NAME

scdaemon − Smartcard daemon for the GnuPG system

SYNOPSIS

scdaemon [−−**homedir** *dir*] [−−**options** *file*] [*options*] −−**server**
scdaemon [−−**homedir** *dir*] [−−**options** *file*] [*options*] −−**daemon** [*command_line*]

DESCRIPTION

The **scdaemon** is a daemon to manage smartcards. It is usually invoked by **gpg-agent** and in general not used directly.

COMMANDS

Commands are not distinguished from options except for the fact that only one command is allowed.

--version
Print the program version and licensing information. Note that you cannot abbreviate this command.

--help, -h
Print a usage message summarizing the most useful command-line options. Note that you cannot abbreviate this command.

--dump-options
Print a list of all available options and commands. Note that you cannot abbreviate this command.

--server
Run in server mode and wait for commands on the **stdin**. The default mode is to create a socket and listen for commands there.

--multi-server
Run in server mode and wait for commands on the **stdin** as well as on an additional Unix Domain socket. The server command **GETINFO** may be used to get the name of that extra socket.

--daemon
Run the program in the background. This option is required to prevent it from being accidentally running in the background.

OPTIONS

--options *file*
Reads configuration from *file* instead of from the default per-user configuration file. The default configuration file is named '*scdaemon.conf*' and expected in the '*.gnupg*' directory directly below the home directory of the user.

--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.

To install GnuPG as a portable application under Windows, create an empty file named '*gpgconf.ctl*' in the same directory as the tool '*gpgconf.exe*'. The root of the installation is then that directory; or, if '*gpgconf.exe*' has been installed directly below a directory named '*bin*', its parent directory. You also need to make sure that the following directories exist and are writable: '*ROOT/home*' for the GnuPG home and '*ROOT/var/cache/gnupg*' for internal cache files.

-v

--verbose
Outputs additional information while running. You can increase the verbosity by giving several verbose commands to **gpgsm**, such as '-vv'.

--debug-level *level*
Select the debug level for investigating problems. *level* may be a numeric value or a keyword:

none No debugging at all. A value of less than 1 may be used instead of the keyword.

basic Some basic debug messages. A value between 1 and 2 may be used instead of the keyword.

advanced
More verbose debug messages. A value between 3 and 5 may be used instead of the keyword.

expert Even more detailed messages. A value between 6 and 8 may be used instead of the keyword.

guru All of the debug messages you can get. A value greater than 8 may be used instead of the keyword. The creation of hash tracing files is only enabled if the keyword is used.

How these messages are mapped to the actual debugging flags is not specified and may change with newer releases of this program. They are however carefully selected to best aid in debugging.

All debugging options are subject to change and thus should not be used by any application program. As the name says, they are only used as helpers to debug problems.

--debug *flags*
This option is only useful for debugging and the behavior may change at any time without notice. FLAGS are bit encoded and may be given in usual C-Syntax. The currently defined bits are:

0 (1) command I/O

1 (2) values of big number integers

2 (4) low level crypto operations

5 (32) memory allocation

6 (64) caching

7 (128) show memory statistics

9 (512) write hashed data to files named **dbgmd-000***

10 (1024)
trace Assuan protocol. See also option **--debug-assuan-log-cats**.

11 (2048)
trace APDU I/O to the card. This may reveal sensitive data.

12 (4096)
trace some card reader related function calls.

--debug-all
Same as **--debug=0xffffffff**

--debug-wait *n*
When running in server mode, wait *n* seconds before entering the actual processing loop and print the pid. This gives time to attach a debugger.

--debug-ccid-driver
Enable debug output from the included CCID driver for smartcards. Using this option twice will also enable some tracing of the T=1 protocol. Note that this option may reveal sensitive data.

--debug-disable-ticker
This option disables all ticker functions like checking for card insertions.

--debug-allow-core-dump
For security reasons we won't create a core dump when the process aborts. For debugging purposes it is sometimes better to allow core dump. This option enables it and also changes the working directory to '*/tmp*' when running in**--ser ver** mode.

--debug-log-tid
This option appends a thread ID to the PID in the log output.

--debug-assuan-log-cats *cats*
Changes the active Libassuan logging categories to *cats*. The value for *cats* is an unsigned integer given in usual C-Syntax. A value of 0 switches to a default category. If this option is not used the categories are taken from the environment variable **ASSUAN_DEBUG**. Note that this option has only an effect if the Assuan debug flag has also been with the option **--debug**. For a list of categories see the Libassuan manual.

--no-detach
Don't detach the process from the console. This is mainly useful for debugging.

--listen-backlog *n*
Set the size of the queue for pending connections. The default is 64. This option has an effect only if **--multi-server** is also used.

--log-file *file*
Append all logging output to *file*. This is very helpful in seeing what the agent actually does. Use '*socket://*' to log to socket.

--pcsc-driver *library*
Use *library* to access the smartcard reader. The current default is '*libpcsclite.so*'. Instead of using this option you might also want to install a symbolic link to the default file name (e.g. from '*libpcsclite.so.1*').

--ctapi-driver *library*
Use *library* to access the smartcard reader. The current default is '*libtowitoko.so*'. Note that the use of this interface is deprecated; it may be removed in future releases.

--disable-ccid
Disable the integrated support for CCID compliant readers. This allows falling back to one of the other drivers even if the internal CCID driver can handle the reader. Note, that CCID support is only available if libusb was available at build time.

--reader-port *number_or_string*
This option may be used to specify the port of the card terminal. A value of 0 refers to the first serial device; add 32768 to access USB devices. The default is 32768 (first USB device). PC/SC or CCID readers might need a string here; run the program in verbose mode to get a list of available readers. The default is then the first reader found.

To get a list of available CCID readers you may use this command:

```
echo scd getinfo reader_list \
 | gpg-connect-agent --decode | awk '/^D/ {print $2}'
```

--card-timeout *n*
If *n* is not 0 and no client is actively using the card, the card will be powered down after *n* seconds. Powering down the card avoids a potential risk of damaging a card when used with certain cheap readers. This also allows applications that are not aware of Scdaemon to access the card. The disadvantage of using a card timeout is that accessing the card takes longer and that the user needs to enter the PIN again after the next power up.

Note that with the current version of Scdaemon the card is powered down immediately at the next timer tick for any value of *n* other than 0.

--enable-pinpad-varlen
Please specify this option when the card reader supports variable length input for pinpad (default is no). For known readers (listed in ccid-driver.c and apdu.c), this option is not needed. Note that if your card reader doesn't supports variable length input but you want to use it, you need to specify your pinpad request on your card.

--disable-pinpad
Even if a card reader features a pinpad, do not try to use it.

--deny-admin
This option disables the use of admin class commands for card applications where this is supported. Currently we support it for the OpenPGP card. This option is useful to inhibit accidental access to admin class command which could ultimately lock the card through wrong PIN numbers. Note that GnuPG versions older than 2.0.11 featured an **--allow-admin** option which was required to use such admin commands. This option has no more effect today because the default is now to allow admin commands.

--disable-application *name*
This option disables the use of the card application named *name*. This is mainly useful for debugging or if a application with lower priority should be used by default.

All the long options may also be given in the configuration file after stripping off the two leading dashes.

CARD APPLICATIONS

scdaemon supports the card applications as described below.

The OpenPGP card application "openpgp"

This application is currently only used by **gpg** but may in future also be useful with **gpgsm**. Version 1 and version 2 of the card is supported.

The specifications for these cards are available at
(**http://g10code.com/docs/openpgp-card-1.0.pdf**) and
(**http://g10code.com/docs/openpgp-card-2.0.pdf**).

The Telesec NetKey card "nks"

This is the main application of the Telesec cards as available in Germany. It is a superset of the German DINSIG card. The card is used by **gpgsm**.

The DINSIG card application "dinsig"

This is an application as described in the German draft standard *DIN V 66291-1*. It is intended to be used by cards supporting the German signature law and its bylaws (SigG and SigV).

The PKCS#15 card application "p15"

This is common framework for smart card applications. It is used by **gpgsm**.

The Geldkarte card application "geldkarte"

This is a simple application to display information of a German Geldkarte. The Geldkarte is a small amount debit card application which comes with almost all German banking cards.

The SmartCard-HSM card application "sc-hsm"

This application adds read-only support for keys and certificates stored on a (**http://www.smartcard-hsm.com, SmartCard-HSM**).

To generate keys and store certificates you may use (**https://github.com/OpenSC/OpenSC/wiki/SmartCardHSM, OpenSC**) or the tools from (**http://www.openscdp.org, OpenSCDP**).

The SmartCard-HSM cards requires a card reader that supports Extended Length APDUs.

The Undefined card application "undefined"

This is a stub application to allow the use of the APDU command even if no supported application is found on the card. This application is not used automatically but must be explicitly requested using the SERIALNO command.

EXAMPLES

```
$ scdaemon --server -v
```

FILES

There are a few configuration files to control certain aspects of **scdaemons**'s operation. Unless noted, they are expected in the current home directory (see: [option --homedir]).

scdaemon.conf
: This is the standard configuration file read by **scdaemon** on startup. It may contain any valid long option; the leading two dashes may not be entered and the option may not be abbreviated. This default name may be changed on the command line (see: [option --options]).

scd-event
: If this file is present and executable, it will be called on every card reader's status change. An example of this script is provided with the distribution

reader_*n*.status
: This file is created by **scdaemon** to let other applications now about reader status changes. Its use is now deprecated in favor of '*scd-event*'.

SEE ALSO

gpg-agent(1), **gpgsm**(1), **gpg2**(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.