

## A focus on secure communication: kgpg

#####  
 The article was obtained at the following URL: <http://www.kfwebs.net/articles/article/20>  
 The article might be distributed further as long as it is provided as it is, with the credits stated.  
 The Article was written and first published by KF Webs, at <http://www.kfwebs.net>  
 #####

*This is an article describing how to use kgpg, a key manager for GNU Privacy Guard. It might be apprehended at <http://developer.kde.org/~kgpg/>.  
 Added: 2005-08-11 04:39:11 - Modified: 2005-08-28 18:08:24 - Level: Beginner*

## About kgpg

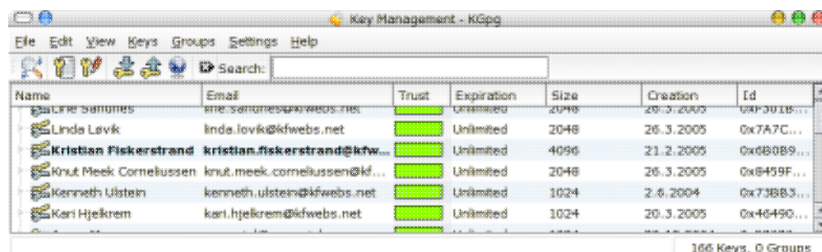
This is an article describing how to use kgpg, a key manager for GNU Privacy Guard. It might be apprehended at <http://developer.kde.org/~kgpg/> .

As the website state the following features of kgpg include:

- Editor mode enables you to type/paste a text and encrypt/decrypt/sign/verify it
- Key manager: import, export, delete, sign, generate and edit keys.
- Integration with konqueror (1): left click on a file to decrypt/verify it.
- Integration with konqueror (2): right click on a file to encrypt/sign it.
- Encryption: support for symetric encryption. Multiple keys & default key encryption. Optional shredding of source files
- Signatures: creation & verification of detached & cleartext signatures
- Drag & drop encryption + clipboard en/decryption

## Using kgpg

When you're first presented with kgpg the following window is presented



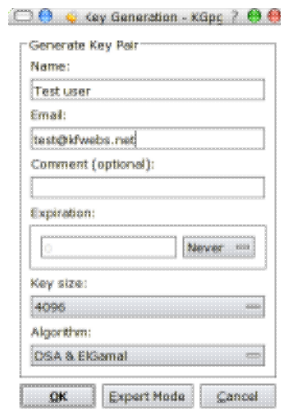
Now, if you are totally unaware of how PGP work you will probably have a hard time understanding the screen you are presented with. In short it show

- The name of the primary userid

- The email of the primary userid
- The calculated trust: Green means trusted, red is expired or marginal, black is revoked.
- The expiration date of the key
- The key size in bits
- The creation date
- The key ID

You might also notice that one of the keys are bolded, this is the default key specified

## Generating a key



Now, if you haven't used gnupg before the first thing you want to do is to generate a new key You start of by pressing Keys > Generate key pair

Yes, you actually generate pairs of keys, in total 4 keys. Two of which are called private keys, and two that are public keys. You share the public keys and keep the private keys secret. One of the keypairs is used for signatures, while the other keypair is used for encryption.

When you are presented with the key generation dialog you fill in your name and your email address. The default key type is a DSA key, which will use an ElGamal key for encryption. I suggest you specify at least a 2048 bit key size, which will give you a 1024 bit DSA key and a 2048 bit ElGamal key, you may also select 4096 here.

*Advanced users:* Worth to mention here is that DSA require the signing algorithm/digest algorithm to be 160 bit (defaulting to sha-1). If you want to use hashes such as SHA-256 and SHA-512 you should select RSA as the key-type. This will however only generate the signing key, and you will have to add an encryption subkey manually

The key generation itself might take some time depending on the size you specified. Just wait, it is quite natural. You might speed up the process by moving the mouse around and pressing keys, such as caps-lock.

## Importing a key

To be able to verify signatures from other people and to encrypt emails you send to others, you will need to have their keypair on your local keyring. The import from keyserver option is a great help here. You can access it by selecting file > Key Server Dialog. You can then enter the name or the key id of the key you wish to access, if it is on the keyserver specified (I usually use the random.sks.keyserver.penguin.de pool) it should be an easy process to get the key, if the key isn't there, you will have to use some other means (like contacting the owner) to get the key. In some cases you will also find the key on exempli gratia websites, in my case on <http://www.kfwebs.net/pgp>

If you download the key as a text file you can import it using Keys > Import keys. This will give you the option to import from the clipboard or from a file.

## Signing a key

Key signing is the basis of the Web of Trust of which OpenPGP is based on. It means that if you know someone having the key, and can verify that the key belongs to the user, you sign it. By this you tell other users that you have verified the key, so if others again in turn can verify your key, they can have a trust going from themselves to the one you signed.

A local key is non-exportable, meaning you can say that yourself is confident in the owner, but you aren't sure enough to let others base their trust on it. These signatures won't be exported to a keyserver if you specify the export option.

## Revoking a key

You should generate a revocation certificate while generating a new key. This certificate is to be used in a case such as if you have lost your password, you have lost your private key, or your key has been compromised.

To generate a revocation certificate you right click on the key and press revoke key. Fill in a proper reason for the revocation, make sure the save certificate checkbox is checked and select a place to store the revocation certificate. Remember, store this in a safe place, preferably print it to hard-copy as well (it is short enough to type in in the case it is needed). Make sure nobody else gets hold of this, as it can invalidate your entire key.

To import this certificate, look at the chapter of how to import a key.

## Related articles:

[A focus on secure communication: Evolution](http://www.kfwebs.net/articles/article/19)[<http://www.kfwebs.net/articles/article/19>] ([Focus on secure communication](#))

[A focus on secure communication: Mozilla Thunderbird and Enigmail](http://www.kfwebs.net/articles/article/22)[<http://www.kfwebs.net/articles/article/22>] ([Focus on secure communication](#))



[A focus on secure communication: Why you should sign and encrypt your emails](http://www.kfwebs.net/articles/article/21) [<http://www.kfwebs.net/articles/article/21>] (Focus on secure communication)