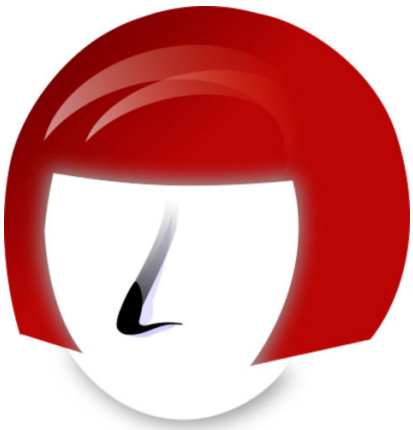
Manuel de Kleopatra

Marc Mutz
Développeur: David Faure
Développeur: Steffen Hansen
Développeur: Matthias Kalle Dalheimer
Développeur: Jesper Pedersen
Développeur: Daniel Molkentin
Traduction française : Joëlle Cornavin
Traduction française : Robin Guitton



Manuel de Kleopatra

Table des matières

Liste des tableaux

Résumé

Kleopatra est un outil pour gérer les certificats X.509 et OpenPGP.

Chapitre 1

Introduction

Kleopatra est l'outil de KDE permettant la gestion des certificats X.509 et OpenPGP dans les trousseaux GpgSM et GPG. Il permet aussi de recevoir les certificats depuis LDAP et d'autres serveurs de certificats.

Vous pouvez démarrer Kleopatra depuis le menu **Outils** → **Gestionnaire des certificats** de KMail aussi bien qu'en ligne de commande. L'exécutable Kleopatra est appelé **`kleopatra`**.

> NOTE
> Ce programme tire son nom de Cléopâtre, une célèbre pharaonne égyptienne qui vivait du temps de Jules César avec qui elle eu un enfant, Caeserion, non reconnu comme son héritier.
> Le nom de ce programme a été choisi car provenant des Projets « Ägypten » (Ägypten signifie « Égypte » en Allemand). Kleopatra est l'orthographe allemande de Cléopâtre.

Chapitre 2

Fonctions principales

2.1 Afficher le trousseau local

La fonction principale de Kleopatra est d'afficher et de modifier le contenu du trousseau local, similaire au concept des trousseaux de clés de GPG, quoiqu'il ne faille pas trop forcer l'analogie.

La fenêtre principale se compose de la grande zone de listage des clés se composant de plusieurs onglets, la barre de menus et la barre de recherche en haut, ainsi que d'une barre d'état en bas.

Chaque ligne de la liste des clés correspond à un certificat, identifié par ce qu'on appelle le **DN du sujet**. DN est un acronyme pour « Nom Distinct » (*Distinguished Name*), un identifiant hiérarchique, tout comme l'emplacement d'un système de fichiers avec une syntaxe inhabituelle, censé identifier globalement et de façon unique un certificat donné.

Pour être valables, donc utilisables, les clés (publiques) doivent être signées par une CA (Autorité de certification, *Certification Authority*). Ces signatures sont appelées certificats, mais d'ordinaire les termes "certificat" et "clé (publique)" s'utilisent de manière interchangeable : en conséquence, nous ne ferons pas de distinction entre elles dans ce manuel, sauf indication explicite.

Les CAs doivent à leur tour être signées par d'autres CAs pour être valables. Naturellement, l'opération doit prendre fin quelque part, de façon que le CA de premier niveau (CA racine) signe sa clé avec elle-même (on parle alors d'auto-signature). Il faut donc affecter manuellement une validité (communément dénommée « confiance ») aux certificats racines, par exemple après avoir comparé l'empreinte numérique avec celle se trouvant sur le site Internet de la CA. Cette tâche est généralement dévolue à l'administrateur système ou au fabricant d'un produit faisant intervenir des certificats, mais peut être effectuée par l'utilisateur au moyen de l'interface en ligne de commande de GpgSM.

Pour voir lesquels des certificats sont des certificats racines, passez en mode liste de clés hiérarchique avec **Affichage → Liste hiérarchique des certificats**.

Vous pouvez voir les détails d'un certificat donné en double-cliquant dessus ou à l'aide de **Affichage → Détails du certificat**. Une boite de dialogue s'ouvre, qui affiche les propriétés les plus courantes du certificat, sa chaine de certificats (c'est-à-dire la chaine des émetteurs jusqu'à la CA racine) ainsi qu'un cliché de toutes les informations que le moteur est en mesure d'extraire du certificat.

Si vous changez le trousseau sans faire appel à Kleopatra (par exemple à l'aide de l'interface en ligne de commande de GpgSM), vous pouvez rafraîchir la vue avec **Affichage → Actualiser (F5)**.

2.2 Rechercher et importer des certificats

La plupart du temps, vous obtiendrez de nouveaux certificats en vérifiant les signatures dans les courriels, lorsque les certificats sont intégrés dans les signatures créées, le plus souvent, en les

utilisant. Cependant, si vous devez envoyer un message à une personne avec qui vous n'avez pas encore eu de contact, il vous faut aller chercher le certificat dans un dossier LDAP (Bien que GpgSM puisse le faire automatiquement) ou depuis un fichier. Vous devez également importer votre propre certificat après avoir reçu la réponse de CA à votre demande de certification.

Pour rechercher un certificat dans une annuaire LDAP ; sélectionner **Fichier** → **Rechercher des certificats sur le serveur** et saisissez du texte (par exemple le nom de la personne à qui vous voulez le certificat) dans le champ de la boite de dialogue **Recherche de certificat sur le serveur de certificats**. Cliquez alors sur le bouton **Rechercher**. Les résultats seront affichés dans la liste de clés sous la barre de recherche, où vous pouvez sélectionner des certificats pour les étudier en cliquant sur le bouton **Détails** ou bien les télécharger dans la trousseau locale avec **Importer**.

Vous pouvez configurer la liste des serveurs LDAP pour rechercher dans la page **Services d'annuaire** de la boite de dialogue de configuration de Kleopatra.

Si vous avez reçu le certificat sous la forme d'un fichier, essayez **Fichier** → **Importer des certificats... (Ctrl+I)** . GpgSM doit comprendre le format du fichier de certificat : reportez-vous au manuel de GpgSM pour obtenir une liste des formats de fichiers pris en charge.

Si vous n'avez pas créé votre paire de clés avec GpgSM, vous devez également importer manuellement la clé publique (ainsi que la clé secrète) à partir du fichier PKCS#12 que vous avez obtenu de la CA. Utilisez pour ce faire la ligne de commande avec **`kleopatra --import-certificate nom-du-fichier`** ou dans Kleopatra avec **Fichier** → **Importer des certificats... (Ctrl+I)** , tout comme vous le feriez pour les certificats "normaux".

2.3 Créer de nouvelles paires de clés

L'élément de menu **Fichier** → **Nouveau certificat... (Ctrl+N)** démarre l'**Assistant de création de paires de certificats**. Ce dernier vous guidera à travers un certain nombre d'étapes pour créer une demande de certificat.

Chaque fois que vous avez terminé une étape dans l'assistant, cliquez sur **Suivant** pour passer à la suivante (ou sur **Précédent** pour revoir les étapes déjà achevées). La création de demande de certificat peut être annulée à tout moment en cliquant sur le bouton**Annuler**.

Sur la première page de l'assistant, choisissez quel type de certificat vous voulez créer :

Créer une paire de clés personnelles OpenPGP

Les paires de clés OpenPGP sont créées localement et sont certifiées par vos amis et connaissances. Il n'y a pas d'autorité de certification centralisée ; chaque individu crée un réseau de confiance personnel en certifiant les clés des autres utilisateurs avec son propre certificat.

Vous devez saisir un **Nom**, une **Adresse électronique** et facultativement un **Commentaire**.

Créer une paire de clés X.509 personnelle et une demande de certification

Les paires de clés X.509 sont créées localement mais sont certifiées de manière centralisée par une autorité de certification (CA). Les CA peuvent certifier d'autres CA, créant ainsi une chaine de confiance hiérarchisée et centralisée.

L'étape suivante de l'assistant vous demande de saisir vos données personnelles pour le certificat. Les champs à renseigner sont :

— **Nom d'usage (CN) :** Votre nom ;
— **Adresse électronique (EMAIL) :** Votre adresse électronique. Prenez soin de la saisir correctement — Ce sera l'adresse à laquelle vos correspondants enverront le courriel lorsqu'ils utilisent votre certificat.
— **Localité (L) :** La ville où vous habitez ;
— **Unité organisationnelle (OU) :** L'unité organisationnelle dans laquelle vous êtes (par exemple, « Logistique ») ;
— **Organisation (O) :** L'organisation que vous représentez (par exemple, l'entreprise dans laquelle vous travaillez) ;

— **Indicatif du pays (C) :** Le code à deux lettres du pays dans lequel vous résidez (par exemple, « FR » pour la France) ;

Dans l'étape suivante, l'assistant vous demande de choisir s'il doit enregistrer le certificat dans un fichier ou l'envoyer directement à une CA. Vous devrez spécifier le nom du fichier ou l'adresse électronique à laquelle envoyer la demande de certificat.

2.3.1 Révoquer une clé

Une paire de clés qui a expirée peu être remise dans un état opérationnel tant que vous avez accès à la clé privée et à la phrase secrète. Pour rendre une clé inutilisable de façon sûre, vous devez la révoquer. Révoquer une clé est fait en ajoutant une signature de révocation spéciale à la clé.

Cette signature de révocation est stockée dans un fichier séparé. Ce fichier peut être importer ultérieurement dans le trousseau de clés et est alors attaché à la clé, la rendant inutilisable. Veuillez noter que pour importer cette signature à la clé, aucun mot de passe n'est requis. Vous devez donc stocker cette signature de révocation dans un endroit sûr, habituellement dans un endroit différent de celui de votre paire de clés. Il est conseillé d'utiliser un emplacement qui est détaché de votre ordinateur, c'est-à-dire soit de le copier sur un périphérique de stockage externe comme une clé USB ou de l'imprimer.

Kleopatra ne fournit pas de fonction de création de telles signatures de révocation n'importe quand, mais vous pouvez le faire depuis l'application KDE KGpg en choisissant **Clés** → **Révoquer une clé** et en important si vous le désirez la signature de révocation dans le trousseau de clé directement.

Une autre façon de générer un certificat de révocation est d'utiliser GPG directement à partir de la ligne de commandes : **`gpg --output revocation_certificate.asc --gen-revoke votre-clé`**. L'argument *`votre-clé`* doit être un spécificateur de clé, soit l'identifiant de clé de votre paire de clés primaires, soit toute partie d'un identifiant utilisateur, référençant votre paire de clés.

Chapitre 3

Liste des menus

3.1 Menu Fichier

Fichier → Nouveau certificat... (Ctrl+N)

Créé une nouvelle paire de clés (publique et privée) et permet d'envoyer la partie publique à une autorité de certification (CA) pour sa signature. Le certificat qui en résulte vous est ensuite renvoyé ou enregistré sur un serveur LDAP pour que vous le téléchargiez dans votre trousseau local, dans lequel vous pouvez vous en servir pour signer et déchiffrer des messages.

Ce mode de fonctionnement est appelé "génération décentralisée des clés" du fait que toutes les clés sont créées localement. Kleopatra (et GpgSM) ne gèrent pas la "génération décentralisée des clés" directement, mais vous pouvez importer le lot de clés publiques/-secrètes que vous recevez de la CA au format PKCS#12 via **Fichier → Importer des certificats... (Ctrl+I)** .

Fichier → Rechercher des certificats sur le serveur... (Ctrl+Maj+I)

Recherche et importe des certificats depuis des serveurs de certificats dans le trousseau local. Voir Section 2.2 pour plus de détails.

Vous devez avoir des serveurs de clés configurés pour cette tâche. Voir Section 5.1 pour plus de détails.

Fichier → Importer des certificats... (Ctrl+I)

Importe des certificats et/ou des clés secrètes depuis des fichiers dans le trousseau local. Voir Section 2.2 pour plus de détails.

Le format du fichier certifié doit être géré par GpgSM/GPG. Reportez-vous au manuel de GpgSM et de GPG pour obtenir une liste des formats pris en charge.

Fichier → Exporter des certificats... (Ctrl+E)

Exporte les certificats sélectionnés dans un fichier.

L'extension du nom de fichier que vous choisissez pour exporter le fichier détermine le format du fichier exporté :

— Pour les certificats OpenPGP, les extensions `gpg` et `pgp` auront comme résultat un fichier binaire, tandis que l'extension `asc` produira un fichier ASCII blindé.
— Pour les certificats S/MIME, l'extension `der` aura comme résultat un fichier binaire encodé en DER, alors que l'extension `pem` produira un fichier ASCII blindé.

À moins que plusieurs certificats ne soient sélectionnés, Kleopatra proposera `empreinte-numérique.{asc,pem}` comme nom de fichier exporté.

Cette fonction est disponible seulement quand un ou plusieurs certificats ont été sélectionné.

> NOTE
> Cette fonction n'exporte que les clés publiques, même si la clé secrète est disponible. Veuillez utiliser **Fichier → Exporter le certificat secret...** pour exporter les clés privées dans un fichier.

Fichier → Exporter le certificat secret...

Exporte la clé secrète dans un fichier.

Dans la boite de dialogue s'affichant, vous pouvez choisir de créer un fichier binaire ou un fichier d'exportation chiffré en ASCII (**chiffrement « ASCII »**). Ensuite, veuillez cliquer sur l'icône du dossier sur le coté droit de la boite de dialogue de saisie **Fichier de sortie** et sélectionner le dossier et le nom du fichier d'exportation. Lors de l'exportation de clés secrètes S/MIME, vous pouvez aussi sélectionner le **Jeu de caractères de la phrase secrète**. Veuillez prendre connaissance de la discussion concernant l'option `--p12-charset charse t` dans le manuel de GpgSM pour plus de détails.

Cette fonction n'est disponible que si exactement un certificat a été sélectionné et que la clé secrète pour ce certificat est disponible.

> AVERTISSEMENT
> L'utilisation de cette fonction devrait être rarement nécessaire, mais s'il faut l'envisager, la prudence est de mise. Planifier la migration d'une clé secrète implique le choix des média de transport et, entre autres choses, une suppression sécurisée des données-clés présentes sur l'ancienne machine, ainsi que sur le moyen de transport.

Fichier → Exporter des certificats vers le serveur... (Ctrl+Maj+E)

Exporte les certificats sélectionnés sur un serveur de clés (seulement pour OpenPGP)..

Le certificat est envoyé au serveur de certificats configuré pour OpenPGP (cf. Section 5.1), si déterminé, ou sinon à `keys.gnupg.net`.

Cette fonction n'est disponible que si au moins un certificat OpenPGP (et non S/MIME) a été sélectionné.

> NOTE
> Quand les certificats OpenPGP ont été exporté vers un serveur d'annuaire publique, il est quasiment impossible de les y supprimer. Avant d'exporter votre certificat vers un serveur d'annuaire publique, assurez vous donc d'avoir créé un certificat de révocation afin de pouvoir révoquer le certificat ultérieurement si besoin.

> NOTE
> La plupart des serveurs de certificats OpenPGP synchronise les certificats entre eux, il est donc vain d'en envoyer plus d'un.
> Il peut arriver qu'une recherche sur un serveur de certificat ne retourne aucun résultat bien que vous veniez d'y envoyer votre certificat. Cela s'explique par le fait que la plupart des adresses de serveur de clés publique utilise la technique du DNS round-robin pour répartir la charge sur plusieurs machines. Ces machines se synchronisent les une avec les autres mais, généralement, seulement toutes les 24 heures voire plus.

Fichier → Déchiffrer/Vérifier des fichiers...

Déchiffre des fichiers et/ou vérifie des signatures sur des fichier.

Fichier → Signer/Chiffrer des fichiers...

Signe et/ou chiffre des fichiers.

Fichier → Fermer (Ctrl+W)

Ferme la fenêtre principale de Kleopatra. Vous pouvez la restaurer depuis la boite à miniatures à n'importe quel moment.

Fichier → Quitter (Ctrl+Q)

Met fin à Kleopatra.

3.2 Menu Affichage

Affichage → Actualiser (F5)

Rafraîchit la liste des certificats.

L'utilisation de cette fonction n'est généralement pas nécessaire, puisque Kleopatra surveille les modifications du système de fichiers et rafraîchit automatiquement la liste des certificats lorsque cela est nécessaire.

Affichage → Arrêter l'opération (Échap)

Arrête (annule) toutes les opérations en attente, par exemple une recherche, un listage des clés ou un téléchargement.

Cette fonction n'est disponible que si au moins une opération est en cours.

> NOTE
> À cause de limitations du moteur, des opérations se bloquent parfois de telle façon que cette fonction ne sera capable de les annuler instantanément, voir pas du tout.
> Dans de tels cas, la seule façon de rétablir l'ordre est de terminer, dans cet ordre, les processus de SCDaemon, DirMngr, GpgSM et GPG grâce aux outils du système d'exploitation (**top**, Gestionnaire des tâches de Windows, etc.), jusqu'à ce que l'opération se débloque.

Affichage → Détails du certificat

Affiche les détails du certificat actuellement sélectionné.

Cette fonction est disponible seulement si exactement un certificat est sélectionné.

Cette fonction est également accessible en double-cliquant directement sur l'élément correspondant dans l'affichage en liste.

Affichage → Liste hiérarchique des certificats

Bascule entre les modes liste hiérarchique et à plat des certificats.

En mode hiérarchique, les certificats sont organisés dans une relation émetteur/sujet, de telle sorte qu'il est facile de voir à quelle hiérarchie de certification un certificat donné appartient. Cependant, ce dernier est ainsi initialement plus difficile à trouver (bien que vous disposiez de la barre de recherche).

En mode à plat, tous les certificats sont affichés dans une liste étendu, triés par ordre alphabétique. Dans ce mode, un certificat donné est facile à trouver, mais il n'est pas évident de savoir directement à quel certificat racine il appartient.

Cette fonction bascule vers le mode hiérarchique par onglet, c'est-à-dire que chaque onglet a son propre état hiérarchique. Vous pouvez donc disposer à la fois d'un listage à plat et hiérarchique, chacun dans leur onglet respectif.

> NOTE
> L'affichage hiérarchique est actuellement seulement implémenté pour les certificats S/MIME. Il y a un désaccord parmi l'équipe de développement sur la façon convenable d'afficher les certificats OpenPGP hiérarchiquement (fondamentalement, "parent = signataire" ou "parent = signataire").

Affichage → Tout développer (Ctrl+.)

Développe tous les éléments de la liste dans l'affichage par liste des certificats, c'est-à-dire rend tous les éléments visibles.

C'est le comportement par défaut lorsqu'on entre en mode liste de clés hiérarchique.

Vous pouvez, naturellement, encore développer et réduire chaque élément individuellement.

Cette fonction est disponible seulement quand **Affichage → Liste hiérarchique des certificats** est activé.

Affichage → Tout réduire (Ctrl+,)

Réduit tous les éléments de la liste dans l'affichage en liste des certificats, c'est-à-dire masque tout sauf les éléments de premier niveau.

Vous pouvez, naturellement, encore développer et réduire chaque élément individuellement.

Cette fonction est disponible seulement quand **Affichage → Liste hiérarchique des certificats** est activé.

3.3 Menu Certificats

Certificats → Changer le niveau de confiance...

Affiche le niveau de confiance du certificat OpenPGP actuellement sélectionné.

Cette fonction est disponible seulement quand exactement un certificat OpenPGP est sélectionné.

Certificats → Certificat racine de confiance

Marque ce certificat racine (S/MIME) comme de confiance.

D'une certaine façon, c'est l'équivalent de **Certificats → Changer le niveau de confiance...** pour les certificats racines S/MIME. Vous pouvez cependant seulement choisir — Dans les termes de OpenPGP — Entre confiance "absolue" et "aucune confiance".

> NOTE
> Le moteur (par l'intermédiaire de GpgAgent) demandera, au moment de l'importation de certificats racines, s'il faut faire confiance au certificat racine importé. Toutefois, cette fonction doit être explicitement activée dans la configuration du moteur (`allow-mark-trusted` dans `gpg-agent.conf`, ou sinon **GnuPG Système → GPG Agent → Autoriser les clients à marquer les clés comme « de confiance »** ou **S/MIME Validation → Autorisé le marquage de confiance de certificats racines** dans chapitre 5).
> Activer cette fonctionnalité dans le moteur peut vous amenez à être dérangé par des menus contextuels venant de PinEntry à des moments inopportuns (c'est-à-dire à la vérification des signatures), et peut ainsi bloquer le traitement des courriers électroniques laissé sans surveillance. Pour cette raison, et parce qu'il est souhaitable d'être en mesure de *ne plus faire confiance* à un certificat racine de confiance de nouveau, Kleopatra permet le réglage manuel du niveau de confiance.

> AVERTISSEMENT
> À cause d'un manque de prise en charge du moteur pour cette fonction, Kleopatra a besoin de travailler directement sur une base de données de confiance GpgSM (`trustlist.txt`). Quand vous utilisez cette fonction, soyez sûr qu'aucune autre opération de cryptographie n'est en cours, qui pourrait concurrencer Kleopatra dans la modification de cette base de données.

Cette fonction est disponible seulement quand exactement un certificat racine S/MIME est sélectionné et que ce certificat n'est pas encore de confiance.

Utilisez **Certificats** → **Certificat racine de méfiance** pour annuler cette fonction.

Certificats → **Certificat racine de méfiance**

Marque ce certificat racine (S/MIME) comme de méfiance.

Cette fonction est disponible seulement quand exactement un certificat racine S/MIME est sélectionné, et que ce certificat est actuellement de confiance.

Utiliser **Certificats** → **Certificat racine de confiance** pour annuler. Voir là-bas pour plus de détails.

Certificats → **Certifier le certificat...**

Vous permet de certifier un autre certificat OpenPGP.

Cette fonction est disponible seulement quand exactement un certificat OpenPGP est sélectionné.

Certificats → **Changer la date d'expiration...**

Vous permet de changer la date d'expiration de votre certificat OpenPGP.

Utilisez cette fonction pour prolonger la durée du vie de vos certificats OpenPGP et comme alternative à la création d'un nouveau, ou définissez une durée de vie illimitée ("n'expire jamais").

Cette fonction est disponible seulement si exactement un certificat OpenPGP est sélectionné et que la clé secrète est disponible pour ce certificat.

Certificats → **Changer la phrase secrète...**

Permet de changer la phrase secrète de votre clé secrète

Cette fonction est disponible seulement si exactement un seul certificat est sélectionné et que la clé secrète est disponible pour ce certificat. Elle requiert un moteur très récent, puisque nous avons changé l'implémentation d'un appel directe de GPG et GpgSM vers un appel s'appuyant sur GpgME.

> NOTE
> Pour des raisons de sécurité, à la fois l'ancienne ainsi que la nouvelle phrase secrète est demandée par PinEntry, un processus séparé. Dépendant de la plate-forme sur laquelle vous tournez et de la qualité de l'implémentation de PinEntry sur cette plate-forme, il peut arriver que la fenêtre de PinEntry se lance en arrière plan. En conséquence, si vous sélectionnez cette fonction et que rien ne se passe, vérifiez la barre des tâche de votre système d'exploitation au cas où la fenêtre de PinEntry se serait ouverte en arrière plan.

Certificats → **Ajouter un identifiant utilisateur...**

Permet l'ajout d'un nouvel identifiant utilisateur à votre certificat OpenPGP.

Utilisez cette fonction pour ajouter une nouvelle identité à un certificat existant et comme alternative à la création d'une nouvelle paire de clé. Un identifiant d'utilisateur OpenPGP à la forme suivante :

```
Nom réel (Commentaire) <Adresse de courriel>
```

Dans la boite de dialogue qui apparait quand vous sélectionnez cette fonction, Kleopatra vous demandera chacun des trois paramètres séparément (*Nom réel*, *Commentaire* et *Adresse de courriel*) et affichera un aperçu des résultats.

> NOTE
> Ces paramètres sont sujets aux mêmes restrictions de l'administrateur que dans les nouveaux certificats. Voir Section 2.3 et Section 6.1 pour plus de détails.

Cette fonction est disponible seulement si exactement un certificat OpenPGP est sélectionné, et que la clé secrète est disponible pour ce certificat.

Certificats → Supprimer (Suppr)

Supprime les certificats sélectionnés du trousseau de clés local.

Cette fonction sert à supprimer des clés inutilisées de votre trousseau local. Toutefois, comme les certificats sont généralement attachés à des courriers électroniques signés, la vérification d'un courriel peut faire réapparaitre dans le trousseau local la clé qui vient d'être supprimée. Il est donc certainement préférable d'éviter de faire appel à cette fonction autant que faire se peut. Si vous êtes perdu, utilisez la barre de recherche ou la fonction **Affichage → Liste hiérarchique des certificats** pour retrouver le contrôle sur l'ensemble des certificats.

> AVERTISSEMENT
> Il y a une exception à ce qui vient d'être dit : quand vous supprimez un de vos propre certificat, vous supprimez du même coup la clé secrète. Cela implique que vous ne serez plus à même de lire d'anciennes communications chiffrées utilisant ce certificat, à moins que vous ne les ayez sauvegardées quelque part.
> Kleopatra vous alertera quand vous tenterez de supprimer une clé secrète.

À cause de la nature hiérarchique des certificats S/MIME, si jamais vous supprimez un émetteur de certificat S/MIME (CA certificat), tous les sujets seront également supprimés. [1]

Bien entendu, cette fonction n'est disponible que si vous sélectionnez au moins un certificat.

Certificats → Copie (Dump) du certificat

Affiche toutes les informations que GpgSM possède au sujet du certificat (S/MIME) sélectionné.

Voir l'explication au sujet de `--dump-key key` dans le manuel de GpgSM pour plus de détails sur cette sortie.

3.4 Menu Outils

Outils → Afficheur de journaux GnuPG...

Démarre GnuPG Log Viewer, un outil qui présente la sortie de débogage des applications GnuPG. Si la signature, le chiffrement ou la vérification s'arrête mystérieusement de fonctionner, vous pourriez trouver pourquoi en regardant à l'intérieur du journal.

Cette fonction n'est pas disponible sous Windows®, étant donné que les mécanismes sous-jacents ne sont pas implémentés dans le moteur sur cette plate-forme.

Outils → Rafraîchir les certificats « OpenPGP »

Rafraîchit tous les certificats OpenPGP en exécutant

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

. Après l'exécution réussi de la commande, votre trousseau local répercutera tous les derniers changements concernant la validité des certificats OpenPGP.

Voir les notes de **Outils → Rafraîchir les certificats « X.509 »** pour quelques mises en garde.

Outils → Rafraîchir les certificats « X.509 »

Rafraîchie tous les certificats S/MIME en exécutant

1. Ce comportement est identique à celui d'un système de fichiers : quand vous supprimez un dossier, tous les dossiers et fichiers qu'il contient sont également supprimés.

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

Après l'exécution réussi de la commande, votre trousseau local répercutera tous les derniers changements concernant la validité des certificats S/MIME.

> NOTE
> Rafraîchir les certificats X.509 et OpenPGP implique le téléchargement de tous les certificats CRLs afin de vérifier qu'aucun d'entre eux n'a été révoqué pendant ce temps.
> Ceci peut mettre à rude épreuve vos propres connexions réseaux ainsi que celles des autres personnes, et peut prendre jusqu'à une heure ou plus à s'achever en fonction de votre connexion réseau et du nombre de certificats à vérifier.

Outils → Importer des LRC depuis un fichier...

Permet d'importer manuellement des CRL depuis des fichiers.

Normalement, les CRL (*Certificate Revocation Lists*, liste de révocation des certificats) sont gérées de manière transparente par le moteur, mais il peut parfois s'avérer utile d'importer une CRL manuellement dans le cache local des CRL.

> NOTE
> Pour que l'importation des CRL fonctionne, l'outil DirMngr doit être dans le `PATH` de recherche. Si l'élément de menu est désactivé, vous devrez contacter l'administrateur système et lui demander d'installer DirMngr.

Outils → Effacer le cache des LRC

Efface le cache CRL de GpgSM.

Vous n'aurez probablement jamais besoin de ceci. Vous pouvez forcer un rafraîchissement du cache des CRL en sélectionnant tous les certificats et en utilisant **Outils → Rafraîchir les certificats « X.509 »** à la place.

Outils → Copie (dump) du cache des LRC

Affiche le contenu détaillé du cache CRL de GpgSM.

3.5 Menu Configuration

Kleopatra possède par défaut le menu **Configuration** de KDE, tel que décrit dans les Fondamentaux de KDE, avec une entrée supplémentaire.

Configuration → Effectuer un contrôle automatique

Effectue une série de tests automatiques et présente leur résultat.

C'est la même série de tests que celle lancée par défaut au démarrage. Si vous avez désactivé les tests automatiques effectués au démarrage, vous pouvez les réactivez ici.

3.6 Menu Fenêtre

Le menu **Fenêtre** vous permet de gérer les onglets. En utilisant les éléments de ce menu, vous pouvez renommer un onglet, en ajouter un nouveau, dupliquer l'onglet courant et le déplacer vers la gauche ou la droite.

En cliquant avec le bouton droit de la souris sur un onglet, vous ouvrez un menu contextuel d'où vous pouvez également sélectionner les même actions.

3.7 Menu Aide

Kleopatra possède par défaut le menu **Aide** de KDE, tel que décrit dans les Fondamentaux de KDE.

Chapitre 4

Liste des options de la ligne de commande

Seules les options spécifiques à Kleopatra sont répertoriées ici. Comme pour toutes les applications de KDE, vous pouvez obtenir une liste complète des options à l'aide de la commande **`kleopatra --help`**.

`--uiserver-socket` ***argument***

Emplacement du socket que le serveur d'interface utilisateur écoute.

`--daemon`

Lance uniquement le serveur d'interfaces, cache la fenêtre principale

`-p --openpgp`

Utilise OpenPGP pour l'opération suivante

`-c --cms`

Utiliser CMS (X.509, S / MIME) pour l'opération suivante

`-i --import-certificate`

Spécifie un fichier ou une URL depuis laquelle importer des certificats (ou des clés secrètes).

C'est la ligne de commande équivalente à **Fichier → Importer des certificats... (Ctrl+I)** .

`-e --encrypt`

Chiffre le(s) fichier(s)

`-s --sign`

Signe le(s) fichier(s)

`-E --encrypt-sign`

Chiffre et/ou signe le(s) fichier(s). Identique à `--sign-encrypt`, ne pas utiliser.

`-d --decrypt`

Déchiffre le(s) fichier(s)

`-V --verify`

Vérification du fichier et de la signature

`-D --decrypt-verify`

Déchiffre et/ou vérifie le(s) fichier(s)

Chapitre 5

Configurer Kleopatra

La boite de dialogue de configuration de Kleopatra est accessible via **ConfigurationConfigurer Kleopatra...**

Chacune des pages qu'elle contient est décrite dans les sections ci-dessous.

5.1 Configurer les services d'annuaire (*Directory Services*)

Sur cette page, vous pouvez configurer quelles serveurs LDAP utiliser pour les recherches de certificats S/MIME et quelles serveurs de clés utiliser pour les recherches de certificats OpenPGP.

> NOTE
> C'est simplement une version plus conviviale de la même configuration que vous pouvez aussi trouver dans la section Section 5.5. Tout ce que vous pouvez configurer ici, vous pouvez le faire également là-bas.

> NOTE CONCERNANT LA CONFIGURATION DE SERVEURS MANDATAIRES
> La configuration de serveurs mandataires pour le HTTP et le LDAP peut être effectuée dans Section 5.4, mais seulement pour GpgSM. Dans le cas de GPG, à cause de la complexité des options de serveurs de clés dans celui-ci et du manque de prise en charge correct pour eux dans GpgConf, vous aurez actuellement besoin de modifier le fichier de configuration `gpg.conf` directement. Veuillez vous référez au manuel de GPG pour plus de détails. Kleopatra conservera cette configuration, mais n'autorise pas encore leur modification depuis le GUI.

La table des **Services d'annuaire** affiche quels serveurs sont actuellement configurés. Double-cliquez sur une cellule de la table pour modifier les paramètres des entrées de serveurs existants.

La signification de chaque colonne est la suivante :

Schéma

Détermine le protocole utilisé pour accéder au serveur. Les schémas les plus souvent utilisées sont **LDAP** (Et son frère **LDAPS** sécurisé avec SSL) pour les serveurs LDAP (protocole courant pour S/MIME ; le seul pris en charge par GpgSM) et **HKP**, *Horowitz Keyserver Protocol*, aujourd'hui habituellement appelé protocole HTTP Keyserver, un protocole fondé sur HTTP prenant en charge littéralement tous les serveurs de clés OpenPGP publiques.

Reportez-vous aux manuels de GPG et de GpgSM pour obtenir une liste des schémas pris en charge.

Nom de serveur

Le nom de domaine du serveur, par exemple `keys.gnupg.net`.

Port du serveur

Le port réseau que le serveur écoute.

Lorsque vous changez le **Schéma**, le port par défaut est automatiquement affecté, à moins qu'il n'ai été fixé de débuter à un port non standard. Si vous aviez changer le port par défaut et n'arrivez pas à le rétablir, essayez de configurer **Schéma** vers **`http`** et **Port du serveur** vers **`80`** (celui par défaut pour le HTTP), puis repartez à partir de là.

ND de base

Le ND de base (seulement pour LDAP et LDAPS), c'est-à-dire la racine de la hiérarchie LDAP à laquelle débuter. Il est souvent également appelé "racine de recherche" ou "base de recherche".

Cela ressemble généralement à **`c=de,o=Foo`**, donné comme faisant partie de l'URL LDAP.

Nom d'utilisateur

Le nom d'utilisateur, s'il y en a un, utilisé pour se connecter au serveur.

Cette colonne est affichée seulement si l'option **Afficher le nom d'utilisateur et le mot de passe** (sous la table) est cochée.

Mot de passe

Le mot de passe, s'il y en a un, utilisé pour se connecter au serveur

Cette colonne est affichée seulement si l'option **Afficher le nom d'utilisateur et le mot de passe** (sous la table) est cochée.

X.509

Cochez cette colonne si cette entrée devrait être utilisée pour les recherches de certificats X.509 (S/MIME).

Seuls les serveurs LDAP (et LDAPS) sont gérés par S/MIME.

OpenPGP

Cochez cette colonne si cette entrée devrait être utilisée pour les recherches de certificats OpenPGP.

Vous pouvez configurer autant de serveurs S/MIME (X.509) que vous le désirez, mais un seul serveur OpenGPG seulement à la fois est autorisé. Le GUI fera respecter cela.

Pour ajouter un nouveau serveur, cliquez sur le bouton **Nouveau**. Cela dupliquera l'entrée sélectionnée, s'il y en a une, ou sinon ajoutera un serveur OpenPGP de défaut. Vous pouvez alors régler le **Nom de serveur**, le **Port du serveur**, le **ND de base**, et les habituelles **Mot de passe** et **Nom d'utilisateur**, qui tous deux ne sont nécessaires que si le serveur requiert une authentification.

Pour ajouter directement une entrée pour un certificat X.509, utilisez **Nouveau** → **X.509** ; utilisez **Nouveau** → **OpenPGP** pour OpenPGP.

Pour supprimer un serveur de la liste de recherche, sélectionnez-le dans la liste et appuyez sur le bouton **Supprimer**.

Pour fixer le délai maximal LDAP, c'est-à-dire la durée maximale durant laquelle le moteur attendra une réponse d'un serveur, renseignez simplement le champ de saisie intitulé **Délai maximal LDAP (minutes :secondes)**.

Si un de vos serveurs comporte une base de données si volumineuse que même des recherches raisonnables comme **`Dupont`** renvoient le **nombre maximal d'éléments retournés par la requête**, vous pourriez être amené à augmenter cette limite. Vous apprendrez aisément si vous atteignez la limite pendant une recherche, car dans pareil cas apparait une boite de dialogue qui vous prévient que les résultats ont été tronqués.

NOTE
Certains serveurs sont susceptibles d'imposer leurs propres limites sur le nombre d'éléments retournés à partir d'une recherche. Dans ce cas, le fait d'augmenter la limite ici ne donnera pas davantage d'éléments retournés.

5.2 Configurer l'Apparence

5.2.1 Configurer les Infobulles

Dans la principale liste de certificats, Kleopatra peut afficher des détails sur un certificats à l'intérieur d'une infobulle. L'information affichée est la même que dans l'onglet **Vue d'ensemble** de la boite de dialogue **Détails du certificat**. Les infobulles peuvent cependant être limitées à l'affichage d'une fraction d'information pour éviter les redondances.

NOTE
L'**ID de clé** est *toujours* affiché afin de s'assurer que, en fin de compte, les infobulles pour différents certificats diffèrent (cela est spécialement important si seulement **Afficher la validité** a été sélectionné.

Vous pouvez activer ou désactiver indépendamment les réglages suivants :

Afficher la validité

Affiche des informations sur la validité du certificat : son état actuel, son DN d'émetteur (S/MIME seulement), ses dates d'expirations (s'il y en a) et ses drapeaux d'utilisation du certificat.

Exemple :

```
Ce certificat est actuellement valable.
Émetteur :            CN=Test-ZS 7,O=Intevation GmbH,C=DE
Validité :          De 25.08.2009 10:42 à 19.10.2010 10:42
Utilisation du certificat : signe des courriels et des fichiers, ↩
    Chiffre des courriels et des fichiers
Empreinte numérique :            DC9D9E43
```

Afficher les informations sur le propriétaire

Affiche des informations sur le propriétaire du certificat : DN du sujet (S/MIME uniquement), identifiants utilisateurs (dont les adresses électroniques) et la confiance envers le propriétaire (OpenPGP seulement).

Exemple OpenPGP :

```
ID utilisateur :           Gpg4winUserA <gpg4winusera@test.hq>
ID de clé :            C6BF6664
Confiance envers le propriétaire :        absolu
```

Exemple S/MIME :

```
Sujet :           CN=Gpg4winTestuserA,OU=Testlab,O=Gpg4win Project,C=DE
Alias :            Gpg4winUserA@test.hq
ID de clé :            DC9D9E43
```

Afficher les détails techniques

Affiche des informations techniques sur le certificat : numéro de série (S/MIME uniquement), type, empreinte numérique et emplacement de stockage.

Exemple :

```
Numéro de série :     27
Type du certificat :  1,024-bit RSA (certificat secret disponible)
Key-ID :            DC9D9E43
Empreinte numérique :       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Conservé :            sur cet ordinateur
```

5.2.2 Configurer les Catégories de certificat.

Kleopatra vous permet de personnaliser l'apparence des certificats dans l'affichage en liste. Cela inclut l'affichage d'une petite icône mais permet également la modification des couleurs d'avant-plan (texte) et d'arrière-plan, ainsi que des polices.

Chaque catégorie de certificat de la liste se voit affecter un ensemble de couleurs, une icône (facultative) et une police dans laquelle sont affichés les certificats appartenant à cette catégorie. La catégorie agit aussi comme un aperçu des paramètres. Les catégories peuvent être définis librement par l'administrateur ou l'utilisateur doté de privilèges : reportez-vous à la section Section 6.2 dans chapitre 6.

Pour définir ou changer l'icône d'une catégorie, sélectionnez-la dans la liste et cliquez sur le bouton **Définir l'icône...**. La boite de dialogue de sélection standard des couleurs de KDE apparait, dans laquelle vous pouvez choisir une icône existante de la collection de KDE ou en charger une personnalisée.

Pour revenir à l'icône standard, cliquez sur le bouton **Apparence par défaut**.

Pour changer la couleur du texte (c'est-à-dire de l'avant-plan) d'une catégorie, sélectionnez-la dans le liste et cliquez sur le bouton **Définir la couleur du texte...**. La boite de dialogue de sélection standard des couleurs de KDE apparait, dans laquelle vous pouvez choisir une couleur existante ou en créer une nouvelle.

Le changement de couleur de l'arrière-plan s'effectue de la même manière. Cliquez simplement à la place sur **Définir la couleur d'arrière-plan...**.

Pour changer la police, deux options vous sont offertes :

1. Modifier la police standard utilisée pour tous les affichages en liste dans KDE.
2. Utiliser une police personnalisée.

La première option présente l'avantage que la police suivra le style que vous choisissez pour l'ensemble de KDE, quel qu'il soit, alors que la seconde vous donne l'entier contrôle sur la police à employer. Ce choix vous appartient.

Pour utiliser la police standard modifiée, choisissez la catégorie dans la liste, puis cochez ou décochez les modificateurs de police **Italique**, **Gras** et/ou **Barrée**. Vous pouvez immédiatement voir l'effet sur la police dans la liste des catégories.

Pour utiliser une police personnalisée, cliquez sur le bouton **Définir la police...**. La boite de dialogue standard de sélection des polices de KDE apparait, dans laquelle vous pouvez sélectionner la nouvelle police.

> NOTE
> Notez que vous pouvez encore vous servir des modificateurs de polices pour changer la police personnalisée, simplement comme pour la modification de la police standard.

Pour revenir à la police standard, cliquez sur le bouton **Apparence par défaut**.

5.2.3 Configurer l'ordre des attributs DN

Bien que les DNs soient hiérarchiques, l'ordre des composants individuels (appelés « DN relatifs » (DNR) ou « attributs DN ») n'est pas défini. L'ordre dans lequel les attributs sont affichés est ainsi une affaire de goût personnel ou de politique d'entreprise, ce qui explique pourquoi il est configurable dans Kleopatra.

> NOTE
> Ce réglage ne s'applique pas seulement à Kleopatra, mais à toutes les applications qui utilisent la technologie Kleopatra. Au moment de la rédaction de ce document, sont concernés KMail, KAddressBook, ainsi que Kleopatra lui-même naturellement.

Cette page de configuration se compose de deux listes : une pour les attributs connus (**Attributs disponibles**) et une décrivant l'**Ordre actuel des attributs**.

Les deux listes contiennent les entrées décrites par la forme abrégée de l'attribut (par exemple **CN**) ainsi que par la forme développée (**Nom d'usage**).

La liste **Attributs disponibles** est toujours triée par ordre alphabétique, alors que l'ordre de la liste **Ordre actuel des attributs** reflète l'ordre des attributs DN configurés : le premier attribut de la liste est aussi celui qui est affiché le premier.

Seuls les attributs explicitement répertoriés dans la liste **Ordre actuel des attributs** sont affichés entièrement. Le reste est masqué par défaut.

Cependant, si l'élément fictif **_X_** (**Tous les autres**) est dans la liste « actuelle », tous les attributs non répertoriés (qu'ils soient connus ou non), sont insérés au niveau de **_X_** dans leur ordre relatif d'origine.

Un petit exemple vous éclairera davantage :

Étant donné le DN
    O=KDE, C=US, CN=Dave Devel, X-BAR=foo, OU=Kleopatra, X-FOO=bar,
L'ordre attribué par défaut de "CN, L, _X_, OU, O, C" générera le DN formaté suivant :
    CN=Dave Devel, X-BAR=foo, X-FOO=bar, OU=Kleopatra, O=KDE, C=US
alors que "CN, L, OU, O, C" générera
    CN=Dave Devel, OU=Kleopatra, O=KDE, C=US
Pour ajouter un attribut à la liste d'ordre d'affichage, sélectionnez-le dans la liste **Attributs disponibles** et cliquez sur le bouton **Ajouter à l'ordre actuel des attributs**.

Pour supprimer un attribut de la liste d'ordre d'affichage, sélectionnez-le dans la liste **Attributs disponibles** et cliquez sur le bouton **Supprimer de l'ordre actuel des attributs**.

Pour déplacer un attribut au début (à la fin), sélectionnez-le dans la liste **Ordre actuel des attributs** et cliquez sur le bouton **Déplacer vers le haut** (**Déplacer vers le bas**).

Pour déplacer un attribut vers le haut (le bas) d'un niveau seulement, sélectionnez-le dans la liste **Ordre actuel des attributs** et cliquez sur le bouton **Remonter** (**Redescendre**).

5.3 Configurer les opérations de chiffrement

5.3.1 Configurer les Opérations de courriel

Vous pouvez configurer ici certains aspects des opérations de courriel du serveur d'interfaces de Kleopatra. Actuellement, vous pouvez seulement configurer si vous voulez ou non utiliser le "Mode rapide" pour, respectivement, signer et chiffrer des courriels.

Quand le "Mode rapide" est activé, aucune boite de dialogue n'est affichée lorsque vous signez (ou chiffrez) des courriels, à moins qu'il n'apparaisse un conflit nécessitant une intervention manuelle.

5.3.2 Configurer les Opérations de fichiers

Vous pouvez configurer ici certains aspects des opérations de fichiers du serveur d'interfaces de Kleopatra. Vous pouvez actuellement choisir le programme de contrôle à utiliser pour **CHECKSUM_CREATE_FILES**.

Servez vous de **Programme de somme de contrôle à utiliser** pour choisir quel programme doit être utilisé lors de la création de fichier de somme de contrôle parmi les programmes configurés.

Lors de la vérification des sommes de contrôle, le programme à utiliser est automatiquement détecté, grâce aux noms des fichiers de contrôle trouvés.

> NOTE
> L'administrateur et l'utilisateur doté de privilèges peuvent entièrement définir quels programmes rendre disponible pour Kleopatra à travers les dénommées "Définitions de la somme de contrôle" dans le fichier de configuration. Voir Section 6.4 dans chapitre 6 pour plus de détails.

5.4 Configuration des aspects de la validation « S / MIME »

Sur cette page, vous pouvez configurer certains aspects de la validation des certificats S/MIME.

> NOTE
> C'est simplement, en grande partie, une version plus conviviale des mêmes réglages que vous pouvez aussi trouver dans Section 5.5. Tout ce que vous pouvez configurer ici, vous pouvez également le faire là-bas, à l'exception de **Vérifie la validité des certificats toutes les *N* heures.** qui est spécifique à Kleopatra.

La signification de chacune des options est la suivante :

5.4.1 Configurer la vérification périodique des certificats

Vérifie la validité des certificats toutes les *N* heures.

Cette option active la vérification périodique de la validité des certificats. L'effet de la vérification périodique est le même que **Affichage → Actualiser (F5)** ; la programmation périodique de **Outils → Rafraîchir les certificats « OpenPGP »** ou **Outils → Rafraîchir les certificats « X.509 »** n'est pas prévu.

> NOTE
> La validation est effectuée implicitement à chaque fois que des fichiers significatifs sont modifiés dans `~/.gnupg`. Cette option, comme **Outils → Rafraîchir les certificats « OpenPGP »** et **Outils → Rafraîchir les certificats « X.509 »**, affecte donc seulement les facteurs externes de la validité des certificats.

5.4.2 Configurer la méthode de validation

Valider les certificats en utilisant des LRC

Si cette option est sélectionnée, les certificats S/MIME sont validés en utilisant les Listes de Révocations de Certificats (LRC).

Voir **Valider les certificats en ligne (OCSP)** pour obtenir des méthodes alternatives de vérification de validité de certificat.

Valider les certificats en ligne (OCSP)

Si cette option est sélectionnée, les certificats S/MIME sont validés en ligne en utilisant le protocole de vérification en ligne de certificat (*Online Certificates Status Protocol*, OCSP).

> AVERTISSEMENT
> Quand vous choisissez cette méthode, une requête est envoyée au serveur de la CA plus ou moins à chaque fois que vous envoyez ou recevez un message chiffré, permettant théoriquement à l'agence de certification émettrice de localiser celui avec qui vous échangez des (par exemple) courriels.

Pour utilisez cette méthode, vous aurez besoin de saisir l'URL du serveur OCSP dans **URL du serveur OCSP**.

Voir **Valider les certificats en ligne (OCSP)** pour obtenir une méthode plus traditionnelle de vérification de validité de certificat qui ne divulgue pas d'informations sur celui avec qui vous échangez des courriels.

URL du serveur OCSP

Saisissez ici l'adresse du serveur pour la validation en ligne des certificats (du serveur OCSP). L'URL commence habituellement par `http://` .

Signature du serveur OCSP :

Sélectionnez ici le certificat avec lequel le serveur OCSP signe ses réponses.

Ignorer l'URL de service des certificats

Chaque certificat S/MIME contient généralement l'URL de son serveur OCSP de l'émetteur (**Certificats → Copie (Dump) du certificat** révélera si un certificat donné en contient une).

Cochez cette option fais ignorer ces URL par GpgSM et seulement prendre en compte celle configurée au-dessus.

Utiliser cela pour, par exemple, imposer l'utilisation d'un serveur mandataire OCSP à travers toute une société.

5.4.3 Configurer les options de validation

Ne pas vérifier les règles de certificat

Par défaut, GpgSM utilise le fichier `~/.gnupg/policies.txt` pour vérifier si une règle de certificat est permise. Si cette option est sélectionnée, les règles ne sont pas vérifiées.

Ne jamais consulter une LRC

Si cette option est activée, les listes de révocation de certificats ne sont jamais utilisées pour valider les certificats S/MIME.

Autoriser le marquage de confiance des certificats racines

Si cette option est activée lorsque le certificat CA racine est importé, il vous sera demandé de confirmer son empreinte numérique et si vous considérez ou non sa signature comme de confiance.

Un certificat racine a besoin d'être de confiance avant de pouvoir considérer les certificats qui en proviennent comme de confiance également. Mais avoir confiance en des certificats racines trop facilement peut abaisser la sécurité générale du système.

> NOTE
> Activer cette fonctionnalité dans le moteur peut vous amenez à être dérangé par des menus contextuels de PinEntry à des moments inopportuns (c'est-à-dire à la vérification des signatures), et peut ainsi bloquer le traitement des courriels laissé sans surveillance. Pour cette raison, et parce qu'il est souhaitable d'être en mesure de *ne plus faire confiance* à un certificat racine de confiance à nouveau, Kleopatra permet le réglage manuel du niveau de confiance en utilisant **Certificats → Certificat racine de confiance** et **Certificats → Certificat racine de méfiance** .
> Les réglages ici n'influencent pas la fonction de Kleopatra.

Recevoir les certificats sans émetteur

Si cette option est activée, les certificats sans émetteur sont reçus lorsque nécessaire (cela s'applique aux deux méthodes de validation, par LRC et par OCSP).

5.4.4 Configurer les options des requêtes HTTP

N'effectuer aucune requête HTTP

Désactiver totalement l'utilisation de HTTP pour S/MIME.

Ignorer le point de distribution de LRC HTTP des certificats

Lorsque l'emplacement d'une LRC est recherché, le certificat à tester contient généralement des entrées connues comme le "point de distribution de LRC" (DP, *CRL Distribution Point*) qui sont des URLs décrivant le moyen d'accéder aux LRC. La première entrée DP trouvée est utilisée.

Avec cette option, toutes les entrées utilisant le protocole HTTP sont ignorées lors de la recherche d'un DP adéquat.

Utiliser le serveur mandataire HTTP du système

Si cette option est sélectionnée, le serveur mandataire HTTP affiché à droite (Correspondant à la variable d'environnement `http_proxy`) sera utilisé pour toute requête HTTP.

Utiliser ce serveur mandataire pour les requêtes HTTP

Si aucun système de serveur mandataire n'est défini, ou si vous avez besoin d'utiliser un serveur mandataire différent pour GpgSM, veuillez saisir son emplacement ici.

Il sera utilisé pour toutes les requêtes HTTP relatives à « S / MIME ».

La syntaxe est **`machine:port`**, c'est-à-dire **`mon-proxy.quelque-part.com:3128`**.

5.4.5 Configurer les options des requêtes LDAP

N'effectuer aucune requête LDAP

Désactive totalement l'utilisation de LDAP pour S/MIME.

Ignorer le point de distribution des LRC LDAP des certificats

Lorsque l'emplacement d'une LRC est recherché, le certificat à tester contient généralement des entrées connues comme « point de distribution de LRC » (DP) qui sont des URLs décrivant un moyen d'accès. La première entrée DP trouvée est utilisée.

Avec cette option, toutes les entrées utilisant le protocole LDAP sont ignorées lors de la recherche d'un DP adéquat.

Hôte primaire pour les requêtes LDAP

Indiquer un serveur LDAP ici fera passer toutes les requêtes LDAP d'abord par ce serveur. Plus précisément, ce réglage prend le pas sur tout *hôte* et *port* spécifié dans une URL LDAP et sera également utilisé si l'*hôte* et le *port* ont été omis dans l'URL.

Les autres serveurs LDAP seront utilisés uniquement si la connexion au "serveur mandataire" échoue. La syntaxe est **hôte** ou **hôte:port**. Si *port* est omis le port 389 (port standard LDAP) sera utilisé.

5.5 Configurer le système GnuPG

Cette partie de la boite de dialogue est générée automatiquement depuis la sortie de **gpgconf --list-components** et, pour tout *composant* que la commande ci-dessus retourne, la sortie de **gpgconf --list-options *composant***.

> NOTE
> La plus utile de ces options a été dupliqué en pages séparées dans la boite de dialogue de configuration de Kleopatra. Reportez vous à Section 5.1 et Section 5.4 pour les deux pages qui contiennent des options sélectionnées depuis cette section de la boite de dialogue.

Le contenu exact de cette section de la boite de dialogue dépend de la version du moteur GnuPG que vous avez installé et, potentiellement, de la plate-forme sur laquelle vous tournez. Ainsi, allons nous discuter seulement la présentation générale de la boite de dialogue, notamment les correspondances permettant de passer des options de GpgConf aux actions du GUI de Kleopatra.

GpgConf retourne des informations de configuration pour plusieurs composants. À l'intérieur de chaque composant, les options individuelles sont réunies en groupes.

Kleopatra affiche un onglet par composant rapporté par GpgConf ; les groupes sont intitulés par une ligne horizontale affichant le nom du groupe comme retourné par GpgConf.

Chaque option de GpgConf a un type. Excepté pour certaines options bien connues que Kleopatra accompagne avec des réglages spécialisés pour une meilleure expérience utilisateur, les correspondances permettant de passer des types GpgConf aux actions du GUI de Kleopatra sont comme suivant :

type GpgConf	**Action de Kleopatra**	
	pour les listes	**pour les non-listes**
`aucun`	Compteur	Case à cocher
`chaine`	N/A	édition de ligne
`int32`	édition de ligne (non formatée)	Compteur
`uint32`		
`nom de l'emplacement`	N/A	action spécialisée
`serveur LDAP`	action spécialisée	N/A
`empreinte clé`	N/A	
`clé publique`		
`clé secrète`		
`liste des alias`		

TABLE 5.1: Correspondance entre les options de GpgConf et les actions du GUI de Kleopatra

Voir le manuel de GpgConf pour des informations supplémentaires sur ce que vous pouvez configurer ici et comment.

Chapitre 6

Guide de l'administrateur

Le guide l'administrateur décrit les différents moyens permettant de personnaliser Kleopatra qui ne sont pas accessibles par l'intermédiaire de l'interface graphique utilisateur, mais uniquement au travers des fichiers de configuration.

Il part du principe que le lecteur connaît déjà la technologie utilisée pour la configuration des applications KDE, y compris la structure, l'emplacement du système de fichiers et l'implantation en cascade des fichiers de configuration de KDE, sans oublier l'infrastructure KIOSK.

6.1 Personnalisation de l'assistant de création des certificats

6.1.1 Personnaliser les champs DN

Kleopatra vous permet de personnaliser les champs que l'utilisateur pourra renseigner afin de créer des certificats.

Créez un groupe appelé `CertificateCreationWizard` dans le fichier `kleopatrarc` pour tout le système. Si vous souhaitez avoir un ordre personnalisé des attributs ou ne voir apparaitre que certains éléments, créez une clé appelée `DNAttributeOrder`. Le ou les arguments sont à choisir parmi `CN`,`SN`,`GN`,`L`,`T`,`OU`,`O`,`PC`,`C`,`SP`,`DC`,`BC`,`EMAIL`. Pour initialiser des champs avec une valeur donnée, écrivez quelque chose comme « Attribut=valeur ». Pour que l'attribut soit considéré comme un attribut requis, ajoutez-y à la fin un point d'exclamation (par exemple, `CN !`,`L`,`OU`,`O !`,`C !`,`EMAIL !`, ce qui s'avère justement être la configuration par défaut).

L'utilisation du modificateur de mode KIOSK `$e` vous permet d'extraire les valeurs issues des variables d'environnement, d'un script ou d'un binaire évalué. Pour en plus désactiver l'édition du champ respectif, faites appel au modificateur `$i`. Pour interdire l'utilisation du bouton **Insérer mon adresse**, réglez `ShowSetWhoAmI` à « False ».

> TUYAU
> En raison de la nature de l'infrastructure KIOSK de KDE, l'emploi du drapeau immuable (`$i`) interdit à l'utilisateur de ne pas tenir compte du drapeau. C'est un comportement intentionnel. `$i` et `$e` peuvent aussi bien être utilisés avec toutes les autres clés de configuration dans les applications KDE.

L'exemple suivant donne un aperçu des personnalisations possibles :

```
[CertificateCreationWizard]
 ; interdit de copier des données personnelles provenant du carnet d' ↩
    adresses, ne pas autoriser la prise de contrôle locale
ShowSetWhoAmI[$i]=false
```

```
 ; définit le nom de l'utilisateur à $UTILISATEUR
CN[$e]=$UTILISATEUR

 ; définit le nom de l'entreprise à « Mon Entreprise », interdit l'édition
O[$i]=Mon Entreprise

 ; définit le nom du département à une valeur retournée par un script
OU[$ei]=$(lookup_dept_from_ip)

 ; définit le pays à FR, mais autorise des changements par l'utilisateur
C=FR
```

6.1.2 Restreindre les types de clés qu'un utilisateur est autorisé à créer

Kleopatra permet aussi de restreindre les types de certificats qu'un utilisateur est autorisé à créer. Notez tout de même qu'un moyen facile de contourner ces restrictions est de simplement en créer un à l'aide de la ligne de commande.

6.1.2.1 Algorithme à clés publiques

Pour contrôler l'algorithme à clés publiques à utiliser, veuillez ajouter la clé de configuration `PGPKeyType` (Et `CMSKeyType`, mais seulement RSA est géré pour CMS de toute façon) à la section `CertificateCreationWizard` de `kleopatrarc`.

Les valeurs autorisées sont`RSA` pour des clés RSA, `DAS` pour les clés (Pour signer uniquement) DSA, et `DSA + ELG` pour une clé (pour signer uniquement) DSA avec une sous-clé ElGamal pour le chiffrement.

La configuration par défaut est lu depuis GpgConf ou sinon depuis `RSA`, si GpgConf n'en fournit pas.

6.1.2.2 Taille des Clés Publiques

Pour restreindre les tailles de clés disponibles pour un algorithme publique, ajouter la clé de configuration `<ALG>Tailles-clé` (où *ALG* peut être `RSA`, `DSA` ou `ELG`) par la `CertificateCreationWizard` section de `kleopatrarc`, contenant une liste de taille de clé (en bits) séparées par des virgules. Une taille de clé par défaut peut être indiquée en la faisant précéder par un trait d'union (`-`).

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

L'exemple ci-dessus restreindra les tailles de clé RSA autorisées à 1536, 2048 et 3072, avec 2048 par défaut.

En plus des tailles elles-même, vous pouvez aussi spécifier une étiquette pour chacune des tailles. Il suffit de fixer la configuration de clé `ALG KeySizeLabels` à une liste d'étiquettes séparées par des virgules.

```
RSAKeySizeLabels = faible,normal,fort
```

Celui de dessus, en liaison avec l'exemple précédent, écrirait quelque chose comme les options suivantes pour la sélection :

```
faible (1536 bits)
              normal (2048 bits)
              fort (3072 bits)
```

Ceux par défaut sont comme si le suivant avait effet :

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

6.2 Créer et éditer des catégories de clés

Kleopatra permet à l'utilisateur de configurer l'apparence visuelle des clés en se basant sur un concept appelé **Catégories de clés**. Les **Catégories de clés** sont aussi utilisées pour filtrer la liste des certificats. Cette section décrit de quelle manière il est possible d'éditer les catégories disponibles et d'en ajouter de nouvelles.

Lorsqu'on essaie de trouver la catégorie à laquelle une clé appartient, Kleopatra tente de faire correspondre une clé à une séquence de filtres de clés, configurée dans le fichier `libkleopatrarc`. Le premier à correspondre définit la catégorie, en s'appuyant sur un concept de *spécificité*, expliqué plus loin.

Chaque filtre de clés est défini dans un groupe de configuration nommé `Key Filter #n`, où *n* est un nombre à partir de `0`.

Les seules clés obligatoires dans un groupe `Key Filter #n` sont `Name`, qui contient le nom de la catégorie tel qu'il est affiché dans la boite de dialogue de configuration, et `id`, qui est utilisé comme référence pour le filtre dans d'autres sections de configuration (comme `Vue #n`).

Tableau 6.1 répertorie toutes les clés qui définissent les propriétés d'affichage des clés appartenant à cette catégorie (c'est-à-dire les clés qui peuvent être ajustées dans la boite de dialogue de configuration), alors que Tableau 6.2 dresse la liste de toutes les clés qui définissent les critères par rapport auxquels le filtre correspond aux clés.

Clé de configuration	Type	Description
`couleur d'arrière-plan`	couleur	La couleur d'arrière-plan à utiliser. Si elle est absente, sera par défaut celle définie globalement pour les affichages en liste.
`couleur d'avant-plan`	couleur	La couleur d'avant-plan à utiliser. Si elle est absente, sera par défaut celle définie globalement pour les affichages en liste.
`police`	police	La police par défaut à utiliser. La police sera mise à l'échelle de façon à correspondre à la taille configurée pour les affichages en liste, et tout attribut de police (voir ci-dessous) sera appliqué.

font-bold	booléen	Si défini à True et si font n'est pas défini, utilise la police par défaut de l'affichage en liste avec ajout du style de police Gras (si disponible). Ignoré si font est également présent.
font-italic	booléen	Analogue à font-bold, mais pour les polices de type italique au lieu de gras.
police-barrée	booléen	Si True, trace une ligne au centre de la police. Appliqué même si font est défini.
icône	texte	Le nom d'une icône à afficher dans la première colonne. N'est pas encore mis en œuvre.

TABLE 6.1: Clés de configuration des filtres de clés définissant les propriétés d'affichage

Clé de configuration	**Type**	**Si spécifié, le filtre correspond quand...**
is-revoked	booléen	la clé a été révoquée.
match-context	contexte[1]	le contexte auquel le filtre correspond.
is-expired	booléen	la clé a expiré.
is-disabled	booléen	la clé a été désactivée (marquée afin de ne pas être utilisée) par l'utilisateur. Ignoré pour les clés S/MIME.
is-root-certificate	booléen	la clé est un certificat racine. Ignoré pour les clés OpenPGP.
can-encrypt	booléen	la clé peut servir pour le chiffrement.
can-sign	booléen	la clé peut servir pour signer.
can-certify	booléen	la clé peut servir pour signer (certifier) d'autres clés.
can-authenticate	booléen	la clé peut servir pour l'authentification (par exemple comme certificat de client TLS).

1. Le contexte est un listage des valeurs autorisées suivantes : appearance, filtering et any.

`is-qualified`	booléen	la clé peut être utilisée pour faire des Signatures Qualifiées (comme définie par la loi allemande sur la signature numérique).
`is-cardkey`	booléen	le matériel clé est stockée sur une carte à puce (et non sur l'ordinateur).
`has-secret-key`	booléen	la clé secrète de cette paire de clés est disponible.
`is-openpgp-key`	booléen	la clé est une clé OpenPGP (`True`) ou une clé S/MIME (`False`).
`was-validated`	booléen	la clé a été validée.
`prefix-ownertrust`	validité[2]	la clé a exactement (*`prefix`* = `is`), n'a rien sauf (*`prefix`* = `is-not`), a au moins (*`prefix`* = `is-at-least`) ou a au plus (*`prefix`* = `is-at-most`) la confiance du propriétaire en question comme valeur pour la clé de configuration. Si plusieurs clés `prefix-ownertrust` (avec des valeurs *`prefix`* différentes) sont présentes dans un seul groupe, le comportement est indéfini.
`prefix-validity`	validité	Analogue à `prefix-ownertrust`, mais pour la validité des clés au lieu de la confiance du propriétaire.

TABLE 6.2: Clés de configuration des filtres de clés définissant les critères du filtre

NOTE

Quelques-uns des critères les plus intéressants, comme `is-revoked` ou `is-expired` ne fonctionneront que sur des clés *validées*, ce qui explique pourquoi par défaut, la révocation et l'expiration n'est vérifiée que pour les clés validées, bien que vous soyez libre de supprimer ces contrôles supplémentaires.

En plus de la liste des clés configurées ci-dessous, un filtre de clés peut aussi avoir un `id` et un `match-contexts`.

En utilisant l'`id` du filtre, qui est par défaut le nom du groupe de configuration du filtre s'il n'est pas donné ou vide, vous pouvez indiquer le filtre de clés autre part dans la configuration, par

2. La validité est un listage (ordonnée) des valeurs autorisées suivantes : `unknown`, `undefined`, `never`, `marginal`, `full`, `ultimate`. Reportez-vous aux manuels de GPG et GpgSM pour une explication détaillée.

exemple dans l'affichage de la configuration de Kleopatra. L'`id` n'est pas interprété par Kleopatra, vous pouvez donc utiliser n'importe quelle chaine, tant quelle reste unique.

`match-contexts` limite la pertinence du filtre. Deux contexte sont actuellement définis : le contexte d'`appearance` est utilisé lors de la définition des couleurs et des propriétés de la police pour la vue. Le contexte `filtering` est utilisé pour inclure (et exclure) sélectivement des certificats de la vue. `any` peuvent être utilisé pour désigner tous les contextes définis actuellement, et c'est celui par défaut si `match-contexts` n'est pas donné, ou sinon ne produit aucun contexte. Cela assure qu'aucun filtre de clés ne se retrouve "mort", c'est-à-dire avec aucun contexte à lui appliquer.

Le format de l'entrée est une liste d'identificateurs, séparés par des caractères qui ne sont pas des mots. Chacun de ces identificateurs peut être précédé par un point d'exclamation (`!`), indiquant la négation. Les identificateurs agissent dans l'ordre sur une liste externe de contextes, qui débute vide. Le mieux est de l'expliquer par un exemple : `tous !appearance` est le même que `filtering` et `appearance !appearance` produit un groupe vide, comme l'est `!any`. Cependant, les deux derniers seront remplacés en interne par `any`, car ils ne produisent aucun contexte du tout.

En général, les critères non spécifiés (c'est-à-dire dont l'élément de configuration n'est pas défini) ne sont pas vérifiés. Si un critère est indiqué, il est déceler et doit correspondre au filtre comme un ensemble pour convenir, c'est-à-dire que les critères sont « combinés en ET » (*AND'ed together*).

Chaque filtre a une "spécificité" tacite qui est utilisée pour classer tous les filtres correspondants. Le filtre le plus spécifique l'emporte sur les filtres les moins spécifiques. Si deux filtres ont la même spécificité, celui qui vient en premier dans le fichier de configuration l'emporte. La spécificité du filtre est proportionnelle au nombre de critère qu'il contient.

Exemple 6.1 Exemples de filtres de clés

Pour vérifier tous les certificats racines arrivés à expiration mais non révoqués, vous devriez utiliser un filtre de clés défini comme suit :

```
[Key Filter #n]
Name=expired, mais pas révoqué
was-validated=true
is-expired=true
is-revoked=false
is-root-certificate=true
 ; ( specificity 4 )
```

Pour vérifier toutes les clés OpenPGP désactivées (Kleopatra ne le gère pas encore) ayant au moins la confiance « minimale » du propriétaire, vous devriez utilisez :

```
[Key Filter #n]
Name=clés OpenPGP désactivées ayant la confiance minimale ou d'un niveau ↩
    plus élevé du propriétaire
is-openpgp=true
is-disabled=true
is-at-least-ownertrust=marginal
 ; ( specificity 3 )
```

6.3 Configurer les gestionnaires d'archives pour être utilisés avec les fichiers signés/chiffrés.

Kleopatra permet à l'administrateur (et à l'utilisateur doté de privilèges) de configurer la liste des gestionnaires d'archives qui sont présentés dans la boite de dialogue Signer/chiffrer des fichiers.

Chaque gestionnaire d'archives est définit dans `libkleopatrarc` comme un groupe d'`Archive Definition #n` séparé, avec les clés obligatoires suivantes :

`extensions`

Une liste d'extensions de nom de fichiers séparés par des virgules qui indique généralement ce format d'archive.

`id`

Un identifiant unique pour identifier ce gestionnaire d'archives en interne. Si vous n'êtes pas sûr, utilisez le nom de la commande.

`Name` (traduit)

Le nom d'utilisateur visible de ce gestionnaire d'archives, comme affiché dans le menu déroulant de la boite de dialogue Signer/Chiffrer des fichiers.

`pack-command`

La commande actuelle pour archiver des fichiers. Vous pouvez utiliser n'importe quelle commande, tant qu'aucun shell n'est requis pour l'exécuter. Le fichier du programme est recherché en utilisant la variable d'environnement `PATH`, à moins que vous n'utilisiez un emplacement de fichier absolu. La citation est prise en charge comme si un shell était utilisé :

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

NOTE

Depuis que l'anti-slash (\) est un caractère d'échappement dans les fichiers de configuration de KDE, vous devez les doubler lors de leurs apparitions dans les noms d'emplacement :

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

. Toutefois, pour la commande en elle-même (Par opposition à ses arguments), vous pourriez peut-être utilisez simplement des slashes (/) comme séparateur d'emplacement sur toutes les plate-formes :

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

. Ceci n'est pas pris en charge dans les arguments comme la plupart des programmes sous Windows® utilise le slash pour les options. Par exemple, la commande suivante ne fonctionnera pas puisque `C:/myarchivescript.bat` est un argument de **cmd.exe** et / n'est pas converti en \ dans les arguments, uniquement les commandes :

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

. Celle-ci doit plutôt être écrite comme ci :

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

6.3.1 Nom de fichier d'entrée passé pour `pack-command`

Il y a trois façons de passer des nom de fichiers à la commande de compression. Pour chacune d'elles, `pack-command` prévoie une syntaxe particulière :

1. Comme argument de la ligne de commande.

   Exemple (tar) :

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

   Exemple (zip) :

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

Dans ce cas, les noms de fichier sont passés dans la ligne de commande, comme ce que vous feriez en utilisant l'invite de commande. Kleopatra n'utilise pas un shell pour exécuter la commande. En conséquence, c'est un moyen sûr de passer des noms de fichier, mais il pourrait survenir des restrictions au sujet de la longueur de la ligne de commande sur certaines plate-formes. Un textuel `%f`, si présent, est remplacé par le noms des fichiers à archiver. Sinon, les noms de fichiers sont ajoutés à la ligne de commande. Ainsi, l'exemple zip ci-dessus pourrait aussi s'écrire comme ceci :

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

2. Via l'entrée standard, séparé par des sauts de ligne : prepend `|`.

   Exemple (Archive « tar » de GNU) :

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

   . Exemple (ZIP) :

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

   . Dans ce cas, les noms de fichiers sont passés au gestionnaire d'archives sur stdin, un par ligne. Ceci évite les problèmes sur les plates-formes définissant une limite basse au nombre d'arguments des lignes de commandes autorisés. Mais, cela ne fonctionne pas lorsque les noms de fichiers contiennent des retours à la ligne.

   > NOTE
   > Kleopatra gère actuellement seulement LF comme séparateur de saut de ligne, et non CRLF. Cela pourrait changer dans de futures versions, en s'appuyant sur les retours utilisateurs.

3. Via l'entrée standard, séparé par des octets NUL : prepend `0|`.

   Exemple (Archive « tar » de GNU) :

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

   . Celui-ci est le même que ci-dessus, excepté que les octets « NULL » sont utilisés pour séparer les noms de fichiers. Depuis que les octets « NULL » sont interdits dans les noms de fichiers, ceci est la façon la plus robuste pour transmettre des noms de fichier, mais tous les gestionnaires d'archives ne le gèrent pas.

6.4 Configurer les programmes de sommes de contrôle pour être utilisés avec Créer/Vérifier des sommes de contrôle

Kleopatra permet à l'administrateur (et à l'utilisateur doté de privilèges) de configurer la liste des programmes de sommes de contrôle que l'utilisateur peut choisir depuis la boite de dialogue et que Kleopatra est capable d'auto-détecter quand demandé pour vérifier une somme de contrôle d'un fichier donné.

NOTE

Pour être utilisable par Kleopatra, la sortie du programme de contrôle (à la fois le fichier de somme de contrôle écrit ainsi que la sortie sur stdout lors de la vérification des sommes de contrôle) doit être compatible avec la commande **md5sum** et **sha1sum** de GNU.
En particulier, le fichier de somme de contrôle doit être fondé sur des lignes, chaque ligne ayant le format suivant :

```
SOMME-DE-CONTRÔLE ' ' ( ' ' | '*' ) NOM-DE-FICHIER
```

où *SOMME-DE-CONTRÔLE* est constitué seulement de caractères hexadécimaux. Si *NOM-DE-FICHIER* contient un caractère de saut de ligne, la ligne doit plutôt être lue

```
\SOMME-DE-CONTRÔLE ' ' ( ' ' | '*' ) NOM-DE-FICHIER-DE-SECOURS
```

où *NOM-DE-FICHIER-DE-SECOURS* est le nom de fichier avec les sauts de ligne remplacés par des \ns, et des antislashes doubles (\↦\\).
De même, la sortie de `verify-command` doit être de la forme

```
NOM-DE-FICHIER ( « : Ok » | « : ÉCHEC » )
```

séparés par des sauts de ligne. Les sauts de ligne et autres caractères *ne sont pas* soustraits de la sortie.[a]

a. Effectivement, ces programmes n'ont pas été écrit avec des interfaces graphiques à l'esprit, et Kleopatra ne parviendra pas à analyser correctement les noms de fichiers pathologiques qui contiennent de multiples « : Ok » et sauts de ligne.

Chaque programme de contrôle est définie dans `libkleopatrarc` comme un groupe `Checksum Definition #n` distinct, avec les clés obligatoires suivantes :

`file-patterns`

Une liste d'expressions rationnelles décrivant les fichiers qui doivent être considérés comme des fichiers de sommes de contrôle pour ce programme de calcul de sommes de contrôle. La syntaxe est celle utilisée pour les listes de chaines dans les fichiers de configuration de KDE.

NOTE

Comme les expressions rationnelles contiennent généralement des anti-slashes, veuillez prendre soin de bien les supprimer du fichier de configuration. L'utilisation d'un outil d'édition de fichier de configuration est recommandée.

La plate-forme définit si les motifs sont traités en prenant en compte ou non la casse.

`output-file`

Le nom du fichier de sortie caractéristique de ce programme de somme de contrôle (doit, évidemment, correspondre à un des `file-patterns`). C'est celui que Kleopatra utilisera comme nom de fichier de sortie quand il créera des fichiers de somme de contrôle de ce type.

`id`

Un identifiant unique utilisé pour identifier ce programme de somme de contrôle en interne. Si vous n'êtes pas sûr, utilisez le nom de la commande.

`Name` (traduit)

Le nom du programme de somme de contrôle visible par l'utilisateur, comme affiché dans le menu déroulant de la boite de configuration de Kleopatra.

`create-command`

La commande actuelle avec laquelle créer des fichiers de sommes de contrôle. La syntaxe,

les restrictions et les options de passage des arguments sont les mêmes que décrits pour `pack-command` dans Section 6.3.

`verify-command`

Pareil que `create-command`, mais pour la vérification de sommes de contrôle.

Voici 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
```

Chapitre 7

Remerciements et licence

CONTRIBUTEURS

— 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

Traduction française par Joëlle Cornavin jcorn@free.fr et Robin Guitton robin.guitton@sud-ouest.org.