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

Rocky Enterprise Linux 9.2 Manual Pages on command 'tss2_verifyquote.1'

$ man tss2_verifyquote.1

tss2_verifyquote(1)   General Commands Manual   tss2_verifyquote(1)

NAME

tss2_verifyquote(1) -

SYNOPSIS

tss2_verifyquote [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_verifyquote(1) - This command verifies that the data returned by a

quote is valid. This includes

? Reconstructing the quoteInfo?s PCR values from the eventLog (if an

eventLog was provided)

? Verifying the quoteInfo using the signature and the publicKeyPath

The used signature verification scheme is specified in the cryptograph?

ic profile (cf., fapi-profile(5)).

An application using tss2_verifyquote() will further have to

? Assess the publicKey?s trustworthiness

? Assess the eventLog entries? trustworthiness

OPTIONS

These are the available options:

? -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 stdin):

Returns the PCR event 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.

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

The JSON-encoded structure holding the inputs to the quote operation.

This includes the digest value and PCR values.

? -k, --publicKeyPath=STRING:

Identifies the signing key. MAY be a path to the public key hierar?

chy /ext.

? -i, --signature=FILENAME or - (for stdin):

The signature over the quoted material.

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_verifyquote   --publicKeyPath="ext/myNewParent"   --qualifyingData=qualifyingData.file
--quoteInfo=quoteInfo.file --signature=signature.file --pcrLog=pcrLog.file
```

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_verifyquote(1)