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_makecredential.1' command

$ man tpm2_makecredential.1

```
tpm2_makecredential(1)      General Commands Manual      tpm2_makecredential(1)

NAME

       tpm2_makecredential(1)  -  Generate  the encrypted-user-chosen-data and

       the wrapped-secret-data-encryption-key for the  privacy-sensitive  cre?

       dentialing process of a TPM object.

SYNOPSIS

       tpm2_makecredential [OPTIONS]

DESCRIPTION

       tpm2_makecredential(1) - The TPM supports a privacy preserving protocol

       for distributing credentials for keys on a TPM.  The process guarantees

       that  the  credentialed-TPM-object(AIK)  is loaded on the same TPM as a

       well-known public-key-object(EK) without knowledge of the specific pub?

       lic  properties  of  the  credentialed-TPM-object(AIK).  The privacy is

       guaranteed  due  to  the  fact  that  only  the  name  of  the  creden?

       tialed-TPM-object(AIK)  is shared and not the credentialed-TPM-object?s

       public key itself.

       Make-credential is the first step in this process where  in  after  re?

       ceiving the public-key-object(EK) public key of the TPM and the name of

       the credentialed-TPM-object(AIK), an encrypted-user-chosen-data is gen?

       erated  and the secret-data-encryption-key is generated and wrapped us?

       ing cryptographic processes  specific  to  credential  activation  that

       guarantees  that  the credentialed-TPM-object(AIK) is loaded on the TPM

       with the well-known public-key-object(EK).
```

tpm2_makecredential can be used to generate the encrypted-user-cho?
sen-data and the wrapped secret-data-encryption-key without a TPM by
using the none TCTI option.

OPTIONS

? -e, --encryption-key=FILE:

DEPRECATED, use -u or ?public instead.

? -u, --public=FILE:

A TPM public key which was used to wrap the seed. NOTE: This option
is same as -e and is added to make it similar with other tools speci?
fying the public key. The old option is retained for backwards com?
patibility.

? -G, --key-algorithm=ALGORITHM:

The key algorithm associated with TPM public key. Specify either
RSA/ ECC. When this option is used, input public key is expected to
be in PEM format and the default TCG EK template is used for the key
properties.

? -s, --secret=FILE or STDIN:

The secret which will be protected by the key derived from the random
seed. It can be specified as a file or passed from stdin.

? -n, --name=FILE:

The name of the key for which certificate is to be created.

? -o, --credential-blob=FILE:

The output file path, recording the encrypted-user-chosen-data and
the wrapped secret-data-encryption-key.

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.

EXAMPLES

```
tpm2 createek -Q -c 0x81010009 -G rsa -u ek.pub
tpm2 createak -C 0x81010009 -c ak.ctx -G rsa -g sha256 -s rsassa -u ak.pub \
-n ak.name -p akpass> ak.out
file_size=`ls -l ak.name | awk {'print $5'}`
loaded_key_name=`cat ak.name | xxd -p -c $file_size`
tpm2 readpublic -c 0x81010009 -o ek.pem -f pem -Q
echo "12345678" | tpm2 makecredential -Q -u ek.pem -s - -n $loaded_key_name \
-o mkcred.out -G rsa
```

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)