

The KGpg Handbook

Jean-Baptiste Mardelle and Rolf Eike Beer



The KGpg Handbook

Contents

1	Introduction	1
2	Getting Started	2
3	Using KGpg	4
3.1	Generating a key	4
3.2	Encrypting Your Data	6
3.2.1	Encrypting a file from Konqueror or Dolphin	6
3.2.2	Encrypting a text with KGpg's applet	6
3.2.3	Encrypting text from KGpg's editor	6
3.3	Decrypting Your Data	7
3.3.1	Decrypting a file from Konqueror or Dolphin	7
3.3.2	Decrypting text with KGpg's applet	7
3.3.3	Decrypting a text from the editor	7
3.4	Key Management	7
3.4.1	Key Manager	8
3.4.2	Key properties	9
3.5	Working with key servers	10
3.5.1	Communication with key servers	10
3.5.2	Key server search results	11
3.6	Configuring KGpg	11
3.6.1	Encryption	12
3.6.2	Decryption	13
3.6.3	Appearance	13
3.6.4	GnuPG Settings	13
3.6.5	Key Servers	13
3.6.6	Misc	13

Abstract

KGpg is a simple graphical interface for GnuPG (<http://gnupg.org>).

Chapter 1

Introduction

KGpg is a simple interface for GnuPG, a powerful encryption utility. GnuPG (also known as gpg) is included in most distributions and should be installed on your system. You can get the latest version on <http://gnupg.org>.

With KGpg you will be able to encrypt and decrypt your files and emails, allowing much more secure communications. A mini howto on encryption with gpg is available on [gnupg's web site](#).

With KGpg, you don't need to remember gpg's command lines and options. Almost everything can be done with a few mouse clicks.

Chapter 2

Getting Started

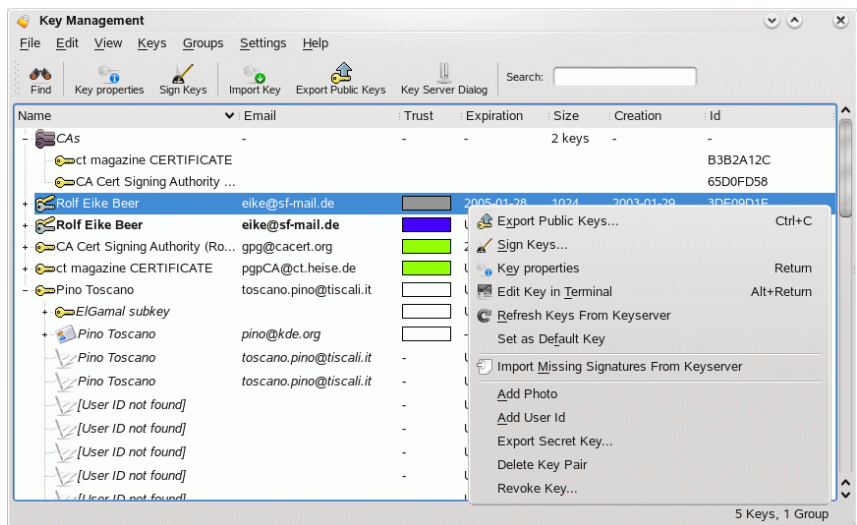
Here is a list of KGpg's main components:

System Tray Icon



When you start KGpg, a system tray icon will appear. A left mouse button click will open the Key Manager window, while a right mouse button click will open a menu allowing quick access to some important features. If you prefer other options you can change the left mouse button action to show the editor or completely disable the system tray icon using the [settings dialog](#).

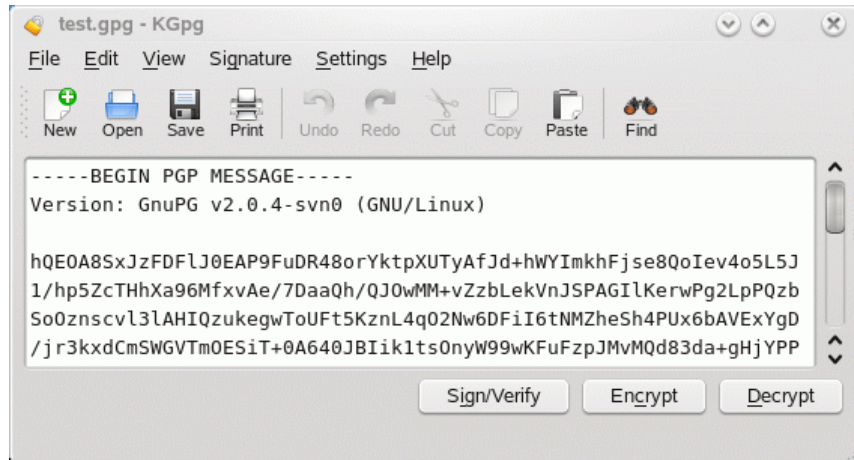
Key Manager Window



The KGpg Handbook

That's the central place to manage your keys. To open the [Key Manager window](#), click with the left mouse button on KGpg's applet. You can import, export, sign and edit your keys. Most actions can be performed with a right mouse button click on a key.

Editor Window



It's a simple text editor, where you can type or paste text to encrypt/decrypt it. To open the [editor](#), click with the right mouse button on KGpg's applet.

File manager integration KGpg is integrated in Konqueror and Dolphin. It means that when you right click on a file, you can choose Actions → Encrypt File to encrypt a file. You can decrypt a file with a left mouse button click.

Chapter 3

Using KGpg

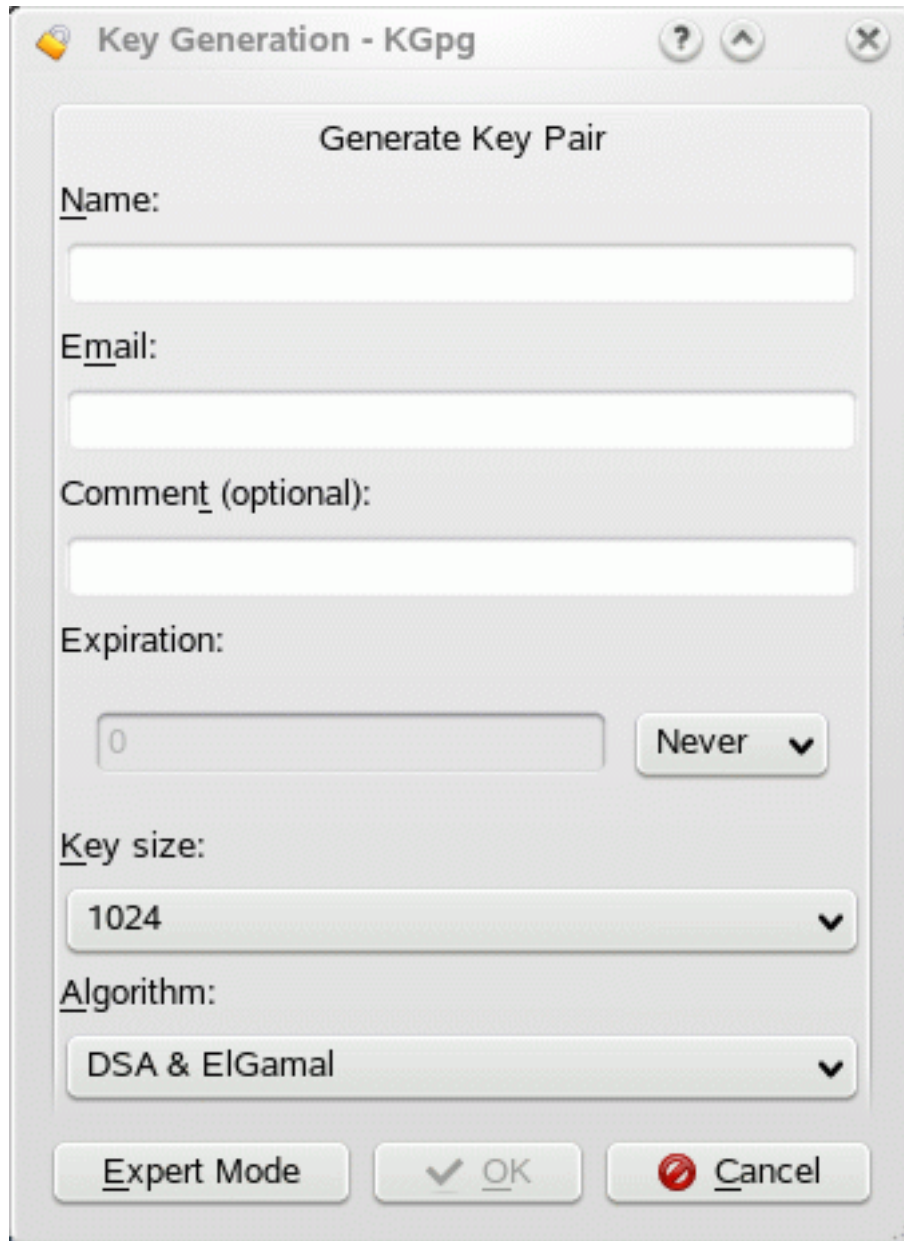
There are two ways to encrypt your data:

- Symmetrical encryption: your data is just encrypted with a password. Anybody who has a computer with `gpg` can decrypt your message if you give him/her the password. To perform a symmetrical encryption, choose "symmetrical encryption" in the options box when asked to choose an encryption key.
- Key encryption: you must first create your key pair (secret key and public key) and give a passphrase. Keep your secret key in a safe place, and exchange your public key with your friends. Then, if you want to send an encrypted message to Alex, you must encrypt the message with Alex's public key. To decrypt the message, the recipient will need Alex's secret key and passphrase.

Key encryption is a bit more complicated (you must exchange keys with your friends) but safer. Remember that if you encrypt a key with someone else's key, you will not be able to decrypt it. You can only decrypt messages that have been encrypted with your public key.

3.1 Generating a key

If you don't have a key, KGpg will automatically pop up the key generation dialog at the first startup. You can also access it in the Key Manager from Keys → Generate Key Pair.



Simply enter your name, Email address and click Ok. This will generate a standard gpg key. If you want more options, you can click on the Expert mode button, which will bring up a Konsole window with all of gpg's options.

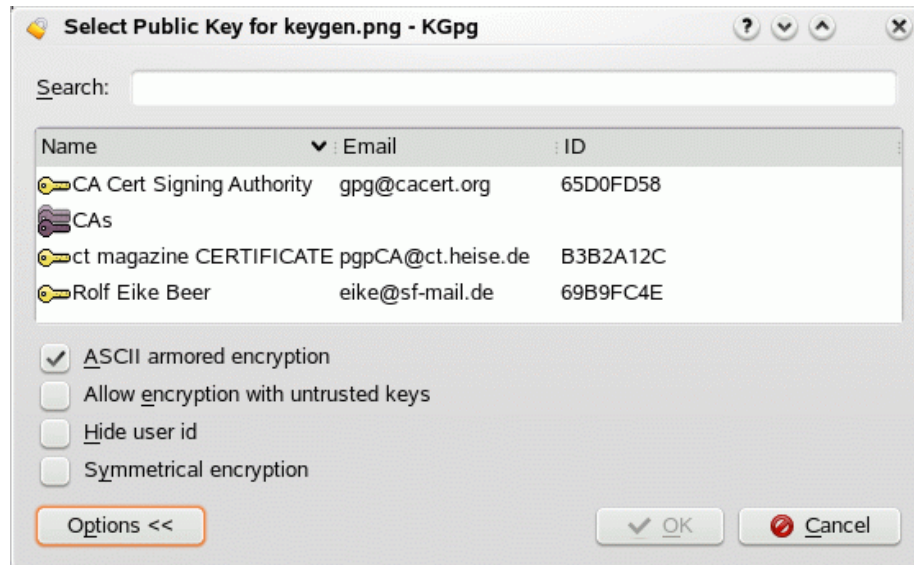
Many people play around with their first key, generate bad user ids, add comments they later regret or simply forget their passphrase. To avoid such keys to stay valid forever it's usually a good idea to limit the lifetime to some 12 month. You can modify the lifetime of your secret keys later using the [key](#)

properties window.

3.2 Encrypting Your Data

3.2.1 Encrypting a file from Konqueror or Dolphin

Click on the file you want to encrypt with the right mouse button. Choose Actions → Encrypt File in the pop up menu. You will then be prompted with the Public key selection dialog. Choose the key of the recipient and click Encrypt. The encrypted file will be saved with a .asc or .pgp extension depending on whether you chose ASCII encryption or not. ASCII encrypted files only use readable characters to represent the data resulting in files that are more robust when copied around or sent by mail but are one third larger.



3.2.2 Encrypting a text with KGpg's applet

You can encrypt the contents of the clipboard by selecting the Encrypt clipboard item in applet menu. When you choose Sign clipboard then the text will be signed instead. Both actions will import the current clipboard contents into an [editor window](#), perform the requested action and paste the contents back into the editor.

3.2.3 Encrypting text from KGpg's editor

This is as simple as clicking on the Encrypt button. You will then be prompted with the Public key selection dialog. Choose your key and click Ok. The en-

encrypted message will appear in the editor window.

Usually you can only encrypt files with keys that are trusted by you. Since you sometimes want to just send a confident note to some random people you are aware of having a GPG key you can set the option Allow encryption with untrusted keys.

To make sure that you can decrypt every file you have encrypted even if they are encrypted with someone else's key you can use the options Always encrypt with and Encrypt files with which are available in the [KGpg configuration](#).

For more information on the encryption options ASCII armor, Allow encryption with untrusted keys and Symmetrical encryption, please refer to gpg's documentation or [man pages](#).

3.3 Decrypting Your Data

3.3.1 Decrypting a file from Konqueror or Dolphin

Left click on the file you want to decrypt. Enter your passphrase and it will be decrypted. You can also drag an encrypted text file and drop it into KGpg's editor window. It will then ask the passphrase and open the decrypted text in KGpg's editor. You can even drop remote files ! You can also use the File → Decrypt File and choose a file to decrypt.

3.3.2 Decrypting text with KGpg's applet

You can also decrypt the contents of the clipboard with the decrypt clipboard menu entry of the KGpg applet. An [editor window](#) will show up with the decrypted text.

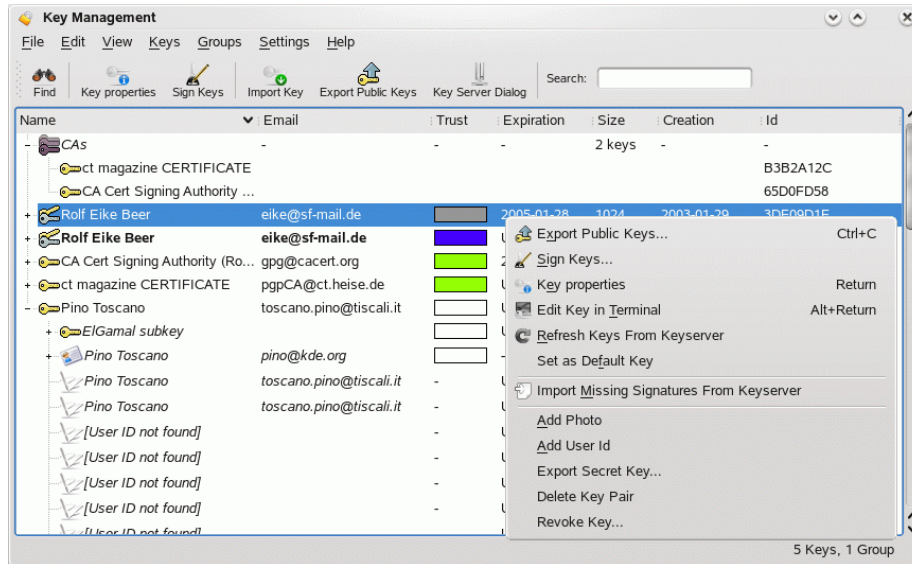
3.3.3 Decrypting a text from the editor

Copy or Drag and Drop the text you want to decrypt, and click on the Decrypt button. You will be prompted for the passphrase.

3.4 Key Management

All basic key management options can be performed through KGpg. To open the key management window click the left mouse button on KGpg's applet. Most options are available with a right click on a key. To import/export public keys, you can use drag and drop or the Copy/Paste keyboard shortcuts.

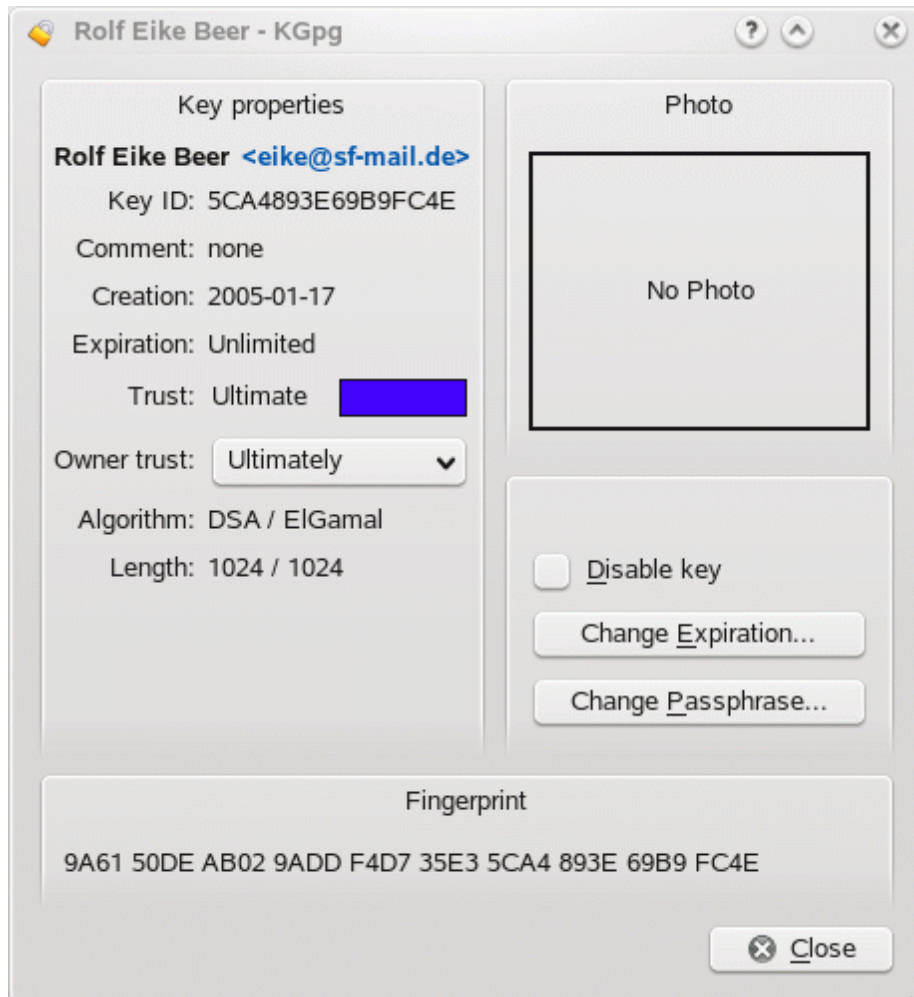
3.4.1 Key Manager



In this example you see a key group containing two keys, two key pairs and three public keys. The third column shows the trust you have in the keys. The first key pair is ultimately trusted and is also set as the default key (bold font) while the second one has expired. Two of the public keys are fully trusted while the trust of the last key is marginal. The last key is expanded, showing it's ElGamal subkey, an additional user id, both also with marginal trust, and some of it's signatures.

Signatures allow navigating through your keyring. Double clicking on a signature or a key shown as member of a group will jump directly to the corresponding primary key.

3.4.2 Key properties



While the key manager allows you to do general actions with one or multiple keys, key groups or signatures, the key properties window gives you access to a single key. You can reach it by pressing enter in the key manager or double clicking the key.

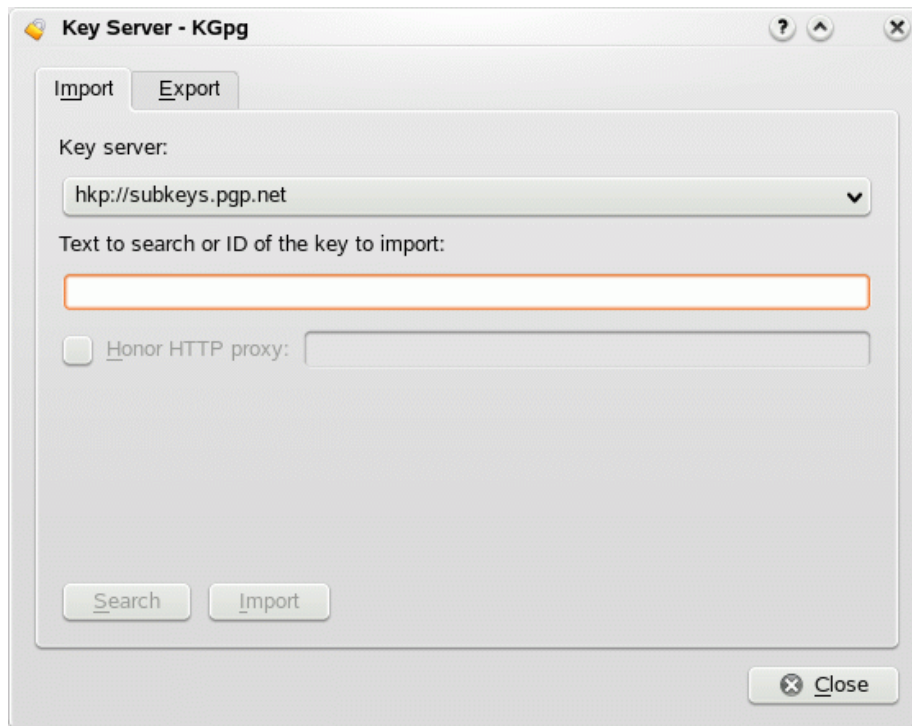
In this window you can change the key passphrase and expiration of your secret keys. For all keys you can also set the owner trust value.

This value indicates how much you trust the owner of this key to correctly verify the identity of the keys he signs. Taking the owner trust into account gpg creates your own web of trust. You trust the keys you signed. If you assign owner trust to these persons you will also trust the keys they have signed without the need that you first have to sign their keys too.

3.5 Working with key servers

3.5.1 Communication with key servers

The public part of a key pair is usually stored on a key server. These servers allow anyone to search for a key belonging to a specific person or mail address. The signatures are also stored on these servers.



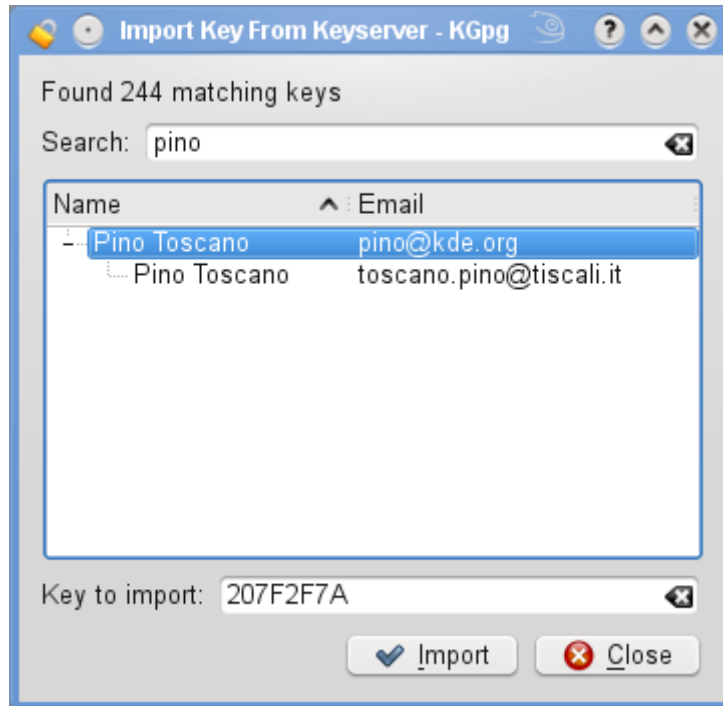
This dialog gives you access to the keyservers. You can search and import keys from a keyserver as well as export keys to a server. An example of searching and importing is when you want to write a mail to someone new. If you would like to encrypt your mail to your contact you can search if he or she has a public key on the key servers. If you have created a new key pair or have signed someone else's key you might want to export the public key (possibly with new signatures) to a keyserver.

Most keyservers synchronize their data between each others so you will get similar search results regardless which server you use. Since there are exceptions of this rule you can choose the keyserver to use in this dialog. It's usually a good idea to choose a default keyserver that is located close to you (i.e. in your country or on your continent) as they usually respond faster to your queries.

Please note that everything you upload to a keyserver usually stays there forever. This is one reason you should usually limit the lifetime of your keys.

Also note that the keyserver are sometimes scanned by spammers for email addresses.

3.5.2 Key server search results



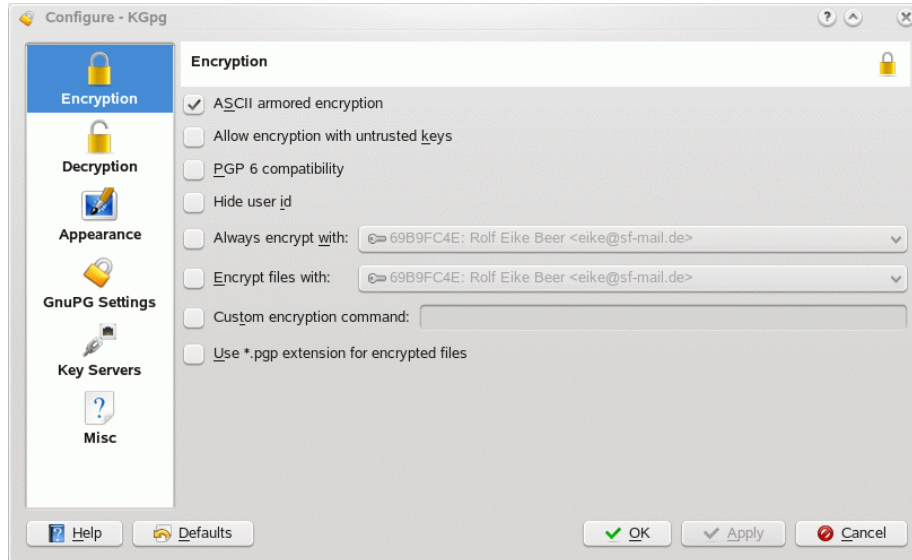
All results of a search are displayed in this window. This picture shows a search for "@kde.org" addresses which showed up 244 results. Using the search field the displayed list was reduced to a single key. This key has two matches: the primary user id itself matches the search string as well as one of the other user ids.

You can select one or more keys to import. The ids of those keys are shown in the Keys to import field at the bottom of the window. When you click on Import the key server is contacted again and the keys are fetched into your keyring.

3.6 Configuring KGpg

Configuration is accessible through the KGpg applet menu (right mouse button click on the applet) or through the main menu (Settings → Configure KGpg). You can set default parameters for encryption, decryption, user interface and applet. Most encryption options are directly related to gpg and are documented in its [man page](#).

3.6.1 Encryption



Here you can configure special options to be passed to GnuPG to change the encryption behaviour. For detailed description please have a look at the GnuPG manual.

- ASCII armored encryption: this causes encrypted files to be stored in a format that uses only printable ASCII characters and has short lines. Files stored this way are bigger than the files in binary format but are easier to send e.g. by email.
- Allow encryption with untrusted keys: this allows you to encrypt files with keys that are not trusted by you.
- PGP 6 compatibility: encrypted files are compatible with the older PGP6 standard. This disables certain features so you should only use this if really needed.
- Hide user id: this removes all evidence of the receiver from the encrypted file. In case the transmission is intercepted noone could gain information about the recipient from the file. If the receiver has multiple keys he needs to try which one was used.
- Always encrypt with: all encryptions are additionally encrypted with this key. If you set this to one of your private keys this makes sure you can read all data you encrypted by the price of bigger messages.
- Encrypt files with: behaves like Always encrypt with for file encryption.
- Custom encryption command: if you need to pass some unusual options to GnuPG you can specify the command line here. Most users will not need this.

- Use *.pgp extension for encrypted files: if you check this option encrypted keys will be named as the input file with the extension .pgp added, otherwise the extension .gpg is used.

3.6.2 Decryption

Here you can specify a custom decryption command. This option is seldomly needed and only useful for advanced users that know of GnuPGs command line options.

3.6.3 Appearance

Here you can configure the way KGpg looks to you. Possible settings are the colors that reflect the different levels of key trust in the [key manager](#) and the font settings for the [editor](#).

3.6.4 GnuPG Settings

Here you can configure which gpg binary and which configuration file and home foldery are used. These values are autodetected on first start and should already work.

Using the [GnuPG agent](#) makes work with GnuPG more comfortable as you do not need to type in your password for every action. It is cached in memory for a while so any operation that would require a password can immediately be done. Note that this may allow other people to use your private keys if you leave your session accessible to them.

3.6.5 Key Servers

Here you can create a list of key servers that are shown to you when you open the [key server dialog](#). If you run GnuPG from the command line only the key server you set as default here will be used.

The protocol used for communication with the key servers is based on HTTP, so it makes sense in some environments to honor the HTTP proxy when available.

3.6.6 Misc

This section allows the setting of some different features that do not fit into the other sections. You can configure for example to start KGpg automatically at login. The option use mouse selection instead of clipboard changes if selection happens by mouse and pasting by middle mouse button or if all operations are done by keyboard shortcuts.

The KGpg Handbook

You can also change if the systray icon of KGpg is shown or not and what action happens if the icon is clicked with the left mouse button. If the systray icon is shown closing the KGpg window will minimize the application to tray. If the systray icon is not shown KGpg will exit when all windows are closed.

Chapter 4

Credits and License

KGpg

Program copyright (c) 2002-2003 Jean-Baptiste Mardelle bj@altern.org.

(c) 2006-2007 Jimmy Gilles jimmygilles@gmail.com

(c) 2006-2008 Rolf Eike Beer kde@opensource.sf-tec.de

This documentation is licensed under the terms of the [GNU Free Documentation License](#).

This program is licensed under the terms of the [GNU General Public License](#).