Rocky Enterprise Linux 9.2 Manual Pages on command 'tpm2_getekcertificate.1'

$ man tpm2_getekcertificate.1

tpm2_getekcertificate(1) General Commands Manual tpm2_getekcertificate(1)

NAME

tpm2_getekcertificate(1) - Retrieve the Endorsement key Certificate.

SYNOPSIS

tpm2_getekcertificate [OPTIONS] [ARGUMENT]

DESCRIPTION

tpm2_getekcertificate(1) - Retrieve the endorsement key certificate.

The certificate is present either on the TCG specified TPM NV indices

OR on the TPM manufacturer?s endorsement certificate hosting server.

Following are the conditions dictating the certificate location lookup.

1. NV-Index:

   Default search location when ARGUMENT is not specified.

2. Intel-EK-certificate-server:

   Search location when EK certificate could not be found in the NV

   index AND tpmEPSgenerated bit is CLEAR AND manufacturer is INTC.

3. Intel-EK-Re-certification-server:

   Search location when EK certificate could not be found in the NV

   index AND tpmEPSgenerated bit is SET AND manufacturer is INTC.

Note:

In this operation information is provided regarding additional software to be run as part of the re-provisioning/ re-certification service.

After re-provisioning/ recertification process is complete, EK cer? tificates can be read from the NV indexes by running another in? stance of tpm2_getekcertificate.

4. Generic or other EK-certificate-server:

Search location when ARGUMENT specifies the EK certificate web hosting address.

OPTIONS

? -o, --ek-certificate=FILE or STDOUT:

The file to save the Endorsement key certificate. When EK certifi? cates are found in the TPM NV indices, this option can be specified additional times to save the RSA and ECC EK certificates in order. The tool will warn if additional EK certificates are found on the TPM NV indices and only a single output file is specified. If the option isn?t specified all the EK certificates retrieved either from the manufacturer web hosting or from the TPM NV indices, are output to stdout.

? -X, --allow-unverified:

Specifies to attempt connecting with the TPM manufacturer provision? ing server without verifying server certificate. This option is ir? relevant when EK certificates are found on the TPM NV indices.

WARNING: This option should be used only on platforms with older CA certificates.

? -u, --ek-public=FILE:

Specifies the file path for the endorsement key public portion in tss format.

? -x, --offline:

This flags the tool to operate in an offline mode. In that the cer? tificates can be retrieved for supplied EK public that do not belong to the platform the tool is run on. Useful in factory provisioning

of multiple platforms that are not individually connected to the In?
ternet. In such a scenario a single Internet facing provisioning
server can utilize this tool in this mode. This forces the tool to
not look for the EK certificates on the NV indices.

? ?raw:
This flags the tool to output the EK certificate as is received from
the source: NV/ Web-Hosting.

? ARGUMENT the command line argument specifies the URL address for the
EK certificate portal. This forces the tool to not look for the EK
certificates on the NV indices.

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.

NOTES

When the verbose option is specified, additional curl debugging infor?
mation is provided by setting the curl mode verbose, see
<https://curl.haxx.se/libcurl/c/CURLOPT_VERBOSE.html> for more informa?
tion.

EXAMPLES

Retrieve EK certificate from TPM manufacturer backend by supplying EK pub?
lic.

```
tpm2_createek -G rsa -u ek.pub -c key.ctx
tpm2_getekcertificate -X -o ECcert.bin -u ek.pub \
https://tpm.manufacturer.com/ekcertserver/
```

Retrieve EK certificate from Intel backend if certificate not found on NV.

```
tpm2_createek -G rsa -u ek.pub -c key.ctx
tpm2_getekcertificate -X -o ECcert.bin -u ek.pub
```

Retrieve EK certificate from Intel backend for an offline platform.

```
tpm2_getekcertificate -X -x -o ECcert.bin -u ek.pub
```

Retrieve EK certificate from TPM NV indices only, fail otherwise.

```
tpm2_getekcertificate -o ECcert.bin
```

Retrieve multiple EK certificates from TPM NV indices only, fail otherwise.

```
tpm2_getekcertificate -o RSA_EK_cert.bin -o ECC_EK_cert.bin
```

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)