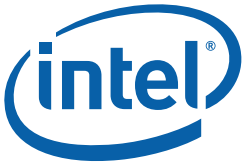


Intel® Trusted Execution Technology – Launch Control Policy

Linux Tools User Manual

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

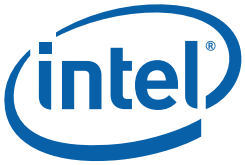
Intel may make changes to specifications and product descriptions at any time, without notice. The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

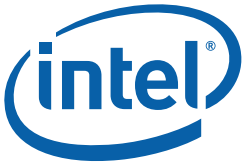
Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's website at http://www.intel.com.



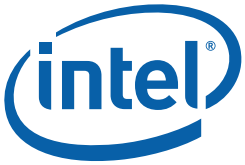
Contents



1 Introduction

In order for Intel® Trusted Execution Technology (Intel® TXT) Launch Control Policy (LCP) to function, the Platform Owner needs the ability to establish a policy on the platform. The LCP Tools described in this document allow end-users to create policies and provision a TPM with the policies.

This document does not describe the Intel® TXT Launch Control Policy functionality. That will be provided in a separate specification to be released shortly.



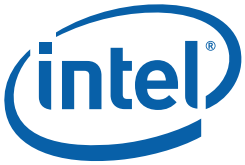
2 Commands

2.1 Pre-requisites

In order to run the tpmnv_* commands, a TPM driver and TSS (TPM Software Stack) must be loaded.

On Linux versions after 2.6.17, the tpm_tis v1.2 TPM driver should be available. It should be loaded as 'modprobe tpm_tis', but in some cases that does not work and it is required to be loaded as 'modprobe tpm_tis force=1 interrupts=0'.

The TSS used does not need to be fully v1.2 compliant but it must at least support the TPM NV (TPM non-volatile memory) commands (Tspi_NV_*). The latest (CVS) version of the TrouSerS TSS has this support.



2.2 tpmnv_defindex

Function:

This command is used to define the TPM NV index where the LCP policies are stored. This command can also be used to define non-LCP TPM NV indices.

Usage:

tpmnv_defindex -i index [-s size] [-pv permission_value] [-p password]

[-av authentication_value] [-wl write_locality]

[-rl read_locality] [-h]

Options:

-i index: UINT32 or String, the index value to define

3 strings are supported for the reserved LCP indices. Strings and default index values for each string are:

"default": 0x50000001 (INDEX_LCP_DEF),

"owner": 0x40000001 (INDEX_LCP_OWN),

"aux": 0x50000002 (INDEX_LCP_AUX)

-pv permission: UINT32, the permission value of the index

Default permission value for indices:

INDEX_LCP_DEF: 0x00002000;

INDEX_LCP_OWN: 0x00000002;

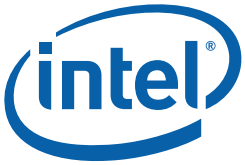
INDEX_LCP_AUX: 0x00000000.

This is optional for the above indices but required for others.

-s data size: UNIT32, the size of the index

Default value for indices:

INDEX_LCP_DEF: 34 bytes;



INDEX_LCP_OWN: 34 bytes;

NDEX_LCP_AUX: 64 bytes.

This is optional for the above indices but required for others.

-av auth value: string, the authentication value for this index

Authentication value for the defined index; it is the password for the NV if the permission is AUTHWRITE or AUTHREAD.

-p password: string, the TPM owner password

-wl write_locality: UINT8, the write locality attributes for this index

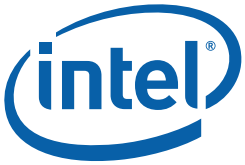
-rl read_locality: UINT8, the read locality attributes for this index

-h help, print help message

Examples:

tpmnv_defindex –i 0x00011101 –pv 0x4 –s 34 –av 123456 –p 123456

tpmnv_defindex –i aux



2.3 tpmnv_relindex

Function:

This command is used to release a previously-defined index. This command only can be used by TPM owner.

Usage:

tpmnv_relindex -i index -p passwd [-h]

Options:

-i index: UINT32 or String, the index value for releasing

3 strings are supported for the reserved LCP indices. Strings and default index values for each string are:

“default”: 0x50000001 (INDEX_LCP_DEF),

”owner”: 0x40000001 (INDEX_LCP_OWN),

“aux”: 0x50000002 (INDEX_LCP_AUX)

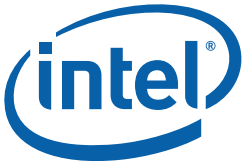
-p password: string, the TPM owner password

-h help, print help message

Examples:

tpmnv_reldndex –i 0x00011101 –p 123456

tpmnv_defindex –h



2.4 tpmnv_lock

Function:

This command will lock the TPM NV. This command is specifically used by platform manufacturers once the platform personalization process is complete. TPM NV lock is a one-way operation: after locking the TPM NV cannot be unlocked.

Usage:

tpmnv_lock [-f] [-h]

Options:

-f force

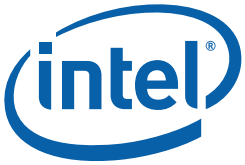
Lock the TPM NV without warning.

-h help

Print out the help message.

Examples:

tpmnv_lock –f



2.5 tpmnv_getcap

Function:

Display the either the list of defined TPM NV indices or the attributes and contents of a specified index.

Usage:

tpmnv_getcap [-i index_value] [-h]

Options:

-i index value: UINT32 or String

3 strings are supported for the reserved LCP indices. Strings and default index values for each string are:

"default": 0x50000001(INDEX_LCP_DEF),

"owner": 0x40000001(INDEX_LCP_OWN),

"aux": 0x50000002(INDEX_LCP_AUX)

If this option is specified, then the public data of the index will be displayed.

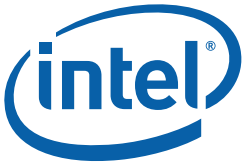
-h help

Print out the help message.

Examples:

tpmnv_getcap –i 0x00011101

tpmnv_getcap



2.6 lcp_crtpconf

Function:

Create a platform configuration measurement. The produced platform configuration measurement will be appended to the input file in binary mode.

Usage:

lcp_crtpconf -p PCR_index1,PCR_index2,...,PCR_indexn [-f filename] [-h]

Options:

-p PCR_index1,PCR_index2,...,PCR_indexN

Index values can be 0-23.

-f file_name: string

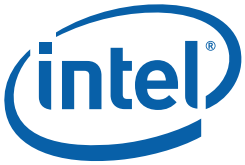
File name to which the measurement is appended.

-h help

Print out the help message.

Examples:

lcp_crtpconf –p 0,1,2,3 –f pconf_file



2.7 lcp_crtpol

Function:

The command is used to create an LCP policy (and optionally policy data), which can later be written to the TPM.

Usage:

lcp_crtpol -t policy_type [-a hashalg] [-v version] [-sr SINIT revocation_counter]

[-s srtm_file] [-m mle_file] [-o policyfile] [-b policydata_file]

[-pcf Policy_Control_Field] [-h]

Options:

-t Policy type: UINT8 or string

5 strings are supported for the reserved LCP Policy Types. Strings and default policy type values for each string are:

"hashonly": 0 (POLTYPE_HASHONLY)

"unsigned": 1 (POLTYPE_ UNSIGNED)

"any": 3 (POLTYPE_ ANY)

"forceowner": 4 (POLTYPE_ FORCEOWNERPOLICY)

-a Algorithm: UINT8 or string

Currently we only support SHA-1 algorithm: POLHALG_SHA1(0 or "sha1").

-v Version: UINT8

Version number. Currently it must be set to 0 if specified.

-s PConf file name: String

File name of the Platform Configuration data, as produced by lcp_crtpconf.

-m MLE file name: String

File name of file containing MLE hash values. This is a text file that contains one SHA-1 hash per line. The values of the hash must be hexadecimal values,

specified either a single un-deliminated set or as space-delimited two-character (i.e. one byte) values. This can be produced by the lcp_mlehash command.

-o policy file name: String

File name to store the output policy.

-b policy_data file name: String

File name to store the LCP Policy data.

-sr SINIT Revocation count number: UINT8

-pcf policy control field: UINT32

-h help.

Print out the help message.

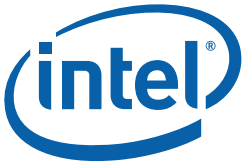
Examples:

lcp_crtpol –t 0 –r 0,0,0 –m mle_file –o policy_hashonly_file

lcp_crtpol –t 1 –m mle_file –s pconf_file –o policy_unsigned_file –b policy_data_file

lcp_crtpol –t 3 –o policy_any_file

lcp_crtpol –t unsigned –a sha1 –m mle_file –s pconf_file –o policy_unsigned_file –b policy_data_file



2.8 lcp_writepol

Function:

The command is used to write LCP Policy into a (previously-defined) TPM NV index. It also supports writing arbitrary data into a specified index.

Usage:

lcp_writepol -i index_value [-f policy_file] [-p passwd] [-e] [-h]

Options:

-i index: UINT32 or String. Index for writing

3 strings are supported for the reserved LCP indices. Strings and default index values for each string are:

"default": 0x50000001(INDEX_LCP_DEF),

"owner": 0x40000001(INDEX_LCP_OWN),

"aux": 0x50000002(INDEX_LCP_AUX)

-f file_name: string

File name of where the policy data is stored. Mutually exclusive with –e option.

-p password: string, the TPM owner password

-e: write 0 length data to the index

This is useful for special indices, such as those whose permission is WRITEDFINE. Mutually exclusive with –f option.

-h help

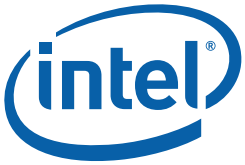
Print out the help message.

Examples:

lcp_writepol –i default –f policy_file

lcp_writepol –i 0x00011101 –e

lcp_writepol –i 0x00011101 –f policy_file –p 123456



2.9 lcp_readpol

Function:

The command is used to read the contents of an LCP policy index. Any index can be specified but the output will be parsed as if it contained a policy.

Usage:

lcp_readpol -i index_value [-f output_file] [-s size] [-p passwd] [-h]

Options:

-i index: UINT32 or String. Index for reading

3 strings are supported for the reserved LCP indices. Strings and default index values for each string are:

"default": 0x50000001(INDEX_LCP_DEF),

"owner": 0x40000001(INDEX_LCP_OWN),

"aux": 0x50000002(INDEX_LCP_AUX)

-f file_name: string

File name to write the policy data to. If no file name is specified then the contents will be displayed.

-s size to read: UINT32

Value size to read from NV store. If no size inputted, read by length as this index defined.

-p password: string, the TPM owner password

-h help

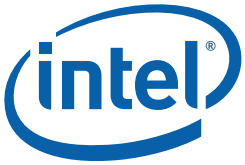
Print out the help message.

Examples:

lcp_readpol –i default –f policy_file

lcp_readpol –i 0x00011101 –s 10

lcp_readpol –i 0x00011101 –f policy_file –p 123456



2.10 lcp_mlehash

Function:

The command is used to generate a SHA-1 hash of the portion of an executable file that contains the Intel® TXT measured launched environment (MLE). In the MLE binary file, the portion of the file to be used as the MLE is specified in the MLE header structure. If verbose mode is not used, the output is suitable for use as the mle_file to the lcp_crtpol command.

Usage:

lcp_mlehash [-h] [-v] mle_file

Options:

mle_file: string

File name of the MLE binary. If it is a gzip file then it will be un-zip'ed before hashing.

-v

Verbose mode.

-h help

Print out the help message.

Examples:

lcp_mlehash sboot.gz