## NAME

swtpm_cert − Tool to create EK and platform certs for swtpm (1.2 & 2.0)

## SYNOPSIS

**swtpm_cert [OPTIONS]**

## DESCRIPTION

**swtpm_cert** is a local CA tool for creating X.509v3 certificates for the TPM's Endorsement Key. The reason for this specific tool is that it works without access to the Endorsement Key's private key. Typically tools require either a self-signed certificate request or access to the private key to issue a certificate. This tool works with only the public key part.

The following options are supported:

**−−type {ek|platform}**
The type of certificate to create; by default an EK certificate is created.

**−−pubkey <filename>**
The public key (EK) in PEM format.

**−−modulus <hex digits>**
The modulus of the public key as a string of hex digits. This option can be used in place of the −−pubkey option.

**−−ecc−x <hex digits>**
The elliptic curve parameter x as string of hex digits.

**−−ecc−y <hex digits>**
The elliptic curve parameter y as string of hex digits.

**−−ecc−curveid <curve id>**
The elliptic curve's id. secp256r1, secp384r1, and secp521r1 are supported. If this option is not given, secp256r1 is assumed.

**−−exponent <exponent>**
The exponent of the public key. By default 0x10001 is assumed.

**−−signkey <filename>**
The key used for signing the certificate. The file must be in PEM format.

**−−signkey−password <password>**
Optional password for the signing key.

**−−signkey−pwd <pwd>**
This is an alternative option for passing the signing key password. The following formats are supported for *pwd*:

```
 − <password>                    : direct password
 − pass:<password>               : direct password
 − file:<filename>               : password in file
 − fd:<file descriptor>          : read password from file descriptor
 − env:<environment variable>    : read password from env. variable
```

All passwords read from files and file descriptors must be a maximum of 255 bytes (plus one byte for terminating NUL byte).

**−−parentkey−password <password>**
Optional password for a parent key. In case a TPM key is used for signing this would be the password for the TPM's storage root key (SRK).

**−−parentkey−pwd <pwd>**
This is an alternative option for passing the parentkey password. See the description above for supported *pwd* formats.

**−−issuercert <filename>**
The X.509 certificate of this signer that takes on the role of a local CA.

**−−out−cert <filename>**
The name of the file to write the X.509v3 certificate into. The output will be in PEM format.

**−−serial <serial number>**
Optional 32bit serial number for the certificate.

**−−days <number>**
The number of days the certificate is valid; by default it is valid for 365 days.

**−−pem**
Write the resulting certificate in PEM format; DER format is the default.

**−−tpm−manufacturer <name>**
The name of the TPM manufacturer.

**−−tpm−model <model>**
The TPM model (part number).

**−−tpm−version <version>**
The TPM's firmware version.

**−−platform−manufacturer <name>**
The name of the platform manufacturer.

**−−platform−model <model>**
The platform model.

**−−platform−version <version>**
The platform's version.

**−−subject <subject>**
Subject to for example provide the location of the TPM in the format of C=<country>,ST=<state>,L=<location>. Note that the location must no contain any spaces.

**−−tpm2**
Issue TPM 2 compliant certificates.

**−−allow−signing**
Create an EK that can also be used for signing. Without this option, the EK can only be used for key encipherment. This option requires −−tpm2.

**−−decryption**
If −−allow−signing is passed and the EK should also be useable for key encipherment, this option must be passed. Otherwise key encipherment is the default. This option requires −−tpm2.

**−−print−capabilities** (since v0.3)
Print capabilities that were added to swtpm_cert after version 0.2. The output may contain the following:

```
{
  "type": "swtpm_cert",
  "features": [
    "cmdarg−signkey−pwd",
    "cmdarg−parentkey−pwd"
  ]
}
```

The maining of the feature verbs is as follows:

**cmdarg-signkey-pwd**
The *−−signkey−pwd* option is supported.

**cmdarg-parentkey-pwd**

The *−−parentkey−pwd* option is supported.

**−−help, −h**

Display the help screen

## SEE ALSO

## REPORTING BUGS

Report bugs to Stefan Berger <stefanb@linux.vnet.ibm.com>