Het handboek van Kleopatra

Marc Mutz
Ontwikkelaar: David Faure
Ontwikkelaar: Steffen Hansen
Ontwikkelaar: Matthias Kalle Dalheimer
Ontwikkelaar: Jesper Pedersen
Ontwikkelaar: Daniel Molkentin
Vertaler/Nalezer: Freek de Kruijf

Het handboek van Kleopatra

Inhoudsopgave

Lijst van tabellen

Samenvatting

Kleopatra is een hulpmiddel voor het beheer van certificaten volgens X.509 en OpenPGP.

Hoofdstuk 1

Inleiding

Kleopatra is het KDE hulpmiddel voor het beheer van certificaten volgens X.509 en OpenPGPin de GpgSM en GPG sleutelringen en voor het ophalen van certificaten uit LDAP en andere servers voor certificaten.

Kleopatra kan gestart worden vanuit het menu van KMail **Hulpmiddelen** → **Certificatenbeheerder**, evenals vanaf de commandoregel. Het Kleopatra programma heeft de naam **`kleopatra`**.

> OPMERKING
> Dit programma is genoemd naar Cleopatra, een beroemde vrouwelijke Egyptische farao die leefde in de tijd van Julius Caesar, waarmee ze een kind had, Caesarion, niet erkent als zijn erfgenaam.
> De naam is gekozen omdat dit programma zijn oorsprong heeft in een Ägypten Projects (Ägypten is Duits voor Egypte). Kleopatra is de Duitse spelling van Cleopatra.

Hoofdstuk 2

Hoofdfuncties

2.1 De lokale sleutelkast bekijken

De hoofd functie van Kleopatra is het weergeven en bewerken van de inhoud van de lokale sleutelkast, wat gelijk is aan het concept sleutelring van GPG, hoewel men deze gelijkenis niet te veel moet doorzetten.

Het hoofdvenster is opgedeeld in het grote gebied voor het weergeven van de sleutels, die bestaat uit verschillende tabbladen, de menubalk en de zoekbalk bovenaan en een statusbalk onderaan.

Elke regel in de lijst met sleutels komt overeen met één certificaat, geïdentificeerd door de zogenaamde **Onderwerp-DN**. DN is een acroniem voor 'Distinguished Name', een hiërarchische identifier, in grote mate overeenkomend met een pad in een bestandssysteem met een ongebruikelijke syntaxis, waarvan verondersteld wordt dat deze een globaal unieke identiteit geeft aan een gegeven certificaat.

Om geldig te zijn en dus bruikbaar, moeten (publieke) sleutels door een CA (Certification Authority) ondertekend zijn. Deze ondertekeningen worden certificaten genoemd, maar de termen 'certificaat' en '(publieke) sleutel' worden uitwisselbaar gebruikt en we zullen ze ook niet in deze handleiding van elkaar onderscheiden, behalve wanneer expliciet genoemd.

CA's moeten op hun beurt worden getekend door andere CA's om geldig te zijn. Natuurlijk moet dit ergens eindigen, dus tekent de CA op het topniveau (root-CA) zijn sleutel met zichzelf (dit wordt zelftekenen genoemd). Root-certificaten moeten dus handmatig geldigheid toegekend worden (gewoonlijk vertrouwen genoemd), bijv. na vergelijking van de vingerafdruk met die op de website van de CA. Dit wordt typisch gedaan door de systeembeheerder of de verkoper van een product dat certificaten gebruikt, maar kan ook gedaan worden door de gebruiker via het commandoregelinterface van GpgSM.

Om te zien welke van de certificaten root-certificaten zijn, schakelt u om naar de hiërarchische modus voor de sleutellijst met **Beeld → Hiërarchische certificatenlijst**.

U kunt de details zien van elk certificaat door er dubbel op te klikken of **Beeld → Details van certificaat** te gebruiken. Deze opent een dialoog die de meest gebruikelijke eigenschappen van het certificaat toont, zijn ketting met certificaten (bijv. de ketting van uitgevers tot op de root-CA) en een dump van alle informatie die de backend uit het certificaat kan halen.

Als u de sleutelkast wijzigt zonder Kleopatra te gebruiken (bijv. met het commandoregelinterface van GpgSM), dan kunt u het beeld vernieuwen met **Beeld → Opnieuw tonen (F5)** .

2.2 Zoeken en importeren van certificaten

Meestal zult u nieuwe certificaten verkrijgen door handtekeningen in e-mails te verifiëren, omdat certificaten meestal ingebed zijn in de gemaakte handtekeningen. Wanneer u echter een e-mail

naar iemand moet zenden, waarmee u nog geen contact hebt gehad, dan moet u het certificaat uit een LDAP-map (hoewel GpgSM dit automatisch kan doen) ophalen of uit een bestand. U moet ook uw eigen certificaat importeren na het ontvangen van het antwoord van de CA op uw verzoek om een certificaat.

Om te zoeken naar een certificaat in een LDAP-directory, selecteert u **Bestand** → **Certificaten op server opzoeken** en voert u enige tekst in (bijv. de naam van de persoon waarvan u het certificaat wilt) in het tekstinvoervak van de dialoog **Certificaten opzoeken op de sleutelserver**, klik daarna op de knop **Zoeken**. De resultaten worden getoond in de lijst met sleutels onder de zoekbalk, waar u certificaten selecteert om ze beter te bekijken door te klikken op de knop **Details** of ze download met **Importeren** in de lokale sleutelkast.

U kunt de lijst met LDAP-servers instellen voor het zoeken in de pagina **Directory Services** van de instellingendialoog van Kleopatra.

Als u het certificaat als een bestand ontvangt, probeer dan **Bestand** → **Certificaten importeren... (Ctrl+I)** . GpgSM moet het formaat van het certificaatbestand begrijpen; kijk in de handleiding van GpgSM voor een lijst van ondersteunde bestandsformaten.

Als u uw eigen sleutelpaar met GpgSM aanmaken niet hebt uitgevoerd, dan moet u ook handmatig de publieke sleutel (evenals de geheime sleutel) importeren uit het PKCS#12-bestand dat u van de CA ontving. U kunt dit op de commandoregel doen met **`kleopatra --import-certificate bestandsnaam`** of in Kleopatra met **Bestand** → **Certificaten importeren... (Ctrl+I)** , zoals u ook zou doen met 'normale' certificaten.

2.3 Nieuwe sleutelparen aanmaken

Het menu-item **Bestand** → **Nieuw certificaat... (Ctrl+N)** start de **Assistent voor aanmaken van een sleutelpaar** die u door een aantal stappen voor het aanmaken van een certificaatverzoek.

Wanneer u klaar bent met een stap in de assistent, druk dan op **Volgende** om naar de volgende stap (of **Terug** om stappen te herzien die al zijn voltooid). Het maken van het certificaatverzoek kan op elk moment worden geannuleerd door op de knop **Annuleren** te drukken.

Op de eerste pagina van de assistent kiest u welk type certificaat u wilt aanmaken:

Een persoonlijk OpenPGP-sleutelpaar aanmaken

OpenPGP sleutelparen worden lokaal aangemaakt en gecertificeerd door uw vrienden en bekenden. Er is geen centrale certificatieautoriteit; in plaats daarvan kan elk individu een persoonlijk ˝Web van vertrouwen˝ door andere sleutelparen te certificeren met zijn eigen certificaat.

U moet een **Naam**, **E-mailadres** en optioneel **Commentaar** invoeren.

Een persoonlijk X.509-sleutelpaar en certificatieverzoek aanmaken

Sleuteparen voor X.509 worden lokaal aangemaakt, maar centraal gecertificeerd door een certificatieautoriteit (CA). Een CA kan een andere CA certificeren, waardoor een centrale, hiërarchische keten van vertrouwen ontstaat.

De volgende stap in de assistent is het invoeren van uw persoonlijke gegevens voor het certificaat. De in te vullen velden zijn:

- **Algemene naam/Common Name (CN):** Uw naam;
- **E-mailadres (EMAIL):** Uw e-mailadres; let er goed op dat dit juist is—dit zal worden gebruikt als het adres waar mensen e-mail naar zenden wanneer ze uw certificaat gebruiken.
- **Locatie (L):** Het dorp of de stad waarin u woont;
- **Organizational unit (OU):** De eenheid in uw organisatie waarin u zich bevindt (bijvoorbeeld, ˝Administratie˝);

- **Organisatie (O):** De organisatie die u vertegenwoordigt (bijvoorbeeld, het bedrijf waarvoor u werkt);
- **Country code/landencode (C):** De tweeletterige code voor het land waarin u woont (bijvoorbeeld, ˝NL˝);

De volgende stap in de assistent is het selecteren of het certificaat in een bestand moet worden opgeslagen of direct verzenden naar een CA. U zult de bestandsnaam of het e-mailadres, waarnaar het certificaatverzoek verzonden moet worden, moeten specificeren.

2.3.1 Een sleutel intrekken

Een verlopen sleutelpaar kan teruggebracht worden in een operationele status zolang u toegang hebt tot de privé sleutel en de wachtwoordzin. Om een sleutelpaar betrouwbaar onbruikbaar te maken moet u het terugtrekken. Terugtrekken wordt gedaan door een speciale handtekening voor terugtrekken aan de sleutel toe te voegen.

Deze handtekening voor terugtrekken is als een apart bestand opgeslagen. Dit bestand kan later geïmporteerd worden in de sleutelring en wordt dan vastgeplakt aan de sleutel waarmee het onbruikbaar wordt. Merk op dat bij het importeren van deze ondertekening naar de sleutel geen wachtwoord is vereist. Daarom moet u deze ondertekening voor terugtrekken op een veilige plek opslaan, gewoonlijk een plek die verschilt van waar uw sleutelpaar is opgeslagen. Een goed advies is om een plek te kiezen die apart van uw computer is, kopieer deze ofwel naar een externe opslag zoals een USB-stick of druk deze af.

Kleopatra biedt geen functie voor het aanmaken van zo'n handtekening voor intrekken op welk moment dan ook, maar u kunt dat doen met de KDE-toepassing KGpg door te kiezen **Sleutels** → **Sleutel intrekken** en, naar keuze, de handtekening voor intrekken direct in uw sleutelring te importeren.

Een alternatieve manier voor het maken van een ˝revocation certificate˝ is met gebruik van GPG direct vanaf de commandoregel: **`gpg --output revocation_certificate.asc --gen-revoke uw_sleutel`**. Het argument *`uw_sleutel`* moet een sleutel specificeren, ofwel de sleutel-ID van uw primaire sleutelpaar of een deel van een gebruikers-ID dat uw sleutelpaar identificeert.

Hoofdstuk 3

Menureferentie

3.1 Menu Bestand

Bestand → Nieuw certificaat... (Ctrl+N)

Maakt een nieuw sleutelpaar (publiek en privé) aan en stelt u in staat om het publieke deel naar een certificatieautoriteit te sturen (CA) ter certificering. Het resulterende certificaat wordt dan naar u teruggezonden of opgeslagen in een LDAP-server zodat u het kunt downloaden in uw lokale sleutelkast, waar u het kan gebruiken om te signeren en e-mails te ontcijferen.

Deze manier van werken wordt 'gedecentraliseerde sleutelgeneratie' genoemd, omdat alle sleutels lokaal worden aangemaakt. Kleopatra (en GpgSM) ondersteunen geen directe 'gecentraliseerde sleutelgeneratie', maar u kunt het publieke/geheime sleutelpaar dat u ontvangt van de CA in het formaat PKCS#12 via **Bestand → Certificaten importeren... (Ctrl+I)** importeren.

Bestand → Certificaten opzoeken op de server... (Ctrl+Shift+I)

Zoekt naar en importeert certificaten op servers voor certificaten naar de lokale sleutelkast. Zie Section 2.2 voor details.
U moet servers voor certificaten hebben geconfigureerd om dit te laten werken. Zie Section 5.1 voor meer details.

Bestand → Certificaten importeren... (Ctrl+I)

Importeert certificaten en/of geheime sleutels uit bestanden in de lokale sleutelkast. Zie Section 2.2 voor details.
Het formaat van het certificaat moet worden ondersteund door GpgSM/GPG. Kijk in de handleiding van GpgSM en GPG voor een lijst van ondersteunde bestandsformaten.

Bestand → Certificaten exporteren... (Ctrl+E)

Exporteert de geselecteerde certificaten naar een bestand.

De extensie van de bestandsnaam die u koos voor het exporteren bepaalt het formaat van het exportbestand:

- Voor OpenPGP-certificaten, resulteren `gpg` en `pgp` in een binair bestand, terwijl `asc` resulteert in een ASCII file.
- Voor S/MIME certificaten, resulteert `der` in een binair, DER-gecodeerd bestand, terwijl `pem` resulteert in een ASCII bestand.

Tenzij meerdere certificaten zijn geselecteerd, zal Kleopatra `vingerafdruk.{asc,pem}` als de naam van het te exporteren bestand voorstellen.

Deze functie is alleen beschikbaar wanneer een of meer certificaten zijn geselecteerd.

> OPMERKING
> Deze functie exporteert alleen de publieke sleutels, zelfs als de geheime sleutel beschikbaar is . Gebruik **Bestand → Geheim sleutels exporteren...** om de geheime sleutels in een bestand te exporteren.

Bestand → Geheim sleutels exporteren...

Exporteert de geheime sleutel naar een bestand.

In de geopende dialoog kunt u kiezen om een binair of ASCII-bestand (**ASCII-bewapend**) voor export aan te maken. Klik vervolgens op het pictogram van de map aan de rechterkant van het tekstvak van het **Uitvoerbestand** en selecteer de map en de naam het exportbestand. Bij exporteren van geheime sleutels van S/MIME kunt u ook de **Tekenset van de wachtwoordzin** kiezen. Zie voor meer details de discussie van de optie `--p12-charset te kenset` in het handboek van GpgSM.

Deze functie is alleen beschikbaar wanneer precies één certificaat is geselecteerd en de geheime sleutel voor dat certificaat beschikbaar is.

> WAARSCHUWING
> Het zou zelden nodig moeten zijn om deze functie te gebruiken, en als dat zo is, dan zou het zorgvuldig gepland moeten worden. De migratie van een geheime sleutel bevat een keuze van het transportmedium en de veilige verwijdering van de sleutelgegevens op de oude machine, evenals die onder andere op het transportmedium.

Bestand → Certificaten naar server exporteren... (Ctrl+Shift+E)

Publiceer de geselecteerde certificaten op een sleutelserver (alleen OpenPGP).

Het certificaat wordt verzonden naar de server voor certificaten geconfigureerd voor OpenPGP (cf. Section 5.1), als die is ingesteld, anders naar `keys.gnupg.net`.

Deze functie is alleen beschikbaar als minstens een OpenPGP (en geen S/MIME) certificaten zijn geselecteerd.

> OPMERKING
> Wanneer OpenPGP-certificaten naar een publieke directory-server geëxporteerd zijn, is het bijna onmogelijk om ze weer te verwijderen. Maak een intrekkingscertificaat aan, voordat u uw certificaten naar de publieke directory-server exporteert, zodat u ze indien nodig later weer kan intrekken.

> OPMERKING
> De meeste publieke OpenPGP servers voor certificaten synchroniseren deze onder elkaar, zodat er weinig reden is ze naar meer dan een server te sturen.
> Het kan zijn dat zoeken op een certificatenserver geen resultaten oplevert zelfs als u zojuist uw certificaat daarheen hebt opgestuurd. Dit is vanwege het feit dat publieke sleutelserveradressen round-robin uit de DNS-server komen om de belasting te balanceren over meerdere machines. Deze machines synchroniseren zich met elkaar, maar gewoonlijk slechts ongeveer elke 24 uur.

Bestand → Ontcijfer/verifieer bestanden...

Ontcijfert bestanden en/of verifieert handtekeningen over bestanden.

Bestand → Onderteken/versleutel bestanden...

Ondertekent en/of versleutelt bestanden.

Bestand → Sluiten (Ctrl+W)

Sluit het hoofdvenster van Kleopatra. U kunt het op elk moment herstellen met het pictogram in het systeemvak.

Bestand → Afsluiten (Ctrl+Q)

Kleopatra wordt beëindigd.

3.2 Menu Beeld

Beeld → Opnieuw tonen (F5)

Ververst de certificatenlijst.

Het gebruik van deze functie is gewoonlijk niet nodig, omdat Kleopatra het bestandssysteem monitort op wijzigingen en automatisch de certificatenlijst ververst indien nodig.

Beeld → Bewerking stoppen (Esc)

Stopt (annuleert) alle gaande acties, bijv. een zoekopdracht, lijst met sleutels tonen of een download.
Deze functie is alleen beschikbaar als minstens een actie actief is.

> OPMERKING
> Vanwege beperkingen in de backend, hangen bewerkingen soms op zo'n manier dat deze functie ze niet direct kan annuleren of zelfs helemaal niet.
> In zulke gevallen is de enige manier om de orde te herstellen het killen van de processen SCDaemon, DirMngr, GpgSM en GPG, in die volgorde, via de systeemhulpmiddelen (**top**, takenbeheerder etc.), totdat de bewerking niet geblokkeerd is.

Beeld → Details van certificaat

Toont de details van het geselecteerde certificaat.

Deze functie is alleen beschikbaar wanneer precies één certificaat is geselecteerd.

Deze functie is ook beschikbaar door direct te dubbelklikken op het overeenkomstige item in de getoonde lijst.

Beeld → Hiërarchische certificatenlijst

Wisselt tussen een hiërarchische en platte modus van de certificatenlijst.

In de hiërarchische modus zijn certificaten gerangschikt in de relatie uitgever/onderwerp, zodat is gemakkelijk is te zien tot welke hiërarchie een gegeven certificaat behoort, maar een gegeven certificaat is initieel moeilijker te vinden (hoewel u natuurlijk de zoekbalk kunt gebruiken).

In platte modus worden alle certificaten in een platte lijst getoond, alfabetisch gesorteerd. In deze modus is een gegeven certificaat gemakkelijk te vinden, maar het is niet direct duidelijk tot welk root-certificaat het behoort.

Deze functie wisselt de hiërarchische modus per tabblad, bijv. elk tabblad heeft zijn eigen hiërarchiestatus. Dit is omdat u zowel een platte als een hiërarchische lijst bij hand kunt hebben, elk in zijn eigen tabblad.

> OPMERKING
> Hiërarchische weergave is nu alleen geïmplementeerd voor S/MIME-certificaten. Er is onder de ontwikkelaars onenigheid over de juiste manier om OpenPGP-certificaten hiërarchisch weer te geven (in wezen, 'ouder = ondertekenaar' of 'ouder = ondertekende').

Beeld → Alles uitvouwen (Ctrl+.)

Vouwt alle items in de lijst in de lijstweergave van de certificaten uit, bijv. maakt alle items zichtbaar.

Dit is de standaard bij het binnengaan in de modus hiërarchische sleutellijst.

U kunt natuurlijk nog steeds elk individueel item invouwen of uitvouwen.

Deze functie is alleen beschikbaar wanneer **Beeld → Hiërarchische certificatenlijst** aan is.

Beeld → Alles invouwen (Ctrl+,)

Vouwt alle items in de lijst met certificaten in, bijv. verbergt alles behalve het bovenste gedeelte van de items.

U kunt natuurlijk nog steeds elk individueel item invouwen of uitvouwen.

Deze functie is alleen beschikbaar wanneer **Beeld → Hiërarchische certificatenlijst** aan is.

3.3 Menu met certificaten

Certificaten → Eigenaarvertrouwen wijzigen...

Wijzigt het vertrouwen in de eigenaar van het geselecteerde OpenPGP-certificaat.

Deze functie is alleen beschikbaar wanneer precies één OpenPGP-certificaat is geselecteerd.

Certificaten → Hoofdcertificaat vertrouwen

Markeert dit (S/MIME)-hoofdcertificaat als vertrouwd.

Op een bepaalde manier is dit het equivalent van **Certificaten → Eigenaarvertrouwen wijzigen...** voor S/MIME-hoofdcertificaten. U kunt echter alleen kiezen tussen—in OpenPGP termen—'volledig' vertrouwen en 'geen vertrouwen'.

> OPMERKING
> De backend (via GpgAgent) zal op het moment van het importeren van het hoofdcertificaat of het geïmporteerde hoofdcertificaat is te vertrouwen. Die functie moet expliciet worden ingeschakeld in instellingen van de backend (`allow-mark-trusted` in `gpg-agent.conf` of ofwel **GnuPG-systeem → GPG-agent → Sta clients toe om sleutels als ˝vertrouwd˝ te markeren** ofwel **S/MIME-validatie → Sta toe hoofdcertificaten als vertrouwd te markeren** onder hoofdstuk 5).
> Die functionaliteit in de backend inschakelen kan leiden tot popups van PinEntry op ongewenste tijden (bijv. bij het verifiëren van handtekeningen) en kan dus onbewaakte e-mailverwerking blokkeren. Daarom en omdat het gewenst is om in staat te zijn een vertrouwd hoofdcertificaat opnieuw te *wantrouwen*, staat Kleopatra handmatig instellen van vertrouwen toe.

> WAARSCHUWING
> Vanwege het ontbreken van ondersteuning voor deze functie door een backend, is het nodig dat Kleopatra direct op de vertrouwensdatabase (`trustlist.txt`) van GpgSM werkt. Bij het gebruiken van deze functie moet u er zeker van zijn dat er geen andere versleutelingsbewerkingen bezig zijn die concurreren met Kleopatra voor wijzigingen in die database.

Deze functie is alleen beschikbaar wanneer precies één S/MIME-hoofdcertificaat is geselecteerd en dat certificaat nog niet vertrouwd wordt.

Gebruik **Certificaten → Wantrouw hoofdcertificaat** om deze functie ongedaan te maken.

Certificaten → Wantrouw hoofdcertificaat

Markeert dit S/MIME-hoofdcertificaat als niet vertrouwd.

Deze functie is alleen beschikbaar wanneer precies één S/MIME-hoofdcertificaat is geselecteerd en dat certificaat wordt nu vertrouwd.

Gebruikt om **Certificaten → Hoofdcertificaat vertrouwen** ongedaan te maken. Zie aldaar voor details.

Certificaten → Certificeer certificaat...

Stelt u in staat om een ander OpenPGP-certificaat te certificeren.

Deze functie is alleen beschikbaar als precies één OpenPGP-certificaat is geselecteerd.

Certificaten → Vervaldatum wijzigen...

Stelt u in staat om de vervaldatum van uw OpenPGP-certificaat te wijzigen.

Gebruik deze functie om de leeftijd van uw OpenPGP-certificaten, als alternatief voor ofwel een nieuwe aanmaken of een onbeperkte leeftijd te gebruiken ('vervalt nooit').

Deze functie is alleen beschikbaar als precies één certificaat is geselecteerd en de geheime sleutel voor dat certificaat beschikbaar is.

Certificaten → Wachtwoordzin wijzigen...

Stelt u in staat om de wachtwoordzin van uw geheime sleutel te wijzigen.

Deze functie is alleen beschikbaar als precies één certificaat is geselecteerd en de geheime sleutel beschikbaar is voor dat certificaat. Het vereist een erg recente backend, omdat we de implementatie van het direct aanroepen van GPG en GpgSM hebben gewijzigd tot een op GpgME gebaseerde.

> OPMERKING
> Uit veiligheidsredenen, wordt zowel de oude als de nieuwe wachtwoordzin gevraagd door PinEntry, een separaat proces. Afhankelijk van het platform waarop u werkt en de kwaliteit van de implementatie van PinEntry op dat platform, kan het zijn dat het venster van PinEntry opkomt in de achtergrond. Dus als u deze functie selecteert en er gebeurt niets, controleer dan taakbalk van het besturingssyteem in geval een venster van PinEntry geopend is in de achtergrond.

Certificaten → Gebruikers-id toevoegen...

Stelt u in staat om een nieuwe gebruikers-id aan uw OpenPGP-certificaat toe te voegen.

Gebruik dit om nieuwe identiteiten aan een bestaand certificaat toe te voegen als alternatief voor het aanmaken van een nieuw sleutelpaar. Een OpenPGP gebruikers-id heeft de volgende vorm:

```
Echte naam (Commentaar) <E-mailadres>
```

In de dialoog die verschijnt wanneer u deze functie selecteert, zal Kleopatra u apart vragen naar elk van de drie parameters (*Echte naam*, *Commentaar* en *E-mailadres*) en het resultaat aan u tonen.

> OPMERKING
> Deze parameters zijn onderworpen aan dezelfde beheerdersbeperkingen als in nieuwe certificaten. Zie Section 2.3 en Section 6.1 voor details.

Deze functie is alleen beschikbaar als precies één OpenPGP-certificaat is geselecteerd en de geheime sleutel voor dat certificaat beschikbaar is.

Certificaten → Verwijderen (Del)

Verwijdert de geselecteerde certificaten uit de lokale sleutelring.

Gebruik deze functie om ongebruikte sleutels uit uw lokale sleutelkast te verwijderen. Certificaten zijn typisch vastgemaakt aan ondertekende e-mails, verifiëren van een e-mail kan er in resulteren dat de zojuist verwijderde weer de kop op steekt in de lokale sleutelkast. Het is dus waarschijnlijk het beste om deze functie zo min mogelijkheid te gebruiken. Als u zich verloren voelt, gebruik dan de zoekbalk of de functie **Beeld → Hiërarchische certificatenlijst** om de controle terug te krijgen over de meeste certificaten.

> WAARSCHUWING
> Er is één uitzondering op het bovenstaande: Als u een van uw eigen certificaten verwijdert, dan verwijdert u daarmee ook de geheime sleutel. Dat betekent dat u niet in staat zult zijn om vroeger met dit certificaat versleutelde communicatie te lezen, tenzij u nog ergens een reservekopie hebt. Kleopatra zal u waarschuwen wanneer u een geheime sleutel probeert te verwijderen.

Vanwege de hiërarchische natuur van S/MIME-certificaten is het zo dat, als u een S/MIME-certificaat van een uitgever (CA-certificaat) verwijdert, alle afgeleiden ook worden verwijderd.[1]

Natuurlijk is deze functie alleen beschikbaar als u minstens één certificaat hebt geselecteerd.

Certificaten → Certificaat dumpen

Toont alle informatie die GpgSM heeft over het geselecteerde (S/MIME-) certificaat.

Zie de discussie over `--dump-key sleutel` in het handboek van GpgSM voor details over de uitvoer.

3.4 Menu hulpmiddelen

Hulpmiddelen → GnuPG-logweergave...

Start KWatchGnuPG, een hulpmiddel om de debuguitvoer van GnuPG toepassingen te tonen. Als ondertekenen, versleutelen of verifiëren mysterieus stop met werken, dan kunt misschien vinden waarom door in de log te kijken.

Deze functie is niet beschikbaar onder Windows®, omdat de onderliggende mechanismen niet in de backend op dat platform zijn geïmplementeerd.

Hulpmiddelen → OpenPGP-certificaten verversen

Alle OpenPGP-certificaten verversen door het uitvoeren van

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

Na succesvolle uitvoering van het commando, bevat uw lokale sleutelbos de laatste wijzigingen met betrekking tot de geldigheid van OpenPGP-certificaten.

Zie de opmerking onder **Hulpmiddelen → X.509-certificaten verversen** voor enige valkuilen.

Hulpmiddelen → X.509-certificaten verversen

Alle S/MIME-certificaten verversen door het uitvoeren van

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

[1] Dit is hetzelfde als een bestandssysteem: wanneer u een map verwijdert, verwijdert u ook alle bestanden en mappen erin.

Na succesvolle uitvoering van het commando bevat uw lokale sleutelbos de laatste wijzigingen met betrekking tot de geldigheid van S/MIME-certificaten.

> OPMERKING
> Het verversen van X.509 of OpenPGP certificaten houdt in het downloaden van alle certificaten en CRL's, om te controleren of ze intussen zijn ingetrokken.
> Dit kan een zware belasting zijn voor uw eigen en andermans netwerk en kan meer dan een uur duren, afhankelijk van de netwerkverbinding en het aantal te controleren certificaten.

Hulpmiddelen → CRL uit een bestand importeren...

Laat u handmatig CRL's uit bestanden importeren.

Normaal worden 'Certificate Revocation Lists' (CRL's) transparent afgehandeld door de backend, maar soms kan het nuttig zijn om een CRL handmatig te importeren in de lokale CRL-cache.

> OPMERKING
> Om het importeren van CRL te laten werken moet het hulpmiddel DirMngr in `PATH` zijn te vinden. Als dit menu-item is uitgeschakeld, dan zou u contact met de systeembeheerder moeten opnemen en hem vragen DirMngr te installeren.

Hulpmiddelen → CRL-cache wissen

Wist de CRL-cache van GpgSM.

U hebt dit waarschijnlijk nooit nodig. U kunt het verversen van de CRL-cache forceren door alle certificaten te selecteren en in plaatst daarvan **Hulpmiddelen → X.509-certificaten verversen** te gebruiken.

Hulpmiddelen → CRL-cache dumpen

Toont de gedetailleerde inhoud van de CRL-cache van GpgSM.

3.5 Menu Instellingen

Kleopatra heeft een standaard **Instellen**-menu voor KDE, zoals is beschreven in de Basisinformatie van KDE met één extra item:

Instellingen → Zelftest uitvoeren

Een set zelftesten uitvoeren en hun resultaat laten zien.
Dit is dezelfde set testen die bij opstarten standaard worden uitgevoerd. Als u de zelftesten bij opstarten hebt uitgeschakeld, dan kunt u ze hier weer aanzetten.

3.6 Venstermenu

Het menu **Venster** stelt u in staat om de tabbladen te beheren. Met de items in dit menu kunt u een tabblad hernoemen, toevoegen, het huidige tabblad dupliceren, sluiten en naar links of rechts verplaatsen.

Door met de rechtermuisknop op een tabblad te klikken opent u een contextmenu, waarin u ook dezelfde acties kunt selecteren.

3.7 Menu Help

Kleopatra heeft een standaard **Help**-menu voor KDE, zoals is beschreven in de Basisinformatie van KDE .

Hoofdstuk 4

Naslag van opties op de commandoregel

Alleen de opties die specifiek zijn voor Kleopatra worden hier weergegeven. Zoals met alle KDE-toepassingen, kunt u een complete lijst met opties krijgen met het commando **kleopatra --help**.

--uiserver-socket ***argument***
: Locatie van de socket waarnaar de ui-server luistert

--daemon
: Alleen UI-server uitvoeren, hoofdvenster verbergen

-p --openpgp
: OpenPGP voor de volgende actie gebruiken

-c --cms
: CMS (X.509, S/MIME) voor de volgende actie gebruiken

-i --import-certificate
: Specificeert een bestand of URL waar vandaan certificaten (of geheime sleutels) geïmporteerd moeten worden.
Dit is het equivalent op de commandoregel van **Bestand → Certificaten importeren... (Ctrl+I)** .

-e --encrypt
: Bestand(en) versleutelen

-s --sign
: Bestand(en) ondertekenen

-E --encrypt-sign
: Versleutel en/of onderteken bestand(en). Zelfde als `--sign-encrypt`, niet gebruiken

-d --decrypt
: Bestand(en) ontcijferen

-V --verify
: Bestand/ondertekening verifiëren

-D --decrypt-verify
: Bestand(en) ontcijferen en/of verifiëren

Hoofdstuk 5

Kleopatra instellen

De instellingendialoog van Kleopatra kan bereikt worden via **Instellingen** → **Kleopatra instellen...**
Elk van zijn pagina's wordt in de secties hieronder beschreven.

5.1 Directory Services instellen

Op deze pagina kunt u instellen welke LDAP-servers te gebruiken voor het zoeken naar S/MIME-certificaten en welke sleutelservers te gebruiken voor zoeken naar OpenPGP-certificaten.

> OPMERKING
> Dit is eenvoudig een meer gebruikersvriendelijke versie van dezelfde instellingen die u ook vindt in Section 5.5. Alles wat u hier in kan stellen, kunt u ook daar instellen.

> EEN OPMERKING OVER PROXY-INSTELLINGEN
> Proxy-instellingen kunne worden geconfigureerd voor HTTP en LDAP in Section 5.4, maar alleen voor GpgSM. Voor GPG, vanwege de complexiteit van de opties voor de keyserver in GPG en het ontbreken van voldoende ondersteuning hiervoor in GpgConf, moet u het configuratiebestand `gpg.conf` direct wijzigen. Kijk in het handboek van GPG voor details. Kleopatra zal zulke instellingen bewaren, maar laat ze nog niet wijzigen in de GUI.

De tabel **Directory services** toont welke servers op dit moment zijn ingesteld. Dubbelklik op een cel in de tabel om parameters van bestaande servers te wijzigen.

De betekenis van de kolommen in de tabel is als volgt:

Schema

Bepaalt het te gebruiken netwerkprotocol voor toegang tot de server. Vaak gebruikt schema's omvatten **ldap** (en zijn SSL-beveiligde tweeling **ldaps**) voor LDAP servers (algemeen protocol voor S/MIME; de enige ondersteund door GpgSM) en **hkp**, het Horowitz Keyserver Protocol, nu is gebruikelijk HTTP Keyserver Protocol, een op het HTTP protocol gebaseerd dat door vrijwel alle publieke OpenPGP keyservers wordt ondersteund.

Kijk in de handleiding van GPG en GpgSM voor een lijst van ondersteunde schema's.

Servernaam
De domeinnaam van de server, bijv. `keys.gnupg.net`.

Poort van server
De netwerkpoort waarop de server luistert.

Dit verandert automatisch naar de standaard poort wanneer u de **Schema**, tenzij het eerst was ingesteld op een niet-standaard poort. Als u de standaard poort hebt gewijzigd en niet terug kan gaan, probeer dan **Schema** naar **`http`** en **Poort van server** naar **`80`** (de standaard voor HTTP) in te stellen en ga dan daar vanaf verder.

Basis-DN
De basis-DN (alleen voor LDAP en LDAPS) is, bijv. het begin van de LDAP hiërarchie om vanaf te starten. Dit wordt vaak ook de 'zoek-root' of 'zoekbasis' genoemd.

Gewoonlijk lijkt het op **`c=nl,o=Foo`**, opgegeven als deel van de LDAP URL.

Gebruikersnaam
De gebruikersnaam, indien nodig, te gebruiken voor aanmelden aan de server.

Deze kolom wordt alleen getoond als de optie **Gebruiker- en wachtwoordinformatie tonen** (onder de tabel) is geactiveerd.

Wachtwoord
De wachtwoord, indien nodig, te gebruiken voor aanmelden aan de server.

Deze kolom wordt alleen getoond als de optie **Gebruiker- en wachtwoordinformatie tonen** (onder de tabel) is geactiveerd.

X.509
Activeer deze kolom als dit item gebruikt moet worden voor zoeken naar X.509 (S/MIME) certificaten.
Alleen LDAP (en LDAPS) servers worden voor S/MIME ondersteund.

OpenPGP
Activeer deze kolom als dit item gebruikt moet worden voor zoeken naar OpenPGP certificaten.

U kunt zoveel S/MIME (X.509) servers instellen als u wilt, maar alleen één OpenPGP server is tegelijk toegestaan. De GUI zal dat afdwingen.

Om een nieuwe server toe te voegen klikt u op de knop **Nieuw**. Dit dupliceert het geselecteerde item, indien aanwezig, of voegt een standaard OpenPGP server in. Daarna kunt u de **Servernaam**, de **Poort van server**, de **Basis-DN** en de gebruikelijke **Wachtwoord** en **Gebruikersnaam** instellen, die beiden alleen nodig zijn als de server authenticatie vereist.authentication.

Om direct een item voor X.509 certificaten in te voegen, gebruikt u **Nieuw** → **X.509**; gebruik **Nieuw** → **OpenPGP** voor OpenPGP.

Om een server uit de zoeklijst te verwijderen, selecteert u deze in de lijst en drukt daarna op de knop **Verwijderen**.

Om de timeout van LDAP in te stellen, bijv. de maximum tijd die de backend zal wachten op een antwoord van de server, gebruikt u eenvoudig het overeenkomstige invoerveld met het label **LDAP-timeout (minuten:seconden)**.

Als een van uw servers een grote database heeft, zodat zelfs redelijke zoekopdrachten zoals **`Jans en`** het **maximale aantal per query teruggegeven items** overstijgen, dan zou u deze limiet willen vergroten. U kunt gemakkelijk te weten komen of u de limiet bij een zoekopdracht overschrijdt, omdat er in dat geval een dialoogvenster te voorschijn komt, die u vertelt dat de resultaten zijn afgekort.

> OPMERKING
> Sommige servers kunnen hun eigen limieten over het aantal terug te geven items op een query hebben. In dat geval, zal het verhogen van de limiet hier niet resulteren in meer teruggegeven items.

5.2 Het uiterlijk instellen

5.2.1 Tekstballonnen instellen

In de hoofdlijst van certificaten kan Kleopatra details tonen over een certificaat in een tekstballon. De getoonde informatie is dezelfde als in het tabblad **Overzicht** van de dialoog **Details van certificaten**. Tekstballonnen kunnen echter beperkt worden om alleen een subset van de informatie te tonen voor een minder uitgebreide ervaring.

> OPMERKING
> De **Key-ID** wordt *altijd* getoond. Dit is om te verzekeren dat tekstballonnen voor verschillende certificaten ook echt verschillen (dit is speciaal belangrijk als alleen **Geldigheid tonen** zijn geselecteerd).

U kunt onafhankelijk de volgende informatiesets in- of uitschakelen:

Geldigheid tonen

Toont informatie over de geldigheid van een certificaat: zijn huidige status, uitgever-DN (alleen S/MIME), verloopdatum (indien aanwezig) en gebruiksvlaggen voor gebruik.

Voorbeeld:

```
Dit certificaat is nu geldig.
Uitgever:          CN=Test-ZS 7,O=Intevation BV,C=NL
Geldigheid:        vanaf 25.08.2009 10:42 tot 19.10.2010 10:42
Certificaatgebruik: E-mails en bestanden, versleuteling e-mails en ↩
    bestanden
Key-ID:            DC9D9E43
```

Eigenaarsinformatie tonen

Toon informatie over de eigenaar van het certificaat: subject-DN (alleen S/MIME), gebruiker-ID's (inclusief e-mailadressen) en vertrouwen in eigenaar (alleen OpenPGP).

OpenPGP voorbeeld:

```
Gebruiker-ID:         Gpg4winUserA <gpg4winusera@test.hq>
Key-ID:               C6BF6664
Gebruikersvertrouwen: ultimate
```

S/MIME voorbeeld:

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

Technische details tonen

Toont technische informatie over het certificaat: serienummer (alleen S/MIME), type, vingerafdruk en opslaglocatie.

Voorbeeld:

```
Serienummer:       27
Certificaattype:  1,024-bit RSA (geheime certificaat beschikbaar)
Key-ID:            DC9D9E43
Vingerafdruk:       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Opgeslagen:            op deze computer
```

5.2.2 Certificaatcategorieën instellen

Kleopatra stelt u in staat om het uiterlijk van certificaten in de lijstweergave aan te passen. Dit omvat het tonen van een klein pictogram, maar u kunt ook de voorgrond (tekst) en achtergrondkleuren beïnvloeden, evenals het lettertype.

Iedere categorie van certificaten in de lijst heeft een set kleuren, een pictogram (optioneel) en een lettertype toegewezen waarin certificaten in die categorie worden weergegeven. De lijst met categorieën fungeert ook als een overzicht van de instellingen. Categorieën kunnen vrij worden gedefinieerd door de beheerder of de zware gebruiker, zie Section 6.2 in hoofdstuk 6.

Om het pictogram van een categorie in te stellen of te wijzigen, selecteert u deze in de lijst en drukt op de knop **Pictogram instellen...**. De standaard dialoog voor selectie van een KDE-pictogram zal verschijnen, waarin u kunt een bestaand pictogram uit de KDE-verzameling kunt selecteren of een eigen exemplaar kunt laden.

Om een pictogram opnieuw te verwijderen moet u de knop **Standaard uiterlijk** indrukken.

Om de tekstkleur (bijv. voorgrond) van een categorie te wijzigen, selecteert u het in de lijst en drukt op de knop **Tekstkleur instellen...**. De standaard kleurkeuzedialoog van KDE zal verschijnen waar u een bestaande kleur kiest of een nieuwe aanmaakt.

De achtergrondkleur veranderen wordt op dezelfde manier gedaan, druk in plaats daarvan eenvoudig op **Achtergrondkleur instellen...**.

Om het lettertype te wijzigen hebt u in principe twee opties:

1. Verander het standaard lettertype, dat wordt gebruikt voor alle weergave van lijsten in KDE.
2. Een aangepast lettertype gebruiken.

De eerste optie heeft het voordeel dat het lettertype elke stijl volgt die u kiest voor geheel KDE, terwijl de laatste u volledige controle geeft over het te gebruiken lettertype. De keuze is aan u.

Om het gewijzigde standaard lettertype te gebruiken, selecteert u de categorie in de lijst en activeert of deactiveert u de modifiers van lettertypen **Cursief**, **Vet** en/of **Doorstrepen**. U kunt onmiddellijk het effect zien op het lettertype in de lijst met categorieën.

Om een eigen lettertype te gebruiken, drukt u op de knop **Lettertype instellen...**. De standaard lettertypeselectiedialoog van KDE zal verschijnen waar u het nieuwe lettertype kunt selecteren.

> OPMERKING
> U kunt nog steeds de lettertype-modifiers gebruiken om het eigen lettertype te wijzigen, net als voor het wijzigen van het standaard lettertype.

Om terug te schakelen naar het standaard lettertype moet u de knop **Standaard uiterlijk** indrukken.

5.2.3 De DN-attribuutvolgorde

Hoewel DN's hiërarchisch zijn, is de volgorde van de individuele componenten (relatieve DN's genoemd (RDNs) of DN-attributen) niet gedefinieerd. De volgorde waarin de attributen getoond worden is dus een zaak van persoonlijke smaak of bedrijfsbeleid, dat is waarom het in Kleopatra is in te stellen.

> OPMERKING
> Deze instelling is niet alleen van toepassing op Kleopatra, maar op alle toepassen die Kleopatra-technologie gebruiken. Op het moment van schrijven hiervan omvat dit KMail, KAddressBook, evenals Kleopatra zelf, natuurlijk.

Deze configuratiepagina bestaat in de basis uit twee lijsten, een voor de bekende attributen (**Beschikbare attributen**) en met de beschrijving van **Huidige attribuutvolgorde**.

Beide lijsten bevatten items beschreven door de korte vorm van het attribuut (bijv. **CN**) evenals de volledige vorm (**Common Name**).

De lijst **Beschikbare attributen** is altijd alfabetisch gesorteerd, terwijl de **Huidige attribuutvolgorde** de volgorde van de lijst van de ingestelde attribuutvolgorde van DN weergeeft: het eerste attribuut in de lijst is ook als eerste weergegeven.

Alleen expliciet in de lijst opgenomen attributen in de lijst met de **Huidige attribuutvolgorde** worden überhaupt getoond. De rest is standaard verborgen.

Wanneer echter het plaatshouderitem **_X_** (**Alle anderen**) in de 'huidige' lijst staat, worden alle niet in lijst opgenomen attributen (bekend of niet) ingevoegd op het punt van de **_X_** in hun originele relatieve volgorde.

Een klein voorbeeld zal helpen dit helderder te maken:

Gegeven de DN

O=KDE, C=NL, CN=David Ontwikkel, X-BAR=foo, OU=Kleopatra, X-FOO=bar,

zal de standaard volgorde van attributen 'CN, L, _X_, OU, O, C' de volgende geformatteerde DN produceren:

CN=David Ontwikkel, X-BAR=foo, X-FOO=bar, OU=Kleopatra, O=KDE, C=NL

terwijl 'CN, L, OU, O, C' zal produceren

CN=David Ontwikkel, OU=Kleopatra, O=KDE, C=NL

Om een attribuut aan de lijst met weergavevolgorde toe te voegen, wordt het geselecteerd in de lijst **Beschikbare attributen** en daarna op de knop **Aan huidige attribuutvolgorde toevoegen** drukken.

Om een attribuut uit de lijst met weergavevolgorde te verwijderen, wordt het geselecteerd in de lijst **Huidige attribuutvolgorde** en daarna op de knop **Uit huidige attribuutvolgorde verwijderen** drukken.

Om een attribuut naar het begin (einde) te verplaatsen wordt het geselecteerd in de lijst **Huidige attribuutvolgorde** en daarna op de knop **Naar de top verplaatsen** (**Naar onderaan verplaatsen**) drukken.

Om een attribuut één omhoog (omlaag) te verplaatsen, wordt het geselecteerd in de lijst **Huidige attribuutvolgorde** en daarna op de knop **Één naar boven verplaatsen** (**Één naar beneden verplaatsen**) drukken.

5.3 Cryptografische bewerkingen instellen

5.3.1 E-mail bewerkingen instellen

Hier kunt u enige aspecten van de e-mail bewerkingen van de UiServer van Kleopatra instellen. Op dit moment kunt u alleen instellen of u 'Snelle modus' voor ondertekenen en versleutelen van e-mails wilt gebruiken of niet.

Met 'Snellemodus 'geactiveerd, wordt er geen dialoog getoond bij respectievelijk ondertekening (versleuteling) van e-mails, tenzij er een conflict is dat handmatig oplossen vereist.

5.3.2 Bestandsbewerkingen instellen

Hier kunt u enkele aspecten van de bestandsbewerkingen van Kleopatra's UiServer instellen. Op dit moment kunt u alleen het te gebruiken controlesomprogramma voor **CHECKSUM_CREATE_FILES** kiezen.

Gebruik **Te gebruiken controlesomprogramma** om te kiezen welk van de geconfigureerde controlesomprogramma 's gebruikt zou moeten worden bij het aanmaken van controlsombestanden.

Bij het verifiëren van controlesommen wordt het te gebruiken programma automatisch gevonden, gebaseerd op de gevonden controlesombestanden.

> OPMERKING
> De systeeembeheerder en grootgebruiker kunnen volledig definiëren welke programma's voor een controlesom beschikbaar gemaakt wordt aan Kleopatra via de zogenaamde 'Controlesomdefinities' in het instellingenbestand. Zie Section 6.4 in hoofdstuk 6 voor details.

5.4 Aspecten van S/MIME-validatie instellen

Op deze pagina kunt u bepaalde aspecten van de validatie van S/MIME-certificaten instellen.

> OPMERKING
> Dit is grotendeels eenvoudig een meer gebruikersvriendelijke versie van dezelfde instellingen die u ook vindt in Section 5.5. Alles wat u hier in kan stelen, kunt u ook daar met uitzindering van **Geldigheid van certificaat elke *N* uren controleren**, wat specifiek voor Kleopatra is.

De betekenis van de opties is als volgt:

5.4.1 Regelmatige controle van certificaten instellen

Geldigheid van certificaat elke *N* uren controleren

Deze optie activeert het regelmatig controleren van geldigheid van certificaten. Ook kan het tijdinterval (in uren) ingesteld worden. Het effect van regelmatig controleren is hetzelfde als **Beeld** → **Opnieuw tonen** (**F5**) ; er is geen voorziening voor regelmatig controleren van **Hulpmiddelen** → **OpenPGP-certificaten verversen** of **Hulpmiddelen** → **X.509-certificaten verversen** .

> OPMERKING
> Validatie wordt impliciet uitgevoerd wordt wanneer belangrijke bestanden in `~/.gnupg` veranderen. Deze optie, evenals **Hulpmiddelen** → **OpenPGP-certificaten verversen** en **Hulpmiddelen** → **X.509-certificaten verversen** , heeft daarom alleen effect bij externe factoren van de geldigheid van een certificaat.

5.4.2 Validatiemethode instellen

Certificaten met CRL's valideren

Wanneer deze optie is geselecteerd, zullen S/MIME-certificaten gevalideerd worden met Certificate Revocation Lists (CRL's).

Zie **Certificaten online valideren (OCSP)** voor een alternatieve methode van het controleren van de geldigheid van een certificaat.

Certificaten online valideren (OCSP)

Als deze optie ingeschakeld is, worden S/MIME-certificaten gevalideerd met gebruikmaking van het Online Certificates Status Protocol (OCSP).

> WAARSCHUWING
> Bij het kiezen van deze methode wordt er een verzoek naar de server van de CA verzonden, meer of minder elke keer dat u een versleuteld bericht verzendt of ontvangt, dus theoretisch stelt u de uitgevende organisatie van uw certificaat in staat om na te gaan met wie u (bijv.) e-mails uitwisselt.

Om deze methode te kunnen gebruiken moet u de URL van de OCSP server invoeren in **URL-adres OCSP-dienst**.

Zie **Certificaten online valideren (OCSP)** voor een meer traditionele methode van het controleren van de geldigheid van een certificaat die geen informatie lekt met wie u berichten uitwisselt.

URL-adres OCSP-dienst

Voer hier het adres in van de server die de certificaten online valideert (OCSP-dienst). Het URL-adres begint doorgaans met `http://` .

Handtekening OCSP-dienst

Hier het certificaat kiezen waarmee de OCSP-server zijn antwoorden ondertekend.

Service-URL van certificaten negeren

Elk S/MIME-certificaat bevat gewoonlijk de URL van de OCSP van de server van zijn uitgever (**Certificaten → Certificaat dumpen** toont of een gegeven certificaat deze bevat).

Het activeren van deze optie zorgt ervoor dat GpgSM deze URL's negeert en alleen de boven ingestelde gebruikt.

Dit bijv. gebruiken om het gebruik van een organisatie-brede OCSP proxy af te dwingen.

5.4.3 Validatieopties instellen

Certificaatbeleid niet controleren

Standaard gebruikt GpgSM het bestand `~/.gnupg/policies.txt` om te controleren of een certificaatbeleid toegestaan is. Wanneer deze optie is geselecteerd wordt het beleid niet gecontroleerd.

Nooit een CRL raadplegen

Als deze optie ingeschakeld is, worden Certificate Revocation Lists nooit gebruikt om S/MIME-certificaten te valideren.

Sta toe om het hoofdcertificaat als vertrouwd te markeren

Als deze optie is geactiveerd, terwijl een root-CA-certificaat wordt geïmporteerd, zult u worden gevraagd om zijn vingerafdruk te bevestigen en te verklaren of u wel of niet dit root-certificaat vertrouwd.

Een root-certificaat moet vertrouwd worden voordat de certificaten die het certificeert vertrouwd worden, maar lichtvaardig root-certificaten in uw certificatenopslag vertrouwen zal de veiligheid van het systeem ondermijnen.

> OPMERKING
> Deze functionaliteit in de backend inschakelen kan leiden tot pop-ups van PinEntry op ongewenste tijden (bijv. bij het verifiëren van handtekeningen) en kan dus onbewaakte e-mailverwerking blokkeren. Daarom en omdat het gewenst is om in staat te zijn een vertrouwd root-certificaat opnieuw te *wantrouwen*, staat Kleopatra handmatig instellen van vertrouwen toe met **Certificaten → Hoofdcertificaat vertrouwen** en **Certificaten → Wantrouw hoofdcertificaat** .
> Deze instelling hier heeft geen invloed op het functioneren van Kleopatra.

Ontbrekende uitgevercertificaten ophalen

Wanneer deze optie is geactiveerd, zullen ontbrekende uitgevers-certificaten worden opgehaald indien nodig (dit is van toepassing op beide methoden, CRL's en OCSP).

5.4.4 Opties voor HTTP-verzoeken instellen

Geen HTTP-verzoeken uitvoeren

Schakelt het gebruik van HTTP voor S/MIME geheel uit.

HTTP CRL-distributiepunt van certificaten negeren

Wanneer u de locatie van een CRL aan het zoeken bent, zal het te testen certificaat items bevatten onder de naam 'CRL Distribution Point' (DP). Deze bevatten URL's die het adres van de CRL beschrijven. Het eerste gevonden DP wordt gebruikt.

Met deze optie worden alle items met het HTTP-schema genegeerd wanneer er gezocht wordt naar een geschikte DP.

HTTP-proxy van systeem gebruiken

Wanneer deze optie is geselecteerd zal de HTTP-proxy, die rechts wordt getoond, gebruikt worden bij elk HTTP-verzoek. (De waarde hiervan komt uit de omgevingsvariabele `http_proxy`).

Deze proxy voor HTTP-verzoeken gebruiken

Als er geen systeemproxy is ingesteld of u moet een andere proxy voor GpgSM, gebruiken, dan kunt u hier de locatie invoeren.

Het zal voor alle HTTP-verzoeken gerelateerd aan S/MIME worden gebruikt.

De syntaxis is **`hostnaam:poort`**, bijv. **`mijnproxy.nergens.nl:3128`**.

5.4.5 Opties voor LDAP-verzoeken instellen

Geen LDAP-verzoeken uitvoeren

Schakelt het gebruik van LDAP voor S/MIME geheel uit.

LDAP CRL-distributiepunt van certificaten negeren

Wanneer u de locatie van een CRL aan het zoeken bent, zal het te testen certificaat items bevatten onder de naam ˝CRL Distribution Point˝ (DP). Deze bevatten URL's die het adres van de CRL beschrijven. Het eerste gevonden DP wordt gebruikt.

Met deze optie worden alle items met het LDAP-schema genegeerd wanneer er gezocht wordt naar een geschikte DP.

Primaire host voor LDAP-verzoeken

Hier een LDAP-server invoeren maakt dat alle LDAP-verzoeken eerst naar die server gaan. Meer precies, deze instelling overschrijft elke gespecificeerde *hostnaam* en *poort* in een LDAP-URL en zal ook worden gebruikt als *hostnaam* en *poort* uit de URL zijn weggelaten.

Andere LDAP-servers zullen alleen worden gebruikt als de verbinding naar de 'proxy' mislukt. De syntaxis is **hostnaam** of **hostnaam:poort**. Als *poort* wordt weggelaten, dan wordt poort 389 (de standaard LDAP-poort) gebruikt.

5.5 Het GnuPG-systeem instellen

Dit deel van de dialoog is automatisch gegenereerd uit de uitvoer van **gpgconf --list-components** en voor elke *component* die het bovenstaande commando terug geeft, de uitvoer van **gpgconf --list-options** ***component***.

> OPMERKING
> De meest nuttige van deze opties zijn overgenomen als aparte pagina's in de instellingendialoog van Kleopatra. Zie Section 5.1 en Section 5.4 voor de twee dialoogpagina's die geselecteerde opties bevatten uit dit gedeelte van de dialoog.

De exacte inhoud van dit gedeelte van de dialoog hangt af van de versie van de geïnstalleerde GnuPG-backend en, in principe, van het platform waarop u werkt. We zullen dus alleen de algemene indeling van de dialoog, inclusief het overeen laten komen van de GpgConf-optie met de GUI besturing van Kleopatra.

GpgConf geeft configuratie-informatie voor meerdere componenten terug. Binnen elke component worden individuele opties gecombineerd in groepen.

Kleopatra toont één tabblad per door GpgConf gerapporteerde component; groepen krijgen een kop met een horizontale lijn met de groepsnaam zoals teruggeven door GpgConf.

Elke optie van GpgConf heeft een type. Behalve voor bepaalde welbekende opties, die Kleopatra ondersteunt met gespecialiseerde besturing voor een betere gebruikerservaring, is de koppeling tussen GpgConf-types en besturing van Kleopatra als volgt:

GpgConf-type	**Besturing van Kleopatra**	
	voor lijsten	**voor niet-lijsten**
`geen`	Numeriek keuzeveld ('getallen'-semantiek)	Keuzevakje
`tekenreeks`	N/A	Regelinvoer
`int32`	Regelinvoer (ongeformatteerd)	Draaiveld
`uint32`		
`padnaam`	N/A	gespecialiseerde besturing
`LDAP-server`	gespecialiseerde besturing	N/A
`vingerafdruk van sleutel`	N/A	
`publieke sleutel`		
`geheime sleutel`		
`aliaslijst`		

Tabel 5.1: Koppeling tussen GpgConf-types en GUI-besturing

Zie het handboek van GpgConf voor meer informatie over wat u hier in kunt stellen en hoe.

Hoofdstuk 6

Systeembeheerdersgids

De systeembeheerdersgids beschrijft de manieren waarop Kleopatra kan worden aangepast, die niet toegankelijk zijn via de GUI, maar alleen via de instellingenbestanden.

De veronderstelling is dat de lezer bekend is met de technologie die wordt gebruikt voor het instellen van KDE toepassingen, inclusief de indeling, locatie van het bestandssysteem en opstapelen van instellingenbestanden, evenals het KIOSK-framework.

6.1 Aanpassen van de assistent Certificaat aanmaken

6.1.1 Aanpassen van de DN-velden

Kleopatra stelt u in staat de velden, die de gebruiker mag invoeren, aan te passen om hun certificaat aan te maken.

Maak een groep genaamd `CertificateCreationWizard` in de systeembrede `kleopatrarc`. Als u een eigen volgorde van attributen wilt of als u alleen bepaalde items wilt laten verschijnen, maak dan een sleutel genaamd `DNAttributeOrder`. Het argument is een of meer uit `CN`, `SN`, `GN`, `L`, `T`, `OU`, `O`, `PC`, `C`, `SP`, `DC`, `BC`, `EMAIL`. Als u velden met een bepaalde waarde wilt initialiseren, schrijf dan zoiets als Attribuut=waarde. Als u het attribuut als vereist wilt behandelen, voeg dan een uitroepteken achter (bijv. `CN!`, `L`, `OU`, `O!`, `C!`, `EMAIL!`, hetwelk de standaard instelling is).

Met gebruik van de KIOSK modus-modifier `$e` kunt u de waarden uit omgevingsvariabelen halen of uit een uitgevoerd script of binair programma. Als u bovendien bewerking van het respectievelijke wilt verbieden, gebruik dan de modifier `$i`. Als u het gebruik van de knop **Mijn adres invoegen** wilt verbieden, zet `ShowSetWhoAmI` dan op false.

> TIP
> Vanwege de aard van het KDE KIOSK framework, maakt het gebruik van de niet-te-vervangen vlag (`$i`) het voor de gebruiker onmogelijk om de vlag te negeren. Dit is bewust gedrag. `$i` en `$e` kunnen ook worden gebruikt met alle andere instellingensleutels in KDE toepassingen.

Het volgende voorbeeld legt uit wat de mogelijke aanpassingen zijn:

```
[CertificateCreationWizard]
;Sta niet toe persoonlijke gegevens uit het adresboek te kopiëren, evenzo ↩
    lokaal overschrijven
ShowSetWhoAmI[$i]=false
```

```
;stelt de gebruikersnaam in op $USER
CN[$e]=$USER

;stelt de bedrijfsnaam in op "Mijn bedrijf", bewerken niet toegestaan
O[$i]=Mijn bedrijf

;stelt de afdelingsnaam in op een waarde teruggegeven door een script
OU[$ei]=$(lookup_dept_from_ip)

; stel het land in op NL, maar mag door de gebruiker gewijzigd worden
C=NL
```

6.1.2 Beperken van de types sleutels die een gebruiker mag aanmaken

Kleopatra kan ook beperken welk type certificaten een gebruiker mag aanmaken. Let op, hier is gemakkelijk omheen te gaan, de gebruiker kan deze nog steeds op de opdrachtregel aanmaken.

6.1.2.1 Algoritmes voor publieke sleutels

Om het te gebruiken algoritme voor de publieke sleutel te beperken, voegt u de configuratiesleutel `PGPKeyType` (en `CMSKeyType`, echter alleen RSA is voor CMS ondersteund) aan de sectie `CertificateCreationWizard` van `kleopatrarc` toe.

De toegestane waarden zijn `RSA` voor RSA-sleutels, `DAS` voor DSA-sleutels (alleen ondertekenen) en `DSA+ELG` voor een DSA-sleutel (alleen ondertekenen) met een Elgamal-subsleutel voor versleuteling.

De standaard wordt gelezen uit GpgConf of is anders `RSA` als GpgConf geen standaard levert.

6.1.2.2 Grootte publieke sleutel

Om de beschikbare sleutellengtes voor een publiek algoritme te beperken, voegt u de configuratiesleutel `<ALG>KeySizes` (waar *ALG* `RSA`, `DSA` of `ELG`) mag zijn, toe aan de sectie `CertificateCreationWizard` van `kleopatrarc`, die een komma-gescheiden lijst van sleutellengtes (in bits) bevat. Een standaard kan worden aangeduid door de sleutellengte te laten voorafgaan door een minteken (-).

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

Het bovenstaande beperkt de toegestane RSA sleutelgrootte tot 1536, 2048 en 3072, met 2048 als de standaard.

Naast de lengtes zelf, mag u labels voor elk van de lengtes specificeren. Stel eenvoudig de configuratiesleutel in op `ALGKeySizeLabels` in op een komma-gescheiden lijst van labels.

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

Het bovenstaande, in combinatie met het vorige voorbeeld, zou zoiets als de volgende opties voor selectie laten zien:

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

De standaarden zijn zoals het volgende laat zien:

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

6.2 Sleutelcategorieën aanmaken en bewerken

Kleopatra stelt de gebruiker in staat om het visuele uiterlijk van toetsen gebaseerd op een concept genaamd **Sleutelcategorieën**. **Sleutelcategorieën** worden ook gebruikt om de lijst met certificaten te filteren. Deze sectie beschrijft hoe u de beschikbare categorieën kunt bewerken en nieuwe kan toevoegen.

Bij het proberen om de categorie te vinden waar een sleutel bij hoort, probeert Kleopatra om de sleutel te laten overeenkomen met een serie sleutelfilters, geconfigureerd in `libkleopatrarc`. De eerste die overeenkomt definieert de categorie, gebaseerd op een concept van *meer specifiek*, hieronder nader verklaart.

Elke sleutelfilter is gedefinieerd in een configuratiegroep genaamd `Key Filter #n`, waar *n* een getal is, beginnend bij `0`.

De enige verplichte sleutels in een `Key Filter #n`-groep zijn `Name`, bevattende de naam van de categorie zoals getoond in de Instellingendialoog en `id`, die wordt gebruikt als een referentie naar het filter in andere instellingensecties (zoals `View #n`).

Tabel 6.1 toont alle sleutels die de weergaveeigenschappen van sleutels behorende bij die categorie (bijv. die sleutels die aangepast kunnen worden in de instellingendialoog), terwijl Tabel 6.2 alle sleutels die de criteria definiëren van het filter waartegen de sleutels worden gehouden.

Configuratiesleutel	Type	Beschrijving
`background-color`	kleur	De te gebruiken achtergrondkleur. Is standaard de achtergrondkleur die globaal is gedefinieerd voor weergave van lijsten, indien deze ontbreekt.
`foreground-color`	kleur	De te gebruiken voorgrondkleur. Is standaard de voorgrondkleur die globaal is gedefinieerd voor weergave van lijsten, indien deze ontbreekt.
`font`	lettertype	Het aangepaste te gebruiken lettertype. Het lettertype zal worden geschaald tot de grootte ingesteld voor weergave van lijsten en elke attribuut van lettertypes (zie onder) zal worden toegepast.

font-bold	boolean	Indien ingesteld op true en font is niet ingesteld, wordt het standaard lettertype gebruikt voor lijstweergave met de stijl vet toegevoegd (indien beschikbaar). Genegeerd als font ook aanwezig is.
font-italic	boolean	Analoog aan font-bold, maar voor de lettertypestijl cursief in plaats van vet.
font-strikeout	boolean	Indien true, tekent een gecentreerde lijn over het lettertype. Wordt zelfs toegepast als font is ingesteld.
icon	tekst	De naam van een pictogram om de eerste kolom te tonen. Nog niet geïmplementeerd.

Tabel 6.1: Instellingensleutels voor sleutelfilters die weergave-eigenschappen definiëren

Configuratiesleutel	**Type**	**Indien gespecificeerd, filter komt overeen wanneer...**
is-revoked	boolean	de sleutel is ingetrokken.
match-context	context[1]	de context waarin dit filter overeenkomt.
is-expired	boolean	de sleutel is verlopen.
is-disabled	boolean	de sleutel is uitgeschakeld (gemarkeerd voor niet-gebruiken) door de gebruiker. Genegeerd voor S/MIME-sleutels.
is-root-certificate	boolean	de sleutel is een root-certificaat. Genegeerd voor OpenPGP-sleutels.
can-encrypt	boolean	de sleutel kan gebruikt worden voor versleuteling.
can-sign	boolean	de sleutel kan gebruikt worden voor ondertekening.
can-certify	boolean	de sleutel kan gebruikt worden voor ondertekening (certificeren) van andere sleutels.

[1] Context is een opsomming met de volgende toegestane waarden: appearance, filtering and any.

`can-authenticate`	boolean	de sleutel kan gebruikt worden voor authenticatie (bijv. als een TLS client-certificaat).
`is-qualified`	boolean	de sleutel kan gebruikt worden om Qualified Signatures te maken (zoals gedefinieerd door de Duitse Digital Signature Law).
`is-cardkey`	boolean	de sleutel is opgeslagen op een smartcard (in plaats van op de computer).
`has-secret-key`	boolean	de geheime sleutel voor dit sleutelpaar is beschikbaar.
`is-openpgp-key`	boolean	de sleutel is een OpenPGP-sleutel (`true`) of een S/MIME-sleutel (`false`).
`was-validated`	boolean	de sleutel is gevalideerd.
`voorloop-ownertrust`	geldigheid[2]	de sleutel heeft exact (*`voorloop`* = `is`), heeft alles behalve (*`voorloop`* = `is-not`), heeft minstens (*`voorloop`* = `is-at-least`) of heeft hooguit (*`voorloop`* = `is-at-most`) het ownertrust gegeven als de waarde van de instellingssleutel. Als meer dan één sleutel `voorloop-ownertrust` (met een verschillende *`voorloop`*-waarde) aanwezig zijn in een enkele groep, dan is het gedrag niet gedefinieerd.
`voorloop-validity`	geldigheid	Analoog aan `voorloop-ownertrust`, maar dan voor de sleutel validity in plaats van ownertrust.

Tabel 6.2: Instellingensleutels voor sleutelfilters die filtercriteria definiëren

OPMERKING

Sommige van de meer interessante criteria, zoals `is-revoked` of `is-expired` zal alleen werken op *gevalideerde* sleutels, dit is waarom, standaard, alleen gevalideerde sleutels gecontroleerd worden op ingetrokken en verlopen, hoewel u vrij bent om deze extra controles te verwijderen.

[2]Geldigheid is een (geordende) opsomming met de volgende toegestane waarden: `unknown`, `undefined`, `never`, `marginal`, `full`, `ultimate`. Zie de handboeken van GPG en GpgSM voor een gedetailleerde uitleg.

Naast de boven weergegeven configuratiesleutels, kan een sleutelfilter ook een `id` en `match-contexts` hebben.

Met het gebruik van het `id` van het filter, die standaard de naam van de configuratiegroep van het filter heeft, indien niet gegeven of leeg, kunt u elders in de configurati aan het sleutelfilter refereren, bijv. in weergaveinstellingen van Kleopatra. De `id` wordt door Kleopatra niet geïnterpreteerd, zodat u elke gewenste tekenreeks kunt gebruiken, als deze maar uniek is.

De `match-contexts` beperkt de toepasbaarheid van het filter. Er zijn nu twee contexten gedefinieerd: De context `appearance` wordt gebruikt bij het definiëren van de kleuren en eigenschappen van lettertypes voor de weergaven. De context `filtering` wordt gebruikt om selectief certificaten mee te nemen (en uit te sluiten) in weergaven. `any` kan worden gebruikt om alle nu gedefinieerde contexten aan te duiden en is de standaard als `match-contexts` niet is gegeven of anders geen contexten oplevert. Dit verzekert dat geen sleutelfilter 'dead' kan eindigen, bijv. zonder dat er een contexts op is toegepast.

Het formaat van het item is een lijst met tokens, gescheiden door niet-woord tekens. Elk van de tokens geeft optioneel een voorloop van een uitroepteken (`!`), hetgeen negatie betekent. De tokens werken in volgorde op een interne lijst met contexten, die leeg beginnen. Dit is het best uitgelegd met een voorbeeld: `any !appearance` is hetzelfde als `filtering` en `appearance !appearance` levert de lege verzameling, evenals `!any`. De laatste twee, echter, zullen intern vervangen worden door `any`, omdat ze helemaal geen contexts opleveren.

In het algemeen worden niet gespecificeerde criteria (bijv. het configuratie-item is niet ingesteld) niet gecontroleerd. Als er een criterium is gegeven, dan wordt er op gecontroleerd en moet als geheel overeenkomen met het filter om overeen te komen, bijv. aan alle criteria moet voldaan (en-functie).

Elk filter heeft een impliciete 'specificity' die wordt gebruikt om alle overeenkomende filters een waardering te geven. Het meer specifieke filter wint boven minder specifieke filters. Als twee filters dezelfde specificity hebben, dan wint degene die als eerste in het instellingenbestand staat. Een specificity is evenredig aan het aantal criteria die het bevat.

Example 6.1 Voorbeelden van sleutelfilters

Om op alle verlopen, maar niet-ingetrokken root-certificaten, te controleren zou u een sleutelfilter als volgt gedefinieerd kunnen gebruiken:

```
[Key Filter #n]
Name=verlopen, maar niet ingetrokken
was-validated=true
is-expired=true
is-revoked=false
is-root-certificate=true
; ( specificity 4 )
```

Om te controleren op alle uitgeschakelde OpenPGP-sleutels (nog niet ondersteund door Kleopatra) met eigenaarsvertrouwen van minstens 'marginaal', zou u moeten gebruiken:

```
[Key Filter #n]
Name=uitgeschakelde OpenPGP-sleutels met marginale of beter ↩
    eigenaarsvertrouwen
is-openpgp=true
is-disabled=true
is-at-least-ownertrust=marginal
; ( specificity 3 )
```

6.3 Archiveerders instellen voor gebruik met ondertekenen/versleutelen van bestanden

Kleopatra stelt de systeembeheerder (en grootgebruiker) in staat om de lijst met archiveerders, die gepresenteerd worden in de dialoog voor ondertekenen/versleutelen van bestanden, in te stellen.

Elke archiveerder is gedefinieerd in `libkleopatrarc` als een aparte `Archive Definition #n` groep, met de volgende verplichte elementen:

`extensies`
: Een komma-gescheiden lijst met bestandsnaamextensies die gewoonlijk dit formaat archief aangeven.

`id`
: Een unieke ID gebruikt om deze archiveerder intern te identificeren. Bij twijfel gebruikt u de naam van het commando.

`Name` (vertaald)
: De naam van deze archiveerder, zichtbaar voor de gebruiker, zoals getoond in het overeenkomende afrolmenu van de dialoog voor ondertekenen/versleutelen van bestanden.

`pack-command`
: Het actuele commando om bestanden te archiveren. U kunt elk commando gebruiken, als er geen shell nodig is om het uit te voeren. Het programmabestand wordt opgezocht met de omgevingsvariabele `PATH`, tenzij u een absoluut bestandspad gebruikt. Gebruik van aanhalingstekens is ondersteund alsof een shell wordt gebruikt:

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

OPMERKING

Omdat de backslash (\) een escape-teken is in KDE configuratiebestanden, moet u ze verdubbelen wanneer ze in padnamen verschijnen:

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

Voor het commando zelf echter (in tegenstelling tot zijn argumenten), mag u gewoon voorwaartse slashes (/) op alle platforms als padscheidingstekens gebruiken:

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

Dit wordt niet ondersteund in argumenten, omdat de meeste Windows®-programma's de voorwaartse slash voor opties gebruiken. Het volgende zal echter niet werken, omdat `C:/myarchivescript.bat` een argument voor **cmd.exe** en / niet in argumenten geconverteerd wordt naar \, alleen commando's:

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

Dit moet, in plaats hiervan, geschreven worden als:

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

6.3.1 Doorgeven van bestandsnamen voor invoer aan `pack-command`

Er zijn drie manieren om bestandsnamen door te geven aan het commando pack. Voor elk van deze biedt `pack-command` een specifieke syntaxis:

1. Als argumenten in de opdrachtregel.

   Voorbeeld (tar):

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

   Voorbeeld (zip):

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

   In dit geval worden bestandsnamen doorgegeven op de opdrachtregel, net zoals u zou doen bij een prompt. Kleopatra gebruikt geen shell om de opdracht uit te voeren. Daarom is dit een veilige manier om bestandsnamen door te geven, maar op sommige platforms kan dat leiden tot beperkingen van de lengte van deze regel. Een literal `%f`, indien aanwezig, wordt vervangen door de namen van de te archiveren bestanden. Anders worden bestandsnamen achtergevoegd op de opdrachtregel. Dus kan het voorbeeld van zip hierboven ook geschreven worden als:

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

2. Via standaard-invoer, gescheiden door nieuwe-regels: voeg voor `|`.

   Voorbeeld (GNU-tar):

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

   Voorbeeld (ZIP):

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

   In dit geval worden bestandsnamen doorgegeven naar de archiveringstoepassing via stdin, een per regel. Dit vermijdt problemen op platforms die een lage limiet zetten op het aantal toegestane argumenten op de opdrachtregel, maar mislukt wanneer bestandsnamen, in feite nieuwe-regels bevatten.

   > OPMERKING
   > Kleopatra ondersteunt nu alleen LF als een nieuwe-regel scheidingsteken, niet CRLF. Dit kan wijzigen in toekomstige versies, gebaseerd op terugkoppeling van de gebruiker.

3. Via standaard-invoer, gescheiden door NUL-bytes: voeg voor `0|`.

   Voorbeeld (GNU-tar):

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

   Dit is hetzelfde als boven, behalve dat NUL-bytes worden gebruikt om bestandsnamen te scheiden. Omdat NUL-bytes verboden zijn in bestandsnamen, dit is de meest robuuste manier van het doorgeven van bestandsnamen, maar niet alle archiveringstoepassingen ondersteunen het.

6.4 Programma's voor controlesommen voor gebruik bij aanmaken/verifiëren van controlesommen

Kleopatra stelt de beheerder (en power-gebruiker) in staat om de lijst met programma's voor controlesommen in te stellen, waaruit de gebruiker kan kiezen in de instellingendialoog en die Kleopatra automatisch kan detecteren wanneer deze gevraagd wordt om de controlesom van een gegeven bestand te verifiëren.

> OPMERKING
> Om bruikbaar te zijn voor Kleopatra moet de uitvoer van programma's voor controlesommen (zowel het geschreven controlesombestand als de uitvoer op stdout bij verifiëren van controlesommen) compatibel zijn met GNU **md5sum** en **sha1sum**.
> Het controlesombestand moet op regels gebaseerd zijn met in elke regel het volgende formaat:
>
> ```
> CONTROLESOM ' ' ( ' ' | '*' ) BESTANDSNAAM
> ```
>
> waar *CONTROLESOM* alleen bestaat uit hex-tekens. Als *BESTANDSNAAM* een teken nieuwe-regel bevat, moet de regel er uit als volgt uitzien:
>
> ```
> \CONTROLESOM ' ' ( ' ' | '*' ) ESCAPED-BESTANDSNAAM
> ```
>
> waar *ESCAPED-BESTANDSNAAM* de bestandsnaam is met nieuwe-regel vervangen door `\n` en backslashes verdubbeld (\↦\\).
> Evenzo moet de uitvoer van `verify-command` van de vorm
>
> ```
> BESTANDSNAAM ( ': OK' | ': FAILED' )
> ```
>
> zijn gescheiden door nieuwe-regels. Nieuwe-regels en andere tekens worden *niet* escaped in de uitvoer.[a]
>
> [a] Ja, deze programma's zijn niet geschreven met een grafisch frontend in gedachten, zodat het Kleopatra niet zal lukken om op de juiste manier pathologische bestandsnamen die ˝: OK˝ plus nieuwe-regel bevatten, te gebruiken.

Elk programma voor controlesommen is gedefinieerd in `libkleopatrarc` als een aparte `Checksum Definition #n` groep, met de volgende verplichte elementen:

`bestandspatronen`
: Een lijst met reguliere expressies die beschrijven welke bestanden beschouwd zouden moeten worden als controlesombestanden voor dit programma voor controlesommen. De syntaxis is die voor lijsten tekenreeksen in KDE configuratiebestanden.

> OPMERKING
> Omdat reguliere expressies gewoonlijk backslashes bevatten, moet zorgvuldig omgegaan worden met het juiste gebruik van escapes in het configuratiebestand. Het gebruik van een bewerkingshulpmiddel voor een configuratiebestand wordt aangeraden.

: Het platform definieert of de patronen behandeld worden met of zonder onderscheid tussen hoofd- en kleine letter.

`uitvoerbestand`
: De typische naam van het uitvoerbestand voor dit programma voor controlesommen (zou natuurlijk overeen moeten komen met een van de `bestandspatronen`). Dit is wat Kleopatra zal gebruiken als de uitvoerbestandsnaam bij het aanmaken van bestanden met controlesommen van dit type.

id

Een unieke ID gebruikt om dit programma voor controlesommen intern te identificeren. Bij twijfel gebruikt u de naam van het commando.

Name (vertaald)

De voor de gebruiker zichtbare naam van dit programma voor controlesommen, zoals getoond in het afrolmenu in de configuratiedialoog van Kleopatra.

create-command

Het actuele commando waarmee controlesombestanden worden aangemaakt. De syntax, beperkingen en opties voor argumentenoverdracht zijn hetzelfde als beschreven voor `pack-command` in Section 6.3.

verify-command

Hetzelfde als `create-command`, echter voor verificatie van de controlesom.

Hier is een volledig voorbeeld:

```
[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
```

Hoofdstuk 7

Dankbetuiging en licentie

MEDEWERKERS

- 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

Op- of aanmerkingen over de vertalingen van de toepassing en haar documentatie kunt u melden op http://www.kde.nl/bugs.

Dit document is vertaald in het Nederlands door Freek de Kruijf freekdekruijf@kde.nl.