SSA süsteemi mudel

http://www.cyber.ee/turve/tooted/ssa/intro/model.html

Turvamata ühendus

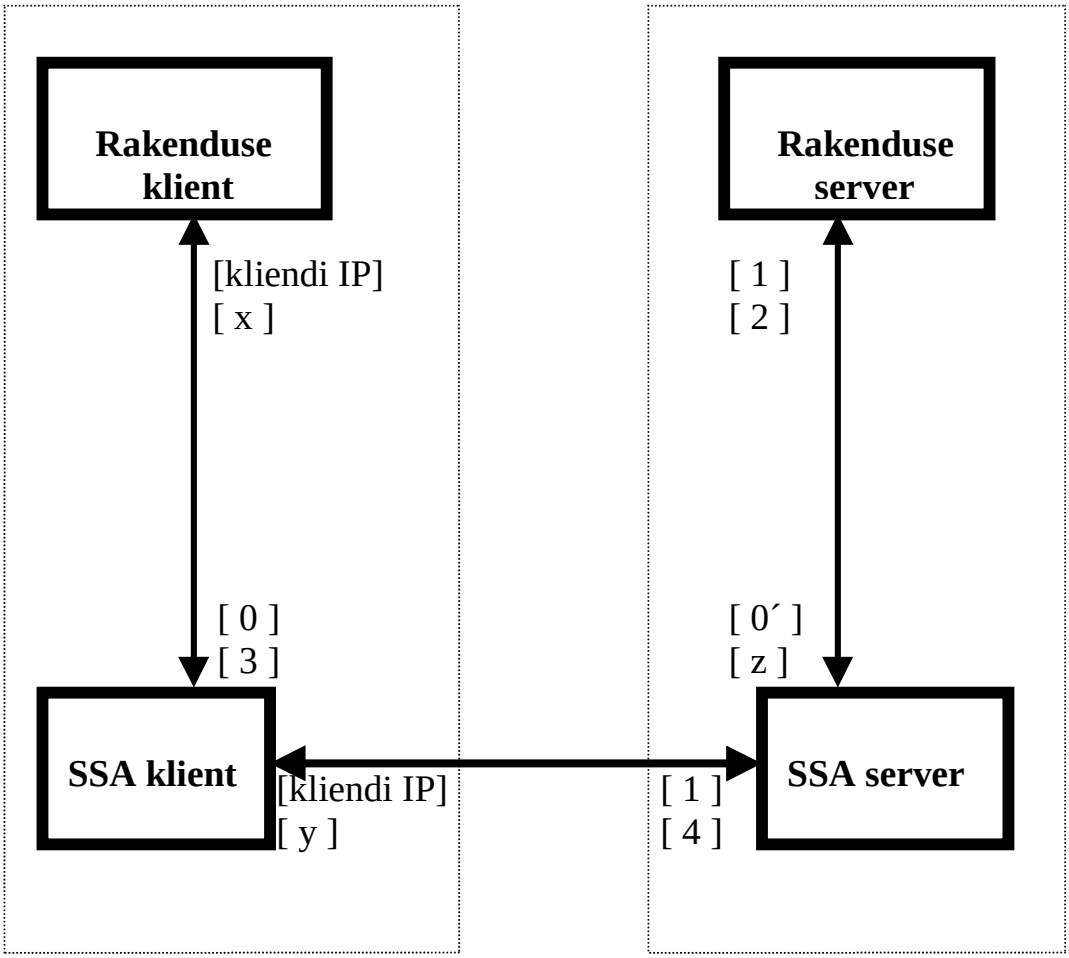
Samm	Kes	Mis	DA	DP	SA	SP
1	rakenduse klient	päring	[1]	[2]	kliendi IP	mingi >1023
2	rakenduse server	vastus	SA(1)	SP(1)	[1]	[2]

Turvatud ühendus

Samm	Kes	Mis	DA	DP	SA	SP
1	rakenduse klient	päring	[0]	[3]	kliendi IP	mingi >1023
2	SSA klient	krüpt	[1]	[4]	kliendi IP	[3] või mingi >1023
3	SSA server	dekrüpt	[1]	[2]	serveri loopback IP aadr.	[4] või mingi >1023
4	rakenduse server	vastus	SA(3)	SP(3)	[1]	[2]
5	SSA server	krüpt	SA(2)	SP(2)	[1]	[4]
6	SSA klient	dekrüpt	SA(1)	SP(1)	[0]	[3]

[0] Kliendi *loopback*'i IP aadress (127.0.0.1)
[1] Serveri IP aadress
[2] Rakenduse serveri TCP port
[3] SSA kliendi TCP port
[4] SSA serveri TCP port

DA Destination Address
DP Destination Port
SA Source Address
SP Source Port



[0] Kliendi *loopback*'i IP aadress (127.0.0.1)
[1] Serveri IP aadress
[2] Rakenduse serveri TCP port
[3] SSA kliendi TCP port
[4] SSA serveri TCP port