***SGX function test***

|  |  |  |
| --- | --- | --- |
| **Update time** | **Author** | **Note** |
| 2018/08/06 | Sunny Wong | First Release |
| 2018/10/01 | Sunny Wong | (1) Modify description of test steps and update procedure of WS. (2) Add picture description. |
| 2018/10/22 | Sunny Wong | Add the test steps of “SGX Launch Control Policy” set to "Intel Locked" into SGX.001~ SGX.007 test cases. |
| 2019/01/09 | Sunny Wong | Modify “SGX.003 SGX Software Control” |
| 2019/03/22 | Sunny Wong | (1) Update “Setting” for SVR2019 / WIN10 (1709) and later OS. (2) Update SGX.005 test result Note. |
| 2019/8/14 | Sunny Wong | Modify “SGX.003” (display of results) |

* **Support Platform**

Greenlow

Mehlow

* **Test cases follow SPEC**

[\\ar-ebios-03\BIOS\TestTool\SGX\Kabylake](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Kabylake)

[576676\_CFL\_SGX\_Test\_\_Cases\_Mehlow\_Servers\_Rev1p0](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow)

[576676-576676-cfl-sgx-test-cases-mehlow-servers-rev1p0(For Greenlow)](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Kabylake)

* **Each SGX.xxx test case is independent**

SGX.001 SGX Enable

SGX.002 SGX Disable

SGX.003 SGX Software Control

SGX.004 Make sure memory allocated for Processor Reserved Memory (PRM) is marked as reserved

SGX.005 SGX Functionality Test

SGX.006 BIOS update should not impact SGX state

SGX.007 EPID and PSE Provisioning

SGX.008 Flex Launch Control locked (Greenlow Platform unsupported)

SGX.009 Flex Launch Control unlocked (Greenlow Platform unsupported)

* **Test tool link**

[Intel(R)\_SGX\_Windows\_x64\_PSW](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\PSW_for_Win)

[SGXBIOSInfoTool](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\BIT_for_Win)

[SGXFunctionalValidationTool](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\FVT_for_Win)

# Setting

|  |  |
| --- | --- |
| **Step1. Check BIOS setup has SGX item and options.** | |
|  | 1. Boot to BIOS. 2. Check BIOS “Software Guard Extensions (SGX)” item has “Disabled”, “Enabled”, “Software Controlled” options.  * If CPU not support SGX, SGX item will hidden. |
| **Step2. Install Windows UEFI OS. (must be UEFI mode)**   1. BIOS load default, press F10 save and exit. 2. Install Windows UEFI OS. (It must install UEFI mode OS) 3. Use SCD to install drivers, check Device Manager without yellow mark.  * **Mehlow: SGX Tool only support E-2186G/ E-2176G/ E-2174G CPU test under 2019 UEFI OS** | |
| **Step3. Install “Intel(R)\_SGX\_Windows\_x64\_PSW” under OS.** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled” 3. Press F10 save and exit.  * Follow Document “Intel SGX Installation Guide for Windows OS”: You need to configure Intel® SGX as “Enabled” in BIOS before installing Intel® SGX PSW. |
|  | 1. Copy test tool “Intel(R)\_SGX\_Windows\_x64\_PSW” folder to OS desktop.  * Tool link:   [\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\PSW\_for\_Win](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\PSW_for_Win) |
|  | **Windows 10 Fall Creators Update (version 1709) and later**   1. Into “PSW\_INF\_WinServer2019” folder. 2. Execute Command Prompt from the tool folder. 3. Execute “pnputil /add-driver sgx\_base.inf /install” 4. Check Driver package added successfully and installed. 5. Execute “pnputil /add-driver sgx\_psw.inf /install” 6. Check Driver package added successfully and installed. |
| **Step3. Copy “SGXBIOSInfoTool” and “SGXFunctionalValidationTool” to OS.** | |
|  | 1. Copy “SGXBIOSInfoTool” and “SGXFunctionalValidationTool” folders to OS desktop.  * Tool link:   [\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\BIT\_for\_Win](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\BIT_for_Win)  [\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\FVT\_for\_Win](file:///\\ar-ebios-03\BIOS\TestTool\SGX\Mehlow\FVT_for_Win) |

# SGX.001 SGX Enable

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled”.   SGX Launch Control Policy set to "Unlocked".(Greenlow Platform unsupported)   1. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt as administrator. 3. Execute “SgxBIOSInfoTool.exe -v -l”   (not support “V”, “L”) and wait 10~15 sec.   1. Confirm result as SGX enabled and without error/ fail message during execution. It will show “Correct SGX BIOS Implementation has been verified.” |
| **rename↓** | 1. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   ※ If file name not change, it will generate new logs in same file in next time executed (will not overwritten old log). |
| **Pass Log↓**          **Fail Log example↓** | 1. Open log file and confirm result as SGX enabled. 2. Check all logs without any error or fail message. 3. Check green area will exist. |
| **Step2. Reboot system, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**   1. Reboot system. 2. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. | |
| **Step3. Resume from S3 state, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**   1. Perform S3 state, resume from S3 state. 2. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. | |
| **Step4. Resume from S4, S5 state, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**   1. Perform S4 state, resume from S4 state. 2. Perform S5 state, resume from S5 state. 3. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. | |
| **Step5. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test SGX is Enabled.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Enabled**”, SGX Launch Control Policy set to "**Intel Locked**". 2. Boot to OS. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. 3. Reboot system. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. 4. Resume from S3 state. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. 5. Resume from S4 state, and resume from S5 state. Run SGX.001 Step1. 4~11 again, confirm result as SGX enabled. | |

# SGX.002 SGX Disable

|  |  |
| --- | --- |
| **Step1. SGX set Disabled, run SGX BIOS Info Tool with -v –l, check SGX is disabled.** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Disabled”.   SGX Launch Control Policy set to "Unlocked", and this item will hide. (Greenlow Platform unsupported)   1. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt as administrator. 3. Execute “SgxBIOSInfoTool.exe -v -l” 4. Confirm result as SGX disabled and without error/ fail message during execution. It will show “If SGX setup option = Disabled. This is expected behavior. PASS.” |
| **rename↓** | 1. Go to tool folder, find   "SgxBIOSInfoToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)  ※ If file name not change, it will generate new logs in same file in next time executed (will not overwritten old log). |
| **Pass Log↓** | 1. Open log file and confirm result as SGX disabled. 2. Check all logs without any error or fail message. 3. Check green area will exist. |
| **Step2. Reboot system, run SGX BIOS Info Tool with -v –l, check SGX is disabled.**   1. Reboot system. 2. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. | |
| **Step3. Resume from S3 state, run SGX BIOS Info Tool with -v –l, check SGX is disabled.**   1. Perform S3 state, resume from S3 state. 2. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. | |
| **Step4. Resume from S4, S5 state, run SGX BIOS Info Tool with -v –l, check SGX is disabled.**   1. Perform S4 state, resume from S4 state. 2. Perform S5 state, resume from S5 state. 3. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. | |
| **Step5. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test SGX is Disabled.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Disabled**”. SGX Launch Control Policy set to "**Intel Locked**" and this item will hide. 2. Boot to OS. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. 3. Reboot system. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. 4. Resume from S3 state. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. 5. Resume from S4 state, and resume from S5 state. Run SGX.002 Step1. 4~11 again, confirm result as SGX disabled. | |

# SGX.003 SGX Software Control

|  |  |
| --- | --- |
| **Step1. Make sure SGX is disabled and select Software Control option in BIOS setup menu.** | |
|  | 1. Boot to BIOS. 2. Make sure Software Guard Extensions (SGX) is “Disabled”. 3. Set to “Software Controlled”. 4. SGX Launch Control Policy set to "Unlocked".(Greenlow Platform unsupported) 5. Press F10 save and exit. |
| **Step2. Boot to OS, run SGX BIOS Info Tool with -v –l, check SGX is disabled.** | |
|  | 1. Boot to OS. 2. Execute Command Prompt from the tool folder. 3. Execute “SgxBIOSInfoTool.exe -v -l” and wait 10~15 sec. 4. Confirm result without error/ fail message. It will show   “SGX has not yet been enabled per CPUID.”  “Software Controlled interface request to enable SGX has been sent. Reboot the system and run the test again.”  “Correct SGX BIOS Implementation has been verified.”  20190814update  用BIOS Info Tool v0.7.1.1，在E3C242D4U2-2T驗證結果**無**綠色字。與BIOS RD Billy確認過，可能與Tool改版有關，如果其他資訊無error並且與SOP一致，則算正常。  **Note:**  **因為前面步驟(unlocked時)是Disabled SGX, 所以這邊result會是Disabled** |
|  | 1. Go to tool folder, find   "SgxBIOSInfoToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   1. Open log file and confirm result   (Green area will exist.)   1. Check all logs without any error or fail message. |
| **Step3. Reboot system, run SGX BIOS Info Tool with -v –l, check SGX is now enabled.** | |
|  | 1. Reboot system, do not enter BIOS setup. 2. Boot to OS. 3. Execute Command Prompt as administrator. 4. Execute “SgxBIOSInfoTool.exe -v -l”. 5. Confirm result as SGX enabled and without error/ fail message during execution. 6. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. (Separate logs of every executed to different file.) 7. Open log file and confirm result as SGX enabled. 8. Check all logs without any error or fail message. 9. Check green area will exist. |
| **Step4. Reboot system and run SGX.003 Step3 again to check SGX is enabled.**   1. Reboot system and into OS. (Do not enter BIOS setup.) 2. Run SGX.003 Step3. 2~9 again, confirm result as SGX enabled. | |
| **Step5. Resume from S3 state, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**   1. Perform S3 state, resume from S3 state. (Do not enter BIOS setup.) 2. Run SGX.003 Step3. 2~9 again, confirm result as SGX enabled. | |
| **Step6. Resume from S4, S5 state, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**   1. Perform S4 state, resume from S4 state. (Do not enter BIOS setup.) 2. Perform S5 state, resume from S5 state. (Do not enter BIOS setup.) 3. Run SGX.003 Step3. 2~9 again, confirm result as SGX enabled. | |
| **Step7. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Software Controlled**”. SGX Launch Control Policy set to "**Intel Locked**". 2. ~~Boot to OS. Run SGX.003 Step2 again, confirm result as SGX disabled.~~ 3. Reboot system. Run SGX.003 Step3 again, confirm result as SGX enabled.   **Note: 因為前面步驟(unlocked時)是Enabled SGX, 所以這邊result都會是Enabled (不會有SGX.003 Step2 result)**   1. Reboot system again. Run SGX.003 Step4 again, confirm result as SGX enabled. 2. Resume from S3 state. Run SGX.003 Step5 again, confirm result as SGX enabled. 3. Resume from S4 state, and resume from S5 state. Run SGX.003 Step6 again, confirm result as SGX enabled. | |

# SGX.004 Make sure memory allocated for Processor Reserved Memory (PRM) is marked as reserved

|  |  |
| --- | --- |
| **Step1. When SGX is enabled, "SgxBIOSInfoToolOutput" log will display PRM range.** | |
|  | 1. "SgxBIOSInfoToolOutput" log will display PRM range.   Ex: C246M WS PRM is set to 0x80000000 - 0x87ffffff (128MB, 0x8000 pages)  Ex: C236M WS PRM is set to 0x70000000 - 0x77ffffff (128MB, 0x8000 pages) |
| **Step2. Boot to UEFI Shell, run memmap and ensure range reported in the MSR is marked as reserved or hardware reserved.** | |
|  | 1. Boot to UEFI Shell. 2. Executes “memmap”. 3. Check PRM are set as reserved.   Ex: C246M WS PRM is set to 0x80000000 - 0x87ffffff (128MB, 0x8000 pages)  Ex: C236M WS PRM is set to 0x70000000 - 0x77ffffff (128MB, 0x8000 pages) |
| **Step3. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to check.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Enabled**”, SGX Launch Control Policy set to "**Intel Locked**". 2. Run SGX.004 Step2 again, run memmap and ensure range reported in the MSR is marked as reserved or hardware reserved. | |

# SGX.005 SGX Functionality Test

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**  **(Same as SGX.001 - Step.1)** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled”.   SGX Launch Control Policy set to "Unlocked".(Greenlow Platform unsupported)   1. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt as administrator. 3. Execute “SgxBIOSInfoTool.exe -v -l”. 4. Confirm result as SGX enabled and without error/ fail message during execution. 5. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. 6. Open log file and confirm result as SGX enabled. 7. Check all logs without any error or fail message. |
| **Step2. Run SGX Functional Validation tool with -v -l -skip\_pse\_tests.** | |
|  | 1. Execute Command Prompt as administrator. 2. Execute “SGXFunctionalValidationTool.exe -v -l -skip\_pse\_tests”.   **WorkStation:**Execute“SGXFunctionalValidationTool.exe -v -l**”**   1. Cmd windows will display “Enter to hibernate the system for testing: (Wake the system to continue)”.   **WorkStation:** Cmd windows will display “Enter to suspend…”, press “Enter”, check system will into S3 state, press power button to resume from S3 state, check Cmd windows will display “Enter to hibernate…”.   1. Press “Enter”, check system will into S4 state. |
|  | 1. Press power button to resume from S4 state. 2. Check Cmd windows will display “Enter to resume test”. 3. Press “Enter”. |
|  | 1. Check Cmd windows will display success message and “Enter to reboot for testing: (Restart application to continue)” 2. Press “Enter”, check system will reboot. |
|  | 1. Execute Command Prompt as administrator. 2. Execute “SGXFunctionalValidationTool.exe -v -l -skip\_pse\_tests” again.   **WorkStation:**Execute“SGXFunctionalValidationTool.exe -v -l**”** again.   1. Check Cmd windows will display “Successfully sealed and unsealed data across reboot.” and “Enter to shutdown for testing: Restart system and application to continue)” 2. Press “Enter”, check system will shutdown. |
| **Step3. Check test result without any fail log.** | |
|  | 1. Press power button to power on system. 2. Boot to OS. 3. Execute Command Prompt as administrator. 4. Execute “SGXFunctionalValidationTool.exe -v -l -skip\_pse\_tests. Again.   **WorkStation:**Execute“SGXFunctionalValidationTool.exe -v -l**”** again.   1. Confirm result without error/ fail message. 2. Check Test Summary without any failure.   **※Note**  If test on **Server** model, test result have “**FAILURE: Test sealing and unsealing data across standby boundary**”, **no need to open bug.**  (Because it is S3 test, Server not support S3, old test tool will skip this test on Sever, new test tool 0-7-15-1 will not skip S3 test.) |
| **Pass Log↓**        **Fail Log example↓** | 1. Go to tool folder, find   "SgxFunctionalValidationToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   1. Open log file and confirm result without any failure. 2. Check the Test Summary (at the bottom of the log file) is same as Green area. |
| **Step4. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test SGX** **Functionality Test.** **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Enabled**”, SGX Launch Control Policy set to "**Intel Locked**". 2. Boot to OS. Run SGX.005 Step1. 4~10 again, confirm result as SGX enabled. 3. Run SGX.005 Step2 again, run SGX Functional Validation tool. 4. Run SGX.005 Step3 again, check test result without any fail log. | |

# SGX.006 BIOS update should not impact SGX state

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**  **(Same as SGX.001 - Step.1)** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled”.   SGX Launch Control Policy set to "Unlocked".(Greenlow Platform unsupported)   1. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt as administrator. 3. Execute “SgxBIOSInfoTool.exe -v -l”. 4. Confirm result as SGX enabled and without error/ fail message during execution. 5. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. 6. Open log file and confirm result as SGX enabled. 7. Check all logs without any error or fail message. |
| **Step2. Update BIOS via Instant flash, run SGX BIOS Info Tool with -v –l, check SGX is still enabled.**   1. Update BIOS via Instant flash. 2. Run SGX.006 Step1. 4~10 again, confirm result still as SGX enabled. | |
| **Step3. Update BIOS via wIFUWIN, run SGX BIOS Info Tool with -v –l, check SGX is still enabled.**   1. Update BIOS via wIFUWIN. 2. Run SGX.006 Step1. 4~10 again, confirm result still as SGX enabled. | |
| **Step4. Update BIOS via wIFUDOS, run SGX BIOS Info Tool with -v –l, check SGX is still enabled.**   1. Update BIOS via wIFUDOS. 2. Run SGX.006 Step1. 4~10 again, confirm result still as SGX enabled. | |
| **Step5. Update BIOS via AFUWIN, run SGX BIOS Info Tool with -v –l, check SGX is still enabled.**   1. Update BIOS via AFUWIN with /p /b /n 2. Run SGX.006 Step1. 4~10 again, confirm result still as SGX enabled. | |
| **Step6. Update BIOS via AFUEFI, run SGX BIOS Info Tool with -v –l, check SGX is still enabled.**   1. Update BIOS via AFUEFI with /p /b /n 2. Run SGX.006 Step1. 4~10 again, confirm result still as SGX enabled. | |
| **Step7. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test BIOS update.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Enabled**”, SGX Launch Control Policy set to "**Intel Locked**". 2. Run SGX.006 Step1. 4~10 again, confirm result as SGX enabled. 3. Boot to BIOS, SGX Launch Control Policy set to "**Intel Locked**". Run SGX.006 Step2 again, confirm result as SGX enabled. 4. Boot to BIOS, SGX Launch Control Policy set to "**Intel Locked**". Run SGX.006 Step3 again, confirm result as SGX enabled. 5. Boot to BIOS, SGX Launch Control Policy set to "**Intel Locked**". Run SGX.006 Step4 again, confirm result as SGX enabled. 6. Boot to BIOS, SGX Launch Control Policy set to "**Intel Locked**". Run SGX.006 Step5 again, confirm result as SGX enabled. 7. Boot to BIOS, SGX Launch Control Policy set to "**Intel Locked**". Run SGX.006 Step6 again, confirm result as SGX enabled. | |

# SGX.007 EPID and PSE Provisioning

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**  **(Same as SGX.001 - Step.1)** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled”.   SGX Launch Control Policy set to "Unlocked".(Greenlow Platform unsupported)   1. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt as administrator. 3. Execute “SgxBIOSInfoTool.exe -v -l”. 4. Confirm result as SGX enabled and without error/ fail message during execution. 5. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. 6. Open log file and confirm result as SGX enabled. Check all logs without any error or fail message. |
| **Step2. Connect platform to the Internet.** | |
|  | 1. Connect LAN cable to MB. 2. Check network connect successfully. |
| **Step3. Run** **SGX Functional Validation Tool with -l -v -skip\_power\_tests -prov\_epid -skip\_pse\_tests.** | |
|  | 1. Execute Command Prompt from the tool folder. 2. Execute “SGXFunctionalValidationTool.exe -l -v -skip\_power\_tests -prov\_epid -skip\_pse\_tests”.   **WorkStation:** Execute “SGXFunctionalValidationTool.exe -l -v -skip\_power\_tests -prov\_epid -prov\_pse” |
| **Step4. Check test result without any fail log.** | |
| **Fail example↓** | 1. Confirm result without error/ fail message. 2. Check Test Summary without any failure. |
| **Pass Log↓**      **Fail Log example↓** | 1. Go to tool folder, find   "SgxFunctionalValidationToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   1. Open log file and confirm result without any failure. 2. Check the Green area will exist. |
| **Step5. Boot to BIOS, SGX Launch Control Policy set to "Intel Locked" to test EPID and PSE Provisioning.**  **(Greenlow Platform unsupported)**   1. Boot to BIOS, Software Guard Extensions (SGX) set to “**Enabled**”, SGX Launch Control Policy set to "**Intel Locked**". 2. Boot to OS. Run SGX.007 Step1. 4~9 again, confirm result as SGX enabled. 3. Run SGX.007 Step2 again, connect the Internet. 4. Run SGX.007 Step3 again, run SGX Functional Validation Tool. 5. Run SGX.007 Step4 again, check test result without any fail log. | |

# SGX.008 Flex Launch Control locked (Greenlow Platform unsupported)

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**  **(Same as SGX.001 - Step.1)** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX) set to “Enabled”. 3. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt from the tool folder. 3. Execute “SgxBIOSInfoTool.exe -v -l”. 4. Confirm result as SGX enabled and without error/ fail message during execution. 5. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. 6. Open log file and confirm result as SGX enabled. Check all logs without any error or fail message. |
| **Step2. Set SGX Flex Launch control policy to “locked” in BIOS.** | |
|  | 1. Boot to BIOS. 2. SGX Launch Control Policy set to “Locked”. |
| **Step3. Set all the SGX LE pubic key hash in BIOS.** | |
| **key in↓** | 1. According to the **SGX LE keys** displayed in FVT (SGX Functional Validation Tool running with -v will display), key in“SGX LE pubic key hash x”.   **※ Can refer to the FVT log of the SGX.005 or SGX.007 test case.**   1. Press F10 save and exit. |
| **Step4. Run** **SGX Functional Validation Tool with -l -v -skip\_power\_tests -skip\_pse\_tests -lcp\_legacy\_locked** | |
|  | 1. Boot to OS. 2. Execute Command Prompt from the tool folder. 3. Execute “SGXFunctionalValidationTool.exe -l -v -skip\_power\_tests -skip\_pse\_tests -lcp\_legacy\_locked”. |
| **Step5. Check test result without any fail log.** | |
| **Fail example↓** | 1. Confirm result without error/ fail message. 2. Check Test Summary without any failure. |
| **Pass Log↓** | 1. Go to tool folder, find   "SgxFunctionalValidationToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   1. Open log file and confirm result without any failure. 2. Check the Green area will exist. |

# SGX.009 Flex Launch Control unlocked (Greenlow Platform unsupported)

|  |  |
| --- | --- |
| **Step1. SGX set Enabled, run SGX BIOS Info Tool with -v –l, check SGX is enabled.**  **(Same as SGX.001 - Step.1)** | |
|  | 1. Boot to BIOS. 2. Software Guard Extensions (SGX)” set to “Enabled”. 3. Press F10 save and exit. |
|  | 1. Boot to OS. 2. Execute Command Prompt from the tool folder. 3. Execute “SgxBIOSInfoTool.exe -v -l”. 4. Confirm result as SGX enabled and without error/ fail message during execution. 5. Go to tool folder, find "SgxBIOSInfoToolOutput" log file, and rename this file. 6. Open log file and confirm result as SGX enabled. Check all logs without any error or fail message. |
| **Step2. Set SGX Flex Launch control policy to “unlocked” in BIOS.** | |
|  | 1. Boot to BIOS. 2. SGX Launch Control Policy set to “Unlocked”. 3. Press F10 save and exit. |
| **Step3. Run** **SGX Functional Validation Tool with -l -v -skip\_power\_tests -skip\_pse\_tests -lcp** | |
|  | 1. Boot to OS. 2. Execute Command Prompt from the tool folder. 3. Execute “SGXFunctionalValidationTool.exe -l -v -skip\_power\_tests -skip\_pse\_tests -lcp”. |
| **Step4. Check test result without any fail log.** | |
|  | 1. Confirm result without error/ fail message. 2. Check Test Summary without any failure. |
| **Pass Log↓** | 1. Go to tool folder, find   "SgxFunctionalValidationToolOutput" log file, and rename this file. (Separate logs of every executed to different file.)   1. Open log file and confirm result without any failure. 2. Check the Green area will exist. |

# Note: First Release Configuration

**E3C236D2I** MB: R1.02 (PPID: 14518963-0000003) + BIOS: L2.50A + BMC: L7.10.00

CPU: ASRS-CPU-KABYLAKE-XEON-1151-E3-1230V6-QMC6-3.5G-100-B0-72W-8M-05

DRAM: ASRS-DDR4-KINGSTON1-4G-2133-15-ECC-1.2V-09, 11

OS: Windows 2016 UEFI OS (1607) (USB install) + SCD: IIC2D-17.03

**E3C246D4U** MB: R1.01 (PPID: 16627027-0000018) + BIOS: P1.10 + BMC: P1.10.00

CPU: ASRS-CPU-COFFEE-S-GT2-XEON-VPRO-1151-E-2174G-QPA0-3.8G-U0-100-71W-8M-04

DRAM: ASRS-DDR4-KINGSTON1-4G-2133-15-ECC-1.2V-09,10

OS: Windows 2016 UEFI OS (1607 Build 14393.1884) (USB install) + SCD: IIC24X-10

**C236M WS** MB: R1.03 (PPID: 14712715-0000019) + BIOS P3.00

CPU: ASRS-CPU-SKYLAKE-S-GT2-SVR-1151-E3-1225V5-QJ7D-3.3G-R0-80W-8M-20

DRAM: ASRS-DDR4-KINGSTON2-4G-2133-15-1.2V-01, 03

OS: Win10 (1607) UEFI OS (PXE Server install) + SCD: IIWS4-12

**C246M WS** MB: R1.02 (PPID: 17144348-0000001) + BIOS L1.03

CPU: ASRS-CPU-COFFEE-S-GT2-XEON-VPRO-1151-E-2174G-QPA0-3.8G-U0-100-71W-8M-04

DRAM: ASRS-DDR4-CRUCIAL-8G-2666-19-ECC-1.2V-03, 04

OS: Win10 (1607) UEFI OS (PXE Server install) + SCD: IIWSC24-10