O Manual do Kleopatra

Marc Mutz
Desenvolvimento: David Faure
Desenvolvimento: Steffen Hansen
Desenvolvimento: Matthias Kalle Dalheimer
Desenvolvimento: Jesper Pedersen
Desenvolvimento: Daniel Molkentin
Tradução: José Pires

O Manual do Kleopatra

Conteúdo

Lista de Tabelas

Resumo

O Kleopatra é uma ferramenta para gerir os certificados de X.509 e OpenPGP.

Capítulo 1

Introdução

O Kleopatra é a ferramenta do KDE para gerir os certificados de X.509 e OpenPGP nos porta-chaves do GpgSM e do GPG, assim como para obter os certificados do LDAP e de outros servidores de certificados.

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

> NOTA
> Este programa obteve o nome da Cleópatra, uma famosa faraó egípcia que viveu na altura de Júlio César, de quem se diz que teve um filho, Pequeno César, não reconhecido como seu herdeiro.
> O nome foi escolhido, dado que este programa tem origem dos Projectos Ägypten (Ägypten significa Egipto em alemão). Kleopatra é a tradução em alemão de Cleópatra.

Capítulo 2

Funções Principais

2.1 Ver a Caixa de Chaves Local

A função principal do Kleopatra é mostrar e editar o conteúdo do chaveiro local, o qual é semelhante ao conceito de chaveiros do GPG, ainda que uma pessoa não se possa 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 cimo e ainda por uma barra de estado em baixo.

Cada linha da lista de chaves corresponde a um certificado, identificado pelo **DN do Sujeito**. O DN é um acrónimo para 'Distinguished Name' ou 'Nome Distinto', um identificador hierárquico, de certa forma semelhante a uma localização num sistema de ficheiros com uma sintaxe ligeiramente diferente, permitindo identificar de forma unívoca e global um dado 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 no caso de ser 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 de topo (a CA de raiz) assina a sua chave consigo própria (isto é chamado de auto-assinatura). Os certificados de raiz precisam, por isso, de ter validade (normalmente chamada de confiança) manualmente, isto é 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 utilizador com a interface da linha de comandos do GpgSM.

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

O utilizador poderá ver os detalhes de qualquer certificado se fizer duplo-click 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 infra-estrutura é capaz de extrair do certificado.

Se você alterar o chaveiro local sem usar o Kleopatra (isto é usando a interface da linha de comandos do GpgSM), poderá actualizar a janela com o **Ver → Voltar a mostrar (F5)** .

2.2 Procurar e Importar Certificados

Na maior parte do tempo, você irá adquirir os certificados novos ao verificar as assinaturas nas mensagens de e-mail, dado 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 contacto, você precisa de obter o certificado de um directório de LDAP (ainda que o GpgSM possa fazer isto automaticamente), ou através de um ficheiro. Também necessita de importar o seu próprio certificado depois de receber a resposta da CA ao seu pedido do certificado.

Para procurar por um certificado num directório de LDAP, seleccione a opção **Ficheiro** → **Procurar os Certificados no Servidor** e introduzir algum texto (isto é o nome da pessoa de quem deseja o certificado) no campo de texto da janela de **Pesquisa de Certificados no Servidor de Chaves**, carregando depois no botão **Procurar**. Os resultados serão apresentados na lista de chaves, por baixo da barra de procura, onde poderá seleccionar os certificados a observar, carregando 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 Directório** da janela de configuração do Kleopatra.

Se você recebeu o certificado como um ficheiro, tente o **Ficheiro** → **Importar os Certificados... (Ctrl+I)** . O GpgSM necessita de compreender o formato do ficheiro de certificado; por favor veja o manual do GpgSM para obter uma lista com os formatos de ficheiros suportados.

Se você não criou o seu par de chaves com o GpgSM, também irá necessitar de importar manualmente as chaves pública e privada do ficheiro PKCS#12 que obteve da CA. Poderá fazê-lo na linha de comandos com a instrução `-i --import-certificate` ou dentro do Kleopatra com o **Ficheiro** → **Importar os Certificados... (Ctrl+I)** , tal como faria para os certificados 'normais'.

2.3 Criar Novos Pares de Chaves

O item do menu **Ficheiro** → **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, carregue em **Próximo** para passar ao passo seguinte (ou **Anterior** para rever os passos já completos). A criação do pedido do certificado poderá ser cancelada em qualquer altura se carregar 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 a nível local, 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 utilizadores com o seu próprio certificado.

Terá de indicar 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 a nível local, mas são certificados por uma autoridade central (a CA). As CA's poderão certificar outras CA's, criando uma cadeia central e hierárquica de confiança.

O próximo passo do assistente é escrever 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; confirme que o introduz correctamente—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, ´´PT´´);

O próximo passo no assistente é seleccionar se é suposto gravar o certificado num ficheiro ou enviá-lo directamente para uma CA. Você terá de indicar o ficheiro ou o endereço de e-mail para onde enviar o pedido do certificado.

2.3.1 Revogar uma chave

Um par de chaves que tenha expirado poderá voltar a um estado operacional, desde que tenha acesso à chave privada e à frase-senha. Para inutilizar de forma fiável uma chave, terá de a revogar. A revogação é feita com a adição de uma assinatura de revogação especial à chave.

Esta assinatura de revogação é guardada num ficheiro separado. Este ficheiro poderá ser importado posteriormente para o porta-chaves e depois será associado à chave, inutilizando-a. Lembre-se que, para importar esta assinatura para a chave, não será necessária qualquer senha. Como tal, deverá guardar esta assinatura de revogação num local seguro, normalmente um que seja diferente do seu par de chaves. É um bom conselho usar um local que esteja dissociado do seu computador; copie-o para um dispositivo externo, como um disco USB, ou imprima-a.

O Kleopatra não oferece uma funcionalidade para criar uma dessas assinaturas de revogação em qualquer altura, mas podê-lo-á fazer com a aplicação do KDE KGpg, escolhendo a opção **Chaves** → **Revogar a chave** e, opcionalmente, importar imediatamente a assinatura de revogação ao seu porta-chaves.

Uma forma alternativa de gerar um certificado de revogação é usar o GPG directamente a partir da linha de comandos: **`gpg --output certificado_revogação.asc --gen-revoke a_sua_chave`**. O argumento *`a_sua_chave`* poderá ser um indicador de chave, sendo o ID de chave do seu par de chaves primário ou qualquer parte de um ID de utilizador que identifica o seu par de chaves.

Capítulo 3

Referência do Menu

3.1 O Menu Ficheiro

Ficheiro → 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 para si ou guardado num servidor LDAP para você obter para o seu porta-chaves local, onde o poderá usar para assinar e descodificar as mensagens de e-mail.

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

Ficheiro → 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.

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

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

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

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

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

Exporta os certificados seleccionados para um ficheiro.

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

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

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

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

> **NOTA**
> Isto exporta apenas as chaves públicas, mesmo que a chave privada esteja disponível. Use a opção **Ficheiro → Exportar as Chaves Privadas...** para exportar tanto as chaves públicas como as privadas para um ficheiro.

Ficheiro → Exportar as Chaves Privadas...

Exporta a chave privada para um ficheiro.

Na janela que aparece, poderá escolher o nome do **Ficheiro de saída**, e se deseja criar um ficheiro de exportação em binário ou em ASCII (**armação em ASCII**). Ao exportar as chaves privadas de S/MIME, poderá também escolher a **Codificação da frase-senha**. Veja a discussão sobre a opção `--p12-charset codificação`, no manual do GpgSM, para mais detalhes.
Esta função só está disponível quando tiver seleccionado exactamente um certificado, estando disponível a chave privada para esse certificado.

> **ATENÇÃO**
> Só raramente é deverá ser necessário usar esta função e, se for, deverá ser planeada 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.

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

Publica os certificados seleccionados 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 seleccionado pelo menos um certificado de OpenPGP (e nenhum S/MIME).

> **NOTA**
> Quando os certificados de OpenPGP tiverem sido exportados para um servidor de directório 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-nos entre si, pelo que não há grande vantagem em enviá-los para mais que um.
> Poderá acontecer que uma pesquisa num servidor de certificados não devolva quaisquer resultados, ainda que 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.

Ficheiro → Descodificar/Verificar os Ficheiros...

Descodifica os ficheiros e/ou verifica as assinaturas dos mesmos.

Ficheiro → Assinar/Encriptar os Ficheiros...

Assina e/ou encripta os ficheiros.

Ficheiro → Fechar (Ctrl+W)

Fecha a janela principal do Kleopatra. Podê-la-á repor a partir do ícone da bandeja em qualquer altura.

Ficheiro → Sair (Ctrl+Q)

Termina o Kleopatra.

3.2 O Menu Ver

Ver → Voltar a mostrar (F5)

Volta a mostrar a lista de certificados.
A utilização desta função normalmente não é necessária, dado que o Kleopatra vigia o sistema de ficheiros à procura de alterações e actualiza automaticamente a lista de certificados, sempre que for necessário.

Ver → Parar a Operação (Esc)

Pára (cancela) todas as operações pendentes, isto é uma procura, uma listagem ou uma transferência.
Esta função só está disponível se estiver pelo menos uma operação activa.

> NOTA
> Devido a limitações na infra-estrutura, algumas vezes as operações ficarão penduradas de tal forma que esta função não será capaz de as cancelar, agora ou mesmo de todo.
> Nesses casos, a única forma de repor a ordem é matar o SCDaemon, o DirMngr, o GpgSM e o GPG, por essa ordem, através das ferramentas do sistema operativo (**top**, Gestor de Tarefas, etc.), até que a operação seja desbloqueada.

Ver → Detalhes do Certificado

Mostra os detalhes do certificado actualmente seleccionado.
Esta função só está disponível se estiver seleccionado exactamente um certificado.

Esta função também está disponível carregando 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 dado certificado, mas é mais difícil encontrar um dado certificado inicialmente (ainda que possa, obviamente, usar à mesma a barra de procura).

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

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

> NOTA
> A visualização hierárquica só está de momento implementada para os certificados S/MIME. Existe algum desacordo entre os programadores no que respeita à forma correcta 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 janela da lista de certificados, isto é torna todos os itens visíveis.

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

Você poderá à mesma expandir e fechar cada item individualmente por si só, como é óbvio.

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

Ver → Fechar Tudo (Ctrl+,)

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

Você poderá à mesma expandir e fechar cada item individualmente por si só, como é óbvio.

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

3.3 O Menu Certificados

Certificados → Modificar a Confiança no Dono...

Modifica a confiança no dono do certificado de OpenPGP seleccionado de momento.

Esta função só está disponível quando tiver exactamente 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. Poderá, contudo, escolher apenas entre —em termos do OpenPGP—confiança 'absoluta' e 'nunca confiar'.

> NOTA
> A infra-estrutura (através do GpgAgent) irá perguntar, na altura da importação do certificado de raiz, se deseja confiar no certificado de raiz importado. Contudo, esta função terá de estar explicitamente activada na configuração da infra-estrutura (`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 de raiz como fidedignos** em capítulo 5).
> Se activar essa funcionalidade na infra-estrutura, poderá fazer com que apareçam mensagens do PinEntry em alturas inoportunas (isto é ao verificar as assinaturas), podendo bloquear o processamento do correio não verificado). Por essa razão, e dado 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 infra-estrutura para esta função, o Kleopatra tem de trabalhar directamente na base de dados de confiança do GpgSM (`trustlist.txt`). Ao usar esta função, certifique-se que não existem operações criptográficas em curso que possam interferir com o Kleopatra, no que respeita a modificações a essa base de dados.

Esta função só está disponível quando estiver seleccionado 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 seleccionado 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 seleccionado 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 seleccionado 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 quando estiver seleccionado um e só um certificado de raiz do OpenPGP e se estiver disponível a chave privada do mesmo. Obriga a ter uma infra-estrutura muito recente, dado que foi modificada a implementação de uma chamada directa ao GPG e ao GpgSM para uma chamada ao 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 está a correr, bem como da qualidade da implementação do PinEntry nessa plataforma, poderá acontecer que a janela do PinEntry apareça em segundo plano. Como tal, se seleccionar esta função e não acontecer nada, verifique a barra de tarefas do sistema operativo para ver se existe alguma janela do PinEntry aberta em segundo plano.

Certificados → Adicionar um ID de Utilizador...

Permite adicionar um novo ID de utilizador 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 utilizador do OpenPGP tem o seguinte formato:

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

Na janela que aparece quando seleccionar esta função, o Kleopatra perguntar-lhe-á 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 seleccionado um e só um certificado de raiz do OpenPGP e se estiver disponível a chave privada do mesmo.

Certificados → Apagar (Delete)

Remove os certificados seleccionados do porta-chaves local.

Use estas funções para remover as chaves não usadas do seu chaveiro local. Todavia, dado que os certificados estão tipicamente anexados às mensagens de e-mail assinadas, a verificação de uma destas mensagens poderá resultar na hipótese de a chave ser removida para depois voltar para o chaveiro local. Como tal, é provavelmente melhor evitar usar esta função o máximo possível. Quando se sentir perdido, use a barra de procura ou a função **Ver → Lista de Chaves Hierárquica** para voltar a ter o controlo sobre o lote de certificados.

> ATENÇÃO
> Existe uma excepção ao caso anterior: Quando apagar um dos seus próprios certificados, você está a apagar a chave privada também com ele. Isto implica que não será capaz de ler as comunicações anteriores encriptadas para si com este certificado, a menos que tenha uma cópia de segurança algures.
> O Kleopatra avisá-lo-á quando 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 seleccionado pelo menos um certificado.

Certificados → Apresentar os Dados do Certificado

Mostra todas as informações que o GpgSM tem acerca do certificado seleccionado (S/MIME).

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

3.4 O Menu Ferramentas

Ferramentas → Visualizador do Registo do GnuPG...

Inicia o KWatchGnuPG, uma ferramenta para apresentar o resultado de depuração da aplicação GnuPG. Se a assinatura, encriptação ou a verificação deixarem de funcionar misteriosamente, poderá descobrir porquê, olhando para o registo.

Esta função não está disponível no Windows®, dado que os mecanismos subjacentes não estão implementados na infra-estrutura dessa plataforma.

Ferramentas → Actualizar os Certificados do OpenPGP

Actualiza todos os certificados de OpenPGP, executando o comando

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

Depois de o comando terminar com sucesso, o seu porta-chaves local irá reflectir as últimas alterações no que respeita à validade dos certificados do OpenPGP.

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

Ferramentas → Actualizar os Certificados X.509

Actualiza 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 ficheiros: Quando apaga uma pasta, irá apagar todos os ficheiros e pastas nela contidos também.

Depois de o comando terminar com sucesso, o seu porta-chaves local irá reflectir as últimas alterações no que respeita à validade dos certificados do S/MIME.

> NOTA
> A actualização dos certificados X.509 ou OpenPGP implica a obtenção de todos os certificados e CRL's, de modo a verificar se entretanto foram revogados.
> Isto poderá colocar bastante incómodo perante si, assim como nas ligações de rede das outras pessoas, podendo levar até uma hora ou mais ainda a terminar, dependendo da sua ligação de rede e do número de certificados a verificar.

Ferramentas → Importar uma CRL de um Ficheiro...

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

Normalmente, as Listas de Revogação de Certificados (ou CRL's) são tratadas de forma transparente pela infra-estrutura, 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 desactivado, deverá contactar o administrador de sistemas e pedir-lhe para instalar o DirMngr.

Ferramentas → Limpar a 'Cache' de CRL's

Limpa a 'cache' de CRL's do GpgSM.

Provavelmente, nunca irá necessitar disto. Poderá forçar uma actualização da sua 'cache' de CRL's, seleccionando todos os certificados e usando o **Ferramentas → Actualizar os Certificados X.509** em alternativa.

Ferramentas → Exportar a 'Cache' de CRL's

Mostra o conteúdo detalhado da 'cache' de CRL's do GpgSM.

3.5 O Menu Configuração

O Kleopatra tem um menu de **Configuração** normal do KDE, tal como descrito nos Fundamentos do KDE, com um item adicional:

Configuração → Efectuar os Testes Automáticos

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

Este é o mesmo conjunto de testes que é executado no arranque, por omissão. Caso tenha desactivado os testes automáticos no arranque, podê-los-á voltar a activar aqui.

3.6 O Menu Janela

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

Ao carregar com o botão direito do rato, poderá carregar numa página para abrir um menu de contexto, onde poderá também seleccionar as mesmas acções.

3.7 O Menu Ajuda

O Kleopatra tem um menu de **Ajuda** normal do KDE, como 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 todas as aplicações do KDE, você poderá obter uma lista completa das opções se usar o comando **`kleopatra --help`**.

`--uiserver-socket` ***argumento***
: Localização do 'socket' do servidor de UI onde atender

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

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

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

`-i --import-certificate`
: Indica um ficheiro ou URL a partir do qual importar os certificados (ou chaves privadas).

  Este é o equivalente na linha de comandos ao **Ficheiro → Importar os Certificados... (Ctrl+I)** .

`-e --encrypt`
: Encriptar os ficheiros

`-s --sign`
: Assinar os ficheiros

`-E --encrypt-sign`
: Encripta e/ou assina os ficheiros. É igual ao `--sign-encrypt`, não usar

`-d --decrypt`
: Descodificar os ficheiros

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

`-D --decrypt-verify`
: Descodificar e/ou verificar os ficheiros

Capítulo 5

Configurar o Kleopatra

A janela de configuração do Kleopatra poderá ser acedida em **Configuração** → **Configurar o Kleopatra...**

Cada uma das suas páginas está descrita nas secções em baixo.

5.1 Configurar os Serviços de Directório

Nesta página, poderá configurar os servidores de 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, terá de modificar o ficheiro de configuração `gpg.conf` directamente. Veja por favor o manual do GPG para saber mais detalhes. O Kleopatra irá preservar essas opções, se bem que não as permite modificar ainda na GUI.

A tabela dos **Serviços de directório** mostra os servidores que estão configurados de momento. Faça duplo-click 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 aceder ao servidor. Os esquemas mais usados incluem o **ldap** (e o seu semelhante em SSL, o **ldaps**) para os servidores de 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, isto é `keys.gnupg.net`.

Porto do Servidor
O porto de rede em que o servidor está à espera de pedidos.

Isto muda automaticamente para o porto predefinido, assim que mudar o **Esquema**, a menos que tenha sido definido com algum porto fora do normal e que não o consiga repor de volta; tente definir o **Esquema** como sendo **`http`** e o **Porto do Servidor** como **`80`** (o valor predefinido 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 Utilizador
O nome do utilizador, se existir, a usar para se autenticar no servidor.

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

Senha
A senha ou palavra-passe, se existir, a usar para se autenticar no servidor.

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

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

Só são suportados os servidores de 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.

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, carregue no botão **Novo**. Isto duplica o item seleccionado, se existir, ou então introduz um servidor predefinido de OpenPGP. Depois poderá definir o **Nome do Servidor**, o **Porto do Servidor**, o **DN de base**, o **Senha** e o **Nome do Utilizador**, sendo os dois últimos necessários apenas se o servidor necessitar de autenticação.

Para introduzir directamente um item para os certificados de 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, seleccione-o na lista e carregue depois no botão **Remover**.

Para definir o tempo-limite do LDAP, isto é o tempo máximo que a infra-estrutura 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**, poderá querer aumentar este limite. Você poderá concluir que, se atingir esse limite durante uma pesquisa, irá aparecer uma janela neste caso, a avisá-lo 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 dado 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 a mostrar apenas um sub-conjunto 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 facto, distintas entre si (isto é especialmente importante se só tiver seleccionado a **Mostrar a validade**).

Poderá activar ou desactivar, de forma independente, os seguintes conjuntos de informações:

Mostrar a validade

Mostra informações acerca da validade de um dado certificado: o seu estado actual, 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 Ficheiros, Encriptar E- ↩
    Mails e Ficheiros
ID-Chave:           DC9D9E43
```

Mostrar a informação do dono

Mostra informações acerca do dono do certificado: o DN do sujeito (apenas para o S/MIME), os ID's dos utilizadores (incluindo os endereços de e-mail) e a confiança no dono (apenas para o OpenPGP).

Exemplo do OpenPGP:

```
ID-Utilizador:          UtilizadorGpg4win <utilizador_gpg4win@teste.qg ↩
    >
ID-Chave:           C6BF6664
Confiança no dono:       absoluta
```

. Exemplo do S/MIME:

```
Sujeito:          CN=UtilizadorGpg4win,OU=Lab_Testes,O=Projecto  ↩
    Gpg4win,C=DE
a.k.a.:           utilizador_gpg4win@teste.qg
ID-Chave:           DC9D9E43
```

Mostrar os detalhes técnicos

Mostra informações técnicas acerca do 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 o tipo de letra.

Cada categoria de certificados à esquerda tem atribuído um conjunto de cores e um tipo de letra, com o qual as chaves que pertencerem a essa categoria são apresentados. A lista de categorias também actua como uma antevisão da configuração. As categorias poderão ser definidas de forma livre pelo administrador ou por um utilizador com privilégios; veja o Seção 6.2 em capítulo 6.

Para definir ou alterar o ícone de uma categoria, seleccione-a na lista e carregue no botão **Alterar o Ícone...**. A janela de selecção de ícones normal do KDE irá aparecer, e nela poderá escolher um ícones existente da colecção do KDE ou carregar um ícone personalizado.

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

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

A alteração da cor de fundo é feita da mesma forma, carregando em alternativa no botão **Alterar a Cor de Fundo...**.

Para alterar o tipo de letra, o utilizador tem duas opções:

1. Modifica o tipo de letra normal, utilizado por todas as listas no KDE.
2. Utilizar um tipo de letra personalizado.

A primeira opção tem a vantagem que o tipo de letra irá seguir o estilo que você definiu a nível do KDE, enquanto que a última dá-lhe um controlo completo sobre o tipo de letra a usar. A escolha é sua.

Para usar o tipo de letra modificado, seleccione a categoria na lista e ligue ou desligue os modificadores do tipo de letra **Itálico**, **Negrito**, e/ou **Traçado**. Você poderá ver imediatamente o efeito do tipo de letra na lista de categorias.

Para usar um tipo de letra personalizado, carregue no botão **Alterar o Tipo de Letra...**. A janela normal de selecção do tipo de letra do KDE irá aparecer e nela poderá seleccionar o novo tipo de letra.

> NOTA
> Poderá usar à mesma os modificadores dos tipos de letra para mudar o tipo de letra personalizado, como faria para modificar o tipo de letra normal.

Para voltar ao tipo de letra normal, terá de carregar no botão **Aparência por Omissão**.

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 todas as aplicações que usam a Tecnologia do Kleopatra. Na altura em que este documento foi escrito, estas incluem o KMail, o KAddressBook, assim como o próprio Kleopatra, como é óbvio.

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

Ambas as listas contêm itens descritos pela forma resumida do atributo (isto é **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 actual dos atributos** reflecte 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 actual dos atributos** é que são mostrados de todo. O resto fica escondido por omissão.

Contudo, se o item de substituição **_X_** (**Todos os outros**) estiver na lista 'actual', 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 clarificar isto:

Dado o DN

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

a ordem de atributos por omissão 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=US

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

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

Para adicionar um atributo à lista da ordem de apresentação, seleccione-o na lista de **Atributos disponíveis** e carregue no botão **Adicionar à ordem actual dos atributos**.

Para remover um atributo da lista da ordem de apresentação, seleccione-o na lista de **Ordem actual dos atributos** e carregue no botão **Remover da ordem actual dos atributos**.

Para mover um atributo para o início (fim), seleccione-o na lista **Ordem actual dos atributos** e carregue no botão **Mover para o topo** (**Mover para o fundo**).

Para mover um atributo apenas uma posição para cima (baixo), seleccione-o na lista **Ordem actual dos atributos** e carregue no botão **Subir** (**Descer**).

5.3 Configurar as Operações Criptográficas

5.3.1 Configurar as Operações de E-Mail

Aqui poderá configurar alguns aspectos das operações de e-mail do UiServer do Kleopatra. De momento, só pode configurar se deve usar o 'Modo Rápido' para assinar e encriptar os e-mails, respectivamente.

Quando o 'Modo Rápido' estiver activo, 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 Ficheiros

Aqui poderá configurar alguns aspectos das operações com ficheiros do UiServer do Kleopatra. De momento, 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 é que será usado para criar os ficheiros de códigos de validação.

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

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

5.4 Configurar os aspectos da Validação S/MIME

Nesta página, 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 excepção 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 activa a verificação periódica da validade dos certificados. Poderá também escolher o intervalo da verificação (em horas). O efeito da verificação periódica é o mesmo que o **Ver → Voltar a mostrar (F5)** ; não existe nenhuma possibilidade de agendar periodicamente o **Ferramentas → Actualizar os Certificados do OpenPGP** ou o **Ferramentas → Actualizar os Certificados X.509** .

> **NOTA**
> A validação é efectuada implicitamente sempre que os ficheiros significativos em `~/.gnupg` forem alterados. Esta opção, tal como a **Ferramentas → Actualizar os Certificados do OpenPGP** e a **Ferramentas → Actualizar os Certificados X.509** , só afecta os factores externos da validade do certificado.

5.4.2 Configurar o método de validação

Validar os certificados com as CRLs

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

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

Validar os 'certificados' a nível 'online' (OCSP)

Se esta opção estiver seleccionada, os certificados de S/MIME são validados a nível '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 de cada vez que envia ou recebe uma mensagem criptográfica, o que permite em teoria à agência de emissão de certificados fazer um seguimento das pessoas com quem trocou mensagens (isto é).

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

Veja o **Validar os 'certificados' a nível '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

Indique 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 o URL de serviço dos 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 dado 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 isto é para forçar a utilização de um 'proxy' de OCSP empresarial.

5.4.3 Configurar as opções de validação

Não verificar políticas de certificados

Por omissão, o GpgSM usa o ficheiro `~/.gnupg/policies.txt` para verificar se uma dada política de certificados é permitida ou não. Se esta opção estiver seleccionada, 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 de raiz como fidedignos

Se esta opção estiver assinalada quando estiver a importar um certificado da CA de raiz, ser-lhe-á pedida a confirmação da sua impressão digital e se considera este certificado de raiz como sendo fidedigno ou não.

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

> NOTA
> Se activar esta funcionalidade na infra-estrutura, poderá obter janelas indesejadas do PinEntry (isto é ao verificar as assinaturas), podendo assim bloquear o processamento de correio não-verificado. Por essa razão, e dado 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 os certificados do emissor em falta

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 efectuar pedidos HTTP

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

Ignorar o ponto de distribuição 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 aceder 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.

Utilizar o 'proxy' HTTP do sistema

Se esta opção estiver seleccionada, 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.

Utilizar este 'proxy' para pedidos HTTP

Se não estiver definido nenhum 'proxy' do sistema, ou caso precise de 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:porto`**, isto é **`proxy.nenhures.com:3128`**.

5.4.5 Configurar as opções dos pedidos de LDAP

Não efectuar pedidos LDAP

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

Ignorar o ponto de distribuição 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 aceder 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 pedidos LDAP

Se indicar aqui um servidor de LDAP, fará com que todos os pedidos de LDAP vão primeiro a este servidor. Para ser mais exacto, esta opção substitui todas as definições de *máquina* e *porto* de um URL de LDAP, sendo também usadas caso a *máquina* e o *porto* tenham sido omitidos do URL.

Os outros servidores de LDAP só serão usados se a ligação ao 'proxy' for mal-sucedida. A sintaxe é **máquina** ou **máquina:porto**. Se o *porto* for omitido, é usado o porto-padrão de LDAP, que é o 389.

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 seleccionadas nesta parte da janela.

O conteúdo exacto desta parte da janela depende da versão da infra-estrutura do GnuPG que tiver instalada e, potencialmente, a plataforma em que está a correr. Deste modo, só iremos discutir a disposição geral da janela, incluindo a associação das opções do GpgConf aos controlos 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. Exceptuando as opções mais conhecidas que o Kleopatra já trata com controlos especializados, para uma melhor experiência do utilizador, a associação entre os tipos do GpgConf e os controlos do Kleopatra é a seguinte:

Tipo do GpgConf	**Controlo do Kleopatra**	
	para listas	**para excepções às listas**
`nenhuma`	Campo incremental (semântica de 'quantidade')	Opção

texto	N/A	Campo de texto
int32	Campo de texto (não formatado)	Campo incremental
uint32		
localização	N/A	controlo especializado
servidor de LDAP	controlo 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 Controlos GUI

Veja o manual do GpgConf para saber 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 ficheiros de configuração.

Assume-se que o leitor está familiarizado com a tecnologia usada para a configuração das aplicações do KDE, incluindo o formato, a localização no sistema de ficheiros e o encadeamento dos ficheiros 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 utilizador 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 dado valor, escreva algo do tipo Atributo=valor. Se quiser que o atributo seja tratado como obrigatório, adicione um ponto de exclamação (isto é `CN!`,`L`,`OU`,`O!`,`C!`,`EMAIL!` que é, de facto, a configuração por omissão).

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

> DICA
> Devido à natureza da plataforma KIOSK do KDE, se usar a opção de inalterável (`$i`), irá impossibilitar ao utilizador a sobreposição da opção. Este é o comportamento pretendido. O `$i` e o `$e` podem ser usados com todas as chaves de configuração das aplicações 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 utilizador 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 PT, mas permitindo alterações pelo utilizador
C=PT
```

6.1.2 Restringir os Tipos de Chaves que um Utilizador Poderá Criar

O Kleopatra também lhe permite restringir o tipo de certificados que um dado utilizador poderá criar. Lembre-se, contudo, que uma forma simples de dar a volta a estas restrições é criar um certificado pela linha de comandos.

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 secção `CertificateCreationWizard` do ficheiro `kleopatrarc`.

Os valores permitidos como `RSA` para as chaves RSA, `DSA` para as chaves DSA (apenas de assinatura), e `DSA+ELG` para uma chave DSA (apenas de assinatura) com uma sub-chave ElGamal para a encriptação.

O valor por omissão 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 secção `CertificateCreationWizard` do ficheiro `kleopatrarc`, contendo uma lista de tamanhos de chaves separadas por vírgulas (em 'bits'). Poderá indicar um valor por omissão 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 por omissão.

Para além dos tamanhos propriamente ditos, 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 género na selecção:

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

Os valores por omissão serão os seguintes:

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

6.2 Criar e Editar Categorias de Chaves

O Kleopatra permite ao utilizador 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 secção descreve como 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*, explicada 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`.

As únicas chaves obrigatórias num grupo `Key Filter #n` é o `Name`, que contém o nome da categoria, tal como aparece na janela de configuração e o `id`, que é usado como referência para o filtro nas outras secções 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 na 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 usar. Se estiver em falta, usa a cor de fundo definida a nível global para as listas.
`foreground-color`	cor	A cor do texto a usar. Se estiver em falta, usa a cor do texto definida a nível global para as listas.
`font`	tipo de letra	O tipo de letra a usar. Esse tipo de letra será ajustado para o tamanho configurado para as listas e todos os atributos dos tipos de letra (ver em baixo) serão aplicados.
`font-bold`	booleano	Se for igual a `true` e o `font` não estiver definido, usa o tipo de letra por omissão 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 um tipo de letra itálico em vez de negrito.
font-strikeout	booleano	Se for igual a true, desenha uma linha centrada por cima do tipo de letra. É aplicado, mesmo que o font esteja definido.
icon	texto	O nome do ícone a mostrar 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 indicadas, o filtro faz correspondência quando...**
is-revoked	booleano	a chave foi revogada.
match-context	context[1]	o contexto a que este filtro corresponde.
is-expired	booleano	a chave expirou.
is-disabled	booleano	a chave foi desactivada (marcada para não ser usada) pelo utilizador. 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 encriptação.
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 (isto é como um certificado de cliente TLS).
is-qualified	booleano	a tecla poderá ser usada para fazer Assinaturas Qualificadas (como está definido na Lei de Assinatura Digital alemã).
is-cardkey	booleano	O material da chave está guardado num 'smartcard' (em vez do computador).

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

`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`	validate[2]	a chave tem exactamente (*`prefixo`* = `is`), tem tudo excepto (*`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 do que uma chave `prefixo-ownertrust` (com vários valores de *`prefixo`*) num único grupo, o comportamento será indefinido.
`prefixo-validity`	validate	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 omissão, só as chaves validadas são verificadas a nível de revogação e expiração, ainda que você seja livre para remover estas verificações extra.

Para 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, poderá referenciar o filtro de chaves mais tarde na configuração, isto é 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 de momento: o contexto `appearance` é usado ao definir as propriedades de cores e tipos de letra das janelas. O contexto `filtering` é usado para incluir (e excluir) de forma selectiva os certificados das janelas. O `any` pode ser usado para se aplicar a todos os contextos definidos de momento,

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

sendo a opção por omissão 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 actuam por 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, dado que corresponde a `!any`. Contudo, os dois últimos serão substituídos por `any`, dado 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 ficheiro 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 de OpenPGP desactivadas (ainda não suportado pelo Kleopatra) com um grau de confiança pelo menos 'marginal', você iria usar:

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

6.3 Configurar os Arquivadores a Usar ao Assinar/Encriptar os Ficheiros

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

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 ficheiros 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 utilizador do arquivador, tal como aparece na lista correspondente na janela para Assinar/Encriptar os Ficheiros.

`pack-command`

O comando real usado para arquivar os ficheiros. Poderá usar qualquer comando, desde que não seja necessária qualquer linha de comandos para o executar. O programa é pesquisado com a variável de ambiente `PATH`, a menos que tenha usado uma localização absoluta para o ficheiro. Existe o suporte para aspas, caso tenha sido utilizada uma linha de comandos:

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

NOTA

Dado que a barra invertida (\) é um carácter de escape nos ficheiros de configuração do KDE, terá de os duplicar quando aparecerem nos nomes dos ficheiros:

```
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, dado 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 Ficheiro de Entrada ao `pack-command`

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

1. Como argumentos da linha de comandos.

   Exemplo (tar):

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

   Exemplo (zip):

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

Nesse caso, os nomes dos ficheiros são passados na linha de comandos, tal como faria ao usar a linha de comandos. O Kleopatra não usa nenhuma linha de comandos para executar o comando. Como tal, esta é uma forma segura de passar os nomes dos ficheiros, mas, se bem que poderá ter algumas restrições quanto ao tamanho da linha de comandos em algumas plataformas. Um `%f` literal, se estiver presente, será substituído pelos nomes dos ficheiros a arquivar. Caso contrário, os nomes dos ficheiros serão adicionados à linha de comandos. Como tal, 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 -@ -
   ```

   Neste caso, os nomes dos ficheiros são passados ao programa de arquivo pelo stdin, um por cada linha. Isto evita os problemas nas plataformas que colocam um limite baixo no número de argumentos permitido pela linha de comandos, mas não resulta quando os nomes dos ficheiros contêm de facto mudanças de linha nos seus nomes.

   > NOTA
   > O Kleopatra só suporta de momento o LF como separador de linhas, não suportando o CRLF. Isto poderá mudar nas próximas versões, dependendo das reacções do utilizador.

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

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

   Este é igual ao anterior, com a diferença que são usados 'bytes' NUL (vazios) para separar os nomes dos ficheiros. Dado que os 'bytes' NUL são proibidos nos nomes dos ficheiros, esta é a forma mais robusta de passar nomes de ficheiros, 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 utilizadores especializados) configurar a lista de programas de geração de códigos de validação de integridade que o utilizador 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 dado ficheiro.

NOTA

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

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

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

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

em que o *NOME-FICHEIRO-ESCAPADO* é o nome do ficheiro 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

```
FICHEIRO ( ': 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, pelo que o Kleopatra não conseguirá processar os ficheiros 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 ficheiros que poderão ser considerados ficheiros de validação de integridade para este programa em particular. A sintaxe é a mesma que é usada para as listas de textos nos ficheiros de configuração do KDE.

  NOTA
  Dado que as expressões regulares normalmente contêm barras invertidas (\), deve-se ter algum cuidado em escapá-las também no ficheiro. Recomenda-se a utilização de uma ferramenta de edição de ficheiros de configuração.

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

`output-file`
: O nome do ficheiro 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 ficheiro de saída, cada vez que criar ficheiros 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 utilizador 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 ficheiros 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

CONTRIBUIÇÕES

- 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 José Nuno Pires zepires@gmail.com