

NAME

gpgtar – Encrypt or sign files into an archive

SYNOPSIS

gpgtar [*options*] *filename1* [*filename2*, ...] *directory1* [*directory2*, ...]

DESCRIPTION

gpgtar encrypts or signs files into an archive. It is an gpg-ized tar using the same format as used by PGP's PGP Zip.

OPTIONS

gpgtar understands these options:

--create

Put given files and directories into a vanilla “ustar” archive.

--extract

Extract all files from a vanilla “ustar” archive.

--encrypt

-e Encrypt given files and directories into an archive. This option may be combined with option **--symmetric** for an archive that may be decrypted via a secret key or a passphrase.

--decrypt

-d Extract all files from an encrypted archive.

--sign

-s Make a signed archive from the given files and directories. This can be combined with option **--encrypt** to create a signed and then encrypted archive.

--list-archive

-t List the contents of the specified archive.

--symmetric

-c Encrypt with a symmetric cipher using a passphrase. The default symmetric cipher used is AES-128, but may be chosen with the **--cipher-algo** option to **gpg**.

--recipient *user*

-r *user* Encrypt for user id *user*. For details see **gpg**.

--local-user *user*

-u *user* Use *user* as the key to sign with. For details see **gpg**.

--output *file*

-o *file* Write the archive to the specified file *file*.

--verbose

-v Enable extra informational output.

- quiet**
-q Try to be as quiet as possible.
- skip-crypto**
Skip all crypto operations and create or extract vanilla “ustar” archives.
- dry-run**
Do not actually output the extracted files.
- directory *dir***
-C *dir* Extract the files into the directory *dir*. The default is to take the directory name from the input filename. If no input filename is known a directory named ‘*GPGARCH*’ is used.
- files-from *file***
-T *file* Take the file names to work from the file *file*; one file per line.
- null** Modify option **--files-from** to use a binary nul instead of a linefeed to separate file names.
- openpgp**
This option has no effect because OpenPGP encryption and signing is the default.
- cms** This option is reserved and shall not be used. It will eventually be used to encrypt or sign using the CMS protocol; but that is not yet implemented.
- set-filename *file***
Use the last component of *file* as the output directory. The default is to take the directory name from the input filename. If no input filename is known a directory named ‘*GPGARCH*’ is used. This option is deprecated in favor of option **--directory**.
- gpg *gpgcmd***
Use the specified command *gpgcmd* instead of **gpg**.
- gpg-args *args***
Pass the specified extra options to **gpg**.
- tar-args *args***
Assume *args* are standard options of the command **tar** and parse them. The only supported tar options are “--directory”, “--files-from”, and “--null” This is an obsolete options because those supported tar options can also be given directly.
- version**
Print version of the program and exit.
- help** Display a brief help page and exit.

EXAMPLES

Encrypt the contents of directory ‘*mydocs*’ for user Bob to file ‘*test1*’:

```
gpgtar --encrypt --output test1 -r Bob mydocs
```

List the contents of archive ‘*test1*’:

```
gpgtar --list-archive test1
```

DIAGNOSTICS

The program returns 0 if everything was fine, 1 otherwise.

SEE ALSO

gpg(1), **tar**(1),

The full documentation for this tool is maintained as a Texinfo manual. If GnuPG and the info program are properly installed at your site, the command

```
info gnupg
```

should give you access to the complete manual including a menu structure and an index.