Advantech ENPD product FAQ

A. How to test NAMB-3260TPM2.0 in Linux

Applicable model list	NAMB-3260TPM2.0 (Chip: SLB9665TT20)
Model name version	N/A
BIOS Version	N/A

Description

Following step is TPM 2.0 module test, and please use CentOS 7.5 (kernel :3.10.0-862.9.1.el7.x86_64) or later and refer following step to test NAMB-3260TPM 2.0 module

1. Please check TPM 2.0 BIOS setting, it needs enable TPM function (TPM20 Device Found)

2. Following command is Checking Linux to detect TPM module or not , it needs report following string when system had installed TPM 2.0 module

```
[root@1012 ~]# dmesg | grep -i tpm

[      0.000000] ACPI: TPM2 000000007e3a55d0 00034 (v03 ALASKA    A M I    00000001

AMI    00000000)

[      3.068547] tpm_tis MSFT0101:00: 2.0 TPM (device-id 0x1A, rev-id 16)
```

3. Advantech TPM 2.0 module is Infineon SLB9665TT20, it needs using following utility to simple check NAMB-3260TPM2.0 module

Infineon Embedded Linux TPM Toolbox 2 (ELTT2) for TPM 2.0
https://github.com/Infineon/eltt2

Please refer following step to download ELTT2 & compile this utility

```
# git clone https://github.com/Infineon/eltt2

Cloning into 'eltt2'...

remote: Counting objects: 215, done.

remote: Total 215 (delta 0), reused 0 (delta 0), pack-reused 215

Receiving objects: 100% (215/215), 840.56 KiB | 320.00 KiB/s, done.

Resolving deltas: 100% (129/129), done.

# cd eltt2/

# ls

eltt2.c    eltt2.h    License.txt    Makefile    README.md    README.txt

# make

gcc -Wall -Wextra -std=c99 -g eltt2.c -o eltt2
```

Please refer following step to simple test TPM2.0 module, and please key-in "./eltt2 –h" to look detail description.

```
# ./eltt2 -g

(Get fixed capability values)



TPM capability information of fixed properties:
```

```
================================================================

TPM_PT_FAMILY_INDICATOR:          2.0

TPM_PT_LEVEL:                     0

TPM_PT_REVISION:                  99

TPM_PT_DAY_OF_YEAR:               206

TPM_PT_YEAR:                      2013

TPM_PT_MANUFACTURER:              IFX

TPM_PT_VENDOR_STRING:             SLB9665

TPM_PT_VENDOR_TPM_TYPE:           1

TPM_PT_FIRMWARE_VERSION:          5.0.1089.2


TPM_PT_MEMORY:

================================================================

Shared RAM:                       0 CLEAR

Shared NV:                        1 SET

Object Copied To Ram:             1 SET


TPM_PT_PERMANENT:

================================================================

Owner Auth Set:                   0 CLEAR

Sendorsement Auth Set:            0 CLEAR
```

Lockout Auth Set: 0 CLEAR

Disable Clear: 0 CLEAR

In Lockout: 0 CLEAR

TPM Generated EPS: 0 CLEAR

./eltt2 -t full

(SelfTest full type)

Successfully tested. Works as expected.

./eltt2 -a 31323334

(Hash Sequence SHA-1 test)

TPM2_HashSequenceStart of '31323334' with SHA-1:

TPM Response:

80 01 TPM TAG

00 00 00 0E RESPONSE SIZE

00 00 00 00 RETURN CODE

Command-specific response Data:

80 00 00 00

TPM2_SequenceUpdate:

TPM Response:

80 02 TPM TAG

00 00 00 13 RESPONSE SIZE

00 00 00 00 RETURN CODE

Command-specific response Data:

00 00 00 00 00 00 01 00 00

TPM2_SequenceComplete:

TPM Response:

80 02 TPM TAG

00 00 00 31 RESPONSE SIZE

00 00 00 00 RETURN CODE

Command-specific response Data:

00 00 00 1E 00 14 71 10 ED A4

D0 9E 06 2A A5 E4 A3 90 B0 A5

72 AC 0D 2C 02 20 80 24 40 00

00 07 00 00 00 00 01 00 00

Hash value extracted from TPM response:

```
0x00000000:  71  10  ED  A4  D0  9E  06  2A

0x00000008:  A5  E4  A3  90  B0  A5  72  AC

0x00000010:  0D  2C  02  20
```