CDOC 2.0

arne.ansper@cyber.ee

CYBERNETICA

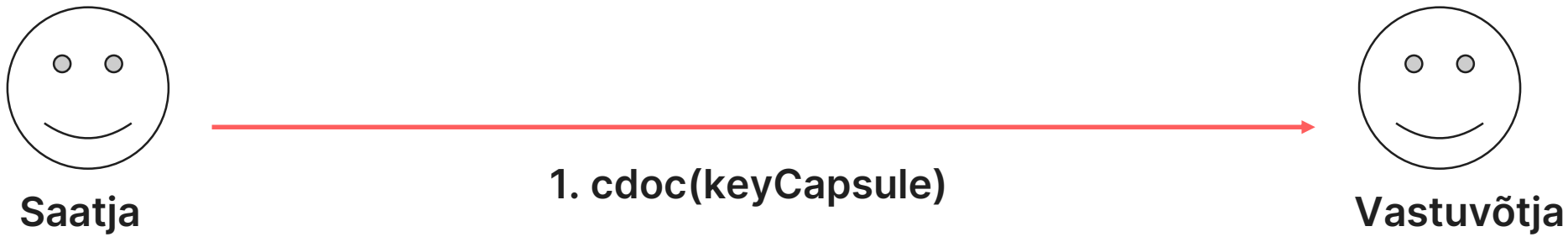
Probleemipüstitus

- Luua lahendus info krüpteeritud edastamiseks ja säilitamiseks
- Võtmesõnad
  - Tulevikuturvalisus
  - Säilituskrüptograafia
  - Kvantarvutikindlus
  - Mobiil-ID ja Smart-ID
- Uus protokoll nullist – krüptograafiliselt ja teostuselt kvaliteetne

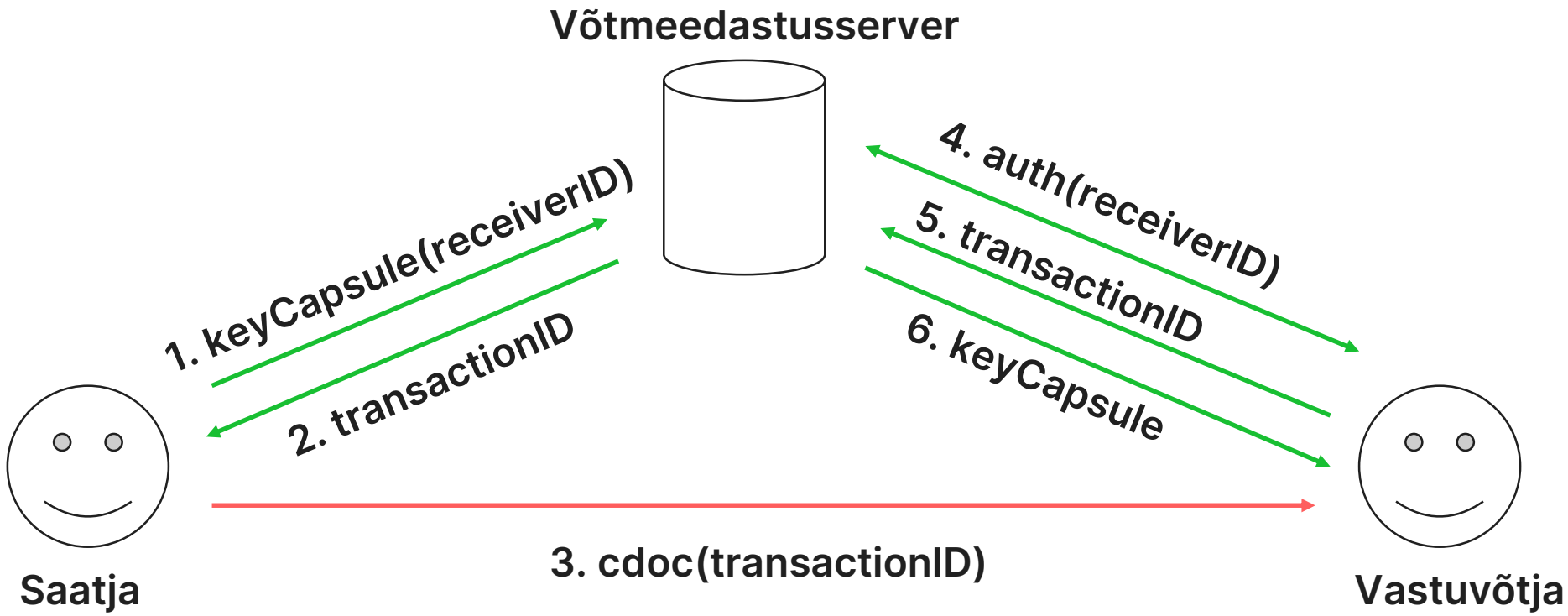
Tulevikuturvalisus

- Info salastatus säilib ka peale info krüpteeritud edastamiseks kasutatud võtmete või algoritmide kompromiteerumist
- ROCA näitas, et see on väga praktiline probleem
- Lahendus: võtmeedastusserver

Praegu



Tulevikus


Võtmeedastusserver
1. keyCapsule(receiverID)
2. transactionID
4. auth(receiverID)
5. transactionID
6. keyCapsule
3. cdoc(transactionID)
Saatja
Vastuvõtja

Võtmeedastusserver

- Ei halvenda konfidentsiaalsusomadusi
- Täiendav server – käideldavus vajab käsitlemist
- Tulevikuideed
  - dokumentide "tagasikutsumine"
  - saatja saab kontrollida kui kaua dokument on dekrüpteeritav
- RIA paigaldab avaliku serveri
- Asutused võivad oma saatjatele paigaldada oma serverid

Säilituskrüptograafia

- Transpordiks krüpteeritud dokumente ei tohi pikaajaliselt talletada
- Kui vastuvõtja vajab dokumentide pikaajalist krüpteeritud talletamist, siis peab ta vastuvõetud dokumendid re-krüpteerima vastavalt oma turvapoliitikale ja vahenditele
- Väga avar teema, universaalsed lahendused ja tööriistad võimalikud vaid väga piiratult

CDOC2.0 säilituskrüptograafia käsitlus

- Re-krüpteerimine
- Isikliku kasutuse ja asutuses arhiveerimise stsenaariumid
  - Parooliga krüpteerimine
  - Krüpteerimine kiipkaardi/HSMi/USB-pulgaga dekrüpteerimiseks

Projekti tulemid

- CDOC 2.0 spetsifikatsioon
- Näidisklient käsurearakendusena ja Java teek
- Võtmeedastusserver
- Täiendatud funktsionaalsusega DigiDoc klient
- Tegevusplaan edasiseks
  - Teeme intervjuusid ja kogume sisendit

Tulevikuplaanid

- Krüpteerimine Mobiil-ID ja Smart-ID jaoks
- DigiDoc kliendi profileerimine
  - Parem tugi säilituskrüptograafiale
  - Käideldavus vs konfidentsiaalsus: m-of-n skeem
- Kvantarvutikindlate algoritmide tugi

Mobiil-ID ja Smart-ID tugi

- Võtmeedastusserveri kasutuse edasiarendus
  - Krüpteerimata võti jagatakse mitme võtmeedastsserveri vahel, turvalisus saavutatakse mitte-krüptograafiliste turvameetmetega
  - Mobiil-ID ja Smart-ID kasutatakse vaid autentimiseks
- Turvatase on madalam kui ID-kaardi korral
- Samas võib leiduda rakendusi mille jaoks on see piisav

DigiDoc kliendi profileerimine

- Võimalus luua asutuse-kohane lisakonfiguratsioonifail DigiDoc kliendile, mis
  - määrab võtmeedastusserverite kasutuse
  - määrab säilituskrüptograafia kasutuse
  - ...

Kvantarvutikindel salastamine

- Plaan valida välja ja võtta kasutusele mõni kvantarvutikindel võtmekehtestusprotokoll
- Hübriidskeem, kus kasutatakse tavalisi, järgiproovitud algoritme paralleelselt kvantarvutikindlatega
- Edukaks ründeks peab murdma mõlemad

Aitäh!

cybernetica

CyberneticaAS

cybernetica_ee

Cybernetica