NAME

swtpm_bios − BIOS simulation tool for swtpm

SYNOPSIS

swtpm_bios [OPTIONS]

DESCRIPTION

swtpm_bios is a tool that can send the commands to the TPM (*swtpm* program) that typically are used by the BIOS to initialize the TPM. The user can choose among several command line options to choose the state the TPM should be set to.

This command requires the environment variable *TCSD_USE_TCP_DEVICE* to be set for communication via TCP. Otherwise it will use the device set in the environment variable *TPM_DEVICE* or fall back to use */dev/tpm0* to send the commands to. In TCP mode, the environment variable *TCSD_TCP_DEVICE_HOSTNAME* is used to indicate the host to send the commands to. By default *localhost* is assumed. The default TCP port is 6545 unless the environment variable *TCSD_TCP_DEVICE_PORT* indicates another port.

In case of success 0 will be returned. In case a TPM error was encountered the return code will be 128. In case of communcation failure 255 is returned. In case the TPM needs to be reset to become activated, 129 will be returned.

This command will send the following sequence of commands to the TPM.

TPM_Startup(chosen mode) — startup TPM
TSC_PhysicalPresence(0x20) — PhysicalPresenceCMDEnable
TSC_PhysicalPresence(0x08) — turn on physical presence
TPM_GetCapability — get permanent flags
TPM_PhysicalEnable — enable the TPM
TPM_PhysicalSetDeactivated(0x0) — activate TPM
TPM_ContinueSelfTest — continue self test
TSC_PhysicalPresence(0x20) — PhysicalPresenceCMDEnable
TSC_PhysicalPresence(0x14) — turn off physical presence & lock it

The following options are supported:

−−tpm−device <device>
Use the given device rather than the default /dev/tpm0. This option overrides the TPM_DEVICE environment variable.

−−tcp <server>:<port>
Connect to the given server and port; if no server is given, 127.0.0.1 is used; if port is not given, the default port 6545 is used.

−−unix <path>
Connect to the given UnixIO path.

−tpm2
The device is a TPM 2.

−c Send TPM_Startup(ST_CLEAR) (default). This instructs the TPM to start with clear state.

−s Send TPM_Startup(ST_STATE). This instructs the TPM to start by restoring previously saved state.

−d Send TPM_Startup(ST_DEACTIVATED). This instructs the TPM to start in deactivated mode. This option has no effect on a TPM 2.

−n Don’t send a TPM_Startup command.

−o Only send the startup command and nothing else.

−ea
Make sure that the TPM is activated; if the TPM requires a reset, the program will exist and return a return code of 129.

−cs Send a TPM_ContinueSelfTest command to a TPM 1.2 and a TPM2_IncrementalSelfTest command to a TPM 2.

−u Give up physical presence on a TPM 1.2. In case of a TPM 2 set the platform hierarchy to a random password.

−v Display version and exit.

−h Display the help screen and exit.

SEE ALSO

REPORTING BUGS

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