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 'tss2_quote.1' command

$ man tss2_quote.1

tss2_quote(1)   General Commands Manual   tss2_quote(1)

NAME

tss2_quote(1) -

SYNOPSIS

tss2_quote [OPTIONS]

SEE ALSO

fapi-config(5) to adjust Fapi parameters like the used cryptographic
profile and TCTI or directories for the Fapi metadata storages.

fapi-profile(5) to determine the cryptographic algorithms and parame?
ters for all keys and operations of a specific TPM interaction like the
name hash algorithm, the asymmetric signature algorithm, scheme and pa?
rameters and PCR bank selection.

DESCRIPTION

tss2_quote(1) - This command performs an attestation using the TPM.
The PCR bank for each provided PCR index and signing scheme are set in
the cryptographic profile (cf., fapi-profile(5)).

OPTIONS

These are the available options:

? -x, --pcrList=STRING:

An array holding the PCR indices to quote against.

? -Q, --qualifyingData=FILENAME or - (for stdin):

A nonce provided by the caller to ensure freshness of the signature.
Optional parameter.

? -l, --pcrLog=FILENAME or - (for stdout):

Returns the PCR log for the chosen PCR. Optional parameter.
PCR event logs are a list (arbitrary length JSON array) of log en?
tries with the following content.

- recnum: Unique record number
- pcr: PCR index
- digest: The digests
- type: The type of event. At the moment the only possible value is: "LINUX_IMA" (legacy IMA)
- eventDigest: Digest of the event; e.g. the digest of the measured file
- eventName: Name of the event; e.g. the name of the measured file.

? -f, --force:

Force overwriting the output file.

? -p, --keyPath=STRING:

Identifies the signing key.

? -q, --quoteInfo=FILENAME or - (for stdout):

Returns a JSON-encoded structure holding the inputs to the quote op?
eration. This includes the digest value and PCR values.

? -o, --signature=FILENAME or - (for stdout):

Returns the signature over the quoted material.

? -c, --certificate=FILENAME or - (for stdout):

The certificate associated with keyPath in PEM format. Optional pa?
rameter.

COMMON OPTIONS

This collection of options are common to all tss2 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 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.

EXAMPLE

```
                         tss2_quote   --keyPath=HS/SRK/quotekey   --pcrList="10,16"   --qualifyingData=qualifyingData.file
--signature=signature.file --pcrLog=pcrLog.file --certificate=certificate.file --quoteInfo=quoteInfo.info
```

RETURNS

0 on success or 1 on failure.

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 APRIL 2019 tss2_quote(1)