Red Hat Enterprise Linux Release 9.2 Manual Pages on 'tpm2_policyduplicationselect.1' command

$ man tpm2_policyduplicationselect.1

tpm2_policyduplicationselectGeneral Commands Matpm2_policyduplicationselect(1)

NAME

   tpm2_policyduplicationselect(1) - Restricts duplication to a specific

   new parent.

SYNOPSIS

   tpm2_policyduplicationselect [OPTIONS]

DESCRIPTION

   tpm2_policyduplicationselect(1) - Restricts duplication to a specific

   new parent.

OPTIONS

   ? -S, --session=FILE:

     The policy session file generated via the -S option to tpm2_star?

     tauthsession(1).

   ? -n, --object-name=FILE:

     Input name file of the object to be duplicated.

   ? -N, --parent-name=FILE:

     Input name file of the new parent.

   ? -L, --policy=FILE:

     File to save the policy digest.

   ? --include-object:

     If exists, the object name will be included in the value in policy

     digest.

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=?de?

vice:/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_TC?

TI=?mssim:host=localhost,port=2321?

? abrmd: For the abrmd TCTI, the configuration string format is a se?

ries 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.ex?

ample.FooBar:

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

Specify the default (abrmd) tcti and a config string of bus_type=ses?

sion:

\--tcti:bus_type=session

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

ules.

EXAMPLES

Setup a duplication role policy to restricted new parent

Create source parent and destination(or new) parent

tpm2_createprimary -C n -g sha256 -G rsa -c dst_n.ctx -Q

tpm2_createprimary -C o -g sha256 -G rsa -c src_o.ctx -Q

Create the restricted parent policy

tpm2_readpublic -c dst_n.ctx -n dst_n.name -Q

tpm2_startauthsession -S session.ctx

tpm2_policyduplicationselect -S session.ctx -N dst_n.name \

-L policydupselect.dat -Q

        tpm2_flushcontext session.ctx

        rm session.ctx

Create the object to be duplicated using the policy

        tpm2_create -C src_o.ctx -g sha256 -G rsa -r dupkey.priv -u dupkey.pub \

        -L policydupselect.dat -a "sensitivedataorigin|sign|decrypt" -c dupkey.ctx -Q

        tpm2_readpublic -c dupkey.ctx -n dupkey.name -Q

Satisfy the policy and duplicate the object

        tpm2_startauthsession -S session.ctx --policy-session

        tpm2_policyduplicationselect -S session.ctx -N dst_n.name -n dupkey.name -Q

        tpm2_duplicate -C dst_n.ctx -c dupkey.ctx -G null -p session:session.ctx \

        -r new_dupkey.priv -s dupseed.dat

        tpm2_flushcontext session.ctx

        rm session.ctx

NOTES

? This command usually cooperates with tpm2_duplicate(1), so referring

 to the man page of tpm2_duplicate(1) is recommended.

? This command will set the policy session?s command code to TPM_CC_Du?

 plicate which enables duplication role of the policy.

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.

Limitations

It expects a session to be already established via tpm2_startauthses?

sion(1) and requires one of the following:

? direct device access

? extended session support with tpm2-abrmd.

Without it, most resource managers will not save session state between

command invocations.

BUGS

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

HELP

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

tpm2-tools   tpm2_policyduplicationselect(1)