulogi suheldes välise sertifitseerimissüsteemiga

Tehingukorraldusetel on kasutajate allkirjad

Kasutajatele antav informatsioon on sertifitseeritud, st tõestatavalt kooskõlas tehingulogiga

Sertifitseeritud tehingulogi abil saab veenduda, et süsteem on seni korrektselt töötanud



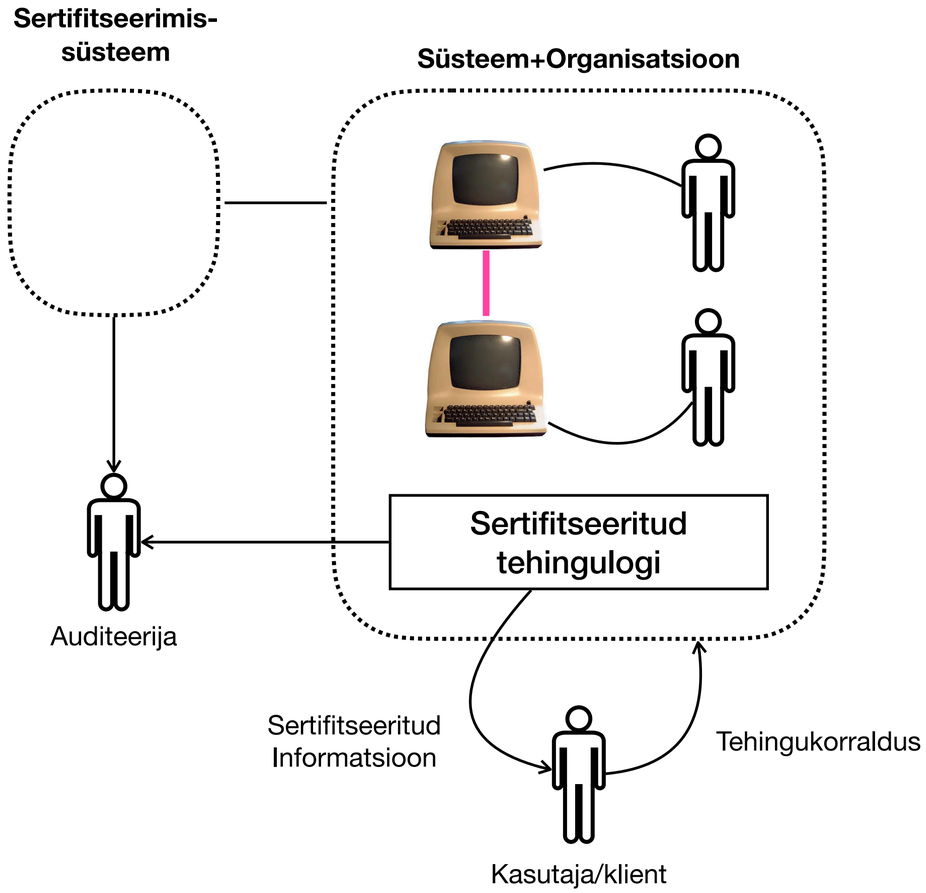
# Väliselt auditeeritav süsteem

**Sertifitseeritud tehingulogi turvaomadus**:

Unikaalsus: Sama ajaperioodi kohta ei ole võimalik esitada kahte erinevat sertifitseeritud logi

Tagab, et:

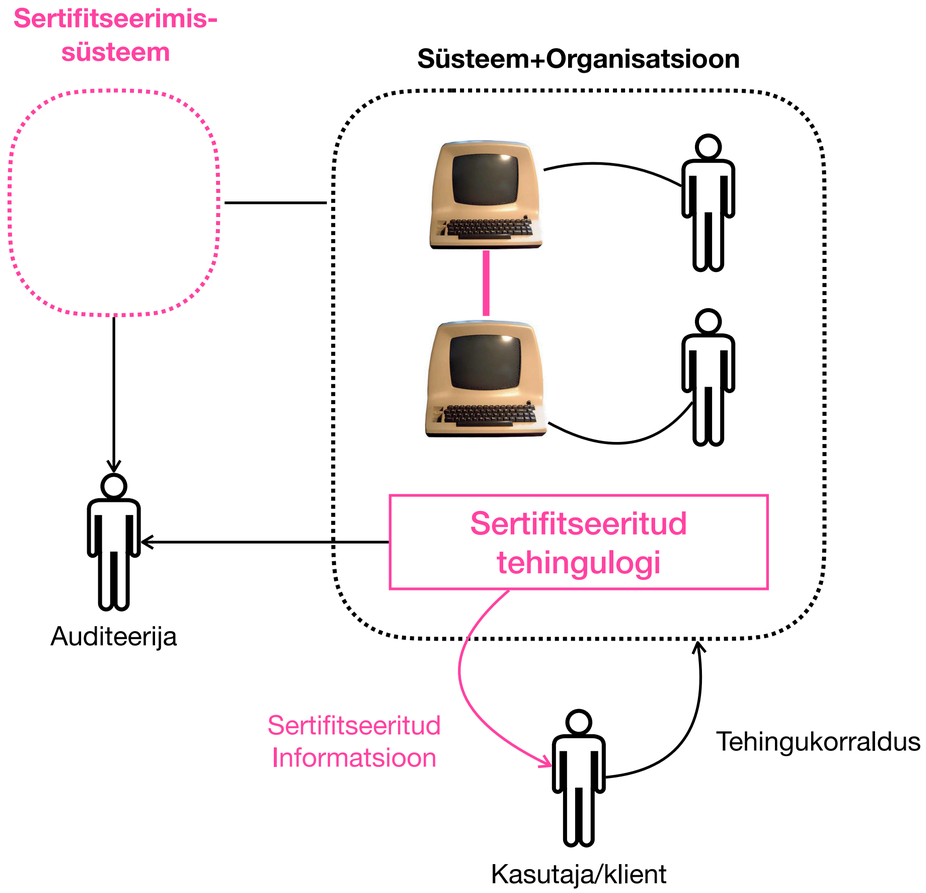
- Süsteemi auditeerija näeb alati täpselt ühte versiooni tehingulogist
- Kasutajaile antav sertifitseeritud informatsioon on kooskõlas just selle versiooniga tehingulogist



# Plokiahel

Plokiahel = sertifitseeritud tehingulogi, millel on unikaalsuse omadus

Plokiaheltehnoloogia = süsteem koos sertifitseerimissüsteemiga, mis loob plokiahela



# Plokiaheltehnoloogia liigid

Eristuvad sertifitseerimisüsteemi olemuse järgi

Tehniline struktuur:

- Arvuti (server)
- Arvutivõrk

Organisatsiooniline  struktuur:

- Ühe organisatsiooni kontrolli all
- Mitme organisatsiooni jagatud kontrolli all
- Iseorganiseeruv (nn. loatu plokiahel): sertifitseeerimissüsteemis osalemine on seotud majandusliku motivatsiooniga -> nõuab süsteemi-spetsiifilist krüptoraha

# Plokiaheltehnoloogiate võrdlus

| | Organisatsioon | Vea- ja ründekindlus | Summarne maksumus | Märkused |
|---|---|---|---|---|
| **Loalised plokiahelad** | Ühe või mitme organisatsiooni kontrolli all | Kõrge | Madal<br><br>Paari serveri halduskulud | Võimaldavad luua väliselt auditeeritavaid süsteeme mõistliku lisakuluga.<br>Põhjalikult akadeemiliselt uuritud<br>Sobilikud süsteemides, millel on määratud vastutav organisatsioon |
| **Loatud plokiahelad** | Mitte ühegi konkreetse organisatsiooni kontrolli all | Kõrge (arvatavasti) | Kõrge<br><br>Näiteks Bitcoinis kasutatakse andmete mitme-tuhande kordset dubleerimist | Võimaldavad luua väliselt auditeeritavaid süsteeme suhteliselt kõrge lisakuluga.<br>Süsteemi töökindlus sõltub majanduskeskkonnast.<br>Vajab rohkem akadeemilist uurimistööd<br><br>Vajalikud ainult süsteemides, kus mingil põhjusel ei saa/ tohi olla fikseeritud vastutavat organisatsiooni. |

# Plokiaheltehnoloogia piirangud

Turvanõuded süsteemile jagunevad kaheks:

- Nõuded, mille täidetus väljendub tehingulogi omadustega
- Nõuded, mille täidetus ei väljendu tehingulogi omadustena

Plokiaheltehnoloogia lubab auditeerida ainult tehingulogi omadustena esitatavate turvanõuete täidetust

**Näiteks**: Andmete konfidentsiaalsus (juurdepääs vaid volitatud isikuile) ei väljendu tehingulogi omadusena.

**Seega**: Plokiaheltehnoloogia ei ole piisav privaatsete e-hääletussüsteemide auditeerimiseks.