GPG documentation

Contains some tricks on using GnuPG[1].

Contents

1 How to sign a release tarball

```
gpg --detach-sign --armor -o release.tar.gz.sign release.tar.gz
```

2 How to get a gpg key fingerprint

```
gpg --fingerprint $name_or_keyid
```

e.g:

```
gpg --fingerprint Sebastien
```

3 How to specify an alternate keyring

```
gpg --no-default-keyring --keyring pubring.gpg [...]
```

or, if this is a private keyring:

```
gpg --no-default-keyring --secret-keyring secring.gpg [...]
```

[1] http://gnupg.org/

4 How to sign a new key

First, import the public key:

```
gpg --import $keyfile
```

or get it from a key server:

```
gpg --search-key $keyid
```

Then edit the key:

```
gpg --edit-key $keyid
```

Use the `fpr` command to check the fingerprints. Use the `list` command to see the key information at any time. Then use the `sign` command to sign it once you have checked everything. Do not forget to set the default key (section 6) if you want to sign with a specific key. You should then change the owner trust using the `trust` command.

Use `save` to save your changes and quit.

Finally, use:

```
gpg --send-keys $keyid
```

to send your signatures back to the key server.

5 How to merge two secret keys and import them

Assume I have a secret key with subkey A, and the same secret key but with subkey B. How do I import a secret key with subkeys A and B ?

The solution is rather involved and uses `gpgsplit`. First, export the two secret keys:

```
gpg --export-secret-keys SECID > firstkey.gpg gpg --export-secret-keys SECID2 > secondk
```

Then split one key:

```
gpgsplit secondkey.gpg
```

And create a new key by concatenating its subkey file with the first key:

```
cat firstkey.gpg 00000x-05.secret-subkey 0000000x-06.sig ... > newkey.gpg
```

And export the new key after having deleted all references to the old ones:

```
gpg --import newkey.gpg
```

This method was given in a post on the GPG mailing list[2]

[2] `http://lists.gnupg.org/pipermail/gnupg-devel/2002-March/018193.html`

6 Setting the default key

The default key is the one that is used by default to sign data. If you have more than one secret key in your keyring, you may want to set a specific one as default. To do this, edit `gpg.conf` and add the following line:

```
default-key $keyid
```

Where `$keyid` is your default key's id.
If you want to override that choice when invoking GPG, give the `--default-key` option.

7 Forcing a particular subkey to be used

You can prefix a key ID with an exclamation mark (`!`) to force this particular subkey to be used. This is sometimes necessary e.g when default signing subkeys are defined.