O Manual do KGpg

Jean-Baptiste Mardelle
Rolf Eike Beer
Tradução: José Pires

O Manual do KGpg

Conteúdo

Resumo

O KGpg é uma interface gráfica simples para o GnuPG (http://gnupg.org).

Capítulo 1

Introdução

O KGpg é uma interface simples para o GnuPG, um utilitário poderoso de encriptação. O GnuPG (também conhecido por 'gpg') vem incluído na maioria das distribuições e deverá estar instalado no seu sistema. Poderá obter a última versão em http://gnupg.org.

Com o KGpg será capaz de cifrar e decifrar os seus ficheiros e e-mails, o que lhe permitirá comunicações muito mais seguras. Está disponível um mini-tutorial sobre encriptação com o gpg na página Web do GnuPG.

Com o KGpg, não terá de se lembrar das linhas de comando e opções do 'gpg'. Quase tudo poderá ser feito com alguns 'clicks' do rato.

Capítulo 2

Começar

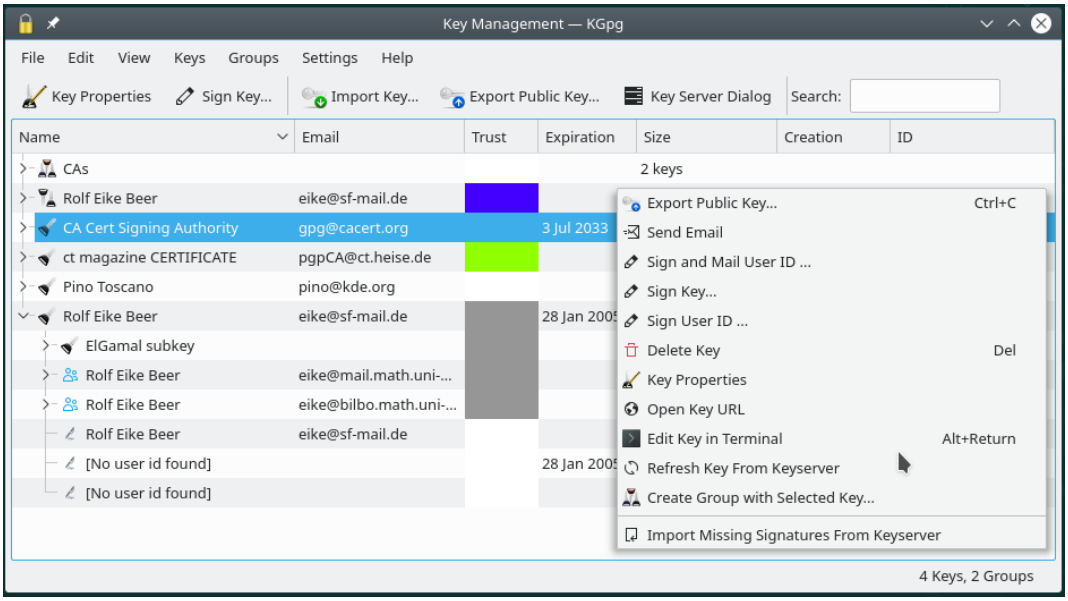
Aqui está uma lista das principais componentes do KGpg:

Ícone da Bandeja do Sistema

Quando iniciar o KGpg, irá aparecer um ícone na bandeja do sistema. Se carregar nele com o botão esquerdo do rato irá abrir a janela de Gestão das Chaves, por outro lado se carregar com o botão direito do rato irá abrir um menu que permite rápido acesso a algumas funcionalidades importantes. Se preferir outras opções, poderá modificar a acção do botão esquerdo do rato para mostrar o editor ou desactivar por completo o ícone da bandeja, usando a janela de configuração.

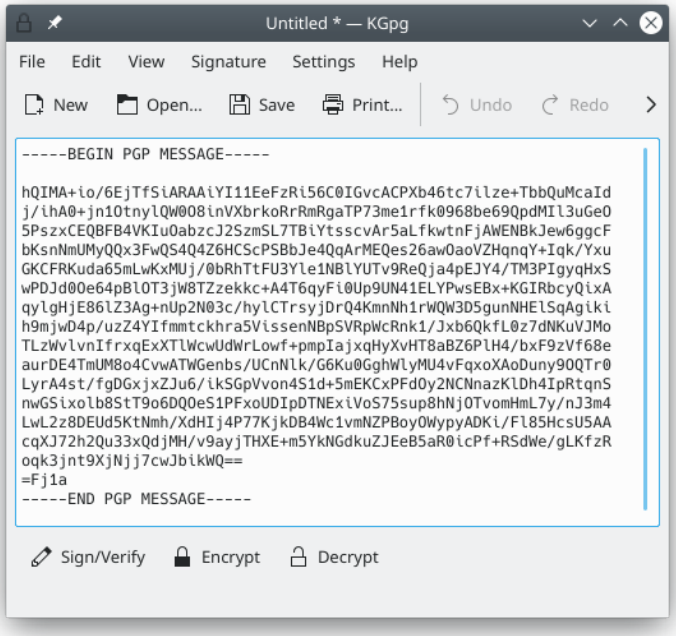
Lembre-se que o ícone da bandeja do KGpg fica marcado como ˝inactivo˝ na maior parte do tempo. Dado que a 'applet' da bandeja irá normalmente esconder os ícones inactivos, o do KGpg poderá não ficar visível até que lhe peça explicitamente para tal. Para mais detalhes, veja a documentação do Plasma.

Janela de Gestão de Chaves



Esse é o local central para gerir as suas chaves. Para abrir a janela de Gestão das Chaves, carregue com o botão esquerdo do rato na 'applet' do KGpg. Poderá importar, exportar, assinar e editar as suas chaves. A maioria das acções poderá ser feita com um 'click' do botão direito do rato numa chave.

Janela do Editor



É um editor de texto simples, onde poderá escrever ou colar texto para o cifrar ou decifrar. Para abrir o editor, carregue com o botão direito do rato na 'applet' do KGpg.

Integração com o gestor de ficheiros

O KGpg está integrado no Konqueror e do Dolphin. Isto significa que, quando carrega num ficheiro, pode optar por **Acções** → **Encriptar o Ficheiro** para o cifrar. Pode decifrá-lo se carregar com o botão esquerdo do rato.

Capítulo 3

Usar o KGpg

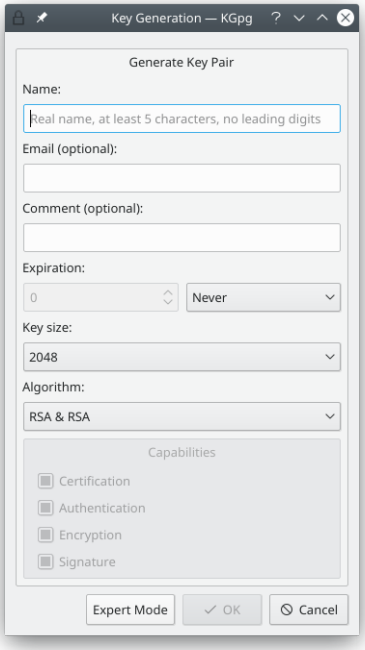
Existem duas formas de cifrar os seus dados:

- Cifra simétrica: os seus dados são apenas cifrados com uma senha. Qualquer pessoa que tiver um computador com o 'gpg' poderá decifrar a sua mensagem se lhe der a senha. Para efectuar uma cifra simétrica, escolha a ˝cifra simétrica˝ na janela de opções quando for pedido para escolher uma senha de cifra.
- Cifra por chave: primeiro terá de criar o seu par de chaves (pública e privada) e indicar uma frase-senha. Mantenha a sua chave privada num local seguro e troque a sua chave pública com os seus amigos. Aí, se quiser enviar uma mensagem cifrada para o Alex, terá de cifrar a mensagem com a chave pública do Alex. Para decifrar a mensagem, o destinatário irá necessitar da chave privada e da frase-senha do Alex.

A cifra por chave é um pouco mais complicada (precisa de trocar chaves com os seus amigos) mas é mais segura. Lembre-se que, se cifrar uma chave com a chave de outra pessoa, não será capaz de a decifrar. Só consegue decifrar as mensagens que tenham sido cifradas com a sua chave pública.

3.1 Gerar uma chave

Se não tiver uma chave, o KGpg irá automaticamente mostrar a janela de geração de chaves no primeiro arranque. Pode também aceder à mesma no Gestor de Chaves a partir da opção **Chaves** → **Gerar um Par de Chaves**.



Basta indicar o seu nome, o endereço de e-mail e carregar em **Ok**. Será gerada uma chave-padrão de GPG. Se quiser mais opções poderá carregar no botão do **Modo Experiente**, o que irá mostrar uma janela do Konsole com todas as opções do 'gpg'.

Muitas pessoas gostam de brincar com a sua primeira chave, geram ID's de utilizadores inválidos, adicionam comentários que se arrependem mais tarde ou simplesmente esquecem a sua senha. Para evitar que essas chaves se mantenham válidas para sempre, é normalmente boa ideia limitar o tempo de vida para cerca de 12 meses. Você poderá modificar o tempo de vida das suas chaves privadas mais tarde com a janela de propriedades da chave.

3.2 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.

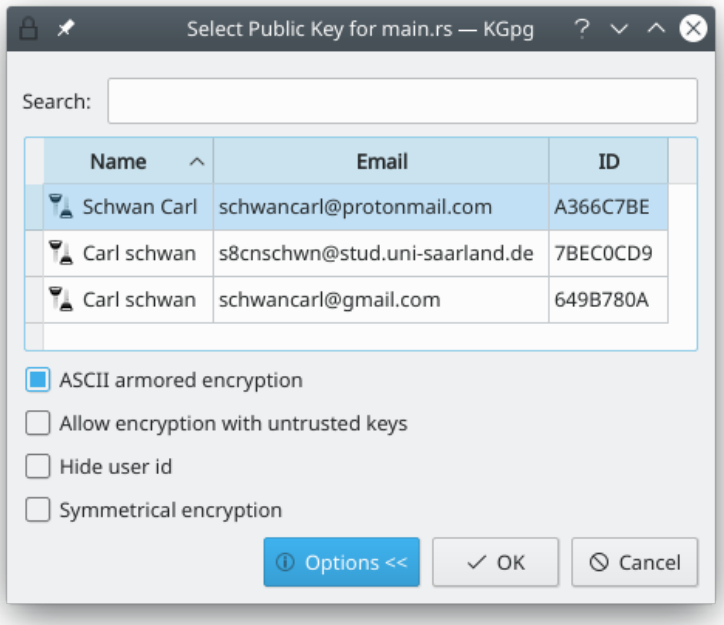
Esta assinatura de revogação poderá ser criada em conjunto com a chave. Nesse caso, é guardada num ficheiro separado. Esse ficheiro poderá então ser importado para o porta-chaves e depois anexado à chave, inutilizando-a. Lembre-se por favor que, para importar esta assinatura para a chave, não é necessária qualquer senha. Como tal, deverá guardar esta assinatura de revogação num local seguro, normalmente num que seja distinto do seu par de chaves. Um bom conselho é usar um local separado do seu computador, seja copiando-o para um dispositivo externo de armazenamento (p.ex., um disco USB) ou imprimindo-o.

Se não tiver criado uma dessas revogações destacadas na criação da chave, poderá criar uma assinatura de revogação em qualquer altura, escolhendo a opção **Chaves** → **Revogar a chave**, importando-a opcionalmente para o seu porta-chaves de imediato.

3.3 Cifrar os Seus Dados

3.3.1 Cifrar um Ficheiro a Partir do Konqueror ou do Dolphin

Carregue no ficheiro que deseja cifrar com o botão direito do rato. Escolha a opção **Acções** → **Cifrar o Ficheiro** no menu de contexto. Ser-lhe-á apresentada a janela de selecção da Chave Pública. Escolha a chave do destinatário e carregue em **Cifrar**. O ficheiro cifrado será gravado com uma extensão `.asc` ou `.gpg`, dependendo se escolheu a **cifra armada ASCII** ou não. Os ficheiros encriptados em ASCII só usam os caracteres visíveis, para representar os dados resultantes, nos ficheiros para serem mais robustos ao copiar ou enviar por e-mail; contudo, são maiores em um terço.



3.3.2 Cifrar um texto com a 'applet' do KGpg

Poderá encriptar o conteúdo da área de transferência, seleccionando para tal a opção **Encriptar a área de transferência** no menu da 'applet'. Quando escolher a opção **Assinar a área de transferência**, então o texto será assinado em alternativa. Ambas as acções irão importar o conteúdo actual da área de transferência para a janela do editor, efectuam a acção pedida e colam o conteúdo de volta no editor.

3.3.3 Cifrar o texto do editor do KGpg

É tão simples como carregar no botão **Encriptar**. Ser-lhe-á então apresentada a janela de selecção da chave pública; escolha a sua chave e carregue em **Ok**. A mensagem cifrada irá então aparecer na janela do editor.

Normalmente, só poderá encriptar os ficheiros que sejam da sua confiança. Dado que, algumas vezes, só deseja enviar uma nota privada a algumas pessoas que sabe que têm uma chave de GPG, poderá activar a opção **Activar a encriptação com chaves não-fiáveis**.

Para se certificar que consegue descodificar os ficheiros que encriptou, mesmo que o tenha feito com a chave de outra pessoa, poderá usar as opções **Encriptar sempre com** e **Encriptar os ficheiros com**, que estão disponíveis na configuração do KGpg.

Para mais informações sobre as opções de encriptação 'Cifra de ASCII armada', 'Permitir a cifra com chaves não fiáveis' e 'Cifra simétrica', por favor veja a documentação ou as páginas do 'man'.

3.4 Decifrar os Seus Dados

3.4.1 Decifrar um Ficheiro a Partir do Konqueror ou do Dolphin

Carregue com o botão esquerdo no ficheiro que quer decifrar. Indique a sua frase-senha e este será decifrado. Também poderá arrastar um ficheiro de texto cifrado e largá-lo na janela do editor do KGpg. Ser-lhe-á então pedida a frase-senha, ao que depois poderá abrir o texto decifrado no editor do KGpg. Poderá inclusive largar aqui ficheiros remotos! Também poderá usar a opção **Ficheiro** → **Decifrar o Ficheiro** e escolher o ficheiro a decifrar.

3.4.2 Decifrar um texto com a 'applet' do KGpg

Poderá também descodificar o conteúdo da área de transferência, usando a opção do menu **Descodificar a Área de Transferência** da 'applet' do KGpg. Irá aparecer uma janela do editor com o texto descodificado.

3.4.3 Decifrar um texto do editor

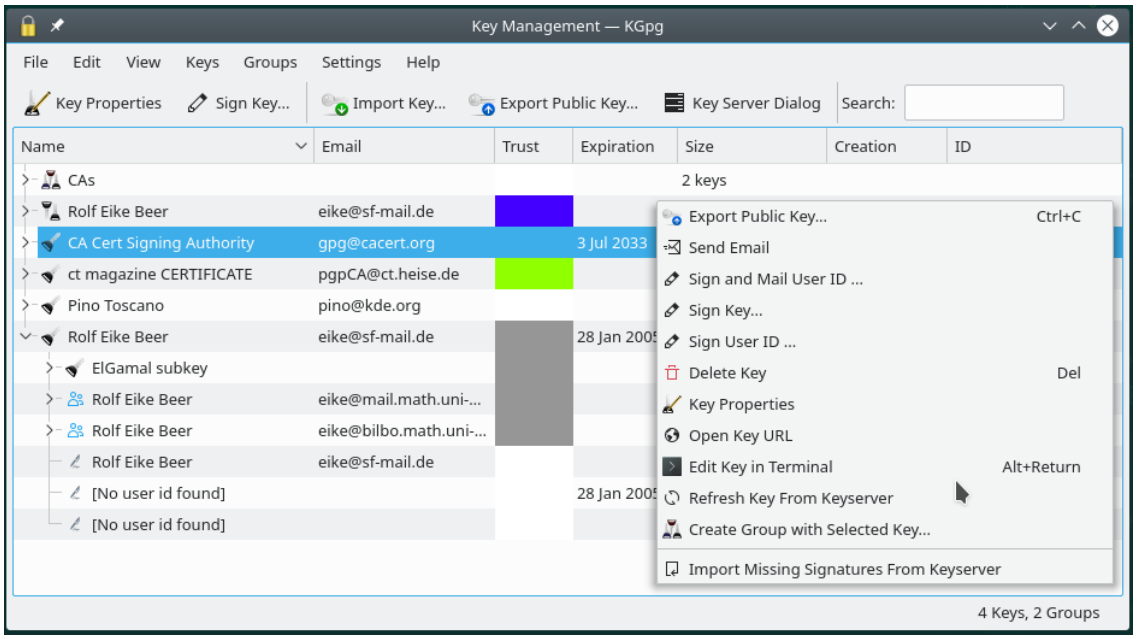
Copie ou arraste e largue o texto que deseja decifrar, e carregue no botão **Decifrar**. Ser-lhe-á pedida a frase-senha.

3.5 Gestão de Chaves

Todas as opções básicas de gestão de chaves poderão ser efectuadas através do KGpg. Para abrir a janela de gestão de chaves, carregue com o botão esquerdo do rato na 'applet' do KGpg. A maioria das opções estão disponíveis se carregar com o botão direito numa chave. Para importar/exportar as chaves públicas, poderá arrastar e largar os itens ou usar os atalhos de teclado Copiar/Colar.

Poderá exportar uma chave pública por e-mail, para a área de transferência, para um servidor de chaves ou para um ficheiro local. Use as opções na janela de exportação para exportar tudo, exportar sem atributos (identificações fotográficas) ou exportar uma chave limpa isto é, a chave em si, incluindo as suas sub-chaves, mas excluindo todas as assinaturas.

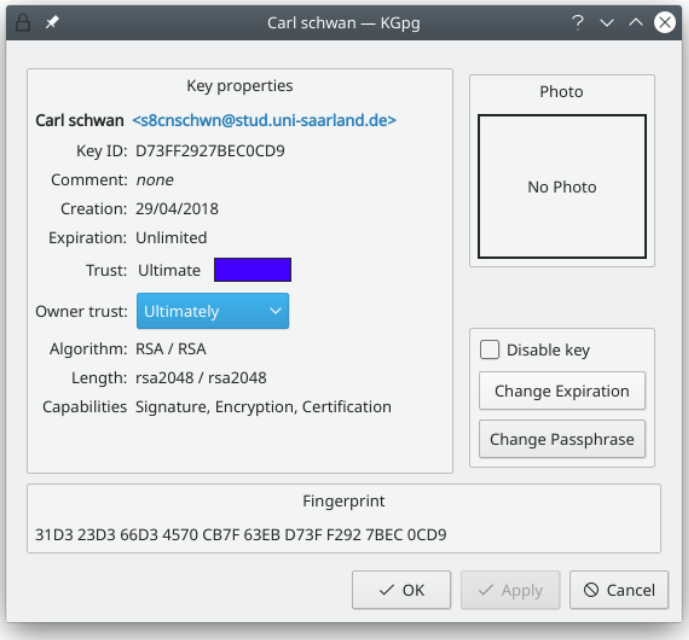
3.5.1 Gestor de Chaves



Neste exemplo, pode ver um grupo de chaves que contém duas chaves, dois pares de chaves e três chaves públicas. A terceira coluna mostra a confiança que deposita nas chaves. O primeiro par de chaves tem a confiança máxima e também está definido como chave predefinida (a negrito), enquanto o segundo expirou. Duas das chaves públicas são de completa confiança e a confiança da última chave é marginal. A última chave é expandida, mostrando a sua sub-chave ElGamal, um ID de utilizador adicional, ambos com confiança marginal, e algumas das suas assinaturas.

As assinaturas permitem navegar pelo seu porta-chaves. Se fizer duplo-click sobre uma assinatura ou uma chave que apareça como membro de um grupo, irá saltar directamente para a chave primária correspondente.

3.5.2 Propriedades da chave



Enquanto o gestor de chaves lhe permite fazer acções genéricas com uma ou várias chaves, grupos de chaves ou assinaturas, a janela de propriedades da chave dá-lhe acesso a uma única chave. Poderá aceder a ela se carregar em Enter no gestor de chaves ou se fizer duplo-click na chave.

Nesta janela, poderá modificar a frase-senha e o prazo de validade das suas chaves privadas. Também pode definir para todas as chaves o valor de confiança do dono.

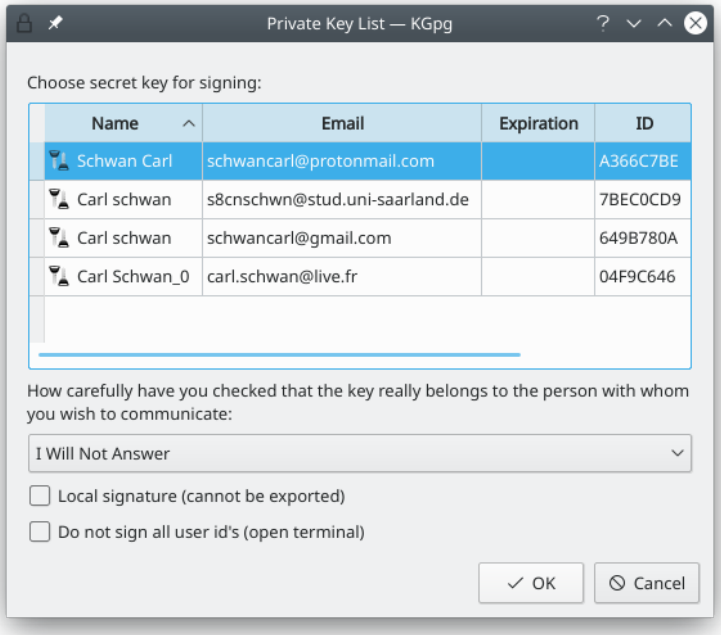
Este valor indica quanto é que confia no dono desta chave, para verificar correctamente a identidade das chaves que ele assina. Ao ter a confiança do dono em conta, o 'gpg' cria a sua própria cadeia de confiança. Você confia nas chaves que assinou. Se atribuir a confiança do dono a essas pessoas, irá confiar também nas chaves que eles assinaram, sem ter a necessidade de assinar também as chaves deles.

3.5.3 Assinar as chaves

Quando assinar a chave de outra pessoa qualquer (vamos assumir que é Alice), você está a anunciar que tem a certeza que esta chave pertence a essa pessoa e que a chave dela é de confiança. Obviamente, já poderá ter verificado isso anteriormente. Isto normalmente significa que terá de se encontrar com a Alice, verificar pelo menos um documento de identificação dela e obter a 'impressão digital' completa da chave dela ou até uma cópia da mesma. Depois, poderá ir para casa e assinar essa chave. Geralmente, irá depois enviar essa chave acabada de assinar para um servidor de chaves, para que toda a gente saiba que verificou essa chave e que o dono dela é de confiança. A Alice provavelmente irá fazer o mesmo, pelo que irão ficar ambos com as vossas chaves assinadas pela outra pessoa. Se um de vocês não tiver um documento de identificação, não será problema caso só exista a assinatura num sentido.

Mas pense no que aconteceria se a Alice vivesse do outro lado do mundo. Você comunica com ela regularmente, mas não existe a hipótese de a ver em breve. Como é que poderá confiar na sua chave?

Quando seleccionar a chave dela e depois escolher a opção **Assinar a Chave...**, irá obter uma janela que lhe permite definir como é que gostaria de assinar essa chave.



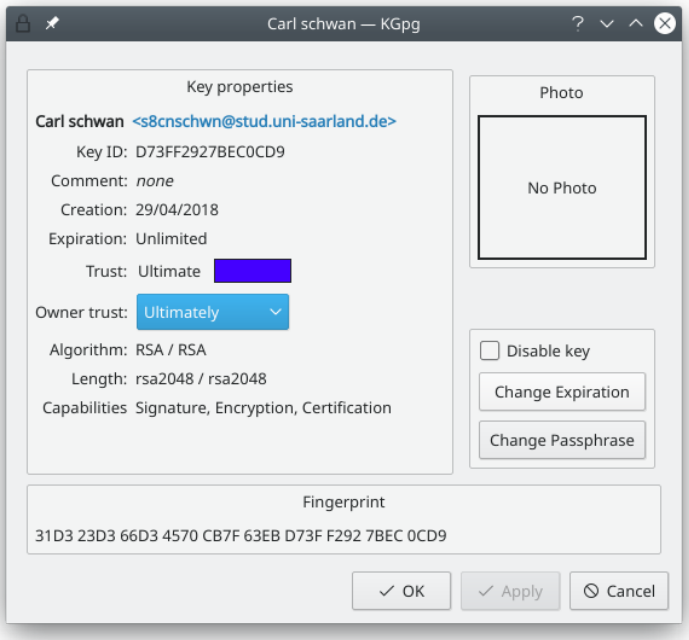
Primeiro poderá escolher a chave que irá usar para assinar a outra chave. Depois, poderá indicar com que cuidado é que verificou que a outra pessoa é de facto quem diz. Essa informação ficará guardada em conjunto com a assinatura, pelo que é uma indicação para todos os outros que possam necessitar dessa assinatura (veremos mais sobre isso em baixo). Depois vem a opção que o irá ajudar, caso não consiga encontrar-se com a Alice em pessoa **Assinatura local (não pode ser exportada)**. Quando activar esta opção, será criada uma versão especial da assinatura que nunca irá sair, mesmo por acidente, do seu porta-chaves local.

Mas porque é que é importante que tenha verificado a identidade da Alice? Quem é que se deverá importar? Existe uma outra forma de resolver o seu problema com a identidade da Alice. Se não for visitar a Alice tão cedo, poderá pensar no Pedro. Assumimos que sabe que o Pedro tem também um porta-chaves. Se souber que o Pedro é um viajante, estando em diferentes continentes duas vezes por mês, se souber que ele irá para algum sítio próximo da Alice em breve. Por isso, poderá ir ter com o Pedro para assinar as chaves. Depois, poderá deixar uma nota à Alice a avisar que o Pedro irá estar com ela em breve e perguntar-lhe se ela poderá ir ter com ele para assinar as chaves. Depois de tudo isso ter acontecido, saberá que a chave do Pedro será de confiança e o Pedro também saberá que a chave da Alice será também fidedigna. Se confiar no Pedro em que ele verificou cuidadosamente a identidade da Alice, poderá então também confiar na chave dela.

Estas relações entre as chaves e os seus donos são o que se chama normalmente de 'cadeia de confiança'. Dentro dessa cadeia, existem alguns valores importantes que definem quão fidedigna uma dada chave é. A primeira coisa é saber com que cuidado foi verificada a identidade do dono da chave. Esse é o valor que viu acima na janela de selecção da chave privada. Por exemplo, poderá saber como verificar o bilhete de identidade do seu país local mas, num país completamente diferente, isso poderá ser mais difícil. Por isso, poderá ter dito que verificou com cuidado a identidade do Pedro, porque viu o bilhete de identidade dele e se parecia muito com o seu. Mas o Pedro, ainda que ele tenha visto o bilhete de identidade e a carta de condução da Alice, poderá dizer que apenas fez uma verificação casual da identidade dela, dado não confiar em absoluto na documentação dessa parte do mundo.

O valor importante a seguir é quanto é que confia na outra pessoa para verificar os documentos. Você sabe que o Pedro é bom nisso. Mas o Jorge, por exemplo, não é uma pessoa que consideraria inteligente. Ele mal olhou para o seu bilhete de identidade quando o encontrou pessoalmente para assinar as chaves. Poderá ter a certeza que o Jorge é a pessoa que diz ser quando você verificou os documentos dele com cuidado. O problema é que ele não parece realmente querer

saber se verifica com cuidado as outras pessoas, pelo que poderá ter uma confiança elevada na chave do Jorge, mas uma confiança muito baixa nas assinaturas feitas por ele. Se abrir as propriedades da chave do Jorge, irá encontrar o campo de **Confiança do Dono**. Aqui é onde poderá definir o grau de confiança que tem no dono da chave, quando ele assina chaves de outros. Este valor não será exportado, pelo que será apenas da sua preferência pessoal.



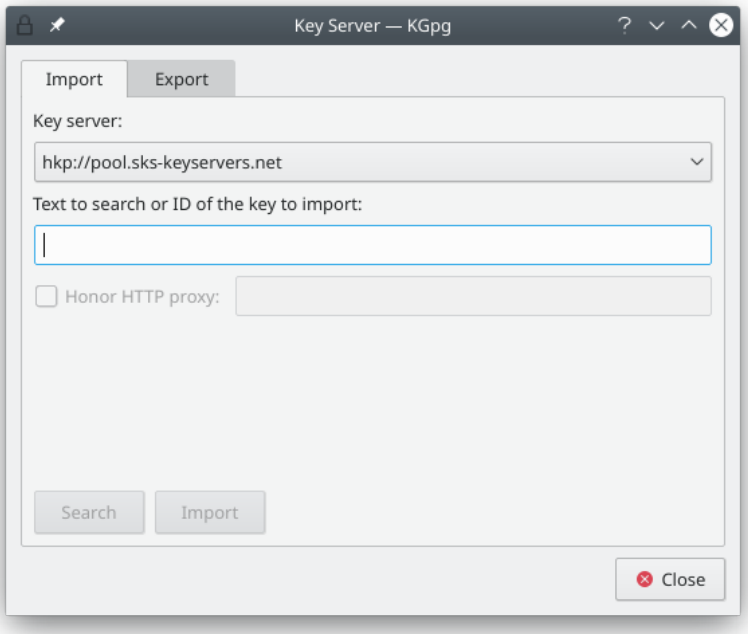
Agora deverá ter uma ideia de como é formada a cadeia de confiança, para que servem os valores de confiança do dono e da chave, e porque é terá de ser bastante cuidadoso ao verificar as identidades: outras pessoas poderão confiar em si. Contudo, existe ainda um elemento por verificar no processo: os endereços de e-mail nas chaves que assinou. A ideia de criar um novo utilizador na sua chave, com o endereço de e-mail da Alice e do Pedro só irá levar mais alguns botões de rato. O Pedro já verificou isso com a sua própria chave. Mas ninguém verificou até agora que você realmente controla os endereços de e-mail das suas identidades de utilizador.

Se escolher a opção **Assinar e Enviar o ID de Utilizador por E-Mail...** no menu, poderá eliminar essa lacuna. A ideia é que irá assinar a sua chave, como de costume e depois a mesma será em dividida em pedaços. Cada pedaço só irá conter uma identidade de utilizador da chave do Pedro e a sua assinatura para a mesma. Esta será encriptada com a chave do Pedro e enviada apenas para o endereço de e-mail indicado nessa identidade. Só se o Pedro conseguir receber este correio e descodificar a mensagem é que conseguir importar essa assinatura para o seu porta-chaves. Você não irá enviar as suas assinaturas; isso será apenas a respeito dele. Se a sua assinatura for aparecer num servidor de chaves, poderá ter a certeza que o Pedro tanto controla a chave dele como o endereço de e-mail que você assinou.

3.6 Lidar com os servidores de chaves

3.6.1 Comunicação com os servidores de chaves

A parte pública de um par de chaves normalmente é guardada num servidor de chaves. Estes servidores permitem a toda a gente procurar por uma chave que pertença a uma dada pessoa ou endereço de e-mail. As assinaturas também são guardadas nestes servidores.

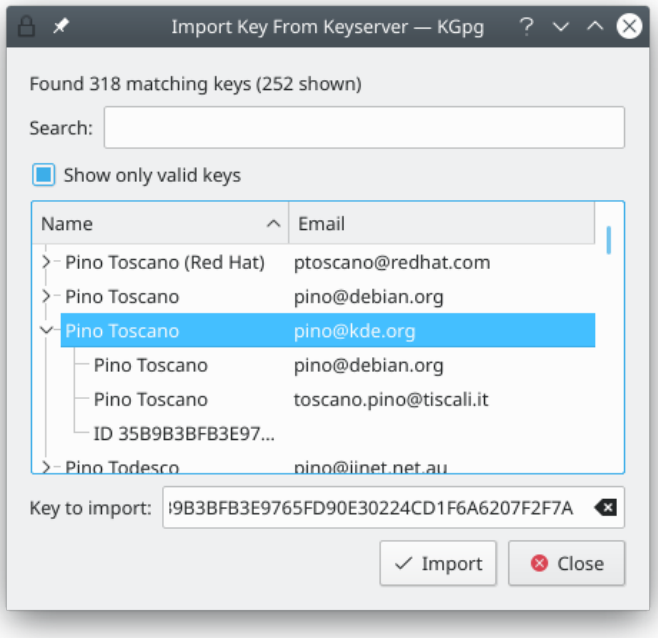


Esta janela dá-lhe acesso aos servidores de chaves. Poderá procurar e importar chaves a partir de um servidor de chaves, assim como exportar as suas chaves para um servidor. Um exemplo de pesquisa e importação acontece quando tenta escrever um e-mail para alguém novo. Se quiser encriptar a sua mensagem para o seu contacto, poderá procurar se ele ou ela tem uma chave nos servidores de chaves. Se tiver criado um novo par de chaves ou tiver assinado a chave de outra pessoa, poderá querer exportar a chave pública (possivelmente com assinaturas novas) para um servidor de chaves.

A maioria dos servidores de chaves sincroniza os seus dados entre si, pelo que poderá obter resultados semelhantes, independentemente do servidor que usar. Dado que existem excepções a esta regra, poderá escolher o servidor de chaves a usar nesta janela. Normalmente é uma boa ideia escolher um servidor predefinido que esteja localizado perto de si (p.ex. no seu país ou no seu continente), dado que estes respondem normalmente mais depressa às suas pesquisas.

Lembre-se que tudo o que enviar para um servidor de chaves normalmente ficará por lá. Esta é uma razão pela qual deverá normalmente limitar o tempo de validade das suas chaves. Lembre-se também que os servidores de chaves são algumas vezes analisados pelos geradores de lixo electrónico para obter endereços de e-mail.

3.6.2 Resultados da pesquisa no servidor de chaves



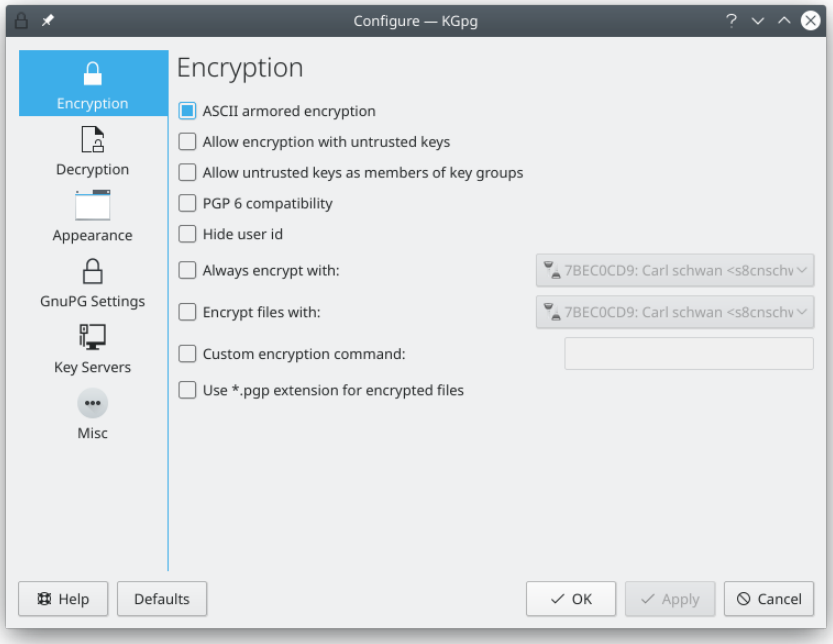
Todos os resultados de uma pesquisa são apresentados nesta janela. Esta imagem mostra uma pesquisa por endereços ˝@kde.org˝ que originaram 244 resultados. Se usar o campo de pesquisa, a lista apresentada foi reduzida a uma única chave. Esta chave tem duas correspondências: o ID do utilizador primário corresponde ao texto da pesquisa, assim como um dos outros ID's do utilizador.

Poderá seleccionar uma ou mais chaves a importar. Os ID's dessas chaves aparecem no campo de **Chaves a importar**, no fundo da janela. Quando carregar em **Importar**, o servidor de chaves será contactado de novo e as chaves serão obtidas para o seu porta-chaves.

3.7 Configurar o KGpg

A configuração está acessível através do menu da 'applet' do KGpg (se carregar com o botão direito do rato na 'applet') ou através do menu principal (**Configuração** → **Configurar o KGpg**). Poderá definir os parâmetros por omissão para a encriptação, a descodificação, a interface do utilizador e a 'applet'. A maioria das opções de encriptação estão relacionadas directamente com o gpg e estão documentadas na sua página do 'man'.

3.7.1 Encriptação



Aqui poderá configurar opções especiais a passar ao GnuPG, para mudar o comportamento da encriptação. Para uma descrição mais detalhada, dê uma vista de olhos no manual do GnuPG.

- **Encriptação ASCII armada**: isto faz com que os ficheiros encriptados fiquem guardados num formato que só use caracteres visíveis do ASCII e tenha linhas curtas. Os ficheiros guardados desta forma são maiores que os ficheiros em binário, mas são mais simples de enviar isto é por e-mail.
- **Permitir cifra com chaves não-fidedignas**: esta opção permite-lhe encriptar os ficheiros com chaves nas quais não confia.
- **Compatibilidade com o PGP 6**: os ficheiros encriptados são compatíveis com a norma antiga do PGP6. Esta desactiva certas funcionalidades; como tal, só a deverá usar se for realmente necessário.
- **Esconder o ID do utilizador**: esta opção remove todos os vestígios do destinatário no ficheiro encriptado. No caso de a transmissão ser interceptada, ninguém poderá obter informações sobre o destinatário a partir do ficheiro. Se este destinatário tiver várias chaves, terá de experimentar para saber qual foi usada.
- **Encriptar sempre com**: todas as encriptações são encriptadas adicionalmente com esta chave. Se configurar esta opção com uma das suas chaves privadas, isto garante que você poderá ler sempre todos os dados encriptados por si, com o custo de mensagens maiores.
- **Encriptar os ficheiros com**: comporta-se como o **Encriptar sempre como** para a encriptação de ficheiros.
- **Comando de encriptação personalizado**: se necessitar de passar algumas opções pouco usuais ao GnuPG, poderá indicar a linha de comandos aqui. A maioria dos utilizadores não irá necessitar disto.
- **Usar a extensão *.pgp para os ficheiros encriptados**: se assinalar esta opção, os ficheiros encriptados terão adicionada ao seu nome a extensão `.pgp`; caso contrário, é utilizada a extensão `.gpg`.

3.7.2 Descodificação

Aqui poderá indicar um comando de descodificação personalizado. Esta opção raramente é usada, e só é útil para os utilizadores avançados que conheçam as opções da linha de comandos.

3.7.3 Aparência

Aqui poderá configurar a forma como lhe aparece o KGpg. As opções possíveis são as cores que reflectem os diferentes níveis de confiança nas chaves do gestor de chaves e a configuração dos tipos de letra do editor.

3.7.4 Configuração do GnuPG

Aqui poderá configurar o executável do 'gpg' e o **ficheiro de configuração** e pasta pessoal a utilizar. Estes valores são detectados automaticamente no primeiro arranque e deverão funcionar logo à partida.

A utilização do agente do GnuPG torna mais confortável o trabalho com o GnuPG, dado que não necessita de escrever a sua senha para todas as acções. Fica guardada numa 'cache' em memória durante algum tempo, de modo que todas as operações que pudessem necessitar de uma senha possam ser feitas imediatamente. Lembre-se que isto poderá permitir às outras pessoas usarem as suas chaves privadas, caso deixe a sua sessão acessível para elas.

3.7.5 Servidores de Chaves

Aqui poderá criar uma lista dos servidores de chaves conhecidos por si quando abrir a janela do servidor de chaves. Se executar o GnuPG a partir da linha de comandos, somente será usado o servidor de chaves que definir por omissão aqui.

O protocolo usado para a comunicação com os servidores de chaves baseia-se em HTTP, por isso fará sentido, em alguns ambientes que se possa **honrar o 'proxy' de HTTP quando disponível**.

3.7.6 Diversos

Esta secção permite a configuração de algumas funcionalidades que não se encaixam noutras secções. Poderá configurar, por exemplo, para **iniciar o KGpg automaticamente no arranque**. A opção **usar a selecção do rato em vez da área de transferência** altera se as selecções são feitas através do botão do meio do rato ou se são feitas por combinações de teclas.

Poderá também alterar se o ícone da bandeja do KGpg aparece ou não e o que acontece se o ícone for seleccionado através do botão esquerdo do rato. Se a 'applet' aparecer, ao fechar, a janela do KGpg irá minimizar a aplicação para a bandeja. Se o ícone não aparecer, o KGpg irá sair quando fechar todas as janelas.

Capítulo 4

Créditos e Licença

KGpg

Tradução de José Nuno Pires zepires@gmail.com