



Euroopa Liit
Euroopa
Regionaalarengu Fond



Eesti tuleviku heaks

X-TEE 5.0

TURVASERVERI KASUTUSJUHEND

5.08

REDAKTSIOONIDE AJALUGU

KUUPÄEV	REDAKTSIOON	KIRJELDUS	AUTORID
27.10.2010	5.0	Uuendused seoses X-tee versiooniga 5.0. Uus dokumendimall.	Märt Laur
28.10.2010	5.01	Üldised täiendused.	Märt Laur
9.02.2011	5.02	Märkused alamasutuste ja -andmekogude toe kohta; pordid ja protsessid tugevdamise jaotises; pöördteisendused; IP-aadressi vahetamine jpm.	Märt Laur
10.03.2011	5.03	Juhised meilivahenduse seadistamiseks, tugevdamine, <i>schema URI</i> jm.	Märt Laur
14.03.2011	5.04	Väljuv port 5555.	Märt Laur
29.04.2011	5.05	Lisatud jaotised "2.4.2 Võtmete kaitse parool", "11.1 Veebikasutajate haldus" ja "11.2 Andmete importimine versioonist 4".	Märt Laur
14.10.2011	5.06	ARR->RIHA, märkus 7zip'i kohta.	Märt Laur
8.11.2011	5.07	Parandus konfigureerimistegevuste järjekorras. Lisatud konfiguratsiooni taastamise järeltegevused.	Märt Laur
7.02.2012	5.08	Lisatud tar'i kasutamise näidis andmete importimiseks versioonist 4. Lisatud riistvaranõuded.	Märt Laur

SISUKORD

1	SISSEJUHDATUS	6
1.1	Sihtgrupp	6
1.2	X-tee turvaserver	6
1.3	Uut versioonis 5.0.....	7
2	PAIGALDAMINE JA KONFIGUREERIMINE	8
2.1	Teadmiseks enne paigaldamist.....	8
2.2	Nõuded turvaserveri riistvarale.....	8
2.3	Tulemüüri seadistamine turvaserveri tööks	8
2.4	Allalaadimine ja paigaldamine	9
2.4.1	Allalaadimine.....	9
2.4.2	Võtmete kaitse parool.....	10
2.5	Keskserverite määramine	10
2.6	DNSi võtme sisestamine	10
2.7	Sertifitseerimiskeskuse võtme sisestamine	11
2.8	IP-aadressidele pöördteisenduste tegemine.....	11
2.9	Turvaserveri seadistamine meilivahenduseks	11
3	TURVASERVERI TUGEVDAMINE	13
3.1	Sissejuhatus	13
3.2	Üldised nõuded.....	13
3.2.1	Mitmesugust	13
3.2.2	Nõuded võrgukonfiguratsioonile	13
3.2.3	Tugevate paroolide kehtestamine	13
3.2.4	GRUBi ja BIOSi parool	13
3.2.5	Apticron.....	14
3.2.6	SSH konfigureerimine.....	14
3.2.7	Suid- ja sgid-bitiga binaarfailid	14
3.2.8	Teavitused juurkasutaja sisselogimisest.....	15
3.2.9	History-fail	15
3.2.10	Portide konfigureerimine.....	15
3.2.11	Automaatne turvaseadistamine	15
4	ORGANISATSIOONI LISAMINE	16
4.1	Sisevõrgu serverite seadistamine	16
4.1.1	Infosüsteemi serveri seadistamine HTTPS kasutamiseks	16
4.1.2	Adapterserveri seadistamine HTTPS kasutamiseks	17
4.2	Organisatsiooni sertifitseerimine	17
4.2.1	Asutuse turvaserveri võtme ja sertifikaadipäringu loomine	18
4.2.2	Asutuse turvaserveri sertifikaadi kasutussevõtmine.....	18
4.2.3	Uue andmekogu lisamine ja sertifitseerimine.....	19
4.2.4	Andmekogu/registri turvaserveri sertifikaadi kasutussevõtt.....	19
4.3	Adapterserveri parameetrite määramine	20

4.4	Pääsuõiguste määramine asutustele ja gruppidele	21
4.4.1	Sissejuhatus	21
4.4.2	Pääsuõiguste andmine	21
4.4.3	Kui tekib probleem... ..	22
5	ANDMEKOGU TURVASERVERI HALDUS	23
5.1	Sissejuhatus	23
5.2	Adapterserverite sertifikaatide laadimine	23
5.3	Adapterserveri parameetrite määramine	24
5.4	Adapterserveri eemaldamine	25
5.5	Pääsuõiguste haldus	25
5.5.1	Pääsuõiguste määramine režiimis <i>Asutus</i> → <i>päring</i>	25
5.5.2	Pääsuõiguste režiim <i>Päring</i> → <i>asutus</i>	27
5.6	Pääsuõiguste sünkroniseerimine klasteris.....	27
5.6.1	Sissejuhatus	27
5.6.2	Alluv server.....	28
5.6.3	Ülemserver	28
5.7	Agregaatandmekogude haldus kodeerimisteenuses	28
5.7.1	Sissejuhatus	28
5.7.2	Kodeerimisvõtme haldus.....	29
5.7.3	Uue agregaatandmekogu loomine.....	29
5.7.4	Agregaatandmekogu lisamine.....	29
5.8	Andmekogu turvaserveri eemaldamine X-teest.....	29
6	ASUTUSE TURVASERVERI HALDUS	31
6.1	Ülevaade	31
6.2	Infosüsteemi serveri häälestamine	31
6.3	Asutuse infosüsteemi parameetrid	31
6.3.1	Sissejuhatus	31
6.3.2	Seadistamine HTTPS kasutamiseks	31
6.4	Asutuse eemaldamine X-teest.....	32
7	VÕTMEVAHETUS VÄLISTE SUBJEKTIDEGA	33
7.1	Sissejuhatus	33
7.2	DNSi võtme vahetamine	33
7.2.1	Ülevaade.....	33
7.2.2	Uue DNSi võtme sisestamine	34
7.2.3	Uue DNSi võtme kasutussevõtt	34
7.3	Sertifitseerimiskeskuse võtmete vahetamine	34
7.3.1	Uue sertifitseerimisvõtme sisestamine	35
7.3.2	Uue sertifitseerimisvõtme kasutussevõtt	35
7.3.3	Vana sertifitseerimisvõtme kustutamine	36
7.4	Turvaserveri võtme vahetamine.....	36
7.4.1	Uue võtme genereerimine	36
7.4.2	Sertifikaadi turvaserverisse laadimine ja kasutussevõtt	37
7.4.3	Tegevused võtme hävimisel või paljastumisel	37

7.5	Päringulogide salastamine ja turvaserveri salastamisvõtme vahetamine.....	37
7.5.1	Salastamine turvaserveri poolel.....	37
7.5.2	Salastusvõtme loomine ja vahetamine	38
8	SÜSTEEMI LISAKONFIGUREERIMINE.....	40
8.1	Turvaserveri IP-aadressi muutmine.....	40
8.2	Konfiguratsiooni varundamine	40
8.3	Konfiguratsiooni taastamine varukoopiast.....	40
8.4	Taimautide ja logimise sätted.....	41
8.5	Süsteemsete logide uurimine	41
8.6	Meilide ümbersuunamine	42
8.7	Turvaserveri paikamine	42
8.8	Päringulogide arhiveerimine	42
8.8.1	Sissejuhatus.....	42
8.8.2	Arhiveerimine kettale.....	43
8.8.3	Käsitsi arhiveerimine üle võrgu	43
8.8.4	Automaatne arhiveerimine üle võrgu	43
9	SEIRE.....	45
9.1	Ülevaade.....	45
9.2	Jälgitavad parameetrid	46
9.3	SNMP-jälgimisjaamade haldus	47
9.4	Kohalike jälgimisjaamade haldus.....	47
9.5	Seiresüsteemi võtme vahetamine	47
10	ASÜNKROONSED TEATED	49
10.1	Sissejuhatus	49
10.2	Asünkroonsete teadete haldus.....	50
10.3	Asünkroonsete teadete logi	50
11	ERITEGEVUSED	51
11.1	Veebikasutajate haldus.....	51
11.2	Andmete importimine versioonist 4.....	51
11.3	Diagnostika	52
11.4	Lülitamine SHA-1 ja SHA-512 vahel	52
11.5	Vanade päringulogide üleräsimine	52
11.6	XOP-stiilis MIME-manuste kasutamine	53
11.7	Turvaserveri teenuste peatamine ja käivitamine	53
12	LISAD.....	54
12.1	SNMP-teadete MIB definitsioon.....	54
12.2	Vigade lahendamine	54
12.3	Veateated turvaserveri ja infosüsteemi/andmekogu suhtlusel	54

1 SISSEJUHATUS

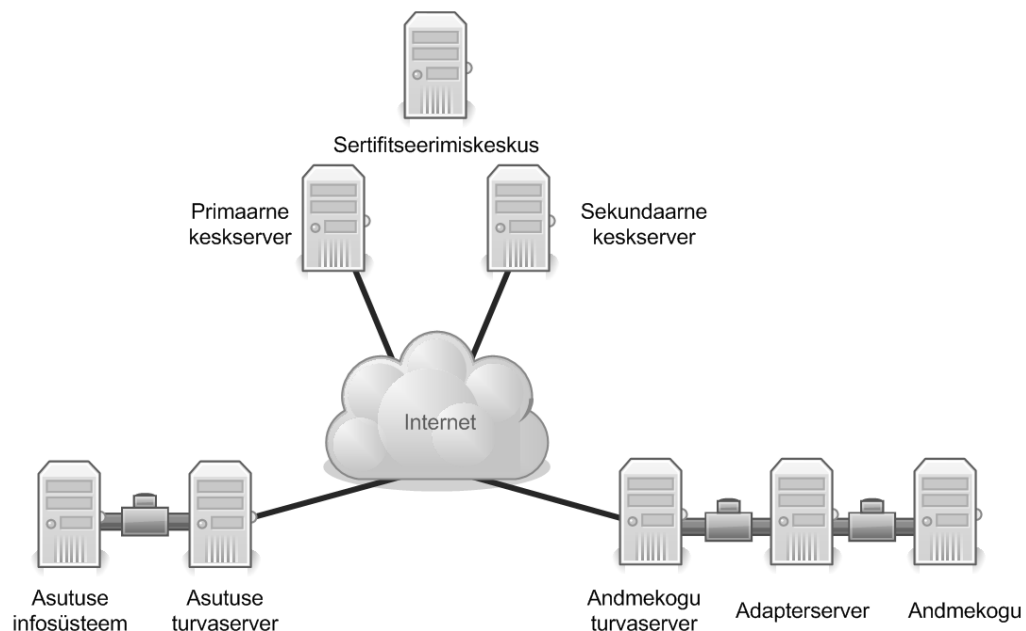
1.1 SIHTGRUPP

Dokument eeldab, et lugejal on vähemalt põhiteadmised Linuxi haldamisest ja arvutivõrkudest.

1.2 X-TEE TURVASERVER

Turvaserveri põhiülesanne on päringute vahendamine (asutusest andmekogusse või vastupidi) viisil, mis tagaks nende hilisema tõendusväärtuse. Juhend kirjeldab tegevusi, mis on vajalikud X-teega liitunud organisatsiooni turvaserveri haldamisel.

Allolev joonis kujutab X-tee põhikomponente.



Turvaserver on ühendatud ühelt poolt avalikku Internetti, teiselt poolt asutuse sisevõrgus paikneva infosüsteemi või adapterserveriga (mis teisendab päringuid andmebaasi ja turvaserveri vahel). Sisuliselt võib turvaserverit käsitleda SOAP-protokolli toetava spetsialiseeritud rakendustaseme tulemüürina, mistõttu võiks turvaserveri paigaldada paralleelselt muid protokolle vahendava asutuse tulemüüriga.

Turvaserverisse on koondatud asutuse infosüsteemi ja adapterserveri vahel vahetatavate andmete turvalisuse tagamiseks vajalik funktsionaalsus.

- Üle avaliku Internetti edastatavad päringud kaitstakse digitaalsignatuuriga ja krüpteeritakse.
- Selleks et oleks võimalik tõestada asutuse poolset andmete väärkasutust või andmekogu poolt väljastatud valeandmeid, salvestatakse päringud turvalisse logisse, mis võimaldab nende toimumist tagantjärele kontrollida.

- Andmekogu-poolne turvaserver rakendab sissetulevatele päringutele pääsukontrolli, tagades, et andmetele saavad juurdepääsu vaid asutused, kellega andmekogul on sõlmitud vastav leping.

Kogu süsteemi käideldavuse tagamiseks on asutuse ja andmekogu turvaserverid dubleeritavad. Üks asutus võib kasutada päringute esitamiseks paralleelselt mitut turvaserverit. Kui andmekogu ühendab sama adapterserveri teenindamiseks võrku mitu turvaserverit, jaotatakse päringute koormus automaatselt turvaserverite vahel. Kui üks andmekogu turvaserveritest rivist välja langeb, suunatakse päringud automaatselt töötavatele turvaserveritele.

Oma töös kasutab turvaserver keskserverit, mis pakub nimeteenust ning kuhu saadetakse perioodiliselt päringute logi vaheväärtusi, et tagada päringute logi usaldusväärse kontrolli võimalus.

Turvaserveri süsteemiülevaate põhiülesanded on turvaserveri paigaldamine, seadistamine ning käigushoidmine. Turvaserveri ja adapterserveri ülemal on volitused ka hädaolukordades tegutsemiseks. Näiteks kui süsteemi rünnatakse ning on karta, et selle tulemusel võib ohtu sattuda andmete terviklus või konfidentsiaalsus, on tal õigus serverid avalikust võrgust lahutada.

Nii turvaserveri kui ka adapterserveri ülemal peab olema koolitatud varuülem, kes asendab teda äraolekul ning on suuteline läbi viima kõiki toiminguid. Oluliste riiklike registrite korral peab süsteemiülevaate olema kindlasti kaks.

1.3 UUT VERSIOONIS 5.0

Alates versioonist 5.0 on turvaserveri kasutajaliides veebipõhine.

Eemaldatud funktsionaalsus:

- Võrgusätete konfigureerimine
- Turvaserveri seiskamine ja taaskäivitamine
- Andmete salvestamine irdmeediale (CD, mälupulk jt) ning sealt lugemine
- Protokoll XML-RPC tugi (kasutatakse eranditult protokoll SOAP)
- PostgreSQL andmebaasi logimine
- Turvaline meilivahetus üle X-tee
- Paikade ja vastupaikade haldus
- UPSi konfigureerimine (soovitav on kasutada paketti "nut", Network UPS Tools)

Muutunud funktsionaalsus:

- Vaikimisi eeldatakse, et turvaserveril on üks võrguliides, mille kaudu toimub kogu suhtlus teiste turvaserverite, keskserverite, andmekogude ja asutustega
- Turvaserveri taaskäivitamisel tuleb konsoolil sisestada *master*-parool, mis kaitseb kõiki turvaserveri privaatvõtmeid.
- Andmete importimine ja eksportimine toimub ainult failide üles- ja allalaadimise teel.
- Turvaserveri uuendusi levitatakse nüüdsest Debiani pakettidena
- Andmekogude menüüsse on lisandunud agregaatandmekogude haldus

Muus osas järgib veebipõhine kasutajaliides võimalikult palju vana kasutajaliidest.

2 PAIGALDAMINE JA KONFIGUREERIMINE

2.1 TEADMISEKS ENNE PAIGALDAMIST

Turvaserver töötab operatsioonisüsteemil Ubuntu Server 10.04 Long-Term Support (LTS); toetatud on nii 32- kui ka 64-bitine platvorm. Turvaserver tarnitakse .deb-pakkidena, mis on kättesaadavad ametlikust X-tee repositooriumist aadressil *ee.x-rd.net*.

Turvaserveri võib paigaldada nii tavalisele kui ka virtualiseeritud riistvarale (testitud on VMWare Server ja Oracle VirtualBox).

Turvaserveri paigaldamiseks läheb vaja järgmisi andmeid:

- Primaarse keskserveri IP-aadress
- Sekundaarsete keskserverite IP-aadressid (kui on)
- DNS-i võtme autentsuskood (küside keskserveri ülemalt)
- Sertifitseerimiskeskuse sertifikaadi autentsuskood (küside keskserveri ülemalt)

Juhend eeldab, et turvaserver paigutatakse ühe võrguliidesega serverisse.

- Kui kasutuses on kaks võrguliidest, tuleb need konfigureerida nii, et neist ühe kaudu on turvaserver ühendatud avalikku Internetti (välisliides), teise kaudu asutuse sisevõrgus paikneva infosüsteemi või adapterserveriga (siseliides).
- Kui kasutuses on üks võrguliides, tuleb dokumendis esinevaid viiteid sise- ja välisliidesele käsitleda sama võrguliidese kohta käivatena.

2.2 NÕUDED TURVASERVERI RIISTVARALE

Soovitavad riistvaraparametrid:

- Server üldiselt peab olema Ubuntu 10.04 poolt toetatud (emaplaat, protsessor, võrgukaardid, salvestussüsteem, graafikaaart);
- 64-bitine Inteli, AMD või ühilduv *dual-core* protsessor;
- 1 GB RAM;
- 100 Mbps võrgukaart;
- 1 vaba USB-pesa mälupulga jaoks.

2.3 TULEMÜÜRI SEADISTAMINE TURVASERVERI TÖÖKS

Kui turvaserver on asutuse tulemüüri taga, peavad tal olema lubatud järgmised sisenevad teenused:

- TCP 5555 – turvaserverite-vaheline SSL/TLS andmevahetus.

Väljuvatest teenustest peavad olema lubatud:

- TCP 25 – SMTP, e-posti (sh tõrketeadete) saatmine Internetti;
- TCP 37 – UNIX'i *time* protokoll diagnostikasüsteemi tarbeks;

- TCP ja UDP 53 – nimeserveri teenused;
- TCP 80 – HTTP, keskserveri võtmete laadimine;
- UDP 123 – NTP, turvaserveri kella sünkroniseerimine;
- TCP 5555 – turvaserverite-vaheline SSL/TLS andmevahetus;
- TCP 5556 – turvaserveri päringute sõnumilühendite logimisprotokoll;
- UDP 6666 – jälgimisjaamadele teabe saatmine (uus SKIP/ESP protokoll, kasutuses alates X-tee versioonist 5.0)

2.4 ALLALAADIMINE JA PAIGALDAMINE

2.4.1 Allalaadimine

Allalaadimiseks tuleb lisada X-tee pakside repositooriumi aadress *apt-get* konfiguratsioonifaili. Selleks tuleb esmalt juurkasutajana redigeerida faili `/etc/apt/sources.list` ja lisada sinna rida:

```
deb http://ee.x-rd.net/packages lucid main
```

Seejärel tuleb anda käsud:

```
sudo apt-get update
sudo apt-get install xtee-keyring
sudo apt-get update
sudo apt-get install xtee-proxy
```

Kuna X-tee pakid on signeeritud, on pakk *xtee-keyring* vajalik, et signeerimisvõti oleks toetatud ja usaldatud, mis võimaldab edaspidi veenduda *xtee-** pakside autentsuses ja installida neid ilma hoiatusteta.

Turvaserveri paigaldamise käigus tuleb määrata turvaserveri privaatvõtmeid kaitsev nn *master-parool*.

Paigaldamise käigus tekitatakse automaatselt ka veebikasutaja:

Kasutajanimi: **webadmin**

Parool: (määrad paigaldusel)

Veebikasutajaid saab hiljem käsurealt lisada ja muuta.

↪ TÄHELEPANU

Enne võtmete ja sertifikaatide konfigureerimist on osa turvaserveri alammenüüdest helestatud. Need menüüd muutuvad kättesaadavaks pärast keskserveri aadressi ning DNS-i ja sertimiskeskuse võtme sisestamist.

Pärast paigaldamist on haldusliides kättesaadav aadressil **<https://serverinimi:3000/>**

2.4.2 Võtmete kaitse parool

Igal turvaserveri käivitamisel tuleb sisestada turvaserveri privaatvõtmeid kaitsev nn *master*-parool. Sellest annab märku algladimise käigus konsoolile ilmuv teade:

Sisesta turvaserveri võtmete kaitse parool (1. katse 3-st)

Sisesta turvaserveri paigaldamisel määratud parool (ekraanil ei kuvata midagi). Õige parooli sisestamiseks on kolm katset; kui ka kolmas katse nurjub, jätkub turvaserveri käivitamine, kuid teenuseid ei hakata vahendama enne, kui veebileidese esilehel on sisestatud õige *master*-parool.

Ülalolev tähendab, et turvaserveri taaskäivitamine nõuab parooli sisestamiseks operaatori füüsilist kohalolu.

Master-parooli vahetamiseks tuleb anda käsk:

```
sudo /usr/xtee/bin/setpwd
```

2.5 KESKSERVERITE MÄÄRAMINE

Oma töös kasutab turvaserver keskserverit, mis pakub nimeteenust (DNS) ning kuhu saadetakse perioodiliselt päringulogide vaheväärtusi. Ehkki keskservereid võib olla mitu (üks primaarne ja üks või rohkem sekundaarset), käsitletakse turvaserveris neid võrdsetena.

Keskserverite lisamiseks:

1. Menüüst **Konfiguratsioon** vali **Serverid**, siis vali **Keskserverid**
2. Klõpsa **Lisa**
3. Sisesta primaarse keskserveri IP-aadress ja klõpsa **Salvesta**
4. Korda eelmisi samme sekundaarse keskserveri (või keskserverite) lisamiseks

2.6 DNSI VÕTME SISESTAMINE

Keskserveri nimeteenuse kaudu levitatavate andmete tervikluse tagamiseks kasutatakse avaliku võtmega krüptograafiat. Keskserver signeerib andmed oma salajase võtmega ning turvaserver kontrollib neid keskserveri avaliku võtmega. Selleks kasutatavaid avalikke võtmeid saab laadida keskserverist. Et vältida valede võtmete laadimist, annab keskserveri ülem turvaserveri ülemale turvaliselt üle võtme sõnumilühendi ehk autentsuskoodi, mis tuleb sisestada turvaserverisse.

Võtme sisestamiseks:

1. Menüüst **Konfiguratsioon** vali **Võtmed ja sertifikaadid**, siis vali **DNSi võtmed**
2. Klõpsa **Sisesta uus võti**
3. Sisesta keskserveri ülemalt saadud DNSi võtme autentsuskood (kujul XX:XX:XX...) ning primaarse keskserveri IP-aadress, seejärel klõpsa **Nõus**. Võtme õnnestunud laadimisel ilmub tema autentsuskood nimekirja olekus "Kehtiv". (*Järgmistel laadimistel, kus kehtiv võti on juba olemas, on lisatud võti kuni aktiveerimiseni olekus "Uus".*)

2.7 SERTIFITSEERIMISKESKUSE VÕTME SISESTAMINE

Turvaserverite-vaheline suhtlus on turvalisuse tagamiseks krüpteeritud, kasutades avaliku võtmega krüptograafia vahendeid. Võtmete hõlpsamaks levitamiseks kasutatakse X-tee keskuses asuva sertifitseerimiskeskuse (CA) väljastatud sertifikaate. Selleks, et neid sertifikaate kontrollida, tuleb turvaserverisse sisestada CA endasigneeritud sertifikaat.

Kuna sertifikaat laaditakse keskserverist üle DNSi, eeldab toiming korrektselt konfigureeritud nimeteenust. Selleks, et vältida valede sertifikaatide laadimist, annab keskserveri ülem turvaserveri ülemale turvaliselt üle CA sertifikaadi sõnumilühendi ehk autentsuskoodi, mis tuleb sisestada turvaserverisse.

Sertifikaadi laadimiseks:

1. Menüüst **Konfiguratsioon** vali **Võtmed ja sertifikaadid**, siis vali **CA sertifikaadid**.
2. Klõpsa **Lisa uus**.
3. Sisesta keskserveri ülemalt saadud autentsuskood (kujul XX:XX:XX...) ning primaarse keskserveri IP-aadress
4. Klõpsa **Nõus**. Võtme õnnestunud laadimisel ilmub tema autentsuskood nimekirja olekuga "Kehtiv".

➤ TÄHELEPANU

Kui sertifikaadi alla laadimisel ilmneb tõrge "Empty answer from dns server", siis tähendab see, et keskserverisse pole CA sertifikaate laaditud. Teata sellest veast keskserveri ülemale.

2.8 IP-AADRESSIDELE PÖÖRDTEISENDUSTE TEGEMINE

Selleks, et turvaserverist saaks korrektselt meili välja saata, tuleb igale turvaserverile anda oma domeenist avalikus võrgus lahenduv hostinimi. (Varasemates X-tee versioonides tekitati selline hostinimi automaatselt domeeni *xtee.riik.ee* alla, alates versioonist 5.0 enam mitte.)

Lisaks tuleb oma võrgus tekitada turvaserverile korrektne IP-aadressi pöördteisendus DNSis (ehk PTR-kirje).

2.9 TURVASERVERI SEADISTAMINE MEILIVAHENDUSEKS

Turvaserver kasutab meiliedastusagendiks (MTA) programmi Postfix. Meili väljasaatmiseks peab turvaserveril olema selline nimi, mida meili vastuvõtjad DNSist näevad. Seega peab serveri nimi DNS-is lahenduma ning serveri IP-aadress peab DNSis lahenduma samaks nimeks.

Postfixi paigaldamisel tuleb valida üks jägmistest ühendusviisidest.

- Vali "Intenet host", kui ühendutakse Internetti otse;
- Vali "Internet host with smarthost" kui meili saab välja saata läbi ühe kindla SMTP-serveri;
- Vali "Local only", kui pole soovi hoiatusteateid meiliga välja saata.

Kui Postfix oli juba varem teisiti konfigureeritud, siis tuleb ümberkonfigureerimiseks anda käsk:

```
sudo dpkg-reconfigure postfix
```

Kui Postfix on konfigureeritud meili välja saatma, hakkab ta kuulama pordil 25 ka sisenevaid ühendusi. See tuleb turvakaalutlustel keelata. Selleks tuleb pärast esialgset (ja pärast iga dpkg-reconfigure abil genereerimist) anda käsud:

```
sudo postconf -e inet_interfaces=loopback-only  
sudo postfix stop  
sudo postfix start
```

3 TURVASERVERI TUGEVDAMINE

3.1 SISSEJUHATUS

Varasemad turvaserveri versioonid tarniti CD-plaadil koos sobivalt eelseadistatud operatsioonisüsteemiga, et tagada süsteemi turvalisus. Alates versioonist 5.0 tarnitakse turvaserver pakkidena, mis tähendab, et vastutus turvaserveri korrektse ja turvalise konfigureerimise eest jääb tema süsteemiülemale kanda.

Lahtiütlus: Järgmised nõuanded turvaserveri tugevdamiseks pole täielikud ega lõplikud.

3.2 ÜLDISED NÕUDED

3.2.1 Mitmesugust

- Et vältida olukorda, kus ründe tulemusel hakkab mõni daemon genereerima liiga palju logisid ja täidab nendega kogu kõvaketta, tuleks katlaog `/var/log` paigutada eraldi partitsioonile.
- Juurkasutaja, tavakasutaja, vajadusel ka GRUBi (*boot loader*) ja BIOSi paroolid tuleb talletada paberil seifis.

3.2.2 Nõuded võrgukonfiguratsioonile

- Failis `/etc/network/interfaces` määra turvaserverile staatiline IP-aadress
- Failis `/etc/resolv.conf` pane DNS-serveriks staatiliselt `127.0.0.1` ja domeeniks `xtee.riik.ee`
- Failis `/etc/hosts` peab olema hostinimi koos IP-aadressiga.

3.2.3 Tugevate paroolide kehtestamine

Anna käsk:

```
sudo apt-get install libpam-cracklib
```

Sätteid saab muuta failist `/etc/pam.d/common-password`. Vaikimisi kehtestatab see paroolide panekul reeglid, et parooli miinimumpikkus on 8 märki (`minlen=8`) ja uus parool peab vanast erinevama 3 märki võrra (`difok=3`).

3.2.4 GRUBi ja BIOSi parool

Kui turvaserverile pääsevad lisaks süsteemiülemale füüsiliselt ligi ka teised isikud, tuleb panna GRUBile (*boot loader*) parool -- siis saab serverit taaskäivitada, aga mitte-vaikimisi valikute lisamiseks on vaja parooli. Sellisel juhul tuleb panna parool ka BIOSile ning lubada alglaadimine ainult kõvakettalt.

3.2.5 Apticron

Paigalda pakk "apticron", mis saadab meili teel teavitusi saadaolevatest turvauuendutest, mida saab konkreetsele serverile paigaldada. Anna käsk:

```
sudo apt-get install apticron
```

Vaikimisi saadetakse teavitused kasutajale "root". Muutmiseks anna käsk:

```
sudo dpkg-reconfigure apticron
```

3.2.6 SSH konfigureerimine

Konfigureerimiseks tuleb muuta faili /etc/sshd_config.

(1) KEELA JUURKASUTAJANA SISSELOGIMINE

Asenda rida "PermitRootLogin yes" reaga "PermitRootLogin no".

NB! Kui varundamise vm jaoks on vaja root-juurdepääsu, siis kasuta direktiivi "PermitRootLogin forced-commands-only".

(2) LUBA AINULT SSH PROTOKOLLI VERSIOON 2 KASUTAMINE

Konfiguratsioonifailis peab olema rida "Protocol 2"

(3) LUBA SSH JUURDEPÄÄS AINULT VOLITATUD KASUTAJATELE

1. Tekita grupp "sshusers", kuhu kuuluvad ainult need kasutajad, kellel peaks olema juurdepääs üle SSH
2. Lisa SSH konfiguratsioonifaili rida "AllowGroups sshusers"
3. Lisa faili /etc/group sektsioon "sshusers" ja pane sinna volitatud kasutajad

(4) VÕIMALUSEL TÕSTA SSH TEISE PORDI PEALE

Vaikimisi kuulab SSH pordis 22. Teatud automaatrünnete vältimiseks võiks pordinumbriks määrata midagi muud kõrgemas pordivahemikus, nt 10022.

3.2.7 Suid- ja sgid-bitiga binaarfailid

Failide leidmiseks anna käsk:

```
sudo find / -perm 4000 -o -perm 2000
```

Suid/sgid biti eemaldamiseks anna käsk:

```
sudo chmod -s <fail>
```

Eemaldamisel tuleb lähtuda igast failist eraldi. Selleks, et paki uuendamisel suid-bitt tagasi ei tuleks, tuleb deb-põhistes distributsioonides need bitid eemaldada permanentselt, kasutades utiliiti *deb-statoverride*. Näiteks kui käsku "at" ei kasutata, saab selle eemaldada järgmiselt:

```
sudo dpkg-statoverride --add root root 755 /usr/bin/at
sudo chown root:root /usr/bin/at
sudo chmod 755 /usr/bin/at
```

3.2.8 Teavitused juurkasutaja sisselogimisest

Konfigureeri süsteem nii, et ta saadaks meili iga kord, kui keegi logib root-kasutajana sisse. Selleks redigeeri faili `/root/.bashrc` (kui on kasutusel Bash) ja lisa sinna järgmine rida:

```
echo -e "Serverisse `hostname` on loginud (`date`)\n`who`" | mail -s "Root logis serverisse `date`" kasutaja@server.ee
```

3.2.9 History-fail

Turvaserveri pakside paigaldusel määratakse failile `.bash_history` automaatselt *append*-atribuut, mis lubab faili avamist ainult ridade lisamiseks.

3.2.10 Portide konfigureerimine

Kõikide kuulavate TCP- ja UDP-portide kuvamiseks anna käsk:

```
sudo lsof -i -n | egrep 'COMMAND|LISTEN|TCP|UDP'
```

Portide sulgemiseks eemalda pordinumbrile vastavat võrguteenust pakkuv pakk või keela võrgus kuulamine muul viisil. Sulgeda ei tohi järgmisi deemonid või protsesse, mis on vajalikud X-tee tööks:

- Andmekogu turvaserver (xtee-producerproxy): TCP 5555
- Infosüsteemi (consumer) Apache: TCP 80 või 443
- Infosüsteemi või andmekogu turvaserveri veebiliides: TCP 3000
- SSH: nagu ülalpool konfigureeritud
- ntpd: UDP *:123
- named: *localhost*, oma port
- postfix: *localhost*, oma port

3.2.11 Automaatne turvaseadistamine

Turvaserveri paki paigaldusel rakendatakse süsteemile automaatselt mõned turvaseadistused. Selleks installitakse uus `/etc/sysctl.conf` fail, mis kehtestab rangemad kerneli turvasätted kui Ubuntu vaikimisi määrab (sealhulgas lülitab välja IPv6, v.a *loopback*-liidesel, kus see on vajalik *ssh -X* kasutamiseks).

4 ORGANISATSIiooni LISAMINE

Selleks, et organisatsioon saaks X-teega suhtlemisel kasutada installeeritud ja seadistatud turvaserverit, tuleb paika panna asutuse infosüsteemi või andmekoguga suhtlemisel kasutatavad parameetrid ning sertifitseerida turvaserver X-tee keskses.

4.1 SISEVÕRGU SERVERITE SEADISTAMINE

Sisevõrgu serverite seadistamise protsess sõltub sellest, kas lisatav organisatsioon on andmeid kasutav asutus või andmeid jagav andmekogu. Esimesel juhul tuleb järgida alajaotises 4.1.1, teisel juhul alajaotistes 4.1.2 ja 4.3 kirjeldatud protseduure.

4.1.1 Infosüsteemi serveri seadistamine HTTPS kasutamiseks

Turvaserver saab infosüsteemi serveritega suhelda kas HTTP- või HTTPS-protokolli vahendusel; vaikimisi on valitud HTTP.

- Protokolli HTTP tuleks kasutada juhul, kui infosüsteemi server ja turvaserver kasutavad omavaheliseks suhtluseks privaatset võrgusegmenti, millesse ei ole ühendatud ühtegi muud arvutit. Samuti ei tohi infosüsteemi server pakkuda interaktiivse sisselogimise võimalust. **Kui tahad seda protokollit kasutada, jätkka organisatsiooni sertifitseerimisega vastavalt jaotisele 4.2**
- Protokolli HTTPS tuleks kasutada juhul, kui infosüsteemi serveri ja turvaserveri vaheliseks suhtluseks pole võimalik eraldi võrgusegmenti eraldada. Sellisel juhul kaitstakse nendevahelist sidet võimaliku jälgimise ja sekkumise eest krüptograafiliste meetoditega. HTTPS-protokolli kasutamisel tuleb infosüsteemi serveri(te) jaoks genereerida sertifikaadid, mis laaditakse turvaserverisse.

Laadi infosüsteemi serveri sertifikaat:

1. Menüüst **Konfiguratsioon** vali **Serverid**, siis vali **Infosüsteemi serverid**
2. Vali organisatsioon, vali lahtrist **Ühendusviis** meetod **HTTPS**, seejärel klõpsa **Laadi**
3. Klõpsa **Browse** ja laadi kettalt infosüsteemi serveri sertifikaat. Fail peab olema kas DER- või PEM-vormingus ning vastavalt *.der* või *.pem* laiendiga.
4. Klõpsa **Nõus**. Õnnestunud laadimisel kuvatakse sertifikaadi sõrmejälgi asutuse sertide loetelus

Genereeri sisevõrgu suhtluseks kasutatav võti:

1. Klõpsa samal lehel **Genereeri uus võti**
2. Sisesta turvaserveri siseliidese IP-aadress ja klõpsa **Nõus**. Turvaserver loob võtme, mida kasutatakse infosüsteemi serverite ja adapterserveritega suhtlemiseks, ning sellele vastava endasigneeritud sertifikaadi. Muutub ka turvaserveri sertifikaadi sõrmejälgi
3. Klõpsa **Ekspordi sertifikaat** ja salvesta pakutav sertifikaat kohalikku arvutisse
4. Klõpsa **Kinnita muudatused**
5. Salvesta eksporditud sertifikaat andmekandjale, vii see asutuse infosüsteemi ning jätkka organisatsiooni sertifitseerimisega vastavalt jaotisele 4.2.

4.1.2 Adapterserveri seadistamine HTTPS kasutamiseks

Selleks et andmekogu või register saaks oma andmeid X-tee kaudu pakkuda, peab ta omama adapterserverit. Adapterserver võtab turvaserverist vastu päringud, mis esitatakse X-tee süsteemis kasutatava SOAP-protokolli vahendusel ning teisendab need andmekogu poolt toetatud keelde (näiteks SQL). Adapterserver võib olla nii eraldiseisev rakendus kui ka andmekogusse juba sisseehitatud tarkvaramoodul.

Turvaserver saab adapterserveriga suhelda kas HTTP- või HTTPS-protokolli vahendusel.

- Kasuta HTTPd, kui adapterserver ja turvaserver suhtlevad võrgusegmenDis, kuhu ei ole ühendatud ühtegi muud arvutit. Samuti ei tohi adapterserver pakkuda interaktiivse sisselogimise võimalust. **HTTP kasutamisel jätkka organisatsiooni sertifitseerimisega vastavalt jaotisele 4.2.**
- Kasuta HTTPSi, kui adapterserveri ja turvaserveri vaheliseks suhtluseks pole võimalik tekitada eraldi võrgusegmenti. Sellisel juhul kaitstakse sidet võimaliku jälgimise ja sekkumise eest krüptograafiliste meetoditega. HTTPS-protokolli kasutamisel tuleb adapterserveri jaoks genereerida sertifikaadid, mis laaditakse turvaserverisse.

Laadi adapterserveri sertifikaat:

1. Menüüst **Konfiguratsioon** vali **Serverid**, siis vali **Adapterserverid**
2. Vali adapterserver, vali lahtrist **Ühendusviis** meetod **HTTPS** ning seejärel klõpsa **Laadi**
3. Klõpsa **Browse** ja laadi kettalt adapterserveri sertifikaat. Fail peab olema kas DER- või PEM-vormingus ning vastavalt *.der* või *.pem* laiendiga.
4. Klõpsa **Nõus**. Õnnestunud laadimisel kuvatakse sertifikaadi sõrmejälgi asutuse sertide loetelus.

Genereeri sisevõrgu suhtluseks kasutatav võti (kui seda veel pole):

1. Klõpsa **Genereeri uus võti**. Turvaserver loob võtme, mida kasutatakse adapterserveri ja infosüsteemi serveritega suhtlemiseks, ning sellele vastava vastava endasigneeritud sertifikaadi. Sertifikaadi sõrmejälgi kuvatakse vastavas lahtris.
2. Klõpsa **Ekspordi sertifikaat** ja salvesta pakutav fail kohaliku arvutisse
3. Salvesta eksporditud sertifikaat andmekandjale, vii see adapterserverisse ning jätkka organisatsiooni sertifitseerimisega vastavalt jaotisele 4.2.

4.2 ORGANISATSIOONI SERTIFITSEERIMINE

Selleks et tagada turvaserverite vahel liikuvate sõnumite konfidentsiaalsus, terviklus ja autentsus, kaitstakse need krüptograafiliste meetoditega. Võtmevahetuse lihtsustamiseks registreeritakse kõigi turvaserverite avalikud võtmed X-tee keskuses, kus neile väljastatakse sertifikaadid.

Enne kui organisatsioon saab turvaserverit päringute vahendamiseks kasutada, peab ta genereerima turvaserveris salajase võtme ning võtma sellele vastavale avalikule võtmele X-tee keskusest sertifikaadi. Sertifikaate levitatakse keskserversis asuva DNS-teenuse vahendusel.

4.2.1 Asutuse turvaserveri võtme ja sertifikaadipäringu loomine

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Asutused**
2. Klõpsa **Lisa**
3. Täida lahtrid *Asutuse nimi* ja *Registrikood* (registrikood võib sisaldada ainult väikeseid ladina tähti, numbreid, miinusmärki ja punkti*), seejärel klõpsa **Salvesta**. Uus asutus kuvatakse nimekirjas
4. Klõpsa nuppu **Salvesta sertifitseerimispäring**, seejärel salvesta pakutav fail kohalikku arvutisse
5. Toimeta sertifitseerimispäring keskserveri ülemale koos järgmise informatsiooniga:
 - Asutuse ametlik nimi;
 - Asutuse registrikood;
 - Asutuse süsteemiülema meiliaadress, kuhu hakatakse saatma tõrketeateid;
 - Turvaserveri IP-aadress.

⚠ TÄHELEPANU

* – Alates versioonist 5.0 saab asutuse nimes kasutada punkti. Selle eesmärk on võimaldada alamasutuste hierarhia loomist. Ehkki X-tee mõistes on tegu sõltumatute asutustega, võimaldab see struktureerida nende nimeruumi, nt registreerides asutusenimesid, mis koosnevad äriregistri koodist ja täiendist. **NB! Alamasutusi saab hakata tekitama alles siis, kui kõik X-tee turvaserverid on uuendatud versioonile 5.0, kuna selles osas pole vanade serveritega tagasiühilduvust.**

4.2.2 Asutuse turvaserveri sertifikaadi kasutussevõtmine

Pärast seda, kui keskserveri ülem on asutusele sertifikaadi väljastanud ning selle DNSi andmebaasi kandnud, saab turvaserveris uue sertifikaadi kasutusse võtta. Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Asutused**
2. Vali asutus ning klõpsa **Halda võtmeid**. Avaneb võtmete halduse lehekülg.
3. Klõpsa **Laadi sertifikaadid**. Toimingu õnnestumisel kuvatakse kehtiva võtme juures olevas lahtris *Sertifikaat* turvaserveri võtmele vastava sertifikaadi sõnumilühend
4. Klõpsa **Salvesta**, et sertifikaat kasutusse võtta

Juhul kui sõnumilühend ei ilmu või kuvatakse viga "Empty answer from DNS server", võib põhjus olla järgmises.

- Sertifikaati pole veel väljastatud.
- Sertifikaat on väljastatud, kuid uuendatud sertide andmebaas pole veel sertimiskeskusest keskserverisse imporditud.
- Sertifikaat on väljastatud ja keskserveri kaudu DNSis publitseeritud, kuid turvaserveri DNSi puhver on värskendamata (uuendus toimub iga 4-6 tunni järel). Sellisel juhul anna menüüst **Konfiguratsioon** käsk **Rekonfigureeri kõik**, mis taaskäivitab *named*-deemoni ja tühjendab sellega puhvri.

4.2.3 Uue andmekogu lisamine ja sertifitseerimine

Andmekogule/registrile sertifikaadipäringu loomiseks tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/registrid**
2. Klõpsa **Lisa andmekogu**
3. Täida lahtrid *Andmekogu nimi* ja *Registrikood* (registrikood võib sisaldada ainult väikeseid ladina tähti, numbreid, sidekriipsu ja punkti*). Lahtrisse *Registrikood* sisesta:
 - a. andmekogu lühinimi, kui andmekogu on registreeritud Riigi infosüsteemi haldussüsteemis (RIHA);
 - b. andmekogu registrikood, kui andmekogu ei ole registreeritud RIHA-s.
4. Klõpsa **Salvesta**. Uus andmekogu kuvatakse nimekirjas.
5. Klõpsa **Salvesta sertifikaadipäring**, seejärel salvesta pakutav fail kohaliku arvutisse
6. Toimeta sertifitseerimispäring keskserveri ülemale koos järgmise informatsiooniga:
 - Andmekogu/registri ametlik nimi;
 - Andmekogu/registri lühinimi või registrikood;
 - Andmekogu süsteemiülema meiliaadress, kuhu hakatakse saatma tõrketeateid;
 - Turvaserveri IP-aadress.

⚠ TÄHELEPANU

* – Alates versioonist 5.0 saab andmekogu nimes kasutada punkti. Selle eesmärk on võimaldada alamüksuste hierarhia loomist. Ehkki X-tee mõistes on tegu sõltumatute andmekogudega, võimaldab see struktureerida nende nimeruumi, nt tehes nimesid, mis koosnevad andmekogu lühinimest ja täiendist. **NB! Alamasutusi saab hakata tekitama alles siis, kui kõik X-tee turvaserverid on uuendatud versioonile 5.0, kuna selles osas pole vanade serveritega tagasiühilduvust.**

4.2.4 Andmekogu/registri turvaserveri sertifikaadi kasutussevõtt

Kui keskserveri ülem on väljastanud andmekogule/registrile sertifikaadi ning kandnud selle DNSi andmebaasi, saab uue sertifikaadi turvaserveris kasutusse võtta. Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/registrid**
2. Vali andmekogu ning klõpsa **Halda võtmeid**
3. Klõpsa **Laadi sertifikaadid**. Toimingu õnnestumisel kuvatakse kehtiva võtme juures olevas lahtris *Sertifikaat* turvaserveri võtmele vastava sertifikaadi sõnumilühend
4. Klõpsa **Salvesta**, et sertifikaat kasutusse võtta. Selle sammu järel peaks olema võimalik turvaserveri vahendusel päringuid esitada

Juhul kui sõnumilühend ei ilmu või kuvatakse viga "Empty answer from DNS server", võib põhjus olla järgmises.

- Keskserveri ülem ei ole veel sertifikaati väljastanud ja nimeteenuse serverisse kopeerinud. Sellisel juhul tuleb oodata, kuni sertifikaat ilmub DNSi andmebaasi
- Sertifikaat on küll DNSi andmebaasis, kuid turvaserveri DNSi puhver on värskendamata (uuendus toimub iga 4-6 tunni järel). Sellisel juhul tuleb puhver käsitsi tühendada, andes menüüst **Konfiguratsioon** käsu **Rekonfigureeri kõik**.

4.3 ADAPTERSERVERI PARAMEETRITE MÄÄRAMINE

Adapterserveri ülesanne on vahendada päringuid andmekogu ja turvaserveri vahel. Andmekogu ja adapterserveri vahel liigub info vastavalt andmebaasispetsiifilisele protokollile; adapterserveri ülesanne on seda tõlgendada ja vahendada turvaserverile standardses SOAP-vormingus. Adapter võib olla ka andmekogusse sisse ehitatud.

Kui turvaserver teenindab andmekogu/registrit, tuleb määrata ka vastava adapterserveri parameetrid.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/registrid**
2. Vali andmekogu ning klõpsa **Adapterserveri parameetrid**
3. Täida lahtrid järgmiselt.
 - **IP** – Adapterserveri IP-aadress
 - **Port** – Adapterserveri HTTP- või HTTPS-päringute vastu võtmiseks kasutatav port (vaikimisi on see HTTP puhul 80 ja HTTPS puhul 443). NB! Kui kasutad protokollit HTTP, siis veendu, et adapterserverite sätetes (Konfiguratsioon > Serverid > Adapterserverid) on samuti valitud protokoll HTTP.
 - **URI** – Adapterserveri URL-i kataloogi ja failinime osa. Näiteks, kui adapterserveri URL on `http://mingiserver/mingikataloog/mingifail`, siis sisesta URI lahtrisse: `/mingikataloog/mingifail`
 - **Skeemi URI** – Adapterserveriga seotud andmekogus teostatud meetodite kirjeldusi sisaldava faili nimi. Näiteks kui päringukirjeldused asuvad aadressil `http://mingiserver/kataloog/andmekogu.wsdl`, siis kirjuta lahtrisse: `/kataloog/andmekogu.wsdl`. Vt ka märkust [1]
 - **Sissetuleva päringuga tegelemise max kestus (sek)** – Maksimaalne aeg, mis kulutatakse ühe andmekogu turvaserverisse tuleva päringuga tegelemiseks. See aeg on mõistlik valida selline, et ta ületaks adapterserveris päringu töötlemiseks ning päringu ja päringuvastuse turvaserverite vahel edastamiseks kuluvat aega. Kui päring või vastus oli manustega SOAP-teade, siis lülitatakse turvaserverite vaheline ajalimiitide loogika ümber ning see aeg tähistab maksimaalset lubatud pausi, mis võib tekkida andmevahetuse käigus. Vt ka märkust [2]
 - **Pingimise intervall (sek)** – Intervall, millega tehakse testpäring andmekogude korrasoleku kontrolliks. Väärtus 0 lülitab kontrolli välja.
4. Klõpsa **Salvesta**

[1] Alates versioonist 5.0 toetab turvaserver teenuseid kirjeldavate XForms-failide allalaadimist. XForm'e otsitakse samast kataloogist, kus on WSDL-schema, ehk lahtris "Skeemi URI" olev failinimi asendatakse otsimisel automaatselt XForms-failinimega. Päringu kuju peab seega olema stiilis: `http://server/cgi-bin/uriproxy?producer=andmekogu&filename=teenus.versioon.xhtml`.

TÄHELEPANU

[2] Ümberlülitamine toimub alles siis, kui turvaserverisse saabub manustega päringu esimene alamosa (SOAP-teade). See tähendab, et tavalise päringu ja manustega vastuse korral peab adapterserver siin määratud aja jooksul turvaserverisse saatma vähemalt manustega sõnumi alguse. Samalaadne üldine piirang on ka asutuse-poolset turvaserveril – aeglaste (suurte) päringute töötlemiseks võib olla vaja pikendada ka asutusepoolset limiiti.

4.4 PÄÄSUÕIGUSTE MÄÄRAMINE ASUTUSTELE JA GRUPPIDELE

4.4.1 Sissejuhatus

Andmekogu/registri turvaserveri kasutussevõtuks tuleb laadida turvaserverisse adapterserveri poolt toetatud päringute nimekiri ning määrata pääsuõigused.

X-tee süsteemis määravad andmete juurdepääsuõigusi nende andmete omanikud. Pääsuõiguste kontroll toimub andmekogu-poolses turvaserveris ning õigusi jagatakse asutuse või asutuste gruppide täpsusega. See tähendab, et mingi päringu sooritamise õigust saab anda vaid tervele asutusele või asutuste grupile. Asutuse töötajatele pääsuõiguste jagamine toimub asutuse infosüsteemis. **NB!** Korrektnel pääsuõiguste kontroll asutuse infosüsteemis on eelduseks asutuse liitumisel X-teega.

Asutuste grupeerimine aitab turvaservereid mugavamalt hallata, kuna gruppidega opereerimine lihtsustab sarnaste asutuste haldamist. Sarnaselt asutustele saab ka asutuste gruppidele anda turvaserveris mitmesuguseid pääsuõigusi. Asutuste grupid luuakse sertifitseerimiskeskuses, turvaserveris neid muuta ei saa.

Pääsuõigusi saab hallata kahes režiimis:

- Režiim **Asutus** → **päring** (vaikevaade) võimaldab määrata päringuid ühele konkreetsele asutusele või grupile. Selguse mõttes käsitleb jaotis ainult seda näidet;
- Režiim **Päring** → **asutus** võimaldab määrata asutusi/gruppe, kellel on õigus ühte konkreetset päringut sooritada.

4.4.2 Pääsuõiguste andmine

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ning klõpsa **Pääsuõigused** (*eeldab häälestatud adapterserverit, vastasel juhul on see nupp helestatud*). Kuvatakse kaks paani: vasakul loetelu gruppide/asutustest (tühi, kui seda pole veel adapterserverist laaditud), paremal loetelu adapterserveri toetatud päringutest.
3. Klõpsa **Lisa**, et valida asutused, kellele hakata pääsuõigusi andma. Valida saab loetelust, mis sisaldab kõiki X-tee keskuses registreeritud subjekte. Vaikimisi kuvatakse ainult grupe, asutuste nägemiseks vali märkeruut **Kuva asutusi**
4. Klõpsa kõiki grupe/asutusi, kellele anda õigus teha päringuid selle turvaserveri teenindatavas andmekogusse, seejärel klõpsa **Nõus**. Valitud subjektid kuvatakse nimekirjas (grupid sinisega, asutused mustaga)
5. Klõpsa **Värskenda**, et laadida turvaserverisse adapterserveri toetatud päringute nimekiri.
6. Määra asutuste/gruppide pääsuõigused: vali vasakpoolsest nimekirjast üksik asutusi/gruppe ning vali märkeruudud nende päringute ees, mille sooritamiseks anda õigus. Kui lisaks on vaja päringut salastada, vaata juhiseid jaotisest 7.5

7. Muudatuste kinnitamiseks klõpsa **Nõus**.

4.4.3 Kui tekib probleem...

Kui asutuse/grupi nimi kuvatakse sulgudes, siis on ta sertifitseerimiskeskusest kustutatud. Soovitav on see asutus/grupp eemaldada ka turvaserverist. Kui kõik asutused ja grupid on sulgudes, võib see tähendada, et turvaserveri ja keskserveri vaheline suhtlus pole töökorras.

Kui päringute laadimine nurjub, on vea põhjuseks tavaliselt valed adapterserveri parameetrid või adapterserveri vale seadistamine. Näiteks veateade "Invalid content type: text/html" võib tähendada järgmist.

- Eelnevalt määratud adapterserveri URI on vigane ning adapterserver vastab päringule HTML-kujul oleva "page not found" veateatega. Kontrolli, et vaates **Konfiguratsioon > Serverid > Adapterserverid** on määratud korrektsed parameetrid.
- Adapterserver on halvasti seadistatud või programmeeritud ning paneb väljastatavate SOAP päringuvastuste tüübiks text/xml asemel text/html. Sel juhul paranda probleem adapterserveris ning proovi uuesti päringute nimekirja laadida.

5 ANDMEKOGU TURVASERVERI HALDUS

5.1 SISSEJUHATUS

Selleks, et andmekogu või register saaks oma andmeid X-tee kaudu pakkuda, peab tal olema adapterserver. Adapterserver võtab turvaserverist vastu SOAP-protokolli vahendusel esitatud päringud ning teisendab need andmekogu poolt toetatud keelde (näiteks SQL).

Turvaserver saab adapterserveriga suhelda kas HTTP- või HTTPS-protokolli vahendusel.

- Kasuta HTTPd juhul, kui adapterserver ja turvaserver suhtlevad võrgusegmendis, millesse ei ole ühendatud ühtegi muud arvutit. Sellisel juhul ei tohi adapterserver pakkuda interaktiivse sisselogimise võimalust.
- Kasuta HTTPSi juhul, kui adapterserveri ja turvaserveri vaheliseks suhtluseks pole võimalik tekitada eraldi võrgusegmenti. Sellisel juhul kaitstakse sidet võimaliku jälgimise ja sekkumise eest krüptograafiliste meetoditega. HTTPSi kasutamisel tuleb adapterserveri jaoks genereerida sertifikaadid ja laadida need turvaserverisse.

HTTPSi kasutamisel rakendatakse autentimist kliendi (turvaserver) ja serveri (adapterserver) pool. Selleks, et turvaserver saaks veenduda, et tema vastaspool on tõesti õige adapterserver, tuleb turvaserverisse laadida adapterserveri sertifikaat. Kasutada võib nii endasigneeritud kui ka kommerts-sertifikaate.

↘ TÄHELEPANU

Valitud protokoll rakendub kõigile adapterserveritele, s.t igale serverile eraldi HTTP või HTTPS kasutamist määrata pole võimalik.

5.2 ADAPTERSERVERITE CERTIFIKAATIDE LAADIMINE

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Serverid**, siis vali **Adapterserverid**
2. Vali lahtrist **Ühendusviis** meetodiks **HTTPS** (*säte kehtib kõigile adapterserveritele*)
3. Vali adapterserver ja klõpsa **Laadi**
4. Klõpsa **Browse** ja laadi kettalt PEM- või DER-vormingus sertifikaat (*cert.pem* või *cert.der*)
5. Klõpsa **Nõus**, seejärel klõpsa **Kinnita muudatused**. Laaditud sertifikaadi sõrmejälj kuvatakse nimekirjas.

Selleks, et kasutada adapterserveriga suhtlemisel kahepoolset autentimist, tuleb adapterserverisse laadida ka turvaserveri sisevõtmele vastav sertifikaat. Kui turvaserveris on olemas varem genereeritud sertifikaat, siis kuvatakse lahtrist "Turvaserveri sertifikaadi sõrmejälj" selle sõnumilühend, kui mitte, kuvatakse tekst "Sertifikaat puudub".

Uue sisevõtme tekitamiseks:

1. Klõpsa samal lehel nuppu **Genereeri uus võti**

2. Sisesta turvaserveri võrguliidese IP-aadress ja klõpsa **Nõus**. Turvaserver tekitab uue võtme, mille sõrmejälj kuvatakse lahtis "Turvaserveri sertifikaadi sõrmejälj".
3. Klõpsa **Ekspordi sertifikaat** ja salvesta pakutav fail (proxycert.tar.gz, sisaldab sertifikaati PEM- ja DER-kujul)
4. Vii sertifikaatide fail adapterserverisse ja lase lisada (või lisa ise) usaldatud sertifikaatide nimekirja. Täpsemad juhised leiad adapterserveri kasutusjuhendist.

⚠ TÄHELEPANU

Turvaserver kasutab adapterserveriga ja asutuse infosüsteemiga suhtluseks sama sisevõtit. See tähendab, et kui sama turvaserver töötab nii asutuse kui ka andmekogu turvaserverina ja kasutab mõlemal juhul HTTPS-protokolli, pead olemasoleva sisevõrgu võtme vahetamisel ümber seadistama nii adapterserveri kui ka asutuse infosüsteemi.

5.3 ADAPTERSERVERI PARAMEETRITE MÄÄRAMINE

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ning klõpsa **Adapterserveri parameetrid**
3. Täida lahtrid järgmiselt
 - **IP** – adapterserveri IP-aadress
 - **Port** – adapterserveris HTTP või HTTPS päringute vastu võtmiseks kasutatav port (vaikimisi on see HTTP puhul 80 ja HTTPS puhul 443)
 - **URI** – adapterserveri kataloog ja failinimi. Näiteks, kui adapterserveri URL on `http://mingiserver/mingikataloog/mingifail`, siis tuleb URI lahtrisse sisestada `/mingikataloog/mingifail`.
 - **Skeemi URI** – adapterserveriga seotud andmekogus teostatud meetodite kirjeldusi sisaldava faili nimi. Näiteks kui päringukirjeldused asuvad failis `/kataloog/andmekogu.wsdl`, siis tuleb lahtrisse kirjutada `/kataloog/andmekogu.wsdl`. **NB!** XForms'i kasutamiseks vt märkust "Skeemi URI" juures jaotises 4.3.
 - **Sissetuleva päringuga tegelemise max kestus (sek)** – maksimaalne aeg, mis kulutatakse ühe andmekogu turvaserverisse tuleva päringuga tegelemiseks. See aeg on mõistlik valida selline, et ta ületaks adapterserveris päringu töötlemiseks ning päringu ja päringuvastuse turvaserverite vahel edastamiseks kuluvat aega. Kui päring või vastus oli manustega SOAP-teade, siis lülitatakse turvaserverite vaheline ajalimiitide loogika ümber ning see aeg tähistab maksimaalset lubatud pausi, mis andmevahetuse käigus võib tekkida. **NB!** Lülitamine toimub alles siis, kui saadetakse manustega päringu esimene alamosa (SOAP teade). See tähendab, et tavalise päringu ja manustega vastuse korral peab adapterserver siin määratud aja jooksul turvaserverisse saatma vähemalt manustega sõnumi alguse. Samalaadne üldine limiit on ka asutuse-poolset turvaserveril – aeglaste (suurte) päringute töötlemiseks võib olla tarvilik pikendada ka asutusepoolset limiiti.
 - **Pingimise intervall (sek)** – Intervall, millega tehakse testpäring andmekogude korrasoleku kontrolliks. Väärtus 0 lülitab kontrolli välja.
4. Klõpsa **Nõus**

5.4 ADAPTERSERVERI EEMALDAMINE

Selleks, et turvaserver ei edastaks adapterserverile ühtki päringut, tuleb muuta adapterserveri parameetreid.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu, mida soovid eemaldada, seejärel klõpsa **Adapterserveri parameetrid**
3. Lahtrisse **IP** kirjuta *0.0.0.0*
4. Tühjenda lahter **Adapterserveri URI**
5. Klõpsa **Kustuta pääsuõiguste andmebaas**. Andmekogu kõigi asutuste pääsuõigused nullitakse, misjärel ei saa ükski asutustest enam andmekogusse päringuid teha. **NB!** Seda toimingut ei saa tagasi võtta.
6. Klõpsa **Nõus**, et muudatused rakendada

5.5 PÄASUÕIGUSTE HALDUS

X-teega liitunud andmekogusse saavad päringuid teha vaid asutused, kes on selle andmekoguga sõlminud vastava lepingu. Päringut tegeva asutuse pääsuõigusi hallatakse ja kontrollitakse andmekogu-poolses turvaserveris. Pääsuõiguste seadmine toimub asutuse täpsusega, asutuses töötavate ametnike volitusi kontrollib asutuse infosüsteem. **NB!** Korrektnel pääsuõiguste kontroll asutuse infosüsteemis on eelduseks asutuse liitumisel X-teega.

Pääsuõigusi saab kuvada kahes režiimis:

- Režiimis **Asutus → päring** kuvatakse valitud asutusele lubatud pääsuõigused. Kasuta seda režiimi juhul, kui on vaja sisestada mõne konkreetse asutusega seotud muudatusi: näiteks uue asutusega andmete kasutamise lepingu sõlmimine, andmete kasutamise lepingu muutmine või lõpetamine.
- Režiimis **Päring → asutus** kuvatakse valitud pääsuõigust omavad asutused. Kasuta seda režiimi juhul, kui on vaja muuta mõne konkreetse päringuga seotud õigusi. Selleks võib vajadus tekkida näiteks juhul, kui adapterserverisse lisatakse uus päring või kui päringuga seotud turvanõuete muutumise tõttu on vaja üle vaadata sellega seotud pääsuõigused.

5.5.1 Pääsuõiguste määramine režiimis **Asutus → päring**

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ning klõpsa **Pääsuõigused eeldab häälestatud adapterserverit, vastasel juhul on see nupp helestatud**). Kuvatakse kaks paani: vasakul loetelu gruppidest/asutustest (tühi, kui seda pole veel adapterserverist laaditud), paremal loetelu adapterserveri toetatud päringutest.

(1) PÄÄSUÕIGUSTE ANDMINE

Eeldusel, et pääsuõiguste aken on avatud, tegutse järgmiselt.

1. Klõpsa **Lisa**, et valida asutused, kellele hakata pääsuõigusi andma. Valida saab loetelust, mis sisaldab kõiki X-tee keskuses registreeritud subjekte. Vaikimisi kuvatakse ainult grappe, asutuste nägemiseks vali märkeruut **Kuva asutusi**
2. Klõpsa kõiki grappe/asutusi, kellele anda õigus teha päringuid selle turvaserveri teenindatavasse andmekogusse, seejärel klõpsa **Nõus**. Valitud subjektid kuvatakse nimekirjas (grupid sinisega, asutused mustaga)
3. Klõpsa **Värskenda**, et laadida turvaserverisse adapterserveri toetatud päringute nimekiri
4. Määra asutuste/gruppide pääsuõigused: vali vasakpoolsest nimekirjast ükshaaval asutusi/gruppe ning vali märkeruudud nende päringute ees, mille sooritamiseks anda õigus. Kui lisaks on vaja päringut salastada, vaata juhiseid jaotisest 7.5
5. Muudatuste kinnitamiseks klõpsa **Nõus**.

Tõrgete korral loe juhiseid jaotisest 4.4.3 "Kui tekib probleem...".

NB! Kui teed pääsuõigustesse muudatusi, siis muutub nupp **Värskenda** seni helestatuks, kuni muudatused on kas salvestatud või neist loobutud.

(2) PÄÄSUÕIGUSTE MUUTUSED VÄRSKENDAMISEL

Kui päringute nimekirja värskendamisel selgub, et mõni päring, mis on ka mõnele asutusele lubatud, on uuest nimekirjast eemaldatud, kuvatakse sellekohane hoiatus. Võimalusi on kaks:

- Kui valid **Eemalda õigused**, kustutatakse kõik selle päringuga seotud õigused;
- Kui valid **Jäta õigused alles**, kustutatakse päring küll toetatud päringute nimekirjast, kuid sellega seonduvad asutuste pääsuõigused jäetakse alles juhaks, kui seda päringut hiljem uuesti toetama hakatakse.

(3) PÄRINGUTE SALASTAMINE

Iga päringu puhul saab määrata, kas valitud asutus võib seda esitada salastatult (tervele grupile salastamisõigust anda ei saa). Päringu salastamise lubamiseks või selle loa äravõtmiseks klõpsa nuppu **Luba päringut salastada**. Salastatavate päringute juures kuvatakse luku ikoon.

TÄHELEPANU! Salastamise lubamine selles dialoogis on vaid üks salastamise eeldustest. Selleks et salastamine tegelikult toimiks, peavad olema täidetud kõik järgmised tingimused:

- Asutus on saanud X-tee keskusest loa päringute salastamiseks ning kantud sertimiskeskuses vastavasse päringu salastajate gruppi;
- Päringuga on kaasa pandud salastamisaotlus;
- Turvaserverisse on laaditud X-tee keskusest saadud salastamisvõti (täpsemat infot selle kohta saad salastamisloa taotlemisel)

(4) PÄÄSUÕIGUSTE EKSPORTIMINE

Pääsuõiguste loendit saab eksportida tekstifailina. Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ja klõpsa **Pääsuõigused**
3. Vali grupp/asutus ja klõpsa **Ekspordi**, et salvestada valitud grupi/asutuse pääsuõigused –või–
Klõpsa **Ekspordi kõik**, et salvestada kõikide gruppide/asutuste pääsuõigused

Salvestamiseks pakutakse faili *proxy_acl.txt*, mis sisaldab pääsuõiguste nimekirja järgmisel kujul:

```
Pääsuõigused:  
AS Testasutus      astest  
    rahvastikuregister.paring1  
    rahvastikuregister.paring2  
    rahvastikuregister.paring5  
Kodanikuportaal   asutus  
    rahvastikuregister.paring2  
    rahvastikuregister.paring6  
Politseiamet      70000728
```

5.5.2 Pääsuõiguste režiim *Päring* → *asutus*

Pääsuõiguste andmine toimub siin sarnaselt režiimiga *asutus* → *päring*, selle erinevusega, et iga päringu kohta saab valida grupi(d) või asutuse(d), millel on õigus seda päringut sooritada.

Erinev on ka pääsuõiguste eksportimine, kus salvestatakse loetelu päringutest ning iga päringu all kõik asutused, kellel on õigus seda päringut sooritada.

5.6 PÄÄSUÕIGUSTE SÜNKRONISEERIMINE KLASTRIS

5.6.1 Sissejuhatus

Pääsuõiguste (ACLide) sünkroniseerimise valikuid on kolm:

- **Iseseisev** – pääsuõigusi ei sünkroniseerita; konkreetsetes turvaserveris oleva andmekogu ACLide muutmine käib ainult selle turvaserveri kasutajaliidese vahendusel ning andmekogu turvaserver ei jaga ACLe teiste turvaserveritega
- **Ülem** – kehtestab oma pääsuõigused alluvatele. Ülemandmekogu saab lisada turvaserverite (välisvõrgu) IP-aadressid, milledele hakatakse saatma ACLi sünkroniseerimise sõnumeid. **Sünkroniseerimine toimub ainult käsitsi.**
- **Alluv** – võtab ülemalt pääsuõigusi vastu; sünkroniseerib ennast vastu võetud ACLide sünkroniseerimise sõnumi peale

Iga lisatud andmekogu turvaserveri kohta näidatakse selle viimati edukalt sünkroniseeritud ACLide konfiguratsiooni kontrollsummat. Kehtivat andmekogu ACLide konfiguratsiooni kontrollsummat näidatakse alati, sõltumata ACLide halduse tüübist.

5.6.2 Alluv server

Valides rolliks "Alluv", kuvatakse ainult pääsuõiguste kontrollsumma. Kõik operatsioonid pääsuõigustega on blokeeritud.

➤ TÄHELEPANU

Alluv-tüüpi turvaserveri taastamisel tuleb tema ülemas sünkroniseerida pääsuõigused iga andmekogu juures.

5.6.3 Ülemserver

Valides rolliks "Ülem", lisanduvad järgmised haldusvõimalused:

- **Lisa** – võimaldab lisada alluvaid IP-aadressi järgi;
- **Eemalda** – eemaldab valitud alluva;
- **Sünkroniseeri** – sünkroniseerib pääsuõigused valitud alluvaga;
- **Sünkroniseeri kõik** – sünkroniseerib pääsuõigused kõigi alluvatega.

Iga alluva kohta kuvatakse tema IP-aadress ja **viimasel edukal sünkroniseerumisel** kasutatud pääsuõiguste kontrollsumma (s.t see ei pruugi vastata alluva tegelikele pääsuõigustele juhul, kui alluvas on näiteks taastatud vanem konfiguratsioon). Kui alluva sünkroniseerimine nurjus, kuvatakse tema kontrollsumma punaselt.

➤ TÄHELEPANU

Ülem-tüüpi turvaserveri taastamisel tuleb sünkroniseerida pääsuõigused iga andmekogu juures.

5.7 AGREGAATANDMEKOGUDE HALDUS KODEERIMISTEENUSES

5.7.1 Sissejuhatus

Alates versioonist 5.0 pakuvad X-tee turvaserverid pseudonümiseerimise ("kodeerimise") teenust, et võimaldada anonüümsete agregaatanalüüside läbiviimist. Teenus kodeerib delikaatsed andmed päringuvastustes nii, et isikut pole võimalik identifitseerida, kuid samas on võimalik erinevatest andmekogudest saadud andmete põhjal koostada vajalik agregaat- ehk koondandmekogu. Sealjuures võib üks andmekogu kuuluda mitmesse agregaatandmekogusse.

Kuna pseudonümiseerimisteenust pakub andmekogu turvaserver, pole sellest tulenevalt süsteemis kesksel nõrka kohta, mis omaks kõiki pseudonümiseerimisvõtmeid või näeks kõiki delikaatseid andmeid avakujul. Allikandmekogudest andmeid saav koondandmekogu on X-tee mõistes asutuse rollis. Koondandmekogu teeb päringuid allikandmekogudesse ning agregeerib saadud pseudonümiseeritud andmed.

Ühe koondandmekogu piires kasutatakse ühte **pseudonümiseerimisvõtit** – see on tähtis, et pseudonümiseeritud andmeid saaks omavahel seostada ja moodustada agregaatandmebaase. Võtit levitatakse kõigile samasse agregaatandmebaasi kuuluvate andmekogude turvaserveritele meetodil, et üks andmekogu (pole oluline, milline) genereerib võtme ning kõik ülejäänud laadivad selle. Pseudonümiseerimisvõtmete levitamine turvaserverite vahel toimub füüsilise andmekandja abil.

5.7.2 Kodeerimisvõtme haldus

Pseudonümiseerimisvõtme **eksportimisel** saab valida, millise andmekogu jaoks võti eksporditakse. Enne allalaadimist krüptitakse võti valitud andmekogu turvaserveri avaliku võtmega ja lisaks signeeritakse veel kohaliku (turvaserveri) kehtiva privaativõtmega

Pseudonümiseerimisvõtme **importimisel** saab valida, milliselt andmekogult võti imporditakse. Importimisel verifitseeritakse imporditud võtme signatuur võtme eksporditud turvaserveri sertifikaadi abil ning krüptitakse võti lahti, kasutades turvaserveri (kehtivat või/ja uut) privaativõtit. Dekrüpteeritud võti salvestatakse turvaserveri konfiguratsiooni ning võetakse kasutusse.

Võtmevahetust pole ette nähtud, sest agregaatandmekogu sisuliselt tähendabki pseudonümiseerimisvõtit, s.t iga uue võtme loomisega luuakse ka uus agregaatandmekogu.

5.7.3 Uue agregaatandmekogu loomine

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**, vali andmekogu ja siis klõpsa **Agregaatandmekogud**
2. Klõpsa **Lisa**
3. Sisesta agregaatandmekogu lühinimi ja kirjeldus
4. Vali pseudonümiseerimisvõtme genereerimine
5. Klõpsa **Salvesta**

5.7.4 Agregaatandmekogu lisamine

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**, vali andmekogu ja siis klõpsa **Agregaatandmekogud**
2. Klõpsa **Lisa**
3. Sisesta agregaatandmekogu lühinimi ja kirjeldus
4. Vali pseudonümiseerimisvõtme importimine
5. Vali kas andmebaas, kust võti laaditakse, või laadi võti kõvakettalt
6. Klõpsa **Salvesta**

5.8 ANDMEKOGU TURVASERVERI EEMALDAMINE X-TEEST

Kui soovid lõpetada andmete jagamise X-tee süsteemi kaudu ning turvaserver teenindab vaid ühte andmekogu, siis tee järgmist:

1. Teata keskserveri ülemale soovist tühistada turvaserveri sertifikaadid;
2. Eemalda turvaserver sisevõrgust;
3. Hävita turvaserveri privaativõtmed, kustutades kõik turvaserveri kõvakettal olevad andmed.

Kui on vaja turvaserver siiski käiku jätta, kuna ta täidab samas organisatsioonis teiste andmekogude/registrite või asutuse turvaserveri rolli, tuleb tühistada andmekogu sertifikaadid. Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ja klõpsa **Võtmed**
3. Kirjuta üles kõigi sertifikaatide autentsuskoodid ning edasta need keskserveri ülemale koos palvega need sertifikaadid tühistada.
4. Klõpsa **Loobu**, et pöörduda tagasi loetelusse, seejärel klõpsa **Eemalda andmekogu**. Toimingule küsitakse kinnitust, seejärel kustutatakse turvaserverist andmekogu teenindamiseks kasutatav privaatvõti, sertifikaadid ning vastav adapterserveri konfiguratsioon koos pääsuõigustega

6 ASUTUSE TURVASERVERI HALDUS

6.1 ÜLEVAADE

X-teega liitunud asutused saavad turvaserveri vahendusel esitada oma infosüsteemist andmekogudesse päringuid. Selleks on vaja paika panna infosüsteemi serveri(te) ja turvaserveri vahelise suhtluse parameetrid. See jaotis kirjeldab vajalikke tegevusi infosüsteemi (alajaotis 6.2) ja turvaserveri (ülejäanud alajaotised) seadistamiseks.

6.2 INFOSÜSTEEMI SERVERI HÄÄLESTAMINE

Selleks et infosüsteem saaks turvaserverit päringute esitamiseks kasutada, peab infosüsteemi häälestama turvaserveri põhiparameetritega. Need on järgmised:

- **IP-aadress** – turvaserveri siseliidese IP-aadress,
- **Port** – HTTP kasutamisel 80, HTTPS kasutamisel 443
- **URI** – /cgi-bin/consumer_proxy
- **HTTPS sertifikaat** – vt. jaotist 4.3.

Infosüsteemi seadistamist kirjeldab "Infosüsteemi halduri kasutajajuhend".

6.3 ASUTUSE INFOSÜSTEEMI PARAMEETRID

6.3.1 Sissejuhatus

Turvaserver saab infosüsteemi serveritega suhelda kas HTTP- või HTTPS-protokolli vahendusel; vaikimisi on valitud HTTP.

- Protokolli HTTP tuleks kasutada juhul, kui infosüsteemi server ja turvaserver kasutavad omavaheliseks suhtluseks privaatset võrgusegmenti, millesse ei ole ühendatud ühtegi muud arvutit. Samuti ei tohi infosüsteemi server pakkuda interaktiivse sisselogimise võimalust.
- Protokolli HTTPS tuleks kasutada juhul, kui infosüsteemi serveri ja turvaserveri vaheliseks suhtluseks pole võimalik eraldi võrgusegmenti eraldada. Sellisel juhul kaitstakse nendevahelist sidet võimaliku jälgimise ja sekkumise eest krüptograafiliste meetoditega. HTTPS-protokolli kasutamisel tuleb infosüsteemi serveri(te) jaoks genereerida sertifikaadid, mis laaditakse turvaserverisse. **NB!** Autentimine toimub sel juhul nii kliendi (infosüsteemi server) kui ka serveri (turvaserver) poolel.

6.3.2 Seadistamine HTTPS kasutamiseks

Laadi infosüsteemi serveri sertifikaat:

1. Menüüst **Konfiguratsioon** vali **Serverid**, siis vali **Infosüsteemi serverid**
2. Vali organisatsioon, vali lahtrist **Ühendusviis** meetod **HTTPS**, seejärel klõpsa **Laadi**

3. Klõpsa **Browse** ja laadi kettalt infosüsteemi serveri sertifikaat. Fail peab olema kas DER- või PEM-vormingus ning vastavalt `.der` või `.pem` laiendiga.
4. Klõpsa **Nõus**. Õnnestunud laadimisel kuvatakse sertifikaadi sõrmejälgi asutuse sertide loetelus

Turvaserveris tuleb genereerida võti infosüsteemi serveritega suhtlemiseks ning laadida võtmele vastav sertifikaat infosüsteemi serveritesse.

Genereeri sisevõrgu suhtluseks kasutatav võti:

1. Klõpsa samal lehel **Genereeri uus võti**
2. Sisesta turvaserveri siseliidese IP-aadress ja klõpsa **Nõus**. Turvaserver loob võtme, mida kasutatakse infosüsteemi serverite ja adapterserveritega suhtlemiseks, ning sellele vastava endasigneeritud sertifikaadi. Muutub ka turvaserveri sertifikaadi sõrmejälgi
3. Klõpsa **Ekspordi sertifikaat** ja salvesta pakutav sertifikaat kohalikku arvutisse
4. Klõpsa **Kinnita muudatused**
5. Salvesta eksporditud sertifikaat andmekandjale, vii see infosüsteemi serveritesse ning lisa või lase see lisada usaldatud sertifikaatide nimekirja.

➤ TÄHELEPANU

Turvaserver kasutab adapterserveriga ja asutuse infosüsteemiga suhtluseks sama sisevõtit. See tähendab, et kui sama turvaserver töötab nii asutuse kui ka andmekogu turvaserverina ja kasutab mõlemal juhul HTTPS-protokolli, pead olemasoleva sisevõrgu võtme vahetamisel ümber seadistama nii adapterserveri kui ka asutuse infosüsteemi.

6.4 ASUTUSE EEMALDAMINE X-TEEST

Kui soovid lõpetada andmete saamise X-tee süsteemi kaudu ning turvaserver teenindab vaid ühte asutust, tegutse järgmiselt:

- teata keskserveri ülemale soovist tühistada turvaserveri sertifikaadid,
- eemalda turvaserver sisevõrgust,
- hävita turvaserveri privaatvõtmed, kustutades kõik turvaserveri kõvakettal olevad andmed.

Juhul kui soovid turvaserveri siiski tööle jätta, kuna see teenindab ka teisi asutusi, siis soorita allpool kirjeldatud tegevused.

Asutuse eemaldamiseks X-tee süsteemist pead tühistama sellele asutusele vastavad sertifikaadid. Selleks tuleb keskserveri ülemale edastada sertifikaatide sõnumilühendid ning kustutada neile vastav privaatvõti turvaserveri kõvakettalt.

1. Menüüst **Konfiguratsioon** vali **Asutused**
2. Vali asutus, seejärel klõpsa **Halda asutuse võtmeid**
3. Kirjuta üles kõigi sertifikaatide autentsuskoodid ning edasta need keskserveri ülemale, koos palvega need sertifikaadid tühistada
4. Asutusele vastava privaatvõtme kustutamiseks klõpsa **Eemalda asutus** ning klõpsa kinnituse küsimise dialoogis **Jah**. Seepeale kustutatakse turvaserverist asutuse teenindamiseks kasutatav privaatvõti ja sertifikaadid.

7 VÕTMEVAHETUS VÄLISTE SUBJEKTIDEGA

7.1 SISSEJUHATUS

Turvaserveri kasutamisel võib tekkida vajadus vahetada üht järgmistest võtmetest:

- DNS-i vastuste kaitsmiseks kasutatav võti
- turvaserverite sertifitseerimiseks kasutatav võti
- turvaserveri poolt päringute signeerimiseks ja side turvamiseks kasutatav võti.

Võtmevahetus võib olla kas korraline või erakorraline. Esimesel juhul vahetatakse kasutatavat võtit perioodiliselt, et vähendada selle kompromiteerumisega seotud riske. Teisel juhul on põhjuseks subjekti privaativõtme kompromiteerumine või hävimine. Selleks, et hoida ära võtme vahetumisega seotud häireid süsteemi töös, koosnevad X-tee süsteemis kõik väliseid subjekte puudutavad võtmete vahetumised mitmest etapist. Tüüpiliselt sisaldab uue võtme kasutussevõtt järgmisi samme.

- Võtit vahetada sooviv osapool genereerib endale uue võtme ja edastab selle oma suhtluspartneritele.
- Suhtluspartnerid sisestavad uue võtme oma süsteemi ning hakkavad paralleelselt aktsepteerima nii uue kui vana võtmega seotud päringuid ja sideseansse.
- Kui on kindel, et kõik suhtluspartnerid on uue võtme kätte saanud, võtab võtit vahetada sooviv osapool uue võtme tegelikult kasutusse.
- Pärast uue võtme kasutusse võtmist kustutavad suhtluspartnerid vana võtme oma süsteemist.

Selline korraldus tagab süsteemi pideva töö ka võtme vahetamise käigus.

7.2 DNSI VÕTME VAHETAMINE

7.2.1 Ülevaade

Selleks et tagada turvaserverite kohta käiva info autentne levitamine, signeerib keskserver kõik DNSi kirjed. Signatuuride kontrollimiseks peab turvaserveris olema keskserveri avalik võti. See võti laaditakse turvaserverisse HTTP-protokolli abil. Selleks et kontrollida alla laaditud võtme korrektsust, saab turvaserveri ülem keskserveri ülemalt võtme autentsuskoodi, mille ta sisestab turvaserverisse.

Selleks et DNS-i võtme vahetamine toimuks sujuvalt ja X-tee süsteemi tööd häirimata, toimub see neljas etapis.

1. Keskserveri ülem genereerib uue DNS-i võtme ja edastab selle autentsuskoodi turvaserverite ülematele. Lisaks teeb ta teatavaks järgmiste sammude tegemise tähtajad.
2. Turvaserverite ülemad sisestavad uue keskserveri võtme autentsuskoodi ning on seega suutelised vastu võtma nii uue kui vana võtmega signeeritud DNS-kirjeid.
3. Keskserveri ülem kustutab vana võtme ning võtab uue kasutusse.
4. Turvaserverite ülemad kustutavad vana võtme.

Järgmised kaks alajaotist sisaldavad juhiseid sammude 2 ja 4 sooritamiseks (sammud 1 ja 3 teeb keskserveri administraator).

7.2.2 Uue DNSi võtme sisestamine

Uue võtme sisestamiseks turvaserverisse pead teadma uue võtme autentsuskoodi.

1. Menüüs **Konfiguratsioon** klõpsa **Võtmed ja sertifikaadid**, siis klõpsa **DNSi võtmed**
2. Klõpsa **Sisesta uus**
3. Sisesta keskserveri IP-aadress ja keskserverist saadud DNS-võtme autentsuskood, siis klõpsa **Nõus**. Õnnestunud laadimisel lisatakse autentsuskood nimekirja.

NB! Autentsuskoodi sisestamisel tuleb sisestada ka koodis sisalduvad koolonid, tähtede sisestamisel suur- ja väiketähti ei eristata.

Kui võtit ei õnnestunud alla laadida, siis kuvatakse sellekohane veateade. Kui sulgudes olevaks selgituseks on "404 Not Found", siis tähendab see, et sisestatud autentsuskood oli vigane.

7.2.3 Uue DNSi võtme kasutussevõtt

Tegutse järgmiselt.

1. Menüüs **Konfiguratsioon** klõpsa **Võtmed ja sertifikaadid**, siis klõpsa **DNSi võtmed**
2. Klõpsa **Kustuta vana võti**
3. Klõpsa **Kinnita muudatused**

7.3 SERTIFITSEERIMISKESKUSE VÕTMETE VAHETAMINE

Turvaserverid kasutavad oma suhtluspartneritega suhtlemisel side turvalisuse tagamiseks avaliku võtme krüptograafiat. Võtmete hõlpsamaks levitamiseks kasutatakse sertifikaate, mis on väljastatud X-tee keskkuses asuva sertifitseerimiskeskuse poolt. Selleks, et neid sertifikaate kontrollida, peab turvaserver sisaldama sertifitseerimiskeskuse endasigneeritud sertifikaati. See laaditakse keskserverist DNS-protokolliga vahendusel, mistõttu see toiming eeldab korrektselt konfigureeritud nimeteenust. Et vältida valede sertifikaatide laadimist, annab keskserveri ülem turvaserveri ülemale turvaliselt üle sertifitseerimiskeskuse sertifikaadi sõnumilühendi ehk autentsuskoodi, mis tuleb sisestada turvaserverisse.

Selleks et sertifitseerimiskeskuse võtme vahetus toimuks sujuvalt, sooritatakse see mitmes järgus.

1. Keskserveri ülem genereerib uue sertifitseerimiskeskuse võtme ja loob sellele vastava endasigneeritud sertifikaadi. Kõigile turvaserveritele antakse välja uue sertifitseerimisvõtme allkirjastatud sertifikaadid. Keskserveri ülem teatab uue sertifikaadi autentsuskoodi turvaserverite ülematele.
2. Turvaserverite ülemad sisestavad uue sertifitseerimisvõtme autentsuskoodi ning on seega suutelised suhtlema nii uut kui ka vana sertifikaati kasutavate turvaserveritega.

3. Kõik turvaserverite ülemad võtavad kasutusse uue sertifitseerimiskeskuse võtmega allkirjastatud sertifikaadid, jätkates ka vana võtmega allkirjastatud sertifikaatide aktsepteerimist.
4. Keskserveri ülem tühistab vana sertifitseerimisvõtme ning sellega välja antud sertifikaadid.
5. Turvaserverite ülemad kustutavad vana sertifitseerimisvõtme ning hakkavad vastu võtma vaid uue sertifitseerimisvõtmega välja antud sertifikaate.

Järgmised alajaotised sisaldavad juhiseid sammude 2, 3 ja 5 sooritamiseks (sammud 1 ja 4 teeb keskserveri ülem).

7.3.1 Uue sertifitseerimisvõtme sisestamine

Tegutse järgmiselt.

1. Menüüs **Konfiguratsioon** klõpsa **Võtmed ja sertifikaadid**, siis klõpsa **Sertifitseerimiskeskuse sertifikaadid**.
2. Klõpsa **Lisa uus**
3. Sisesta keskserveri ülemalt saadud autentsuskood ning klõpsa **Nõus**. Sertifikaat laaditakse alla ja lisatakse nimekirja olekus "Uus". Seejärel suudab turvaserver sõnumeid vahetada nii uut kui ka vana sertifitseerimiskeskuse sertifikaati kasutavate turvaserveritega.

Kui tekib tõrge:

- Kui kuvatakse veateade "Empty answer from dns server", siis tähendab see, et keskserverisse ei ole CA sertifikaate veel laaditud. Sellisel juhul teata veast keskserveri ülemale.
- Kui kuvatakse veateade "Turvaserveri võtmele ei õnnestu uut sertifikaati laadida", siis tähendab see, et ebaõnnestus uue sertifitseerimisvõtmega kõigi turvaserverite sertifikaatide uuesti väljaandmine. Teata sellest veast keskserveri ülemale.

7.3.2 Uue sertifitseerimisvõtme kasutussevõtt

Pärast seda, kui kõigi turvaserverite ülemad on uue sertifitseerimisvõtme sisestanud ning turvaserverid on valmis uute sertifikaatide kasutamiseks, tuleb turvaserverites kasutusse võtta uue sertifitseerimisvõtmega välja antud sertifikaadid. See ei pea toimuma igal pool samaaegselt, sest paralleelselt toetatakse ka vanu sertifikaate.

1. Menüüs **Konfiguratsioon** klõpsa **Võtmed ja sertifikaadid**, siis klõpsa **Sertifitseerimiskeskuse sertifikaadid**. Kuvatakse kaks sertifikaati, millest üks on olekus "Kehtiv" (hetkel kasutuses) ja teine "Uus" (toetatud, aga mitte veel kasutuses)
2. Klõpsa **Võta uus kasutusse**. Uus sertifikaat muudetakse kehtivaks, senine sertifikaat viiakse olekusse "Vana", et tagada sõnumivahetus teiste turvaserveritega seni, kuni nad pole uut serti kasutusse võtnud.

7.3.3 Vana sertifitseerimisvõtme kustutamine

Vana sertifitseerimisvõtme võib kustutada alles siis, kui kõigis turvaserverites on uus sertifitseerimisvõti kasutusse võetud.

1. Menüüs **Konfiguratsioon** klõpsa **Võtmed** ja **sertifikaadid**, siis klõpsa **Sertifitseerimiskeskuse sertifikaadid**
2. Klõpsa **Kustuta vana**

7.4 TURVASERVERI VÕTME VAHETAMINE

Turvaserveri võtit on vaja vahetada järgmistel põhjustel:

- võtme avalikuks tulekul,
- võtme hävimisel (juhul kui turvaserveri konfiguratsioonist ei olnud varukoopiat tehtud),
- profülaktika mõttes on soovitatav võtme vahetamine kord aastas, et vähendada võtme avalikuks tulemise tõenäosust ning sellega seotud riske.

Kahel esimesel põhjusel toimub erakorraline võtmevahetus, mille käigus tehakse järgmised sammud.

1. Turvaserveri ülem teatab keskserveri ülemale avalikuks tulnud või hävinud võtmega seotud sertifikaatide sõrmejäljed;
2. Keskserveri administraator tühistab avalikuks tulnud võtmele vastavad sertifikaadid;
3. Turvaserveri ülem genereerib uue võtme ning loob sertifitseerimispäringu ;
4. Turvaserveri ülem edastab sertifitseerimispäringu keskserveri ülemale;
5. Keskserveri ülem väljastab sertifitseerimispäringu põhjal sertifikaadi;
6. Turvaserveri ülem laadib uue sertifikaadi turvaserverisse ja võtab selle kasutusse.

Kolmandal põhjusel toimub korraline võtmevahetus, mille käigus tehakse järgmised sammud.

1. Turvaserveri ülem genereerib uue võtme ning loob sertifitseerimispäringu;
2. Turvaserveri ülem edastab sertifitseerimispäringu keskserveri ülemale;
3. Keskserveri ülem väljastab sertifitseerimispäringu põhjal sertifikaadi;
4. Turvaserveri ülem laadib uue sertifikaadi turvaserverisse ja võtab selle kasutusse;
5. Turvaserveri ülem teatab keskserveri ülemale kustutatud võtmega seotud sertifikaatide sõrmejäljed;
6. Keskserveri administraator tühistab kustutatud võtmele vastavad sertifikaadid.

7.4.1 Uue võtme genereerimine

Asutuse turvaserveris:

1. Menüüst **Konfiguratsioon** vali **Asutused**
2. Vali asutus ja klõpsa **Võtmed**
3. Klõpsa **Genereeri uus võti**. Real "Uus võti" kuvatakse "Olemas"
4. Salvesta pakutav serdipäringu fail *certreq.gz* kohalikule kettale
5. Klõpsa **Nõus** kinnitamiseks

Andmekogu turvaserveris:

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ja klõpsa **Võtmed**
3. Klõpsa **Genereeri uus võti**. Real "Uus võti" kuvatakse "Olemas"
4. Salvesta pakutav serdipäringu fail *certreq.gz* kohalikule kettale
5. Klõpsa **Nõus** kinnitamiseks

Mõlemal juhul edasta sertifitseerimispäring keskserveri ülemale koos organisatsiooni ametliku nime ja registrikoodiga.

7.4.2 Sertifikaadi turvaserverisse laadimine ja kasutussevõtt

Pärast seda, kui keskserveri ülem on organisatsioonile uue sertifikaadi väljastanud ning selle DNSi andmebaasi kandnud, võib turvaserveris uue sertifikaadi kasutusse võtta.

NB! Kuna kõik turvaserverid puhverdavad DNSi andmebaasi, siis kulub uue sertifikaadi levitamiseks vähemalt neli tundi. Seetõttu on soovitatav uus sertifikaat kasutusse võtta vähemalt 4-6 tundi pärast selle väljaandmist.

7.4.3 Tegevused võtme hävimisel või paljastumisel

Juhul kui turvaserveris kasutatav võti tuleb avalikuks või hävib, on vaja keskserveri ülemale teatada sellele võtmele välja antud sertifikaatide sõnumilühendid. Tegutse järgmiselt.

Asutuse turvaserveris:

1. Menüüst **Konfiguratsioon** vali **Asutused**
2. Vali asutus ja klõpsa **Võtmed**
3. Kastist **Kehtiv võti** kopeeri real **Sertifikaat** olev võtme sõrmejälgi ja edasta see keskserveri ülemale

Andmekogu turvaserveris:

1. Menüüst **Konfiguratsioon** vali **Andmekogud/Registrid**
2. Vali andmekogu ja klõpsa **Võtmed**
3. Kastist **Kehtiv võti** kopeeri real **Sertifikaat** olev võtme sõrmejälgi ja edasta see keskserveri ülemale

7.5 PÄRINGULOGIDE SALASTAMINE JA TURVASERVERI SALASTAMISVÕTME VAHETAMINE

7.5.1 Salastamine turvaserveri poolel

X-tee süsteemis saab päringulogisid salastada (krüpteerida) kolmel eri viisil, millest üks (ID-kaardi autentimisserdiga salastamine) jääb käesoleva dokumendi raamest välja. Ülejäänud kaks salastamismeetodit on järgmised.

(1) SALASTAMINE KESKSERVERI VÕTMEGA

X-tee keskuse võtmega salastamist teostatakse ainult andmekogu turvaserveris. Protseduur on järgmine.

1. Asutus taotleb X-tee keskusest luba X-tee keskuse võtmega salastatud päringute esitamiseks.
2. Loa saamisel taotleb asutus andmekoguga kokkulepet teatud teenuste päringute salastamiseks.
3. Andmekogu pidaja otsustab, vajadusel seaduslikku põhjendust nõudes, kas kokkulepe sõlmida.
4. Kui asutuse soov rahuldatakse, siis päringud, mida see asutus edaspidi vastavale teenusele esitab, logib andmekogu turvaserver krüpteeritult.

Avakujul info päringu kohta on andmekogu infosüsteemis olemas vaid päringu esitamise hetkel; hiljem pole andmekogul võimalik kindlaks teha, kas selline päringu üldse esitati. Päringute dešifreerimiseks vajalik võti on volitatud järelevalveorgani valduses, kes vajadusel saab logitud päringu dešifreerida. Kui päringu salastamine turvaserveris ebaõnnestub (näiteks salastamine pole lubatud), siis tagastatakse veateade.

NB! Selline salastamine eeldab, et andmekogu turvaserverisse on laaditud keskserveri avalik võti.

(2) SALASTAMINE TURVASERVERI SALASTUSVÕTMEGA (LOKAALSALASTAMINE)

Sõnumite logimine avakujul sisaldab endas mitmeid riske. Turvaserveri ülemal jt turvaserverile juurdepääsu omavatel isikutel on teoreetiliselt võimalik näha sõnumite sisu, samuti on oht, et arhiivikoopiate varguse või kopeerimise korral näevad ründajad arhiveeritud päringuid ja päringuvastuseid.

Riskide vähendamiseks logivad X-tee turvaserverid kõiki päringuid krüpteeritult, lisaks salastatakse kõik logid (nn esimese taseme salastamine). Päringud krüpteeritakse turvaserveri salastusvõtmega, seda nii andmekogu kui ka infosüsteemi turvaserveris. Salastamise kasutamiseks tuleb andmekogu/infosüsteemi turvaserveris genereerida salastusvõti ning salastamine sisse lülitada (vt allpool).

Kui turvaserver on määratud päringuid salastama (see on kohalik teave, mida päringud ei sisalda), siis krüpteeritakse tema salastusvõtmega kõik päringud, mis ei ole määratud ID-kaardiga salastamiseks. Kui turvaserver ei saa nõutud päringut salastada, siis seda päringut ei töödelda ega logita ning päringu esitajale antakse tagasi vastav veateade. Juhul kui lokaalsalastamist kasutavasse serverisse tuleb salastamisnõudega päring, siis salastatakse see veel kord, kasutades X-tee keskserveri võtit (eeldusel, et selleks vajalikud tingimused on täidetud.)

7.5.2 Salastusvõtme loomine ja vahetamine

Selleks et turvaserver saaks salastada logitavaid päringuid, tuleb turvaserveris genereerida salastusvõti. Selle genereerib serveri administraator turvaüleva juuresolekul ning ekspordib võtmepaari privaativõtme osa välisele andmekandjale (flopi, CD, DVD või USB-mälupulk).

Salastusvõtme loomiseks:

1. Menüüst **Konfiguratsioon** vali **Võtmed ja sertifikaadid**, siis vali **Salastamise võti**
2. Vali märkeruut **Kasuta lokaalsalastamist**, mis lülitab sisse salastamise funktsionaalsuse. Kui lokaalsalastamist ei kasutata, logitakse päringud avakujul
3. Klõpsa **Genereeri uus võti**. Süsteem genereerib uue võtmepaari ning uuendab lahtreid CN (Common Name, ühisnimi) ja SN (seerianumber). Päringu tõestamisel otsitakse võtit just nende kahe parameetri järgi.
4. Salvesta pakutav võtmefail (*localseal.tar.gz*, sisaldab loodud võtmepaari privaatvõtme osa).
5. Klõpsa **Kinnita muudatused**, et uus võti kasutusse võtta
6. Tee salvestatud võtmefailist vähemalt kaks koopiat eri andmekandjatele

NB! Eksporditud võtit kasutatakse krüpteeritud logide avamiseks juhtudel, kus tekib vajadus kontrollida mõne päringu õiguspärasust. Seetõttu tuleb võtme koopiaid sisaldavad andmekandjad talletada turvalises asukohas vastavalt organisatsioonilistele reeglitele.

8 SÜSTEEMI LISAKONFIGUREERIMINE

8.1 TURVASERVERI IP-AADRESSI MUUTMINE

Turvaserveri esmasel paigaldamisel lisatakse tema konfiguratsiooni automaatselt välis- ja siseliidese IP-aadressid. Kui emba-kumba aadressi hiljem süsteemis muuta (ükskõik kas käsurealt või Ubuntu graafilisest liidesest), ei muutu see turvaserveris automaatselt õigeks. Selleks et muudatused jõuaks turvaserverisse, tuleb käsurealt anda käsk:

```
sudo dpkg-reconfigure xtee-proxy
```

8.2 KONFIGURATSIOONI VARUNDAMINE

Turvaserveri konfiguratsioonist tuleb teha regulaarselt varukoopiaid. Tegutse järgmiselt.

1. Menüüst **Süsteem** vali **Varunda konfiguratsioon**
2. Klõpsa **Varunda konfiguratsioon**. Varunduseks määratud failid kogutakse ajutisse kataloogi, tehakse arhiiviks ja pakutakse allalaadimiseks. Arhiivifaili nimi on kujul *conf_backup_AAAAkkpp-tmmss*, kus AAAA - varundamise aasta, KK - kuu, PP - kuupäev, tt - tund, mm - minut, ss - sekund.
3. Salvesta arhiivifail turvalisuse huvides otse välisele andmekandjale ja talleta see turvalises kohas, nt seifis. Ära salvesta faili vaheetapina kohalikule kettale!

➤ TÄHELEPANU

Turvaserveri konfiguratsiooni varukoopiaid sisaldavad muuhulgas päringute signeerimiseks ja andmevahetuse turvamiseks kasutatavaid privaatvõtmeid. Seepärast veendu, et varukoopiate konfidentsiaalsus on tagatud!

8.3 KONFIGURATSIOONI TAASTAMINE VARUKOOPIAST

Tegutse järgmiselt.

1. Menüüst **Süsteem** vali **Taasta konfiguratsioon**
2. Klõpsa **Browse** ja vali taastamiseks kasutatav konfiguratsioonifail
3. Klõpsa **Taasta konfiguratsioon**

Kohe pärast konfiguratsiooni taastamist tuleb ära muuta keskserveri IP-aadress ja DNS-i võti (kuna need on igas X-tee 5.0 keskkonnas erinevad), seejärel valida menüüst **Konfiguratsioon** käsk **Rekonfigureeri kõik**. Taastatud konfiguratsiooni korrektsuse kontrollimiseks tuleb menüüst **Süsteem** valida **Diagnostika** ning sealt valida **Testi kõike**. Kui kõik testid õnnestuvad, on turvaserveri konfiguratsioon edukalt taastatud.

➤ TÄHELEPANU

Kui tegu on klastris oleva turvaserveriga, tuleb lisaks läbi viia pääsuõiguste sünkroniseerimine. Alluv-tüüpi turvaserveri puhul tuleb pääsuõigused sünkroniseerida ülem-turvaserveris. Ülem-turvaserveri puhul tuleb sünkroniseerida tema alluvad. Sünkroniseerimine on andmekogupõhine,

ehk kui turvaserveris on mitu andmekogu, tuleb pärast taastamist need ükshaaval läbi käia ja igäühes käivitada pääsuõiguste sünkroniseerimine.

8.4 TAIMAUTIDE JA LOGIMISE SÄTTED

Määrata saab järgmised parameetrid.

- **Andmekogusse tehtavate päringute maksimaalne kestus.** Kui päring edastatakse andmekogule, oodatakse siin määratud perioodi jooksul vastust päringu sooritamise tulemuse kohta. Kui päring või vastus on manustega SOAP-teade, siis kasutatakse seda väärtust pikima lubatud pausina, mille kestel andmeid ei vahetata. NB! Kui tegu on tavalise päringuga ja manustega vastusega, toimub ajalimiitide ümberhäälestamine alles siis, kui andmekogu turvaserver on edastanud esimese osa mitmeosalisest teatest. Seega peaks siin määratud aja jooksul kõik kasutatavad manustega vastuseid saatvad andmekogud vähemalt alustama vastuse saatmist.
- **Logiräside keskserverisse saatmise intervall.** Ajavahemik, mille järel logikirjed keskserverisse saadetakse. Kirjete jäädvustamine keskserveris tagab päringute hilisema tõendusväärtuse. Saatmise intervalli alampiir on 6 minutit (360s), kuna keskserver tõlgendaks sagedasemat saatmist teenusetõkestusründena ja ignoreeriks.
- **Logide kettale sünkroniseerimise intervall.** Iga määratud kirje järel tühjendatakse logifaili puhvid, et süsteemi krahhimisel läheks võimalikult vähe kirjeid kaduma, ning et räsiachel oleks võimalikult suure tõenäosusega jätkatav. Kui intervalli väärtus on 1, kirjutatakse logifailid kettale täiesti sünkroonselt.
- **Päringulogide automaatse arhiveerimise URL, HTTP-meetod ja logide pakkimise lubamine.** HTTP-protokolliga arhiveerimist käsitleb põhjalikumalt jaotis 8.8 "Päringulogide arhiveerimine".
- **Asünkroonse sõnumi esimese ja teise saatmiskatse vahe** (sekundites). Kui saatmine ebaõnnestub, toimub teine katse siin määratud aja möödudes. Iga järgneva katse juures katsetevaheline paus kahekordistub.
- **Järjestikuste saatmiskatsete maksimaalne vahe** (sekundites). Kui ka teine saatmiskatse ebaõnnestub, hakatakse saatmist kordama järjest pikemate pausidega. Selle parameetri väärtus on maksimaalse vahe pikkus sekundites. Kui pausi pikkus kasvaks suuremaks kui maksimaalne lubatud paus, kasutatakse siinset maksimaalset väärtust.
- **Maksimaalselt paralleelselt töödeldavate sõnumite arv.** Arv määrab, mitut sõnumit kõige rohkem korraga üritatakse saata. (Korraga saab saata ainult erinevatele andmekogudele mõeldud teateid)
- **Logide arhiveerimise serverite sertifikaatide sõrmejäljed.** Logide plaadile arhiveerimise alternatiiv on nende edastamine mõnda arhiveerimisega tegelevasse serverisse, kasutades HTTPS-protokolli. Selleks, et veenduda logisid vastu võtva serveri ehtsuses, tuleb turvaserverisse laadida tolle serveri autentimissertifikaat. Kui sertifikaadi importimine õnnestub, kuvatakse serdi sõrmejälg käesolevas lahtris. Vt ka jaotist 8.8 "Päringulogide arhiveerimine".

8.5 SÜSTEEMSETE LOGIDE UURIMINE

Tegutse järgmiselt.

1. Menüüst **Süsteem** vali **Süsteemsed logifailid**.
2. Klõpsa ülemises veerus logifaili nime, et kuvada faili sisu (maksimum 1000 uusimat rida).

Logide meilimiseks sisesta meiliaadress logiakna all olevasse tekstikasti ja klõpsa **Saada**. Eelduseks on, et turvaserver on konfigureeritud meili saatma.

8.6 MEILIDE ÜMBERSUUNAMINE

Selleks et süsteemiülem saaks operatiivselt teada saada süsteemis toimuvast, on võimalik turvaserveri süsteemsete kasutajate *root* ja *postmaster* kirjad ümber suunata välisele meiliaadressile.

1. Menüüst **Süsteem** vali **Meilide ümbersuunamine**
2. Sisesta lahtrisse meiliaadress, kuhu süsteemsed kirjad suunata
–või–
Tühjenda juba täidetud lahter, et suunamine lõpetada
3. Klõpsa **Kinnita muudatused**

Muudatus hakkab kehtima kohe.

8.7 TURVASERVERI PAIKAMINE

Alates versioonist 5.0 ei kasuta X-tee serverid, sh turvaserver, enam spetsiaalset paikade laadimise mehhanismi. Selle asemel levitatakse uusi versioone X-tee repositooriumi kaudu, kust neid saab laadida kas käsurealt (käsuga *apt-get*) või graafilise Package Manageri abil.

Uue versiooni laadimiseks käsurealt (eeldusel, et repositooriumi aadress on määratud vastavalt jaotisele 2.4) tuleb sisestada:

```
sudo apt-get install xtee-proxy
```

Vanemale versioonile tagasipöördumiseks tuleb sisestada käsureale:

```
sudo apt-get install xtee-proxy=5.0
```

Kus "5.0" tuleb asendada soovitud versiooninumbri.

8.8 PÄRINGULOGIDE ARHIVEERIMINE

8.8.1 Sissejuhatus

Turvaserver salvestab kõik tema poolt vastu võetud sõnumid (päringud või päringuvastused) päringulogisse. Kuna päringulogid kasvavad pidevalt, tuleb logid aeg-ajalt arhiveerida ning turvaserverist kustutada. Arhiveerimiseks on järgmised võimalused:

- Andmete edastamine logiserverisse üle Interneti (HTTP või HTTPS).
- Andmete automaatne edastamine logiserverisse üle Interneti (HTTP või HTTPS). Arhiveerimine toimub automaatselt, kui on kogunenud piisavalt andmeid.

Arvesta päringulogide arhiveerimisel, et logikirjed võivad sisaldada konfidentsiaalset teavet. Seetõttu tuleb arhiveeritud logide käitlemisel rakendada samu turvanõudeid, mida rakendatakse adapterserveris või asutuse infosüsteemis salvestatud andmete käitlemisel.

HTTP/HTTPS-protokolliga arhiveerimisel võib kasutada HTTP-meetodit PUT või POST. Meetodit PUT kasutatakse vastavalt HTTP/1.1 standardile (RFC 2616). POST-meetodiga faili saatmisel saadetakse serverisse vastus mõttelisele HTML-vormile, mille ainus element on:

```
<input name="fail" type="file">
```

Serverisse saadetakse *multipart/form-data* tüüpi keha, kusjuures kasutatava välja nimi on "fail". Saadetava faili nimi esitatakse vastavas *Content-Disposition* päises atribuudiga *filename*. Täpsemalt vt RFC 1867.

Kui arhiveerimiseks kasutatav URL sisaldab stringi "%f", siis asendatakse see arhiveeritava faili nimega. Viimane koosneb arhiveerimise kuupäevast ja kellaajast, millisekundi täpsusega. HTTPS-protokollil kasutamisel kasutatakse arhiveerimisserveriga suhtlemisel samu seadeid, mis adapterserveri või infosüsteemi serveriga andmete vahetamisel. Nende seadete muutmist kirjeldab jaotis 6.3.

8.8.2 Arhiveerimine kettale

Tegutse järgmiselt.

1. Menüüst **Süsteem** vali **Arhiveeri päringute logid**
2. Vali **Arhiveeri andmekandjale** ja klõpsa **Arhiveeri**. Toimub logide roteerimine ja ettevalmistamine kirjutamiseks.
3. Salvesta pakutav fail kõvakettale.
4. Vali, kas arhiveeritud logid turvaserverist kustutada või sinna alles jätta. Logide allesjätmine võimaldab teha uuematest logifailidest jooksvalt varukoopiaid ning kustutada failid alles siis, kui on võimalik arhiveerida terve CD- või DVD-täis andmeid.

8.8.3 Käsitsi arhiveerimine üle võrgu

Tegutse järgmiselt.

1. Menüüst **Süsteem** vali **Arhiveeri päringute logid**
2. Vali **Saada HTTP kaudu teise serverisse**
3. Sisesta arhiveerimisserveri URL, vali pöördusmeetod (PUT või POST), siis vali, kas arhiveerida logid pakitult
4. Klõpsa **Arhiveeri**. Toimub logide roteerimine ja ettevalmistamine saatmiseks, seejärel edastatakse kõik logifailid arhiveerimisserverisse. Juhul kui mõne logifaili edastamine ebaõnnestus, loetakse kogu toiming ebaõnnestunuks ning järgmisel katsel saadetakse uuesti kõik failid.

8.8.4 Automaatne arhiveerimine üle võrgu

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Taimauidid ja logimine**

2. Kastis **Päringulogide automaatne arhiveerimine** määra järgmised andmed

- Logide automaatse arhiveerimise URL
- HTTP-meetod (PUT või POST)
- Kas aktiveerida automaatne arhiveerimine
- Kas arhiveerida logifailid gzip'iga pakitult
- Arhiveerimisserveri sertifikaat (vajalik ainult juhul, kui arhiveerid logisid üle HTTPSi; vt ka jaotis 8.4 "Taimautide ja logimise sätted")

Päringulogid arhiveeritakse automaatselt siis, kui logideemon (*sslogd*) taaskäivitatakse, kui logideemonile saadetakse signaal HUP või kui logifail kasvab suuremaks kui ca 20 MB.

Erinevate turvaserverite päringulogid võib HTTP-arhiveerimisel suunata ühte kataloogi, sest arhiveeritava faili ette pannakse hostinimi (nt *myproxy-20100903-144835-1283514515-713867.gz*).

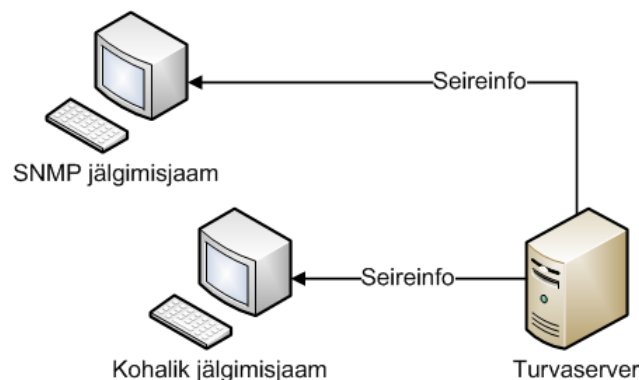
9 SEIRE

9.1 ÜLEVAADE

Ükski süsteem ei püsi turvalise ja töövõimelisena ilma tema töö sagedase jälgimiseta. Samuti peab olema võimalik töö käigus tekkivatele probleemidele (sidekatkestused, riist- ja tarkvara tõrked, serveri ülekoormus jm) kiirelt reageerida. See kehtib ka X-tee kohta.

Tavaliselt paikneb turvaserver serveriruumis, kus süsteemiülem pidevalt ei viibi ning ei saa seetõttu ka serveri oleku kohta piisavalt teavet. Selle tarbeks on X-tee varustatud seiresüsteemiga, mis annab süsteemiülemale operatiivset teavet tema haldusalas olevate turvaserverite hetkeseisu ning kasutatavuse kohta.

Serveritelt info kogumiseks ühendatakse X-tee süsteemiga eriotstarbeline tööjaam, mida nimetatakse kohalikuks jälgimisjaamaks. Kohalik jälgimisjaam võtab vastu seireinfot süsteemiülemala haldusalas olevatelt turvaserveritelt. Lisaks sellele on turvaserveriga võimalik ühendada ka standardset SNMP jälgimistarkvara, mis võtab vastu ja kuvab SNMP *trap* teateid.



Turvaserverid saadavad jälgimisjaamadele kolme liiki sõnumeid:

- Olekuinfo – serverid saadavad perioodiliselt oma olekut kirjeldavate parameetrite (protsessori koormus, vaba mälu maht, jne.) väärtuseid.
- Tõrketeaded – kui päringute vahendamisel tekkis tõrge, siis edastatakse sellekohane teade jälgimisjaamale.
- Päringuinfo – turvaserverid saadavad iga vahendatud päringu kohta jälgimisjaamale päringu päises oleva info (päringu esitanud asutus ja ametniku isikukood, andmekogu ning päringu nimi). See võimaldab jälgimisjaamas teha statistikat päringute populaarsuse ning süsteemi võimalike väärkasutuse tuvastamiseks.

Turvaserveri ja kohaliku jälgimisjaama vahel edastatav seireinfo on krüptitud. Krüptimiseks kasutatakse spetsiaalset seiresüsteemi võtit, mida levitatakse DNS-i vahendusel. Server saadab oma seiresüsteemi võtme automaatselt keskserverile, kus see seostatakse kõigi turvaserveris sisalduvate organisatsioonidega (asutused ja andmekogud) ning lisatakse DNS-i. Kohaliku jälgimisjaama võti viiakse andmekandjal turvaserverisse, kus see salvestatakse.

Turvaserveri ja SNMP jälgimisjaama vaheline info on avalik. Kuna SNMP-protokolliga edastatavaid teateid ei krüptita, siis päringuinfot kui potentsiaalselt konfidentsiaalse iseloomuga andmeid SNMP protokolliga vahendusel ei edastata.

9.2 JÄLGITAVAD PARAMETRID

Turvaserver saadab kõigile jälgimisjaamadele serveris toimuva kohta andmeid. Sellest päringute kasutamise statistika osa (ehk teave selle kohta, kes ja kui palju on esitanud mingit päringut) liigitub turvatundlikuks infoks.

Turvaserver saadab jälgimisjaamadele perioodiliselt järgmisi andmeid.

- **Koormus** – hetkel protsessoriaega ootavate protsesside keskmine arv
- **Vaba aeg** – protsessori vaba ressurs protsentides. Sama suurus, mida näitab utiliit *top*
- **Ootavate ühenduste arv** – hetkel teenindamist ootavate ühenduste arv (teenusetõkestuse-vastase järjekorra suurus). See parameeter kehtib vaid andmekogu turvaserveri kohta
- **Vaba ketas** – vaba kõvakettaruumi maht (MB)
- **Kokku mälu** – kogu operatiivmälu maht (MB)
- **Vaba mälu** – vaba operatiivmälu maht (MB)
- **Kokku saaleala** – kogu saaleala maht (MB)
- **Vaba saaleala** – vaba saaleala maht (MB)
- **Päringute arv** – eelmise teate saatmisest möödunud aja jooksul teenindatud päringute arv. Kehtib vaid turvaserveri kohta
- **Vigade arv** – eelmise teate saatmisest möödunud aja jooksul tekkinud tõrgete arv
- **HTTP-päringute arv** – eelmise teate saatmisest möödunud aja jooksul keskserverile tehtud HTTP-päringute arv
- **Logipäringute arv** – eelmise teate saatmisest möödunud aja jooksul keskserveri logiserverile saadetud logikirjete arv
- **Sissetulev võrguliiklus** – perioodi jooksul võrgust sisse tulnud baitide arv
- **Väljaminev võrguliiklus** – perioodi jooksul võrgust välja läinud baitide arv

Turvaserver edastab jälgimisjaamadele (v.a SNMP-jälgimisjaamad) iga tema poolt vahendatud päringu kohta järgmised andmed:

- päringu esitanud asutus;
- päringu esitaja isikukood;
- päringu nimi;
- andmekogu nimi.

Turvaserver edastab iga ette tuleva vea kohta jälgimisjaamale järgmised andmed:

- vea kood – võimaldab vigade masintõtlust;
- veateade – inimloetav tekst.

9.3 SNMP-JÄLGIMISJAAMADE HALDUS

SNMP jälgimisjaamas töötab standardne SNMP-jälgimistarkvara, mis võtab vastu ja kuvab SNMP *trap* teateid (vt jaotis 12.1). See võimaldab süsteemiülemal, kelle hallata võib olla mitu erinevat turvaserverit, oma serverite olekut mugavamalt jälgida. Kuna serveri ja jälgimisjaama andmevahetus on avalik, siis turvaserver turvatundlikke teateid (s.t. päringute esitamise statistikat) ei vahenda.

SNMP-jälgimisjaama lisamiseks:

1. Menüüst **Konfiguratsioon** vali **Jälgimisjaamad**, siis vali **SNMP jälgimisjaamad**
2. Klõpsa **Lisa**
3. Sisesta jälgimisjaama IP-aadress (see peab olema turvaserverile kättesaadav) ja klõpsa **Nõus**. Uus jälgimisjaam ilmub nimekirja.
4. Klõpsa **Kinnita muudatused**

9.4 KOHALIKE JÄLGIMISJAAMADE HALDUS

Kohalik jälgimisjaam on spetsiaalselt X-tee süsteemi tarvis loodud tarkvara, mis võimaldab süsteemiülemal turvaserveri olekut ja koormust jälgida serverite füüsilisest asukohast sõltumatult.

Serveri ja jälgimisjaama vaheline andmevahetus krüpteeritakse, kasutades protokolle SKIP/ESP. Selleks vajavad mõlemad suhtluspartnerid teise poole avalikku võtit. Turvaserveri vastav võti genereeritakse automaatselt installeerimise käigus ning registreeritakse keskserveris. Kohaliku jälgimisjaama lisamiseks turvaserverile tuleb jaama (jälgimisjaamas genereeritud) võti laadida andmekandjalt (vt ka jaotist "Seiresüsteemi võtme vahetamine").

Kohaliku jälgimisjaama lisamiseks:

1. Menüüst **Konfiguratsioon** vali **Jälgimisjaamad**, siis vali **Kohalikud jälgimisjaamad**
2. Klõpsa **Lisa**
3. Sisesta jälgimisjaama IP-aadress (see peab olema turvaserverile kättesaadav)
4. Klõpsa nuppu **Browse** ja laadi jälgimisjaama võti (*key.gz*)
5. Klõpsa **Nõus**. Uus jälgimisjaam ilmub nimekirja.
6. Klõpsa **Kinnita muudatused**

9.5 SEIRESÜSTEEMI VÕTME VAHETAMINE

Turvaserveri ja jälgimisjaamade vaheline suhtlus krüpteeritakse ainult selleks otstarbeks kasutatava seiresüsteemi võtmega, mis genereeritakse automaatselt turvaserveri installeerimisel.

Selle võtme vahetamine võib toimuda korraliselt või erakorraliselt. Esimesel juhul vahetatakse kasutatavat võtit perioodiliselt (suhteliselt harva), et vähendada selle kompromiteerumisega seotud riske. Teisel juhul on põhjuseks privaatvõtme kompromiteerumine või hävimine.

Tegutse järgmiselt.

1. Menüüst **Konfiguratsioon** vali **Võtmed ja sertifikaadid**, siis vali **Seiresüsteemi võti**
2. Klõpsa **Genereeri uus**. Kuvatakse uue võtme sõrmejalg, võti ise veel kasutuses pole
3. Klõpsa **Kinnita muudatused**, et võti kasutusse võtta

Uus võti võetakse kasutusse kohe pärast salvestamist ning registreeritakse automaatselt ka keskserveris. Võti jõuab DNSi andmebaasi umbes kümne minuti jooksul, misjärel on jälgimisjaamad võimelised uue võtmega krüpteeritud andmeid dekrüpteerima.

10 ASÜNKROONSED TEATED

10.1 SISSEJUHATUS

Asünkroonsed teated on kohest vastust mitte eeldavad teated. Asünkroonsete teadete edastamisel säilitatakse teadet asutuse turvaserveris seni kuni sõnumi saatmine õnnestub või kuni turvaserveri haldur selle kustutab. Asutuse infosüsteem saab kohe kätte sõnumi turvaserverisse jõudmist näitava kviitungi ning edaspidi on teate edastamine turvaserveri vastutuses.

Asünkroonsete teadete edastamine sarnaneb elektronposti edastamisele – klientprogramm annab kirja meiliserverile, kes selle esimesel võimalusel sihtkohta toimetab. Asünkroonsete teate saatmine asutuse infosüsteemist asutuse turvaserverisse õnnestub ka siis, kui asutuse või andmekogu turvaserveri võrguühendus on teate saatmise hetkel katkestatud.

Saatmine loetakse õnnestunuks, kui ei tekkinud sidevigu ning saadud vastus ei ole veateade (*Fault*) adapterserverilt. Kui saatmine ei õnnestu, saadab asutuse turvaserveris asünkroonsete teadete edastamisega tegelev protsess kohalikule administraatorile meili, mis sisaldab muuhulgas vastava andmekogu lühinime.

Konkreetsel andmekogule mõeldud asünkroonsed teated edastatakse sihtkohta samas järjekorras nagu need asutuse turvaserverisse jõudsid. See tähendab, et kui mõne teate edastamine ebaõnnestub sellepärast, et andmekogu adapterserveri vastas veaga, siis jääbki turvaserver seda teadet uuesti saatma ning järgnevate teadete saatmiseni ei jõutagi. Sellisel juhul peaks turvaserveri administraator uurima nurjumise põhjuseid ja eemaldama turvaserveri järjekorrast kas ainult katkise või kõik teated.

Iga andmekogu kohta peetakse turvaserveris eraldi asünkroonsete teadete järjekorda. See tähendab, et probleemid ühe andmekoguga ei takista teistele andmekogudele mõeldud sõnumite kohalejõudmist.

Asünkroonsete sõnumite edastamisega tegeleb turvaserveris spetsiaalne protsess. Iga umbes 10 sekundi järel kontrollitakse kõikide andmekogude järjekordi. Kui järjekorra esimene teade on märgitud eemaldatavaks (vt allpool), siis see eemaldatakse lõplikult. Kui eelmisest saatmiskatses on möödunud piisavalt aega, proovitakse uuesti.

Kõik saatmiskatsed ja teadete lõplikud eemaldamised logitakse asünkroonsete teadete logisse (vt. jaotist 10). Logisid roteeritakse automaatselt korra nädalas ning turvaserveris säilitatakse vähemalt viimase 4 nädala logid. Asünkroonsete teadete logisid ei varundata.

Saatmiskatsete sageduse juhtimine toimub menüü Konfiguratsioon valiku Taimaudid ja logimine abil (vt jaotist 8.4). Järjekordade haldus toimub asünkroonsete teadete halduri abil (vt jaotist 10.2).

10.2 ASÜNKROONSETE TEADETE HALDUS

Asünkroonsete teadete kuvamiseks vali menüüst **Süsteem** funktsioon **Asünkroonsed teated**. Kuvatakse aken, mis annab ülevaate teadete järjekordade hetkeseisust, näitab ebaõnnestunud katsete väljundit ning võimaldab eemaldada teateid järjekorrast.

Kuvatakse järgmine teave.

- **Andmekogu** – Andmekogu täisnimi
- **Sõnumeid** – Saatmata teadete arv
- **Viimane katse** – Teate viimase saatmiskatse aeg
- **Katseid** – Teate saatmiseks tehtud katsete arv
- **Järgmine** – Teate järgmise saatmiskatse aeg
- **Saabus** – Aeg, millal saabus turvaserverisse andmekogu järjekorra esimene teade (see ja eelmine väli omavad väärtust vaid siis kui selles järjekorras on teateid).
- **Lühinimi** – Andmekogu lühinimi

Kui andmekogusse teate saatmine on nurjunud, muutuvad aktiivseks järgmised nupud:

- **Katse väljund** – avab akna viimase saatmiskatse väljundiga, kus on eeldatavalt kirjas ebaõnnestumise põhjus;
- **Nulli saatmisloendur** – nullib saatmiskatsete loenduri ja viimase saatmise aja. Nullimine toob kohe kaasa uue saatmiskatse, nt siis kui ebaõnnestumise põhjus on kõrvaldatud. NB! Ka logisse sattuv katsete loendur nullitakse!

Nimekirjas oleva teate olekut saab muuta:

- **Eemalda** – Eemaldab teate järjekorrast
- **Taasta** – Paneb teate tagasi järjekorda

TÄHELEPANU

Eemaldatuks märgitud esimene teade järjekorras eemaldatakse järjekorrast lõplikult ja ilma seda saatmata kohe, kui saatmisdeemon järjekorda uuesti kontrollima asub (hrl 10 sekundi jooksul). Pärast lõplikku eemaldamist teadet enam taastada ei saa.

10.3 ASÜNKROONSETE TEADETE LOGI

Asünkroonsete teadete logisse tekib kirje iga saatmiskatse või eemaldatuks märgitud teate lõpliku eemaldamise kohta.

11 ERITEGEVUSED

11.1 VEEBIKASUTAJATE HALDUS

Turvaserveri paigaldamisel tekitatakse automaatselt konto "webadmin". Teiste kasutajakontode lisamiseks tuleb käsurealt kasutaja "ui" õigustes anda käsk:

```
/usr/xtee/www/script/newuser <kontonimi> <pärisnimi> <parool>
```

Kontonimi on ühesõnaline, pärisnimi võib olla mitmesõnaline (mis puhul tuleb see panna jutumärkidesse). Näiteks:

```
/usr/xtee/www/script/newuser jrt "Jaan Richard Tamm" 1234abcd
```

Kasutaja parooli muutmiseks tuleb anda sama käsk uue parooliga:

```
/usr/xtee/www/script/newuser jrt "Jaan Richard Tamm" dcba4321
```

(Muutmisele küsitakse kinnitust.)

Kasutaja kustutamiseks tuleb anda käsud:

```
sudo /usr/xtee/www/script/delwebuser <kontonimi>  
sudo /etc/init.d/apache2 reload
```

(Kustutamisele küsitakse kinnitust.)

11.2 ANDMETE IMPORTIMINE VERSIOONIST 4

X-tee v5 turvaserveris saab kasutada vanas (v4) turvaserveris tehtud varukoopiaid, kuid need tuleb enne veebiliidese kaudu üleslaadimist TAR-vormingus kokku pakkida. Windows-keskkonnas tuleb selleks kasutada *GNU Tar* porti* (<http://gnuwin32.sourceforge.net/packages/gtar.htm>), Linux-keskkonnas aga kaasasolevat utiliiti "tar". Loodava arhiivi failinimi võib olla vabalt valitud.

Näidis (Linux-keskkonnas, tekitab korrektse arhiivifaili *varukoopia.tar*, mis on valmis veebiliidese kaudu laadimiseks). Eelduseks on, et failid on andmekandjalt kopeeritud ajutisse kataloogi /tmp/backup.

```
kasutaja@server:~$ cd /tmp
```

```
kasutaja@server:~$ ls backup/  
backup.tar  
backup.tar.sum  
MD5SUMS  
patchlevel  
xteehosttype
```

```
kasutaja@server:/tmp$ tar cvf varukoopia.tar -C backup/ backup.tar \  
backup.tar.sum MD5SUMS patchlevel xteehosttype
```

***Märkus:** Mitte kasutada utiliiti 7zip, mis teadaolevalt tekitab katkiseid TAR-arhiive.

11.3 DIAGNOSTIKA

X-tee on hajutatud süsteem, mille veatu töö eeldab kõigi komponentide koostööd. Tavaliselt on rikete ilmnemisel keeruline selgusele jõuda, kus rike tekis ning kuidas seda lahendada. Diagnostikasüsteemi eesmärk on aidata süsteemiülemat turvaserveri mittetöötamise tuvastamisel ja pakkuda lahendusi tõrgete kõrvaldamiseks.

Diagnostikasüsteem käib samm-sammult läbi turvaserveri konfiguratsiooni ja võrguühenduse ning tõrgete leidmisel pakub neile lahendusi. Teste saab käitada nii automaatsena (käiakse läbi kõik testid kuni esimese vea või kõigi testide õnnestumiseni) kui ka ükshaaval.

Diagnostika käivitamiseks:

1. Menüüst **Süsteem** vali **Diagnostika**
2. Klõpsa **Testi kõike**, et käivitada kõik üheksa testi
–või–
Klõpsa **Käivita** ühe konkreetse testi juures

Kui test nurjub või katkestatakse, kuvatakse vastava testi juures nupp **Anna nõu**. Nupu klõpsamisel kuvatakse probleemi võimalikud põhjused ja lahendusvariandid.

Sõltumata testi tulemusest saab uurida tema väljundit, klõpsates nuppu **Väljund**. Kuvatavat teavet saab kasutada näiteks põhjalikumaks veaotsinguks.

11.4 LÜLITAMINE SHA-1 JA SHA-512 VAHEL

Võib juhtuda, et turvaserver kasutab sellist OpenSSL'i versiooni, mis ei toeta räsialgoritmi SHA-512. Vanema räsialgoritmi (SHA-1) kasutamine võib aga põhjustada probleeme suhtluses turvaserveriga liidestatud infosüsteemide või adapterserveritega. Probleemi lahendamiseks saab turvaserveri lülitada ühilduvusrežiimi, kasutades selleks skripti `obsolete_intcert.sh`:

obsolete_intcert	– näitab senist väärtust
obsolete_intcert 1	– lülitub ühilduvusrežiimi (SHA-1 tugi)
obsolete_intcert 0	– lülitub tavarežiimi (SHA-512 tugi)

Muudatus hakkab kehtima kohe.

11.5 VANADE PÄRINGULOGIDE ÜLERÄSIMINE

Alates versioonist 5.0 kasutab turvaserver päringulogide räsimiseks algoritmi SHA-512, kuna räsifunktsiooni SHA-1 kasutamine polnud enam turvaline. Räsifunktsiooni väljavahetamine tagab aga ainult lisanduvate uute logide jaoks turvalise linkimisahela, mistõttu tuleb kaitsta ka vana räsifunktsiooniga loodud linkimisahelat rünnete eest.

See tähendab, et **turvalisuse huvides peab turvaserveri ülem vanad päringulogid üle räsima**. Juhised selleks on dokumendis "X-tee turvaserveri päringulogide üleräsamise utiliidi kasutajajuhend".

11.6 XOP-STIILIS MIME-MANUSTE KASUTAMINE

Alates versioonist 5.0 toetab turvaserver XOP-stiili (*XML-binary Optimized Packaging*). Selle kasutamiseks tuleb MIME-konteineriga sõnumis anda parameetrile "Content-type" väärtus "application/xop+xml"

11.7 TURVASERVERI TEENUSTE PEATAMINE JA KÄIVITAMINE

Vealahenduse eesmärgil võib olla vaja järgmisi teenuseid käivitada või peatada, milleks Ubuntu on vastavalt käsud *stop* ja *start*. Käskude vorming on:

```
sudo start <teenusenimi>
```

–või–

```
sudo stop <teenusenimi>
```

<Teenusenimi> võib olla üks järgmistest:

- xtee-adapterchecker
- xtee-asyncmanager
- xtee-consumerproxy
- xtee-datasender
- xtee-idlesender
- xtee-mangler
- xtee-netstats
- xtee-producerproxy
- xtee-sslogd

12 LISAD

12.1 SNMP-TEADETE MIB DEFINITSIOON

SNMP-teadete MIB (*Management Information Base*) definitsioon tarnitakse alates versioonist 5.0 koos turvaserveriga, failis `/usr/xtee/etc/snmp_mib_definitions.txt`.

12.2 VIGADE LAHENDAMINE

Enamiku probleemidest lahendavad järgmised tegevused.

Probleemi allikas...	Võimalikud lahendused
Üldine	<ul style="list-style-type: none"> • Proovi toimingut uuesti • Sisesta andmed uuesti • Menüüst Konfiguratsioon vali Rekonfigureeri kõik • Arhiveeri logifailid, et vabastada kõvakettaruumi • Taaskäivita süsteem, et kustutada ajutised failid
Konfiguratsioon (üldine)	<ul style="list-style-type: none"> • Kontrolli konfiguratsioon üle ja sisesta andmed vajadusel uuesti • Taasta konfiguratsioon varukoopiast
Konfiguratsiooni lukustumine	<ul style="list-style-type: none"> • Kontrolli, et pole kasutajale 'www-data' kuuluvaid ripakil semafore (loetlemiseks käsk ipcs, kustutamiseks käsk ipcrm). Veendu, et tead, mida teed!
DNSi võti	<ul style="list-style-type: none"> • Oota, kuni DNSi võti on keskserveris kättesaadavaks tehtud • Kontrolli võrguühendust • Veendu, et võti pärineb volitatud allikast • Veendu, et autentsuskood on sisestatud korrektselt • Võta ühendust keskserveri süsteemiülemaga
Päringute sooritamise või värskendamise	<ul style="list-style-type: none"> • Veendu, et adapterserveri konfiguratsioonis on õige URL • Veendu, et tegu pole adapterserveri sisemise veaga
Vaikimisi lubatud päringute puudumine	<ul style="list-style-type: none"> • Lisa päringud <i>getCharge</i> ja <i>describeMethodAsXML</i> käsitsi
SSL-ühenduse algatamine	<p>Veendu järgnevas:</p> <ul style="list-style-type: none"> • turvaserver saab ühenduse DNSiga, • turvaserveri DNSi puhver on värskendatud, • vastaspoole turvaserver omab kehtivat sertifikaati, • turvaserveris on korrektne DNSi võti.
HTTPS-suhtlus adapterserveriga	<ul style="list-style-type: none"> • Veendu, et oled laadinud adapterserveri sertifikaadi ja adapter on laadinud turvaserveri endasigneeritud sertifikaadi

12.3 VEATEATED TURVASERVERI JA INFOSÜSTEEMI/ANDMEKOGU SUHTLUSEL

Järgmises tabelis on X-tees kasutatava SOAP-protokolli võimalikud veakoodid ning nende selgitused. Vead saadetakse süsteemiülemale tõrketeadetena.

SOAPi veakood	Selgitus
Client.InvalidQuery	Vigane SOAP-päring (viga dekodeerimisel)

SOAPI veakood	Selgitus
Server.InternalError	Sisemine viga serveris. Täpsema põhjuse selgitamiseks tuleb uurida logisid.
Server.Producer.ProcessingError	Andmekogu turvaserveri päringu töötlemine võimatu (põhjused: päring ei sisaldanud kogu vajaliku infot, ei saanud konfiguratsioonile ligi vms.)
Server.Consumer.CannotSign	Asutuse turvaserver ei suutnud päringut signeerida
Server.NoResponse	Ei saanud vastust andmeallikalt (andmekogu turvaserver või adapterserver)
Server.Consumer.InvalidSignature	Andmekogu turvaserverist tulnud vastus ei olnud korrektselt signeeritud
Server.Consumer.InvalidResponse	Andmekogu turvaserverist tulnud vastus ei sisaldanud korrektset SOAP päringuvastust
Server.Consumer.CannotLog	Asutuse turvaserveris ei õnnestunud päringut või päringuvastust korrektselt logida
Server.Producer.CannotReceive	Andmekogu turvaserver ei saanud korrektselt päringut kätte
Server.Producer.InvalidSignature	Asutuse turvaserverist tulnud päringu signatuur oli ebakorrekne
Server.Producer.InvalidQuery	Asutuse turvaserverist tulnud päring ei sisaldanud korrektset SOAP päringut
Server.Producer.NotAllowed	Asutusel ei ole õigust seda päringut teha
Server.Producer.CannotListQueries	Andmekogu turvaserveris ebaõnnestus *.allowedMethods päringu täitmine.
Server.Producer.CannotSign	Andmekogu turvaserver ei suutnud päringut signeerida
Server.Consumer.NoProducerList	Andmekogude nimekirja saamine keskserverist ebaõnnestus
Server.Consumer.FormResponse	Asutuse turvaserveris ebaõnnestus SOAP vastuse moodustamine
Server.Producer.NoPartnerCertificate	Andmekogu turvaserveril ei õnnestunud kätte saada partneri sertifikaati, et teateid verifitseerida.
Server.Producer.InvalidFault	Adapterserver väljastas vigase struktuuriga veateate.
Server.Consumer.NoDiskSpace	Asutuse turvaserveris ei ole piisavalt vaba kettaruumi päringulogide salvestamiseks.
Server.Producer.NoDiskSpace	Andmekogu turvaserveris ei ole piisavalt vaba kettaruumi päringulogide salvestamiseks.
Server.Producer.PeerCertificate	Päringus olev asutuse nimi ei langenud kokku asutuse sertifikaadis olevaga.
Server.Producer.CannotLog	Andmekogu turvaserveris ei õnnestunud päringut või päringuvastust korrektselt logida
Server.Consumer.ProcessingError	Asutuse turvaserveris päringu töötlemine võimatu (põhjused: päring ei sisaldanud kogu vajaliku infot, ei saanud konfiguratsioonile ligi vms.)
Client.UnsupportedQuery	Tundmatu päring
VersionMismatch.*	Vastav tundmatu veastring SOAP-teates
MustUnderstand.*	
Client.*	
Server.*	

