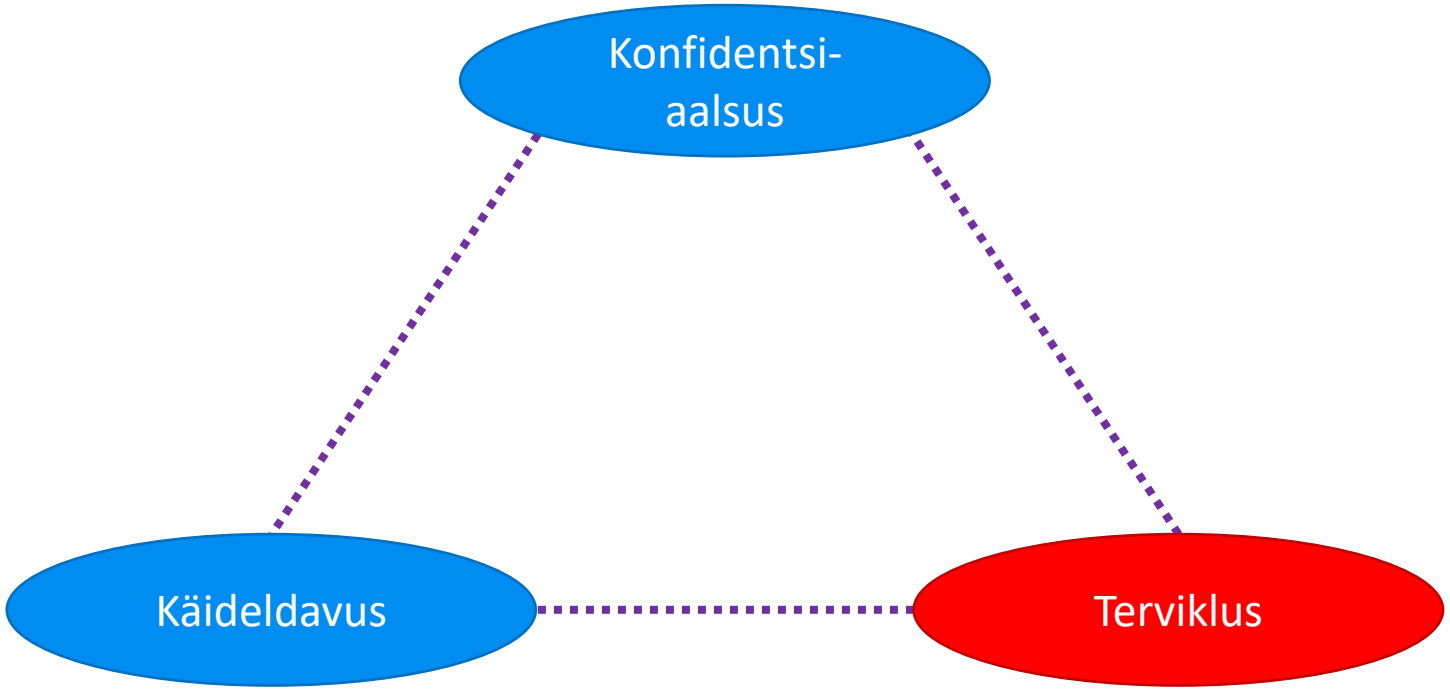
Digiallkirjadest

Informaatikaolümpiaadi õppesessioon 20.01.2024

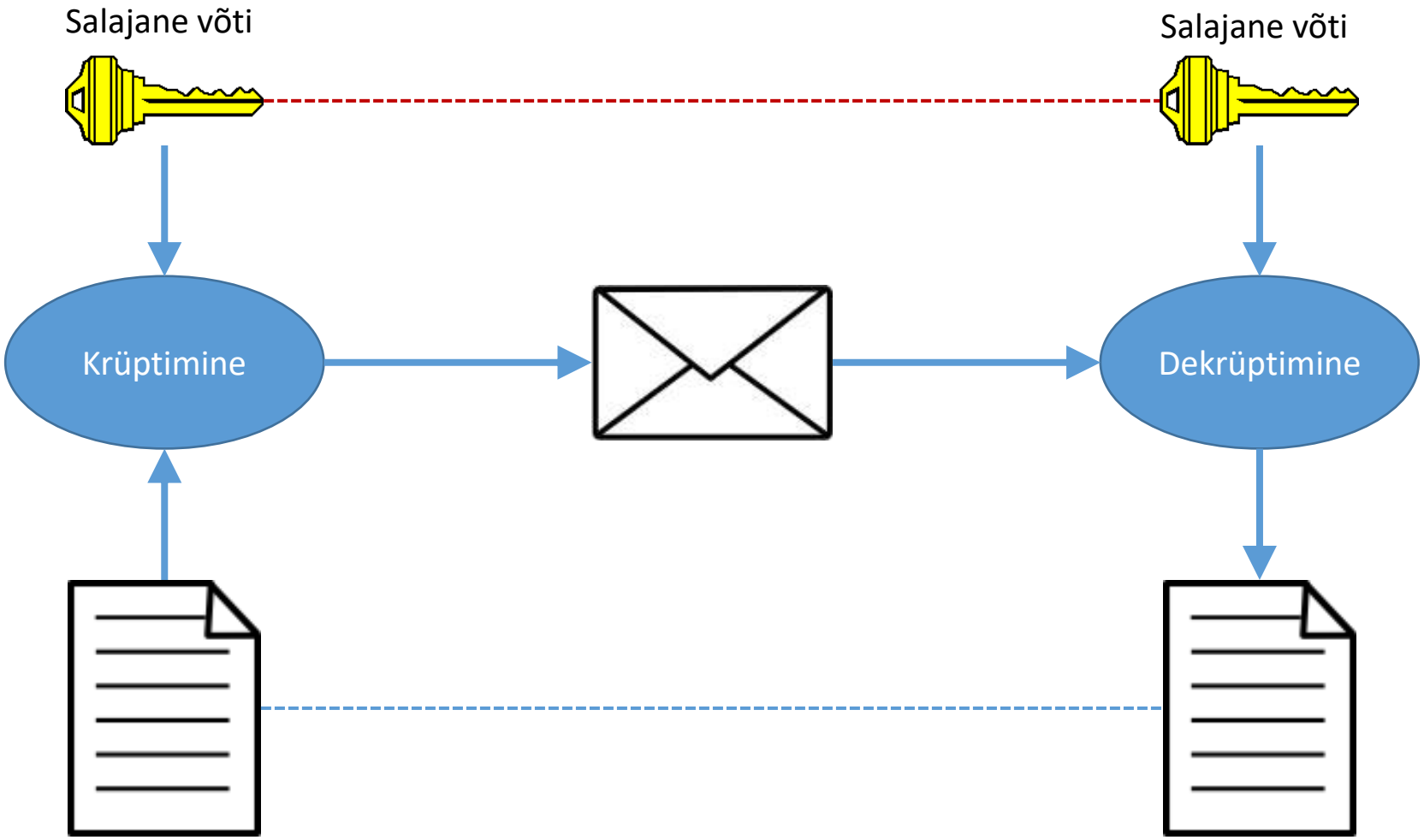
Ahto Truu, ahto.truu@ut.ee

Infoturbe kolm sammast

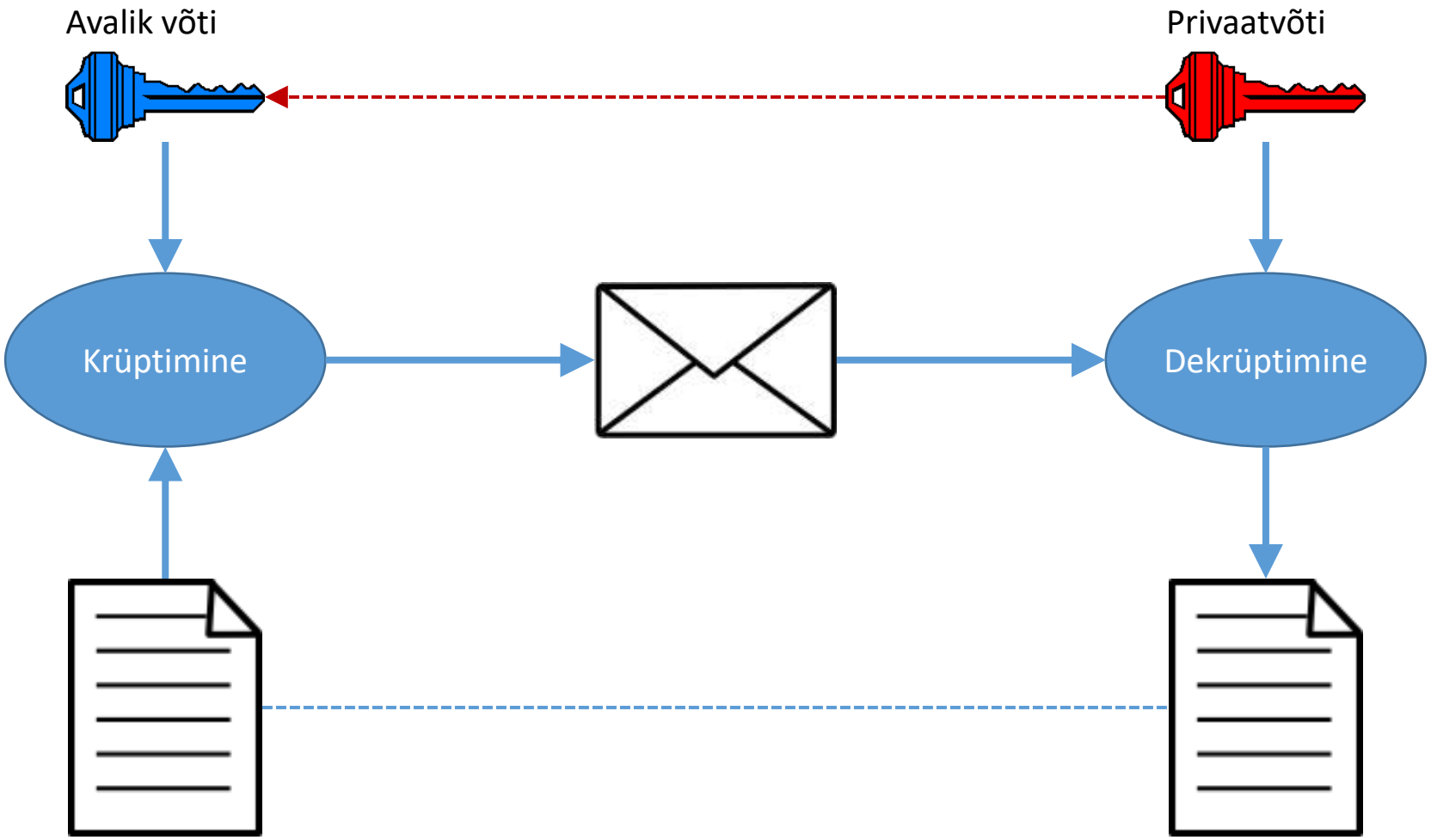
- Konfidentsiaalsus (salajasus)
- Käideldavus
- Terviklus



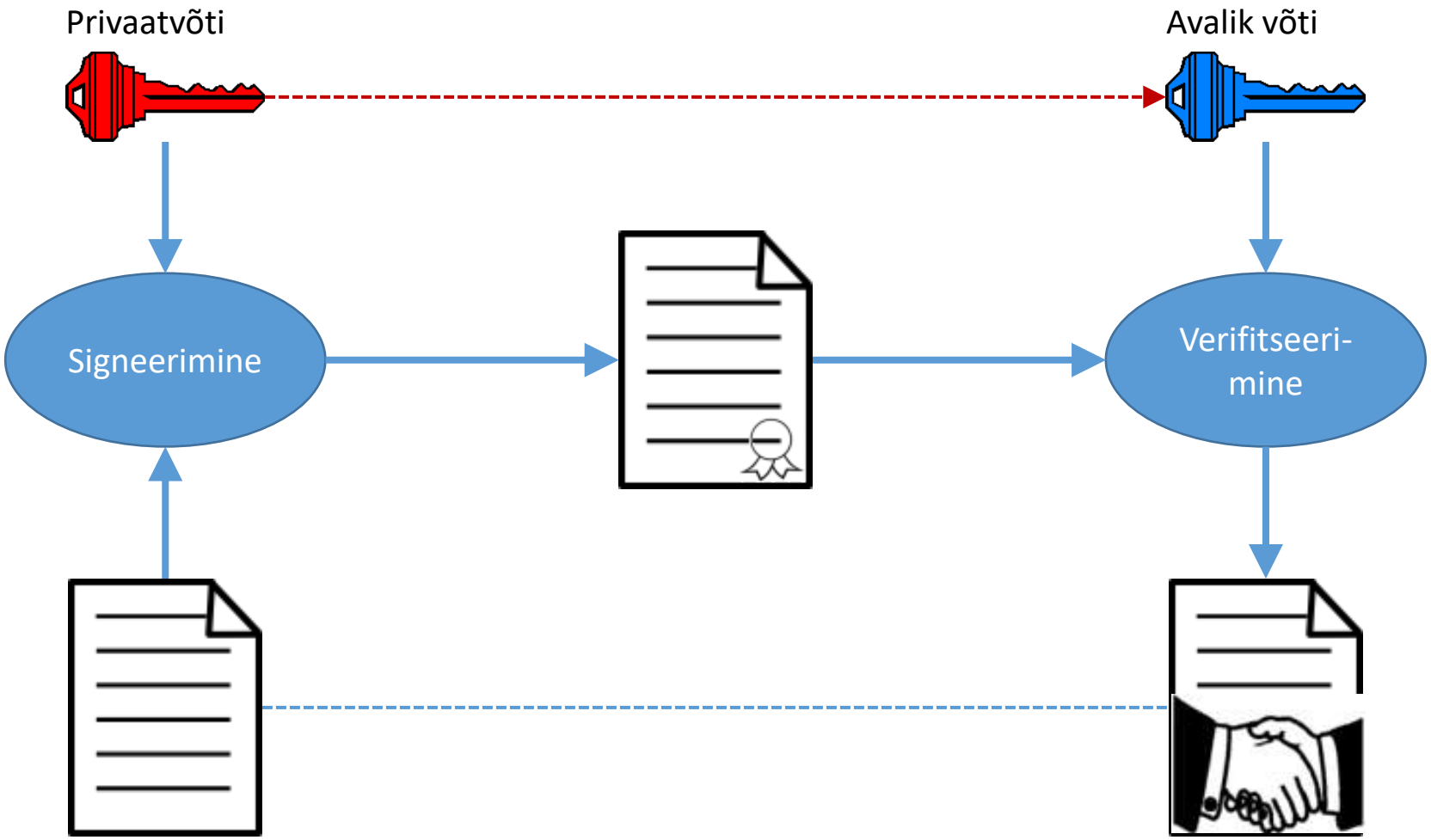
Sümmeetriline krüptimisskeem



Asümmeetriline krüptimisskeem



Signeerimisskeem



Digiallkirja olemus

- Eesmärk: omakäelise allkirja digitaalne analoog
- Tahteavaldus: nõusoleku või heakskiidu kinnitus

- Terviklus: dokumendi sisu puutumatus
- Autentsus: dokumendi päritolu (seos allkirjastaja isikuga)
- Salgamatus: võimalik tõend allkirjastaja vastu

Kasutusviisid

Allkirjastatud dokumendi vastuvõtja saab

- dokumendi autentsust **ise kontrollida**
- dokumendi autentsust **teistele tõestada**

Seos allkirjastaja isikuga?

- Probleem: avalik võti on lihtsalt baidijada või suur arv
- Kasutamiseks tuleb võti kuidagi siduda selle omanikuga

- Sertifikaat seob avaliku võtme ja selle omaniku identiteedi
- Lisaks veel mõned atribuudid, näiteks lubatud kasutusviisid
- Kinnitatud sertifitseerimisasutuse digiallkirjaga

Funktsionaalne mudel

Igal kasutajal on kaks võtit

- privaatne signeerimisvõti
- avalik verifitseerimisvõti

Signeerimisskeem kui kolm algoritmi

- Võtmete genereerimine: entroopia → privaatne ja sellele vastav avalik võti
- Signeerimine: dokument, privaatvõti → allkiri
- Verifitseerimine: dokument, allkiri, avalik võti → otsus: kas allkiri on loodud dokumendist ja avalikule võtmele vastavast privaatvõtmest?

Turvamudel

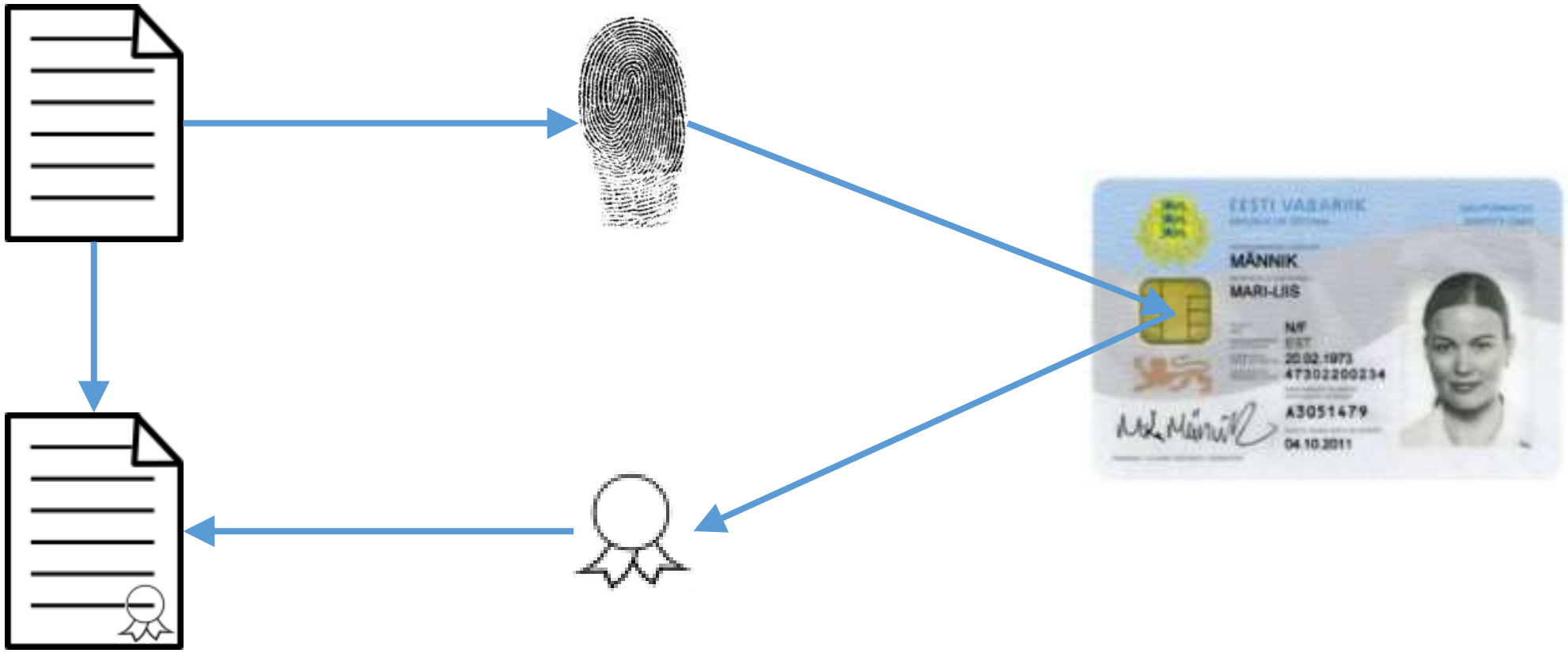
Turvalisuseks peab ründajal olema ületamatult raske

- dokumenti muuta nii, et verifitseerimine endiselt õnnestub
- luua allkirju ilma privaatvõtit teadmata
- tuletada privaatvõtit avalikust võtmest või allkirjast

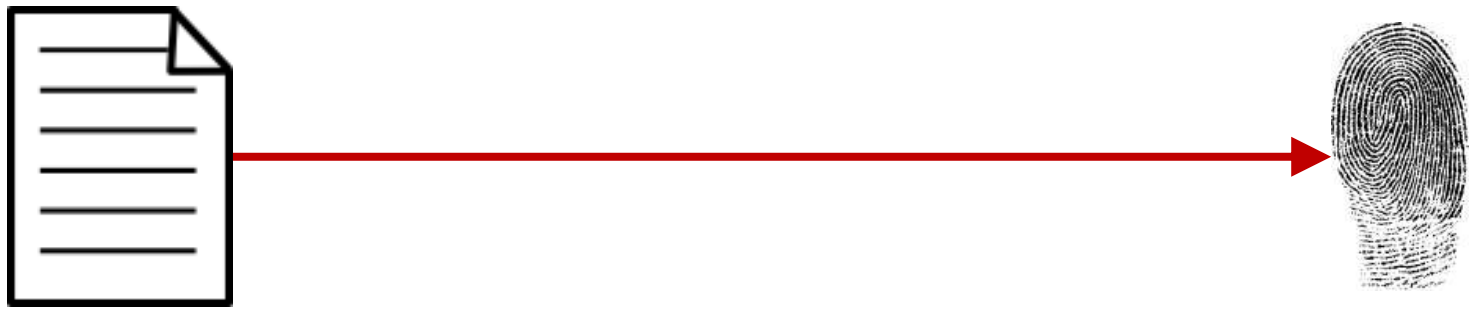
Praktikas peab lisaks privaatvõtit lekkimise eest kaitsma

- võtmepaar genereeritakse turvamoodulis
- eksporditakse ainult avalik võti, privaatvõti jääb turvamoodulisse
- signeerimiseks läheb dokument moodulisse, mitte ei tule võti välja

ID-kaardiga signeerimine



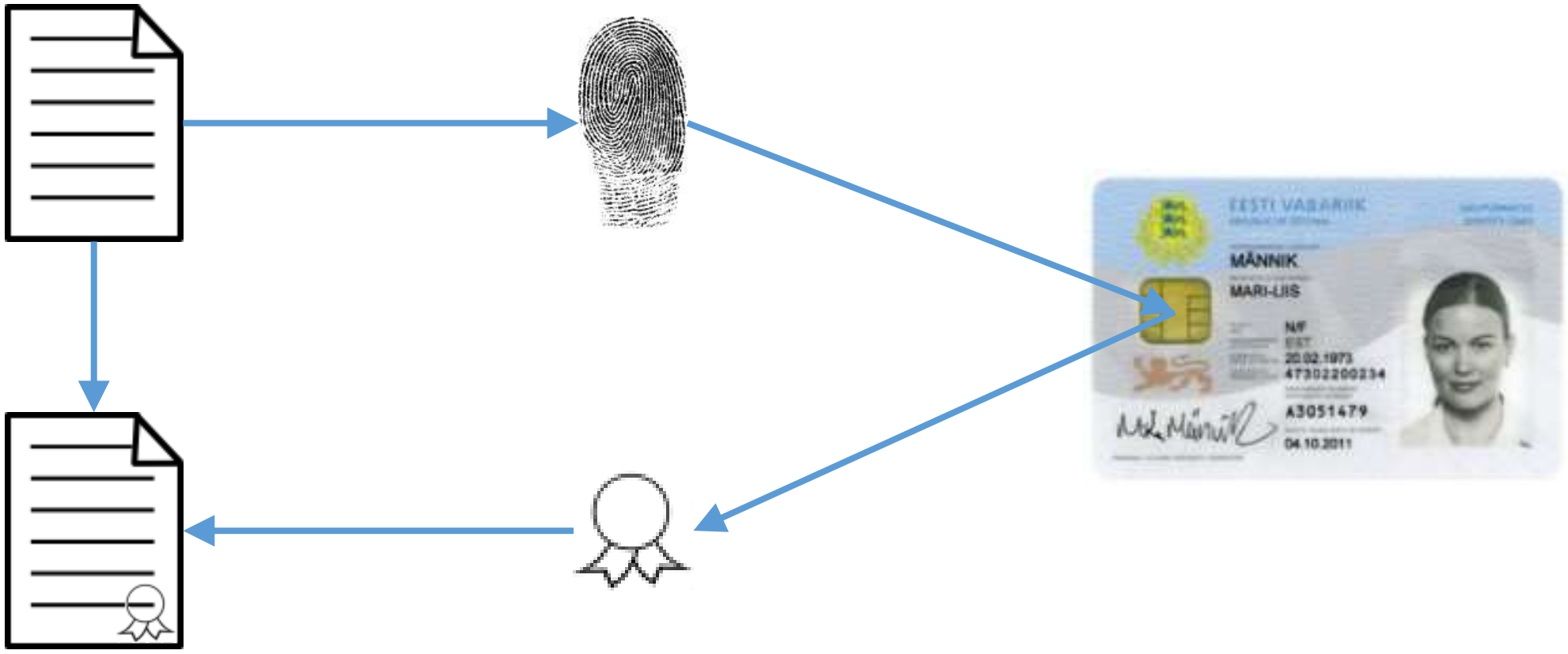
Kõrvalepõige: räsifunktsioon



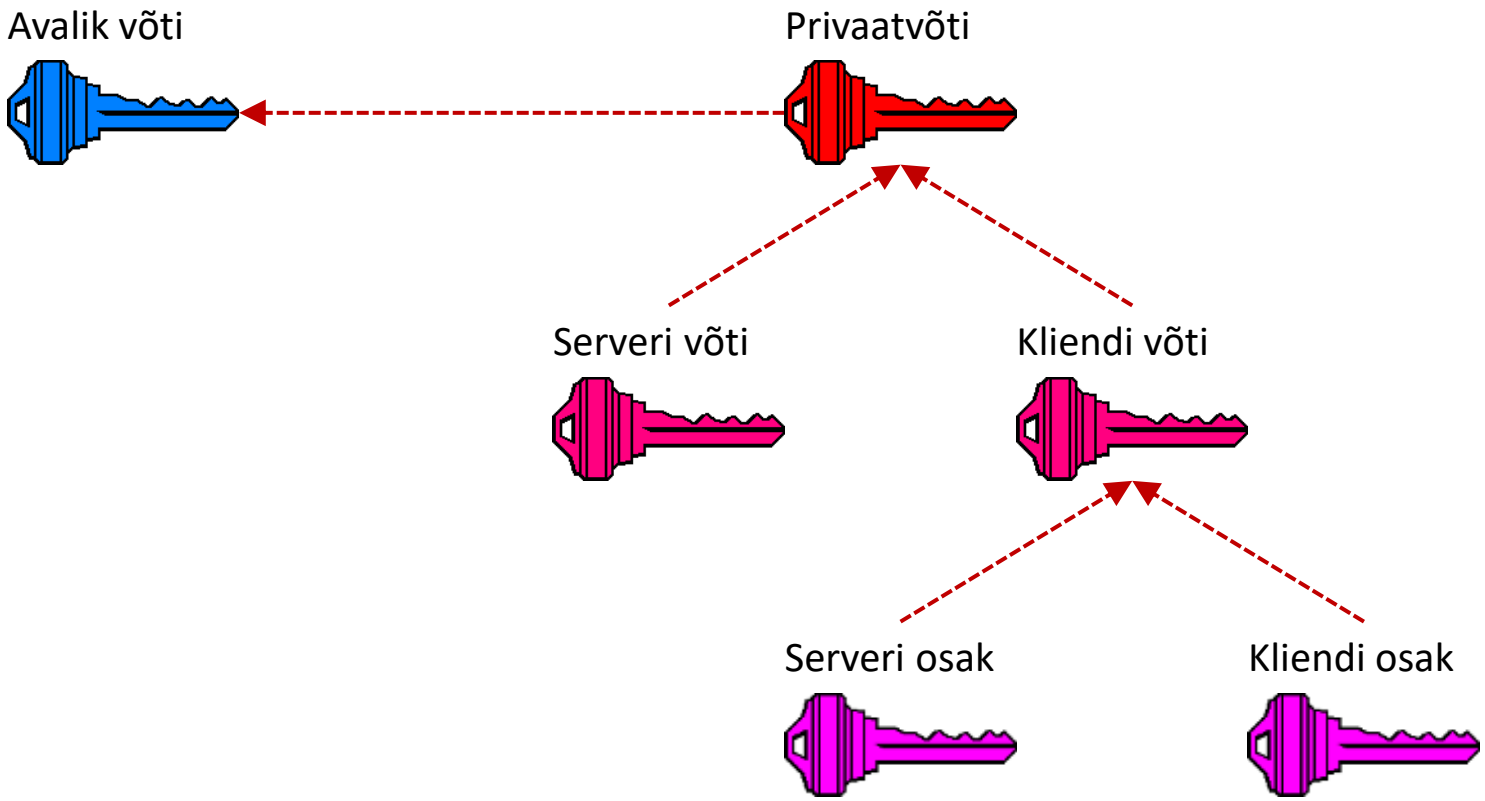
Räsifunktsioonide omadused

- Efektiivsus
  - Kui X on teada, siis on Y = h(X) kiiresti arvutatav
- Ühesuunalisus
  - Ületamatult raske leida antud Y jaoks X, et h(X) = Y
- Lisaoriginaalikindlus
  - Ületamatult raske leida antud X jaoks X’, et X’ ≠ X, aga h(X’) = h(X)
- Kollisioonikindlus
  - Ületamatult raske leida paare X_1 ja X_2, et $X_1 \neq X_2$, aga $h(X_1) = h(X_2)$

ID-kaart kui turvamoodul



Smart-ID – jagatud privaatvõti



RSA krüptimisskeem

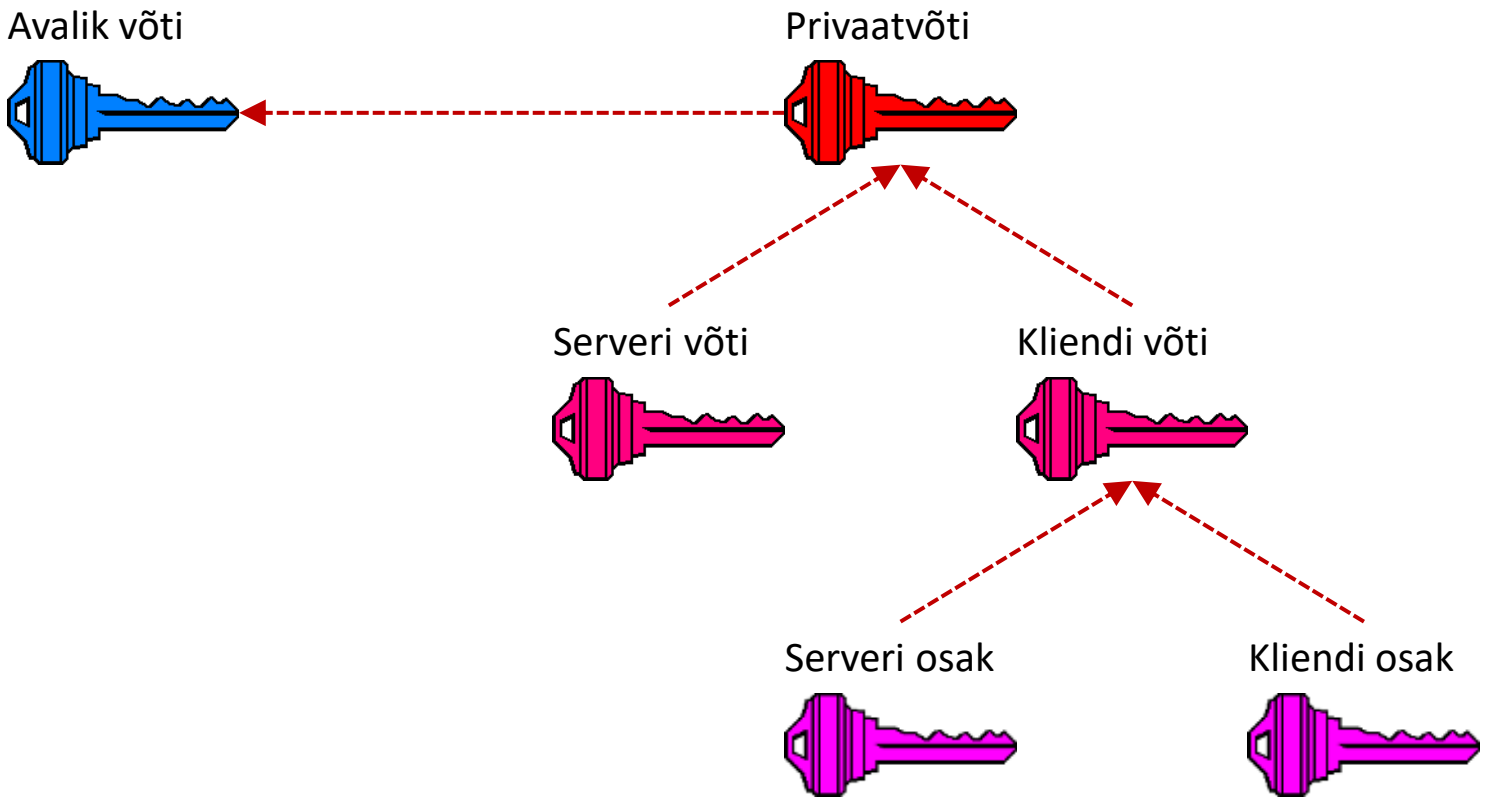
- Võtmete genereerimine
  - Vali kaks algarvu p, q
  - Arvuta $N = p \cdot q$, $\Phi = (p-1) \cdot (q-1)$
  - Vali e nii et SÜT(e, Φ) = 1
  - Leia d nii et $d \cdot e = 1 \pmod{\Phi}$, ehk $d \cdot e = \Phi \cdot k + 1$ mingi k korral
  - Hävita p, q, Φ
  - Avalik võti on (N, e)
  - Privaatvõti on (N, d)
- M (M<N) krüptimine
  - Arvuta $C = M^e \bmod N$
  - Saada C
- C dekrüptimine
  - Arvuta $M = C^d \bmod N$
  - Kasuta M
- Dekrüptimine töötab, sest
  - $C^d = M^{e \cdot d} = M^{\Phi \cdot k + 1} = M \cdot M^{(p-1) \cdot (q-1) \cdot k}$
  - $M^{(p-1) \cdot (q-1) \cdot k} = 1^{(q-1) \cdot k} = 1 \pmod{p}$
  - $M^{(q-1) \cdot (p-1) \cdot k} = 1^{(p-1) \cdot k} = 1 \pmod{q}$
  - $M^{(p-1) \cdot (q-1) \cdot k} = 1 \pmod{p \cdot q}$

RSA signeerimisskeem

- M (M<N) signeerimine
  - Arvuta $S = M^d \bmod N$
  - Saada (M, S)
- (M, S) verifitseerimine
  - Arvuta $X = S^e \bmod N$
  - Aktsepteeri M, kui X = M
- See “õpikuversioon” on
  - Sageli kasutamatu
  - Ebaturvaline!!!

- Signeerimine praktikas
  - Räsi m = h(M)
  - Signeeri $S = m^d \bmod N$
  - Saada (M, S)
- Verifitseerimine praktikas
  - Arvuta $X = S^e \bmod N$
  - Aktsepteeri M, kui X = h(M)

Smart-ID – kontekst



Serveri võti + kliendi võti – genereerimine

- Nõue: tahame serveri võtit hoida standardses turvamoodulis
- Idee: kombineerime kaks eraldi RSA signatuuri üheks

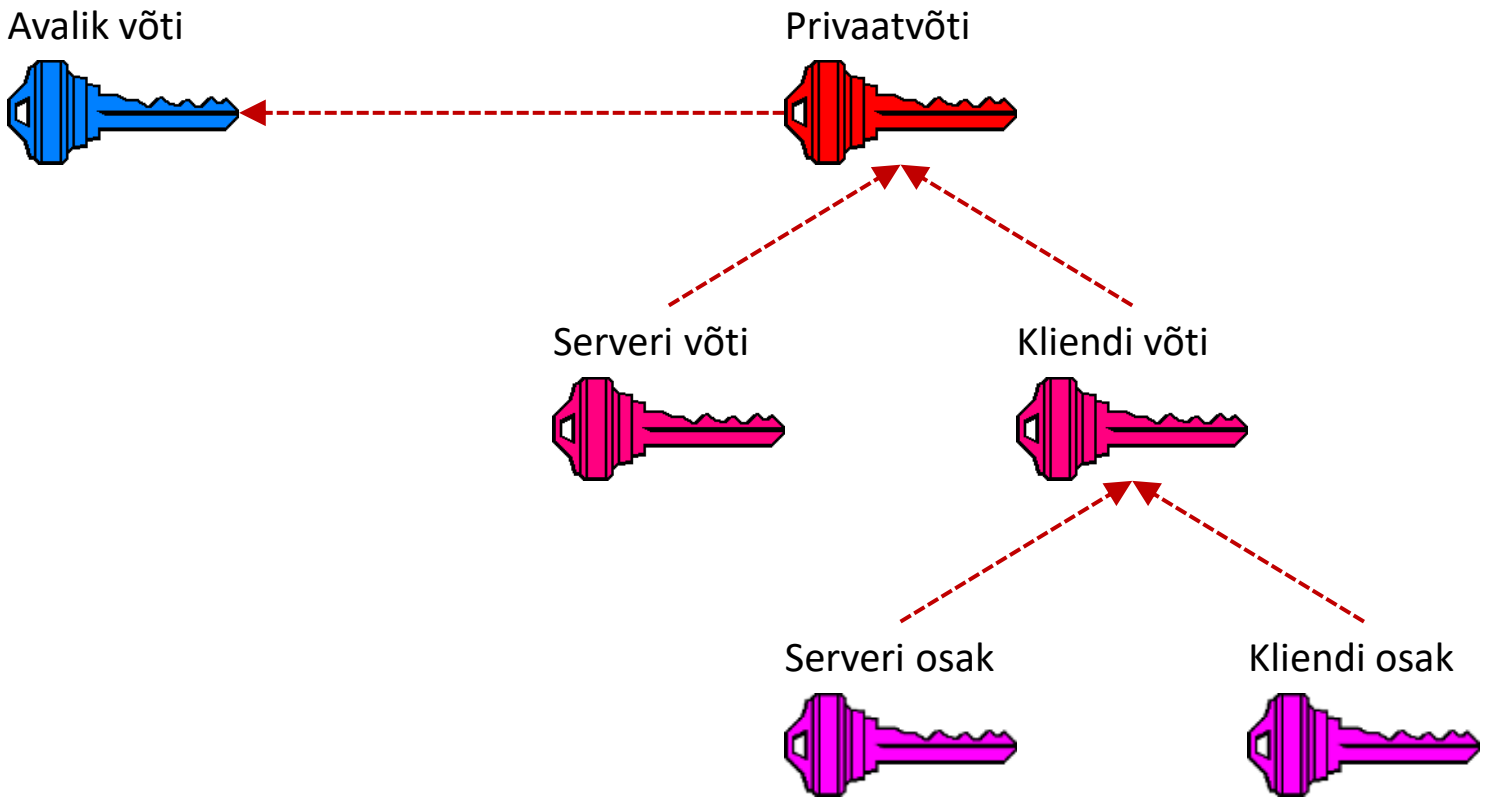
- Server valib e, p_s, q_s; arvutab N_s, d_s; saadab e kõigile klientidele
- Klient valib p_c, q_c; arvutab N_c, d_c; saadab N_c serverile
- Server arvutab $N = N_c \cdot N_s$; leiab α_s, α_c nii et $\alpha_s \cdot N_s + \alpha_c \cdot N_c = 1$

- Avalik võti on (N, e)
- Serveri privaatvõti on (N_s, d_s)
- Kliendi privaatvõti on (N_c, d_c)

Serveri võti + kliendi võti – signeerimine

- Klient arvutab $S_c = m^{dc} \bmod N_c$; saadab (m, S_c) serverile
- Server arvutab $S_s = m^{ds} \bmod N_s$; $S = (\alpha_s \cdot N_s \cdot S_c + \alpha_c \cdot N_c \cdot S_s) \bmod (N_c \cdot N_s)$
- Verifitseerimine on standardne
  - Arvuta $X = S^e \bmod N$
  - Aktsepteeri M, kui $X = h(M)$
  - $S^e = (\alpha_s \cdot N_s \cdot S_c + \alpha_c \cdot N_c \cdot S_s)^e = (\alpha_s \cdot N_s \cdot S_c)^e = ((1-\alpha_c \cdot N_c) \cdot S_c)^e = (S_c - \alpha_c \cdot N_c \cdot S_c)^e = S_c^e = m \pmod{N_c}$
  - $S^e = (\alpha_s \cdot N_s \cdot S_c + \alpha_c \cdot N_c \cdot S_s)^e = (\alpha_c \cdot N_c \cdot S_s)^e = ((1-\alpha_s \cdot N_s) \cdot S_s)^e = (S_s - \alpha_s \cdot N_s \cdot S_s)^e = S_s^e = m \pmod{N_s}$
  - $S^e = m \pmod{N_c \cdot N_s}$

Smart-ID – kontekst



Serveri osak + kliendi osak – genereerimine

- Nõue: tahame takistada PINi proovimise teel ära arvamist
- Idee: jagame kliendi privaatvõtme kliendi ja serveri vahel nii, et kliendi osakut eraldi ei saa kontrollida (ja server ei saa üksi midagi signeerida)

- Klient enne
  - Valib p_c, q_c; arvutab N_c, d_c; saadab N_c serverile
- Klient nüüd
  - Valib p_c, q_c; arvutab N_c, d_c
  - Jagab $d_c = (d_{c1} + d_{c2}) \bmod N_c$
  - Saadab (N_c, d_{c2}) serverile
  - Hävitab p_c, q_c, d_c, d_{c2}; salvestab ainult (N_c, d_{c1})

Serveri osak + kliendi osak – signeerimine

- Enne
  - Klient arvutab $S_c = m^{dc} \bmod N_c$; saadab (m, S_c) serverile
- Nüüd
  - Klient arvutab $S_{c1} = m^{dc1} \bmod N_c$; saadab (m, S_{c1}) serverile
  - Server arvutab $S_{c2} = m^{dc2} \bmod N_c$; $S_c = S_{c1} \cdot S_{c2} \bmod N_c$
  - Tulemus $S_c = S_{c1} \cdot S_{c2} = m^{dc1} \cdot m^{dc2} = m^{dc1+dc2} = m^{dc} \pmod{N_c}$

Kliendi kopeerimise tuvastamine

- Nõue: tuvastada kliendi andmete (võtme osak + PIN) kopeerimine
- Idee: kasutame ühekordseid paroole

- Võtme genereerimisel ja igal signeerimisel lepivad klient ja server kokku uue juhusliku ühekordse parooli
- Igal signeerimisel esitab klient eelmisel korral kokku lepitud parooli
- Kui kliendi signatuuriosak on õige, aga parool vale, teab server, et kliendi andmed on kopeeritud ja blokeerib teenuse
- Kopeerimise kiiremaks avastamiseks võib klient aeg-ajalt juhuslikke väärtusi signeerida

Smart-ID kokkuvõte

- Jagatud võtmetel põhinev RSA-ühilduv signatuuriskeem
- Sobib klientidele, kellel pole privaatvõtme turvamoodulit
- Server üksi ei saa midagi signeerida
- Klient (või kliendi koopia) üksi ei saa midagi signeerida
- Server saab tuvastada, kui kliendi andmetest on koopia tehtud
- Ründaja ei saa kliendi PINi ära arvata ilma serveriga suhtlemata
- Verifitseerimine nagu tavaliste RSA signatuuride korral