I installed SGX-driver, SDK, and PSW and tested it successfully. However, when I want to install the Rust-SGX-SDK I got into the problem that the driver was not installed well.

I am missing /dev/isgx

also after running dmesg | grep sgx

I get

[2.042902] intel_sgx: loading out-of-tree module taints kernel. [2.042938] intel_sgx: module verification failed: signature and/or required key missing - tainting kernel [6671.285546] intel_sgx: SGX is not enabled [7166.587822] intel_sgx: SGX is not enabled [7414.562652] intel_sgx: SGX is not enabled

Although I have it Software Controlled

in BIOS (no other option than Disabled

is possible there).

Output after cpuid | grep SGX

SGX: Software Guard Extensions supported = true SGX_LC: SGX launch config supported = false SGX capability (0x12/0): SGX1 supported = false SGX2 supported = false SGX: Software Guard Extensions supported = true SGX_LC: SGX launch config supported = false SGX capability (0x12/0): SGX1 supported = false SGX2 supported = false SGX: Software Guard Extensions supported = true SGX_LC: SGX launch config supported = false SGX capability (0x12/0): SGX1 supported = false SGX2 supported = false SGX: Software Guard Extensions supported = true SGX_LC: SGX launch config supported = false SGX capability (0x12/0): SGX1 supported = false SGX2 supported = false

The processor is Intel G4560, which has SGX supported with Intel® ME
https://ark.intel.com/content/www/us/en/ark/products/97143/intel-pentium-processor-g4560-3m-cache-3-50-ghz.html

Did anyone had a similar issue? I tried to google but did not find anything that would help.