Rocky Enterprise Linux 9.2 Manual Pages on command 'tpm2.1'

$ man tpm2.1

tpm2(1) General Commands Manual tpm2(1)

NAME

tpm2(1) - A single small executable that combines the various tpm2-tools much like a BusyBox that provides a fairly complete environ? ment for any small or embedded system.

SYNOPSIS

tpm2 [OPTIONS] [ARGUMENTS]

DESCRIPTION

tpm2(1) - To ease installation of tpm2-tools in initrd or embedded sys? tems where size-optimization and limited resources are important, it is convenient to have a single executable that can dispatch the various TPM2 functionalities specified by the argument which is one of the available tool names.

The options and arguments that follow are either the common options or those specific to the tool name.

It is important to note that individual tools with prefix tpm2_ can still be invoked, however, they are now soft-linked to this tpm2 exe? cutable. And so unlike BusyBox, full functionality of the individual

tools is available in the executable. For example: tpm2_getrandom 8

can alternatively be specified as tpm2 getrandom 8.

ARGUMENTS

List of possible tool names. NOTE: Specify only one of these. Look at

examples.

certifyX509certutil

checkquote

eventlog

print

rc_decode

activatecredential

certify

changeauth

changeeps

changepps

clear

clearcontrol

clockrateadjust

create

createak

createek

createpolicy

setprimarypolicy

createprimary

dictionarylockout

duplicate

getcap

gettestresult

encryptdecrypt

evictcontrol

flushcontext

getekcertificate

getrandom

gettime

hash

hierarchycontrol

hmac

import

incrementalselftest

load

loadexternal

makecredential

nvdefine

nvextend

nvincrement

nvreadpublic

nvread

nvreadlock

nvundefine

nvwrite

nvwritelock

nvsetbits

pcrallocate

pcrevent

pcrextend

pcrread

pcrreset

policypcr

policyauthorize

policyauthorizenv

policynv

policycountertimer

policyor

policynamehash

policytemplate

policycphash

policypassword

policysigned

policyticket

policyauthvalue

policysecret

policyrestart

policycommandcode

policynvwritten

policyduplicationselect

policylocality

quote

readclock

readpublic

rsadecrypt

rsaencrypt

send

selftest

sessionconfig

setclock

shutdown

sign

certifycreation

nvcertify

startauthsession

startup

stirrandom

testparms

unseal

verifysignature

setcommandauditstatus

getcommandauditdigest

getsessionauditdigest

geteccparameters

ecephemeral

commit

ecdhkeygen

ecdhzgen

zgen2phase

References

COMMON OPTIONS

This collection of options are common to many programs and provide in? formation that many users may expect.

? -h, --help=[man|no-man]: Display the tools manpage. By default, it attempts to invoke the manpager for the tool, however, on failure will output a short tool summary. This is the same behavior if the ?man? option argument is specified, however if explicit ?man? is re? quested, the tool will provide errors from man on stderr. If the ?no-man? option if specified, or the manpager fails, the short op? tions will be output to stdout.

To successfully use the manpages feature requires the manpages to be installed or on MANPATH, See man(1) for more details.

? -v, --version: Display version information for this tool, supported tctis and exit.

? -V, --verbose: Increase the information that the tool prints to the console during its execution. When using this option the file and line number are printed.

? -Q, --quiet: Silence normal tool output to stdout.

? -Z, --enable-errata: Enable the application of errata fixups. Useful if an errata fixup needs to be applied to commands sent to the TPM.

Defining the environment TPM2TOOLS_ENABLE_ERRATA is equivalent. in? formation many users may expect.

TCTI Configuration

The TCTI or ?Transmission Interface? is the communication mechanism with the TPM. TCTIs can be changed for communication with TPMs across different mediums.

To control the TCTI, the tools respect:

1. The command line option -T or --tcti

2. The environment variable: TPM2TOOLS_TCTI.

Note: The command line option always overrides the environment vari?

able.

The current known TCTIs are:

? tabrmd - The resource manager, called tabrmd (https://github.com/tpm2-software/tpm2-abrmd). Note that tabrmd and abrmd as a tcti name are synonymous.

? mssim - Typically used for communicating to the TPM software simula? tor.

? device - Used when talking directly to a TPM device file.

? none - Do not initalize a connection with the TPM. Some tools allow for off-tpm options and thus support not using a TCTI. Tools that do not support it will error when attempted to be used without a TCTI connection. Does not support ANY options and MUST BE presented as the exact text of ?none?.

The arguments to either the command line option or the environment variable are in the form:

<tcti-name>:<tcti-option-config>

Specifying an empty string for either the <tcti-name> or <tcti-op? tion-config> results in the default being used for that portion respec? tively.

TCTI Defaults

When a TCTI is not specified, the default TCTI is searched for using dlopen(3) semantics. The tools will search for tabrmd, device and mssim TCTIs IN THAT ORDER and USE THE FIRST ONE FOUND. You can query what TCTI will be chosen as the default by using the -v option to print the version information. The ?default-tcti? key-value pair will indi? cate which of the aforementioned TCTIs is the default.

Custom TCTIs

Any TCTI that implements the dynamic TCTI interface can be loaded. The tools internally use dlopen(3), and the raw tcti-name value is used for the lookup. Thus, this could be a path to the shared library, or a li?

brary name as understood by dlopen(3) semantics.

TCTI OPTIONS

This collection of options are used to configure the various known TCTI modules available:

? device: For the device TCTI, the TPM character device file for use by the device TCTI can be specified. The default is /dev/tpm0.

Example: -T device:/dev/tpm0 or export TPM2TOOLS_TCTI=?device:/dev/tpm0?

? mssim: For the mssim TCTI, the domain name or IP address and port number used by the simulator can be specified. The default are 127.0.0.1 and 2321.

Example: -T mssim:host=localhost,port=2321 or export TPM2TOOLS_TCTI=?mssim:host=localhost,port=2321?

? abrmd: For the abrmd TCTI, the configuration string format is a series of simple key value pairs separated by a `,' character. Each key and value string are separated by a `=' character.

? TCTI abrmd supports two keys:

1. `bus_name' : The name of the tabrmd service on the bus (a string).
2. `bus_type' : The type of the dbus instance (a string) limited to `session' and `system'.

Specify the tabrmd tcti name and a config string of bus_name=com.example.FooBar:

\--tcti=tabrmd:bus_name=com.example.FooBar

Specify the default (abrmd) tcti and a config string of bus_type=session:

\--tcti:bus_type=session

NOTE: abrmd and tabrmd are synonymous. the various known TCTI modules.

EXAMPLES

Get 8 rand bytes from the TPM

tpm2 getrandom 8 | xxd -p

Send a TPM Startup Command with flags TPM2_SU_CLEAR

tpm2 startup -c

Returns

Tools can return any of the following codes:

? 0 - Success.

? 1 - General non-specific error.

? 2 - Options handling error.

? 3 - Authentication error.

? 4 - TCTI related error.

? 5 - Non supported scheme. Applicable to tpm2_testparams.

BUGS

Github Issues (https://github.com/tpm2-software/tpm2-tools/issues)

HELP

See the Mailing List (https://lists.01.org/mailman/listinfo/tpm2)