El manual del Kleopatra

Marc Mutz
Desenvolupador: David Faure
Desenvolupador: Steffen Hansen
Desenvolupador: Matthias Kalle Dalheimer
Desenvolupador: Jesper Pedersen
Desenvolupador: Daniel Molkentin
Traductor: Antoni Bella

Índex

Índex de taules

Resum

El Kleopatra és una eina per a gestionar certificats X.509 i OpenPGP.

Capítol 1

Introducció

El Kleopatra és una eina KDE per a gestionar certificats X.509 i OpenPGP als anells de claus GpgSM i GPG, així com per a rebre certificats des de servidors LDAP i d'altres.

El Kleopatra es pot iniciar des del menú **Eines** → **Gestor de certificats** del KMail, així com des de la línia d'ordres. L'executable del Kleopatra s'anomena **`kleopatra`**.

NOTA

Aquest programa s'anomena Cleòpatra, com una famosa faraona egípcia que va viure al temps d'en Juli Cèsar, amb qui es diu que va tenir un fill, Cesarió, no reconegut com el seu hereu.
El nom es va escollir donat que el programa s'originà des del projecte Ägypten (Ägypten és Egipte en alemany). El Kleopatra és la manera d'escriure Cleopatra en alemany.

Capítol 2

Funcions principals

2.1 Veure l'anell de claus local

La funció principal del Kleopatra és mostrar i editar el contingut de la caixa de claus local, el qual és similar al concepte dels anells de claus de GPG, encara que no s'ajusti massa a aquesta analogia.

La finestra principal està dividida en l'àrea gran del llistat de claus amb diverses pestanyes, la barra de menús i la barra de cerca a dalt, i la barra d'estat de baix.

Cada línia en la llista de claus es correspon amb un certificat, que s'identifica per l'anomenat **Assumpte DN**. DN és l'acrònim de «Nom distintiu», un identificador jeràrquic, quelcom com un camí cap al sistema de fitxers amb una sintaxi poc usual, se suposa que és un identificador global únic per a un certificat en qüestió.

Perquè siguin vàlides, i per tant usables, les claus (públiques) han d'estar signades per una CA (Autoritat certificadora). Aquestes signatures s'anomenen certificats, però normalment els termes «certificat» i «clau (pública)» s'utilitzen indistintament, i en aquest manual no en farem distincions, a excepció de quan s'indiqui de manera explícita.

Les CA poden estar signades per altres CA per a ser vàlides. Per descomptat, ha d'existir algun límit, així que la CA de nivell superior (CA arrel) signa la seva clau amb ella mateixa (això s'anomena signar a si mateix). Als certificats arrel se'ls ha d'assignar manualment una validesa (sovint anomenada confiança), p. ex., després de comparar l'empremta digital amb la del lloc web de la CA. Normalment, sol fer-ho l'administrador del sistema o el venedor d'un producte que empri certificats, però també pot fer-ho qualsevol usuari amb la interfície de línia d'ordres de GpgSM.

Per a veure quins dels certificats són certificats arrel, podeu canviar al mode de llista jeràrquica de claus amb **Visualitza → Llista jeràrquica de certificats**.

Podeu veure els detalls de qualsevol certificat fent-hi doble clic o utilitzant **Visualitza → Detalls del certificat**. Això obrirà un diàleg que us mostrarà les propietats més freqüents del certificat, la vostra cadena de certificat (és a dir, la cadena de l'emissora fins a la CA arrel) i un bolcat de tota la informació del certificat que es pot extraure des del dorsal.

Si canvieu l'anell de claus sense utilitzar el Kleopatra (p. ex., utilitzant la interfície de la línia d'ordres de GpgSM), hauríeu d'actualitzar la vista amb **Visualitza → Torna a mostrar (F5)** .

2.2 Cercar i importar els certificats

La majoria de les vegades, adquirireu certificats nous en verificar signatures als correus electrònics, atès que els certificats són incrustats en les signatures que es fan en utilitzar-los. De tota

manera, si us cal enviar un correu a algú amb el que encara no heu contactat, haureu d'obtenir el certificat des d'un directori LDAP (tot i que GpgSM pot fer-ho automàticament), o des d'un fitxer. També haureu d'importar el vostre propi certificat després de rebre la resposta de la CA a la vostra petició de certificació.

Per a cercar un certificat en un directori LDAP, seleccioneu **Fitxer** → **Cerca de certificats en el servidor** i escriviu algun text (p. ex., el nom de la persona de la qual voleu el certificat) a la línia d'edició del diàleg **Cerca de certificats en servidors de certificats**, a continuació, feu clic al botó **Cerca**. Els resultats es mostraran a la llista de claus sota la barra de cerca, on podeu seleccionar els certificats per a veure'ls fent clic al botó **Detalls** o amb el botó **Importa** descarregar-lo a l'anell de claus local.

Podeu configurar la llista de servidors LDAP per a les cerques en la pàgina **Serveis de directori** des del diàleg de configuració del Kleopatra.

Si vàreu rebre el certificat com a un fitxer, intenteu **Fitxer** → **Importa els certificats... (Ctrl+I)** . GpgSM necessita entendre el format del fitxer de certificat; si us plau, consulteu el manual de GpgSM per a una llista dels formats de fitxer admesos.

Si no vàreu crear el vostre parell de claus amb GpgSM, també haureu d'importar manualment la clau pública (així com la clau privada) des del fitxer PKCS#12 que vàreu obtenir de la CA. Podeu fer-ho des de la línia d'ordres amb `kleopatra --import-certificate nom_fitxer` o des del Kleopatra amb **Fitxer** → **Importa els certificats... (Ctrl+I)** , tal com ho faríeu amb els certificats «normals».

2.3 Crear un parell de claus nou

L'element de menú **Fitxer** → **Certificat nou... (Ctrl+N)** inicia l'**Assistent per a la creació del parell de claus**, el qual us guiarà a través d'un cert nombre de passos per tal de crear el certificat que esteu sol·licitant.

Una vegada realitzat cada pas dintre de l'assistent, premeu **Següent** per a anar cap al pas següent (o **Enrere** per a tornar a veure els passos que ja heu completat). La creació d'una sol·licitud de certificat pot cancel·lar-se en qualsevol moment prement el botó **Cancel·la**.

A la primera pàgina de l'assistent escollireu quin tipus de certificat voleu crear:

Crea un parell de claus OpenPGP personal

El parell de claus OpenPGP es crea localment, i és certificat pels vostres amics i coneguts. No existeix una autoritat de certificació central, sinó que cada individu crea un web de confiança personal mitjançant la certificació de parells de claus d'altres usuaris amb el seu propi certificat.

Heu d'introduir un **Nom**, un **Correu electrònic** i de manera opcional un **Comentari**.

Crea un parell de claus X.509 personal i una sol·licitud de certificació

El parell de claus X.509 es crea localment, però el centre de certificats per a una autoritat de certificació (CA). Les CA poden certificar altres CA, creant una cadena central, jeràrquica de confiança.

El primer pas en l'assistent serà el d'omplir el certificat amb les vostres dades personals. Els camps a omplir són:

- **Nom comú (CN):** El vostre nom;
- **Adreça de correu-e (EMAIL):** La vostra adreça de correu electrònic. Assegureu-vos que és correcta -aquesta serà l'adreça a la qual la gent us enviarà el correu emprant aquest certificat-.
- **Ubicació (L):** El poble o ciutat a on viviu.
- **Unitat organitzativa (OU):** La unitat organitzacional en la qual esteu (per exemple «Logística»).

- **Organització (O):** L'organització a la qual representeu (per exemple, l'empresa per a la qual treballeu).
- **Codi de país (C):** Les dues lletres pel país a on us trobeu (per exemple, «ES»).

El pas següent en l'assistent serà el de seleccionar a on desar-lo, en un fitxer o enviar-lo directament a una CA. Aquí podreu especificar un nom de fitxer o una adreça de correu electrònic a on enviar el certificat.

2.3.1 Com revocar una clau

Un parell de claus que han expirat es poden tornar a un estat funcional, sempre que tingueu accés a la clau privada i a la frase de pas. Per a tornar llegible una clau inusable necessitareu revocar-la. La revocació es porta a terme mitjançant l'afegit d'una signatura de revocació especial a la clau.

Aquesta signatura de revocació s'emmagatzema en un fitxer a part. Aquest fitxer podrà ser importat més endavant al clauer i després afegit a la clau inusable. Si us plau, tingueu en compte que per a la importació d'aquesta signatura a la clau no és necessària la contrasenya. Per tant, hauríem d'emmagatzemar aquesta signatura de revocació en un lloc segur, en general diferent del parell de claus. És un bon consell utilitzar un lloc separat del vostre ordinador, o bé copiar-la a un dispositiu d'emmagatzematge extern com una memòria USB o imprimir-la.

El Kleopatra no proporciona en cap moment una funció per a crear una signatura de revocació, però es pot fer amb l'aplicació KGpg del KDE escollint **Claus** → **Revoca la clau** i, de manera opcional, importar immediatament la signatura de revocació al vostre clauer.

Una forma alternativa de generar un certificat de revocació és utilitzar GPG directament des de la línia d'ordres: **`gpg --output certificat_de_revocació.asc --gen-revoke la_vostra_clau`**. L'argument *`la_vostra_clau`* haurà de ser un especificador de la clau, l'ID de la clau del vostre parell de claus primari o qualsevol part d'un ID de l'usuari que identifiqui el vostre parell de claus.

Capítol 3

Referència del menú

3.1 El menú Fitxer

Fitxer → Certificat nou... (Ctrl+N)

Crea un parell nou de claus (pública i privada) i permet enviar la part pública a una autoritat certificadora (CA) perquè la signi. El certificat resultant és el que us han de tornar o desar-lo en un servidor LDAP perquè el descarregueu al vostre anell de claus local, perquè pugueu usar-lo per a signar i desencriptar correus.

Aquest mode d'operació s'anomena «generació de claus descentralitzada», donat que totes les claus es creen localment. El Kleopatra (i GpgSM) no admeten directament la «generació de claus centralitzada», però podeu importar recopilacions de claus públiques/privades que rebeu des de la CA en format PCKS#12 mitjançant **Fitxer → Importa els certificats... (Ctrl+I)** .

Fitxer → Cerca certificats al servidor... (Ctrl+Maj+I)

Cerca i importa certificats des de servidors de certificació a l'anell de claus local. Vegeu Secció 2.2 pels detalls.

Necessitareu tenir configurats els servidors de claus perquè això funcioni. Per a més detalls, vegeu Secció 5.1.

Fitxer → Importa els certificats... (Ctrl+I)

Importa certificats i/o claus privades des de fitxers cap a l'anell de claus local. Vegeu Secció 2.2 pels detalls.

El format del fitxer del certificat hauria de ser un que estigui acceptat per GpgSM/GPG. Si us plau, consulteu els manuals de GpgSM i de GPG per a una llista dels formats admesos.

Fitxer → Exporta els certificats... (Ctrl+E)

Exporta els certificats seleccionats a un fitxer.

L'extensió del nom de fitxer que escolliu per a exportar determinarà el format del fitxer exportat:

- Per a certificats OpenPGP, `gpg` i `pgp` resultaran en un fitxer binari, mentre que `asc` resultarà en un fitxer amb armadura ASCII.
- Per a certificats S/MIME, `der` resultarà en un fitxer binari, un fitxer codificat amb DER, mentre que `pem` resultarà en un fitxer amb armadura ASCII.

Si no se seleccionen diversos certificats, el Kleopatra proposarà `empremta_digital.{asc,pem}` com el nom del fitxer exportat.

Aquesta funcionalitat només estarà disponible si s'han seleccionat un o més certificats.

> **NOTA**
> Això només exportarà les claus públiques, encara que la clau privada estigui disponible. Utilitzeu **Fitxer → Exporta les claus secretes...** per a exportar les claus privades a un fitxer.

Fitxer → Exporta les claus secretes...

Exporta la clau privada a un fitxer.

En el diàleg que s'obrirà, podeu triar si s'ha de crear un fitxer d'exportació binari o amb armadura ASCII (**Armadura ASCII**). Després feu clic sobre la icona de carpeta al costat dret del quadre de text **Fitxer de sortida** i seleccioneu la carpeta i el nom del fitxer d'exportació. En exportar claus secretes S/MIME, també podreu triar el **Joc de caràcters per a la frase de pas**. Per a més detalls, vegeu el debat de l'opció `--p12charset joc_de_caràcters` en el manual de GpgSM.

Aquesta funcionalitat només estarà disponible si s'ha seleccionat exactament només un certificat, i si està disponible la clau secreta per a aquest.

> **AVÍS**
> Rarament hauria de ser necessari utilitzar aquesta funcionalitat i, si ho fos, s'hauria de planificar amb cura. Planificar la migració d'una clau privada implica l'elecció del suport de transport i l'eliminació segura de les dades de la clau de la màquina antiga, així com del suport de transport, entre altres coses.

Fitxer → Exporta els certificats al servidor... (Ctrl+Maj+E)

Publica els certificats seleccionats a un servidor de claus (només OpenPGP).

El certificat s'envia al servidor de certificats configurat per a OpenPGP (cf. Secció 5.1), si està establert, en cas contrari a `keys.gnupg.net`.

Aquesta funcionalitat només estarà disponible si almenys s'ha seleccionat un certificat OpenPGP (i no S/MIME).

> **NOTA**
> Quan s'han exportat els certificats OpenPGP a un servidor de directori públic, és pràcticament impossible eliminar-los. Abans d'exportar el vostre certificat a un servidor de directori públic, assegureu-vos que heu creat un certificat de revocació de manera que pugueu revocar-lo més tard, si cal.

> **NOTA**
> La majoria dels servidors de certificació OpenPGP públics sincronitzen els certificats entre si, de manera que no té gaire sentit enviar-lo a més d'un.
> Pot passar que una cerca en un servidor de certificats no doni cap resultat tot i que només li heu enviat el vostre certificat. Això és perquè la majoria d'adreces de servidor de claus públics utilitzen DNS amb «round-robin» per a equilibrar la càrrega entre diverses màquines. Aquestes màquines se sincronitzen entre si, però en general, només cada 24 hores.

Fitxer → Desencripta/verifica fitxers...

Desencripta els fitxers i/o verifica les signatures als fitxers.

Fitxer → Signa/encripta fitxers...

Signa i/o encripta els fitxers.

Fitxer → Tanca (Ctrl+W)

Tanca la finestra principal de Kleopatra. Podeu restaurar-la en qualsevol moment des de la icona a la safata del sistema.

Fitxer → Surt (Ctrl+Q)

Fa que finalitzi Kleopatra.

3.2 El menú Visualitza

Visualitza → Torna a mostrar (F5)

Actualitza la llista de certificats.

L'ús d'aquesta funció generalment no és necessari, atès que Kleopatra supervisa el sistema de fitxers per als canvis i actualitza automàticament la llista de certificats quan sigui necessari.

Visualitza → Atura l'operació (Esc)

Atura (cancel·la) totes les operacions pendents, p. ex., una cerca, un llistat de claus o una descàrrega.

Aquesta funció només està disponible si almenys hi ha una operació activa.

> NOTA
> Per les limitacions del dorsal, de vegades les operacions es pengen de manera que aquesta funció no serà capaç de cancel·lar, immediatament, o en absolut.
> En aquests casos, l'única manera de restablir l'ordre és matar els processos SCDaemon, DirMngr, GpgSM i GPG, en aquest ordre, a través de les eines del sistema operatiu (**top**, el Gestor de tasques, etc.), fins que l'operació es desbloquegi.

Visualitza → Detalls del certificat

Mostra els detalls del certificat actualment seleccionat.

Aquesta funció només està disponible si s'ha seleccionat exactament un certificat.

Aquesta funció també està disponible fent doble clic directament sobre l'element corresponent de la vista de llista.

Visualitza → Llista jeràrquica de certificats

Canvia entre el mode jeràrquic i pla de la llista de claus.

En el mode jeràrquic, els certificats estan ordenats per relacions emissor/subjecte, així que és fàcil veure a quina certificació jeràrquica pertany un certificat donat, però és més difícil trobar un certificat inicialment (per descomptat, també podeu utilitzar la barra de cerca).

En mode pla, es mostren tots els certificats en una llista plana, ordenats alfabèticament. En aquest mode, és fàcil de trobar un certificat indicat, però no s'apreua clarament a quin certificat arrel pertany.

Aquesta funció canvia la manera jeràrquica per pestanya, és a dir, cada pestanya té el seu propi estat de jerarquia. Això és perquè podeu tenir un llistat pla i un llistat jeràrquic a mà, cadascun en la seva pròpia pestanya.

> NOTA
> Actualment, mostrar jeràrquicament només s'implementa per certificats S/MIME. Hi ha desacord entre els desenvolupadors sobre la forma correcta per a mostrar jeràrquicament els certificats OpenPGP (bàsicament, «pare = signador» o «pare = signant»).

Visualitza → Expandeix-ho tot (Ctrl+.)

Expandeix tots els elements en la vista de llista de certificats, és a dir, fa que tots els elements estiguin visibles.

És el valor predeterminat quan s'entra en el mode jeràrquic de llistat de claus.

Per descomptat, encara podeu expandir i contraure els elements individualment.

Aquesta funció només està disponible quan **Visualitza → Llista jeràrquica de certificats** està activat.

Visualitza → Redueix-ho tot (Ctrl+,)

Contrau tots els elements de la llista en la vista de llista de certificats, és a dir oculta tots els elements, excepte els de nivell superior.

Per descomptat, encara podeu expandir i contraure els elements individualment.

Aquesta funció només està disponible quan **Visualitza → Llista jeràrquica de certificats** està activat.

3.3 El menú Certificats

Certificats → Canvia la confiança del propietari...

Canvia la confiança del propietari del certificat OpenPGP seleccionat.

Aquesta funció només està disponible quan se selecciona exactament un certificat OpenPGP.

Certificats → Confia en el certificat arrel

Marcar això (S/MIME) fa el certificat arrel com de confiança.

D'alguna manera, això és l'equivalent a **Certificats → Canvia la confiança del propietari...** per a certificats arrel S/MIME. Podeu, de tota manera, només triar entre els termes d'OpenPGP confiança «ultimate» i «never trust».

> NOTA
> El dorsal (per mitjà de GpgAgent) demanarà en el moment de la importació de certificats arrel si confieu en el certificat arrel d'importació. Tanmateix, aquesta funció ha de ser explícitament permesa en la configuració del dorsal (`allow-mark-trusted` a `gpg-agent.conf`, o bé **Sistema GnuPG → Agent GPG → Permet als clients marcar les claus com a fiables** o **Validació S/MIME → Permet marcar els certificats arrel com a fiables** sota capítol 5).
> Habilitar aquesta funcionalitat en el dorsal pot produir emergents des de PinEntry en moments inoportuns (p. ex., en la verificació de signatures), i per tant es pot blocar desatenent el processament del correu electrònic. Per aquesta raó, i perquè és convenient per a poder establir la *desconfiança* a un nou certificat arrel de confiança, Kleopatra permet l'ajust manual de la confiança.

> AVÍS
> A causa de la falta de suport del dorsal per a aquesta funció, Kleopatra ha de treballar directament sobre la base de dades de confiança de GpgSM (`trustlist.txt`). En utilitzar aquesta funció, assegureu-vos que no hi ha altres operacions de criptografia en curs que podrien competir amb Kleopatra en la modificació de la base de dades.

Aquesta funció només està disponible quan està seleccionat exactament un certificat arrel S/MIME, i aquest encara no és de confiança.

Utilitzeu **Certificats → Desconfia del certificat arrel** per a desfer aquesta funcionalitat.

Certificats → Desconfia del certificat arrel

Marca aquest certificat arrel (S/MIME) com de no confiança.

Aquesta funció només està disponible quan està seleccionat exactament un certificat arrel S/MIME, i aquest és de confiança.

Utilitzeu **Certificats → Confia en el certificat arrel** per a desfer aquesta funcionalitat. Veure-ho per a més detalls.

Certificats → Certifica un certificat...

Us permet certificar un altre certificat OpenPGP.

Aquesta funció només està disponible si s'ha seleccionat exactament un certificat OpenPGP.

Certificats → Canvia la data de venciment...

Permet canviar la data de venciment del certificat OpenPGP.

Utilitzeu aquesta funcionalitat per a allargar la vida útil dels certificats OpenPGP com una alternativa a crear-ne un de nou, o l'ús il·limitat d'aquest («mai caduca»).

Aquesta funcionalitat només està disponible si s'ha seleccionat exactament només un certificat OpenPGP, i està disponible la clau secreta per a aquest.

Certificats → Canvia la frase de pas...

Permet canviar la frase de pas de la clau secreta.

Aquesta funció només està disponible si s'ha seleccionat exactament un certificat, i la clau secreta està disponible per a aquest. Es requereix un dorsal molt recent, ja que hem canviat la implementació de la crida directa de GPG i GpgSM a una basada en GpgME.

> NOTA
> Per raons de seguretat, PinEntry demana tant l'antiga com la nova frase de pas, en un procés a part. Depenent de la plataforma on s'executen i sobre la qualitat de la implementació de PinEntry en aquesta plataforma, pot succeir que la finestra de PinEntry aparegui al fons. Per tant, si se selecciona aquesta funció i no passa res, comproveu la barra de tasques del sistema operatiu per si una finestra de PinEntry està oberta en segon pla.

Certificats → Afegeix un ID d'usuari...

Permet afegir un nou ID d'usuari pel certificat d'OpenPGP.

Utilitzeu aquesta opció per a afegir noves identitats a un certificat ja existent com a alternativa a la creació d'un nou parell de claus. Una ID d'usuari d'OpenPGP té la forma següent:

```
Nom_real (Comentari) <Correu_electrònic>
```

En el diàleg que apareix quan se selecciona aquesta funció, Kleopatra us demanarà separadament per cadascun dels tres paràmetres (*Nom_real*, *Comentari* i *Correu_electrònic*), i mostrarà el resultat en una vista prèvia.

> NOTA
> Aquests paràmetres estan subjectes a les mateixes restriccions d'administrador que en els nous certificats. Per a més detalls vegeu Secció 2.3 i Secció 6.1.

Aquesta funcionalitat només està disponible si s'ha seleccionat exactament només un certificat OpenPGP, i està disponible la clau secreta per a aquest.

Certificats → Suprimeix (Supr)

Suprimeix el(s) certificat(s) seleccionat(s) de l'anell de claus local.

Utilitzeu aquesta funció per a eliminar les claus no usades del vostre anell de claus local. De tota manera, com que els certificats són afegits normalment als correus electrònics signats, la verificació d'un correu electrònic pot provocar que la clau eliminada torni a l'anell de claus local. Per tant, probablement serà millor evitar aquesta funció sempre que sigui possible. Quan es perdi, useu la barra de cerca o la funció **Visualitza → Llista jeràrquica de certificats** per a tornar a tenir el control sobre la gran quantitat de certificats.

> AVÍS
> Hi ha una excepció a l'anterior: quan se suprimeix un dels certificats propis, també suprimiu la clau secreta. Això implica que no sereu capaç de llegir les comunicacions encriptades del passat fetes amb aquest certificat, llevat que tingueu una còpia de seguretat en algun lloc. Kleopatra us advertirà quan s'intenti suprimir una clau secreta.

A causa de la naturalesa jeràrquica dels certificats S/MIME, si suprimiu un emissor del certificat S/MIME (certificat CA), també se suprimiran tots els assumptes.[1]

Naturalment, aquesta funció només està disponible si heu seleccionat almenys un certificat.

Certificats → Bolca un certificat

Mostra tota la informació que té GpgSM sobre el certificat (S/MIME) seleccionat.

Veure el debat sobre `--dump-key clau` en el manual de GpgSM per a obtenir detalls sobre la sortida.

3.4 El menú Eines

Eines → Visualitzador del registre de GnuPG

Inicia GnuPG Log Viewer, una eina per a presentar la sortida de depuració d'aplicacions GnuPG. Si la signatura, encriptatge, o verificació deixen de funcionar misteriosament, és possible esbrinar per què mirant al registre.

Aquesta funció no està disponible en Windows®, ja que els mecanismes subjacents no estan implementats en el dorsal per a aquesta plataforma.

Eines → Actualitza els certificats OpenPGP

Actualitza tots els certificats OpenPGP mitjançant l'execució de

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

Després de completar amb èxit l'ordre, l'anell de claus local reflectirà els canvis pel que fa a la validesa dels certificats OpenPGP.

Vegeu la nota sota **Eines → Actualitza els certificats X.509** per a algunes advertències.

Eines → Actualitza els certificats X.509

Actualitza tots els certificats S/MIME mitjançant l'execució de

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

Després de completar amb èxit l'ordre, l'anell de claus local reflectirà els últims canvis pel que fa a la validesa dels certificats S/MIME.

[1] Això és el mateix que en un sistema de fitxers: quan se suprimeix una carpeta, també suprimiu tots els fitxers i carpetes dins seu.

> NOTA
> L'actualització de certificats X.509 o OpenPGP implica la descàrrega de tots els certificats i les CRL, per a comprovar si algun ha estat revocat en l'interval.
> Això pot provocar una congestió de la connexió de la xarxa (també la d'altres persones), i pot trigar fins a una hora en acabar, en funció de la vostra connexió de xarxa i el nombre de certificats a verificar.

Eines → **Importa la CRL des d'un fitxer...**

Us permet importar manualment les CRL des de fitxers.

Normalment, les llistes de certificats revocats (les CRL) es manegen de forma transparent pel dorsal, però de vegades pot ser útil per a importar una CRL manualment a la memòria cau de CRL locals.

> NOTA
> Perquè la importació de la CRL funcioni, l'eina DirMngr haurà d'estar present en la cerca de la variable d'entorn `PATH`. Si aquest element de menú està inhabilitat, haureu de contactar amb l'administrador del sistema i preguntar-li si pot instal·lar DirMngr.

Eines → **Neteja el cau de la CRL**

Neteja el cau CRL de GpgSM.

Probablement mai us caldrà. Podeu forçar una actualització del cau CRL seleccionant tots els certificats i usant en el seu lloc **Eines** → **Actualitza els certificats X.509** .

Eines → **Bolcat del cau de la CRL**

Mostra el contingut detallat del cau CRL de GpgSM.

3.5 El menú Arranjament

El Kleopatra disposa del menú **Arranjament** predeterminat del KDE, com es descriu en els Fonaments del KDE amb una entrada addicional:

Arranjament → **Executa una autocomprovació**

Realitza una sèrie de proves automàtiques i presenta els seus resultats.

Aquest és el mateix conjunt de proves que s'executa en l'arrencada per omissió. Si heu inhabilitat startup-time self-tests, ho podeu tornar a habilitar aquí.

3.6 El menú Finestra

El menú **Finestra** us permet manejar les pestanyes. L'ús dels elements en aquest menú pot canviar el nom d'una pestanya, afegir-ne una de nova, duplicar l'actual, tancar l'actual, i moure l'actual a l'esquerra o a la dreta.

En fer clic amb botó dret del ratolí sobre una pestanya s'obrirà un menú contextual, on també es poden seleccionar les mateixes accions.

3.7 El menú Ajuda

El Kleopatra disposa del menú **Ajuda** predeterminat del KDE, com es descriu en els Fonaments del KDE.

Capítol 4

Referència de les opcions de la línia d'ordres

Tan sols es mostren aquelles opcions específiques de Kleopatra. Com amb totes les aplicacions de KDE, podeu tenir una llista completa d'aquestes opcions executant l'ordre **`kleopatra --help`**.

`--uiserver-socket` ***`argument`***
: Ubicació del sòcol que està escoltant el servidor d'IU

`--daemon`
: Executa només el servidor d'IU, amaga la pantalla principal.

`-p --openpgp`
: Usa OpenPGP per a la següent operació.

`-c --cms`
: Usa CMS (X.509, S/MIME) per a l'operació següent.

`-i --import-certificate`
: Especifica un fitxer o un URL des d'on importar els certificats (o claus privades).
Aquesta és la línia d'ordres equivalent de **Fitxer → Importa els certificats... (Ctrl+I)** .

`-e --encrypt`
: Encripta el/s fitxer/s.

`-s --sign`
: Signa el/s fitxer/s.

`-E --encrypt-sign`
: Encripta i/o signa el/s fitxer/s. Igual que `--sign-encrypt`, no l'utilitzeu.

`-d --decrypt`
: Desencripta el/s fitxer/s.

`-V --verify`
: Verifica el fitxer/signatura.

`-D --decrypt-verify`
: Desencripta i/o verifica el/s fitxer/s.

Capítol 5

Configurar Kleopatra

Es pot accedir al diàleg de configuració del Kleopatra mitjançant **ArranjamentConfigura Kleopatra...**

Cadascuna de les seves pàgines es descriu en les següents seccions.

5.1 Configurar els serveis de directori

En aquesta pàgina, podeu configurar quins servidors LDAP utilitzar per a les cerques de certificats S/MIME, i quins servidors de claus utilitzar per a les cerques de certificats OpenPGP.

> NOTA
> Això és simplement una versió més fàcil d'usar de la mateixa configuració que també es troba en Secció 5.5. Tot el que podeu configurar aquí, també ho podeu configurar allà.

> UNA NOTA SOBRE LA CONFIGURACIÓ DE L'INTERMEDIARI (PROXY)
> La configuració de l'intermediari es pot configurar per HTTP i LDAP en Secció 5.4, però només per a GpgSM. Per a GPG, a causa de la complexitat de les opcions de servidor de claus en GPG i la manca de suport adequat en GpgConf, actualment haureu de modificar directament el fitxer de configuració `gpg.conf`. Si us plau, consulteu el manual de GPG per a més detalls. Kleopatra conservarà aquestes preferències, però encara no permet modificar-les en l'IGU.

La taula **Serveis de directori** mostra quins servidors estan configurats. Feu doble clic en una cel·la de la taula per a canviar els paràmetres d'entrades de servidor existent.

El significat de les columnes en la taula és el següent:

Esquema

Determina el protocol de xarxa que s'utilitza per a accedir al servidor. Els esquemes d'ús freqüent són **ldap** (i el seu germà segur SSL **ldaps**) pels servidors LDAP (protocol comú per S/MIME, l'únic suportat per GpgSM), i **hkp**, el protocol de servidor de claus Horowitz, avui en dia el protocol de servidor de claus HTTP, un protocol basat en HTTP que pràcticament suporten tots els servidors de claus OpenPGP públics.

Si us plau, consulteu els manuals de GPG i de GpgSM per a una llista dels esquemes suportats.

Nom del servidor
El nom de domini del servidor, p. ex., `keys.gnupg.net`.

Port del servidor
El port de xarxa on el servidor està escoltant.

Això canvia automàticament al port per omissió quan es canvia el **Esquema**, a menys que s'hagi establert en un port no estàndard. Si heu canviat el port per omissió i no es pot recuperar, intenteu establir **Esquema** a **`http`** i **Port del servidor** a **`80`** (el per omissió per a HTTP), llavors partiu d'aquí.

DN Base
La DN base (només per a LDAP i LDAPS), és a dir, l'arrel de la jerarquia LDAP. Sovint l'anomenen «cerca arrel (search root)» o «cerca base (search base)».

En general, s'assembla a **`c=de,o=Foo`**, com a part de l'URL de LDAP.

Nom d'usuari
El nom d'usuari, si és el cas, s'usa per a iniciar la sessió al servidor.

Aquesta columna només es mostra si l'opció **Mostra la informació d'usuari i contrasenya** (a la taula de sota) està marcat.

Contrasenya
La contrasenya, si és el cas, s'usa per a iniciar la sessió al servidor.

Aquesta columna només es mostra si l'opció **Mostra la informació d'usuari i contrasenya** (a la taula de sota) està marcat.

X.509
Reviseu aquesta columna si aquesta entrada s'ha d'usar per a les cerques de certificats X.509 (S/MIME).

Només els servidors LDAP (i LDAPS) són compatibles amb S/MIME.

OpenPGP
Reviseu aquesta columna si aquesta entrada s'ha d'usar per a les cerques de certificats OpenPGP.

Podeu configurar tants servidors S/MIME (X.509) com vulgueu, però en qualsevol moment només es permet un servidor OpenPGP. L'IGU ho forçarà.

Per a afegir un nou servidor, feu clic al botó **Nou**. Això duplica l'entrada seleccionada, si existeix, o s'insereix un servidor OpenPGP per omissió. A continuació, podeu establir la **Nom del servidor**, la **Port del servidor**, la **DN Base**, i l'habitual **Contrasenya** i **Nom d'usuari**, dos dels quals només són necessaris si el servidor requereix autenticació.

Per a inserir directament una entrada per a certificats X.509, useu **Nou** → **X.509**; useu **Nou** → **OpenPGP** per a OpenPGP.

Per a eliminar un servidor de cerca de la llista, seleccioneu-lo i després premeu el botó **Suprimeix**.

Per a definir el temps d'espera LDAP, és a dir, el temps màxim que s'esperarà el dorsal per a rebre la resposta del servidor, simplement useu el corresponent camp d'entrada, anomenat **Temps d'expiració LDAP (minuts:segons)**.

Si un dels servidors necessita una base de dades enorme, de manera que cada cerca raonable com **`Smith`** abasti el **Nombre màxim d'elements retornats per aquesta consulta**, potser voldreu incrementar aquest límit. Podeu esbrinar fàcilment si s'abasta aquest límit durant la cerca, perquè en aquest cas es mostrarà un diàleg per a dir-vos que es truncaran els resultats.

> NOTA
> Alguns servidors poden imposar els seus propis límits al nombre d'elements que retornen des d'una consulta. En aquest cas, l'increment del límit no resultarà en el retorn de més elements.

5.2 Configurar l'aparença

5.2.1 Configurar els Consells

A la llista de certificats principal, Kleopatra pot mostrar els detalls d'un certificat en un consell. La informació mostrada és la mateixa que en la pestanya **Vista general** del diàleg **Detalls del certificat**. Els consells, però, es poden limitar a només mostrar un subconjunt de la informació per a una experiència menys detallada.

> NOTA
> La **ID de clau** *sempre* es mostra. Això és per a assegurar que els consells per als diferents certificats, de fet, són diferents (això és especialment important si només s'ha seleccionat **Mostra la validesa**).

De forma independent podeu habilitar o inhabilitar la informació següent:

Mostra la validesa

Mostra informació sobre la validesa d'un certificat: el seu estat actual, la DN de l'emissor (només S/MIME), les dates d'expiració (si escau) i les etiquetes d'ús del certificat.

Exemple:

```
Aquest certificat és vàlid en l'actualitat.
Emissor:            CN=Test-ZS 7,O=Intevation GmbH,C=DE
Validesa:          des del 25.08.2009 10:42 fins al 19.10.2010 10:42
Ús del certificat: Signatura de correus i fitxers, Encriptatge de ↩
    correus i fitxers
ID de clau:            DC9D9E43
```

Mostra la informació del propietari

Mostra informació sobre el propietari del certificat: assumpte-DN (només S/MIME), ID d'usuari (incloent-hi les adreces de correu electrònic) i confiança de l'usuari (només OpenPGP).

OpenPGP exemple:

```
ID d'usuari:           Gpg4winUserA <gpg4winusera@test.hq>
ID de clau:            C6BF6664
Confiança de l'usuari:        fonamental
```

Exemple S/MIME:

```
Assumpte:           CN=Gpg4winTestuserA,OU=Testlab,O=Gpg4win Project,C= ↩
    DE
t.c.c.:            Gpg4winUserA@test.hq
ID de clau:            DC9D9E43
```

Mostra els detalls tècnics

Mostra la informació tècnica sobre el certificat: número de sèrie (només S/MIME), tipus, empremta digital, i ubicació d'emmagatzematge.

Exemple:

```
Número de sèrie:     27
Tipus de certificat:  1,024-bit RSA (certificat secret disponible)
ID de clau:            DC9D9E43
Empremta digital:       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Emmagatzemada:           en aquest ordinador
```

5.2.2 Configurar les Categories de certificat

Kleopatra us permet personalitzar l'aparença dels certificats en la vista de llista. Inclou mostrar una petita icona, però també podeu influir en els colors de primer pla i de fons (pel text), així com en la lletra.

A cada categoria de certificat en la llista se li assigna un conjunt de colors, una icona (opcional) i una lletra per a quan es mostrin els certificats que pertanyen a aquesta categoria. La llista de categories actua com a vista prèvia de les opcions. Les categories poden ser definides lliurement per l'administrador o l'usuari avançat, mireu Secció 6.2 en capítol 6.

Per a establir o canviar la icona d'una categoria, seleccioneu-la en la llista i premeu el botó **Estableix la icona...**. Apareixerà el diàleg de selecció d'icones estàndard del KDE i podreu seleccionar-ne una d'existent des de la col·lecció del KDE o carregar-ne una de personalitzada.

Per a eliminar una icona, necessiteu prémer el botó **Aparença per defecte**.

Per a canviar el color del text (és a dir, primer pla) d'una categoria, seleccioneu-la en la llista i premeu el botó **Estableix el color del text...**. Apareixerà el diàleg de selecció de color estàndard del KDE i podreu seleccionar o crear un color nou.

El canvi del color de fons es fa de la mateixa manera, simplement premeu **Estableix el color del text...**.

Per a canviar la lletra, bàsicament necessiteu dues opcions:

1. Modificar la lletra estàndard, usada en totes les vistes de llista del KDE.
2. Usar una lletra personalitzada.

La primera opció necessita l'avantatge que la lletra segueixi l'estil que escolliu per a tot el KDE, mentre que l'última us dona control complet sobre la lletra que s'usarà. La decisió és vostra.

Per a utilitzar la lletra estàndard modificada, seleccioneu la categoria de la llista, i marqueu o desmarqueu els modificadors de lletra **Cursiva**, **Negreta** i/o **Ratllat**. Podeu veure immediatament l'efecte en la lletra a la llista de categories.

Per a utilitzar una lletra personalitzada, premeu el botó **Estableix la lletra...**. Apareixerà el diàleg de selecció de la lletra estàndard del KDE i podreu seleccionar la lletra nova.

> NOTA
> Pot seguir utilitzant els modificadors de lletra per a canviar la lletra personalitzada, així com per a modificar la lletra estàndard.

Per a tornar a la lletra estàndard, necessiteu prémer el botó **Aparença per defecte**.

5.2.3 Configurar l'Ordre dels atributs DN

Tot i que els DN són jeràrquics, l'ordre dels components individuals (anomenats DN relatius (les RDN), o atributs DN) no està definit. L'ordre en què es mostren els atributs és, per tant, qüestió de gustos personals o de política d'empresa, d'aquí que sigui configurable al Kleopatra.

> NOTA
> Aquesta opció no només s'aplica al Kleopatra, sinó a totes les aplicacions que utilitzen la seva tecnologia. En el moment d'escriure aquestes línies, entre elles estaven el KMail, el KAddressBook, així com el mateix Kleopatra, per descomptat.

Aquesta pàgina de configuració consta bàsicament de dues llistes, una per als atributs coneguts (**Atributs disponibles**) i una per a descriure l'**Ordre actual dels atributs**.

Ambdues llistes contenen entrades que es descriuen com la forma breu de l'atribut (p. ex., **CN**), així com la manera expandida (**Nom comú**).

La llista **Atributs disponibles** sempre s'ordena alfabèticament, mentre que la llista **Ordre actual dels atributs** reflecteix l'ordre de l'atribut DN configurat: El primer atribut de la llista també és el que es mostra primer.

Tan sols els atributs que es mostren explícitament en la llista **Ordre actual dels atributs**.La resta estan ocults per omissió.

De tota manera, si l'entrada marcador de posició **_X_** (**Tots els altres**) estan en la llista «actual», tots els atributs que sense llistar (siguin o no coneguts) seran inserits al punt **_X_**, en el seu ordre relatiu original.

Un petit exemple ajudarà a aclarir l'assumpte:

Donar el DN

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

l'ordre per omissió dels atributs «CN, L, _X_, OU, O, C» presentarà el DN en el següent format:

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

mentre que «CN, L, OU, O, C» presentarà

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

Per a afegir un atribut a l'ordre de visualització de la llista, seleccioneu-lo en la llista **Atributs disponibles** i premeu el botó **Afegeix a l'ordre actual dels atributs**.

Per a eliminar un atribut de l'ordre de visualització de la llista, seleccioneu-lo en la llista **Atributs disponibles** i premeu el botó **Elimina de l'ordre actual dels atributs**.

Per a moure un atribut al començament (final), seleccioneu-lo en la llista **Ordre actual dels atributs** i premeu el botó **Mou a dalt** (**Mou a baix**).

Per a moure un atribut cap avall (a sota) tan sols una posició, seleccioneu-lo de la llista **Ordre actual dels atributs** i premeu el botó **Mou un amunt** (**Mou un avall**).

5.3 Configurar les Operacions de criptografia

5.3.1 Configurar les Operacions amb correu electrònic

Aquí es poden configurar alguns aspectes de les operacions de correu electrònic del UiServer de Kleopatra. En l'actualitat, només es pot configurar si voleu utilitzar o no el «mode ràpid» per a signar i encriptar missatges de correu electrònic, individualment.

Quan s'habilita el «mode ràpid» no es mostra cap diàleg en signar (encriptar) els correus electrònics, a menys que hi hagi un conflicte que necessiti una resolució manual.

5.3.2 Configurar les Operacions amb fitxers

Aquí podeu configurar alguns aspectes de les operacions amb fitxers del UiServer de Kleopatra. En l'actualitat, només podeu triar el programa de suma de verificació a utilitzar per **CHECKSUM_CREATE_FILES**.

Utilitzeu **Programa de suma de verificació a usar** per a triar quin dels programes de suma de verificació configurats s'ha d'utilitzar en crear fitxers de suma de verificació.

Quan es comproven les sumes de verificació, el programa a utilitzar les troba automàticament, a partir dels noms dels fitxers de suma de verificació trobats.

> NOTA
> L'usuari administrador i l'usuari avançat poden definir quins programes de suma de verificació poden estar a disposició de Kleopatra través de les anomenades «Definicions de la suma de verificació» al fitxer de configuració. Vegeu Secció 6.4 aquí capítol 6 per a més detalls.

5.4 Configurar l'aparença de la validació S/MIME

En aquesta pàgina, podeu configurar certs aspectes de la validació dels certificats de S/MIME.

> NOTA
> En la seva major part, això és simplement una versió més fàcil d'usar de la mateixa configuració que també es troba en Secció 5.5. Tot el que podeu configurar aquí, també ho podeu configurar allà, amb l'excepció de **Comprova la validesa del certificat cada *N* hores**, que és específic de Kleopatra.

El significat de les opcions és el següent:

5.4.1 Configuració de l'interval de comprovació del certificat

Comprova la validesa del certificat cada *N* hores

Aquesta opció permet marcar l'interval de la validesa del certificat. També podeu triar l'interval de comprovació (en hores). L'efecte de marcar l'interval és el mateix que **Visualitza → Torna a mostrar (F5)** , no hi ha cap disposició per a programar l'interval de **Eines → Actualitza els certificats OpenPGP** o **Eines → Actualitza els certificats X.509** .

> NOTA
> La validació es realitza implícitament cada vegada que els fitxers importants en `~/.gnupg` canviïn. Aquesta opció, igual que **Eines → Actualitza els certificats OpenPGP** i **Eines → Actualitza els certificats X.509** , per tant, només afecta els factors externs de validesa del certificat.

5.4.2 Configurar el mètode de validació

Valida els certificats usant les CRL

Si seleccioneu aquesta opció, els certificats S/MIME es validen utilitzant llistes de certificats revocats (les CRL -Certificate Revocation Lists-).

Vegeu **Valida els certificats en línia (OCSP)** pel mètode alternatiu de comprovació de la validesa del certificat.

Valida els certificats en línia (OCSP)

Si seleccioneu aquesta opció, els certificats S/MIME són validats en línia amb el protocol d'estat de certificats en línia (OCSP -Online Certificates Status Protocol-).

> AVÍS
> En triar aquest mètode, s'envia una sol·licitud al servidor de CA més o menys cada vegada que s'envia o es rep un missatge xifrat, el que teòricament permet a l'agència d'emissió de certificats realitzar un seguiment amb qui intercanvieu (p. ex.) correus.

Per a utilitzar aquest mètode, cal introduir l'URL de la resposta OCSP en **URL del contestador OCSP**.
Vegeu **Valida els certificats en línia (OCSP)** per a un mètode més tradicional de comprovar la validació del certificat que no perdi informació sobre amb qui intercanvieu missatges.

URL del contestador OCSP

Introduïu aquí l'adreça del servidor per a la validació de certificats en línia (contestador OCSP). L'URL en general comença amb `http://` .

Signatura del contestador OCSP

Seleccioneu aquí el certificat amb el qual el servidor OCSP signa les seves respostes.

Ignora l'URL de servei dels certificats

Cada certificat S/MIME en general conté l'URL de resposta OCSP del seu emissor (**Certificats → Bolca un certificat** revelarà si un certificat determinat la conté).
En seleccionar aquesta opció fa que GpgSM ometi els URL i només utilitza la configuració de sobre.
Utilitzeu-la per a p. ex., forçar l'ús d'un intermediari OCSP a tota l'empresa.

5.4.3 Configurar les opcions de validació

No comprovar les polítiques del certificat

Per omissió, GpgSM utilitza el fitxer `~/.gnupg/policies.txt` per a comprovar si està permesa la política de certificats. Si seleccioneu aquesta opció, no es comprovaran les polítiques.

No consultar mai una CRL

Si aquesta opció està marcada, no s'empraran mai les llistes de revocació de certificats per a validar els certificats S/MIME.

Permetre marcar els certificats arrel com a fiables

Si aquesta opció està marcada, mentre s'importa un certificat CA arrel, se us demanarà que confirmeu la seva empremta digital i que indiqueu si es té o no com de confiança aquest certificat arrel.
Un certificat arrel necessita ser de confiança abans que els certificats que certifica siguin de confiança, però confiar a la lleugera en certificats arrel en el vostre magatzem de certificats posarà en perill la seguretat del sistema.

> NOTA
> Habilitar aquesta funcionalitat en el dorsal pot produir emergents des de PinEntry en moments inoportuns (p. ex., en la verificació de signatures), i per tant es pot blocar desatenent el processament del correu electrònic. Per aquesta raó, i perquè és convenient per a poder establir la *desconfiança* a un nou certificat arrel de confiança, Kleopatra permet l'ajust manual de la confiança usant **Certificats → Confia en el certificat arrel** i **Certificats → Desconfia del certificat arrel** .
> Aquesta configuració no influeix en la funció de Kleopatra.

Obtén els certificats de l'emissor que falten

Si aquesta opció està marcada, els certificats d'emissor que manquen es recuperen quan és necessari (això s'aplica als mètodes de validació CRL i OCSP).

5.4.4 Configurar les opcions de la petició HTTP

No fer cap sol·licitud HTTP

Inhabilita per complet l'ús de l'HTTP per a S/MIME.

Ignora el punt de distribució CRL mitjançant HTTP dels certificats

Quan se cerca la ubicació d'un CRL, el certificat a provar en general conté el que es coneix com a entrades «CRL Punt de distribució» (DP), que són URL que descriuen la manera d'accedir a la CRL. S'utilitza la primera entrada DP.

Amb aquesta opció, totes les entrades que usin l'esquema HTTP seran ignorades quan se cerca un DP adequat.

Usa l'intermediari HTTP del sistema

Si se selecciona aquesta opció, el valor de l'intermediari HTTP que es mostra a la dreta (provinent de la variable d'entorn `http_proxy`) s'usarà per a totes les peticions HTTP.

Usa aquest intermediari per a les sol·licituds HTTP

Si no s'ha definit cap intermediari del sistema o heu d'utilitzar un intermediari diferent per a GpgSM, introduïu aquí la seva ubicació.

S'utilitzarà per a totes les peticions HTTP relatives a S/MIME.

La sintaxi és **`màquina:port`**, p. ex., **`intermediari.enlloc.com:3128`**.

5.4.5 Configurar les opcions de la petició LDAP

No fer cap sol·licitud LDAP

Inhabilita per complet l'ús de LDAP per a S/MIME.

Ignora el punt de distribució CRL mitjançant LDAP dels certificats

Quan se cerca la ubicació d'un CRL, el certificat a provar en general conté el que es coneix com a entrades «CRL Punt de distribució» (DP), que són URL que descriuen la manera d'accedir a la CRL. S'utilitza la primera entrada DP.

Amb aquesta opció, totes les entrades que usin l'esquema LDAP seran ignorades quan se cerca un DP adequat.

Màquina primària per a sol·licituds LDAP

Introduir aquí un servidor LDAP farà que totes les peticions LDAP vagin primer a aquest servidor. Més precisament, aquesta configuració substitueix qualsevol especificació a la part *`màquina`* i *`port`* en un URL LDAP i també s'utilitzarà si la *`màquina`* i el *`port`* s'han omès a l'URL.

Els altres servidors LDAP només s'utilitzaran si la connexió a l'«intermediari» ha fallat. La sintaxi és **`màquina`** o **`màquina:port`**. Si s'omet el *`port`* , s'utilitzarà el port 389 (el port LDAP estàndard).

5.5 Configurar el sistema GnuPG

Aquesta part del diàleg és autogenerada a partir de la sortida de **gpgconf `--list-components`** i, per a cada *`component`* que retorna l'ordre anterior, la sortida de **gpgconf `--list-options` *`component`***.

> NOTA
> El més útil d'aquestes opcions ha estat duplicat com a pàgines independents en el diàleg de configuració de Kleopatra. Vegeu Secció 5.1 i Secció 5.4 per a les dues pàgines de diàleg que contenen les opcions seleccionades en aquesta part del diàleg.

El contingut exacte d'aquesta part del diàleg depèn de la versió del dorsal de GnuPG que hi hagi instal·lat i, potencialment, la plataforma en què s'executa. Per tant, només analitzarem la disposició general del diàleg, incloent-hi l'assignació des de l'opció de GpgConf al control de l'IGU Kleopatra.

GpgConf retorna informació de configuració per a múltiples components. Dins de cada component, les opcions individuals es combinen en grups.

Kleopatra mostra una pestanya per a cada component informat per GpgConf, els grups estan encapçalats per una línia horitzontal que mostra el nom del grup com l'ha retornat GpgConf.

Cada opció de GpgConf té un tipus. A excepció de certes opcions conegudes que Kleopatra sosté amb controls especialitzats per a una millor experiència d'usuari, l'associació entre tipus de GpgConf i controls de Kleopatra és el següent:

<table>
<tr><th rowspan="2">Tipus de GpgConf</th><th colspan="2">Control de Kleopatra</th></tr>
<tr><th>per a les llistes</th><th>per a no-llistes</th></tr>
<tr><td>none</td><td>Botó de selecció de valors («count»-semantics)</td><td>Casella de selecció</td></tr>
<tr><td>string</td><td>N/A</td><td>Línia d'edició</td></tr>
<tr><td>int32</td><td rowspan="2">Línia d'edició (sense format)</td><td rowspan="2">Botó de selecció de valors</td></tr>
<tr><td>uint32</td></tr>
<tr><td>pathname</td><td>N/A</td><td>control especialitzat</td></tr>
<tr><td>ldap server</td><td>control especialitzat</td><td>N/A</td></tr>
<tr><td>key fingerprint</td><td colspan="2" rowspan="4">N/A</td></tr>
<tr><td>pub key</td></tr>
<tr><td>sec key</td></tr>
<tr><td>alias list</td></tr>
</table>

Taula 5.1: Associació de tipus GpgConf a controls de l'IGU

Consulteu el manual de GpgConf per a obtenir més informació sobre el que podeu configurar aquí, i com.

Capítol 6

Guia de l'administrador

La guia de l'administrador descriu maneres per a personalitzar Kleopatra a les que no es pot accedir mitjançant l'IGU, sinó tan sols amb fitxers de configuració.

S'assumeix que el lector està familiaritzat amb la tecnologia que s'usa per a configurar les aplicacions KDE, incloent-hi la disposició, la ubicació en el sistema de fitxers i la cascada de fitxers de configuració del KDE, així com l'entorn KIOSK.

6.1 Personalització de l'assistent de creació de certificats

6.1.1 Personalitzar els camps de DN

Kleopatra us permet personalitzar els camps que permeten introduir l'usuari per a crear el seu certificat.

Creeu un grup anomenat `CertificateCreationWizard` en el fitxer `kleopatrarc` del sistema. Si voleu que l'ordre dels atributs sigui personalitzat, o si voleu que tan sols apareguin certs elements, creeu una clau anomenada `DNAttributeOrder`. L'argument és un o més d'entre `CN`,`SN`,`GN`,`L`,`T`,`OU`,`O`,`PC`,`C`,`SP`,`DC`,`BC`,`EMAIL`. Si voleu inicialitzar els camps amb algun valor, escriviu quelcom com Atribut=valor. Si voleu que l'atribut sigui requerit, afegiu una marca d'exclamació (per exemple, `CN!`,`L`,`OU`,`O!`,`C!`,`EMAIL!`, el qual resultarà ser la configuració per omissió).

Usant el modificador de mode `$e` de KIOSK, se us permet recuperar els valors de les variables d'entorn o d'un script o binari avaluat. Si voleu desactivar l'edició del camp respectiu, useu el modificador `$i`. Si voleu desactivar l'ús del botó **Insereix la meva adreça**, estabiu `ShowSetWhoAmI` a «false».

> SUGGERIMENT
> Per la naturalesa de l'entorn KIOSK de KDE, usant l'etiqueta immutable (`$i`), fa que sigui impossible per a l'usuari ometre l'etiqueta. És un comportament intencionat. `$i` i `$e` també es poden utilitzar amb totes les claus de configuració de les aplicacions de KDE.

El següent exemple apunta les possibles personalitzacions:

```
[CertificateCreationWizard]
;No permet copiar les dades personals des de la llibreta d'adreces, ni ↩
    sobrepassar localment
ShowSetWhoAmI[$i]=false

;estableix el nom de l'usuari a $USER
```

```
CN[$e]=$USER

;estableix el nom de l'empresa a «La meva empresa», no permet editar
O[$i]=La meva empresa

;estableix el nom del departament segons què retorni l'script
OU[$ei]=$(lookup_dept_from_ip)

;estableix el país a AD, però permet que l'usuari el canviï
C=AD
```

6.1.2 Restringir els tipus de claus que un usuari pot crear

Kleopatra també permet restringir el tipus de certificats que es permet crear a un usuari. Tingueu en compte, però, que una manera fàcil d'evitar aquestes restriccions és crear-ne una a la línia d'ordres.

6.1.2.1 Els algorismes de clau pública

Per a restringir l'algorisme de clau pública a usar, afegiu la clau de configuració `PGPKeyType` (i `CMSKeyType`, però de totes maneres només RSA és compatible amb CMS) a la secció `CertificateCreationWizard` de `kleopatrarc`.

Els valors permesos són `RSA` per a les claus RSA, `DAS` per a les claus DSA (només firma), i `DSA+ELG` per a una clau DSA (només firma) amb una subclau Elgamal per a l'encriptatge.

Per omissió es llegeix GpgConf o bé `RSA` si GpgConf no proporciona un valor per omissió.

6.1.2.2 Mida de la clau pública

Per a restringir la mida de les claus per a un algorisme públic, afegiu la clau de configuració `<ALG>KeySizes` (on *ALG* pot ser `RSA`, `DSA` o `ELG`) a la secció `CertificateCreationWizard` de `kleopatrarc` trobareu una llista separada per comes de mides de claus (en bits). Es pot indicar un valor per omissió pel prefix de la mida de clau amb un guió (-).

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

Això permet restringir la mida de clau RSA de 1536, 2048 i 3072, amb 2.048 el valor per omissió.

A més de les mides en si mateixes, també podeu donar les etiquetes de cadascuna de les mides. Només cal ajustar la clau de configuració `ALGKeySizeLabels` a una llista separada per comes de les etiquetes.

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

Això, en relació amb l'exemple anterior, imprimirà quelcom a les següents opcions per a la selecció:

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

Els valors per omissió són com si el següent estigués en efecte:

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

6.2 Crear i editar categories de claus

Kleopatra permet a l'usuari configurar l'aparença visual de les claus basant-se en un concepte anomenat **Categories de claus**. Aquesta secció descriu com es poden editar les categories disponibles i afegir-ne de noves.

Quan s'intenta localitzar la categoria a la qual pertany una clau, Kleopatra intenta fer coincidir la clau amb una seqüència de filtres de claus, configurats en el fitxer `libkleopatrarc`. El primer que coincideix defineix la categoria, basant-se en un concepte d'*especificitat*, s'explica a continuació.

Cada filtre de clau està definit en un grup de configuració anomenat `Key Filter #n`, en el que *n* és un número, començant pel `0`.

Les úniques claus obligatòries en un grup `Key Filter #n` és `Name`, que contenint el nom de la categoria que es mostrarà en el diàleg de configuració, i `id`, que s'utilitza com a referència pel filtre en altres seccions de la configuració (com ara `View #n`).

Taula 6.1 Llista totes les claus que defineixen les propietats de visualització de claus que pertanyen a aquesta categoria (és a dir, les claus que es poden ajustar en el diàleg de configuració), mentre que Taula 6.2 llista totes les claus que coincideixen amb els criteris definits de filtratge de claus.

Clau a configurar	Tipus	Descripció
`background-color`	color	El color de fons que a usar. Si no s'indica, per omissió serà el color de fons definit globalment per a les vistes de llista.
`foreground-color`	color	El color de primer pla a usar. Si no s'indica, per omissió serà el color de primer pla definit globalment per a les vistes de llista.
`font`	lletra	La lletra personalitzada a usar. La lletra s'escalarà fins a la mida configurada per a les vistes de llista, i s'aplicaran els atributs de lletra (s'expliquen a sota).
`font-bold`	booleà	Si està establert a `true` i `font` no està establert, usa la lletra predeterminada de la vista de llista amb l'estil de lletra negreta afegit (si està disponible). S'ignora si també està present `font`.

font-italic	booleà	Anàleg a font-bold, però amb l'estil de lletra cursiva en comptes de negreta.
font-strikeout	booleà	Si és true, dibuixa una línia per sobre de la lletra. S'aplica encara que estigui establerta font.
icon	text	El nom d'una icona que es mostra en la primera columna. Encara no implementat.

Taula 6.1: Configurar el filtre de clau definint les propietats de visualització

Clau a configurar	**Tipus**	**Si s'especifica, els filtres coincideixen quan...**
is-revoked	booleà	la clau ha estat revocada.
match-context	context[1]	el context en què això coincideix amb el filtre.
is-expired	booleà	la clau ha caducat.
is-disabled	booleà	la clau ha estat inhabilitada (marcada perquè no s'usi) per l'usuari. S'ignora per a claus S/MIME.
is-root-certificate	booleà	la clau és un certificat arrel. S'ignora per a claus OpenPGP.
can-encrypt	booleà	la clau es pot utilitzar per a l'encriptatge.
can-sign	booleà	la clau es pot utilitzar per a signar.
can-certify	booleà	la clau es pot utilitzar per a signar (certificar) altres claus.
can-authenticate	booleà	la clau es pot utilitzar per autenticació (p. ex. com un certificat de client TLS).
is-qualified	booleà	la clau es pot utilitzar per a fer firmes reconegudes (com es defineix en la Llei alemanya de firma digital).
is-cardkey	booleà	el material de claus s'emmagatzema en una targeta intel·ligent (en lloc de l'ordinador).
has-secret-key	booleà	està disponible la clau privada per a aquest parell de claus.

[1] El context és una enumeració amb els següents valors permesos: appearance, filtering i any.

`is-openpgp-key`	booleà	la clau és una clau OpenPGP (`true`), o una clau S/MIME (`false`).
`was-validated`	booleà	la clau ha estat validada.
`prefix-ownertrust`	validity[2]	la clau disposa exactament (*`prefix`* = `is`), ho té tot excepte (*`prefix`* = `is-not`), almenys té (*`prefix`* = `is-at-least`), o a més té (*`prefix`* = `is-at-most`) la confiança del propietari dona el valor de la clau de configuració. Si hi ha més d'una clau `prefix-ownertrust` (amb diferents valors de *`prefix`*) en tan sols un grup, el comportament està sense definir.
`prefix-validity`	validity	Anàleg a `prefix-ownertrust`, però per a la validesa de les claus en comptes de per a la confiança del propietari.

Taula 6.2: Criteri de filtratge definint claus a la configuració de filtres de clau

NOTA

Alguns dels criteris més interessants, com `is-revoked` (està revocada) o `is-expired` (ha caducat) tan sols funcionarà amb claus *validades*, d'aquí que, per omissió, tan sols es comprovi la validesa de les claus per a la revocació i la caducitat, encara que pugueu eliminar aquestes comprovacions extres.

A més de les claus de configuració esmentades anteriorment, un filtre de clau també pot tenir un `id` i `match-contexts`.

L'ús del filtre `id`, que per omissió és el filtre de configuració de nom de grup si no s'indica o és buit, podeu fer referència a la clau del filtre en algun lloc de la configuració, p. ex. en les configuracions de visualització de Kleopatra. La `id` no és interpretada per Kleopatra, així que podeu utilitzar qualsevol cadena que vulgueu, sempre que sigui única.

L'opció `match-contexts` limita l'aplicació del filtre. Hi ha definits dos contexts: el context `appearance` s'utilitza en la definició de color i les propietats de lletra per a les visualitzacions. El context `filtering` s'utilitza per a incloure (i excloure) de manera selectiva certificats de les visualitzacions. El context `any` es pot utilitzar per a indicar tots els contexts definits actualment, i és el per omissió si `match-contexts` no s'ha indicat, o d'altra manera no produeix contexts. Això assegura que un filtre de clau no pot finalitzar «mort», és a dir, sense contexts per a aplicar.

[2] La validesa és una enumeració ordenada amb els següents valors: `unknown` (desconegut), `undefined` (sense definir), `never` (mai), `marginal`, `full` (completa), `ultimate` (definitiva). Vegeu els manuals de GPG i GpgSM per a una explicació detallada.

El format de l'entrada és una llista de símbols, separats per caràcters no-paraula. Cadascun dels símbols és opcionalment precedit per un signe d'exclamació (`!`), que indica negació. Els símbols actuen en ordre sobre una llista interna de contexts, la qual comença buida. Això s'explica millor amb un exemple: `any !appearance` és el mateix que `filtering`, i `appearance !appearance` presentarà el conjunt buit, tal com `!any`. Tanmateix, els dos últims se substitueixen internament per `any`, ja que no produeixen contexts.

En general, els criteris no especificats (és a dir, l'entrada de configuració no està definida) no són comprovats. Si es dona un criteri, es comprova i aquest haurà de coincidir en tot amb el filtre perquè es faci coincidir, és a dir, els criteris són a la vegada AND.

Cada filtre té una «especificitat» implícita que s'utilitza per a classificar tots els filtres que coincideixen. Els filtre més específic guanya sobre els menys específics. Si dos filtres tenen la mateixa especificitat, guanya el que està primer en el fitxer de configuració. L'especificitat d'un filtre és proporcional al nombre de criteris que conté.

Example 6.1 Exemples de filtres de clau

Per a comprovar tots els certificats arrel caducats però no revocats, podeu usar un filtre de claus definit de la manera següent:

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

Per a comprovar que totes les claus OpenPGP inhabilitades (Kleopatra encara no ho permet) amb una confiança del propietari d'almenys «marginal», hauríeu d'usar:

```
[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 Configurar arxivadors per a l'ús amb fitxers signa/encripta

Kleopatra permet a l'administrador (i a l'usuari avançat) configurar la llista d'arxivadors que es presenten en el diàleg de signar/encriptar fitxers.

Cada arxivador es defineix en `libkleopatrarc` com un grup separat `Archive Definition #n`, amb les següents claus obligatòries:

`extensions`
: Una llista separada per comes d'extensions de noms de fitxer que solen indicar aquest format de fitxer.

`id`
: Un ID únic utilitzat per a identificar aquest arxiu internament. En cas de dubte, utilitzeu el nom de l'ordre.

`Name` (traduït)
: El nom visible per l'usuari d'aquest arxivador, com es mostra en el menú desplegable corresponent del diàleg signa/encripta fitxers.

pack-command

L'ordre real per a arxivar fitxers. Podeu utilitzar qualsevol ordre, sempre que no es requereixi un intèrpret d'ordres per a executar-la. El fitxer del programa se cerca amb la variable d'entorn `PATH`, llevat que utilitzeu un camí de fitxer absolut. Les cometes estan suportades com si s'estigués usant un intèrpret d'ordres:

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

NOTA

Atès que la barra inversa (\) és un caràcter d'escapament en els fitxers de configuració del KDE, necessitareu duplicar-la quan aparegui en els noms de camí:

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

. Tanmateix, per l'ordre en si (com oposat als seus arguments), podeu utilitzar només barres inclinades (/) com separadors de camins en totes les plataformes:

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

. Això no s'admet pels arguments, com la majoria dels programes de Windows® utilitzen la barra inclinada per a opcions. Per exemple, el següent no funcionarà, donat que `C:/myarchivescript.bat` és un argument a **cmd.exe**, i / no es converteix en els arguments a \, només en les ordres:

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

. Això es necessita escriure com:

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

6.3.1 Passar el nom de fitxer d'entrada per `pack-command`

Hi ha tres formes de passar noms de fitxer a l'ordre d'empaquetar. Per a cadascuna, `pack-command` proporciona una sintaxi especial:

1. Com a arguments de la línia d'ordres.
   Exemple (tar):

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

   Exemple (zip):

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

   En aquest cas, els noms de fitxer es passen a la línia d'ordres, igual que ho faria quan s'utilitza un indicador d'ordres. Kleopatra no utilitza un intèrpret d'ordres per a executar l'ordre. Per tant, aquesta és una manera segura de passar els noms de fitxer, però podríeu trobar restriccions de longitud de línia d'ordres en algunes plataformes. Si és present un literal `%f`, serà substituït pels noms de fitxer a arxiu. En cas contrari, els noms de fitxer s'afegeixen a la línia d'ordres. Així, l'anterior exemple zip en forma equivalent es pot escriure així:

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

2. Via entrada estàndard, separada per salts de línia: anteposar `|`.
   Exemple (TAR de GNU):

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

Exemple (ZIP):

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

En aquest cas, els noms de fitxer es passen a l'arxivador sobre stdin, un per línia. Això evita problemes en les plataformes que posen un límit sobre el nombre d'arguments de la línia d'ordres que estan permesos, però falla quan els noms de fitxer contenen, en realitat, salts de línia.

> NOTA
> Kleopatra actualment només suporta LF com un separador de salt de línia, no CRLF Això podria canviar en futures versions, basades en comentaris dels usuaris.

3. Via entrada estàndard, separada per octets NUL: anteposar `0|`.
   Exemple (TAR de GNU):

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

Aquest és el mateix que l'anterior, llevat que els octets NUL s'utilitzen per a separar els noms de fitxer. Atès que els octets NUL estan prohibits en els noms de fitxer, aquesta és la forma més robusta de passar els noms de fitxer, però no ho admeten tots els arxivadors.

6.4 Configurar els programes de verificació pel seu ús creant o verificant sumes de verificació

Kleopatra permet a l'administrador (i a l'usuari avançat) configurar la llista de programes de verificació que tria l'usuari en el diàleg de configuració i que Kleopatra és capaç de detectar automàticament quan us demana verificar la suma de verificació d'un fitxer determinat.

> NOTA
> Perquè els pugui utilitzar Kleopatra, la sortida d'un programa de suma de verificació (tant el fitxer de suma de verificació escrit, com la sortida sobre stdout quan es verifiquen les sumes de verificació) ha de ser compatible amb **md5sum** i **sha1sum** de GNU.
> Específicament, els fitxers de suma de verificació han d'estar basats en línies, cada línia amb el següent format:
>
> ```
> SUMA_DE_VERIFICACIÓ ' ' ( ' ' |'*' ) NOM_DE_FITXER
> ```
>
> on *SUMA_DE_VERIFICACIÓ* només consta de caràcters hexadecimals. Si *NOM_DE_FITXER* conté un caràcter de salt de línia, s'haurà de llegir la línia en el seu lloc:
>
> ```
> \SUMA_DE_VERIFICACIÓ ' ' ( ' ' | '*' ) NOM_DE_FITXER_AMB_ESCAPE
> ```
>
> on *NOM_DE_FITXER_AMB_ESCAPE* serà el nom de fitxer amb els salts de línia substituïts per `\n`, les barres inverses inclinades (\↦\\).
> De la mateixa manera, la sortida de `verify-command` ha de ser de la forma
>
> ```
> NOM_DE_FITXER (': OK' | ': FAILED')
> ```
>
> separats per salts de línia. Salts de línia i altres caràcters *no* s'escapen en la sortida.[a]
>
> [a] Sí, aquests programes no van ser escrits amb frontals gràfics en ment, i Kleopatra falla en analitzar correctament els noms de fitxer patològics que contenen «: OK» seguit del salt de línia.

Cada programa de suma de verificació es defineix en `libkleopatrarc` com un grup separat `Checksum Definition #n`, amb les següents claus obligatòries:

`file-patterns`
: Una llista d'expressions regulars que descriuen quins fitxers s'han de considerar com fitxers de suma de verificació per a aquest programa de suma de verificació. La sintaxi és la utilitzada per a les llistes de cadenes en els fitxers de configuració del KDE.

> NOTA
> Com que les expressions regulars solen contenir barres invertides, s'ha de tenir cura d'escaparles adequadament al fitxer de configuració. Es recomana l'ús d'una eina d'edició del fitxer de configuració.

La plataforma permet definir si els patrons són o no tractats distingint majúscules i minúscules.

`output-file`
: La sortida típica pel nom de fitxer per aquest programa de suma de verificació (ha de coincidir amb un dels `file-patterns`, per descomptat). Aquest és el que Kleopatra utilitzarà com a nom de fitxer de sortida en crear fitxers de suma de verificació d'aquest tipus.

`id`
: Un ID únic utilitzat per a identificar aquest programa de suma de verificació internament. En cas de dubte, utilitzeu el nom de l'ordre.

`Name` (traduït)
: El nom visible per l'usuari d'aquest programa de suma de verificació, com es mostra en el menú desplegable corresponent del diàleg de configuració de Kleopatra.

`create-command`
: L'ordre real amb què crear fitxers de suma de verificació. La sintaxi, les restriccions i les opcions de pas d'arguments són les mateixes que les descrites per `pack-command` a Secció 6.3.

`verify-command`
: Igual com `create-command`, però per a la verificació de la suma de verificació.

Aquí tenim un exemple complet:

```
[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
```

Capítol 7

Crèdits i llicència

Kleopatra copyright 2002 Steffen Hansen, Matthias Kalle Dalheimer i Jesper Pedersen, copyright 2004 Daniel Molkentin, copyright 2004, 2007, 2008, 2009, 2010 Klarälvdalens Datakonsult AB

Copyright de la documentació 2002 Steffen Hansen, copyright 2004 Daniel Molkentin, copyright 2004, 2010 Klarälvdalens Datakonsult AB

COL·LABORADORS

- 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

Traductor/Revisor de la documentació: Antoni Bella antonibella5@yahoo.com

Aquesta documentació està llicenciada d'acord amb les clàusules de la Llicència de Documentació Lliure de GNU.

Aquest programa està llicenciat d'acord amb les clàusules de la Llicència Pública General de GNU.