Handbok Kleopatra

Marc Mutz
Utvecklare: David Faure
Utvecklare: Steffen Hansen
Utvecklare: Matthias Kalle Dalheimer
Utvecklare: Jesper Pedersen
Utvecklare: Daniel Molkentin
Översättare: Stefan Asserhäll
Handbok Kleopatra
Innehåll

1 Inledning 7

2 Huvudfunktioner 8
   2.1 Visa den lokala nyckellådan ................................. 8
   2.2 Söka efter och importera certifikat ............................ 8
   2.3 Skapa nya nyckelpar ........................................... 9
      2.3.1 Återkalla en nyckel ..................................... 10

3 Menyreferens 11
   3.1 Menyn Arkiv .................................................. 11
   3.2 Menyn Visa .................................................... 13
   3.3 Menyn Certifikat .............................................. 14
   3.4 Menyn Verktyg ............................................... 16
   3.5 Menyn Inställningar .......................................... 17
   3.6 Menyn Fönster ............................................... 17
   3.7 Menyn Hjälp .................................................. 17

4 Referens till kommandoradsväljare 18

5 Anpassa Kleopatra 19
   5.1 Anpassa Katalogtjänster ..................................... 19
   5.2 Anpassning av utseende ...................................... 21
      5.2.1 Anpassning av Verktygstips ............................. 21
      5.2.2 Anpassning av Certifikatkategorier .................... 22
      5.2.3 Anpassning av DN-egenskapsordning .................. 22
   5.3 Anpassning av krypteringsåtgärder .......................... 23
      5.3.1 Anpassning av E-poståtgärder .......................... 23
      5.3.2 Anpassning av Filåtgärder .............................. 24
   5.4 Anpassning av aspekter rörande S/MIME-validering ........ 24
      5.4.1 Anpassning av intervall mellan certifikatkontroller 24
      5.4.2 Anpassning av valideringsmetod ......................... 24
      5.4.3 Anpassning av valideringsalternativ ................... 25
      5.4.4 Anpassning av alternativ för HTTP-begäran .......... 26
      5.4.5 Anpassning av alternativ för LDAP-begäran .......... 26
   5.5 Anpassning av GnuPG-systemet ............................. 27
6 Administrationsguide

6.1 Anpassning av guiden för att skapa certifikat ........................................ 28
  6.1.1 Anpassa domännamnsfälten ......................................................... 28
  6.1.2 Begränsa typer av nycklar som en användare tillåts skapa .......... 29
    6.1.2.1 Algoritmer för öppna nycklar ............................................... 29
    6.1.2.2 Storlek på öppen nyckel ..................................................... 29
  6.2 Skapa och redigera nyckelkategorier ............................................... 30

6.3 Anpassa arkiveringsverktyg för användning med signerade och krypterade filer . 33
  6.3.1 Skicka indatafilnamn till pack-command ..................................... 34

6.4 Anpassa checksummeringsprogram för användning när checksummor skapas och verifieras ................................................................. 35

7 Tack till och licens .................................................................................. 37
Tabeller

5.1  Avbildning från typer i GpgConf till grafiska kontroller . . . . . . . . . . . . . . . 27

6.1  Inställningsalternativ för att definiera visningsegenskaper i nyckelfilter . . . . . . . 31
6.2  Inställningsalternativ för att definiera filterkriterier i nyckelfilter . . . . . . . . . 32
Sammanfattning

Kleopatra är ett verktyg för att hantera X.509- och OpenPGP-certifikat.
Kapitel 1

Inledning


NOT
Programmet är uppkallat efter Kleopatra, en berömd kvinnlig egyptisk farao som levde samtidigt som Julius Caesar, med vilken hon hade ett barn, Caesarion, dock inte erkänd som hans arvinge. Namnet valdes eftersom programmet har sitt ursprung i projektet Ägypten (Ägypten är tyska för Egypten). Kleopatra stavas också på samma sätt på tyska.
Kapitel 2

Huvudfunktioner

2.1 Visa den lokala nyckellådan

Kleopatras huvudfunktion är att visa och redigera innehållet i den lokala nyckellådan, vilket liknar konceptet i GPG med nyckelringar, även om man inte ska läsa ut för mycket ur jämförelsen.

Huvudfönstret är uppdelat i ett stort område för att lista nycklar som består av flera flikar, menyraden och sökraden längst upp, och en statusrad längst ner.

Varje rad i nyckellistan motsvarar ett certifikat, som identifieras av det så kallade Subjekt DN. DN är en förkortning som betyder ‘Distinguished Name’ (särskiljande namn), en hierarkisk identifiering som i mycket liknar en sökväg i filsystemet med en ovanlig syntax, som är avsett att unikt identifiera ett givet certifikat i hela världen.

För att vara giltiga, och sålunda användbara, måste (öppna) nycklar vara signerade av en certifikatutfärdare (CA). Signaturerna kallas certifikat, men oftast används begreppen ‘certifikat’ och ‘(öppen) nyckel’ omväxlande, och vi skiljer inte heller på dem i den här handboken, utom när det anges explicit.

Certifikatutfärdare måste i sin tur vara signerade av andra certifikatutfärdare för att vara giltiga. Det här måste förstås sluta någonstans, så certifikatutfärdare på toppnivå (rotcertifikatutfärdare) signerar sin nyckel själv (det kallas en självsignatur). Rotcertifikat måste därför tilldelas giltighet (vanligen kallad pålitlighet) för hand, dvs. efter att ha jämfört fingeravtrycket med det som finns på certifikatutfärdarens webbplats. Det görs typiskt av systemadministratören eller leverantören av en produkt som använder certifikat, men kan också göras av användaren via GpgSMs kommandoradsgränssnitt.

När du ändrar nyckellådan utan att använda Kleopatra (t.ex. genom att använda kommandoradgränssnittet i GpgSM), kan du uppdatera vyn med Visa → Visa igen (F5).

2.2 Söka efter och importera certifikat

För det mesta skaffar du nya certifikat genom att kontrollera signaturer i e-post, eftersom certifikat oftast är inbäddade i signaturerna som skapats med dem. Om du dock behöver skicka ett
brev till någon som du ännu inte har haft kontakt med, måste du hämta certifikatet från en LDAP-katalog (även om GpgSM kan göra det automatiskt), eller från en fil. Du måste också importera ditt eget certifikat efter att ha tagit emot certifikatsutfårdarens svar på din certifikatbegäran.

För att söka efter ett certifikat i en LDAP-katalog, välj Arkiv → Slå upp certifikat på server och skriv in någon text (t.ex. namnet på personen vars certifikat du vill ha) med redigeringsraden i dialogrutan Nyckelserver certifikatuppslagning, och klicka därefter på knappen Sök. Resultatet visas i nyckellistan under sökraden, där du kan markera certifikat för att titta på dem genom att klicka på knappen Detaljinformation eller ladda ner dem till den lokala nyckellådan med Importera.

Du kan ställa in listan med LDAP-servrar som ska sökas i på sidan Katalogtjänster i Kleopatras inställningsdialogruta.

Om du tog emot certifikatet som en fil, försök med Arkiv → Importera certifikat... (Ctrl+I).

GpgSM måste förstå certifikatfilens format. Se handboken för GpgSM för en lista med filformat som stöds.

Om du inte skapade ditt eget nyckelpar med GpgSM, måste du också manuellt importera den öppna nyckeln (och den hemliga nyckeln) från PKCS#12-filen du fick från certifikatsutfårdaren. Du kan göra det från kommandoraden med kleopatra --import-certificate filnamn eller inne i Kleopatra med Arkiv → Importera certifikat... (Ctrl+I), precis som du skulle göra för ‘normala’ certifikat.

2.3 Skapa nya nyckelpar

Menyalternativet Arkiv → Nytt certifikat... (Ctrl+N) startar Guide för att skapa nyckelpar, som leder dig genom ett antal steg för att skapa en begäran om ett certifikat.

Så fort du är klar med ett steg i guiden, tryck på Nästa för att gå till nästa steg (eller Tillbaka för att kontrollera steg som redan är färdiga). Skapandet av begäran om certifikat kan avbrytas när som helst genom att trycka på knappen Avbryt.

Välj vilken typ av certifikat du vill skapa på guidens första sida:

Skapa ett personligt OpenPGP-nyckelpar

OpenPGP-nyckelpar skapas lokalt, och certifieras av dina vänner och bekanta. Det finns ingen central certifikatsutfårdare, istället skapar varje individ ett personligt pålitlighetsnät genom att certifiera andra användares nyckelpar med sitt eget certifikat.

Du måste skriva in Namn, E-post och en valfri Kommentar.

Skapa ett personligt X.509-nyckelpar och en personlig certifikatbegäran

X.509-nyckelpar skapas lokalt, men certifieras centralt av en certifikatsutfårdare (CA). En CA kan certifiera andra certifikatsutfårdare, vilket skapar en central hierarkiskt pålitlighetskedja.

Nästa steget i guiden är att skriva in din personliga data för certifikatet. Fälten som ska fyllas i är:

- Vanligt namn (CN): Ditt namn.
- Plats (L): Staden eller kommunen du bor i.
- Avdelning (OU): Enheten i organisationen där du finns (till exempel ´´Logistik´´).
- Organisation (O): Organisationen du representerer (t.ex. företaget du arbetar på).
- Landskod (C): Koden med två bokstäver för landet du bor i (till exempel “SE”).

Nästa steg i guiden är att välja om certifikatet ska lagras i en fil eller skickas direkt till certifikatsutfårdaren. Du måste ange filnamn eller e-postadress dit begäran om certifikatet ska skickas.
2.3.1 Återkalla en nyckel

Ett nyckelpar som har utgått kan återställas till användbart skick under förutsättning att du har tillgång till den privata nyckeln och lösenordsfrasen. För att göra en nyckel oanvändbar på ett tillförlitligt sätt måste den återkallas. Att återkalla görs genom att lägga till en särskild återkallelsesignature i nyckeln.


Kleopatra tillhandahåller inte en funktion för att skapa en sådan återkallelsesignatur när som helst, men du kan göra det med KDE-programmet KGpg genom att välja Nycklar → Återkalla nyckel och valfritt importera återkallelsesignaturen till din nyckelring omedelbart.

Kapitel 3

Menyreferens

3.1 Menyn Arkiv

Arkiv → Nytt certifikat... (Ctrl+N)
Det här arbetssättet kallas ‘decentraliserad nyckelframtagning’, eftersom alla nycklar skapas lokalt. Kleopatra (och GpgSM) stöder inte ‘centraliserad nyckelframtagning’ direkt, men du kan importera nyckelknippan med öppen och hemlig nyckel som du tog emot från certifikatutfärdaren med PKCS#12-format via Arkiv → Importera certifikat... (Ctrl+I).

Arkiv → Slå upp certifikat på server... (Ctrl+Skift+I)
Söker efter, och importerar certifikat från certifikatserver till den lokala nyckellådan. Se Avsnitt 2.2 för detaljinformation.
Nykellådorna måste vara installerade för att det ska fungera. Se Avsnitt 5.1 för mer information.

Arkiv → Importera certifikat... (Ctrl+I)
Importerar certifikat och/eller hemliga nycklar från filer till den lokala nyckellådan. Se Avsnitt 2.2 för detaljinformation.
Certifikatfilens format ska vara ett som kan förstås av GpgSM/GpgSM. Se manualen för GpgSM och GPG för en lista av format som stöds.

Arkiv → Exportera certifikat... (Ctrl+E)
Exportera markerade certifikat till en fil.
Filnamnsändelsen som väljs för exportfilen bestämmer exportfilens format:

- För OpenPGP-certifikat, ger gpg och pgp en binärfil, medan asc ger en ASCII-bepansrad fil.
- För S/MIME certifikat, ger der en binär, DER-kodad fil, medan pem ger en ASCII-bepansrad fil.

Om inte flera certifikat är markerade, föreslår Kleopatra fingeravtryck.{asc,pem} som exportfilnamn.
Funktionen är bara tillgänglig om ett eller flera certifikat har markerats.
NOT
Funktionen exporterar bara de öppna nycklarna, även om de hemliga nycklarna är tillgängliga.
Använd Arkiv → Exportera hemliga nycklar... för att exportera den hemliga nyckeln till en fil.

Arkiv → Exportera hemliga nycklar...
Exportera den hemliga nyckeln till en fil.
Funktionen är bara tillgänglig om exakt ett certifikat har markerats, och certifikatets hemliga nyckel är tillgänglig.

WARNING
Det bör sällan vara nödvändigt att använda funktionen, och om det är det, måste det planeras noggrant. Planering av förflyttning av en hemlig nyckel omfattar bland annat val av transportmedia, och saker borttagning av nyckeldata på den gamla datorn, samt på transportmedia.

Arkiv → Exportera certifikat till server... (Ctrl+Skift+E)
Publicera markerade certifikat på en nyckelserv (bara OpenPGP).
Certifikatet skickas till certifikatservern inställd för OpenPGP (se Avsnitt 5.1), om det finns någon, annars till keys.gnupg.net.
Funktionen är bara tillgänglig om åtminstone ett OpenPGP (och inget S/MIME) certifikat har markerats.

NOT
När OpenPGP-certifikat har exporterats till en öppen katalogserver, är det nästan omöjligt att ta bort dem igen. Innan du exporterar ditt certifikat till en öppen katalogserver, försäkra dig om att du har skapat ett återkallelsecertifikat så att du kan återkalla certifikatet om det senare behövs.

NOT

Arkiv → Avkoda och verifiera filer...
Avkodar filer och/eller verifierar signaturer för filer.

Arkiv → Signera och kryptera filer...
Signerar och/eller krypterar filer.

Arkiv → Stäng (Ctrl+W)
Stänger Kleopatras huvudfönster. Det kan återställas från ikonen i systembrickan när som helst.

Arkiv → Avsluta (Ctrl+Q)
Avslutar Kleopatra.
3.2 Menyn Visa

Visa → Visa igen (F5)
Uppdaterar certifikatlistan.
Att använda funktionen är oftast inte nödvändigt, eftersom Kleopatra övervakar filsystemet efter ändringar och automatiskt uppdaterar certifikatlistan vid behov.

Visa → Stoppa åtgärd (Esc)
Stoppar (avbryter) alla pågående åtgärder, t.ex. en sökning, nyckellistning eller en nerladning.
Funktionen är bara tillgänglig om åtminstone en åtgärd är aktiv.

NOT
På grund av begränsningar i gränssnitt, blockeras åtgärder på ett sådant sätt att den här funktionen inte kommer att kunna avbryta dem direkt, eller överhuvudtaget.
I sådana fall är det enda sättet att återställa ordringen att döda processerna SCDaemon, DirMngr, GpgSM och GPG, i den ordringen, via operativsystemets verktyg (top, aktivitetshanterare, etc.), till blockeringen av åtgärden försvinner.

Visa → Certifikatinformation
Visar detaljinformation om certifikatet som för närvarande är markerat.
Funktionen är bara tillgänglig om exakt ett certifikat har markerats.
Funktionen är också tillgänglig genom att direkt dubbelklicka på motsvarande objekt i listvyn.

Visa → Hierarkisk certifikatlista
Byter mellan hierarkiskt och enkelt läge för certifikatlistan.
I hierarkiskt läge ordnas certifikat enligt förhållandet utfärdare och subjekt, så det är enkelt att se vilken certifikathierarki som ett givet certifikat tillhör, men ett givet certifikat är svårare att hitta från början (även om du förstås kan använda sökraden).
I enkelt läge visas alla certifikat i en enkel lista, alfabetiskt sorterade. Ett givet certifikat är enkelt att hitta i detta läge, men det är inte direkt klart vilket rotcertifikat det tillhör.
Funktionen växlar hierarkiskt läge per flik, dvs. varje flik har sitt eget hierarkiska läge. Det är på detta vis så att man kan ha både en listning med enkelt och hierarkiskt läge, var och en under sin egen flik.

NOT
Hierarkisk visning är för närvarande bara implementerat för S/MIME certifikat. Utvecklarna är inte överens om det rätta sättet att visa OpenPGP certifikat hierarkiskt (i huvudsak, ’överliggande certifikat lika med det signerat av utfärdaren’ eller ’överliggande certifikat lika med det signerat av användaren’).

Visa → Expandera alla (Ctrl+.)
Expandera alla listobjekt i certifikatlistans vy, dvs. gör alla objekt synliga.
Det här är normalt när hierarkiskt läge väljes för nyckellistans.
Du kan förstås fortfarande expandera eller dra ihop varje enskild rad för sig.
Funktionen är bara tillgänglig när Visa → Hierarkisk certifikatlista är på.

Visa → Dra ihop alla (Ctrl+.)
Drar ihop alla listobjekt i certifikatlistans vy, dvs. döljer alla utom toppnivåobjekten.
Du kan förstås fortfarande expandera eller dra ihop varje enskild rad för sig.
Funktionen är bara tillgänglig när Visa → Hierarkisk certifikatlista är på.
3.3 Menyn Certifikat

Certifikat → Ändra ägarens pålitlighet...
Ändrar ägarens pålitlighet för det markerade OpenPGP certifikatet.
Funktionen är bara tillgänglig när exakt ett OpenPGP certifikat är markerat.

Certifikat → Lita på rotcertifikat
Markerar det här (S/MIME) rotcertifikatet som pålitligt.
På ett sätt är det ekvivalent med Certifikat → Ändra ägarens pålitlighet... för S/MIME rotcertifikat. Man kan dock bara välja mellan ‘fullständig’ pålitlighet och ‘lita aldrig på’, enligt terminologin i OpenPGP.

NOT
Gränssnittet frågar om det importerade rotcertifikatet ska anses pålitligt när rotcertifikatet importereras (via GpgAgent). Dock måste funktionen explicit aktiveras i gränssnittets inställning (all ow-mark-trusted i gpg-agent.conf, eller antingen GnuPG-system → GPG-agent → Tillåt klienter att markera nycklar som “pålitliga” eller S/MIME Validation → Tillåt att rotcertifikat markeras som pålitliga under kapitel 5).
Att aktivera funktionen i gränssnittet kan orsaka att dialogrutor från PinEntry dyker upp vid olämpliga tillfällen (t.ex. när signaturer verifieras), och kan på så sätt blockera behandling av brev vid frånvaro. Av den orsaken, och eftersom det är önskvärt att kunna sluta lita på ett pålitligt rotcertifikat igen, tillåter Kleopatra att pålitlighet ställs in manuellt.

WARNING
På grund av att stöd för funktionen saknas i gränssnittet, måste Kleopatra arbeta direkt med GpgSM pålitlighetsdatabas (trustlist.txt). Försäkra dig om att inga andra krypteringsåtgärder pågår som skulle kunna tävla med Kleopatra om att ändra databasen, när funktionen används.

Funktionen är bara tillgänglig om exakt ett S/MIME rotcertifikat har markerats, och certifikatet ännu inte är pålitligt.
Använd Certifikat → Lita inte på rotcertifikat för att ångra funktionen.

Certifikat → Lita inte på rotcertifikat
Markerar det här (S/MIME) certifikatet som opålitligt.
Funktionen är bara tillgänglig om exakt ett S/MIME rotcertifikat har markerats, och certifikatet för närvarande är pålitligt.
Använd för att ångra Certifikat → Lita på rotcertifikat. Se det för detaljinformation.

Certifikat → Certifiera certifikat...
Låter dig certifiera ett annat OpenPGP certifikat.
Funktionen är bara tillgänglig om exakt ett OpenPGP certifikat är markerat.

Certifikat → Ändra utgångsdatum...
Låter dig ändra ditt OpenPGP certifikats utgångsdatum.
Använd funktionen för att utöka livslängden hos dina OpenPGP certifikat, som alternativ till att antingen skapa nya, eller använda obegränsad livslängd (‘går aldrig ut’).
Funktionen är bara tillgänglig om exakt ett OpenPGP certifikat är markerat, och den hemliga nyckeln är tillgänglig för certifikatet.
Certifikat → Ändra lösenordsfras...
Låter dig ändra din hemliga nyckels lösenordsfras.

NOT
Av säkerhetsskäl efterfrågas både den gamla och den nya lösenodsfasen av PinEntry, en separat process. Beroende på plattformen du använder och kvaliteten hos implementeringen av PinEntry, kan det inträffa att PinEntry's fönster dyker upp i bakgrunden. Så om du väljer funktionen och ingenting händer, kontrollera operativsystemets aktivitetsfält ifall PinEntry's fönster är öppet i bakgrunden.

Certifikat → Lägg till användar-id...
Låter dig lägga till ett nytt användar-id till ett OpenPGP certifikat.
Använd det här för att lägga till nya identiteter i ett befintligt certifikat, som alternativ till att skapa ett nytt nyckelpar. Ett OpenPGP användar-id har följande form:

Verkligt namn (Kommentar) <E-postadress>

I dialogrutan som dyker upp när funktionen väljes, frågar Kleopatra dig om var och en av de tre parametrarna (Verkligt namn, Kommentar och E-postadress) separat, och visar resultatet i en förhandsgranskning.

NOT
Dessa parametrar lyder under samma administratörsbegränsningar som för nya certifikat. Se Avsnitt 2.3 och Avsnitt 6.1 för detaljinformation.

Funktionen är bara tillgänglig när exakt ett OpenPGP certifikat är markerat, och den hemliga nyckeln är tillgänglig för certifikatet.

Certifikat → Ta bort (Delete)
Tar bort markerade certifikat från den lokala nyckelringen.

WARNING
Kleopatra varnar dig när du försöker ta bort en hemlig nyckel.


---

1 Det är samma sak som i ett filsystem. När du tar bort en katalog, tar du också bort alla filer och kataloger i den.
Certifikat → Hämta innehåll i certifikat
Visar all information som GpgSM har om det markerade (S/MIME) certifikatet.
Se beskrivningen av --dump-key nyckel i handboken för GpgSM för detaljinformation om utmatningen.

3.4 Menyn Verktyg

Verktyg → GnuPG-loggvisning...
Startar KWatchGnuPG, ett verktyg för att visa felsökningsutmatning från GnuPG-programmen. Om signering, kryptering eller verifikation slutar fungera utan anledning, kan du kanske ta reda på varför genom att titta i loggen.
Funktionen är inte tillgänglig på Windows®, eftersom de underliggande mekanismerna inte är implementerade i den plattformens gränssnitt.

Verktyg → Uppdatera OpenPGP-certifikat
Uppdaterar alla OpenPGP certifikat genom att köra
```
gpg --refresh-keys
```
Efter att kommandot har gjorts färdigt med lyckat resultat, kommer din lokala nyckellåda motsvara de senaste ändringarna med avseende på giltighet hos OpenPGP certifikat.
Se anmärkningen under Verktyg → Uppdatera X.509-certifikat för några varningar.

Verktyg → Uppdatera X.509-certifikat
Uppdaterar alla S/MIME certifikat genom att köra
```
gpgsm -k --with-validation --force-crl-refresh --enable-crl-checks
```
Efter att kommandot har gjorts färdigt med lyckat resultat, kommer din lokala nyckellåda motsvara de senaste ändringarna med avseende på giltighet hos S/MIME certifikat.

NOT
Att uppdatera X.509- eller OpenPGP-certifikat innebär att ladda ner alla certifikat och certifikatåterkallningslistor, för att kontrollera om någon av dem återkallats under tiden.
Det kan orsaka påfrestning både på din egen och andras nätverksanslutning, och kan ta mer än en timme att göra färdigt, beroende på nätverksanslutning och antal certifikat att kontrollera.

Verktyg → Importera CRL från fil...
Låter dig manuellt importera certifikatåterkallningslistor från filer.
Normalt hanteras certifikatåterkallningslistor (CRL:er) transparent av gränssnittet, men det kan ibland vara användbart att importera en CRL manuellt till den lokala CRL-cachen.

NOT
För att CRL-import ska fungera, måste verktyget DirMngr finnas i sökvägen PATH. Om menyalternativet är inaktiverat, bör du kontakta systemadministratören och be dem installera DirMngr.

Verktyg → Rensa CRL-cache
Rensar GpgSm:s CRL-cache.
Verktyg → Rensa CRL-cache
Visar detaljinnehållet i GpgSMs CRL-cache.

3.5 Menyn Inställningar

Kleopatra har KDE:s vanliga meny Inställningar som beskrivs i KDE:s grunder, med ytterligare ett alternativ:

Inställningar → Utför självtest
Utför ett antal självtester och presenterar deras resultat.
Det här är samma uppsättning tester som normalt körs vid start. Om du inaktiverade självtester vid start, kan du aktivera dem igen här.

3.6 Menyn Fönster

Menyn Fönster låter dig hantera flikarna. Genom att använda alternativen i menyn kan du byta namn på en flik, lägga till en ny flik, duplicera nuvarande flik, stänga nuvarande flik, och flytta nuvarande flik åt vänster eller höger.
Genom att klicka med höger musknapp på en flik öppnas en sammanhangsberoende meny, där man också kan välja samma alternativ.

3.7 Menyn Hjälp

Kleopatra har KDE:s vanliga Hjälp-meny som beskrivs i KDE:s grunder.
Kapitel 4

Referens till kommandoradsväljare

Bara väljare som är specifika för Kleopatra listas här. Som med alla KDE-program, kan du få en fullständig lista med väljare genom att ge kommandot `kleopatra --help`.

```plaintext
--uiserver-socket argument
    Plats för uttaget som UI-servern lyssnar på

--daemon
    Kör bara UI-server, dölj huvudfönster

-p --openpgp
    Använd OpenPGP för följande åtgärd

-c --cms
    Använd CMS (X.509, S/MIME) för följande åtgärd

-i --import-certificate
    Anger en fil eller webbadress som ska användas för att importera certifikat (eller hemliga nycklar).
    Det här är motsvarigheten till Arkiv → Importera certifikat... (Ctrl+I) på kommandoraden.

-e --encrypt
    Kryptera fil(er)

-s --sign
    Signera fil(er)

-E --encrypt-sign
    Kryptera och/eller signera fil(er). Samma som --sign-encrypt, använd inte

-d --decrypt
    Avkoda fil(er)

-V --verify
    Verifiera fil/signatur

-D --decrypt-verify
    Avkoda och/eller verifiera fil(er)
```
Kapitel 5

Anpassa Kleopatra

Kleopatras inställningsdialogruta kan kommas åt via Inställningar → Anpassa Kleopatra...
Var och en av dess sidor beskrivs i avsnitten nedan.

5.1 Anpassa Katalogtjänster

På den här sidan kan du ställa in vilka LDAP-servrar som ska användas för sökningar efter S/MIME certifikat, och vilka nyckelservrar som ska användas för sökningar efter OpenPGP certifikat.

**NOT**

Det är helt enkelt en mer användarvänlig version av samma inställningar som också finns i Avsnitt 5.5. Allt du kan ställa in här, kan du också ställa in där.

**EN ANMÄRKNING OM PROXY-INSTÄLLNINGAR**

Proxyinställningar kan ställas in för HTTP och LDAP i Avsnitt 5.4, men bara för GpgSM. För GPG, på grund av komplexiteten hos alternativen för nyckelservrar i GPG och avsaknad av riktigt stöd för dem i GpgConf, måste man för närvarande ändra inställningsfilen gpg.conf direkt. Se handboken för GPG för detaljinformation. Kleopatra bevarar sådana inställningar, men tillåter inte ännu att de ändras i det grafiska gränssnittet.

Tabellen **Katalogtjänster** visar vilka servrar som för närvarande är inställda. Dubbelklicka på en cell i tabellen för att ändra de befintliga serverposternas parametrar.
Kolumnernas betydelse i tabellen är följande:

**Schema**

Bestämmer nätverksprotokollet som används för att komma åt servern. Ofta använda metoder omfattar ldap (och dess syskon ldaps, säkrad med SSL) för LDAP-servrar (vanligt protokoll för S/MIME, det enda som stöds av GpgSM), och hkp, Horowitz nyckelserverprotkoll, nufrödigen oftast HTTP nyckelserverprotkoll, ett HTTP-baserat protokoll som i stort sett alla öppna OpenPGP nyckelservrar stöder.
Se manualen för GPG och GpgSM för en lista av metoder som stöds.
Handbok Kleopatra

Servernamn
Serverns domännamn, t.ex. keys.gnupg.net.

Serverport
Nätverksporten som servern lyssnar på.
Det här ändras automatiskt till standardporten när man ändrar Schema, om det inte var inställt till något annat än en standardport från början. Om man ändrar standardport, och inte kan få tillbaka den, försök ställa in Schema till http och Serverport till 80 (standardvärdet för HTTP), och fortsätta därifrån.

Basdomännamn
Basdomännamnet (bara för LDAP och LDAPS), dvs. roten för LDAP-hierarkin att starta från. Den kallas ofta också ‘sökroten’ eller ‘sökbasen’.
Den ser oftast ut som c=de, o=Foo, angiven som en del av LDAP webbadressen.

Användarnamn
Användarnamnet, om något finns, att använda för att logga in på servern.
Kolumnen visas bara om alternativet Visa användare och lösenordsinformation (under tabellen) är markerat.

Lösenord
Lösenordet, om något finns, att använda för att logga in på servern.
Kolumnen visas bara om alternativet Visa användare och lösenordsinformation (under tabellen) är markerat.

X.509
Markera kolumnen om posten ska användas för X.509 (S/MIME) certifikatsökningar.
Bara LDAP- (och LDAPS)-servrar stöds för S/MIME.

OpenPGP
Markera kolumnen om posten ska användas för OpenPGP certifikatsökningar.


Klicka på knappen Ny för att lägga till en ny server. Det duplicerar den markerade posten, om det finns någon, eller infogar annars en OpenPGP standardserver. Därefter kan man ställa in Servernamn, Serverport, Basdomännamn samt de vanliga Lösenord och Användarnamn, vilka båda bara behövs om servern kräver behörighetskontroll.

Använd Ny → X.509 för att direkt infoga en post för X.509 certifikat, använd Ny → OpenPGP för OpenPGP.

För att ta bort en server från söklistan, markera den i listan och tryck därefter på knappen Ta bort.
För att ställa in tidsgränsen för LDAP, dvs. den maximala tiden som gränssnittet väntar på att en server ska svara, använd helt enkelt motsvarande inmatningsfält som heter LDAP-tidsgräns (minuter:sekunder).
Om en av dina servrar har en stor databas, så att till och med rimliga sökningar som Johansson når maximalt antal objekt som returneras av en fråga, kanske du vill öka gränsen. Du kan enkelt ta reda på om du når gränsen under en sökning, eftersom en dialogruta som talar om för dig att resultatet har avkortats dyker upp, om det är fallet.

NOT
Vissa servrar kan införa egna begränsningar på antal objekt som returneras vid en fråga. Om det är fallet, resulterar inte en ökning av gränsen här att flera objekt returneras.
5.2 Anpassning av utseende

5.2.1 Anpassning av Verktygstips

I huvudcertifikatlistan kan Kleopatra visa information om ett certifikat i ett verktygstips. Informationen som visas är samma som under fliken Översikt i dialogrutan Certifikatinformation. Verktygstips kan dock begränsas att bara visa en delmängd av informationen för en mindre detaljerad upplevelse.

**NOT**

**Nyckel-ID** visas *alltid*. Det görs för att försäkra att verktygstips för olika certifikat verkligen skiljer sig åt (det är särskilt viktigt om bara **Visa giltighet** har valts).

Man kan oberoende aktivera eller inaktivera följande informationsmängder:

**Visa giltighet**

Visar information om ett certifikats giltighet: dess nuvarande status, utfärdarens domännamn (bara S/MIME), utgångsdatum (om det finns något) och användningsflaggor för certifikatet.

Exempel:

<table>
<thead>
<tr>
<th>Certifikatet är för närvarande giltigt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utfärdare: CN=Test-ZS 7,O=Intevation GmbH,C=DE</td>
</tr>
<tr>
<td>Giltighet: från 2009-08-25 10:42 till och med 2010-10-19 10:42</td>
</tr>
<tr>
<td>Certifikatanvändning: Signering av e-post och filer, Kryptering av e-post och filer</td>
</tr>
<tr>
<td>Nyckel-ID: DC9D9E43</td>
</tr>
</tbody>
</table>

**Visa ägarinformation**

Visar information om certifikatets ägare: ägar-DN (bara DN),

OpenPGP exempel:

<table>
<thead>
<tr>
<th>Användar-id: Gpg4winUserA <a href="mailto:gpg4winusersa@test.hq">gpg4winusersa@test.hq</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Nyckel-ID: C6BF6664</td>
</tr>
<tr>
<td>Ägarens pålitlighet: fullständig</td>
</tr>
</tbody>
</table>

S/MIME exempel:

<table>
<thead>
<tr>
<th>Ägare: CN=Gpg4winTestuserA,OU=Testlab,O=Gpg4win Project,C=DE</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias: <a href="mailto:Gpg4winUserA@test.hq">Gpg4winUserA@test.hq</a></td>
</tr>
<tr>
<td>Nyckel-ID: DC9D9E43</td>
</tr>
</tbody>
</table>

**Visa teknisk detaljinformation**

Visar teknisk information om certifikatet: serienummer (bara S/MIME), typ, fingeravtryck och lagrinsplats.

Exempel:

<table>
<thead>
<tr>
<th>Serienummer: 27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certifikattyp: 1,024-bit RSA (hemligt certifikat tillgängligt)</td>
</tr>
<tr>
<td>Nyckel-ID: DC9D9E43</td>
</tr>
<tr>
<td>Fingeravtryck: 854F62EEBBB41BFDD3BE05D124971E09DC9D9E43</td>
</tr>
<tr>
<td>Lagrad: på den här datorn</td>
</tr>
</tbody>
</table>
5.2.2 Anpassning av Certifikatkategorier

Kleopatra låter dig anpassa utseendet hos (kontrollerade) nycklar i listvyn. Det omfattar att visa en liten ikon, men du kan också påverka förgrundsfärgen (textfärgen) och bakgrundsfärgen, samt teckensnittet.


För att ändra ikonen för en kategori, markera den i listan och tryck på knappen Ange ikon.... KDE:s vanliga ikonvalsdialogruta visas, där du kan välja en befintlig ikon i KDE:s samling, eller läsa en egen.

För att ta bort en ikon igen, måste du trycka på knappen Förvalt utseende.

För att ändra textfärgen (dvs. förgrundsfärgen) hos en kategori, markera den i listan och tryck på knappen Ange textfärg.... KDE:s vanliga färgvalsdialogruta visas, där du kan välja färg eller skapa en ny färg.

Att ändra bakgrundsfärg görs på samma sätt, klicka bara på Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, men du har ingen fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, men den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.

För att ändra teckensnitt har du egentligen två alternativ:

1. Ändra standardteckensnitt som används för alla listvyer i KDE.

2. Använd ett eget teckensnitt.

Det första alternativet har fördelen att teckensnittet följer vilken stil du än väljer i hela KDE, medan den senare ger dig fullständig kontroll över teckensnittet som används. Valet är ditt.

För att ändra bakgrundsfärgen momentant, markera den i listan och tryck på knappen Ange bakgrundsfärg istället.
Den här inställningssidan består i huvudsak av två listor, en för de kända egenskaperna (Tillgängliga egenskaper) och en som beskriver Nuvarande egenskapsordning.

Båda listor innehåller poster som beskrivs av egenskapens korta form (t.ex. CN) samt den utskrivna formen (Vanligt namn).

Listan Tillgängliga egenskaper är alltid sorterad i alfabetisk ordning, medan ordningen i listan Nuvarande egenskapsordning motsvarar den inställda DN-egenskapsordningen: den första egenskapen i listan är också den som visas först.

Bara egenskaper som explicit listas i Nuvarande egenskapsordning visas över huvud taget. Övriga döljs normalt.

Om platsmarkörposten _X_ (Alla andra) dock finns i ‘nuvarande’ listan, infogas alla egenskaper som inte listas (vare sig de är kända eller inte) på platsen _X_, i sin ursprungliga relativa ordning.

Ett litet exempel hjälper till att klargöra detta:

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

förvald egenskapsordning för ‘CN, L, _X_, OU, O, C’ ger följande formaterade DN:

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

medan ‘CN, L, OU, O, C’ ger

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

Vid att lägga till en egenskap i listan med egenskapsordning, markera den i listan Tillgängliga egenskaper, och tryck på knappen Lägg till i nuvarande egenskapsordning.

Vid att ta bort en egenskap från listan med egenskapsordning, markera den i listan Nuvarande egenskapsordning, och tryck på knappen Ta bort från nuvarande egenskapsordning.

Vid att bara flytta en egenskap till början (eller slutet), markera den i listan Nuvarande egenskapsordning, och tryck på knappen Flytta längst upp (eller Flytta längst ner).

Vid att bara flytta en egenskap uppåt (eller neråt) ett steg, markera den i listan Nuvarande egenskapsordning, och tryck på knappen Flytta upp ett steg (eller Flytta ner ett steg).

### 5.3 Anpassning av krypteringsåtgärder

#### 5.3.1 Anpassning av E-poståtgärder


När ’Snabbläge’ är aktiverat visas ingen dialogruta när brev signeras, eller krypteras, om det inte finns en konflikt som behöver löses upp manuellt.
5.3.2 Anpassning av Filåtgärder

Här kan man ställa in vissa aspekter av filåtgärder för Kleopatras UiServer. För närvarande kan man bara välja checksummeringsprogrammet att använda för CHECKSUM_CREATE_FILES.

Använd Program för checksummering att använda för att välja vilket av de inställda checksummeringsprogrammen som ska användas när checksummeringsfiler skapas.

När checksummor verifieras, hittas programmet att använda automatiskt baserat på de funna checksummeringsfilernas namn.

**NOT**

Administratörer och avancerade användare kan helt och hållet definiera vilka checksummeringsprogram som ska vara tillgängliga i Kleopatra via så kallade ‘checksummeringsdefinitioner’ i inställningsfilen. Se Avsnitt 6.4 i kapitel 6 för detaljinformation.

5.4 Anpassning av aspekter rörande S/MIME-validering

På den här sidan kan man ställa in vissa aspekter av valideringen av S/MIME certifikat.

**NOT**

Till största delen är det helt enkelt en mer användarvändig version av samma inställningar som också finns i Avsnitt 5.5. Allt du kan ställa in här, kan du också ställa in där, med undantag av Kontrollera certifikatgiltighet var n:te timma, som är specifik för Kleopatra.

Alternativens betydelse är följande:

5.4.1 Anpassning av intervall mellan certifikatkontroller

Kontrollera certifikatgiltighet var n:te timma


**NOT**

Validering utförs implicit så fort viktigare filer i ~/ .gnupg ändras. Alternativet påverkar därför bara externa faktorer rörande certifikatens giltighet, precis som Verktyg → Uppdatera OpenPGP-certifikat och Verktyg → Uppdatera X.509-certifikat.

5.4.2 Anpassning av valideringsmetod

Validera certifikat med CRL:er

Om alternativet väljes, valideras S/MIME certifikat genom att använda certifikatåterkallningslistor (CRL:er).

Se Direktvalidera certifikat (OCSP) för ett alternativt sätt att kontrollera certifikatens giltighet.
Direktvalidera certifikat (OCSP)

Om alternativet är markerat, valideras S/MIME certifikat direkt med OCSP (Online Certificates Status Protocol).

**WARNING**

När den här metoden är vald, skickas en begäran till certifikatutfärdarens server mer eller mindre varje gång man skickar eller tar emot ett krypterat brev, vilket sålunda i teorin låter certifikatutfärdaren spåra vem man (exempelvis) utbyter brev med.

För att använda metoden måste man skriva in webbadressen för OCSP besvararen i Webbadress för OCSP-besvarare.

Se Direktvalidera certifikat (OCSP) för ett mer traditionellt sätt att kontrollera certifikatens giltighet, som inte läcker information om vem du utbyter brev med.

**Webbadress för OCSP-besvarare**

Skriv in adressen till servern för direktvalidering av certifikat (OCSP besvararen). Webbadressen börjar vanligtvis med http://

**Signatur för OCSP-besvarare**

Välj certifikatet som OCSP-servern signerar sina svar med här.

**Ignorera tjänstwebbadress för certifikat**

Varje S/MIME certifikat innehåller oftast webbadressen till utfärdarens OCSP-besvarare (Certifikat → Hämta innehåll i certifikat avslöjar om ett givet certifikat innehåller den).

Att markera alternativet gör att GpgSM ignorerar dessa webbadresser och bara använder den som är inställd ovan.

Använd det för att t.ex. tvinga att en företagsomfattande OCSP-proxy används.

5.4.3 Anpassning av valideringsalternativ

**Kontrollera inte certifikatpolicy**

Normalt använder GpgSM filen ~/.gnupg/policies.txt för att kontrollera om en certifikatpolicy är tillåten. Om alternativet är markerat kontrolleras inte policyn.

**Konsultera aldrig en CRL**

Om det här alternativet är markerat, används certifikatåterkallningslistor aldrig för att validera S/MIME certifikat.

**Tillåt att rocertifikat markeras som pålitliga**

Om alternativet är markerat när rocertifikat från certifikatutfärdarens importeras, får du tillfrågad om att bekräfta dess fingeravtryck och tillstånd vare sig du anser att rocertifikatet är pålitligt eller inte.

Ett rocertifikat måste vara pålitligt innan de certifikat som det certifierar kan anses pålitliga, men att lättvindligt tillåta pålitliga rocertifikat i din certifikatlagring, underminerar systemets säkerhet.

**NOT**

Att aktivera funktionen i gränssnittet kan orsaka att dialogrutor från PinEntry dyker upp vid olämpliga tillfällen (t.ex. när signaturer verifieras), och kan på så sätt blockera behandling av brev vid frånvaro. Av den orsaken, och eftersom det är önskvärt att kunna sluta lita på ett pålitligt rocertifikat igen, tillåter Kleopatra att pålitlighet ställs in manuellt genom att använda Certifikat → Lita på rocertifikat och Certifikat → Lita inte på rocertifikat .

Inställningen hän påverkar inte Kleopatrars funktion.
Hämta saknade utfärdarcertifikat
Om det här alternativet är markerat, hämtas saknade utgivarcertifikat om nödvändigt (detta gäller båda valideringsmetoderna, CRL:er och OCSP).

5.4.4 Anpassning av alternativ för HTTP-begäran

Utför inte någon HTTP-begäran
Inaktiverar användning av HTTP för S/MIME helt och hållet.

Ignorera HTTP CRL-distributionsställe för certifikat
Vid sökning efter platsen för en CRL, innehåller certifikatet som ska testas oftast poster med så kallade ‘CRL-distributionsställen’ (DS) vilka är webbadresser som beskriver sättet att komma åt en CRL. Den första DS-posten som hittas används.
Med det här alternativet ignoreras alla poster som använder HTTP-metoden vid sökning efter en lämplig DS.

Använd systemets HTTP-proxy
Om det här alternativet markeras, används värdet på HTTP-proxyn som visas till höger (som kommer från miljövariabeln http_proxy) för varje HTTP-begäran.

Använd denna proxy för HTTP-begäran
Om ingen systemproxy är inställd, eller om du måste använda en annan proxy för GpgSM, kan du skriva in dess plats här.
Den kommer att användas för varje HTTP-begäran som har med S/MIME att göra.
Syntaxen är värddator:port, t.ex. minproxy.någonstans.se:3128.

5.4.5 Anpassning av alternativ för LDAP-begäran

Utför inte någon LDAP-begäran
Inaktiverar användning av LDAP för S/MIME helt och hållet.

Ignorera LDAP CRL-distributionsställe för certifikat
Vid sökning efter platsen för en CRL, innehåller certifikatet som ska testas oftast poster med så kallade ”CRL-distributionsställen” (DS) vilka är webbadresser som beskriver sättet att komma åt CRL:en. Den första DS-posten som hittas används.
Med det här alternativet ignoreras alla poster som använder LDAP-metoden vid sökning efter en lämplig DS.

Huvudvärddator för LDAP-begäran
Att skriva in en LDAP-server här gör att varje LDAP-begäran går först till denna server. Närmer bestämt överskrider inställningen alla specifika host och port i en LDAP-webbadress, och används också om host och port har utelämnats från webbadressen.
5.5 Anpassning av GnuPG-systemet

Den här delen av dialogrutan skapas automatiskt av utdata från `gpgconf --list-components` och för varje komponent som ovanstående kommando returnerar, utdata från `gpgconf --list-options` komponent.

**NOT**

De mest användbara av dessa alternativ har duplicerats som separata sidor i Kleopatras inställningsdialogruta. Se Avsnitt 5.1 och Avsnitt 5.4, de två dialogrutorna som innehåller utvalda alternativ från den här delen av dialogrutan.

Det exakta innehållet i den här delen av dialogrutan beror på versionen av GnuPG-gränssnittet som är installerat, och möjligtvis plattformen som används. Sådana beskriver vi bara dialogrutans allmänna utläggning, inklusive avbildningen från alternativ i GpgConf till det grafiska gränssnittets kontroller i Kleopatra.

GpgConf returnerar inställningsinformation för flera komponenter, inne i varje komponent är enskilda alternativ kombinerade i grupper.

Kleopatra visar en flik per komponent rapporterad av GpgConf. Grupper inleds med en horisontell linje som visar gruppnamnet som returneras från GpgConf.

Varje alternativ i GpgConf har en typ. Förutom vissa välkända alternativ som Kleopatra tar omhand med särskilda kontroller för en bättre användarupplevelse, är avbildningen mellan typer i GpgConf och kontroller i Kleopatra den följande:

<table>
<thead>
<tr>
<th>typ i GpgConf</th>
<th>kontroll i Kleopatra</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Nummerruta ('antal')</td>
</tr>
<tr>
<td>string</td>
<td>Ej tillämplig</td>
</tr>
<tr>
<td>int32</td>
<td>Radeditor (oformaterad)</td>
</tr>
<tr>
<td>uint32</td>
<td>Nummerruta</td>
</tr>
<tr>
<td>pathname</td>
<td>Ej tillämplig</td>
</tr>
<tr>
<td>ldap server</td>
<td>särskild kontroll</td>
</tr>
<tr>
<td>key fingerprint</td>
<td>särskild kontroll</td>
</tr>
<tr>
<td>pub key</td>
<td>Ej tillämplig</td>
</tr>
<tr>
<td>sec key</td>
<td></td>
</tr>
<tr>
<td>alias list</td>
<td></td>
</tr>
</tbody>
</table>

Tabell 5.1: Avbildning från typer i GpgConf till grafiska kontroller

Se handboken för GpgConf för mer information om vad man kan ställa in här, och hur.
Kapitel 6

Administrationsguide

Administrationsguiden beskriver sätt att anpassa Kleopatra som inte är tillgängliga via det grafiska gränssnittet, utan bara via inställningsfiler.

Det antas att läsaren känner till teknologin som används för att anpassa KDE-program, inklusive layout, plats i filesystemet och ordning hos KDE:s inställningsfiler, samt KIOSK-ramverket.

6.1 Anpassning av guiden för att skapa certifikat

6.1.1 Anpassa domännamnsfälten

Kleopatra låter dig anpassa fälten som användaren får skriva in för att skapa sitt certifikat.


Genom att använda kiosklägets flaggor $e blir det möjligt att hämta värden från miljövariabler eller från utvärdering av ett skript eller ett körbart program. Om du dessutom vill förhindra redigering av respektive fält, använd flaggan $i. Om du vill förhindra att knappen Infoga min adress används, anges värdet false för ShowSetWhoAmI.

**TIPS**

Beroende på naturen hos KDE:s kiosk-ramverk, blir det omöjligt för användaren att överskrida flaggan för oförändringsbarhet ($i) när den används. Det är avsett beteende. $i och $e kan också användas med vilken annan inställningsnyckel som helst i KDE-program.

Följsande exempel ger en översikt av möjliga anpassningar:

```conf
[CertificateCreationWizard]
; Tillåt inte kopiering av personlig data från adressboken, tillåt inte → lokal överskrivning
ShowSetWhoAmI[$i]=false

; ställer in användarnamnet till $USER
CN[$e]=$USER
```
6.1.2 Begränsa typer av nycklar som en användare tillåts skapa


6.1.2.1 Algoritmer för öppna nycklar

För att begränsa algoritmerna för öppna nycklar som används, lägg till inställningsnyckeln PGPK eyType (och CMSKeyType, men bara RSA stöds för CMS ändå) under sektionen CertificateCreationWizard i kleopatrarc.

De tillåtna värdena är RSA för RSA-nycklar, DAS för DSA-nycklar (bara för signatur), och DSA+ELG för en DSA-nyckel (bara för signatur) med en Elgamal-delnyckel för kryptering.

Standardvärden läses från GpgConf eller från RSA om GpgConf inte tillhandahåller något standardvärde.

6.1.2.2 Storlek på öppen nyckel

För att begränsa tillgängliga nyckelstorlekar för en öppen algoritm, lägg till inställningsnyckeln <ALG>KeySizes (där ALG kan vara RSA, DSA eller ELG) under sektionen CertificateCreationWizard i kleopatrarc, som innehåller en lista med nyckelstorlekar (i bitar) åtskilda av kommatecken. Ett standardvärde kan anges genom att inleda nyckelstorleke med ett tankstreck (-).

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

Ovanstående skulle begränsa tillåtna storlekar för RSA-nycklar till 1536, 2048 och 3072, med 2048 som standardstorlek.

Förutom själva storlekarerna, kan du också ange beteckningar för varje storlek. Ställ helt enkelt in inställningsnyckeln ALGKeySizeLabels till en lista med beteckningar åtskilda av kommatecken.

```
RSAKeySizeLabels = svag,normal,stark
```

Ovanstående tillsammans med föregående exempel, skulle skriva ut något som liknar följande alternativ att välja:

```
svag (1536 bitar)
normal (2048 bitar)
stark (3072 bitar)
```

Standardvärden är som om följande gällde:
Handbok Kleopatra

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

6.2 Skapa och redigera nyckelkategorier


Vid försök att hitta kategorin som en nyckel hör till, försöker Kleopatra matcha nyckeln med en följd av nyckelfilter, angivna i filen libkleopatrarc. Det första som matchar definierar kategorin, baserat på konceptet säregenhet (eng. specificity), som förklaras närmare nedan.

Varje nyckelfilter definieras i en konfigurationsgrupp som heter Key Filter #n, där n är ett tal som börjar på 0.

Det enda alternativen som krävs i gruppen Key Filter #n är Name, som innehåller namnet på kategorin som den visas i inställningsdialogrutan, och id som används för att referera till filtret i andra inställningssektioner (såsom View #n).

Tabell 6.1 listar alla nycklar som definierar visningsegenskaperna för nycklar som hör till kategorin (dvs. de nycklar som kan ställas in i inställningsdialogrutan), medan Tabell 6.2 anger alla alternativ som definierar de kriterier som filtret använder för att matcha nycklar.

<table>
<thead>
<tr>
<th>Inställningsalternativ</th>
<th>Typ</th>
<th>Beskrivning</th>
</tr>
</thead>
<tbody>
<tr>
<td>background-color</td>
<td>färg</td>
<td>Bakgrundsfärgen som ska användas. Om den saknas får den som standardvärde vilken bakgrundsfärg som än är definierad globalt för listvyer.</td>
</tr>
<tr>
<td>foreground-color</td>
<td>färg</td>
<td>Förgrundsfärgen som ska användas. Om den saknas får den som standardvärde vilken förgrundsfärg som än är definierad globalt för listvyer.</td>
</tr>
<tr>
<td>font</td>
<td>teckensnitt</td>
<td>Det egna teckensnittet som ska användas. Teckensnittet skalas till storleken som är inställd för listvyer, och eventuella teckenegenskaper (se nedan) införs.</td>
</tr>
<tr>
<td>font-bold</td>
<td>boolean</td>
<td>Om angiven som true och font inte är angiven, används standardteckensnittet i listvyn med teckenstilen fetstil tillagd (om tillgänglig). Ignoreras om font också finns med.</td>
</tr>
<tr>
<td>Inställningsalternativ</td>
<td>Typ</td>
<td>Om angivet matchar filtret när...</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>is-revoked</td>
<td>boolean</td>
<td>nyckeln har återkallats.</td>
</tr>
<tr>
<td>match-context</td>
<td>context¹</td>
<td>sammanhanget där filtret matchar.</td>
</tr>
<tr>
<td>is-expired</td>
<td>boolean</td>
<td>nyckeln har gått ut.</td>
</tr>
<tr>
<td>is-disabled</td>
<td>boolean</td>
<td>nyckeln har inaktiverats (markerats för att inte användas) av användaren. Ignoreras för S/MIME-nycklar.</td>
</tr>
<tr>
<td>is-root-certificate</td>
<td>boolean</td>
<td>nyckeln är ett rotcertifikat. Ignoreras för OpenPGP-nycklar.</td>
</tr>
<tr>
<td>can-encrypt</td>
<td>boolean</td>
<td>nyckeln kan användas för kryptering.</td>
</tr>
<tr>
<td>can-sign</td>
<td>boolean</td>
<td>nyckeln kan användas för signering.</td>
</tr>
<tr>
<td>can-certify</td>
<td>boolean</td>
<td>nyckeln kan användas för att signera (certifiera) andra nycklar.</td>
</tr>
<tr>
<td>can-authenticate</td>
<td>boolean</td>
<td>nyckeln kan användas för behörighetskontroll (t.ex. som ett TLS-klientcertifikat).</td>
</tr>
<tr>
<td>is-qualified</td>
<td>boolean</td>
<td>nyckeln kan användas för att skapa kvalificerade signaturer (enligt definitionen i tysk lag rörande digitala signaturer).</td>
</tr>
<tr>
<td>is-cardkey</td>
<td>boolean</td>
<td>nyckeln lagras på ett smartkort (istället för på datorn).</td>
</tr>
<tr>
<td>has-secret-key</td>
<td>boolean</td>
<td>den hemliga nyckeln i det här nyckelparet är tillgänglig.</td>
</tr>
</tbody>
</table>

¹Context är ett uppräkningsvärde med följande tillåtna värden: appearance, filtering och any.
Tabell 6.2: Inställningsalternativ för att definiera filterkriterier i nyckelfilter

<table>
<thead>
<tr>
<th>parameter</th>
<th>type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is-openpgp-key</td>
<td>boolean</td>
<td>nyckeln är en OpenPGP-nyckel (true), eller en S/MIME-nyckel (false).</td>
</tr>
<tr>
<td>was-validated</td>
<td>boolean</td>
<td>nyckeln har validerats.</td>
</tr>
<tr>
<td>prefix-ownertrust</td>
<td>validity</td>
<td>nyckeln har exakt (prefix = is), har vad som helst utom (prefix = is-not), har åtminstone (prefix = is-at-least), eller har som mest (prefix = is-at-most ägarpålitligheten som anges som värde i inställningsalternativet. Om mer än en nyckel med prefix-ownertrust (med olika prefix värden) finns i en enstaka grupp, är beteendet odefinierat.</td>
</tr>
<tr>
<td>prefix-validity</td>
<td>validity</td>
<td>Motsvarar prefix-ownertrust, men för nyckelgiltighet istället för ägarpålitlighet.</td>
</tr>
</tbody>
</table>

Förutom de inställningsvärden som listas ovan, kan ett nyckelfilter också ha id och match-contexts.

Genom att använda filtrets id, som normalt är filtrets gruppnamn i inställningarna om det inte anges eller är tomt, kan du referera till nyckelfiltret på andra ställen i inställningarna, t.ex. i Kleopatras vyinställningar. Värdet id tolkas inte av Kleopatra, alltså kan du använda vilken sträng som helst, under förutsättning att den är unik.


NOT
Några av de mest intressanta kriterierna, som is-revoked eller is-expired fungerar bara med kontrollerade nycklar, vilket är orsaken till att det normalt bara undersöks att kontrollerade nycklar är återkallade eller utgångna, även om det är fritt att ta bort de extra villkoren.
Handbok Kleopatra


I allmänhet undersöks inte kriterier som inte anges (dvs. om inställningsalternativet inte är med). Om ett kriterium anges, undersöks det och måste matcha för att filtret som helhet ska matcha, dvs. kriterierna sammanfogas med OCH.


**Example 6.1 Exempel på nyckelfilter**

För att söka efter alla utgångna men inte återkallade rotcertifikat, skulle du använda ett nyckelfilter som definieras på följande sätt:

```
[Key Filter #n]
Name=utgångna, men inte återkallade
was - validated=true
is - expired=true
is - revoked=false
is - root - certificate =true
; ( specificity 4 )
```

För att söka efter alla inaktiverade OpenPGP-nycklar (som ännu inte stöds av Kleopatra) med åtminstone ‘marginell’ ägarpålitlighet, skulle du använda:

```
[Key Filter #n]
Name=inaktivera OpenPGP-nycklar med marginell eller bättre ägarpålitlighet
is - openpgp=true
is - disabled=true
is - at - least - ownertrust = marginal
; ( specificity 3 )
```

### 6.3 Anpassa arkiveringsverktyg för användning med signerade och krypterade filer

Kleopatra låter administratör (eller avancerad användare) ställa in listan med arkiveringsverktyg som presenteras i fildialogrutan Signera/kryptera.

Varje arkiveringsverktyg definiertas i libkleopatrarc som en separat grupp Archive Definition #n, med följande nödvändiga nycklar:

**extensions**

En lista med filnamnsändelser åtskilda av kommatecknen, som oftast anger arkiveringsformatet.

**id**

En unik identifierare som används för att identifiera arkiveringsverktyget internt. Om tveksam, använd kommandots namn.
**Namn (översatt)**

Namnet på arkiveringsverktyget synligt för användaren, som det visas i motsvarande kombinationsmenyn i fildialogrutan Signera/Kryptera.

**pack-command**

Själva kommandot för att arkivera filer. Vilket kommando som helst kan användas, så länge inget skal krävs för att köra det. Programfilen slås upp med miljövariabeln PATH,

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

**NOT**

Eftersom bakstreck (\) är ett skyddande tecken i KDE:s inställningsfiler, måste de dubbleras när de ingår i sökvägar:

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

För själva kommandot (i motsats till dess argument), kan man dock använda vanliga snedstreck (/ ) som avskiljare i sökvägar på alla plattformar:

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

Det stöds inte i argument, eftersom de flesta program på Windows® använder vanliga snedstreck för väljare. Exempelvis fungerar inte följande, eftersom C:/myarchivescript.bat är ett argument till cmd.exe, och / inte konverteras till \ i argument, bara kommandon:

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

Det måste istället skrivas som:

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

### 6.3.1 Skicka indatafilnamn till pack-command


1. Som kommandoradsväljare.
   
   **Exempel (tar):**
   
   ```
   pack-command=tar cf -
   ```
   
   **Exempel (zip):**
   
   ```
   pack-command=zip -r - %f
   ```
   
   I detta fall skickas filnamn på kommandoraden, precis som man skulle göra vid användning av en terminal. Kleopatra använder inte ett skal för att köra kommandot. Därför är detta ett säkert sätt att skicka filnamn, men det kan råka ut för begränsningar av kommandoradens längd på vissa plattformar. Teckenföljden %f, om den finns, ersätts med namnen på filerna att arkivera. Annars läggs filnamnen till sist på kommandoraden. Sålunda skulle zip-exemplet ovan ekvivalent kunna skrivas så här:
   
   ```
   pack-command=zip -r -
   ```
2. Via standardinmatningen, åtskilda med nyrader: lägg till | först

Exempel (GNU-tar):

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

Exempel (ZIP):

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

I detta fall skickas filnamn till arkiveringsverktyget på standardinmatningen, ett per rad. Det undviker problem på platfformar som har en låg gräns för antal kommandoradsväljare som tillåts, men misslyckas när filnamn faktiskt innehåller nyrader.

**NOT**

Kleopatra stöder för närvarande bara LF som nyradstecken, inte CRLF. Det kan komma att ändras i framtida versioner, baserat på återmatning från användare.

3. Via standardinmatningen, åtskilda med NUL-tecken: lägg till 0| först

Exempel (GNU-tar):

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

Detta är samma sak som ovan, utom att NUL-tecken används för att skilja filnamn åt. Eftersom NUL-tecken är förbjudna i filnamn, är detta det säkraste sättet att skicka filnamn, men inte alla arkiveringsverktyg stöder det.

### 6.4 Anpassa checkummeringsprogram för användning när checksummar skapas och verifieras

Kleopatra låter administratör (eller avancerad användare) ställa in listan med checkummeringsprogram som användaren kan välja bland i inställningsdialogrutan, och Kleopatra klarar av att automatiskt detektera verktyg när det ombeds att verifiera en given fils checksumma.

**NOT**

För att vara användbart av Kleopatra, måste utdata från checkummeringsprogram (både den skriva checkummeringsfilen, och standardutmatningen vid verifiering av checkummer) vara kompatibelt med GNU *md5sum* och *sha1sum*.

Närmare bestämt måste checkummeringsfilen vara radbaserad, med varje rad på följande format:

```
CHECKSUMMA ' ' ( ' ' | '*' ) FILNAMN
```

där CHECKSUMMA endast består av hexadecimala tecken. Om FILNAMN innehåller ett nyradstecken, måste raden istället lyda:

```
\CHECKSUMMA ' ' ( ' ' | '*' ) SKYDDAT-FILNAMN
```

där SKYDDAT-FILNAMN är filnamnet med nyrader ersatta med \n, och bakstreck dubblerade (\&#8614;\()

På liknande sätt måste utdata från verify-command ha formen

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

åtskilda med nyrader. Nyrader och andra tecken skyddas inte i utdata.

---

*a* Jo, dessa program skrevs inte med grafiska gränssnitt i åtanke, och Kleopatra misslyckas tolka patologiska filnamn som innehåller "::OK" och nyrad riktigt.
Varje checksummeringsprogram definieras i libkleopatrarc som en separat grupp Checksum Definition #n, med följande nödvändiga nycklar:

**file-patterns**
En lista med reguljära uttryck som beskriver vilka filer som ska anses vara checksummeringsfiler för det här checksummeringsprogrammet. Syntaxen är den som används för stränglistor i KDE:s inställningsfiler.

**output-file**
Det typiska utdatafilnamnet för det här checksummeringsprogrammet (ska naturligtvis motsvara ett av file-patterns). Det är vad Kleopatra kommer att använda som utdatafilnamn när checksummeringsfiler av den här typen skapas.

**id**
En unik identifierare som används för att identifiera checksummeringsprogrammet internt. Om tveksam, använd kommandots namn.

**Namn (översatt)**
Namnet på checksummeringsprogrammet synligt för användaren, som det visas i kombinationsmenyn i Kleopatras inställningsdialogruta.

**create-command**
Själva kommandot som används för att skapa checksummeringsfiler. Syntaxen, begränsningar och alternativ för att skicka väljare är samma som beskrivs för pack-command i Avsnitt 6.3.

**verify-command**
Samma som create-command, men för verifiering av checksummor.

Här är ett fullständigt exempel:

```
[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
```
Kapitel 7

Tack till och licens

Dokumentation copyright 2002 Steffen Hansen, copyright 2004 Daniel Molkentin, copyright 2004, 2010 Klarälvdalens Datakonsult AB

BIDRAGSGIVARE

• 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

Översättning Stefan Asserhäll stefan.asserhall@bredband.net

Den här dokumentationen licensieras under villkoren i GNU Free Documentation License. Det här programmet licensieras under villkoren i GNU General Public License.