Kleopatra käsiraamat

Marc Mutz
Arendaja: David Faure
Arendaja: Steffen Hansen
Arendaja: Matthias Kalle Dalheimer
Arendaja: Jesper Pedersen
Arendaja: Daniel Molkentin
Tõlge eesti keelde: Marek Laane

Kleopatra käsiraamat

Sisukord

Tabelid

Kokkuvõte

Kleopatra aitab hallata X.509 ja OpenPGP sertifikaate.

Peatükk 1

Sissejuhatus

Kleopatra on KDE tööriist X.509 ja OpenPGP sertifikaatide haldamiseks GpgSM ja GPG võtmekastis ja sertifikaatide tõmbamiseks LDAP ja muudest sertifikaadiserveritest.

Kleopatra saab käivitada nii KMaili menüüst **Tööriistad** → **Sertifikaadihaldur** kui ka käsurealt. Kleopatra käivitatava faili nimi on **`kleopatra`**.

> MÄRKUS
> Rakendus on nime saanud kuulsa Egiptuse naisvaarao Kleopatra järgi, kes elas Julius Caesari ajastul ja kel teatavasti olid Caesariga ka lähedased suhted, millest sündis ka poeg Caesarion.
> Sellise nimevaliku taga seisab asjaolu, et programm on alguse saanud projektist Ägypten (Ägypten tähendab saksa keeles Egiptust).

Peatükk 2

Põhifunktsioonid

2.1 Kohaliku võtmekasti vaatamine

Kleopatra põhifunktsioon on näidata ja võimaldada muuta kohaliku võtmekasti sisu. Võtmekast vastab põhimõtteliselt GPG võtmehoidjale, kuigi seda analoogiat ei peaks väga sõna-sõnalt võtma.

Peaaken jaguneb suureks, mitmest kaardist koosnevaks võtmete nimekirja alaks, menüüribaks, otsinguribaks akna ülaservas ja olekuribaks allservas.

Iga rida võtmete nimekirjas vastab ühele sertifikaadile, mida identifitseerib niinimetatud **Subjekti DN**. DN tähendab 'Distinguished Name' ehk eesti keeles 'eraldusnimi'. See hierarhiline identifikaator sarnaneb mõnevõrra failisüsteemides kasutatavale otsinguteele ning peab olema antud sertifikaadi korral globaalselt unikaalne.

Et (avalik) võti oleks kehtiv ja seeläbi kasutatav, peab selle olema allkirjastanud SK (sertifitseerimiskeskus). Sellist allkirja nimetatakse sertifikaadiks, kuid reeglina kasutatakse mõisteid 'sertifikaat' ja '(avalik) võti' sünonüümidena. Nii talitame ka meie käesolevas käsiraamatus, kui me just otsesõnu neid ei erista.

Et SK-d oleksid kehtivad, peavad nad olema signeeritud teiste SK-de poolt. Selline ahel ei saa mõistagi olla lõputu ning tipptaseme SK (juur-SK) signeerib oma võtme ise (seda nimetatakse segi omasignatuuriks). Seepärast tuleb juursertifikaatide kehtivus (tavaliselt nimetatakse seda usaldusväärsuseks) anda käsitsi, nt. pärast sõrmejälje kontrollimist SK veebilehekülje. Tavaliselt teeb seda süsteemiadministraator või sertifikaate kasutava toote tarnija, kuid seda võib GpgSM käsurida pruukides teha ka kasutaja ise.

Kui soovid näha, millised sertifikaadid on juursertifikaadid, võid lülituda hierarhilisele võtmeloendi vaatele käsuga **Vaade → Hierarhiline sertifikaatide nimekiri**.

Iga sertifikaadi üksikasju saab vaadata sellel topeltklõpsu tehes või käsuga **Vaade → Sertifikaadi üksikasjad**. Seejärel ilmub dialoog, mis näitab sertifikaadi põhiomadusi, sertifikaadiahelat (st. väljaandjate ahelat juur-SK-ni) ning kogu infot, mida taustaprogramm on suuteline sertifikaadist ammutama.

Kui oled muutnud võtmekasti Kleopatrat kasutamata (nt. GpgSM käsurealiidesega), saad vaadet värskendada käsuga **Vaade → Näita uuesti (F5)** .

2.2 Sertifikaadi otsimine ja import

Enamasti saad sa uusi sertifikaate e-kirjade allkirjade ehtsust kontrollides, sest üldjuhul on sertifikaadid allkirja põimitud. Kui sul on aga vaja saata e-kiri kellelegi, kellega sa pole varem suhelnud, tuleb sul tõmmata sertifikaat LDAP kataloogist (seda võib GpgSM küll ka automaatselt

teha) või hankida see failist. Samuti tuleb sul importida pärast SK-lt oma sertifikatsiooninõudele vastuse saamist enda sertifikaat.

Sertifikaadi otsimiseks LDAP kataloogis vali **Fail** → **Otsi sertifikaate serverist** ja sisesta mingi tekst (nt. isiku nimi, keda soovid sertifitseerida) dialoogi **Võtmeserveri sertifikaadiotsing** tekstireale ning klõpsa nupule **Otsi**. Tulemusi näeb võtmeloendis otsinguriba all, kus võib valida sertifikaadi ja seda uurida klõpsuga nupule **Üksikasjad** või alla laadida kohalikku võtmekasti klõpsuga nupule **Impordi**.

Otsitavaid LDAP servereid saab määrata Kleopatra seadistustedialoogi **Kataloogiteenuste** kaardil.

Kui said sertifikaadi failina, proovi käsku **Fail** → **Impordi sertifikaadid... (Ctrl+I)** GpgSM peab selleks aru saama sertifikaadifaili vormingust, nii et vaata GpgSM manuaalist, millised vormingud on toetatud ja millised mitte.

Kui sa ei loo oma võtmepaari GpgSM-i kasutades, pead ka käsitsi importima nii avaliku kui salajase võtme SK-lt saadud PKCS#12 failist. Seda saab teha käsureal **`kleopatra --import-certificate failinimi`** või Kleopatra käsuga **Fail** → **Impordi sertifikaadid... (Ctrl+I)** , nagu see käib ka 'tavaliste' sertifikaatide korral.

2.3 Uue võtmepaari loomine

Menüükäsk **Fail** → **Uus sertifikaat... (Ctrl+N)** käivitab **sertifikaadi loomise nõustaja**. See aitab sul mõne sammuga valmis saada sertifikaadisoovi.

Kui oled nõustajas mingi sammuga ühele poole saanud, vajuta nupule **Järgmine**, et minna edasi järgmise sammu juurde (või nupule **Tagasi**, et vaadata kriitilise pilguga üle juba tehtu). Sertifikaadi loomise võib igal hetkel peatada, vajutades nupule **Loobu**.

Nõustaja esimesel lehel saab valida, millist tüüpi sertifikaat luua:

Isikliku OpenPGP võtmepaari loomine

OpenPGP võtmepaarid luuakse kohalikult ning neid sertifitseerivad sinu sõbrad ja tuttavad. Keskne sertifitseerimiskeskus puudub, selle asemel loob iga üksikisik omaenda usaldusringi, sertifitseerides teiste kasutajate võtmepaare omaenda sertifikaadiga.

Sisestada tuleb **nimi**, **e-posti aadress** ja soovi korral ka **kommentaar**.

Isikliku X.509 võtmepaari ja sertifikaadipäringu loomine

X.509 võtmepaarid luuakse kohalikult, aga sertifitseeritakse tsentraalselt sertifitseerimiskeskuse (SK) poolt. SK võib sertifitseerida teisi SK-sid, luues tsentraliseeritud ja hierarhilise usaldusahela.
Järgmine samm nõustajas on sisestada sertifikaadi tarbeks enda andmed. Täitmist vajavad väljad on järgmised:

- **Üldnimi (CN):** sinu nimi;
- **E-posti aadress:** sinu e-posti aadress. Kirjuta sinna kindlasti kehtiv aadress, sest sellele saadavad inimesed kirju, kui nad sinu sertifikaati kasutavad.
- **Asukoht (L):** linn või asula, kus sa elad.
- **Allüksus (OU):** organisatsiooni allüksus, kuhu sa kuulud. Näiteks ˝Raamatupidamine˝.
- **Organisatsioon (O):** organisatsioon, mida sa esindad (näiteks firma, milles töötad).
- **Maakood (C):** selle maa kahetäheline kood, kus sa elad. Näiteks ˝EE˝.

Järgmine samm nõustajas on valik, kas salvestada sertifikaat faili või saata otse SK-le. Sertifikaadisoovi saatmiseks tuleb määrata failinimi või e- posti aadress.

2.3.1 Võtme tühistamine

Aegunud võtmepaari saab taas kasutusele võtta, kui on ligipääs privaatvõtmele ja paroolifraasile. Et muuta võti kindlalt kasutuskõlbmatuks, tuleb see tühistada. Selleks lisatakse võtmele spetsiaalne tühistamisallkiri.

Tühistamisallkiri salvestatakse see eraldi faili, mille võib hiljem importida võtmerõngasse, millega see lisatakse võtmele ja muudetakse viimane kasutuskõlbmatuks. Palun pane tähele, et allkirja importimisel võtmesse ei ole parool nõutav. Seepärast tuleks tühistamisallkiri salvestada turvalisse, reeglina võtmepaarist erinevasse kohta. Soovitatav on salvestada see arvutist eraldi, näiteks kopeerida välisele salvestile (USB-pulk või midagi muud) või lausa trükkida.

Kleopatra ei paku võimalust luua niisugust tühistamisallkirja, kuid seda võib teha KDE rakendusega KGpg, valides menüükäsu **Võtmed** → **Tühista võti** ning soovi korral importides otsekohe tühistamisallkirja oma võtmerõngasse.

Teine viis tühistamissertifikaati genereerida on kasutada GPG-d otse käsureal: **`gpg --output tühistamis_sertifikaat.asc --gen-revoke sinu_võti`**. Argument *`sinu_võti`* peab määrama võtme: see võib olla su primaarse võtmepaari võtme ID või mis tahes osa sinu võtmepaari tuvastavast kasutaja ID-st.

Peatükk 3

Menüükirjed

3.1 Menüü Fail

Fail → Uus sertifikaat... (Ctrl+N)

Loob uue võtmepaari (avalik ja privaatne) ja võimaldab saata avaliku võtme signeerimiseks sertifitseerimiskeskusele (SK). Sealt saadetakse sertifikaat sulle tagasi või salvestatakse LDAP serveris, kust saad selle alla tõmmata, et siis oma e-kirju signeerida ja krüptida.

Sellist tegutsemisviisi nimetatakse 'detsentraliseeritud võtmetekitamiseks', sest kõik võtmed loovad kasutajad ise. Kleopatra (ja GpgSM) ei toeta otseselt 'tsentraliseeritud võtmetekitamist', kuid sa võid käsuga **Fail → Impordi sertifikaadid... (Ctrl+I)** importida avaliku/salajase võtmekimbu, mille said SK-lt PKCS#12 vormingus.

Fail → Sertifikaadi otsing serveris... (Ctrl+Shift+I)

Otsib ja impordib sertifikaadid sertifikaadiserveritest kohalikku võtmekasti. Täpsemalt kõneleb Sektsioon 2.2.
Selleks peavad olema seadistatud võtmeserverid. Täpsemalt kõneleb Sektsioon 5.1.

Fail → Impordi sertifikaadid... (Ctrl+I)

Impordib sertifikaadid ja/või salajased võtmed failist kohalikku võtmekasti. Täpsemalt kõneleb Sektsioon 2.2.
Sertifikaadifaili vorming peab olema mõistetav taustaprogrammile GpgSM/GPG. Täpsemat infot vaata GpgSM ja GPG manuaalist.

Fail → Ekspordi sertifikaadid... (Ctrl+E)

Salvestab valitud sertifikaadid faili.
Eksporditavale failile valitud failinime laiend määrab ära faili vormingu.

- OpenPGP sertifikaatide korral annavad `gpg` ja `pgp` tulemuseks binaarfaili, `asc` aga ASCII vormingus faili.
- S/MIME sertifikaatide korral annab `der` tulemuseks DER-kodeeringus faili, `pem` aga ASCII vormingus faili.

Kui valitud pole just mitut sertifikaati, pakub Kleopatra eksportfaili nimeks `fingerprint.{asc,pem}`.
Seda funktsiooni saab kasutada ainult siis, kui valitud on vähemalt üks sertifikaat.

> MÄRKUS
> See ekspordib ainult avaliku võtme isegi juhul, kui saada on salajane võti. Salajase võtme salvestamiseks faili kasuta käsku **Fail → Ekspordi salajased võtmed...** .

Fail → Ekspordi salajased võtmed...

Salvestab salajase võtme faili.

Vali avanevas dialoogis, kas soovid luua binaarfaili või ASCII vormingus eksportfaili (**ASCII armor**). Seejärel klõpsa kataloogiikoonile paremal pool tekstikasti **Väljundfail** ning vali eksportfaili kataloog ja nimi. S/MIME salajaste võtmete eksportimisel saab valida ka **paroolifraasi kodeeringu**. Täpsemalt vaata arutelu `--p12-charset kodeeringu` üle GpgSM manuaalis.
Seda funktsiooni saab kasutada ainult siis, kui valitud on üks sertifikaat ning saadaval on selle sertifikaadi salajane võti.

> HOIATUS
> Seda võimalust läheb haruharva vaja ja kui läheb, peaks ikkagi väga ettevaatlik olema. Salajase võtme migreerimiseks tuleb muu hulgas valida teisaldamiseks sobiv andmekandja ning viis, kuidas võtmeinfo vanalt masinalt turvaliselt kustutada.

Fail → Ekspordi sertifikaadid serverisse... (Ctrl+Shift+E)

Avaldab valitud sertifikaadid võtmeserveris (ainult OpenPGP puhul).

Sertifikaat saadetakse sertifikaadiserverisse, mis on OpenPGP puhul seadistatud (vt Šektsioon 5.1), vastasel juhul serverisse `keys.gnupg.net`.

Seda funktsiooni saab kasutada ainult juhul, kui valitud on vähemalt üks OpenPGP (aga mitte S/MIME) sertifikaat.

> MÄRKUS
> Kui OpenPGP sertifikaadid on eksporditud avalikku kataloogiserverisse, on neid peaaegu võimatu taas eemaldada. Enne oma sertifikaadi eksportimist avalikku kataloogiserverisse kontrolli, et oleksid loonud tühistamissertifikaadi, millega saad sertifikaadi vajaduse korral hiljem tühistada.

> MÄRKUS
> Enamik avalikke OpenPGP sertifikaadiservereid sünkroonib omavahel sertifikaate, nii et pole erilist mõtet saata neid enam kui ühte serverisse.
> Võib juhtuda, et otsing sertifikaadiserveris ei anna tulemusi, kuigi oled oma sertifikaadi just äsja sinna saatnud. Põhjuseks on see, et enamik avalikke võtmeserveri aadresse kasutab DNS-i roteerimist koormuse tasakaalustamiseks eri masinate vahel. Need masinad sünkroonivad oma andmeid, aga tavaliselt toimub see umbes kord ööpäevas.

Fail → Krüpti failid lahti/verifitseeri failid...

Krüptib failid lahti ja/või kontrollib failide allkirju.

Fail → Allkirjasta/krüpti failid...

Allkirjastab ja/või krüptib faile.

Fail → Sulge (Ctrl+W)

Sulgeb Kleopatra peaakna. Selle saab taastada süsteemisalve ikoonist.

Fail → Välju (Ctrl+Q)

Sulgeb Kleopatra.

3.2 Menüü Vaade

Vaade → Näita uuesti (F5)

Uuendab sertifikaatide loendit.
Selle funktsiooni kasutamine ei ole enamasti vajalik, sest Kleopatra jälgib failisüsteemi muudatusi ning värskendab vajaduse korral automaatselt sertifikaatide nimekirja.

Vaade → Peata tegevus (Esc)

Peatab kõik ootel toimingud, nt. otsingu, võtmete nimekirja laadimise või allalaadimise.

Seda funktsiooni saab kasutada ainult siis, kui parajasti on käsil mõni toiming.

> MÄRKUS
> Taustaprogrammi piirangute tõttu toimingud mõnikord hanguvad, nii et see funktsioon ei suuda nende tegevust otsekohe või üldse lõpetada.
> Sellistel juhtudel on ainuke lahendus maha tappa SCDaemon, DirMngr, GpgSM ja GPG protsessid (just sellises järjekorras) operatsioonisüsteemi tööriistade abil (**top**, Task-Manager jne.), kuni toiming pole enam tõkestatud.

Vaade → Sertifikaadi üksikasjad

Näitab parajasti valitud sertifikaadi üksikasju.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks sertifikaat.

Seda käsku saab kasutada ka vahetult loendis oleval kirjel topeltklõpsu tehes.

Vaade → Hierarhiline sertifikaatide nimekiri

Lülitab sertifikaatide loendi hierarhilist ja ühetaolist vaaterežiimi.

Hierarhilises režiimis korraldatakse sertifikaadid väljaandja ja subjekti suhete järgi, mis võimaldab ühe pilguga näha, millisesse sertifikaadihierarhiasse mingi sertifikaat kuulub, kuid sertifikaati ennast on esmapilgul raskem leida (kuigi selleks saab mõistagi kasutada otsinguriba).

Ühetaolises režiimis näidatakse kõiki sertifikaate mittehierarhiliselt, tähestiku järgi järjestatuna. Nii on iga sertifikaati lihtne üles leida, kuid samas ei ole alati kohe selge, milline on selle juursertifikaat.

Selle abil saab lülitada hierarhilist režiimi antud kaardil, s.t igal kaardil on oma hierarhiaolek. Nii võib sul eri kaartidel olla korraga avatud nii hierarhiline kui ka mittehierarhiline nimekiri.

> MÄRKUS
> Hierarhiline esitus on praegu võimalik ainult S/MIME sertifikaatide puhul. Arendajad ei ole jõudnud üksmeelele, kuidas oleks õige esitada hierarhiliselt OpenPGP sertifikaate (põhimõtteliselt käib vaidlus selle üle, kas 'eellane = allkirjastaja' või 'eellane = allkirjastatu').

Vaade → Ava kõik (Ctrl+.)

Avab kõik sertifikaadiloendi elemendid, st. muudab kõik elemendid nähtavaks.

See on hierarhilise võtmeloendi vaikeolek.

Iga elementi võib avada või sulgeda mõistagi ka käsitsi.

Seda funktsiooni saab kasutada ainult siis, kui valitud on käsk **Vaade → Hierarhiline sertifikaatide nimekiri**.

Vaade → Sulge kõik (Ctrl+,)

Sulgeb kõik sertifikaadiloendid elemendid, st. peidab kõik, välja arvatud tipptaseme elemendid.

Iga elementi võib avada või sulgeda mõistagi ka käsitsi.

Seda funktsiooni saab kasutada ainult siis, kui valitud on käsk **Vaade → Hierarhiline sertifikaatide nimekiri**.

3.3 Menüü Sertifikaadid

Sertifikaadid → Muuda omaniku usaldusväärsust...

Võimaldab muuta valitud OpenPGP sertifikaadi omaniku usaldusväärsust.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks OpenPGP sertifikaat.

Sertifikaadid → Usalda juursertifikaati

Tähistab selle (S/MIME) juursertifikaadi kui usaldusväärse.

Mõneti on see S/MIME juursertifikaatide korral sama, mis **Sertifikaadid → Muuda omaniku usaldusväärsust...** . Valida saab siiski ainult— OpenPGP mõisteid kasutades—'täieliku' usaldamise ja 'mitte kunagi usaldamise' vahel.

> MÄRKUS
> Taustaprogramm (GpgAgent) küsib juursertifikaadi importimise ajal, kas usaldada importi-tud juursertifikaati. Siiski peab see funktsioon olema taustaprogrammi seadistuses konkreetselt sisse lülitatud (`allow-mark-trusted` failis `gpg-agent.conf` või kas **GnuPGšüsteem → GPG agent → Juursertifikaadid märgitakse usaldusväärseks** või **S/MIME kontrollimine → Juursertifikaadid märgitakse usaldusväärseks** seadistustedialoogis peatükk 5).
> Selle funktsiooni sisselülitamine taustaprogrammis võib tuua kaasa PinEntry hüpikdialoogide avanemise väga ebasobival ajal (nt. allkirju verifitseerides) ning seeläbi tõkestada kirjade töötlemise. Sel põhjusel, aga ka seepärast, et soovitatav on omada võimalust *umbusaldada* usaldusväärset juursertifikaati kunagi tulevikus, võimaldab Kleopatra usaldusväärsust käsitsi määrata.

> HOIATUS
> Et taustaprogramm seda funktsiooni ei toeta, peab Kleopatra suhtlema otse GpgSM usaldusväärsuse andmebaasiga (`trustlist.txt`). Selle funktsiooni kasutamisel kontrolli, et käimas poleks ükski muu krüptotoiming, mis võiks põrkuda Kleopatraga kokku andmebaasi muutmise käigus.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks S/MIME juursertifikaat ja see ei ole veel usaldusväärne.

Selle tagasivõtmiseks kasuta käsku **Sertifikaadid → Ära usalda juursertifikaati** .

Sertifikaadid → Ära usalda juursertifikaati

Tähistab selle (S/MIME) juursertifikaadi kui mitteusaldusväärse.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks S/MIME juursertifikaat ja see on usaldusväärne.
Kasutatakse käsu **Sertifikaadid → Usalda juursertifikaati** tühistamiseks; vaata lähemalt selle käsu kirjeldust.

Sertifikaadid → Sertifitseeri sertifikaat...

Võimaldab sertifitseerida teist OpenPGP sertifikaati.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks OpenPGP sertifikaat.

Sertifikaadid → Muuda aegumisaega...

Võimaldab muuta OpenPGP sertifikaadi aegumistähtaega.

Selle abil saab pikendada oma OpenPGP sertifikaatide kehtivusaega, nii et ei ole vaja luua uut sertifikaati ega määrata neile piiramatut kehtivusaega ('ei aegu mitte kunagi').

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks OpenPGP sertifikaat ning saadaval on selle sertifikaadi salajane võti.

Sertifikaadid → Muuda paroolifraasi...

Võimaldab muuta oma salajase võtme paroolifraasi.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks sertifikaat ja saadaval on selle salajane võti. See nõuab üsna uut taustaprogrammi, sest me oleme muutnud teostust, eelistades GPG ja GpgSM otsese väljakutsumise asemel GpgME-põhist lahendust.

> MÄRKUS
> Turbekaalutlustel pärib PinEntry nii vana kui ka uut paroolifraasi eri protsessina. Sõltuvalt sinu platvormist ja PinEntry konkreetse versiooni kvaliteedist sellel platvormil võib juhtuda, et PinEntry aken ilmub taustal. Nii et kui valid selle ja midagi ei juhtu, uuri igaks juhuks tegumiriba - äkki on PinEntry aken avatud, aga ei ole lihtsalt näha.

Sertifikaadid → Lisa kasutaja ID...

Võimaldab lisada oma OpenPGP sertifikaadile uue kasutaja ID.

Selle abil saab lisada olemasolevale sertifikaadile uusi identiteete, mitte ei pea looma uusi võtmepaare. OpenPGP kasutaja ID on järgmise kujuga:

```
Pärisnimi (Kommentaar) <E-posti aadress>
```

Ilmuvas dialoogis palub Kleopatra kõiki kolme parameetrit (*pärisnimi*, *kommentaar* ja *e-posti aadress*) eraldi ning näitab tulemust eelvaatlusena.

> MÄRKUS
> Need parameetrid alluvad samasuguste administraatori piirangutele nagu uute sertifikaatide puhul. Täpsemalt kõneleb Sektsioon 2.3 ja Sektsioon 6.1.

Seda funktsiooni saab kasutada ainult siis, kui valitud on üks OpenPGP sertifikaat ning saadaval on selle sertifikaadi salajane võti.

Sertifikaadid → Kustuta (Del)

Kustutab valitud sertifikaadid kohalikust võtmerõngast.

Kasuta seda tarvitamata võtmete eemaldamiseks oma kohalikust võtmekastist. Siiski arvesta, et kuna sertifikaadid on tavaliselt lisatud signeeritud e-kirjadele, võib kirja kontrollimisel selle käsuga eemaldatud võti taas kohalikku võtmekasti sattuda. Seepärast on ilmselt parem seda käsku võimalikult vähe kasutada. Kui sertifikaadid silme eest kirjuks löövad, kasuta tasakaalu tagasisaamiseks otsinguriba või menüükäsku **Vaade → Hierarhiline sertifikaatide nimekiri**.

> HOIATUS
> Ülaltoodul on üks erand. Kui kustutad mõne omaenda sertifikaadi, kustutad koos sellega ka salajase võtme. See tähendab, et sa ei ole enam võimeline lugema varasemaid sõnumeid, mis on sulle saadetud selle sertifikaadiga krüptides, kui sul pole just sellest tehtud varukoopiat. Kleopatra hoiatab, kui kavatsed kustutada salajast võtit.

S/MIME sertifikaatide hierarhilise iseloomu tõttu kustutatakse juhul, kui kustutad S/MIME väljaandja sertifikaadi (SK sertifikaadi), ka kogu ahel.[1]

Loomulikult saab seda funktsiooni kasutada ainult siis, kui valitud on vähemalt üks sertifikaat.

Sertifikaadid → Tee sertifikaadi tõmmis

Näitab kogu teavet, mida GpgSM omab valitud (S/MIME) sertifikaadi kohta.

Väljundi üksikasjade kohta vaata täpsemalt võtme `--dump-key võti` kirjeldus GpgSM manuaalis.

[1] See sarnaneb failisüsteemile: kui kustutad kataloogi, kustutad ka kõik selles leiduvad failid ja (alam)kataloogid.

3.4 Menüü Tööriistad

Tööriistad → GnuPG logi näitaja...

Käivitab KWatchGnuPG ehk tööriista GnuPG rakenduse silumisväljundi näitamiseks. Kui allkirjastamine, krüptimine või kontrollimine arusaamatul põhjusel peatub, võib selle abil leida, mis on lahti.

See funktsioon pole saadaval Windowsis, sest sel platvormil pole taustaprogrammi vastavad mehhanismid lihtsalt teostatud.

Tööriistad → Värskenda OpenPGP sertifikaate

Värskendab kõiki OpenPGP sertifikaate, käivitades käsu

```
gpg --refresh-keys
```

Käsu eduka täitmise järel kajastab sinu kohalik võtmehoidla viimaseid OpenPGP sertifikaatide kehtivust puudutavaid muudatusi.

Vaata mõningate ohtude kohta märkust **Tööriistad → Värskenda X.509 sertifikaate** juures.

Tööriistad → Värskenda X.509 sertifikaate

Värskendab kõiki S/MIME sertifikaate, käivitades käsu

```
gpgsm -k --with-validation --force-crl-refresh --enable-crl-checks
```

Käsu eduka täitmise järel kajastab sinu kohalik võtmehoidla viimaseid S/MIME sertifikaatide kehtivust puudutavaid muudatusi.

> MÄRKUS
> X.509 või OpenPGP sertifikaatide värskendamine tähendab kõigi sertifikaatide ja CRL-ide allalaadimist kontrollimaks, kas neid ei ole vahepeal tühistatud.
> See võib seada tõsise koormuse alla nii sinu kui ka teiste inimeste võrguühenduse ning võtta aega isegi üle mitme tunni sõltuvalt sinu võrguühendusest ja kontrollitavate sertifikaatide arvust.

Tööriistad → Impordi CRL failist...

Võimaldab käsitsi importida CRL-id failist.

Tavaliselt tegeleb sertifikaatide tühistamise loenditega (CRL-id) läbipaistvalt taustaprogramm, aga mõnikord on kasulik importida CRL käsitsi oma kohalikku CRL-puhvrisse.

> MÄRKUS
> Et CRL-i import toimiks, peab tööriist DirMngr asuma otsinguteel (`PATH`). Kui menüü ei ole kasutatav, tuleks võtta ühendus süsteemiadministraatoriga ja paluda tal paigaldada DirMngr.

Tööriistad → Puhasta CRL vahemälu

Puhastab GpgSM CRL puhvri.

Tõenäoliselt ei ole seda siiski kunagi vaja ette võtta. Selle asemel võib CRL puhvri uuendamise peale sundida kõiki sertifikaate ja käsku **Tööriistad → Värskenda X.509 sertifikaate** valides.

Tööriistad → CRL vahemälu

Näitab GpgSM CRL puhvri üksikasjalikku sisu.

3.5 Menüü Seadistused

Kleopatra kasutab tavapärast KDE **seadistuste**menüüd, mida kirjeldab KDE põhialuste käsiraamat, kuid sel on siiski üks lisakirje:

Seadistused → **Soorita enesetest**

Sooritab rea eneseteste ja näitab nende tulemust.

Tegemist on samade testidega, mis sooritatakse vaikimisi rakenduse käivitamisel. Kui oled käivitusaegsed enesetestid keelanud, saab neid siin taas sisse lülitada.

3.6 Menüü Aken

Menüü **Aken** võimaldab hallata kaarte. Selle menüü abil saab kaarte ümber nimetada, lisada uusi kaarte, kloonida aktiivse kaardi, sulgeda aktiivse kaardi ning liigutada aktiivse kaardi vasakule või paremale.

Klõpsates hiire parema nupuga kaardi sakile, avaneb kontekstimenüü, kus leiab samad toimingud.

3.7 Menüü Abi

Kleopatra kasutab tavapärast KDE **abi**menüüd, mida kirjeldab KDE põhialuste käsiraamat.

Peatükk 4

Käsurea võtmete seletused

Siin on ära toodud ainult Kleopatra spetsiifilised võtmed. Nagu KDE rakendustes ikka, saab võtmete täieliku loendi käsuga **`kleopatra --help`**.

`--uiserver-socket` ***`argument`***
: Sokli asukoht, mida UI server jälgib

`--daemon`
: Ainult UI serveri käivitamine, peaaken peidetakse

`-p --openpgp`
: OpenPGP kasutamine järgmiseks toiminguks

`-c --cms`
: CMS-i (X.509, S/MIME) kasutamine järgmiseks toiminguks

`-i --import-certificate`
: Määrab faili või URL -i, kust importida sertifikaadid (või salajased võtmed).
See on samane menüükäsuga **Fail → Impordi sertifikaadid... (Ctrl+I)** .

`-e --encrypt`
: Failide krüptimine

`-s --sign`
: Failide allkirjastamine

`-E --encrypt-sign`
: Failide krüptimine ja/või allkirjastamine. Sama, mis `--sign-encrypt`, ära seda kasuta.

`-d --decrypt`
: Failide lahtikrüptimine

`-V --verify`
: Faili/allkirja verifitseerimine

`-D --decrypt-verify`
: Failide lahtikrüptimine ja/või verifitseerimine

Peatükk 5

Kleopatra seadistamine

Kleopatra seadistustedialoogi saab avada menüükäsuga **Seadistused** → **Kleopatra seadistamine...**
Järgnevalt kirjeldame dialoogi kõiki kaarte.

5.1 Kataloogiteenuste seadistamine

Siin saab seadistada, milliseid LDAP servereid kasutada S/MIME sertifikaatide otsimisel ja milliseid võtmeservereid kasutada OpenPGP sertifikaatide otsimisel.

> MÄRKUS
> See on lihtsalt kasutajasõbralikum versioon seadistustest, mida pakub Sektsioon 5.5. Kõike, mida saab seadistada siin, saab seadistada ka seal.

> MÄRKUS PUHVERSERVERI SEADISTUSTE KOHTA
> Puhverserverit saab seadistada nii HTTP kui ka LDAP puhul dialoogis Sektsioon 5.4, aga seda ainult GpgSM korral. GPG korral tuleb GPG võtmeserveri võtmete keerukuse ja selle tõttu, et GpgConf neid korralikult ei toeta, praegu muuta käsitsi seadistusfaili `gpg.conf`. Täpsemalt kõneleb sellest GPG manuaal. Kleopatra arvestab nende seadistustega, kuid ei võimalda neid veel graafilises kasutajaliideses muuta.

Kataloogiteenuste tabel näitab, millised serverid on parajasti seadistatud. Topeltklõps mõnel tabeli lahtril lubab muuta olemasolemate serverikirjete parameetreid.

Tabeli veergude tähendus on järgmine:

Skeem

Määrab võrguprotokolli, mida kasutatakse ligipääsuks serverile. Levinumad skeemid on **ldap** (ja selle SSL-turbega sugulane **ldaps**) LDAP serverite jaoks (tavaline protokoll S/MIME korral ning ainuke, mida GpgSM toetab) ning **hkp** ehk Horowotzi võtmeserveri protokoll, tänapäeval tavaliselt HTTP võtmeserveri protokoll ehk HTTP-põhine protokoll, mida toetavad sisuliselt kõik avalikud OpenPGP võtmeserverid.

Toetatud skeemide kohta vaata täpsemat teavet GPG ja GpgSM manuaalist.

Serveri nimi

Serveri domeeninimi, nt. `keys.gnupg.net`.

Serveri port

Võrguport, mida server jälgib.

See muutub automaatselt vaikimisi pordiks, kui muudad **Skeem**, kui selleks pole just algusest peale määratud mingi mittestandardne port. Kui oled muutnud vaikeporti ja ei saa seda enam tagasi, püüa määrata **Skeem** väärtuseks **`http`** ning **Serveri port** väärtuseks **`80`** (vaikeväärtused HTTP korral) ning siis vali see siin.

Baas DN

Baas DN (ainult LDAP ja LDAPS korral) ehk LDAP hierarhia alus, millest kõike arvama hakatakse. Sageli nimetatakse seda ka 'otsingujuureks' (ingl search root) või 'otsingubaasiks' (ingl search base).

Tavaliselt on see umbes selline: **`c=de,o=Foo`**, ning see antakse LDAP URL-i osana.

Kasutajanimi

Kasutajanimi, kui seda on vaja serverisse logimiseks.

See veerg on näha ainult siis, kui märgitud on valik **Kasutaja ja parooliteabe näitamine** (tabeli all).

Parool

Parool, kui seda on vaja serverisse logimiseks.

See veerg on näha ainult siis, kui märgitud on valik **Kasutaja ja parooliteabe näitamine** (tabeli all).

X.509

Märgi veerg, kui kirjet tuleb kasutada X.509 (S/MIME) sertifikaadi otsingus.

Ainult LDAP (ja LDAPS) serverid on toetatud S/MIME korral.

OpenPGP

Märgi veerg, kui kirjet tuleb kasutada OpenPGP sertifikaadi otsingus.

S/MIME (X.509) servereid võib seadistada nii palju, kui süda lustib, aga OpenPGP servereid tohib korraga olla ainult üks. Graafiline kasutajaliides ei lasegi viimaseid rohkem seadistada.

Uue serveri lisamiseks klõpsa nupule **Uus**. See kloonib valitud kirje, kui oled mõne valinud, või lisab vaikimisi OpenPGP serveri. Seejärel saab määrata järgmised omadused: **Serveri nimi**, **Serveri port**, **Baas DN** ning tavaliselt ka **Parool** ja **Kasutajanimi**, kuigi viimaseid kahte läheb vaja ainult siis, kui server nõuab autentimist.

Otseseks X.509 sertifikaadi kirje lisamiseks vali **Uus** → **X.509** ning **Uus** → **OpenPGP**, kui soovid lisada OpenPGP sertifikaadi kirje.

Serveri eemaldamiseks otsimisloendist vali server ja klõpsa nupule **Kustuta**.

LDAP aegumise, st. maksimaalse aja määramiseks, mille kestel taustaprogramm ootab serverilt vastust, kasuta vastavat välja **LDAP aegumine (min:sek)**.

Kui mõnel serveritest on suur andmebaas, nii et isegi mõistlik otsing, nagu näiteks **`Smith`**, ületab võimalusega **maksimaalne päringu vastuste arv** määratu, siis võiks mainitud läve tõsta. Seda, kas oled piiranguni jõudnud või mitte, saab teada imelihtsalt - kui see otsingu ajal peaks juhtuma, ilmub dialoog, mis annab teada, et tulemusi on seetõttu kärbitud.

> MÄRKUS
> Mõned serverid võivad ka omalt poolt kehtestada päringu vastuste limiidi. Sellisel juhul ei anna limiidi suurendamine sinu poolt mõistagi mingit tulemust.

5.2 Välimuse seadistamine

5.2.1 Kohtspikrite seadistamine

Kleopatra võib sertifikaatide põhiloendis näidata sertifikaadi üksikasju kohtspikrina. Näidatav teave on sama, mida näeb dialoogi **Sertifikaadi üksikasjad** kaardil **Ülevaade**. Kohtspikrite puhul võib siiski määrata, et nad näitaksid ka oluliselt vähem teavet.

> MÄRKUS
> **Võtme-ID**-d näidatakse *alati*. Nii tagatakse, et eri sertifikaatide kohtspikrid tõepoolest ka erineksid (see on eriti oluline siis, kui on valitud **Kehtivuse näitamine**).

Üksteisest sõltumatult saab lasta näidata või peita järgmist teavet:

Kehtivuse näitamine
: Näitab teavet sertifikaadi kehtivuse kohta: aktiivne olek, väljaandja DN (ainult S/MIME korral), kehtivusaeg (kui see on määratud), kasutamise lipud.

  Näide:

```
This certificate is currently valid.
Issuer:            CN=Test-ZS 7,O=Intevation GmbH,C=DE
Validity:          from 25.08.2009 10:42 through 19.10.2010 10:42
Certificate usage: Signing EMails and Files, Encrypting EMails and ↩
    Files
Key-ID:            DC9D9E43
```

Omaniku teabe näitamine
: Näitab teavet sertifikaadi omaniku kohta: subjekti DN (ainult S/MIME korral), kasutaja-ID-d (kaasa arvatud e-posti aadressid) ja omaniku usaldusväärsus (ainult OpenPGP korral).

  OpenPGP näide:

```
User-ID:           Gpg4winUserA <gpg4winusera@test.hq>
Key-ID:            C6BF6664
Ownertrust:        ultimate
```

  S/MIME example:

```
Subject:           CN=Gpg4winTestuserA,OU=Testlab,O=Gpg4win Project,C= ↩
    DE
a.k.a.:            Gpg4winUserA@test.hq
Key-ID:            DC9D9E43
```

Näita tehnilisi üksikasju
: Näitab sertifikaadi tehnilist teavet: seerianumber (ainult S/MIME korral), tüüp, sõrmejälg ja salvestamise asukoht.

  Näide:

```
Serial Number:     27
Certificate type:  1,024-bit RSA (secret certificate available)
Key-ID:            DC9D9E43
Fingerprint:       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Stored:            on this computer
```

5.2.2 Sertifikaadikategooriate seadistamine

Kleopatra võimaldab muuta võtmete välimuse loendivaates just selliseks, nagu sa tahad. Muuta on võimalik nii esiplaani (teksti) ja tausta värvi kui ka fonti, samuti lasta näidata väikest ikooni.

Igale nimekirjas asuvale **sertifikaadi kategooria**le on omistatud värvid, ikoon (ei pruugi olla) ja font, millega kategooriasse kuuluvaid võtmeid näidatakse. Kategoorialoend on ühtlasi siin määratud seadistuste eelvaatluseks. Administraator või tema õigustes isik võib kategooriad vabalt määrata ja/või muuta - vaata Sektsioon 6.2 (peatükk 6).

Kategooria ikooni muutmiseks vali loendis kategooria ja klõpsa nupule **Määra ikoon...** Ilmub KDE tavapärane ikooni valimise dialoog, kus saad valida mõnes KDE kogus leiduva või kohandatud ikooni.

Ikooni eemaldamiseks klõpsa nupule **Vaikevälimus**.

Kategooria teksti (esiplaani) värvi muutmiseks vali loendis kategooria ja klõpsa nupule **Määra teksti värv...** Ilmub KDE tavapärane värvi valimise dialoog, kus saad valida olemasoleva või luua uue värvi.

Taustavärvi valimine käib samamoodi, ainult et klõpsata tuleb nupule **Määra taustavärv...**

Fonti saab muuta kahel põhimõtteliselt erineval viisil:

1. Muutes standardset fonti, mida kasutatakse KDE kõigis loendivaadetes.
2. Kasutades kohandatud fonti.

Esimese võimaluse eeliseks on see, et font järgib stiili, mille valid kogu KDE jaoks. Teine võimalus annab aga sulle kasutatava fondi üle igakülgse kontrolli. Nii et valik on sinu.

Muudetud standardse fondi kasutamiseks vali loendis kategooria ning märgi või eemalda märge fondikastidest **kaldkiri**, **rasvane** ja/või **läbikriipsutatud**. Tulemust võid kohe näha kategooria loendis.

Kohandatud fondi kasutamiseks klõpsa nupule **Määra font...** Ilmub tavapärane KDE fondi valimise dialoog, kus saab valida uue fondi.

> MÄRKUS
> Pane tähele, et ülaltoodud kastidega saab muuta ka kohandatud fondi välimust.

Kui soovid standardset fonti tagasi, klõpsa nupule **Vaikevälimus**.

5.2.3 DN atribuutide järjekorra määramine

Kuigi DN-id on hierarhilised, ei ole üksikute komponentide (neid nimetatakse suhtelisteks ehk relatiivseteks DN-ideks (RDN või ka DN atribuudid). Seepärast on järjekord, milles atribuute näidatakse, isikliku eelistuse või firma reeglite otsustada, mistõttu Kleopatra võimaldab seda ka muuta.

> MÄRKUS
> Siinsed seadistused rakenduvad mitte ainult Kleopatrale, vaid kõigile Kleopatra tehnoloogiat kasutavatele rakendustele. Käsiraamatu kirjutamise ajal olid neiks KMail, KDE aadressiraamat ja mõistagi Kleopatra ise.

Seadistustekaart koosneb kahest loendist, millest üks on teadaolevate atribuutide jaoks (**Saadaolevad atribuudid**), teises aga seisab **praegune atribuutide järjekord**.

Mõlemad nimekirjad koosnevad kirjetest, mis sisaldavad nii atribuudi lühivormi (nt. **CN**) kui ka pikka vormi (**Ühine nimi**).

Saadaolevad atribuudid on alati tähestikulises järjekorras, **Praegune atribuutide järjekord** aga kajastab olemasolevat DN atribuutide järjekorda, kus esimesena toodud atribuuti ka esimesena näidatakse.

Näidatakse ainult atribuute, mida toob ära **Praegune atribuutide järjekord**, ülejäänud on vaikimisi peidetud.

Kui aga kohanäitaja **_X_** (**Kõik muud**) seisab 'praeguste' loendis, lisatakse kõik loendist puuduvad atribuudid (sõltumata sellest, kas nad on teada või mitte) **_X_** asukohta nende algupärases suhtelises järjekorras.

Toome selgituseks näite:

Kui DN on

> O=KDE, C=US, CN=Dave Devel, X-BAR=foo, OU=Kleopatra, X-FOO=bar,

atribuutide vaikimisi järjekord 'CN, L, _X_, OU, O, C' annab tulemuseks järgmiselt vormindatud DN:

> CN=Dave Devel, X-BAR=foo, X-FOO=bar, OU=Kleopatra, O=KDE, C=US

'CN, L, OU, O, C' aga

> CN=Dave Devel, OU=Kleopatra, O=KDE, C=US

Atribuudi lisamiseks näidatavate atribuutide loendisse vali see loendis **Saadaolevad atribuudid** ning klõpsa nupule **Lisa praegusse atribuutide järjekorda**.

Atribuudi eemaldamisks näidatavate atribuutide loendis vali see loendis **Praegune atribuutide järjekord** ja klõpsa nupule **Eemalda praegusest atribuutide järjekorras**.

Atribuudi liigutamiseks algusse/lõppu vali see loendis **Praegune atribuutide järjekord** ja klõpsa nupule **Liiguta esimeseks** (**Liiguta viimaseks**).

Atribuudi liigutamiseks ühe positsiooni võrra üles/alla vali see loendis **Praegune atribuutide järjekord** ja klõpsa nupule **Liiguta üles** (**Liiguta alla**).

5.3 Krüptotoimingute seadistamine

5.3.1 E-posti toimingute seadistamine

Siin saab seadistada mõningaid Kleopatra UiServeri e-posti toimingute aspekte. Praegu saab määrata ainult seda, kas kirjade allkirjastamisel ja krüptimisel kasutada 'kiirrežiimi' või mitte.

Kui 'kiirrežiim' on lubatud, ei näidata kirjade allkirjastamisel või krüptimisel dialoogi, kui ei teki just konflikt, mis vajab käsitsi lahendamist.

5.3.2 Failitoimingute seadistamine

Siin saab seadistada mõningaid Kleopatra UiServeri failitoimingute aspekte. Praegu saab valida ainult kontrollsumma programmi, mida kasutakse käsu **CHECKSUM_CREATE_FILES** korral.

Valikuga **Kasutatav kontrollsummaprogramm** saab määrata, millist seadistatud kontrollsummaprogrammi tuleb kasutada kontrollsummafailide loomisel.

Kontrollsummade verifitseerimisel leitakse vajalik programm automaatselt leitud kontrollsummafailide nimede põhjal.

MÄRKUS
Administraator ja kogenud kasutaja võivad igakülgselt määrata, millised kontrollsummaprogrammid on üldse Kleopatrale kättesaadavad niinimetatud 'kontrollsummadefinitsioonide' abil seadistusfailis. Täpsemalt kõneleb sellest Sektsioon 6.4 peatükk 6is.

5.4 S/MIME valideerimise omaduste seadistamine

Siin saab seadistada mõningaid S/MIME sertifikaatide kontrollimise aspekte.

MÄRKUS
See on lihtsalt kasutajasõbralikum versioon seadistustest, mida pakub Sektsioon 5.5. Kõike, mida saab seadistada siin, saab seadistada ka seal, välja arvatud **Sertifikaadi kehtivuse kontrollimine iga *N* tunni järel**, mis on ainuomane Kleopatrale.

Valikud on järgmised:

5.4.1 Sertifikaatide kontrollimise intervalli seadistamine

Sertifikaadi kehtivuse kontrollimine iga *N* tunni järel

Selle valikuga lülitatakse sisse sertifikaadi kehtivuse kontrollimine kindla ajavahemiku järel. Siin saab ka määrata kontrollimise intervalli tundides. See on sama toimega nagu **Vaade → Näita uuesti (F5)** , samas ei pakuta kindla ajavahemiku tagant kontrollimist ei **Tööriistad → Värskenda OpenPGP sertifikaate** ega **Tööriistad → Värskenda X.509 sertifikaate** korral.

MÄRKUS
Kontrollimine võetakse kindlasti ette siis, kui muutuvad olulised failid asukohas `~/.gnupg`. Nagu **Tööriistad → Värskenda OpenPGP sertifikaate** ja **Tööriistad → Värskenda X.509 sertifikaate** , mõjutab ka see valik ainult sertifikaadi kehtivuse välistegureid.

5.4.2 Kontrollimise meetodi seadistamine

Sertifikaatide kontroll CRL-ide vahendusel

Selle valimisel kontrollitakse S/MIME sertifikaate sertifikaatide tühistamise nimekirju (CRL) kasutades.

Alternatiivsest sertifikaadi kehtivuse meetodist kõneleb **Sertifikaatide kontroll võrgus (OCSP)**.

Sertifikaatide kontroll võrgus (OCSP)

Selle valimisel kontrollitakse S/MIME sertifikaate võrgus interneti sertifikaatide staatuse protokolli (OCSP) kasutades.

HOIATUS
Selle meetodi valimisel saadetakse päring SK serverisse enam-vähem iga kord, kui saadad või saad krüptitud sõnumi, mis teoreetiliselt võimaldab sertifikaadi väljaandjal jälgida, kellega sa vahetad näiteks kirju.

Meetodi kasutamiseks tuleb **OCSP-serveri URL** all sisestada OCSP keskuse URL.

Traditsioonilisemakst sertifikaadi kehtivuse meetodist kõneleb **Sertifikaatide kontroll võrgus (OCSP)** (see ei lekita teavet selle kohta, kellega kirju vahetad).

OCSP-serveri URL

Anna siin sertifikaatide kontrollimise serveri aadress (OCSP keskus). URL-i alguses seisab tavaliselt `http://` .

OCSP-serveri signatuur

Siin saab valida sertifikaadi, millega OCSP server allkirjastab oma vastused.

Sertifikaatide teenuse URL-i ignoreerimine

Iga S/MIME sertifikaat sisaldab tavaliselt oma väljaandja OCSP serveri URL-i (**Sertifikaadid → Tee sertifikaadi tõmmis** näitab, kas konkreetne sertifikaat sisaldab seda või mitte).

Selle märkimisel eirab GpgSM neid URL-e ning kasutab ainult ülal määratuid.

Seda võib kasutada näiteks kogu ettevõttele kehtiva OCSP puhverserveri kehtestamiseks.

5.4.3 Kontrollimise valikute seadistamine

Sertifikaadi reegleid ei kontrollita

Vaikimisi kasutab GpgSM faili `~/.gnupg/policies.txt` kontrollimaks, kas sertifikaadi reegel on lubatud. Selle valimisel aga reegleid ei kontrollita.

CRL-i ei kontrollita kunagi

Sisselülitamisel ei kasutata S/MIME sertifikaatide kontrollimiseks kunagi sertifikaatide tühistamise loendeid (CRL).

Juursertifikaadid märgitakse usaldusväärseks

Kui see on märgitud ning imporditakse SK juursertifikaati, palutakse sul kinnitada selle sõrmejälg ning määrata, kas pidada seda juursertifikaati usaldusväärseks või mitte.

Juursertifikaat peab olema usaldusväärne, enne kui saab usaldada sertifikaate, mida see sertifitseerib, kuid juursertifikaatide kergemeelne usaldamine ja nende paigutamine oma sertifikaadihoidlasse võib õõnestada süsteemi turvalisust.

> MÄRKUS
> Selle funktsiooni sisselülitamine taustaprogrammis võib tuua kaasa PinEntry hüpikdialoogide avanemise väga ebasobival ajal (nt. allkirju verifitseerides) ning seeläbi tõkestada kirjade töötlemise. Sel põhjusel, aga ka seepärast, et soovitatav on omada võimalust *umbusaldada* usaldusväärset juursertifikaati kunagi tulevikus, võimaldab Kleopatra usaldusväärsust käsitsi määrata, mida võimaldavad **Sertifikaadid → Usalda juursertifikaati** ja **Sertifikaadid → Ära usalda juursertifikaati** .
> See seadistus ei mõjuta Kleopatra funktsiooni.

Tõmmatakse puuduvad väljaandja sertifikaadid

Selle märkimisel tõmmatakse vajadusel puuduvad väljaandja sertifikaadid (kasutusel nii CRL-ide kui OCSP korral;).

5.4.4 HTTP päringute valikute seadistamine

HTTP päringuid ei sooritata

Keelab täielikult HTTP kasutamise S/MIME korral.

HTTP sertifikaatide CRL jagamispunkte ignoreeritakse

CRL-i asukoha otsimisel sisaldab testitav sertifikaat tavaliselt niinimetatud 'CRL-i jagamispunkti' (DP) kirjet, mis kujutab endast vajalikule CRL-ile viivat URL-ide rida. Kasutatakse esimesena leitud jagamispunkti.

Selle valikuga jäetakse sobiva DP otsimisel kõrvale kõik HTTP-skeemi kasutavad kirjed.

Süsteemi HTTP puhverserveri kasutamine

Selle valimisel kasutatakse paremal asuvat HTTP puhverserveri väärtust (mille määrab keskkonnamuutuja `http_proxy`) kõigi HTTP päringute korral.

HTTP päringuteks kasutatakse järgmist puhverserverit

Kui süsteemset puhverserverit pole määratud või pead GpgSM jaoks kasutama mõnda teist puhverserverit, saab siin määrata selle asukoha.

Seda kasutatakse kõigi HTTP päringute jaoks S/MIME puhul.

Süntaks on **`masin:port`**, nt. **`minupuhverserver.kuskil.ee:3128`**.

5.4.5 LDAP päringute valikute seadistamine

LDAP päringuid ei sooritata

LDAP täielik keelamine S/MIME puhul.

LDAP sertifikaatide CRL jagamispunktide eiramine

CRL-i asukoha otsimisel sisaldab testitav sertifikaat tavaliselt niinimetatud ˝CRL-i jagamispunkti˝ (DP) kirjet, mis kujutab endast vajalikule CRL-ile viivat URL-ide rida. Kasutatakse esimesena leitud jagamispunkti.

Selle valikuga jäetakse sobiva DP otsimisel kõrvale kõik LDAP-skeemi kasutavad kirjed.

LDAP päringute primaarne masin

Kui sisestada siia LDAP server, siis suunduvad kõik LDAP päringud esmalt sinna. Konkreetsemalt tühistab see seadistus kõik *`masina`* ja *`pordi`* määrangud LDAP URL-is ning neid kasutatakse ka siis, kui *`masin`* ja *`port`* on URL-is üldse ära jäetud.

Teisi LDAP servereid kasutatakse ainult siis, kui ühendus 'puhverserveriga' katkeb. Süntaks on **`masin`** või **`masin:port`**. Kui *`port`* on ära jäetud, kasutatakse porti 389 (standardne LDAP port).

5.5 GnuPG süsteemi seadistamine

Dialoogi see osa täidetakse automaatselt käsu **gpgconf `--list-components`** väljundiga ning iga *`komponendi`* puhul, mida mainitud käsk tagastab, käsu **gpgconf `--list-options` *`komponent`*** väljundiga.

> MÄRKUS
> Neist kõige tulusamad võtmed on topeldatud Kleopatra seadistustedialoogi teistel lehtedel. Sektsioon 5.1 ja Sektsioon 5.4 on kaks dialoogilehte, mis sisaldavad mõningaid selle dialoogiosa valikuid.

Dialoogi selle osa täpne sisu sõltub paigaldatud GnuPG taustaprogrammi täpsest versioonist ning mõnikord ka platvormist, millel seda kasutad. Sestap käsitletakse siin dialoogi üldisi võimalusi, sealhulgas GpgConfi võtmete vasteid Kleopatra graafilise kasutajaliidese valikute seas.

GpgConf tagastab seadistusteabe paljude komponentide kohta. Iga komponendi sees on üksikvõtmed ühendatud gruppidesse.

Kleopatra näitab üht kaarti iga komponendi kohta, mida GpgConf tagastab, ning gruppe alustavad rõhtsad read, mis näitavad grupi nime sel kujul, nagu seda andis teada GpgConf.

Igal GpgConfi võtmel on tüüp. Kui jätta välja mõned hästi tuntud võtmed, mida Kleopatra toetab spetsiaalsete juhtelementidega, et võimaldada kasutajale nende paremat ärakasutamist, on GpgConfi tüüpide ja Kleopatra juhtelementide seosed järgmised:

GpgConfi tüüp	**Kleopatra valik**	
	loendi korral	**mitteloendi korral**
`none`	Kerimiskast ('arvu'semantika)	Märkekast
`string`	N/A	Tekstikast
`int32`	Tekstikast (vormindamata)	Kerimiskast:
`uint32`		
`pathname`	N/A	spetsiaalne valik
`ldap server`	spetsiaalne valik	N/A
`key fingerprint`	N/A	
`pub key`		
`sec key`		
`alias list`		

Tabel 5.1: GpgConfi tüüpide ja graafilise kasutajaliidese valikute seosed

Täpsemalt, mida ja kuidas saab siin seadistada, kõneleb GpgConfi manuaal.

Peatükk 6

Administraatori juhised

Administraatori juhistes kirjeldame Kleopatra kohandamise neid võimalusi, mida saab teha ainult konfiguratsioonifaile muutes, mitte aga graafiliselt, GUI abil.

Me eeldame, et lugeja tunneb KDE rakenduste konfigureerimise tehnoloogiat, sealhulgas paigutust, asukohti failisüsteemis ja KDE konfiguratsioonifailide kaskaadiseadmist ning KIOSKI raamistikku.

6.1 Sertifikaadi loomise nõustaja kohandamine

6.1.1 DN väljade kohandamine

Kleopatra lubab kohandada välju, mida kasutajal on lubatud täita oma sertifikaadi loomisel.

Loo süsteemses failis `kleopatrarc` grupp `CertificateCreationWizard`. Kui soovid kohandada atribuutide järjekorda või lubada ainult teatud elementide näitamist, loo võti `DNAttributeOrder`. Argumendiks võivad olla `CN`,`SN`,`GN`,`L`,`T`,`OU`,`O`,`PC`,`C`,`SP`,`DC`,`BC`,`EMAIL`. Kui soovid täita väljad eelnevalt määratud väärtustega, pane vajalikud väärtsed kirja kujul atribuut=väärtus. Kui soovid, et atribuut oleks nõutav, lisa selle järele hüüumärk (nt. `CN!`,`L`,`OU`,`O!`,`C!`,`EMAIL!`, mis muide esineb ka vaikekonfiguratsioonis).

KIOSKi režiimi muutujate `$e` kasutamine lubab hankida väärtused keskkonnamuutujatest või konkreetsest skriptist või binaarfailist. Kui soovid lisaks keelata mõne välja muutmise, kasuta muutujat `$i`. Kui soovid keelata nupu **Lisa minu aadress** kasutamise, määra `ShowSetWhoAmI` väärtuseks 'väär' (false).

> VIHJE
> KDE KIOSKi raamistiku iseloomu tõttu muudab muutmist vältiva lipu `$i` pruukimine kasutajal selle tühistamise võimatuks. Sellel on oma kindel mõte. Muutujaid `$i` ja `$e` saab kasutada mis tahes muu KDE rakendustest tarvitatava võtmega.

Järgnev näide selgitab kohandamisvõimalusi:

```
[CertificateCreationWizard]
;Keelab isiklike andmete kopeerimise aadressiraamatust, ei luba kohalikku ↩
    tühistamist
ShowSetWhoAmI[$i]=false

;määrab kasutaja nimeks $USER
```

```
CN[$e]=$USER

;määrab firma nimeks "Minu firma", keelab muutmise
OU[$i]=Minu firma

;määrab osakonna nime hankimise skripti väärtusest
O[$ei]=$(lookup_dept_from_ip)

; määrab riigiks EE, kuid lubab kasutajal seda muuta
C=EE
```

6.1.2 Võtmetüüpide piiramine, mida kasutajal on lubatud luua

Kleopatra võimaldab samuti piirata seda, milliseid sertifikaaditüüpe on kasutajal lubatud luua. Pane siiski tähele, et neist piirangutest saab hõlpsasti mööda, kui luua vajalik tüüp käsureal.

6.1.2.1 Avaliku võtme algoritmid

Kasutatava avaliku võtme algoritmi piiramiseks lisa faili `kleopatrarc` sektsiooni `CertificateCreationWizard` seadistusvõti `PGPKeyType` (ja `CMSKeyType`, kuid CMS-i puhul on nagunii toetatud ainult RSA).

Lubatud väärtused on `RSA` RSA võtmete, `DAS` DSA (ainult allkirjastamiseks mõeldud) võtmete ja `DSA+ELG` DSA (ainult allkirjastamiseks mõeldud) võtmete puhul koos krüptimiseks mõeldud Elgamali alamvõtmega.

Vaikeväärtuse annab GpgConf või kasutatakse `RSA`-d, kui GpgConf ei anna vaikeväärtust.

6.1.2.2 Avaliku võtme suurus

Avaliku algoritmi võtmete suuruse piiramiseks lisa faili `kleopatrarc` sektsiooni `CertificateCreationWizard` seadistusvõti `<ALG>VõtmeSuurused` (kus *ALG* võib olla `RSA`, `DSA` või `ELG`), mis sisaldab komadega eraldatult võtmesuuruste (bittides) loendit. Vaikeväärtuse võib tähistada võtmesuurusele sidekriipsu (-) ette lisades.

```
RSAKeySizes = 1536,-2048,3072
```

Ülaltoodu piirab RSA võtmete suurust. lubades neid luua 1536-, 2048- ja 3072-bitisena, kusjuures vaikeväärtus on 2048.

Lisaks suurusele endale võib määrata ka iga suuruse nimetuse. Selleks määra lihtsalt seadistusvõti `ALGVõtmeSuuruseNimed` ning anna komadega eraldatult nimede loend.

```
RSAKeySizeLabels = weak,normal,strong
```

Koos eelmisega annab ülaltoodu valikuks järgmised võimalused:

```
weak (1536 bits)
             normal (2048 bits)
             strong (3072 bits)
```

Vaikeväärtused on järgmised:

```
RSAKeySizes = 1536,-2048,3072,4096
             RSAKeySizeLabels =
             DSAKeySizes = -1024,2048
             DSAKeySizeLabels = v1,v2
             ELGKeySizes = 1536,-2048,3072,4096
```

6.2 Võtme kategooriate loomine ja muutmine

Kleopatra võimaldab kasutajal seadistada võtme välimust, võttes aluseks **võtme kategooriate** kontseptsiooni. **Võtme kategooriaid** kasutatakse ka sertifikaatide nimekirja filtreerimiseks. Käesolevas osas kirjeldame, kuidas muuta olemasolevaid kategooriad ja kuidas lisada uusi.

Võtme kategooria tuvastamisel püüab Kleopatra leida selle vastet võtmefiltrite jadas, mis on kindlaks määratud failis `libkleopatrarc`. Esimene leitud sobivus määrabki kategooria, tuginedes allpool selgitatavale *spetsiifilisuse* kontseptsioonile.

Võtmefiltrid on kindlaks määratud grupis `Key Filter #n`, kus *n* on arv alates `0`.

Ainsad kohustuslikud võtmed grupis `Key Filter #n` on `Name`, mis sisaldab kategooria nime kujul, nagu seda näitab seadistustedialoog, ja `id`, mida kasutatakse filtri viitena teistes seadistussektsioonides (näiteks `View #n`).

Tabel 6.1 toob ära kõik võtmed, mis defineerivad kategooriasse kuuluvate võtmete näitamise omadusi (st. nende võtmete, mida saab kohandada seadistustedialoogis) ning Tabel 6.2 toob ära kõik võtmed, mis defineerivad kriteeriumid, millega filtrites võtmeid võrreldakse.

Konfiguratsioonivõti	Tüüp	Kirjeldus
`background-color`	värv	Kasutatav taustavärv. Kui puudub, on vaikeväärtuseks globaalselt loenditele määratud taustavärv.
`foreground-color`	värv	Kasutatav esiplaani värv. Kui puudub, on vaikeväärtuseks globaalselt loenditele määratud esiplaani värv.
`font`	font	Kasutatav kohandatud font. See skaleeritakse loenditele määratud suurusele, samuti rakendatakse kõiki määratud fondiatribuute (vaata allpool).
`font-bold`	tõeväärtus	Kui on `true` ja `font` on määramata, kasutatakse loendite vaikefonti rasvasel kujul (kui võimalik). Seda ignoreeritakse, kui `font` on määratud.
`font-italic`	tõeväärtus	Nagu `font-bold`, ainult et kaldkiri rasvase kirja asemel.
`font-strikeout`	tõeväärtus	Kui on `true`, tõmmatakse fondi keskelt joon läbi. Rakendatakse ka siis, kui `font` on määratud.
`icon`	tekst	Esimeses veerus näidatava ikooni nimi. Pole veel teostatud.

Tabel 6.1: Võtmefiltri näitamise omadusi määravad konfiguratsioonivõtmed

Konfiguratsioonivõti	**Tüüp**	**Määramise korral filter sobib, kui...**
`is-revoked`	tõeväärtus	võti on tühistatud.
`match-context`	context[1]	kontekst, milles antud filter vastab.
`is-expired`	tõeväärtus	võti on aegunud.
`is-disabled`	tõeväärtus	võti on keelatud (märgitud mittekasutatavaks) kasutaja poolt. Ignoreeritakse S/MIME võtmete puhul.
`is-root-certificate`	tõeväärtus	võti on juursertifikaat. Ignoreeritakse OpenPGP võtmete puhul.
`can-encrypt`	tõeväärtus	võtit saab kasutada krüptimiseks.
`can-sign`	tõeväärtus	võtit saab kasutada krüptimiseks.
`can-certify`	tõeväärtus	võtit saab kasutada muude võtmete signeerimiseks (sertifitseerimiseks).
`can-authenticate`	tõeväärtus	võtit saab kasutada autentimiseks (nt.TLS kliendi sertifikaadina).
`is-qualified`	tõeväärtus	võtit saab kasutada kvalifitseeritud allkirja loomiseks (nagu seda määratleb Saksamaa digitaalallkirja seadus).
`is-cardkey`	tõeväärtus	võtme sisu on salvestatud kiipkaardile, mitte arvutisse.
`has-secret-key`	tõeväärtus	saada on selle võtmepaari salajane võti.
`is-openpgp-key`	tõeväärtus	võti on OpenPGP võti (`true`) või S/MIME võti (`false`).
`was-validated`	tõeväärtus	võti on tunnistatud kehtivaks.

[1] Kontekst on loend järgmiste lubatud väärtustega: `appearance`, `filtering` ja `any`.

`prefiks-ownertrust`	usaldusväärsus[2]	võtmel on täpselt (*`prefiks`* = `is`), pole üldse (*`prefiks`* = `is-not`), on vähemalt (*`prefiks`* = `is-at-least`) või on maksimaalselt (*`prefiks`* = `is-at-most`) konfiguratsioonivõtme väärtusega antud usaldusväärsus. Kui ühes grupis esineb enam kui üks `prefiks-ownertrust` võtit (erinevad *`prefiks`*id), on käitumine defineerimata.
`prefiks-validity`	usaldusväärsus	Sarnane võtmega `prefiks-ownertrust`, kuid omaniku usaldusväärsuse asemel kontrollitakse võtme usaldusväärsust.

Tabel 6.2: Võtmefiltri filtri kriteeriume määravad konfiguratsioonivõtmed

> **MÄRKUS**
> Mõningaid huvitavamaid kriteeriume, näiteks `is-revoked` või `is-expired`, saab kasutada ainult *kontrollitud* võtmete puhul, mistõttu ka ainult kontrollitud võtmete korral kontrollitakse tühistamist ja aegumist, kuigi sa võid muidugi sellisest kontrollist ka loobuda.

Lisaks eespool loetletud seadistusvõtmetele võib võtmefiltril olla ka `id` ja `match-contexts`.

Filtri `id` abil, milleks vaikimisi on filtri seadistustegrupi nimi, kui midagi muud pole antud, võib viidata võtmefiltrile mujal seadistuses, nt. Kleopatra vaateseadistuses. `id` jääb Kleopatra poolt interpreteeritamata, nii et selleks võib kasutada mis tahes stringi tingimusel, et see oleks unikaalne.

`match-contexts` piirab filtri tegevusvälja. Praegu on defineeritud kaks konteksti: `appearance` on kasutusel vaate värvi- ja fondiomaduste määramisel, `filtering` aga sertifikaadi valikuliseks kaasamiseks või välistamiseks vaates. `any` võimaldab arvestada kõiki defineeritud kontekste ja see ongi vaikeväärtus, kui `match-contexts` on andmata või mingit muud konteksti pole. See tagab, et ükski võtmefilter ei muutu 'surnuks', st. ei ole kontekstita, mida sellele rakendada.

Kirje vorming on kohatäitjate loend, mida eristavad mittesõna-märgid. Iga kohatäitja ette võib vajaduse korral lisada hüüumärgi (`!`), mis tähendab eitust. Kohatäitjad rakenduvad järjekorras kontekstide sisemisele nimekirjale, mis esialgu on tühi. Sellest saab kõige paremini aru näite varal: `any !appearance` on sama, mis `filtering`, ning `appearance !appearance` annab tulemuseks tühja kogu, nagu ka `!any`. Kuid kahe viimase asemele pannakse seesmiselt `any`, sest nad ei paku üldse mingit konteksti.

Üldiselt ei kontrollita vastavust kriteeriumidele, mida ei ole määratud (st. mille seadistuskirjet pole antud). Kui kriteerium on antud, seda ka kontrollitakse ja see peab vastama täielikult filtrile, et see tunnistatakse sobivaks, st. kriteeriumid on seotud loogilise tehtega JA (AND).

Igal filtril on oma 'spetsiifilisus', mida kasutatakse kõigi sobivate filtrite järjestamiseks. Spetsiifilisem filter asetseb vähem spetsiifilise ees. Kui kahel filtril on ühesugune spetsiifilisus, seisab

[2] Usaldusväärsus on (järjekorrastatud) loend järgmiste võimalike väärtustega: `tundmatu`, `defineerimata`, `mitte kunagi`, `kesine`, `täielik`, `ülim`. Vaata lähemalt GPG ja GpgSM manuaale.

eespool see, mis on eespool seadistustefailis. Filtri spetsiifilisus on seotud temas leiduvate kriteeriumide arvuga.

Example 6.1 Võtmefiltrite näited

Kõigi aegunud, kuid mittetühistatud juursertifikaatide kontrollimiseks sobib selline võtmefilter:

```
[Key Filter #n]
Name=expired, but not revoked
was-validated=true
is-expired=true
is-revoked=false
is-root-certificate=true
; ( specificity 4 )
```

Kõigi keelatud OpenPGP võtmete kontrollimiseks (pole veel Kleopatra poolt toetatud), mille usaldusväärsus on vähemalt 'kesine':

```
[Key Filter #n]
Name=disabled OpenPGP keys with marginal or better ownertrust
is-openpgp=true
is-disabled=true
is-at-least-ownertrust=marginal
; ( specificity 3 )
```

6.3 Pakkimisprogrammide seadistamine kasutamiseks failide allkirjastamisel/krüptimisel

Kleopatra võimaldab administraatoril (ja kogenud kasutajal) seadistada pakkimisprogrammide nimekirja, mida saab kasutada failide allkirjastamise/krüptimise dialoogis.

Iga pakkimisprogramm on failis `libkleopatrarc` defineeritud omaette grupina `Archive Definition #n`, milles peavad olema järgmised võtmed:

`extensions`
: Komadega eraldatud failinime laiendite loend, mis tavaliselt osutavad arhiivifaili vormingule.

`id`
: Seda pakkimisprogrammi seesmiselt tuvastav unikaalne ID. Kahtluse korral kasuta käsu nime.

`Name` (tõlgitud)
: Kasutajale nähtav pakkimisprogrammi nimi, nagu seda näeb failide allkirjastamise/krüptimise dialoogi vastavas rippmenüüs.

`pack-command`
: Tegelik käsk, millega failid pakitakse. See võib olla milline tahes, ainult et see ei tohi nõuda käivitamiseks shelli. Teostusfaili otsitakse keskkonnamuutuja `PATH` määratluse põhjal, kui sa ei anna just faili absoluutset asukohta. Toetatud on ka tsiteerimine, nagu shelli puhul.

```
pack-command="/opt/ZIP v2.32/bin/zip" -r -
```

MÄRKUS

Et längkriips (\) on KDE seadistusfailides paomärk, tuleb neid asukohanimes kasutada topelt:

```
pack-command=C:\\Programs\\GNU\\tar\\gtar.exe ...
```

Käsu enda puhul (erinevalt argumentidest) võib siiski kasutada kõigil platvormidel ka asukohaeraldajana lihtsalt kaldkriipsu (/):

```
pack-command=C:/Programs/GNU/tar/gtar.exe ...
```

Argumentides see toetatud ei ole, sest enamik Windows® programme kasutab kaldkriipsu võtmete jaoks. Näiteks alltoodu ei toimi, sest `C:/myarchivescript.bat` on **cmd.exe** argument ning argumentides ei teisendata / , vaid ainult käskudes:

```
pack-command=cmd.exe C:/myarchivescript.bat
```

Niisiis tuleb see kirjutada hoopis nii:

```
pack-command=cmd.exe C:\\myarchivescript.bat
```

6.3.1 Sisendi failinime edastamine käsule `pack-command`

Failinimesid saab pakkimiskäsule edastada kolmel viisil. Kõigi nende puhul kasutab `pack-command` konkreetset süntaksit:

1. Käsureaargumentidena.

   Näide (tar):

   ```
   pack-command=tar cf -
   ```

   Näide (zip):

   ```
   pack-command=zip -r - %f
   ```

   Sel juhul edastatakse failinimed käsureal samamoodi nagu ehtsat käsurida kasutades. Kleopatra ei kasuta käsu käivitamiseks shelli. Seepärast on see turvaline viis failinimede edastamiseks, aga mõnel platvormil võivad tekkida probleemid käsurea pikkuse piirangutega. Kui on antud, asendatakse literaal `%f` arhiveeritavate failide nimedega. Vastasel juhul lisatakse failinimed käsureale. Niisiis võib ülaltoodud zip-näite kirjutada ka nii:

   ```
   pack-command=zip -r -
   ```

2. Standardsisendi kaudu reavahetustega eraldatult: ette tuleb lisada `|`.

   Näide (GNU-tar):

   ```
   pack-command=|gtar cf - -T-
   ```

   Näide (ZIP):

   ```
   pack-command=|zip -@ -
   ```

   Sel juhul edastatakse failinimed pakkimisprogrammile standardsisendist (stdin), üks iga rea kohta. Nii välditakse probleeme platvormidel, kus lubatud käsureaargumentide arv on väga piiratud ning reavahetuste kasutamine ajab asja üldse nurja.

> **MÄRKUS**
> Kleopatra toetab praegu reavahetusmärgina ainult LF, mitte CRLF. Sõltuvalt kasutajate tagasisidest võib see tulevikus muutuda.

3. Standardsisendi kaudu NUL-baitidega eraldatult: ette tuleb lisada `0|`.
   Näide (GNU-tar):

```
pack-command=0|gtar cf - -T- --null
```

   See on sama, nagu eespool, ainult et failinimede eraldamiseks kasutatakse nullbaite. Et nullbaidid on failinimedes keelatud, on see kõige töökindlam failinimede edastamise viis, aga seda ei toeta sugugi kõik pakkimisprogrammid.

6.4 Kontrollsummaprogrammide seadistamine kasutamiseks kontrollsummade loomisel/kontrollimisel

Kleopatra võimaldab administraatoril (ja kogenud kasutajal) seadistada kontrollsummaprogrammide loendit, mille seast kasutaja saab valida seadistustedialoogis ja mida Kleopatra on võimeline automaatselt tuvastama, kui tal palutakse kontrollida antud faili kontrollsummat.

> **MÄRKUS**
> Kleopatrale sobimiseks peab kontrollsummaprogrammi väljund (nii kirjutatud kontrollsummafail kui ka standardväljundi (stdout) väljund kontrollsumma kontrollimisel) olema ühilduv GNU programmidega **md5sum** ja **sha1sum**.
> Konkreetsemalt peab kontrollsummafail koosnema ridadest, millel kõigil on järgmine vorming:

```
KONTROLLSUMMA ' ' ( ' ' | '*' ) FAILINIMI
```

> kus *KONTROLLSUMMA* koosneb ainult 16nd-koodis märkidest. Kui *FAILINIMI* sisaldab reavahetuse märki, peab see välja nägema selline:

```
\KONTROLLSUMMA ' ' ( ' ' | '*' ) VARJESTATUD-FAILINIMI
```

> kus *VARJESTATUD-FAILINIMI* on failinimi, milles reavahetuste asemel on `\n` ning längkriipsud on topeldatud (\↦\\).
> Samamoodi peab `verify-command` väljund olema kujul

```
FAILINIMI ( ': OK' | ': FAILED' )
```

> eraldatuna reavahetustega. Reavahetusi ja teisi märke väljundis *ei varjestata*.[a]
>
> [a] Jah, nende programmide kirjutamisel ei arvestatud graafiliste kasutajaliidestega ning Kleopatra ei suudaks korrektselt parsida patoloogilisi failinimesid, mis sisaldavad ˝:ÕK˝ ning reavahetusi.

Iga kontrollsummaprogramm on failis `libkleopatrarc` defineeritud omaette grupina `Checksum Definition #n`, milles peavad olema järgmised võtmed:

`file-patterns`

Regulaaravaldiste loend, mis kirjeldab, milliseid faile tuleks selle kontrollsummaprogrammi puhul pidada kontrollsummafailideks. Süntaks on samasugune nagu KDE seadistusfailides stringiloendite puhul.

> **MÄRKUS**
> Et regulaaravaldised sisaldavad tavaliselt längkriipse, peab neid seadistusfailis hoolikalt varjestama. Soovitatav on kasutada mõnda seadistusfailide redigeerimise tööriista.

Vastavalt platvormile tõlgendatakse mustreid kas tõstutundlikult või -tundetult.

`output-file`

Antud kontrollsummaprogrammi tüüpilise väljundi failinimi (peab sobima loomulikult sellega, mida annab `file-patterns`). Seda kasutab Kleopatra väljundi failinimena antud tüüpi kontrollsummafaile luues.

`id`

Seda kontrollsummaprogrammi seesmiselt tuvastav unikaalne ID. Kahtluse korral kasuta käsu nime.

`Name` (tõlgitud)

Kasutajale nähtav kontrollsummaprogrammi nimi, nagu seda näeb Kleopatra seadistustedialoogi rippmenüüs.

`create-command`

Tegelik käsk kontrollsummafailide loomiseks. Süntaks, piirangud ja argumentide edastamise viisid on samad, mida kirjeldati käsu `pack-command` korral osas Sektsioon 6.3.

`verify-command`

Sama, mis `create-command`, kuid kontrollsumma kontrollimiseks.

Toome siin täieliku näite:

```
[Checksum Definition #1]
          file-patterns=sha1sum.txt
          output-file=sha1sum.txt
          id=sha1sum-gnu
          Name=sha1sum (GNU)
          Name[de]=sha1sum (GNU)
          ...
          create-command=sha1sum -- %f
          verify-command=sha1sum -c -- %f
```

Peatükk 7

Autorid ja litsents

KAASAUTORID

- Marc Mutz mutz@kde.org
- David Faure faure@kde.org
- Steffen Hansen hansen@kde.org
- Matthias Kalle Dalheimer kalle@kde.org
- Jesper Pedersen blackie@kde.org
- Daniel Molkentin molkentin@kde.org

Tõlge eesti keelde: Marek Laanebald@starman.ee