**Intel SGX BiosInfoTool & FVT Test SOP**

**(Note: secure boot should not be disabled and anti-virus does not need to disable)**

**Prerequisite:**

Install Intel SGX PSW for Windows latest version

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

C:\Program Files\Intel\IntelSGXPSW

**Run SgxBiosInfoTool Ver.0.5.21.0 or later**

Step 1:

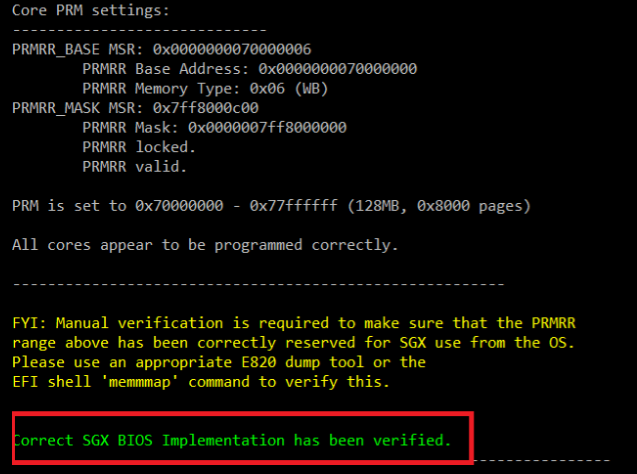
Run CMD as administer and enter into SGXBiosInfoTool\_v0.5.21.0 folder

Run command “SgxBIOSInfotool.exe –v”

Step 2:

Check the test result if BIOS implementation check is pass.

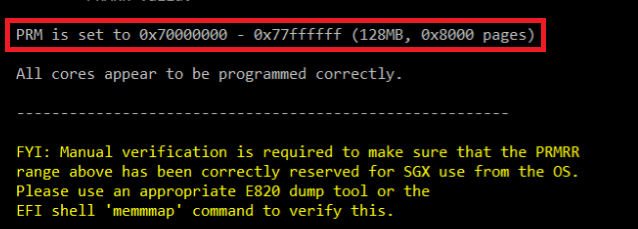
It shall show “Correct SGX BIOS Implementation has been verified”



Step 3:

Use appropriate E820 dump tool or EFI shell to check PRM address range is reserved

Here the example is from 0x70000000 to 0x77ffffff (the range to check is based on the result you run on SgxBiosInfoTool). You should find this range status is “reserved”.



**Run** **SGXFunctionalValidationTool\_v.0.7.7.0 or later**

Step 1:

Connect to internet

Step 2:

Run CMD as administer and enter into SGXFunctionalValidationTool\_v.0.7.7.0 folder

Run command “Sgxfunctionalvalidationtool.exe –v –prov\_epid –prov\_pse”

Step 3:

It should show “SGX functionality has been verified” and the test result of all test summary list items should show “success”

