Step.1

Please install Intel SGX PSW for Windows v1.7.100.35600

After install , you will found intel SGX driver on below folder

```
C:\Program Files\Intel\IntelSGXPSW
```

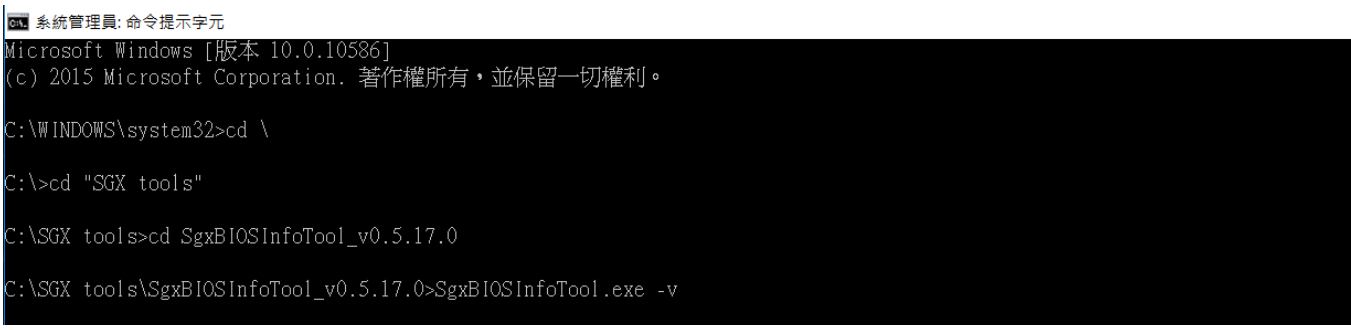
Step.2 Put SGX tool folder in C:\

Step.3

Run CMD as administer and enter to SGX tool folder

Enter into SGXBiosInfoTool_v0.5.17.0 folder

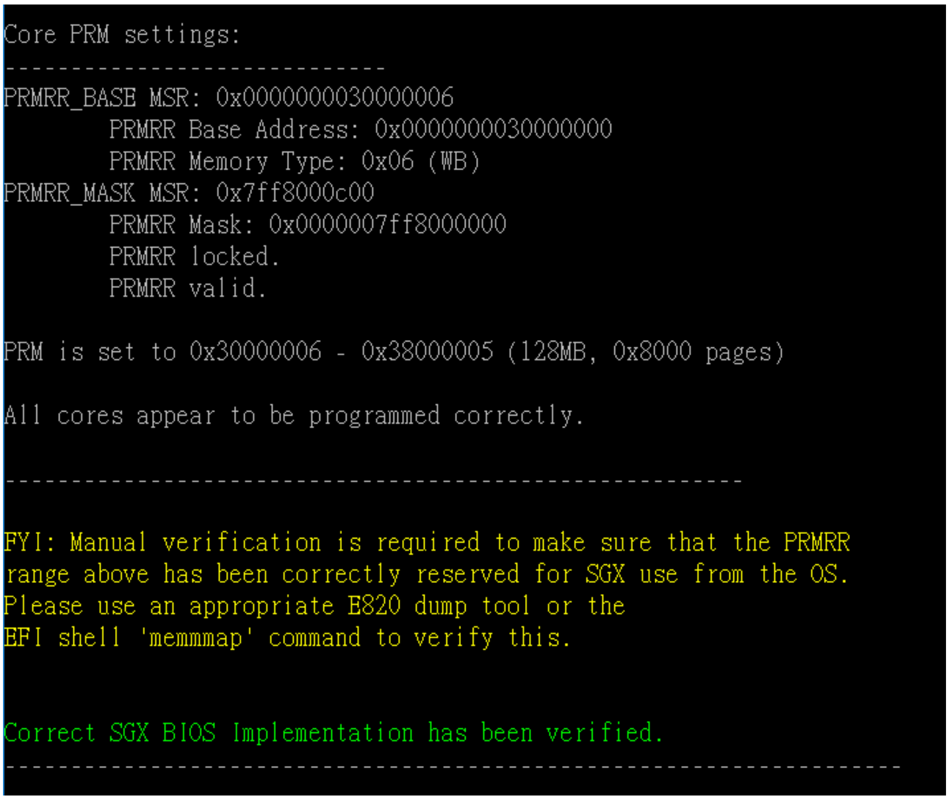
Run command “SgxBIOSInfotool.exe –v”



```
Microsoft Windows [版本 10.0.10586]
(c) 2015 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\WINDOWS\system32>cd \

C:\>cd "SGX tools"

C:\SGX tools>cd SgxBIOSInfoTool_v0.5.17.0

C:\SGX tools\SgxBIOSInfoTool_v0.5.17.0>SgxBIOSInfoTool.exe -v
```

Step.4

You will see below information to check whether system   support SGX function.



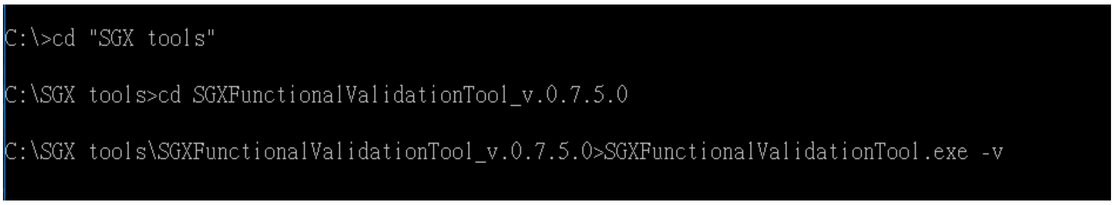
```
Core PRM settings:
-----------------------------
PRMRR_BASE MSR: 0x0000000030000006
        PRMRR Base Address: 0x0000000030000000
        PRMRR Memory Type: 0x06 (WB)
PRMRR_MASK MSR: 0x7ff8000c00
        PRMRR Mask: 0x0000007ff8000000
        PRMRR locked.
        PRMRR valid.

PRM is set to 0x30000006 - 0x38000005 (128MB, 0x8000 pages)

All cores appear to be programmed correctly.

-------------------------------------------------------

FYI: Manual verification is required to make sure that the PRMRR
range above has been correctly reserved for SGX use from the OS.
Please use an appropriate E820 dump tool or the
EFI shell 'memmmap' command to verify this.


Correct SGX BIOS Implementation has been verified.
-------------------------------------------------------------------
```

Step 5.

Back to SGXFunctionalValidationTool_v.0.7.5.0 folder

And key in below command

“SGXFunctionalValidationTool_v.0.7.5.0.exe –v ”

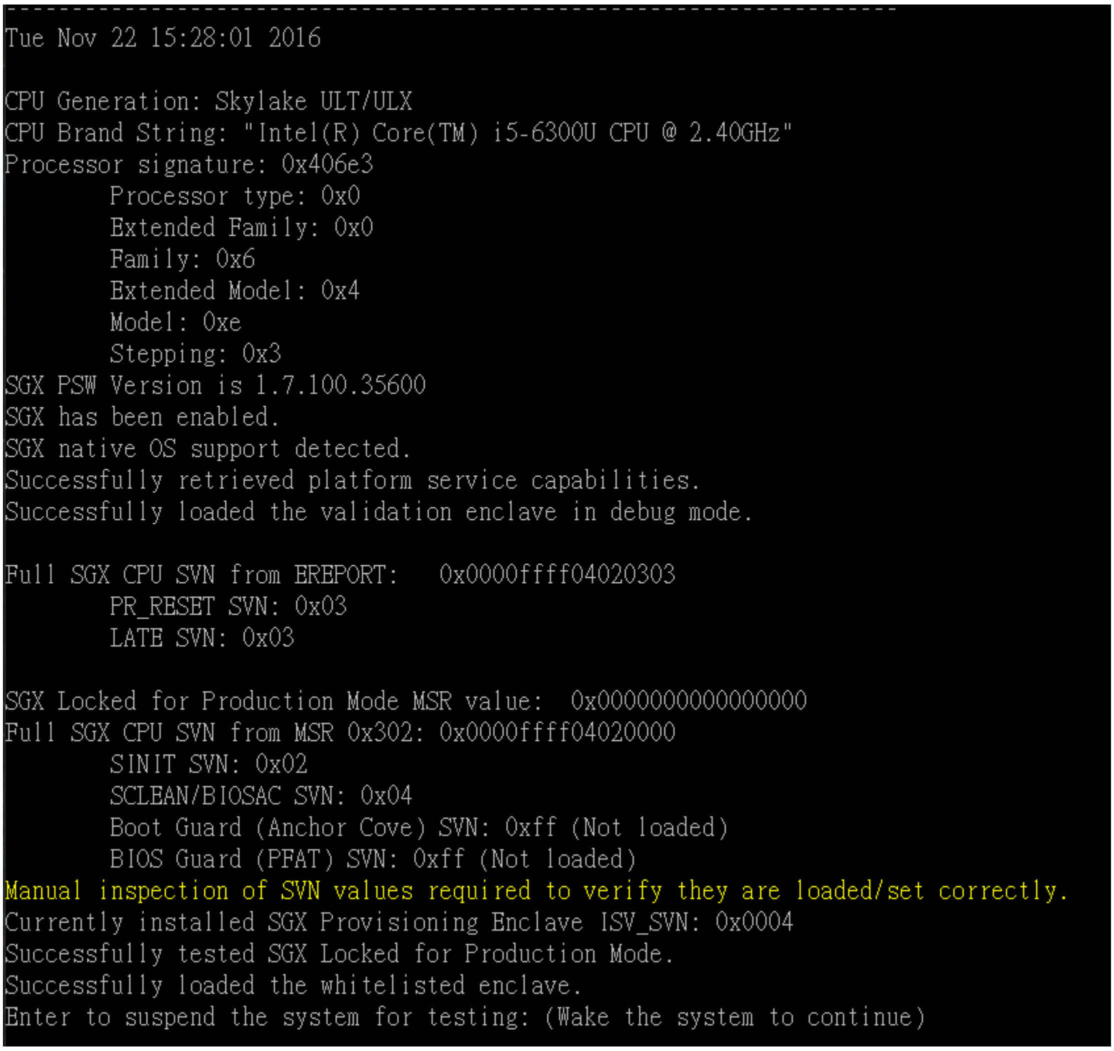


```
C:\>cd "SGX tools"

C:\SGX tools>cd SGXFunctionalValidationTool_v.0.7.5.0

C:\SGX tools\SGXFunctionalValidationTool_v.0.7.5.0>SGXFunctionalValidationTool.exe -v
```

Step.6

You will see “Enter to resume” request, please press Enter key to run process

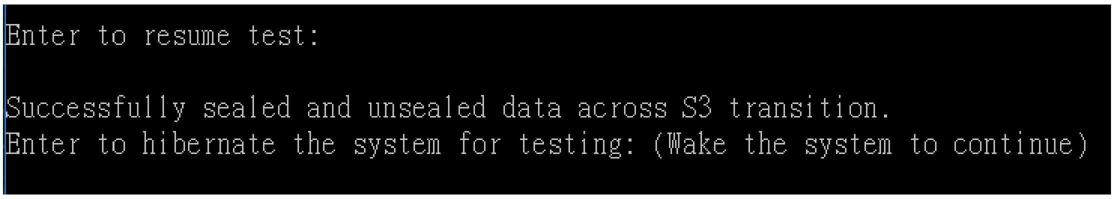
System will enter to S3 and then please resume system from S3 by press any key



```
-------------------------------------------------------------------
Tue Nov 22 15:28:01 2016

CPU Generation: Skylake ULT/ULX
CPU Brand String: "Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz"
Processor signature: 0x406e3
        Processor type: 0x0
        Extended Family: 0x0
        Family: 0x6
        Extended Model: 0x4
        Model: 0xe
        Stepping: 0x3
SGX PSW Version is 1.7.100.35600
SGX has been enabled.
SGX native OS support detected.
Successfully retrieved platform service capabilities.
Successfully loaded the validation enclave in debug mode.

Full SGX CPU SVN from EREPORT:   0x0000ffff04020303
        PR_RESET SVN: 0x03
        LATE SVN: 0x03

SGX Locked for Production Mode MSR value:  0x0000000000000000
Full SGX CPU SVN from MSR 0x302: 0x0000ffff04020000
        SINIT SVN: 0x02
        SCLEAN/BIOSAC SVN: 0x04
        Boot Guard (Anchor Cove) SVN: 0xff (Not loaded)
        BIOS Guard (PFAT) SVN: 0xff (Not loaded)
Manual inspection of SVN values required to verify they are loaded/set correctly.
Currently installed SGX Provisioning Enclave ISV_SVN: 0x0004
Successfully tested SGX Locked for Production Mode.
Successfully loaded the whitelisted enclave.
Enter to suspend the system for testing: (Wake the system to continue)
```

Step.7

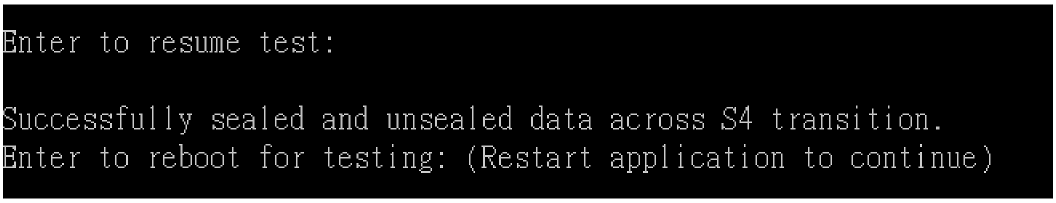
After resume from S3 , You will see “Successfully …across S3 and Enter to Hibernate” request, please press Enter key to run process , System will enter to S4 and then please resume system from S3 by press power button



```
Enter to resume test:

Successfully sealed and unsealed data across S3 transition.
Enter to hibernate the system for testing: (Wake the system to continue)
```

Step.8

After resume from S4 , You will see “Successfully …across S4 and Enter to reboot” request, please press Enter key to run process , System will run reboot process

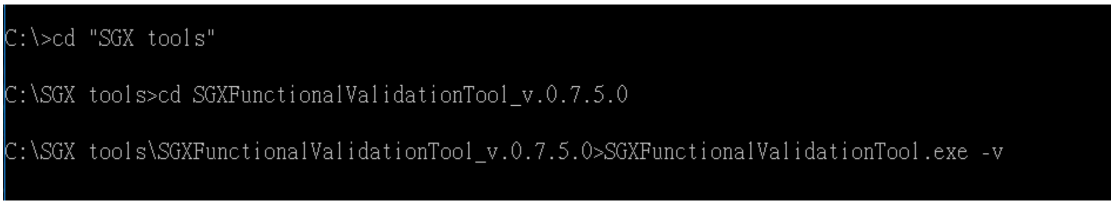


```
Enter to resume test:

Successfully sealed and unsealed data across S4 transition.
Enter to reboot for testing: (Restart application to continue)
```

Step.9

After system reboot , please re- run CMD as administer and enter to SGXFunctionalValidationTool_v.0.7.5.0 folder r

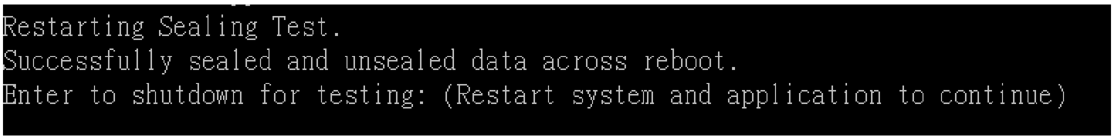
And run command “SGXFunctionalValidationTool_v.0.7.5.0.exe –v ”



```
C:\>cd "SGX tools"

C:\SGX tools>cd SGXFunctionalValidationTool_v.0.7.5.0

C:\SGX tools\SGXFunctionalValidationTool_v.0.7.5.0>SGXFunctionalValidationTool.exe -v
```

Step.10

You will see “Successfully …across reboot and Enter to reboot” request, please press Enter key to run process , System will run shutdown process



```
Restarting Sealing Test.
Successfully sealed and unsealed data across reboot.
Enter to shutdown for testing: (Restart system and application to continue)
```

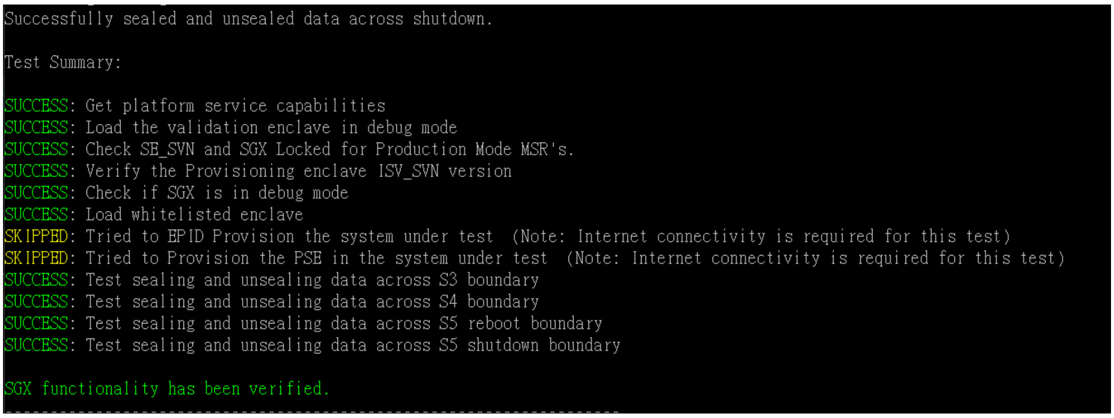
Step.11

Press power button let system resume from shutdown , please re- run CMD as administer and enter to SGXFunctionalValidationTool_v.0.7.5.0 folder r

And run command “SGXFunctionalValidationTool_v.0.7.5.0.exe –v ”

You will see “Successfully …across shutdown” and tool will list you SGX test summary

Please capture your test summary to DQM, the test result can’t show red , and yellow test result need confirm with DQM.



```
Successfully sealed and unsealed data across shutdown.

Test Summary:

SUCCESS: Get platform service capabilities
SUCCESS: Load the validation enclave in debug mode
SUCCESS: Check SE_SVN and SGX Locked for Production Mode MSR's.
SUCCESS: Verify the Provisioning enclave ISV_SVN version
SUCCESS: Check if SGX is in debug mode
SUCCESS: Load whitelisted enclave
SKIPPED: Tried to EPID Provision the system under test  (Note: Internet connectivity is required for this test)
SKIPPED: Tried to Provision the PSE in the system under test  (Note: Internet connectivity is required for this test)
SUCCESS: Test sealing and unsealing data across S3 boundary
SUCCESS: Test sealing and unsealing data across S4 boundary
SUCCESS: Test sealing and unsealing data across S5 reboot boundary
SUCCESS: Test sealing and unsealing data across S5 shutdown boundary

SGX functionality has been verified.
-------------------------------------------------------------------
```