



Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'tpm2_policynameshash.1' command

\$ man tpm2_policynameshash.1

tpm2_policynameshash(1) General Commands Manual tpm2_policynameshash(1)

NAME

tpm2_policynameshash(1) - Couples a policy with names of specific objects.

SYNOPSIS

tpm2_policynameshash [OPTIONS]

DESCRIPTION

tpm2_policynameshash(1) - Couples a policy with names of specific objects. This is a deferred assertion where the hash of the names of all object handles in a TPM command is checked against the one specified in the policy.

OPTIONS

? -L, --policy=FILE:

File to save the compounded policy digest.

? -S, --session=FILE:

The policy session file generated via the -S option to tpm2_star? tpm2_star(1).

? -n, --name=FILE:

The file containing the name hash of the referenced objects.

References

COMMON OPTIONS

This collection of options are common to many programs and provide information 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 requested, the tool will provide errors from man on stderr. If the ?no-man? option is specified, or the manpager fails, the short options 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. Information 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 variable.

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 simulator.

tor.

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

? none - Do not initialize 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-option-config> results in the default being used for that portion respectively.

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 indicate 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 library 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_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

Restrict key duplication to specific new parent and specific duplicable

key.

Generate a duplicable object

```
openssl genrsa -out signing_key_private.pem 2048
```

```
openssl rsa -in signing_key_private.pem -out signing_key_public.pem -pubout
```

```
tpm2_loadexternal -G rsa -C o -u signing_key_public.pem -c signing_key.ctx \
```

```
-n signing_key.name
```

```
tpm2_startauthsession -S session.ctx -g sha256
```

```
tpm2_policyauthorize -S session.ctx -L authorized.policy -n signing_key.name
```

```
tpm2_policycommandcode -S session.ctx -L policy.dat TPM2_CC_Duplicate
```

```
tpm2_flushcontext session.ctx
```

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

The duplicable key

```
tpm2_create -Q -C primary.ctx -g sha256 -G rsa -r key.prv -u key.pub \  
-L policy.dat -a "sensitivedataorigin|sign|decrypt"  
tpm2_load -Q -C primary.ctx -r key.prv -u key.pub -c key.ctx
```

Create the new parent

```
tpm2_create -Q -C primary.ctx -g sha256 -G rsa -r new_parent.prv \  
-u new_parent.pub \  
-a "decrypt|fixedparent|fixedtpm|restricted|sensitivedataorigin"  
tpm2_loadexternal -Q -C o -u new_parent.pub -c new_parent.ctx
```

Modify the duplicable key policy to namehash policy to restrict parent and key

```
tpm2_readpublic -Q -c new_parent.ctx -n new_parent.name  
tpm2_readpublic -Q -c key.ctx -n key.name  
cat key.name new_parent.name | openssl dgst -sha256 -binary > name.hash  
tpm2_startauthsession -S session.ctx -g sha256  
tpm2_policynamehash -L policy.namehash -S session.ctx -n name.hash  
tpm2_flushcontext session.ctx  
openssl dgst -sha256 -sign signing_key_private.pem \  
-out policynamesignature policy.namehash  
tpm2_startauthsession -S session.ctx -g sha256  
tpm2_policyauthorize -S session.ctx -L authorized.policy -i policy.namehash \  
-n signing_key.name  
tpm2_policycommandcode -S session.ctx -L policy.dat TPM2_CC_Duplicate  
tpm2_flushcontext session.ctx
```

Satisfy the policy and attempt key duplication

```
tpm2_verifysignature -c signing_key.ctx -g sha256 -m policy.namehash \  
-s policynamesignature -t verification.tkt -f rsassa  
tpm2_startauthsession -S session.ctx --policy-session -g sha256  
tpm2_policynamehash -S session.ctx -n name.hash  
tpm2_policyauthorize -S session.ctx -i policy.namehash -n signing_key.name \  
-t verification.tkt  
tpm2_policycommandcode -S session.ctx TPM2_CC_Duplicate  
tpm2_duplicate -C new_parent.ctx -c key.ctx -G null -p "session:session.ctx" \  
-r dupprv.bin -s dupseed.dat
```

tpm2_flushcontext session.ctx

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_policynameshash(1)