NAME

swtpm−localca − Local CA to create EK and platform certs for swtpm

SYNOPSIS

swtpm-localca [OPTIONS]

DESCRIPTION

swtpm-localca is a tool to create TPM Endorsement Key (EK) and platform certificates on the host. It uses the *swtpm_cert* program to create the certificates.

The program will typically be invoked by the *swtpm_setup* program that uses the */etc/swtpm_setup.conf* configuration file where a variable needs to be set that points to this program. It implements command line options that the *swtpm_setup* program uses to provide the necessary parameters to it.

swtpm-localca will automatically try to create the signing key and certificate if the configuration points to a missing signing key. Since this certificate must be signed by a CA, a root certificate authority will also be created and will sign this certificate. The root CA's private key and certificate will be located in the same directory as the signing key and have the names swtpm−localca−rootca−privkey.pem and swtpm−localca−rootca−cert.pem respectively. The environment variable SWTPM_ROOTCA_PASSWORD can be set for the password of the root CA's private key.

The following options are supported:

−−type type
: This parameter indicates the type of certificate to create. The type parameter may be one of the following: *ek*, or *platform*

−−dir dir
: This parameter indicates the directory into which the certificate is to be stored. The EK certificate is stored in this directory under the name ek.cert and the platform certificate under the name platform.cert.

−−ek ek
: This parameter indicates the modulus of the public key of the endorsement key (EK). The public key is provided as a sequence of ASCII hex digits.

  In case ECC (elliptic curve crypography) keys are used, the parameter must have the format −−ek x=<hex digits>,y=<hex digits>,id=<curve id>. The id=<curve id> part is optional and only necessary for ECC curves other than secp256r1.

−−vmid ID
: This parameter indicates the ID of the VM for which to create the certificate.

−−logfile <logfile>
: The log file to log output to; by default logging goes to stdout and stderr on the console.

−−configfile <configuration file>
: The configuration file to use. If omitted, the default configuration file */etc/swtpm−localca.conf* will be used.

−−optsfile <options file>
: The options file to use. If omitted, the default options file */etc/swtpm−localca.options* will be used.

−−tpm−spec−family, **−−tpm−spec−revision**, **−−tpm−spec−level**
: TPM specification parameters that describe the specification that was followed for the TPM implementation. The parameters will be passed to swtpm_cert for the creation of the EK certificate.

−−tpm2
: Create 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.

SEE ALSO

swtpm−localca.conf, **swtpm−localca.options**, **swtpm_setup**, **swtpm_setup.conf**

REPORTING BUGS

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