

NAME

gpgv2 - Verify OpenPGP signatures

SYNOPSIS

gpgv2 [*options*] *signed_files*

DESCRIPTION

gpgv2 is an OpenPGP signature verification tool.

This program is actually a stripped-down version of **gpg** which is only able to check signatures. It is somewhat smaller than the fully-blown **gpg** and uses a different (and simpler) way to check that the public keys used to make the signature are valid. There are no configuration files and only a few options are implemented.

gpgv2 assumes that all keys in the keyring are trustworthy. That does also mean that it does not check for expired or revoked keys.

If no **--keyring** option is given, **gpgv** looks for a “default” keyring named ‘*trustedkeys.kbx*’ (preferred) or ‘*trustedkeys.gpg*’ in the home directory of GnuPG, either the default home directory or the one set by the **--homedir** option or the **GNUPGHOME** environment variable. If any **--keyring** option is used, **gpgv** will not look for the default keyring. The **--keyring** option may be used multiple times and all specified keyrings will be used together.

RETURN VALUE

The program returns 0 if everything is fine, 1 if at least one signature was bad, and other error codes for fatal errors.

OPTIONS

gpgv2 recognizes these options:

--verbose

-v Gives more information during processing. If used twice, the input data is listed in detail.

--quiet

-q Try to be as quiet as possible.

--keyring *file*

Add *file* to the list of keyrings. If *file* begins with a tilde and a slash, these are replaced by the HOME directory. If the filename does not contain a slash, it is assumed to be in the home-directory ("~/gnupg" if --homedir is not used).

--output *file***-o *file***

Write output to *file*; to write to stdout use -. This option can be used to get the signed text from a cleartext or binary signature; it also works for detached signatures, but in that case this option is in general not useful. Note that an existing file will be overwritten.

--status-fd *n*

Write special status strings to the file descriptor *n*. See the file DETAILS in the documentation for a listing of them.

--logger-fd *n*

Write log output to file descriptor *n* and not to stderr.

--log-file *file*

Same as **--logger-fd**, except the logger data is written to file **file**. Use 'socket://' to log to socket.

--ignore-time-conflict

GnuPG normally checks that the timestamps associated with keys and signatures have plausible values. However, sometimes a signature seems to be older than the key due to clock problems. This option turns these checks into warnings.

--homedir *dir*

Set the name of the home directory to *dir*. If this option is not used, the home directory defaults to '~/gnupg'. It is only recognized when given on the command line. It also overrides any home

directory stated through the environment variable '*GNUPGHOME*' or (on Windows systems) by means of the Registry entry *HKCU\Software\GNU\GnuPG:HomeDir*.

On Windows systems it is possible to install GnuPG as a portable application. In this case only this command line option is considered, all other ways to set a home directory are ignored.

--weak-digest name

Treat the specified digest algorithm as weak. Signatures made over weak digests algorithms are normally rejected. This option can be supplied multiple times if multiple algorithms should be considered weak. MD5 is always considered weak, and does not need to be listed explicitly.

--enable-special-filenames

This option enables a mode in which filenames of the form '*-&n*', where *n* is a non-negative decimal number, refer to the file descriptor *n* and not to a file with that name.

--assert-pubkey-algo *algotlist*

This option works in the same way as described for **gpg**.

EXAMPLES

gpgv2 pgpfile

gpgv2 sigfile [datafile]

Verify the signature of the file. The second form is used for detached signatures, where **sigfile** is the detached signature (either ASCII-armored or binary) and **datafile** contains the signed data; if **datafile** is "-" the signed data is expected on **stdin**; if **datafile** is not given the name of the file holding the signed data is constructed by cutting off the extension (".asc", ".sig" or ".sign") from **sigfile**.

FILES

~/.gnupg/trustedkeys.gpg

The default keyring with the allowed keys.

ENVIRONMENT

HOME

Used to locate the default home directory.

GNUPGHOME

If set directory used instead of "~/.gnupg".

SEE ALSO

gpg(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.