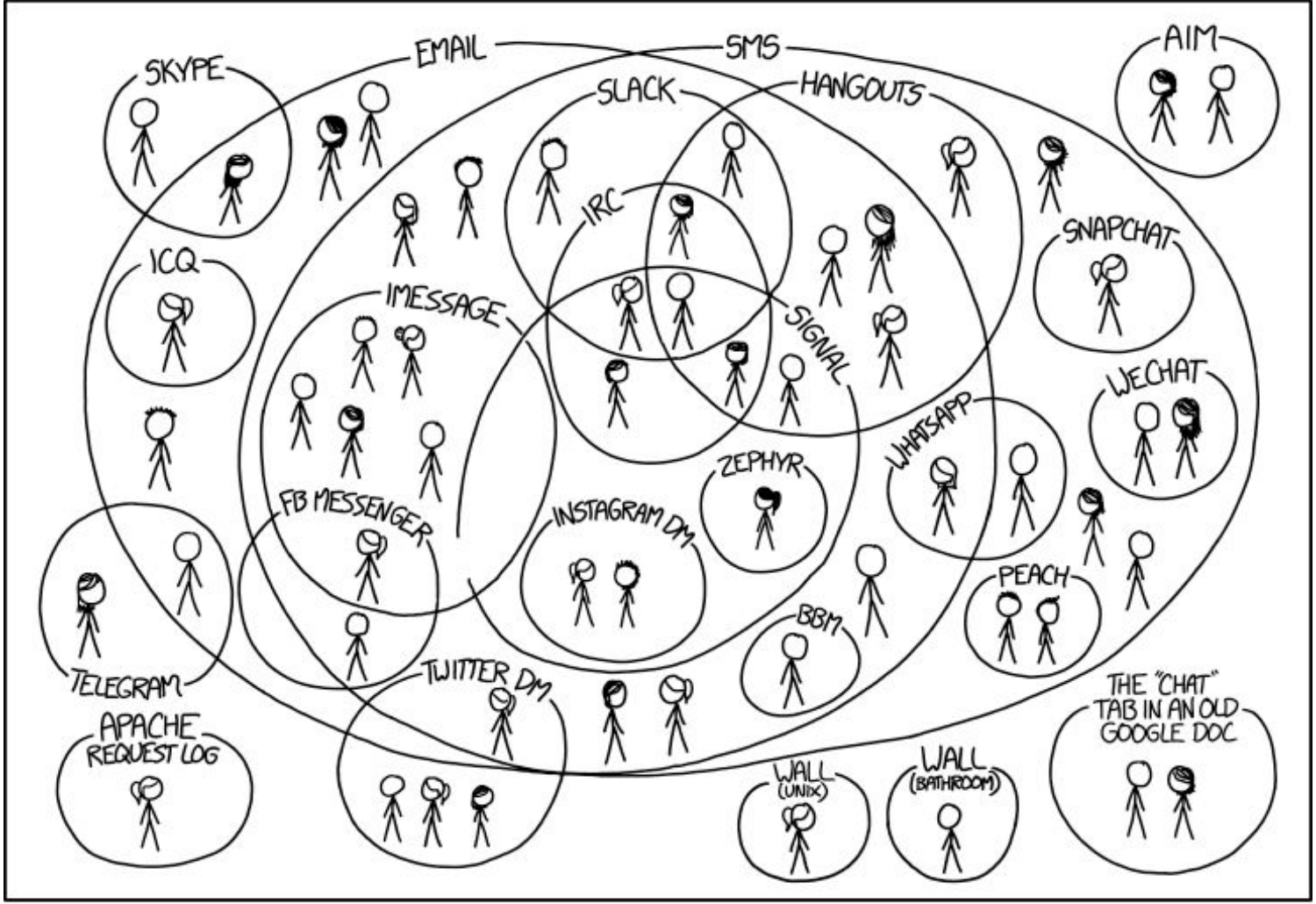
E-posti krüpteerimine

Lauri Võsandi

Loengu eesmärk

- Ülevaade kuidas e-post töötab
- E-postiga seonduvad probleemid
- Kuidas turvata e-posti

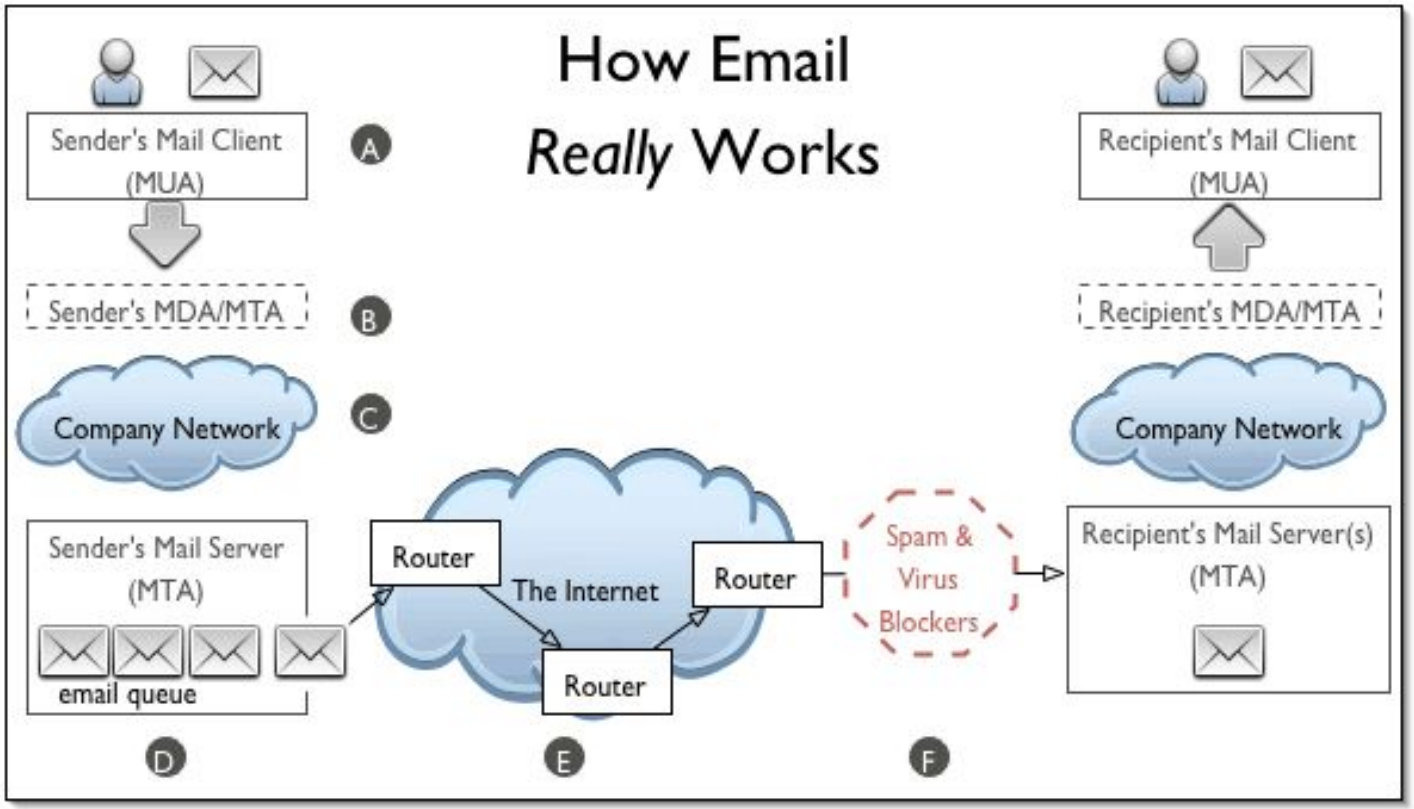


I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.

Terminoloogiast

- MUA ehk Mail User Agent
  - Outlook, Thunderbird
  - Veeb
- MTA ehk Mail Transfer Agent
  - Postfix, Exchange
- MDA ehk Mail Delivery Agent
  - Dovecot, Exchange


How Email Appears to Work
Sender's Outbox
Recipient's Inbox


How Email
Really Works
Sender's Mail Client
(MUA)
A
Sender's MDA/MTA
B
Company Network
C
Sender's Mail Server
(MTA)
email queue
D
Router
The Internet
Router
Router
E
Spam &
Virus
Blockers
F
Recipient's Mail Client
(MUA)
Recipient's MDA/MTA
Company Network
Recipient's Mail Server(s)
(MTA)

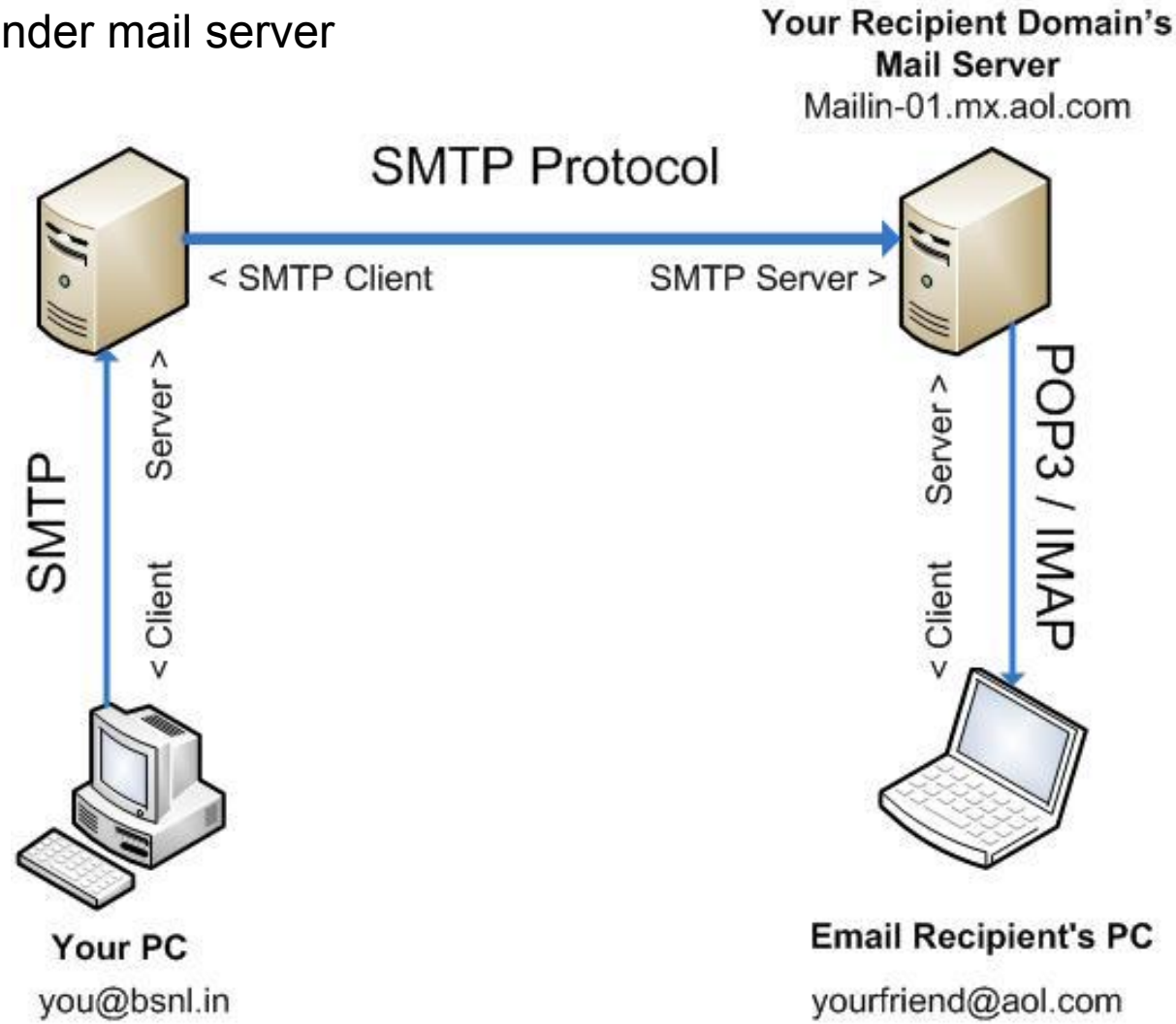
Kirjade saatmine

- SMTP ehk Simple Mail Transfer Protocol
- Kasutab TCP porti 25
- Sinu MUA-st liigub kiri üle SMTP sinu e-postiserverisse
- Sinu e-postiserver saadab SMTP abil kirja vastuvõtja e-postiserverisse
- Seni päris tihti turvamata SMTPS (SMTP+TLS) abil
- SMTPS käib tavaliselt TCP port 465 peal

Kirjade lugemine

- IMAP ehk Internet Message Access Protocol
- Kasutab TCP porti 143
- Sinu MUA ühendub e-postiserverisse et sealseid kirju alla laadida sinu arvutisse
- Tuleb ka ette et on turvamata IMAPS (IMAP+TLS) abil
- IMAPS kasutab TCP porti 993

Sender mail server



E-postiga seotud probleemid

- Serveri tarkvara turvaprobleemid
  - Pahalased saavad ligi e-kirjadele
- Postkasti parool lekib
  - Pahalased saavad seeläbi ligi teistele teenustele
- E-kirjade spoofimine (SPF)

E-postiga seotud probleemid

- Spämm
  - Kehvasti organiseeritud domeenidelt (.pw)
  - E-postiserver kehvasti seadistatud (open relay)
- Ründed
  - Õngitsuskirjad (phishing, spear phishing)
  - Viirused, pahavara, lunavara
- Tavakasutaja ei märka/oska tuvastada võltskirju
- Pealtkuulatav kuna ei krüpteerita

Otspunktide vaheline krüpto

- Klassikaline PKI (public key infrastructure)
  - ID-kaardi tarkvaraga .bdoc ja .cdoc
  - S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Usaldusvõrgustik
  - PGP (Pretty Good Privacy)
  - GPG (GNU Privacy Guard)

… omadused

- Allkirjastamine
  - Saatja identiteedi tõendamiseks (authentication)
  - Kaasneb ka terviklikkusse kontroll (integrity)
- Krüpteerimine
  - Ainult vastuvõtja saab lugeda (confidentiality)
- Kehtib nii DigiDoc, S/MIME kui PGP puhul

… millest koosneb

- Sümmeetriline sihver, sisu krüpteerimiseks
- Räsialgoritm sisu kontrollsummade arvutamiseks
- Asümmeetriline sihver
  - räsi allkirjastamiseks
  - sümmeetrilise võtme krüpteerimiseks
- Kombinatsioon neist kehtib nii DigiDoc, S/MIME, PGP kui ka tegelikult TLS korral

Räsimine

- Tänapäeval enimlevinum SHA-256 (?)
- Sisendi muutmisel väljund muutub täielikult
- Kasutatakse failide sisu kontrollimiseks a’la:

```
sha256sum \
ubuntu-16.04.2-desktop-amd64.iso
```

Sümmeetriline krüpto

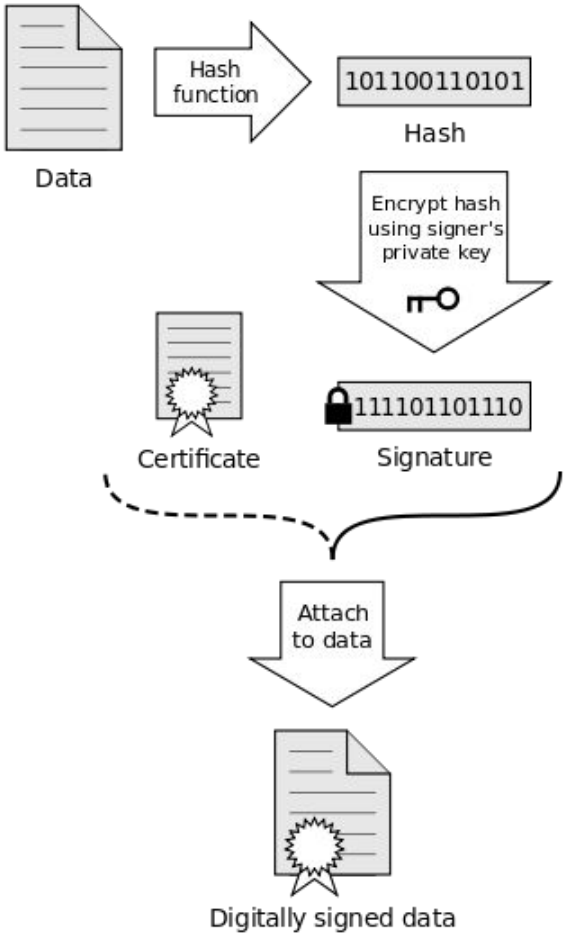
- Tänapäeval enimlevinum 128-bit AES
- Toimetab ploki kaupa (nt 16 baiti)
- Kasutatakse failide sisu krüpteerimiseks a’la:

```
openssl enc -aes-128-cbc \
   -in plain.txt -out encrypted.bin \
   -K e0e0e0e0f1f1f1f1
```

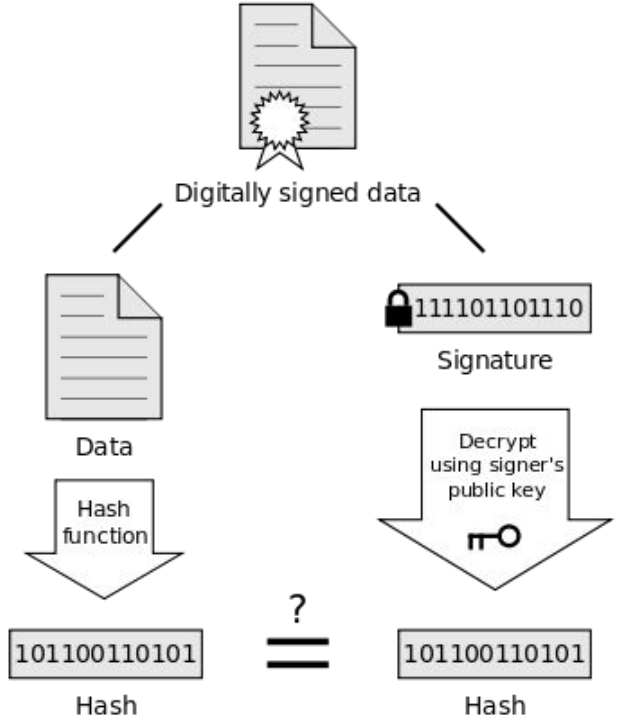
Asümmeetrilisest krüptost

- Tänapäeva krüpto poleks võimalik RSA-ta
- See tähendab, et igal kasutajal on privaatne/avalik võtmepaar
- Selleks et krüpteeritud kirja saata, peab sul olema vastuvõtja avalik võti
- Selleks et allkirja verifitseerida peab sul olema saatja avalik võti

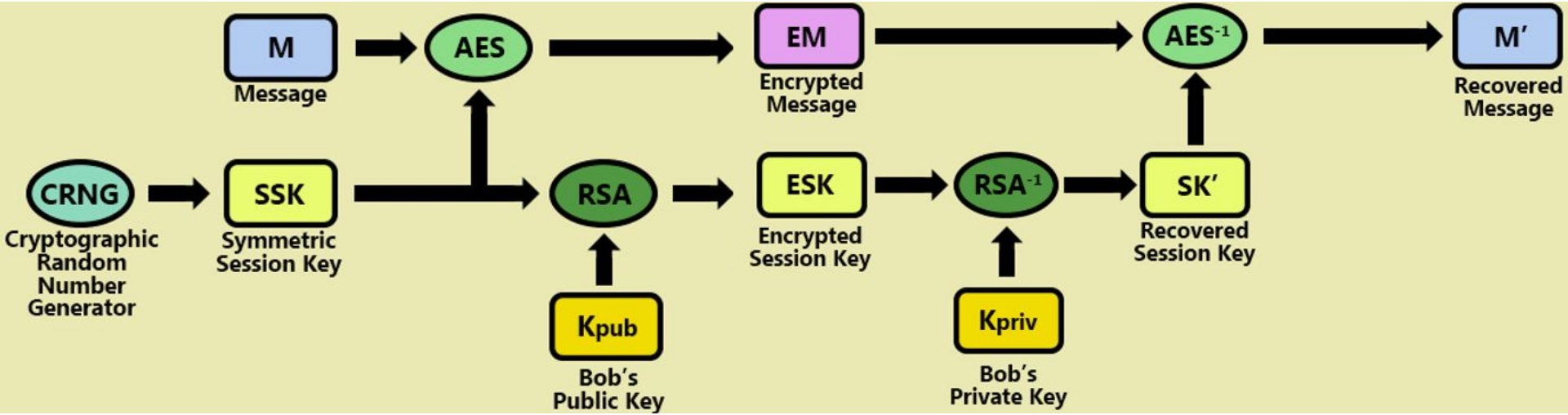
Signing



Verification



If the hashes are equal, the signature is valid.


M
Message
AES
EM
Encrypted Message
AES-1
M'
Recovered Message
CRNG
Cryptographic Random Number Generator
SSK
Symmetric Session Key
RSA
ESK
Encrypted Session Key
RSA-1
SK'
Recovered Session Key
Kpub
Bob's Public Key
Kpriv
Bob's Private Key

Sertifikaatidest

- Kolmanda osapoole (nt Sertifitseerimiskeskus AS) allkirjastatud avalikku võtit koos allkirja kehtivusajaga nimetatakse sertifikaadiks
- Eesti ID-kaardi sertifikaate saab pärida SK LDAP serverist a’la
- ```
  ldapsearch -x -h ldap.sk.ee -b c=EE \
    "(serialNumber=38810240348)"
  ```
  ```

DigiDoc Krüpto

- ID-kaardi tarkvaraga tulevad kaasa SK juurserdid
- Kasutaja sisestab isikukoodi
- Tarkvara laadib sertifikaadid serverist
- Kontrollib, et isiku sertifikaat on tõepoolest allkirjastatud SK poolt
- Kasutab ID-kaardi ja Digi-ID sertifikaatides leiduvaid avalikke võtmeid sisu krüpteerimiseks

Usaldusvõrgustikud a’la PGP

- Võtmepaari genereerid ise
- Oma võtme saad üles laadida võtmeserverisse või üles riputada kodulehele
- Iga võrgustikus osalev arvutikasutaja on iseenda sertifitseerimiskeskus
- Oma allkirja andmine kellegi teise avalikule võtmele sümboliseerib sinu usaldust tema vastu

“Ideaalses” OpenPGP maailmas

- Sinul on käputäis usaldatud inimesi
- Läbi usaldatud isikute saad *sort-of* usaldada isikuid keda sa ise otse ei usaldada
- Seeläbi saad saata kirju suvalistele inimestele krüpteeritult
- Vastusvõetud kirjade autentsuses saad kohesel veenduda

Praktikum

- Seadista Thunderbird oma igapäevase postkasti lugemiseks
- Paigalda Enigmail pistikprogramm
- Säti üles GPG
- Saada mulle GPG abil krüpteeritud ning allkirjastatud e-kiri
- Lisa manusesse oma DigiDoc abil allkirjastatud GPG võti

Kuidas oma e-postiserver teha

- Arvuti või pilveserver (5-20€/kuus)
- Staatiline IP aadress (6€/kuu Telias)
- Domeen registreerida (8-9€/aastas)
- Seadista Let’s Encrypt sertifikaadid
- Paigalda MDA/MTA nt Dovecot/Postfix
- Seadistada spämmifilter a’la Spamhaus
- Kui oled äriregistris blokeeri Palau domeen (.pw)