Manuel de KGpg

Jean-Baptiste Mardelle
Rolf Eike Beer
Traduction française : Damien Raude-Morvan
Traduction française : Xavier Besnard

Manuel de KGpg

Table des matières

Résumé

KGpg est une interface graphique simple pour GnuPG ((http://gnupg.org)).

Chapitre 1

Introduction

KGpg est une interface graphique basique pour GnuPG, un outil de chiffrement puissant. GnuPG (aussi connu sous le nom de « gpg ») est inclus dans la plupart des distributions et est probablement installé sur votre système. Vous pouvez obtenir la dernière version sur https://gnupg.org.

Avec KGpg, vous pourrez chiffrer et déchiffrer vos fichiers ou vos courriers électroniques, offrant ainsi des communications plus sécurisées. Un petit guide sur le chiffrement avec « gpg » est disponible sur le site Internet de GnuPG.

Avec KGpg, vous n'avez pas besoin de connaître les lignes de commandes et les options du programme gpg. Tout ou presque peut être réalisé en quelques clics de souris.

Chapitre 2

Premiers pas

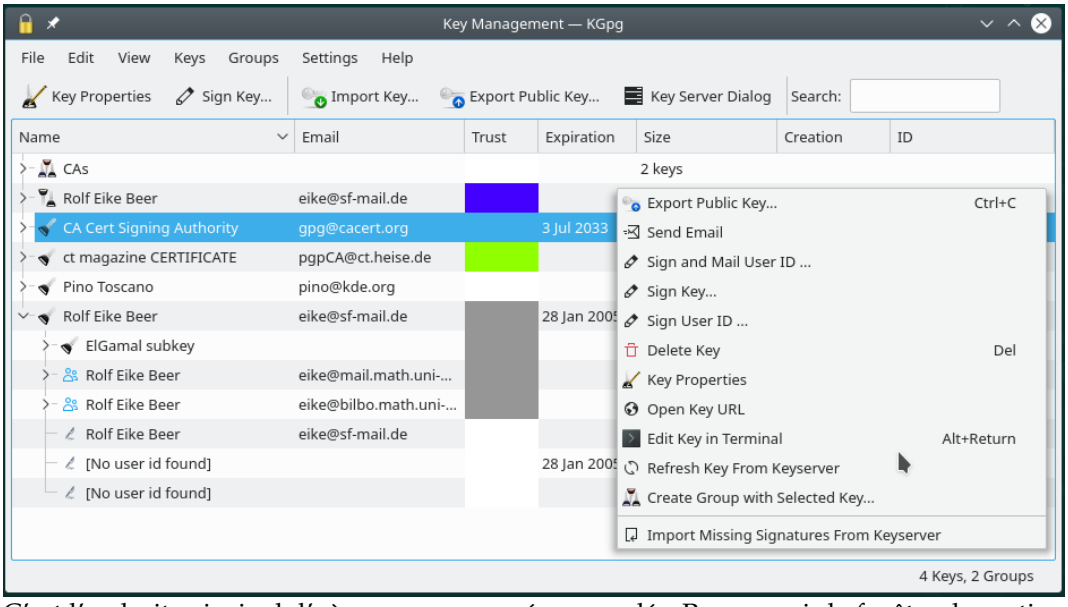
Voici une liste des composants principaux de KGpg :

Icône de la barre des tâches

Quand vous démarrez KGpg, une icône apparaît dans la barre des tâches. Un clic avec le bouton gauche de la souris ouvre la fenêtre de gestion des clés, alors qu'un clic avec le bouton droit de la souris affiche un menu permettant un accès rapide aux fonctions importantes. Vous pouvez aussi glisser-déposer des fichiers ou du texte sur l'icône de l'applet pour les chiffrer ou les déchiffrer.

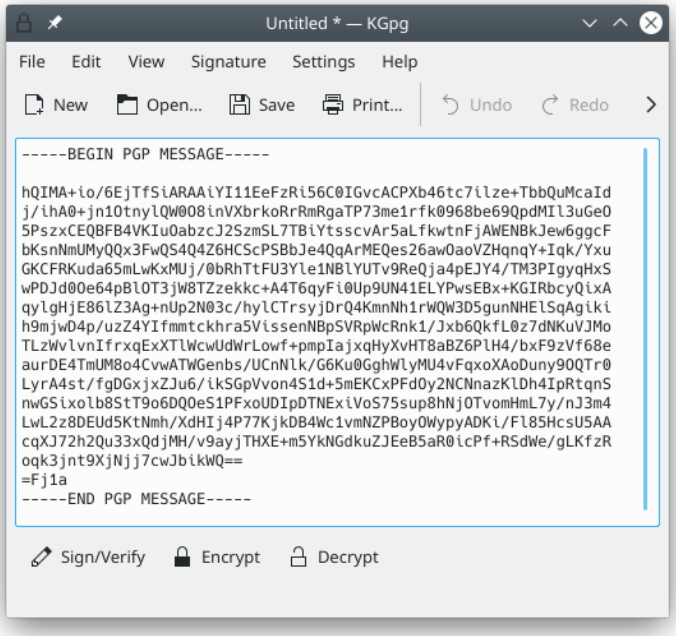
Veuillez noter que l'icône dans la barre de tâches est indiquée comme ˝inactive˝ comme la plupart du temps. Puisque l'applet de la barre de tâches cachera généralement les icônes inactives, KGpg ne sera affiché que si vous le demandez explicitement. Pour plus de détails, veuillez regarder la documentation de Plasma.

Fenêtre de gestion des clés



C'est l'endroit principal d'où vous pouvez gérer vos clés. Pour ouvrir la fenêtre de gestion des clés, un clic avec le bouton gauche de la souris sur l'applet KGpg suffit. Vous pouvez importer, exporter, signer et éditer vos clés. La plupart des actions peuvent être effectuées avec un clic du bouton gauche de la souris sur une clé.

Fenêtre d'édition



C'est un éditeur de texte simpliste, où vous pouvez saisir ou coller votre texte pour le chiffrer / déchiffrer. Pour ouvrir l'éditeur, un clic avec le bouton droit de la souris sur l'applet KGpg suffit.

Intégration dans le gestionnaire de fichiers

KGpg est intégré à Konqueror et à Dolphin. Cela signifie que quand vous effectuez un clic sur un fichier, vous pouvez choisir **Actions** → **Chiffrer le fichier** pour chiffrer le fichier. Vous pouvez également déchiffrer un fichier avec un clic du bouton droit de la souris.

Chapitre 3

Utilisation de KGpg

Il y a deux manières de chiffrer vos données :

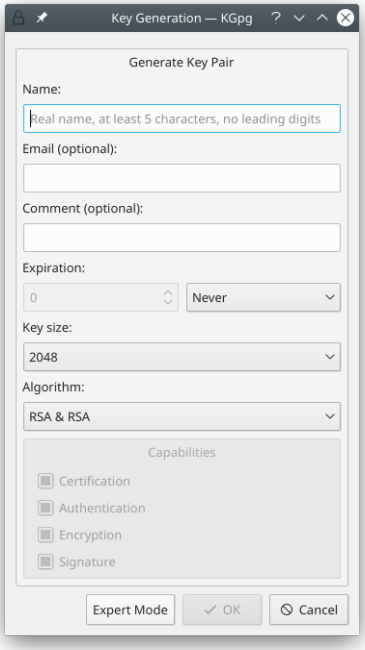
— Chiffrement symétrique : vos données sont juste chiffrées avec un mot de passe. N'importe qui, avec un ordinateur et Gnupg, peut déchiffrer votre message si vous lui fournissez le mot de passe. Pour utiliser un chiffrement symétrique, choisissez « chiffrement symétrique » dans la liste des options quand vous devez choisir une clé de chiffrement.

— Chiffrement par clé publique (ou asymétrique) : vous devez d'abord créer votre paire de clés (clé publique et clé privée) et définir votre mot de passe. Conservez votre clé privée dans un endroit sûr, et échangez votre clé publique avec vos amis. Ensuite, si vous voulez envoyer un message chiffré à Alex, vous devez chiffrer ce message avec la clé publique d'Alex. Pour déchiffrer le message, le destinataire (sûrement Alex) aura besoin de la clé privée d'Alex et de son mot de passe.

Le chiffrement par clé publique est un peu plus compliqué (vous devez échanger vos clés avec vos amis).mais il est plus sûr. Rappelez-vous que si vous chiffrez un message avec la clé publique de quelqu'un d'autre, vous ne pourrez pas le déchiffrer ! Vous pouvez uniquement déchiffrer les messages qui ont été chiffrés avec votre clé publique.

3.1 Générer une clé

Si vous n'avez pas de clé, KGpg affichera automatiquement la fenêtre de génération au premier démarrage. Vous pouvez aussi y avoir accès depuis la fenêtre de gestion des clés avec **Clés** → **Générer une paire de clés**.



Donnez simplement votre nom, votre adresse électronique et cliquez sur le bouton **Ok**. Cela générera votre paire de clés gpg standard. Si vous voulez plus d'options, vous pouvez cliquer que le bouton mode expert, qui affichera une fenêtre de Konsole avec toutes les options de Gnupg.

De nombreuses personnes jouent avec leurs premières clés, génèrent de mauvais identifiants d'utilisateur, ajoutent des commentaires qu'ils regrettent plus tard ou tout simplement oublient leurs mots de passe. Pour éviter que de telles clés restent valables pour toujours, une bonne idée est de limiter leurs durées de vie à 12 mois par exemple. Vous pouvez modifier la durée de vie de vos clés secrètes plus tard en utilisant la fenêtre de propriétés des clés.

3.2 Révoquer une clé

Une paire de clés ayant expiré peut être remise dans un état opérationnel tant que vous avez accès à la clé privée et au mot de passe. Pour rendre une clé inutilisable de façon sûre, vous devez la révoquer. La révocation est réalisée en ajoutant une signature de révocation à la clé.

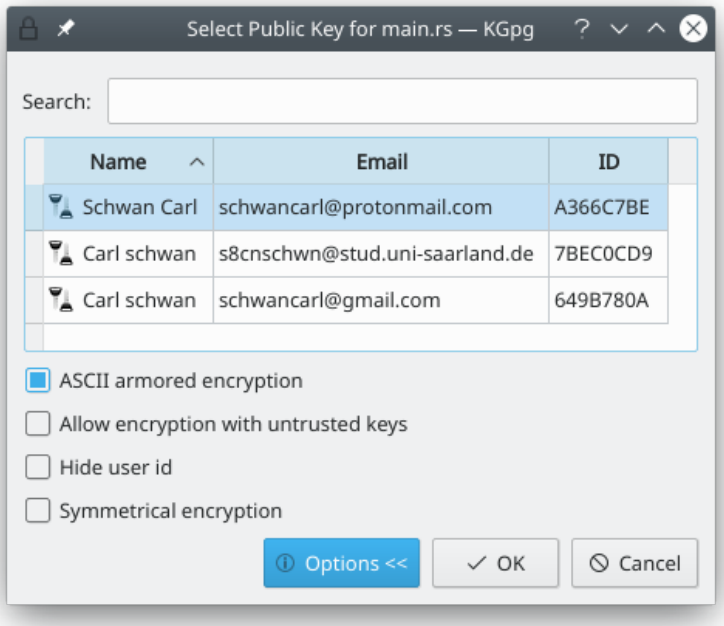
La signature de révocation peut être créée en même temps que la clé. Dans ce cas, elle est stockée dans un fichier à part. Ce fichier peut être importé plus tard dans le trousseau de clés et est alors attaché à la clé pour la rendre inutilisable. Veuillez noter qu'aucun mot de passe n'est demandé pour importer la signature vers la clé. Cependant, vous devriez stocker la signature de révocation dans un endroit sûr, généralement, à un endroit différent de celui de votre paire de clés. Un bon conseil : utiliser un endroit en dehors de votre ordinateur, soit en la stockant sur un périphérique de stockage externe tel qu'un clé USB ou en l'imprimant.

Si vous n'avez pas produit une révocation séparée lors de la création de la clé, vous pouvez créer cette signature de révocation à n'importe quel moment en sélectionnant **Clés** → **Révocation de la clé**, avec en option, son importation immédiate dans votre trousseau de clés.

3.3 Chiffrer vos données

3.3.1 Chiffrer un fichier depuis Konqueror ou Dolphin

Cliquez sur le fichier à chiffrer avec le bouton droit de la souris. Choisissez **Actions** → **Chiffrer le fichier** dans le menu contextuel. KGpg affiche ensuite la fenêtre de sélection de la clé publique. Choisissez la clé publique de votre destinataire. Cliquez sur **Chiffrer**. Le fichier chiffré sera enregistré avec l'extension `.asc` ou `.gpg` suivant si vous choisissez le chiffrement blindé ASCII ou non.



3.3.2 Chiffrer un texte avec l'applet KGpg

Vous pouvez chiffrer les contenus du presse-papier en sélectionnant l'élément **Chiffrer le presse-papier** dans l'applet de menu. Quand vous choisissez **Signer le presse-papier**, le texte ne sera alors que signé. Les deux actions importeront les contenus courants du presse-papier dans une fenêtre d'éditeur, réaliseront l'action demandée et copieront en retour les contenus dans l'éditeur.

3.3.3 Chiffrer du texte depuis l'éditeur de KGpg

C'est aussi simple que de cliquer sur le bouton **Chiffrer**. La fenêtre de sélection de clés s'affichera pour sélectionner la clé publique. Choisissez une clé et cliquez sur **Ok**. Le message chiffré apparaît alors dans la fenêtre de l'éditeur.

Généralement, vous ne pouvez chiffrer des fichiers qu'avec des clés dans lesquelles vous avez confiance. Quelquefois, quand vous ne voulez qu'envoyer une note confidentielle à une personne au hasard mais que vous savez posséder une clé GPG, vous pouvez utiliser l'option **Autoriser le chiffrement avec des clés non de confiance**.

Pour être sûr que vous pouvez déchiffrer tout fichier que vous avez chiffré, même si vous avez chiffré avec un clé de quelqu'un d'autre, vous pouvez utiliser les options **Toujours chiffrer avec** et **Chiffrer les fichiers avec** qui sont disponibles dans la Configuration de KGpg.

Pour plus d'informations sur les options de chiffrement, notamment "le blindage ASCII", "l'autorisation du chiffrement avec des clés non sûres" et "le chiffrement symétrique", référez-vous à la documentation de gpg ou aux pages man.

3.4 Déchiffrer vos données

3.4.1 Déchiffrer un fichier depuis Konqueror ou Dolphin

Cliquez avec le bouton gauche sur le fichier à déchiffrer. Donnez votre mot de passe, et il sera déchiffré. Vous pouvez aussi glisser-déposer un fichier texte chiffré dans l'éditeur de KGpg. Il vous demande votre mot de passe, puis affiche le texte déchiffré dans l'éditeur. Vous pouvez même déposer des fichiers distants ! Vous pouvez aussi utiliser le menu **Fichier** → **Déchiffrer un fichier...**, puis choisir le fichier à déchiffrer.

3.4.2 Déchiffrer un texte avec l'applet de KGpg

Vous pouvez aussi déchiffrer les contenus du presse-papier avec l'entrée de menu **Déchiffrer le presse-papier** du composant graphique de KGpg. Le texte déchiffré apparaîtra dans une fenêtre d'édition.

3.4.3 Déchiffrer un texte avec l'éditeur

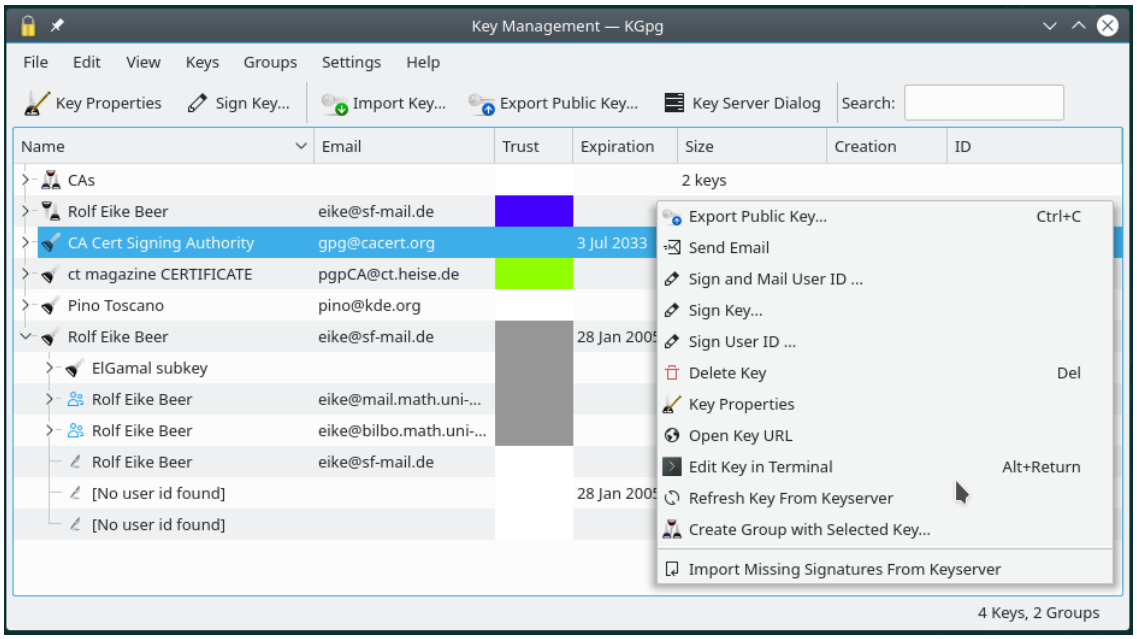
Copiez ou glissez-déposez le texte que vous voulez déchiffrer, puis cliquez sur le bouton **Déchiffrer**. Le mot de passe vous sera demandé.

3.5 Gestion des clés

Toutes les fonctions basiques de gestion des clés peuvent être effectuées avec KGpg. Pour ouvrir la fenêtre de gestion des clés, cliquez avec le bouton gauche de la souris sur l'applet KGpg. La plupart des options sont accessibles d'un clic droit sur la clé. Pour importer / exporter des clés publiques, vous pouvez utiliser le glisser-déposer ou les raccourcis clavier du copier-coller.

Vous pouvez exporter une clé publique par courriel vers le presse-papier, vers un serveur de clés ou un fichier local. Utiliser les options dans une boîte de dialogue d'exportation pour tout exporter, exporter sans attributs (photo d'identité) ou exporter une nouvelle clé, c'est-à-dire, la clé elle-même, y compris les sous-clés mais sans toutes les signatures.

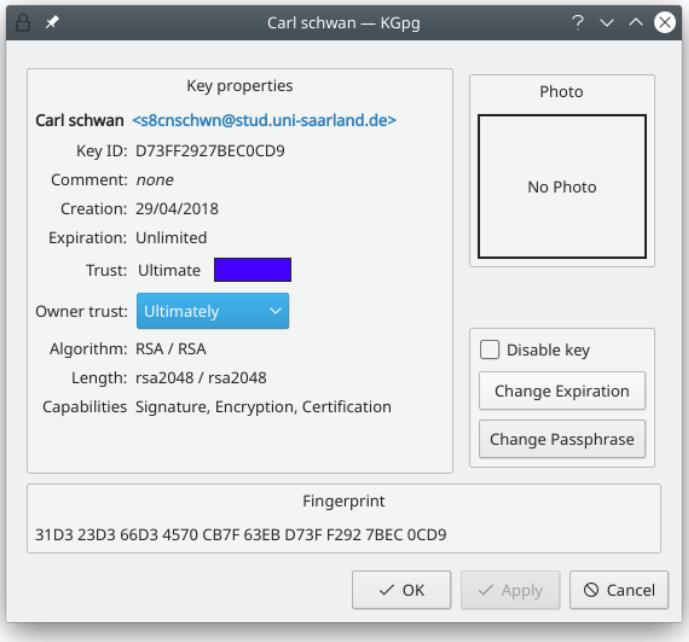
3.5.1 Gestion des clés



Cet exemple vous présente un groupe de clé contenant deux clés, deux paires de clés et trois clés publiques. La troisième colonne montre le niveau de confiance que vous avez dans les clés. La première paire est parfaitement de confiance et est aussi définie comme clé par défaut (en gras). La deuxième clé a expiré. Deux des clés publiques sont parfaitement de confiance alors que la confiance dans la dernière clé est limitée. La dernière clé est développée, montrant sa sous-clé ElGamal, un identifiant additionnel d'utilisateur mais avec un niveau de confiance limité pour les deux et quelques unes de ses signatures.

Les signatures vous permettent de naviguer dans le trousseau de clés. Un double clic sur une signature ou sur une une clé affichée comme membre du groupe, vous permettra d'accéder directement à la clé primaire correspondante.

3.5.2 Propriétés des clés



Alors que le gestionnaire de clés vous permet de réaliser des actions générales avec une ou plusieurs clés, groupes de clés ou signatures, la fenêtre des propriétés de clés vous donne accès à une unique clé. Vous pouvez l'atteindre en appuyant sur « Entrée » dans le gestionnaire de clé ou en double cliquant sur la clé.

Dans cette fenêtre, vous pouvez aussi modifier votre mot de passe et votre date d'expiration de clé pour vos clés secrètes. Pour toutes les clés, vous pouvez aussi fixer une valeur de confiance envers le propriétaire.

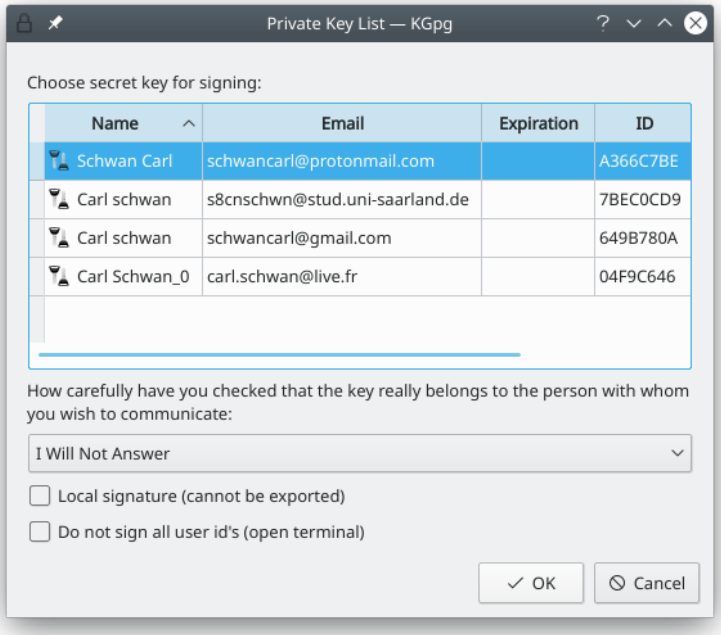
Cette valeur indique le niveau de confiance que vous avez dans le propriétaire de la clé lors de la vérification d'identité des clés qu'il a signées. Prendre en compte la confiance du propriétaire permet à gpg de créer votre propre web de confiance.

3.5.3 Signer des clés

Quand vous signez la clé de quelqu'un d'autre (Par exemple, Alice), vous annoncez que vous êtes sûr que cette clé lui appartient vraiment et que cette clé est de confiance. Bien sûr, vous devriez avoir réellement vérifié cela. Cela veut dire, en général, que vous avez rencontré Alice, que vous avez vérifié au moins une pièce d'identité et que vous avez pris une empreinte complète de la clé ou une copie de sa clé. Alors, vous pouvez rentrer chez vous et signer cette clé. Généralement, vous chargerez plus tard la clé récemment signée vers un serveur de clés. Ainsi, chacun pourra savoir que vous avez vérifié que la clé et son propriétaire sont dignes de confiance. Alice fera probablement la même chose et chacun des deux aura ses clés signées par l'autre. Si l'un n'a pas de pièce d'identité disponible, ce n'est pas un problème mais la signature ne se fera que dans une seule direction.

Mais, pensons à ce qui se passerait si Alice vivait de l'autre coté du monde ? Vous communiquez avec elle régulièrement mais il y a peu de chance de la voir à court terme. Comment pouvez vous avoir confiance dans sa clé ?

Quand vous sélectionnez sa clé puis ensuite vous choisissez **Signer la clé...** , vous verrez apparaître une boîte de dialogue. Celle-ci vous permettra de choisir les options sur comment vous aimeriez signer cette clé.



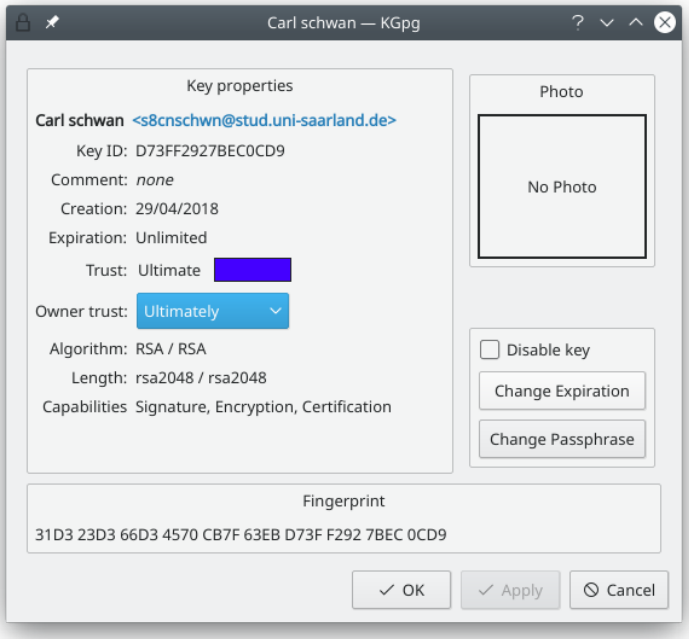
D'abord, vous pouvez choisir la clé que vous voulez utiliser pour signer la clé. Ensuite, vous pouvez saisir avec quelle attention vous avez vérifié qu'elle est bien la personne qu'elle prétend être. Cette information sera stockée avec la signature (Plus de détails ci-dessous). Enfin, voici l'option qui vous aidera si vous ne pouvez rencontrer Alice en personne : **Signature locale (ne peux pas être exportée)**. Quand vous activez cette option, une version spéciale d'une signature sera créée, impossible à perdre dans votre trousseau de clés, même par accident.

Mais, pourquoi est-il si important de savoir avec quel soin vous avez vérifié l'identité d'Alice ? Qui s'en préoccupe ? Il y a une façon différente de résoudre votre problème avec l'identité d'Alice. Si vous ne pouvez rendre visite à Alice à court terme, pensez juste à Trent. Vous savez que Trent possède aussi une paire de clés. Trent est un grand voyageur, changeant de continent au moins deux fois par mois. Avec de la chance, il sera de passage près de chez Alice. Ainsi, vous pouvez voir Trent et le rencontrer pour signer des clés. Vous envoyez un message à Alice pour lui dire que Trent sera bientôt près de chez elle et pour lui demander si elle peut le rencontrer pour signer les clés. Après que tout cela se soit passé, vous savez que vous pouvez avoir confiance dans les clés de Trent et que Trent savait qu'il peut avoir confiance dans les clés d'Alice. Si vous avez confiance dans Trent pour avoir vérifié avec soin l'identité d'Alice, alors, vous pouvez ainsi avoir confiance dans la clé d'Alice.

Ces relations entre clés et propriétaires forment ce qui est dénommé un web de confiance. Dans ce web de confiance, il y a d'importantes valeurs qui définissent le niveau de confiance associé à une clé. La première chose concerne le soin avec lequel l'identité du propriétaire de la clé a été vérifiée. Cette valeur a été affichée ci-dessus dans la fenêtre de sélection de clé secrète. Par exemple, vous devriez savoir comment vérifier une carte d'identité de votre pays mais une carte d'identité d'un pays complètement différent pourrait être plus difficile à vérifier. Ainsi, vous pourriez dire que vous avez vérifié avec soin la carte d'identité de Trent parce que vous l'avez vu et qu'elle ressemble fortement à la votre. Mais, Trent, bien qu'il ait vu la carte d'identité d'Alice et son permis de conduire pourrait dire qu'il a fait des vérifications basiques de son identité comme il n'est absolument pas sûr sur les documents correspondants dans cette partie du monde.

La valeur suivante importante est le niveau de confiance que vous accordez à l'autre personne pour vérifier les documents. Vous savez que Trent est bon pour cela. Mais, par exemple, George est quelqu'un que vous diriez moins recommandable. Il a regardé rapidement votre carte d'identité quand vous vous êtes rencontrés pour signer les clés. Vous êtes sûr que George est bien la personne qu'il prétend être parce que vous avec vérifié ces documents d'identité avec soin. Mais, il ne semble pas prendre beaucoup de précautions lorsqu'il vérifie d'autres personnes. Ainsi,

vous aurez une grande confiance dans la clé de George mais une faible confiance dans les signatures de George. Si vous ouvrez les propriétés d'une clé, vous trouverez le champ **Confiance dans le propriétaire**. Cela indique le niveau de confiance envers le propriétaire de la clé quand il signe des clés. Cette valeur ne sera pas exporté, cela est totalement à votre entière discrétion.



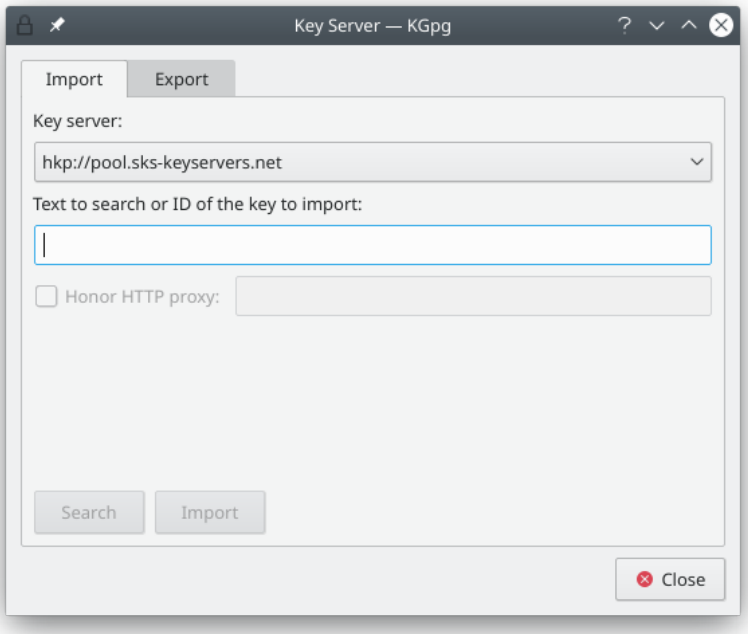
Maintenant, vous devriez avoir une idée de comment est construit une web de confiance, à quoi servent les valeurs de confiance pour un propriétaire et pour une clé et pourquoi vous devriez toujours vérifier avec beaucoup de soins les identités. Les autres personnes doivent pouvoir avoir confiance en vous. Mais, un élément dans le processus reste toujours non vérifié : les adresses de courriels dans les clés que vous avez signées. La création d'une nouvelle identité d'utilisateur dans votre clé avec l'adresse de courriel d'Alice ou de Trent prendra seulement quelques clics de souris. Vous avez vérifié que Trent est le réel propriétaire de sa clé. Mais, personne n'a vérifié jusqu'à présent que Trent maîtrise réellement les adresses de courriel de ses identités d'utilisateur.

Si vous sélectionnez **Signer et envoyer l'identifiant utilisateur...** dans le menu à la place, vous pouvez combler ce manque. L'idée est que vous signerez la clé classiquement et après, elle sera scindée en 2 morceaux. Chaque morceau ne contiendra qu'une identité d'utilisateur de la clé de Trent et sa signature. Celui-ci sera chiffré avec la clé de Trent et envoyé uniquement à l'adresse de courriel donnée dans cette identité. Seulement si Trent peut recevoir ce courriel et déchiffrer le message, alors, Trent pourra importer cette signature dans son trousseau de clés. Vous ne téléchargerez pas vos signatures, cela est entièrement à la discrétion de Trent. Si votre signature s'affiche sur un serveur de clés, vous pouvez être sûr que Trent contrôle réellement à la fois sa clé aussi bien que l'adresse de courriel que vous avez signée. Les signatures que vous avez faites dans ce processus ne feront pas partie de votre trousseau de clé. Ainsi, juste après avoir signé la clé de Trent, elle ne sera toujours pas affichée comme digne de confiance dans votre trousseau de clés. Une fois que Trent aura reçu votre courriel et importé votre signature dans son trousseau de clés, il pourra les télécharger sur un serveur de clés. Quand vous mettez à jour sa clé à partir d'un serveur de clés, vous réceptionnez les nouvelles signatures. Même si cela peut paraître peu pratique, d'abord, cela permet d'être sûr que vous ne pourrez pas voir par accident une des ses identités considérée comme de confiance mais qu'il ne contrôle pas. Seules les signatures qui sont affichées sur le serveur de clés sont celles où chacun, y compris vous, peut être sûr qu'il contrôle réellement les courriels correspondants.

3.6 Travailler avec des serveurs de clés

3.6.1 Communication avec des serveurs de clés

La partie publique de la paire de clés est généralement stockée sur un serveur de clés. Ces serveurs permettent à tout le monde de chercher un clé associée à une personne ou une adresse de courriel particulière.

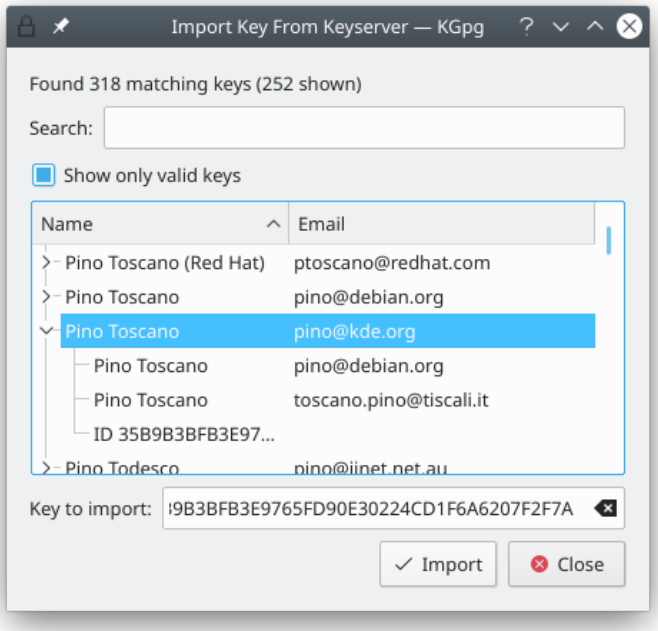


Cette boîte de dialogue vous donne accès aux serveurs de clés. Vous pouvez chercher et importer des clés d'un serveur de clés aussi bien que exporter des clés vers un serveur. Par exemple, la recherche et l'importation se font quand vous voulez écrire un courriel vers un nouveau destinataire. Si vous vouliez chiffrer votre courriel à votre contact, vous pouvez rechercher si elle ou lui a une clé publique sur les serveurs de clés. Si vous avez créé une nouvelle paire de clés ou si vous avez signé une clé de quelqu'un d'autre, vous pourriez vouloir exporter la clé publique (potentiellement avec de nouvelles signatures) vers un serveur de clés.

La plupart des serveurs de clés synchronisent leurs données entre eux. Ainsi, vous obtiendrez des résultats de recherche similaires, indépendamment du serveur utilisé. Depuis qu'il y a des exceptions à cette règle, vous pouvez choisir dans cette boîte de dialogue, le serveur de clés à utiliser. En général, la bonne solution est de choisir un serveur de clé par défaut qui est proche de vous (par exemple, dans votre pays ou dans votre continent) parce qu'il répond plus rapidement à vos requêtes.

Veuillez noter que toute chose que vous chargez dans un serveur de clé, y reste en général de façon permanente. C'est ma raison pour laquelle vous devriez généralement limiter la durée de vie de vos clés. Notez aussi que les serveurs de clés sont quelquefois analysés par des spammeurs à la recherche d'adresses de courriels.

3.6.2 Résultats de recherche d'un serveur de clés



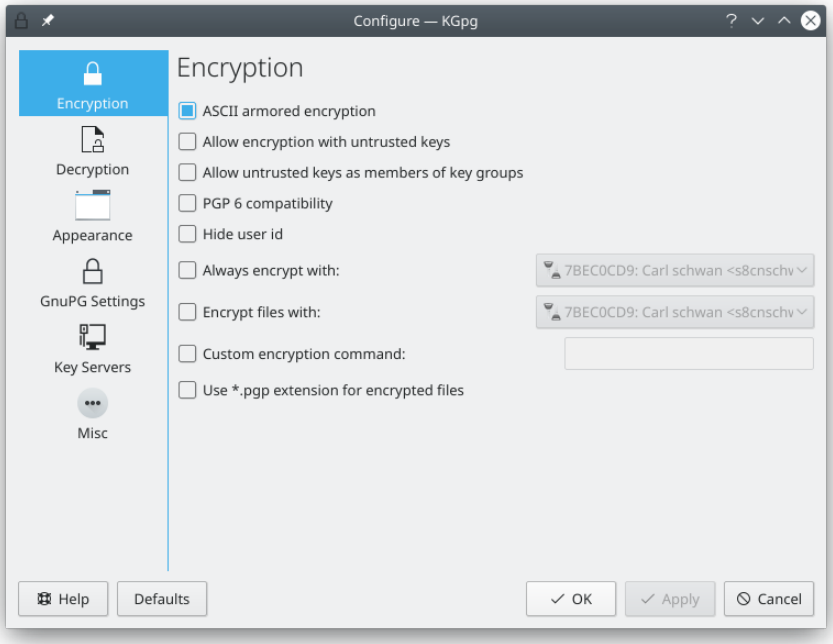
Tous les résultats d'une recherche sont affichés dans cette fenêtre. Cette figure montre une recherche pour les adresses ˝@kde.org˝, ce qui donne jusqu'à 244 résultats. En utilisant le champ de recherche, la liste affichée se réduit à une unique clé. Ce clé a deux correspondances : l'identifiant utilisateur primaire correspond à la chaîne de recherche aussi bien que l'un des autres identifiants d'utilisateur.

Vous pouvez sélectionner une ou plusieurs clés à importer. Les identifiants de ces clés sont montrés dans le champ **Clés à importer** au bas de la fenêtre. Quand vous cliquez sur **Importer**, le serveur de clé est contacté de nouveau et les clés sont rapatriées dans votre trousseau de clés.

3.7 Configurer KGpg

La configuration est accessible à partir du menu de l'applet KGpg (cliquez avec le bouton droit de la souris sur l'applet) ou par le menu principal (**Paramètres** → **Configurer KGpg**). Vous pouvez définir les paramètres par défaut pour le chiffrement, le déchiffrement, l'interface et l'applet. La plupart des options de chiffrement sont directement liées à gpg et sont documentées dans sa page man.

3.7.1 Chiffrement



Vous pouvez configurer ici des options spéciales à passer à GnuPG pour changer le comportement du chiffrement. Pour une description détaillée, veuillez consulter le manuel GnuPG.

— **Chiffrement ASCII renforcé** : cela provoque le stockage des fichiers chiffrés dans un format n'utilisant que des caractères ASCII imprimables et avec des lignes courtes. Les fichiers produits de cette façon sont plus volumineux que les fichiers en format binaire mais sont plus faciles à envoyer par exemple par courriel.

— **Permettre le chiffrement avec des clés non de confiance** : cela vous permet de chiffrer des fichiers avec des clés auxquelles vous n'accordez pas de confiance.

— **Compatibilité PGP 6** : les fichiers chiffrés sont compatibles avec l'ancien standard PGP6. Cela désactive certaines fonctionnalités mais vous ne devriez utiliser seulement ceci que si réellement nécessaire.

— **Cacher l'identifiant utilisateur** : cela enlève toute trace du destinataire venant du fichier chiffré. Dans le cas où la transmission est interceptée, personne ne pourra accéder dans le fichier, des informations sur le destinataire. Si le destinataire possède de multiples clés, il devra trouver laquelle a été utilisée.

— **Toujours chiffrer avec** : tous les chiffrements sont réalisés avec cette clé. Si vous choisissez comme paramètre, une de vos clés privées, cela vous garantit que vous pourrez lire toutes les données que vous avez chiffrées au prix de messages plus volumineux.

— **Chiffrer des fichiers avec** : se comporte comme **Toujours chiffrer avec** pour le chiffrement de fichiers.

— **Commande personnalisée de chiffrement** : si vous avez besoin de passer des options inhabituelles à GnuPG, vous pouvez spécifier la ligne de commande ici. La plupart des utilisateurs n'auront pas besoin de ceci.

— **Utiliser une extension *.pgp pour les fichiers chiffrés** : si vous activez cette option, les fichiers chiffrés seront nommés comme les fichiers d'entrée avec l'extension `.pgp`, sinon l'extension `.gpg` est utilisée.

3.7.2 Déchiffrement

Vous pouvez spécifier ici une commande personnalisée de déchiffrement. Cette option est rarement requise et seulement utile pour les utilisateurs avancés qui connaissent les options des

lignes de commandes de GnuPG.

3.7.3 Apparence

Vous pouvez configurer ici la façon dont KGpg vous est affiché. Les réglages possibles sont les couleurs qui montrent les différents niveaux de confiance dans la clé dans le gestionnaire de clés et les réglages de polices de caractères dans l'éditeur.

3.7.4 Paramètres de GnuPG

Vous pouvez configurer ici quel exécutable gpg, quel **fichier de configuration** et quel dossier personnel sont utilisés. Ces valeurs sont détectées automatiquement au premier démarrage et devrait toujours fonctionner.

L'utilisation de l'agent GnuPG rendra la mise en œuvre de GnuPG plus confortable en vous dispensant de saisir votre mot de passe pour chaque action. Il sera mis en cache en mémoire durant un moment, ainsi, toute opération nécessitant un mot de passe, pourra être exécutée immédiatement. Veuillez noter que cela peut autoriser d'autres personnes à utiliser vos clés privées si vous leur laissez votre session ouverte.

3.7.5 Serveurs de clés

Vous pouvez créer ici une liste de serveurs de clés qui vous sont affichés quand vous ouvrez la boîte de dialogue pour les serveurs de clés. Si vous exécutez GnuPG à partir de la ligne de commande, seul le serveur de clés défini par défaut sera utilisé.

Le protocole utilisé pour la communication avec les serveurs de clé est fondé sur HTTP. Ainsi, cela a du sens que dans certains environnements de **privilégier un serveur mandataire HTTP lorsque disponible**.

3.7.6 Divers

Cette section autorise des réglages de fonctionnalités différentes qui ne rentrent pas dans les autres sections. Vous pouvez par exemple configurer le **Démarrage automatique de KGpg à la connexion**. L'option **Utiliser la sélection avec la souris au lieu de la sélection avec le presse-papier** change si la sélection se fait par la souris et en collant avec le bouton central de la souris ou si toutes les opérations sont faites par des raccourcis clavier.

Vous pouvez aussi indiquer si l'icône de la boîte à miniature de KGpg doit être montrée ou pas et quelle action doit être réalisée sur un clic sur l'icône avec le bouton gauche de la souris. Si l'icône de la boîte à miniature est affichée, la fermeture de la fenêtre de KGpg fera passer l'application en miniature. Si elle n'est pas affichée, KGpg sera fermé quand toutes les fenêtres seront fermées.

Chapitre 4

Remerciements et licence

KGpg

Traduction française par Xavier Besnard ktranslator31@yahoo.fr.