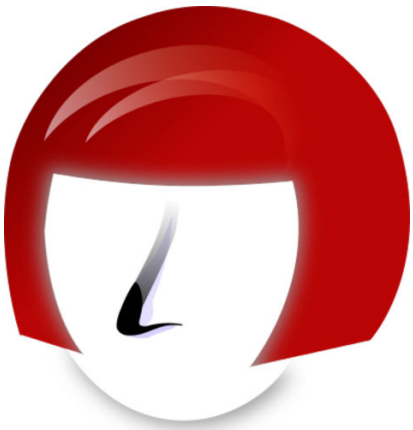
Manual do Kleopatra

Marc Mutz
Desenvolvimento: David Faure
Desenvolvimento: Steffen Hansen
Desenvolvimento: Matthias Kalle Dalheimer
Desenvolvimento: Jesper Pedersen
Desenvolvimento: Daniel Molkentin
Tradução: Marcus Gama
Tradução: André Marcelo Alvarenga



Conteúdo

Lista de Tabelas

Resumo

Kleopatra é uma ferramenta para gerenciar certificados X.509 e OpenPGP.

Capítulo 1

Introdução

Kleopatra é a ferramenta do KDE para gerenciar certificados X.509 e OpenPGP nos chaveiros do GpgSM e do GPG e também para obter certificados de servidores LDAP e de outros servidores.

O Kleopatra poderá ser iniciado a partir do menu **Ferramentas** → **Gerenciador de Certificados** do KMail, assim como a partir da linha de comando. O executável do Kleopatra chama-se **`kleopatra`**.

> NOTA
> Este programa obteve o nome da Cleópatra, uma famosa faraó egípcia que viveu no tempo de Júlio César, com quem teve um filho, Pequeno César, não reconhecido como seu herdeiro.
> O nome foi escolhido, uma vez que este programa tem origem nos Projetos Ägypten (Ägypten significa Egito em alemão). Kleopatra é a tradução em alemão de Cleópatra.

Capítulo 2

Funções Principais

2.1 Vendo a Caixa de Chaves Local

A função principal do Kleopatra é mostrar e editar o conteúdo do chaveiro local, que é semelhante ao conceito de chaveiros do GPG, ainda que uma pessoa não possa se limitar a esta analogia em demasia.

A janela principal está dividida na grande área de listagem de chaves, na barra de menu e na barra de procura no topo e ainda por uma barra de estado na base.

Cada linha da lista de chaves corresponde a um certificado, identificado pelo **DN do Sujeito**. O DN é um acrônimo para 'Distinguished Name' ou 'Nome Distinto', um identificador hierárquico, de certa forma semelhante a uma localização num sistema de arquivos com uma sintaxe ligeiramente diferente, permitindo identificar de forma única e global um determinado certificado.

Para serem válidas e para poderem ser usadas, as chaves (públicas) devem ser assinadas por uma CA (Autoridade de Certificação). Estas assinaturas são chamadas de certificados, mas normalmente os termos 'certificado' e 'chave (pública)' são usados nas mesmas circunstâncias, razão pela qual não será também feita nenhuma distinção entre elas neste manual, a não ser quando indicado explicitamente.

As CA deverão estar, por sua vez, assinadas por outras CAs para serem válidas. Obviamente isto terá de parar em algum ponto, como tal a CA do nível superior (a CA raiz) assina a sua chave com ela própria (isto é chamado de auto-assinatura). Os certificados raiz precisam, por isso, ser validados (normalmente chamada de confiança) manualmente, por exemplo depois de comparar a impressão digital com a da página Web da CA. Isto é feito tipicamente pelo administrador do sistema ou pelo distribuidor de um produto que use os certificados, mas poderá ser feito pelo usuário com a interface da linha de comando do GpgSM.

Para ver quais os certificados são da raiz, você poderá mudar para o modo de listagem hierárquica de chaves com o **Ver** → **Lista de Chaves Hierárquica**.

O usuário poderá ver os detalhes de qualquer certificado se fizer duplo-clique nele ou usar os **Ver** → **Detalhes do Certificado**. Isto abre uma janela que apresenta as propriedades mais comuns do certificado, a sua cadeia de certificação (isto é a cadeia de emissores até à CA de raiz), e o conteúdo de toda a informação que a infraestrutura é capaz de extrair do certificado.

Se você alterar o chaveiro local sem usar o Kleopatra (por exemplo usando a interface da linha de comando do GpgSM), você poderá atualizar a janela com o .

2.2 Procurando e Importando Certificados

Na maior parte do tempo, você irá adquirir os certificados novos ao verificar as assinaturas nas mensagens de e-mail, uma vez que os certificados estão incorporados nas assinaturas criadas

que as usam. Contudo, se você precisar de enviar uma mensagem para alguém com quem ainda nunca tenha tido contato, você precisa obter o certificado de um diretório LDAP (ainda que o GpgSM possa fazer isto automaticamente), ou através de um arquivo. Você também necessita importar o seu próprio certificado depois de receber a resposta da CA ao seu pedido do certificado.

Para procurar por um certificado num diretório LDAP, selecione a opção **Arquivo** → **Procurar os Certificados no Servidor** e insira algum texto (por exemplo o nome da pessoa de quem deseja o certificado) no campo de texto da janela de **Pesquisa de Certificados no Servidor de Chaves**, pressionando depois no botão **Procurar**. Os resultados serão apresentados na lista de chaves, abaixo da barra de procura, onde você poderá selecionar os certificados observando-os ao clicar no botão de **Detalhes** ou transferi-los com a opção **Importar** na área de chaves locais.

Você poderá configurar a lista de servidores LDAP onde procurar na página **Serviços de Diretório** da janela de configuração do Kleopatra.

Se você recebeu o certificado como um arquivo, tente o . O GpgSM precisa compreender o formato do arquivo de certificado; por favor veja o manual do GpgSM para obter uma lista com os formatos de arquivos suportados.

Se você não criou o seu par de chaves com o GpgSM, também irá precisar importar manualmente as chaves pública e privada do arquivo PKCS#12 que obteve da CA. Você poderá fazer isso na linha de comando com a instrução ou dentro do Kleopatra com o , tal como faria para os certificados 'normais'.

2.3 Criando Novos Pares de Chaves

O item do menu **Arquivo** → **Novo Certificado... (Ctrl+N)** inicia o **Assistente de Criação do Certificado** que o guiará por um conjunto de passos para criar um pedido de certificado.

Sempre que terminar um passo no assistente, clique em **Próximo** para passar ao passo seguinte (ou **Anterior** para rever os passos já completos). A criação do pedido do certificado poderá ser cancelada a qualquer momento clicando no botão **Cancelar**.

Na primeira página do assistente, escolha o tipo de certificado que deseja criar:

Criar um par de chaves do OpenPGP pessoal

Os pares de chaves OpenPGP são criados localmente, sendo certificados pelos seus amigos e conhecidos. Não existe nenhuma autoridade de certificação central. Em vez disso, cada indivíduo cria uma Cadeia de Confiança pessoal, certificando os pares de chaves dos outros usuários com o seu próprio certificado.

Você terá que inserir um **Nome**, **E-Mail** e, opcionalmente, um **Comentário**.

Criar um par de chaves X.509 pessoal e um pedido de certificação

Os pares de chaves X.509 são criados localmente, mas certificados centralizadamente por uma autoridade de certificação (CA). As CAs podem certificar outras CAs, criando uma cadeia de confiança central e hierárquica.

O próximo passo do assistente é inserir os seus dados pessoais para o certificado. Os campos a preencher são:

- **Nome Comum (CN):** O seu nome;
- **Endereço de e-mail (EMAIL):** O seu endereço de e-mail; certifique-se de inseri-lo corretamente—será este o endereço para onde as pessoas irão enviar as mensagens sempre que usarem o seu certificado.
- **Localização (L):** A cidade onde vive;
- **Departamento (OU):** A unidade organizacional onde se encontra (por exemplo, ˝Logística˝);

- **Organização (O):** A organização que você representa (por exemplo, a companhia para quem trabalha);
- **Código do país (C):** O código de duas letras para o país em que vive (por exemplo, ´´BR´´);

O próximo passo no assistente é selecionar se deve-se gravar o certificado num arquivo ou enviá-lo diretamente para uma CA. Você terá que especificar o arquivo ou o endereço de e-mail para onde enviar o pedido do certificado.

2.3.1 Revogando uma chave

Um par de chaves que expirou pode ser restaurado para um estado operacional caso você tenha acesso à chave privada e frase-senha. Para gerar com confiança uma chave inutilizável, você precisa revogá-la. A revogação é feita adicionando uma assinatura especial de revogação à chave.

Esta assinatura de revogação é armazenada em um arquivo separado. Este arquivo pode depois ser importado para o chaveiro sendo então anexado à chave tornando-a inutilizável. Por favor, note que para importar esta assinatura à chave nenhuma senha é necessário. No entanto, você deve armazenar a assinatura de revogação em um local seguro, normalmente diferente do local do seu par de chaves. Uma boa dica é usar um local que possa ser desconectado de seu computador, copiando para um dispositivo de armazenamento externo como um pendrive USB ou imprimindo-a.

O Kleopatra não oferece uma funcionalidade para criar uma dessas assinaturas de revogação a qualquer momento, mas pode fazer com o aplicativo KGpg do KDE, escolhendo a opção **Chaves** → **Revogar a chave** e, opcionalmente, importar imediatamente a assinatura de revogação para o seu porta-chaves.

Uma forma alternativa de gerar um certificado de revogação é usar o GPG diretamente a partir da linha de comando: **`gpg --output certificado_de_revogação.asc --gen-revoke sua_chave`**. O argumento *`sua_chave`* pode ser um indicador de chave, sendo o ID da chave do seu par de chaves primário ou qualquer parte de um ID de usuário que identifica o seu par de chaves.

Capítulo 3

Referência do menu

3.1 Menu Arquivo

Arquivo → Novo Certificado... (Ctrl+N)

Cria um novo par de chaves (pública e privada) e permite-lhe enviar a parte pública para uma autoridade de certificação (CA) para ser assinada. O certificado resultante é então enviado de volta ou guardado em um servidor LDAP para você obter para o seu chaveiro local, onde poderá usá-lo para assinar e descriptografar as mensagens de e-mail.

Este modo de funcionamento é chamado de 'geração de chaves descentralizada', uma vez que todas as chaves são criadas localmente. O Kleopatra (e o GpgSM) não suporta a 'geração de chaves centralizada' diretamente, mas o usuário poderá importar o pacote de chaves pública/privada que recebe da CA no formato PKCS#12 através do **Arquivo → Importar os Certificados... (Ctrl+I)** .

Arquivo → Procurar por Certificados no Servidor... (Ctrl+Shift+I)

Procura e importa os certificados dos servidores de certificados para o porta-chaves local. Veja mais detalhes em Seção 2.2.

Você deverá ter os servidores de chaves configurados para isto funcionar. Veja mais detalhes em Seção 5.1.

Arquivo → Importar os Certificados... (Ctrl+I)

Importa certificados e/ou chaves secretas de arquivos na caixa de chaves local. Veja mais detalhes em Seção 2.2.

O formato do arquivo de certificado deve ser suportado pelo GpgSM/GPG. Por favor consulte no manual do GpgSM e do GPG a lista de formatos suportados.

Arquivo → Exportar os Certificados... (Ctrl+E)

Exporta os certificados selecionados para um arquivo.

A extensão do nome do arquivo que escolher para o arquivo de exportação determina o formato do mesmo:

- Para os certificados do OpenPGP, o `gpg` e o `pgp` irão dar origem a um arquivo binário, enquanto o `asc` irá originar um arquivo suportado em ASCII.
- Para os certificados S/MIME, o `der` irá dar origem a um arquivo binário, codificado em DER, enquanto o `pem` irá resultar num arquivo suportado em ASCII.

A menos que sejam selecionados vários certificados, o Kleopatra irá propor `impressão-digital.{asc,pem}` como nome para o arquivo de exportação.

Esta função só está disponível quando tiver selecionado um ou mais certificados.

> NOTA
> Esta função exporta apenas as chaves públicas, mesmo que a chave privada esteja disponível. Use a opção **Arquivo → Exportar chaves privadas...** para exportar as chaves privadas para um arquivo.

Arquivo → Exportar chaves privadas...

Exporta a chave privada para um arquivo.

Na caixa de diálogo que aparece, você poderá escolher se deseja criar um arquivo de exportação binário ou ASCII (**armação em ASCII**). Depois, clique no ícone da pasta à direita do campo **Arquivo de destino** e selecione a pasta e o nome do arquivo. Ao exportar as chaves privadas S/MIME, você também poderá escolher a **Codificação da frase-senha**. Para mais detalhes, veja a discussão sobre a opção `--p12-charset codificação`, no manual do GpgSM.

Esta função só está disponível quando tiver selecionado exatamente um certificado, estando disponível a chave privada para esse certificado.

> ATENÇÃO
> Só raramente deverá ser necessário usar esta função e, se for, deverá ser planejada com cuidado. A migração de uma chave privada envolve a escolha do meio de transporte e a remoção segura dos dados da chave da máquina antiga, entre outras coisas.

Arquivo → Exportar os Certificados para um Servidor... (Ctrl+Shift+E)

Publica os certificados selecionados num servidor de chaves (apenas no OpenPGP).

O certificado é enviado para o servidor configurado para o OpenPGP (cf. Seção 5.1), se estiver definido, caso contrário é enviado para o `keys.gnupg.net`.

Esta função só está disponível se estiver selecionado pelo menos um certificado de OpenPGP (e nenhum S/MIME).

> NOTA
> Quando os certificados de OpenPGP tiverem sido exportados para um servidor de diretório público, será quase impossível removê-los de novo. Antes de exportar o seu certificado para um servidor público, certifique-se que criou um certificado de revogação, caso queira revogar o certificado posteriormente.

> NOTA
> A maioria dos servidores de certificados de OpenPGP públicos sincronizam-se entre si, assim não há grande vantagem em enviá-los para mais de um.
> Poderá acontecer que uma pesquisa num servidor de certificados não devolva quaisquer resultados, ainda que você tenha enviado o seu certificado para lá. Isto acontece porque a maioria dos servidores públicos de chaves usam o balanceamento sequencial 'round-robin' do DNS para distribuir a carga por várias máquinas. Estas máquinas sincronizam-se umas com as outras, mas isso normalmente só acontece ao fim de cerca de 24 horas.

Arquivo → Descriptografar/Verificar os arquivos...

Descriptografa os arquivos e/ou verifica as assinaturas dos mesmos.

Arquivo → Assinar/Criptografar os arquivos...

Assina e/ou criptografa os arquivos.

Arquivo → Fechar (Ctrl+W)

Fecha a janela principal do Kleopatra. Você poderá restaurá-la a partir do ícone da área de notificação a qualquer momento.

Arquivo → Sair (Ctrl+Q)

Termina o Kleopatra.

3.2 O menu Exibir

Ver → Reexibir (F5)

Atualiza a lista de certificados.

O uso desta função normalmente não é necessária, uma vez que o Kleopatra monitora o sistema de arquivos à procura de alterações e atualiza automaticamente a lista de certificados, sempre que for necessário.

Ver → Parar a operação (Esc)

Pára (cancela) todas as operações pendentes, por exemplo uma procura, listagem ou transferência.

Esta função só está disponível se estiver pelo menos uma operação ativa.

> NOTA
> Devido a limitações na infraestrutura, algumas vezes as operações ficarão penduradas de tal forma que esta função não será capaz de cancelá-las, agora ou mesmo de todo jeito.
> Nesses casos, a única forma de restaurar a ordem é finalizar a execução do SCDaemon, DirMngr, GpgSM e GPG, nessa ordem, através das ferramentas do sistema operacional (**top**, Gerenciador de Tarefas, etc.), até que a operação seja desbloqueada.

Ver → Detalhes do Certificado

Mostra os detalhes do certificado atualmente selecionado.

Esta função só está disponível se estiver selecionado exatamente um certificado.

Esta função também está disponível clicando duas vezes no item correspondente na lista.

Ver → Lista de Chaves Hierárquica

Comuta a lista de chaves entre modo hierárquico e simples.

No modo hierárquico, os certificados estão organizados numa relação de emissor/sujeito, por isso é fácil ver a que hierarquia de certificação pertence um determinado certificado, mas é mais difícil encontrar um determinado certificado inicialmente (ainda que você possa, obviamente, usar a barra de procura).

No modo simples, todos os certificados são mostrados numa lista normal, ordenados de forma alfabética. Neste modo, um determinado certificado é fácil de encontrar, mas não é imediatamente óbvio a que certificado de raiz ele pertence.

Esta função ativa ou desativa o modo hierárquico por página, isto é cada página tem o seu próprio estado hierárquico. Isto acontece para que você possa ter tanto uma listagem plana ou hierárquica à mão, cada uma para sua página.

> NOTA
> A visualização hierárquica só está atualmente implementada para os certificados S/MIME. Existe algum desacordo entre os programadores no que diz respeito à forma correta de apresentar os certificados de OpenPGP de forma hierárquica (basicamente, 'pai = assinante' ou 'pai = assinado').

Ver → Expandir Tudo (Ctrl+.)

Expande todos os itens da lista na visão da lista de certificados, isto é torna todos os itens visíveis.

Este é o valor padrão ao entrar no modo de lista de chaves hierárquico.

Você poderá ainda, é claro, expandir e fechar cada item individualmente.

Esta função só está disponível quando a **Ver → Lista de Chaves Hierárquica** está ativada.

Ver → Fechar Tudo (Ctrl+,)

Fecha todos os itens da lista na visão de lista do certificado, isto é oculta todos os itens menos os de topo.

Você poderá ainda, é claro, expandir e fechar cada item individualmente.

Esta função só está disponível quando a **Ver → Lista de Chaves Hierárquica** está ativada.

3.3 O menu Certificados

Certificados → Modificar a confiança no dono...

Modifica a confiança no dono do certificado de OpenPGP atualmente selecionado.

Esta função só está disponível quando tiver exatamente um certificado de OpenPGP.

Certificados → Confiar no certificado de raiz

Marca este certificado de raiz (S/MIME) como fidedigno.

De alguma forma, isto é o equivalente ao **Certificados → Modificar a confiança no dono...** para os certificados de raiz em S/MIME. Você poderá, contudo, escolher apenas entre —em termos do OpenPGP—confiança 'absoluta' e 'nunca confiar'.

> NOTA
> A infraestrutura (através do GpgAgent) irá perguntar, no momento da importação do certificado de raiz, se deseja confiar no certificado de raiz importado. Contudo, esta função terá que estar explicitamente ativada na configuração da infraestrutura (`allow-mark-trusted` no `gpg-agent.conf`, ou então o **Sistema GnuPG → Agente GPG → Permitir aos clientes marcarem as chaves como ´´fidedignas´´** ou ainda o **Validação S/MIME → Permitir marcar os certificados raiz como confiáveis** em capítulo 5).
> Ativar essa funcionalidade na infraestrutura, poderá fazer com que apareçam mensagens do PinEntry em momentos inoportunos (por exemplo ao verificar as assinaturas), podendo bloquear o processamento do correio não verificado. Por essa razão, e uma vez que se pretende ser possível *renegar* um certificado de raiz fidedigno, o Kleopatra permite a definição manual da confiança.

> ATENÇÃO
> Devido à ausência de suporte por parte da infraestrutura para esta função, o Kleopatra tem que trabalhar diretamente na base de dados de confiança do GpgSM (`trustlist.txt`). Ao usar esta função, certifique-se de que não existem operações criptográficas em curso que possam interferir com o Kleopatra, no que diz respeito a modificações a essa base de dados.

Esta função só está disponível quando estiver selecionado um e só um certificado de raiz do S/MIME, e caso esse certificado ainda não seja de confiança.

Use o **Certificados → Renegar o certificado de raiz** para anular esta função.

Certificados → Renegar o certificado de raiz

Marca este certificado de raiz (S/MIME) como não-fidedigno.

Esta função só está disponível quando estiver selecionado um e só um certificado de raiz do S/MIME, e caso esse certificado esteja marcado como sendo de confiança.

É usado para anular o **Certificados → Confiar no certificado de raiz** . Consulte essa opção para mais detalhes.

Certificados → Certificar o certificado...

Permite-lhe certificar outro certificado de OpenPGP.

Esta função só está disponível quando estiver selecionado um e só um certificado de raiz do OpenPGP.

Certificados → Mudar a data de validade...

Permite modificar a data de expiração do seu certificado de OpenPGP.

Use esta função para aumentar o tempo de vida dos seus certificados de OpenPGP, como alternativa à criação de um novo ou à definição de um tempo de vida ilimitado ('nunca expira').

Esta função só está disponível quando estiver selecionado um e só um certificado de raiz do OpenPGP e se estiver disponível a chave privada do mesmo.

Certificados → Mudar a frase-senha...

Permite modificar a frase-senha da sua chave privada.

Esta função só está disponível se apenas um certificado estiver selecionado e a chave secreta do certificado estiver disponível. Ela precisa de uma infraestrutura muito recente, uma vez que foi modificada a implementação de uma chamada direta ao GPG e ao GpgSM para uma chamada baseada no GpgME.

> NOTA
> Por razões de segurança, tanto a frase-senha antiga como a nova serão pedidas pelo PinEntry, num processo separado. Dependendo da plataforma em que você o está rodando, bem como da qualidade da implementação do PinEntry nessa plataforma, poderá acontecer que a janela do PinEntry apareça em segundo plano. Assim, se você selecionar esta função e não acontecer nada, verifique a barra de tarefas do sistema operacional para ver se existe alguma janela do PinEntry aberta em segundo plano.

Certificados → Adicionar um ID de usuário...

Permite adicionar um novo ID de usuário ao seu certificado de OpenPGP.

Use isto para criar identidades novas a um certificado existente, como alternativa à criação de um novo par de chaves. Um ID de usuário do OpenPGP tem o seguinte formato:

```
Nome Verdadeiro (Comentário) <E-mail>
```

Na janela que aparece quando selecionar esta função, o Kleopatra perguntará cada um dos três parâmetros (*`Nome Verdadeiro`*, *`Comentário`* e *`E-mail`*) em separado, apresentando o resultado numa antevisão.

> NOTA
> Estes parâmetros estão sujeitos às mesmas restrições do Administrador, tal como acontece nos certificados novos. Veja mais detalhes em Seção 2.3 e Seção 6.1.

Esta função só está disponível quando estiver selecionado um e só um certificado de raiz do OpenPGP e se estiver disponível a chave privada do mesmo.

Certificados → Apagar (Delete)

Remove os certificados selecionados do chaveiro local.

Use estas funções para remover as chaves não usadas do seu chaveiro local. Todavia, uma vez que os certificados estão tipicamente anexados às mensagens de e-mail assinadas, a verificação de uma destas mensagens poderá fazer com que uma chave removida retorne para o chaveiro local. Assim, provavelmente é melhor evitar usar esta função o máximo possível. Quando se sentir perdido, use a barra de procura ou a função para voltar a ter o controle sobre o lote de certificados.

> ATENÇÃO
> Existe uma exceção ao caso anterior: Quando apagar um dos seus próprios certificados, você está apagando a chave privada também com ele. Isto implica que não será capaz de ler as comunicações anteriores criptografas para você com este certificado, a menos que tenha uma cópia de segurança em algum lugar.
> O Kleopatra irá avisá-lo quando você tentar apagar uma chave privada.

Devido à natureza hierárquica dos certificados S/MIME, se apagar um certificado emissor de S/MIME (certificado da CA), todos os sujeitos são também removidos.[1]

Naturalmente, esta função só está disponível se tiver selecionado pelo menos um certificado.

Certificados → Apresentar os Dados do Certificado

Mostra todas as informações que o GpgSM possui sobre o certificado selecionado (S/MIME).

Veja a discussão sobre o `--dump-key chave`, no manual do GpgSM, para saber mais detalhes sobre o resultado.

3.4 O menu Ferramentas

Ferramentas → Visualizador do Registro do GnuPG...

Inicia o KWatchGnuPG, uma ferramenta para apresentar o resultado de depuração do aplicativo GnuPG. Se a assinatura, criptografia ou a verificação deixarem de funcionar misteriosamente, você poderá descobrir o porquê, olhando para o registro.

Esta função não está disponível no Windows®, uma vez que os mecanismos subjacentes não estão implementados na infraestrutura dessa plataforma.

Ferramentas → Atualizar os certificados OpenPGP

Atualiza todos os certificados de OpenPGP, executando o comando

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

Depois do comando terminar com sucesso, o seu chaveiro local irá refletir as últimas alterações no que diz respeito à validade dos certificados do OpenPGP.

Veja a nota **Ferramentas → Atualizar os Certificados X.509** para mais detalhes.

Ferramentas → Atualizar os Certificados X.509

Atualiza todos os certificados de S/MIME, executando o comando

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

[1] Isto é igual a um sistema de arquivos: Quando você apaga uma pasta, irá apagar todos os arquivos e pastas nela contidos também.

Depois do comando terminar com sucesso, o seu chaveiro local irá refletir as últimas alterações no que diz respeito à validade dos certificados do S/MIME.

> NOTA
> A atualização dos certificados X.509 ou OpenPGP implica na obtenção de todos os certificados e CRLs, de modo a verificar se eles foram revogados.
> Isto poderá ser inconveniente para você, assim como para as conexões de rede das outras pessoas, podendo levar até uma hora ou mais ainda para terminar, dependendo da sua conexão de rede e do número de certificados a verificar.

Ferramentas → Importar uma CRL de um arquivo...

Permite-lhe importar manualmente as CRL's a partir de arquivos.

Normalmente, as Listas de Revogação de Certificados (ou CRL's) são tratadas de forma transparente pela infraestrutura, mas poderá às vezes ser útil importar manualmente uma CRL para a 'cache' local de CRL's.

> NOTA
> Para a importação de CRL's funcionar, a ferramenta DirMngr deverá estar na `PATH` de pesquisa. Caso este item de menu esteja desativado, você deverá contactar o administrador de sistemas e pedir-lhe para instalar o DirMngr.

Ferramentas → Limpar a 'Cache' de CRLs

Esvazia o cache de CRLs do GpgSM.

Provavelmente você nunca precisará usar isso. Você poderá ordenar uma atualização do cache de CRLs se selecionar todos os certificados e usar o **Ferramentas → Atualizar os Certificados X.509** em alternativa.

Ferramentas → Apresentar a 'Cache' de CRLs

Mostra o conteúdo detalhado do cache de CRLs do GpgSM.

3.5 O menu Configurações

O Kleopatra tem um menu de **Configurações** padrão do KDE, tal como se encontra descrito nos Fundamentos do KDE, com um item adicional:

Configurações → Efetuar os testes automáticos

Efetua um conjunto de testes automáticos, apresentando depois os seus resultados.

Este é o mesmo conjunto de testes que é executado na inicialização, por padrão. Caso tenha desativado os testes automáticos na inicialização, você poderá reativá-los aqui.

3.6 O menu Janela

O menu **Janela** permite-lhe gerenciar as páginas. Usando os itens deste menu, você poderá mudar o nome de uma página, adicionar uma nova, duplicar a atual, fechar a página atual e deslocar a página atual para a esquerda ou direita.

Clique com o botão direito do mouse, numa página para abrir um menu de contexto, onde poderá também selecionar as mesmas ações.

3.7 O menu Ajuda

O Kleopatra tem um menu de **Ajuda** padrão do KDE, tal como se encontra descrito nos Fundamentos do KDE.

Capítulo 4

Referência das Opções de Linha de Comando

Só são listadas aqui as opções específicas do Kleopatra. Como em todos os aplicativos do KDE, você poderá obter uma lista completa das opções usando o comando **`kleopatra --help`**.

`--uiserver-socket` ***argumento***
: Localização do socket do servidor de UI está aguardando em

`--daemon`
: Executar apenas o servidor de UI, ocultar a janela principal

`-p --openpgp`
: Usar OpenPGP para a seguinte operação

`-c --cms`
: Usar o CMS (X.509, S/MIME) para a operação a seguir

`-i --import-certificate`
: Indica um arquivo ou URL a partir do qual importar os certificados (ou chaves privadas). Esta é a linha de comando equivalente a **Arquivo → Importar os Certificados... (Ctrl+I)** .

`-e --encrypt`
: Criptografar arquivo(s)

`-s --sign`
: Assinar arquivo(s)

`-E --encrypt-sign`
: Criptografa e/ou assina o(s) arquivo(s). É igual ao `--sign-encrypt`, não usar

`-d --decrypt`
: Descriptografar arquivo(s)

`-V --verify`
: Verificar o arquivo/assinatura

`-D --decrypt-verify`
: Descriptografar e/ou verificar arquivo(s)

Capítulo 5

Configurando o Kleopatra

A caixa de diálogo de configuração do Kleopatra poderá ser acessada em **Configurações** → **Configurar o Kleopatra...**

Cada uma das suas páginas está descrita nas seções abaixo.

5.1 Configurar os Serviços de Diretório

Nesta página, você poderá configurar os servidores LDAP a usar para as pesquisas por certificados de S/MIME, assim como os servidores de chaves a usar para as pesquisas por certificados do OpenPGP.

> NOTA
> Esta é apenas uma versão mais amigável da configuração que também irá encontrar em Seção 5.5. Tudo o que puder configurar aqui, também poderá configurar no outro local.

> UMA NOTA SOBRE OS SERVIDORES 'PROXY'
> As opções do 'proxy' podem ser configuradas para o HTTP e o LDAP no Seção 5.4, mas apenas no caso do GpgSM. Para o GPG, devido à complexidade das opções do servidor de chaves no GPG e à falta de suporte adequado para elas no GpgConf, você terá que modificar o arquivo de configuração `gpg.conf` diretamente. Veja por favor o manual do GPG para saber mais detalhes. O Kleopatra irá preservar essas opções, apesar de não permitir modificá-las ainda na GUI.

A tabela dos **Serviços de diretório** mostra os servidores que estão configurados atualmente. Faça duplo-clique sobre uma célula da tabela para modificar os parâmetros dos servidores existentes.

O significado das colunas da tabela é o seguinte:

Esquema

Define o protocolo de rede usado para acessar o servidor. Os esquemas mais usados incluem o **ldap** (e o seu semelhante em SSL, o **ldaps**) para os servidores LDAP (um protocolo comum para o S/MIME; o único que é suportado pelo GpgSM), e o **hkp** (Horowitz Keyserver Protocol), que é conhecido hoje em dia como Protocolo dos Servidores de Chaves em HTTP, um protocolo baseado em HTTP que praticamente todos os servidores públicos de chaves de OpenPGP suportam.

Por favor consulte os manuais do GpgSM e do GPG para obter a lista de formatos suportados.

Nome do Servidor
O nome do domínio do servidor, por exemplo `keys.gnupg.net`.

Porta do servidor
A porta de rede em que o servidor está esperando pedidos.

Isto muda automaticamente para a porta padrão, assim que mudar o **Esquema**, a menos que tenha sido definido com alguma porta fora do normal e que não consiga restaurá-la. Tente definir o **Esquema** como sendo **`http`** e o **Porta do servidor** como **`80`** (o valor padrão para o HTTP), seguindo depois a partir daí.

DN de base
O DN de Base (apenas para o LDAP e o LDAPS), isto é o topo da hierarquia de LDAP onde iniciar a pesquisa. Isto também é normalmente chamado de 'raiz da pesquisa' ou 'base da pesquisa'.

Normalmente parece-se com algo do tipo **`c=de,o=Xpto`**, e é indicado como parte do URL de LDAP.

Nome do usuário
O nome do usuário, se existir, a usar para se autenticar no servidor.

Esta coluna só aparece caso a opção **Mostrar a informação do usuário e senha** (abaixo da tabela) esteja assinalada.

Senha
A senha, se existir, a usar para se autenticar no servidor.

Esta coluna só aparece caso a opção **Mostrar a informação do usuário e senha** (abaixo da tabela) esteja assinalada.

X.509
Assinale esta coluna se este item deve ser usado para as pesquisas por certificados X.509 (S/MIME).

Só são suportados os servidores LDAP (e LDAPS) para o S/MIME.

OpenPGP
Assinale esta coluna se acha que este item deverá ser usado para as pesquisas de certificados do OpenPGP.

Você poderá configurar tantos servidores de S/MIME (X.509) quantos desejar, mas só é permitido um servidor de OpenPGP de cada vez. A GUI encarrega-se de limitar isso.

Para adicionar um novo servidor, clique no botão **Novo**. Isto duplica o item selecionado, se existir, ou então introduz um servidor padrão de OpenPGP. Depois poderá definir o **Nome do Servidor**, o **Porta do servidor**, o **DN de base**, o **Senha** e o **Nome do usuário**, sendo os dois últimos necessários apenas se o servidor necessitar de autenticação.

Para inserir diretamente um item para os certificados X.509, use a opção **Novo** → **X.509**; use o **Novo** → **OpenPGP** para o caso do OpenPGP.

Para remover um servidor da lista de procura, selecione-o na lista e pressione depois no botão **Remover**.

Para definir o tempo-limite do LDAP, isto é o tempo máximo que a infraestrutura irá esperar pela resposta de um servidor, basta usar o campo de texto correspondente denominado **tempo-limite do LDAP (minutos:segundos)**.

Se um dos servidores tiver uma base de dados grande, de modo que as pesquisas razoáveis do tipo **`Sousa`** atinjam o **número máximo de itens devolvidos pela pesquisa**, você poderá desejar aumentar este limite. Você poderá detectar isso facilmente, uma vez que ao atingir esse limite durante uma pesquisa, irá aparecer uma caixa de diálogo avisando-o que os resultados foram truncados.

NOTA
Alguns servidores poderão impor os seus próprios limites no número de itens devolvidos por uma pesquisa. Neste caso, o aumento do limite aqui não irá resultar em mais itens devolvidos.

5.2 Configurar a Aparência

5.2.1 Configurar as Dicas

Na lista principal de certificados, o Kleopatra pode mostrar os detalhes de um determinado certificado numa dica. A informação apresentada é a mesma que aparece na área de **Vista Geral** da janela de **Detalhes do Certificado**. As dicas, contudo, poderão ser restringidas para mostrar apenas um subconjunto da informação para uma experiência menos descritiva.

NOTA
O **ID da Chave** é *sempre* apresentado. Isto serve para garantir que as dicas dos diferentes certificados são, de fato, distintas entre si (isto é especialmente importante se só tiver selecionado a **Mostrar a validade**).

Você poderá ativar ou desativar, de forma independente, os seguintes conjuntos de informações:

Mostrar a validade

Mostra informações sobre a validade de um determinado certificado: o seu estado atual, o DN do emissor (apenas para o S/MIME), as datas de validade (se existirem) e as opções de utilização do certificado.

Exemplo:

```
Este certificado é válido neste momento.
Emissor:            CN=ZS-Teste 7,O=Intevation GmbH,C=DE
Validade:          de 25/08/2009 10:42 até 19/10/2010 10:42
Utilização do certificado: Assinar E-Mails e Arquivos, Criptografar E- ↩
    Mails e Arquivos
ID-Chave:            DC9D9E43
```

Mostrar a informação do dono

Mostra informações sobre o dono do certificado: o DN do sujeito (apenas para o S/MIME), os IDs dos usuários (incluindo os endereços de e-mail) e a confiança no dono (apenas para o OpenPGP).

Exemplo do OpenPGP:

```
ID-Usuário:           UsuárioGpg4win <usuário_gpg4win@teste.qg>
ID-Chave:            C6BF6664
Confiança no dono:        absoluta
```

. Exemplo do S/MIME:

```
Sujeito:           CN=UsuárioGpg4win,OU=Lab_Testes,O=Projeto Gpg4win,C= ↩
    DE
a.k.a.:            usuário_gpg4win@teste.qg
ID-Chave:            DC9D9E43
```

Mostrar os detalhes técnicos

Mostra informações técnicas sobre o certificado: o número de série (apenas para o S/-MIME), o tipo, a impressão digital e a localização do armazenamento.

Exemplo:

```
Número de Série:     27
Tipo de certificado:  RSA de 1,024-bits (certificado privado disponível ↩
    )
ID-Chave:            DC9D9E43
Impressão digital:       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Armazenado:            neste computador
```

5.2.2 Configurar as Categorias de certificados

O Kleopatra permite-lhe personalizar a aparência dos certificados na lista. Isto inclui a apresentação de um pequeno ícone, mas também poderá definir as cores do texto e do fundo, assim como a fonte a ser usada.

A cada categoria de certificados na lista é atribuído um conjunto de cores um ícone (opcional) e uma fonte, com o qual os certificados desta categoria são apresentados. A lista de categorias também atua como uma antevisão das configurações. As categorias podem ser definidas livremente pelo administrador ou por um usuário com privilégios. Veja o Seção 6.2 em capítulo 6.

Para definir ou alterar o ícone de uma categoria, selecione-a na lista e clique no botão **Alterar o ícone...**. A janela de seleção de ícones normal do KDE irá aparecer, e nela você poderá escolher um ícones existente da coleção do KDE ou carregar um ícone personalizado.

Para remover um ícone de novo, você precisa carregar no botão **Aparência padrão**.

Para alterar a cor do texto (isto é a cor principal) de uma categoria, selecione-a na lista e clique no botão **Alterar a cor do texto...**. A janela de seleção de cores normal do KDE irá aparecer, e nela você poderá escolher ou criar uma cor nova.

A alteração da cor de fundo é feita da mesma forma, clicando no entanto no botão **Configurar Cor de Fundo...**.

Para alterar a fonte, o usuário tem duas opções:

1. Modificar a fonte padrão, usada por todas as listas no KDE.
2. Usar uma fonte personalizada.

A primeira opção tem a vantagem que a fonte irá seguir o estilo que você definiu a nível do KDE, enquanto que a última lhe fornece um controle completo sobre a fonte a ser usada. A escolha é sua.

Para usar a fonte padrão modificada, selecione a categoria na lista e ligue ou desligue os modificadores de fonte **Itálico**, **Negrito**, e/ou **Tachado**. Você poderá ver imediatamente o efeito da fonte na lista de categorias.

Para usar uma fonte personalizada, clique no botão **Alterar a fonte...**. A janela normal de seleção de fonte do KDE irá aparecer e nela você poderá selecionar o novo tipo de fonte.

> NOTA
> Você ainda poderá usar os modificadores de fonte para mudar o tipo de fonte personalizado, como faria para modificar o tipo de fonte normal.

Para voltar à fonte padrão, você precisa de clicar no botão **Aparência Padrão**.

5.2.3 Configurar a Ordem dos Atributos do DN

Ainda que os DNs sejam hierárquicos, a ordem dos componentes individuais (chamados de DNs relativos (RDNs) ou atributos do DN) não está definida. A ordem pela qual aparecem os atributos é, por isso, uma questão de gosto pessoal ou da empresa, razão pela qual é configurável no Kleopatra.

> NOTA
> Esta opção não só se aplica ao Kleopatra, mas a todos os aplicativos que usam a Tecnologia do Kleopatra. No momento em que este documento foi escrito, estas incluem o KMail, o KAddressBook, assim como o próprio Kleopatra, obviamente.

Esta página de configuração consiste basicamente em duas listas, uma para os atributos conhecidos (**Atributos disponíveis**) e outra que descreve a **Ordem atual dos atributos**.

Ambas as listas contém itens descritos pela forma resumida do atributo (por exemplo **CN**), assim como a forma por extenso (**Common Name - Nome Comum**).

A lista de **Atributos disponíveis** está sempre ordenada alfabeticamente, enquanto que a sequência da lista **Ordem atual dos atributos** reflete a ordem configurada de atributos do DN: o primeiro atributo da lista é também o atributo mostrado em primeiro lugar.

Só os atributos listados explicitamente na lista **Ordem atual dos atributos** são mostrados. O resto fica oculto por padrão.

Contudo, se o item de substituição **_X_** (**Todos os outros**) estiver na lista 'atual', todos os atributos não listados (sejam conhecidos ou não), são inseridos no local do **_X_**, na sua ordem relativa original.

Um pequeno exemplo ajudará a esclarecer isto:

Fornecido o DN

> O=KDE, C=BR, CN=David Programador, X-BAR=foo, OU=Kleopatra, X-FOO=bar,

a ordem de atributos padrão do 'CN, L, _X_, OU, O, C' irá gerar o seguinte DN formatado:

> CN=David Programador, X-XPTO2=xpto, X-XPTO=xpto2, OU=Kleopatra, O=KDE, C=BR

enquanto o 'CN, L, OU, O, C' irá produzir

> CN=David Programador, OU=Kleopatra, O=KDE, C=BR

Para adicionar um atributo à lista de ordem de exibição, selecione-o na lista de **Atributos disponíveis** e clique no botão **Adicionar à ordem atual dos atributos**.

Para remover um atributo da lista de ordem de exibição, selecione-o na lista de **Ordem atual dos atributos** e clique no botão **Remover da ordem atual dos atributos**.

Para mover um atributo para o início (fim), selecione-o na lista **Ordem atual dos atributos** e clique no botão **Mover para topo** (**Mover para base**).

Para mover um atributo apenas uma posição para cima (baixo), selecione-o na lista **Ordem atual dos atributos** e clique no botão **Mover acima** (**Mover abaixo**).

5.3 Configurar as Operações Criptográficas

5.3.1 Configurar as Operações de E-Mail

Aqui você poderá configurar alguns aspectos das operações de e-mail do UiServer do Kleopatra. Atualmente, você só pode configurar se deve usar o 'Modo rápido' para assinar e criptografar os e-mails, individualmente.

Quando o 'Modo Rápido' estiver ativo, não será apresentada nenhuma janela ao assinar (encriptar) as mensagens de e-mail, respectivamente, a menos que exista um conflito que necessite de uma resolução manual.

5.3.2 Configurar as Operações com arquivos

Aqui você poderá configurar alguns aspectos das operações com arquivos do UiServer do Kleopatra. Atualmente, você só pode escolher o programa de validação de integridade a usar para o **CHECKSUM_CREATE_FILES**.

Use o **Programa de códigos de validação a usar** para escolher qual dos programas de geração de códigos de validação instalados será usado para criar os arquivos de códigos de validação.

Ao verificar os códigos de validação, o programa a usar será encontrado automaticamente, com base nos nomes dos arquivos de códigos de validação encontrados.

> NOTA
> O administrador e o superusuário poderão definir por completo quais os programas de validação disponibilizar ao Kleopatra, através das 'Definições de Códigos de Validação' do arquivo de configuração. Veja mais detalhes em Seção 6.4 na seção capítulo 6.

5.4 Configurar os aspectos da Validação S/MIME

Nesta página, você poderá configurar alguns aspectos da validação dos certificados de S/-MIME.

> NOTA
> Para a maior parte dos casos, isto é apenas uma versão mais amigável das mesmas opções que iria encontrar no Seção 5.5. Tudo o que configurar aqui, poderá configurar no outro local também, com a exceção do **Verifica a validade dos certificados a cada *N* horas**, que é específico do Kleopatra.

O significado das opções é o seguinte:

5.4.1 Configurar a verificação de certificados periódica

Verifica a validade dos certificados a cada *N* horas

Esta opção ativa a verificação periódica da validade dos certificados. Você poderá também escolher o intervalo da verificação (em horas). O efeito da verificação periódica é o mesmo que o **Ver** → **Reexibir (F5)** ; não existe nenhuma possibilidade de agendar periodicamente o **Ferramentas** → **Atualizar os certificados OpenPGP** ou o **Ferramentas** → **Atualizar os Certificados X.509** .

> **NOTA**
> A validação é efetuada implicitamente sempre que os arquivos significativos em `~/.gnupg` forem alterados. Esta opção, tal como a **Ferramentas → Atualizar os certificados OpenPGP** e a **Ferramentas → Atualizar os Certificados X.509** , só afeta os fatores externos da validade do certificado.

5.4.2 Configurar o método de validação

Validar certificados usando CRLs

Se esta opção estiver selecionada, os certificados de S/MIME são validados de acordo com as Listas de Revogação de Certificados (CRL's).

Veja o **Validar certificados online (OCSP)** para conhecer um método alternativo de verificação da validade dos certificados.

Validar certificados online (OCSP)

Se esta opção estiver selecionada, os certificados de S/MIME são validados 'online', usando o Protocolo 'Online' de Estado dos Certificados (OCSP).

> **ATENÇÃO**
> Ao escolher este método, é enviado um pedido ao servidor da CA, mais ou menos a cada vez que envia ou recebe uma mensagem criptografada, o que permite em teoria à agência de emissão de certificados fazer um rastreamento das pessoas com quem trocou mensagens (por exemplo).

Para usar este método, você deve indicar o URL do servidor de respostas de OCSP no **URL de resposta do OCSP**.

Veja o **Validar certificados online (OCSP)** para obter um método mais tradicional de verificação da validação dos certificados, que não passa qualquer informação sobre as pessoas com quem trocou mensagens.

URL de resposta do OCSP

Insira aqui o endereço do servidor de validação 'online' dos certificados (servidor de respostas do OCSP). O URL normalmente começa por `http://` .

Assinatura de resposta do OCSP

Escolha aqui o certificado com o qual o servidor de OCSP assina as suas respostas.

Ignorar URL do serviço de certificados

Cada certificado de S/MIME normalmente contém o URL do servidor de OCSP do seu emissor (o **Certificados → Apresentar os Dados do Certificado** irá revelar se um determinado certificado o contém).

Se assinalar esta opção, fará com que o GpgSM ignore esses URL's e só use o que estiver configurado acima.

Use isto por exemplo para forçar a utilização de um 'proxy' de OCSP empresarial.

5.4.3 Configurar as opções de validação

Não verificar as políticas de certificados

Por padrão, o GpgSM usa o arquivo `~/.gnupg/policies.txt` para verificar se uma determinada política de certificados é permitida ou não. Se esta opção estiver selecionada, as políticas não são verificadas.

Nunca consultar uma CRL

Se esta opção estiver assinalada, as Listas de Revogação de Certificados nunca são usadas para validar os certificados de S/MIME.

Permitir marcar os certificados raiz como confiáveis

Se esta opção estiver assinalada quando você estiver importando um certificado da CA de raiz, será pedida a confirmação da sua impressão digital e se considera este certificado de raiz como sendo fidedigno ou não.

Um certificado de raiz tem que ser considerado fidedigno, antes de confirmar a confiança nos certificados que ele certificou; se fizer apenas uma avaliação ligeira dos certificados de raiz, poderá minar a segurança do sistema.

> NOTA
> Se ativar esta funcionalidade na infraestrutura, poderá obter janelas indesejadas do PinEntry (por exemplo ao verificar as assinaturas), podendo assim bloquear o processamento de correio não-verificado. Por essa razão, e uma vez que se pretende ser possível *renegar* um certificado de raiz fidedigno, o Kleopatra permite a definição manual da confiança, usando o **Certificados → Confiar no certificado de raiz** e o **Certificados → Renegar o certificado de raiz** .
> Esta opção aqui não influencia o funcionamento do Kleopatra.

Obter certificados faltantes do emissor

Se esta opção estiver assinalada, os certificados do emissor em falta serão obtidos quando for necessário (isto aplica-se a ambos os métodos de validação, as CRL's e o OCSP).

5.4.4 Configurar as opções dos pedidos de HTTP

Não efetuar pedidos HTTP

Desativa por completo a utilização do HTTP para o S/MIME.

Ignorar o ponto de distribuição de CRL HTTP dos certificados

Ao procurar pela localização de uma CRL, o certificado a testar contém normalmente alguns elementos chamados de 'Pontos de Distribuição da CRL' (DP), que são URL's que descrevem a forma de acessar à CRL. É usado o primeiro item DP que for encontrado.

Com esta opção, todos os itens que usem o esquema de HTTP serão ignorados ao procurar por um DP adequado.

Usar o proxy HTTP do sistema

Se esta opção estiver selecionada, aparecerá o valor do 'proxy' de HTTP do lado direito (que vem da variável de ambiente `http_proxy`) que será usado para qualquer pedido de HTTP.

Usar este proxy para pedidos HTTP

Se não estiver definido nenhum 'proxy' do sistema, ou caso precise usar um 'proxy' diferente para o GpgSM, poderá indicar aqui a sua localização.

Será usada para todos os pedidos de HTTP que digam respeito ao S/MIME.

A sintaxe é **`máquina:porta`**, por exemplo **`meuproxy.nenhumlugar.com:3128`**.

5.4.5 Configurar as opções dos pedidos de LDAP

Não efetuar requisições LDAP

Desativa por completo a utilização do LDAP para o S/MIME.

Ignorar o ponto de distribuição de CRL LDAP dos certificados

Ao procurar pela localização de uma CRL, o certificado a testar contém normalmente alguns elementos chamados de ˝Pontos de Distribuição da CRL˝ (DP), que são URL's que descrevem a forma de acessar à CRL. É usado o primeiro item DP que for encontrado.

Com esta opção, todos os itens que usam o esquema LDAP são ignorados ao procurar por um DP adequado.

Servidor primário para requisições LDAP

Indicar aqui um servidor LDAP, fará com que todos os pedidos de LDAP vão primeiro a este servidor. Para ser mais exato, esta opção substitui todas as definições de *máquina* e *porta* de um URL de LDAP, sendo também usadas caso a *máquina* e a *porta* tenham sido omitidas do URL.

Os outros servidores LDAP só serão usados se a conexão ao 'proxy' for mal-sucedida. A sintaxe é **máquina** ou **máquina:porta**. Se a *porta* for omitida, será usada a porta 389 (padrão do LDAP).

5.5 Configurar o sistema GnuPG

Esta parte da janela é gerada automaticamente a partir do resultado do comando **gpgconf --list-components** e, para cada um dos *componentes* que o comando acima devolver, é apresentado o resultado do comando **gpgconf --list-options** ***componente***.

> NOTA
> A mais útil destas opções foi duplicada como páginas separadas na janela de configuração do Kleopatra. Veja em Seção 5.1 e Seção 5.4 as duas janelas em questão, que contêm as opções selecionadas nesta parte da janela.

O conteúdo exato desta parte da janela depende da versão da infraestrutura do GnuPG que tiver instalada e, potencialmente, a plataforma em que está rodando. Deste modo, só iremos discutir a disposição geral da janela, incluindo a associação das opções do GpgConf aos controles da GUI do Kleopatra.

O GpgConf devolve a informação de configuração dos vários componentes. Dentro de cada um dos componentes, as opções individuais estão organizadas em grupos.

O Kleopatra mostra uma página por cada componente indicado pelo GpgConf; os grupos são antecedidos por uma linha horizontal que mostra o nome do grupo, tal como foi devolvido pelo GpgConf.

Cada opção do GpgConf tem um tipo associado. Excetuando as opções mais conhecidas que o Kleopatra já trata com controles especializados, para uma melhor experiência do usuário, a associação entre os tipos do GpgConf e os controles do Kleopatra é a seguinte:

Tipo GpgConf	**Controle do Kleopatra**	
	para listas	**para exceções às listas**
`nenhum`	Campo incremental (semântica de 'quantidade')	Opção

texto	N/A	Campo de texto
int32	Campo de texto (não formatado)	Campo incremental
uint32		
localização	N/A	controle especializado
servidor LDAP	controle especializado	N/A
impressão digital de chave	N/A	
chave pública		
chave privada		
lista de nomes alternativos		

Tabela 5.1: Associação Entre os Tipos do GpgConf e os Controles GUI

Veja o manual do GpgConf para obter mais informações sobre o que poderá configurar aqui, bem como a forma de o fazer.

Capítulo 6

Guia do Administrador

Este Guia do Administrador descreve as formas de personalizar o Kleopatra que não estão disponíveis através da GUI, mas apenas através de arquivos de configuração.

Assume-se que o leitor está familiarizado com a tecnologia usada para a configuração dos aplicativos do KDE, incluindo o formato, a localização no sistema de arquivos e o encadeamento dos arquivos de configuração do KDE, assim como a plataforma KIOSK.

6.1 Personalização do Assistente de Criação de Certificados

6.1.1 Personalizar os campos DN

O Kleopatra permite-lhe personalizar os campos que o usuário tem permissão para introduzir, de forma a criar o seu certificado.

Crie um grupo chamado `CertificateCreationWizard` no `kleopatrarc` do sistema. Se você quiser uma ordem personalizada dos atributos ou se desejar que apareçam apenas alguns itens, crie uma chave chamada `DNAttributeOrder`. O argumento é um ou mais itens da lista `CN`,`SN`,`GN`,`L`,`T`,`OU`,`O`,`PC`,`C`,`SP`,`DC`,`BC`,`EMAIL` Se quiser inicializar os campos com um determinado valor, escreva algo do tipo Atributo=valor. Se quiser que o atributo seja tratado como obrigatório, adicione um ponto de exclamação (por exemplo `CN!`,`L`,`OU`,`O!`,`C!`,`EMAIL!` que é, de fato, a configuração padrão).

Usando o modificador de modo do KIOSK `$e`, você poderá obter os valores das variáveis de ambiente, ou então a partir de um programa ou script avaliado. Se quiser proibir a edição do respectivo campo, além disso, use o modificador `$i`. Se quiser proibir o uso do botão **Inserir Meu Endereço**, configure o `ShowSetWhoAmI` como false.

> DICA
> Devido à natureza da plataforma KIOSK do KDE, usando a opção de inalterável (`$i`), irá impossibilitar ao usuário a sobreposição da opção. Este é o comportamento pretendido. O `$i` e o `$e` podem ser usados com todas as chaves de configuração dos aplicativos do KDE, da mesma forma.

O seguinte exemplo representa as personalizações possíveis:

```
[CertificateCreationWizard]
;Proibir a cópia de dados pessoais do livro de endereços, não permitir ↩
    sobreposições locais
ShowSetWhoAmI[$i]=false

;configurar o nome do usuário igual a $USER
```

```
CN[$e]=$USER

;configura o nome da empresa como sendo "A Minha Empresa", proibindo as ↩
    alterações
O[$i]=A Minha Empresa

;configura o nome do departamento como sendo um valor devolvido por um ↩
    programa
OU[$ei]=$(devolver_depart_pelo_ip)

; configura o país como BR, mas permitindo alterações pelo usuário
C=BR
```

6.1.2 Restringir os tipos de chaves que um usuário poderá criar

O Kleopatra também lhe permite restringir o tipo de certificados que um determinado usuário poderá criar. Lembre-se, contudo, que uma forma simples de contornar estas restrições é criar um certificado pela linha de comando.

6.1.2.1 Algoritmos de chave pública

Para restringir o algoritmo de chave pública a usar, adicione a variável de configuração `PGPKeyType` (e `CMSKeyType`, mas só é suportado o RSA para o CMS, de qualquer forma), na seção `CertificateCreationWizard` do arquivo `kleopatrarc`.

Os valores permitidos são `RSA` para as chaves RSA, `DAS` para as chaves DSA (apenas de assinatura), e `DSA+ELG` para uma chave DSA (apenas de assinatura) com uma subchave ElGamal para a criptografia.

O valor padrão é lido do GpgConf ou então é igual a `RSA`, caso o GpgConf não devolva qualquer valor.

6.1.2.2 Tamanho da chave pública

Para restringir os tamanhos de chaves para um algoritmo público, adicione a variável de configuração `<ALG>KeySizes` (onde o *ALG* poderá ser `RSA`, `DSA` ou `ELG`) na seção `CertificateCreationWizard` do arquivo `kleopatrarc`, contendo uma lista de tamanhos de chaves separadas por vírgulas (em 'bits'). Poderá ser indicado um valor padrão se anteceder o tamanho da chave com um hífen (-).

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

O valor acima iria restringir os tamanhos permitidos para as chaves RSA a 1536, 2048 e 3072, sendo o 2048 o valor padrão.

Além dos tamanhos propriamente ditos, você poderá indicar algumas legendas para cada um dos tamanhos. Basta definir a variável `ALGKeySizeLabels` como uma lista de legendas separadas por vírgulas.

```
RSAKeySizeLabels = fraca,normal,forte
```

O valor acima, em conjunto com o exemplo anterior, iria imprimir algo do gênero na seleção:

```
fraca (1536 bits)
              normal (2048 bits)
              forte (3072 bits)
```

Os valores padrão serão os seguintes:

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

6.2 Criando e Editando Categorias de Chaves

O Kleopatra permite ao usuário configurar a aparência visual das chaves com base num conceito chamado de **Categorias das Chaves**. Estas também podem ser usadas para filtrar a lista de certificados. Esta seção descreve como você poderá editar as categorias disponíveis, bem como adicionar novas.

Ao tentar procurar a categoria a que uma chave pertence, o Kleopatra tenta corresponder a chave a uma sequência de filtros de chaves, configurada no `libkleopatrarc`. A primeira a corresponder define a categoria, baseada num conceito de *especificidade*, explicado mais abaixo.

Cada filtro de chaves está definido num grupo de configuração chamado `Key Filter #n`, em que o *n* é um número que começa em `0`.

A única chave obrigatória num grupo `Key Filter #n` é o `Name`, que contém o nome da categoria, tal como aparece na janela de configuração e `id`, que é usado como referência para o filtro nas outras seções de configuração (como o `View #n`).

Tabela 6.1 lista todas as chaves que definem as propriedades de visualização das chaves que pertencem a essa categorias (isto é aquelas chaves que poderão ser ajustadas no janela de configuração), em que o Tabela 6.2 lista todas as chaves que definem o critério com o qual o filtro faz a correspondência das chaves.

Chave de Configuração	Tipo	Descrição
`background-color`	cor	A cor de fundo a ser usada. Se não estiver definida, usa a cor de fundo definida a nível global para as listas.
`foreground-color`	cor	A cor do texto a ser usada. Se não estiver definida, usa a cor do texto definida a nível global para as listas.
`font`	fonte	A fonte a ser usada. A fonte será ajustada para o tamanho configurado para as listas e todos os atributos de fonte (ver abaixo) serão aplicados.
`font-bold`	booleano	Se for igual a `true` e o `font` não estiver definido, usa a fonte padrão das listas com um estilo negrito adicionado (se estiver disponível). É ignorado se o `font` estiver também disponível.

font-italic	booleano	É igual ao font-bold, só que para uma fonte itálica em vez de negrito.
font-strikeout	booleano	Se for igual a true, desenha uma linha centrada por cima da fonte. É aplicado, mesmo que o font esteja definido.
icon	texto	O nome do ícone a ser mostrado para a primeira coluna. Ainda não está implementado.

Tabela 6.1: Chaves de Configuração do Filtro de Chaves que Definem Propriedades de Visualização

Chave de Configuração	**Tipo**	**Se forem especificadas, o filtro faz correspondência quando...**
is-revoked	booleano	a chave foi revogada.
match-context	contexto[1]	o contexto a que este filtro corresponde.
is-expired	booleano	a chave expirou.
is-disabled	booleano	a chave foi desativada (marcada para não ser usada) pelo usuário. É ignorada no caso das chaves S/MIME.
is-root-certificate	booleano	a chave é um certificado de raiz. Ignorado nas chaves OpenPGP.
can-encrypt	booleano	a chave pode ser utilizada para criptografia.
can-sign	booleano	a chave pode ser utilizada para assinar.
can-certify	booleano	a chave por ser utilizada para assinar (certificar) outras chaves.
can-authenticate	booleano	a chave pode ser utilizada para autenticação (por exemplo como um certificado de cliente TLS).
is-qualified	booleano	a chave pode ser usada para criar Assinaturas Qualificadas (como definidas pela Lei de Assinatura Digital da Alemanha).

[1] O contexto é uma enumeração com os valores permitidos: appearance, filtering e any.

`is-cardkey`	booleano	o material da chave é armazenado em um smartcard (ao invés do computador).
`has-secret-key`	booleano	a chave secreta deste par da chaves está disponível.
`is-openpgp-key`	booleano	a chave é uma chave OpenPGP (`true`), ou uma chave S/MIME (`false`).
`was-validated`	booleano	a chave foi validada.
`prefixo-ownertrust`	validade[2]	a chave tem exatamente (*`prefixo`* = `is`), tem tudo exceto (*`prefixo`* = `is-not`), tem pelo menos (*`prefixo`* = `is-at-least`), ou tem no máximo (*`prefixo`* = `is-at-most`) o grau de confiança dado como valor da chave de configuração. Se for indicada mais de uma chave `prefixo-ownertrust` (com vários valores de *`prefixo`*) num único grupo, o comportamento será indefinido.
`prefixo-validity`	validade	É igual ao `prefixo-ownertrust`, mas para a validade da chave em vez do grau de confiança do dono.

Tabela 6.2: Chaves de Configuração do Filtro de Chaves que Definem Critérios de Filtragem

NOTA

Alguns dos critérios mais interessantes, como o `is-revoked` ou o `is-expired` só irão funcionar com as chaves *validadas*, razão pela qual, por padrão, só as chaves validadas são verificadas a nível de revogação e expiração, ainda que você seja livre para remover estas verificações adicionais.

Além das chaves de configuração indicadas acima, um filtro de chaves poderá também ter um `id` e um `match-contexts`.

Se usar o `id` do filtro, o que corresponde ao nome do grupo de configuração do filtro se não for indicado ou for vazio, você poderá referenciar o filtro de chaves mais tarde na configuração, por exemplo na configuração da Janela do Kleopatra. O `id` não é interpretado pelo Kleopatra; como tal, pode usar o texto que desejar, desde que seja único.

O `match-contexts` limita a possibilidade de aplicação do filtro. Estão definidos dois contextos atualmente: o contexto `appearance` é usado ao definir as propriedades de cores e tipos de fonte

[2] A validade é uma enumeração (ordenada) com os seguintes valores permitidos: `unknown` (desconhecido), `undefined` (indefinido), `never` (nunca), `marginal` (relativa), `full` (completa), `ultimate` (máxima). Veja os manuais do GPG e do GpgSM para uma explicação detalhada.

das janelas. O contexto `filtering` é usado para incluir (e excluir) de forma seletiva os certificados das janelas. O `any` pode ser usado para se aplicar a todos os contextos definidos atualmente, sendo a opção padrão se o `match-contexts` não for indicado ou se não produzir contextos de outra forma. Isto garante que nenhum filtro de chaves poderá terminar 'morto', isto é sem quaisquer contextos aplicados.

O formato do item é uma lista de elementos separados por caracteres separadores de palavras. Cada um destes elementos é antecedido opcionalmente de um ponto de exclamação (`!`), o que indica uma negação. Os elementos atuam em ordem sobre uma lista de contextos interna, que começa inicialmente vazia. Isto é melhor explicado com um exemplo: `any !apperance` é o mesmo que `filtering`, assim como `appearance !appearance` produz um conjunto vazio, uma vez que corresponde a `!any`. Contudo, os dois últimos serão substituídos por `any`, uma vez que não produzem quaisquer contextos.

De um modo geral, os critérios não indicados (isto é o item de configuração não está definido) não são validados. Se um critério for indicado, é validado e terá de corresponder para que o filtro como um todo seja validado, isto é os critérios são agrupados com um E lógico.

Cada filtro tem uma 'especificidade' implícita que é usada para classificar todos os filtros correspondentes. Os filtros mais específicos têm precedência sobre os menos específicos. Se dois filtros tiverem a mesma especificidade, o que vier primeiro no arquivo de configuração ganha. A especificidade de um filtro é proporcional ao número de critérios que contém.

Example 6.1 Exemplos de filtros de chaves

Para verificar todos os certificados expirados mas não revogados, você iria usar um filtro de chaves definido da seguinte forma:

```
[Key Filter #n]
Name=expirada mas não revogada
was-validated=true
is-expired=true
is-revoked=false
is-root-certificate=true
; ( specificity 4 )
```

Para verificar todas as chaves OpenPGP desativadas (ainda não suportado pelo Kleopatra) com um grau de confiança pelo menos 'relativa', você iria usar:

```
[Key Filter #n]
Name=chaves de OpenPGP desativadas com confiança relativa ou boa
is-openpgp=true
is-disabled=true
is-at-least-ownertrust=marginal
; ( specificity 3 )
```

6.3 Configurar os Arquivadores a Usar ao Assinar/Criptografar os Arquivos

O Kleopatra permite ao administrador (e aos usuários especializados) configurar a lista de arquivadores que estão presentes na janela para Assinar/Criptografar os Arquivos.

Cada arquivador está definido no `libkleopatrarc` como um grupo `Archive Definition #n` separado, com as seguintes chaves obrigatórias:

`extensions`
: Uma lista, separa por vírgulas, das extensões de arquivos que indicam normalmente este formato de arquivo.

id

Um ID único que é usado para identificar este arquivador internamente. Em caso de dúvida, use o nome do comando.

Name (traduzido)

O nome visível para o usuário do arquivador, tal como aparece na lista correspondente na janela para Assinar/Criptografar os Arquivos.

pack-command

O comando real usado para arquivar os arquivos. Você poderá usar qualquer comando, desde que não seja necessária qualquer linha de comando para executá-lo. O programa é pesquisado com a variável de ambiente `PATH`, a menos que tenha usado uma localização absoluta para o arquivo. Existe o suporte para aspas, caso tenha sido utilizada uma linha de comando:

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

NOTA

Uma vez que a barra invertida (\) é um caractere de escape nos arquivos de configuração do KDE, você terá que duplicá-los quando aparecerem nos nomes dos arquivos:

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

Contudo, para o comando em si (em oposição aos seus argumentos), poderá apenas usar as barras normais (/) como separadores entre pastas para todas as plataformas:

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

Isto não é suportado nos argumentos, porque a maioria dos programas do Windows® usam as barras normais para as opções. Por exemplo, o seguinte não irá funcionar, uma vez que o `C:/programa-arquivo.bat` é um argumento do **cmd.exe**, e o / não será assim convertido para \ nos argumentos, somente nos comandos:

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

Este comando deverá sim ser descrito como:

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

6.3.1 Passagem do Arquivo de Entrada ao `pack-command`

Existem três formas de passar os nomes dos arquivos ao comando de arquivo. Para cada uma delas, o `pack-command` oferece uma sintaxe em particular:

1. Como argumentos da linha de comando.

   Exemplo (tar):

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

   Exemplo (zip):

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

Nesse caso, os nomes dos arquivos são passados na linha de comando, tal como faria ao usar a linha de comando. O Kleopatra não usa nenhuma linha de comando para executar o comando. Assim, esta é uma forma segura de passar os nomes dos arquivos, mas que poderá ter algumas restrições quanto ao tamanho da linha de comando em algumas plataformas. Um `%f` literal, se estiver presente, será substituído pelos nomes dos arquivos a arquivar. Caso contrário, os nomes dos arquivos serão adicionados à linha de comando. Assim, o exemplo para o ZIP, acima descrito, seria escrito de forma equivalente da seguinte forma:

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

2. Através do 'standard-in' (STDIN), separado por mudanças de linha: coloque antes um `|`.
   Exemplo (tar da GNU):

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

   Exemplo (ZIP):

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

   Nesse caso, os nomes dos arquivos são passados ao programa de arquivo pelo stdin, um por cada linha. Isso evita os problemas nas plataformas que colocam um limite baixo no número de argumentos permitido pela linha de comando, mas não resulta quando os nomes dos arquivos contêm de fato mudanças de linha nos seus nomes.

   > NOTA
   > O Kleopatra só suporta no momento o LF como separador de linhas, não suportando o CRLF. Isto poderá mudar nas próximas versões, dependendo das reações do usuário.

3. Através do 'standard-in', separado por 'bytes' NUL: coloque anteriormente `0|`.
   Exemplo (tar da GNU):

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

   Esse é igual ao anterior, com a diferença que são usados bytes NUL (vazios) para separar os nomes dos arquivos. Uma vez que os bytes NUL são proibidos nos nomes dos arquivos, esta é a forma mais robusta de passar nomes de arquivos, só que infelizmente nem todos os programas a suportam.

6.4 Configurar os Programas de Validação a Usar para Criar/Verificar Códigos de Validação

O Kleopatra permite ao administrador (e aos usuários especializados) configurar a lista de programas de geração de códigos de validação de integridade que o usuário poderá escolher, a partir da janela de configuração, desde que o Kleopatra consiga detectar automaticamente, quando for pedido para verificar o código de integridade de um determinado arquivo.

NOTA

Para poder ser usado pelo Kleopatra, o resultado dos programas de validação (tanto o arquivo de códigos salvo, como o resultado para o stdout, na verificação dos códigos de validação) terá que ser compatível com os comandos da GNU **md5sum** e **sha1sum**.
De uma forma específica, o arquivo de códigos de validação será composto por várias linhas, tendo cada uma delas o seguinte formato:

```
CÓDIGO-VALIDAÇÃO ' ' ( ' ' | '*' ) NOME-ARQUIVO
```

em que o *CÓDIGO-VALIDAÇÃO* consiste apenas em caracteres hexadecimais. Se o *NOME-ARQUIVO* tiver um caractere de mudança de linha, a linha deverá ser lida então como:

```
\CÓDIGO-VALIDAÇÃO ' ' ( ' ' | '*' ) NOME-ARQUIVO-ESCAPADO
```

em que o *NOME-ARQUIVO-ESCAPADO* é o nome do arquivo com as mudanças de linha substituídas por `\n`'s e as barras invertidas duplicadas (\↦\\).
Do mesmo modo, o resultado do `verify-command` deverá estar no formato

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

, separado por mudanças de linha. Estas e os outros caracteres *não* são escapados no resultado.[a]

[a] Sim, estes programas não foram feitos com as interfaces gráficas em mente, assim o Kleopatra não conseguirá processar os arquivos patológicos que contenham ˝: OK˝ e uma mudança de linha no seu nome.

Cada programa de validação está definido no `libkleopatrarc` como um grupo `Checksum Definition #n` separado, com as seguintes chaves obrigatórias:

`file-patterns`
: Uma lista de expressões regulares que descrevem quais os arquivos que poderão ser considerados arquivos de validação de integridade para este programa em particular. A sintaxe é a mesma que é usada para as listas de textos nos arquivos de configuração do KDE.

  NOTA

  Uma vez que as expressões regulares normalmente contêm barras invertidas, deve-se ter algum cuidado em escapá-las também no arquivo. Recomenda-se a utilização de uma ferramenta de edição de arquivos de configuração.

  A plataforma define se os padrões são tratados com ou sem distinção entre maiúsculas e minúsculas.

`output-file`
: O nome do arquivo de saída típico para este programa de validação (deverá corresponder a um dos `file-patterns`, obviamente). Isto é o que o Kleopatra irá usar como arquivo de saída, cada vez que criar arquivos de códigos de validação deste tipo.

`id`
: Um ID único que é usado para identificar este programa internamente. Em caso de dúvida, use o nome do comando.

`Name` (traduzido)
: O nome visível para o usuário deste programa de validação de integridade, tal como irá aparecer na lista respectiva da janela de configuração do Kleopatra.

`create-command`
: O comando real com que são criados os arquivos de validação de integridade. A sintaxe, as restrições e as opções de passagem de argumentos são as mesmas que foram descritas para o `pack-command` nas Seção 6.3.

verify-command

É igual ao create-command, mas usado na verificação dos códigos de validação de integridade.

Aqui está um exemplo completo:

```
[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
```

Capítulo 7

Créditos e licença

CONTRIBUIDORES

- 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

Tradução de Marcus Gama marcus.gama@gmail.com e André Marcelo Alvarenga alvarenga@kde.org