Rocky Enterprise Linux 9.2 Manual Pages on command 'tpm2_nvreadpublic.1'

$ man tpm2_nvreadpublic.1

tpm2_nvreadpublic(1) General Commands Manual tpm2_nvreadpublic(1)

NAME

tpm2_nvreadpublic(1) - Display all defined Non-Volatile (NV)s indices.

SYNOPSIS

tpm2_nvreadpublic [OPTIONS]

DESCRIPTION

tpm2_nvreadpublic(1) - Display all defined Non-Volatile (NV)s indices

to stdout in a YAML format.

Display metadata for all defined NV indices. Metadata includes:

? The size of the defined region.

? The hash algorithm used to compute the name of the index.

? The auth policy.

? The NV attributes as defined in section ?NV Attributes?.

Example Output

0x1500015:

hash algorithm:

friendly: sha256

value: 0xB

attributes:

friendly: ownerwrite|ownerread

value: 0x2000200

size: 32

authorization policy:

0x1500017:

hash algorithm:

friendly: sha256

value: 0xB

attributes:

friendly: ownerwrite|ownerread

value: 0x2000200

size: 32

authorization policy:

OPTIONS

This tool takes no tool specific options.

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.

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.

NV Attributes

NV Attributes are used to control various properties of the NV defined

space. When specified as an option, either the raw bitfield mask or

?nice-names? may be used. The values can be found in Table 204 Part 2

of the TPM2.0 specification, which can be found here:

<https://trustedcomputinggroup.org/wp-content/uploads/TPM-

Rev-2.0-Part-2-Structures-01.38.pdf>

Nice names are calculated by taking the name field of table 204 and re?

moving the prefix TPMA_NV_ and lowercasing the result. Thus, TP?

MA_NV_PPWRITE becomes ppwrite. Nice names can be joined using the bit?

wise or ?|? symbol.

Note that the TPM_NT field is 4 bits wide, and thus can be set via nt=

format. For instance, to set The fields TPMA_NV_OWNERREAD, TP?

MA_NV_OWNERWRITE, TPMA_NV_POLICYWRITE, and TPMA_NT = 0x2, the argument

would be:

ownerread|ownerwrite|policywrite|nt=0x2

Additionally, the NT field, which denotes the type of the NV index, can

also be specified via friendly names: * ordinary - Ordinary contains

data that is opaque to the TPM that can only be modified using

TPM2_NV_Write. * extend - Extend is used similarly to a PCR and can

only be modified with TPM2_NV_Extend. Its size is determined by the

length of the hash algorithm used. * counter - Counter contains an

8-octet value that is to be used as a counter and can only be modified

with TPM2_NV_Increment * bits - Bit Field contains an 8-octet value to

be used as a bit field and can only be modified with TPM2_NV_SetBits.

* pinfail - PIN Fail contains an 8-octet pinCount that increments on a

PIN authorization failure and a pinLimit. * pinpass - PIN Pass con?

tains an 8-octet pinCount that increments on a PIN authorization suc?

cess and a pinLimit.

For instance, to set The fields TPMA_NV_OWNERREAD, TPMA_NV_OWNERWRITE, TPMA_NV_POLICYWRITE, and TPMA_NT = bits, the argument would be:

ownerread|ownerwrite|policywrite|nt=bits

EXAMPLES

List the defined NV indices to stdout

```
tpm2_nvreadpublic
```

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)