NAME

gpg-preset-passphrase – Put a passphrase into gpg-agent's cache

SYNOPSIS

gpg-preset-passphrase [*options*] [*command*] *cache-id*

DESCRIPTION

The **gpg-preset-passphrase** is a utility to seed the internal cache of a running **gpg-agent** with passphrases. It is mainly useful for unattended machines, where the usual **pinentry** tool may not be used and the passphrases for the to be used keys are given at machine startup.

This program works with GnuPG 2 and later. GnuPG 1.x is not supported.

Passphrases set with this utility don't expire unless the **--forget** option is used to explicitly clear them from the cache --- or **gpg-agent** is either restarted or reloaded (by sending a SIGHUP to it). Note that the maximum cache time as set with **--max-cache-ttl** is still honored. It is necessary to allow this passphrase presetting by starting **gpg-agent** with the **--allow-preset-passphrase**.

gpg-preset-passphrase is invoked this way:

    gpg-preset-passphrase [options] [command] *cacheid*

cacheid is either a 40 character keygrip of hexadecimal characters identifying the key for which the passphrase should be set or cleared. The keygrip is listed along with the key when running the command: **gpgsm --with-keygrip --list-secret-keys**. Alternatively an arbitrary string may be used to identify a passphrase; it is suggested that such a string is prefixed with the name of the application (e.g **foo:12346**). Scripts should always use the option **--with-colons**, which provides the keygrip in a "grp" line (cf. '*doc/DE-TAILS*')/

One of the following command options must be given:

--preset

 Preset a passphrase. This is what you usually will use. **gpg-preset-passphrase** will then read the passphrase from **stdin**.

--forget

 Flush the passphrase for the given cache ID from the cache.

The following additional options may be used:

-v
--verbose

 Output additional information while running.

-P *string*
--passphrase *string*

 Instead of reading the passphrase from **stdin**, use the supplied *string* as passphrase. Note that this makes the passphrase visible for other users.

SEE ALSO

gpg(1), **gpgsm**(1), **gpg-agent**(1), **scdaemon**(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.

gpg(1), **gpgsm**(1), **gpg-agent**(1), **scdaemon**(1)