Intel® Server Platform Services Manageability Engine Firmware for Icelake D Product Line NM, SiEn

Customer Release Notes

Power-On Release for Idaville Platforms

Document Version 1.0

May 2020

Contents

List of Tables

1. Introduction

These release notes are intended for the Power-On release of the Intel® Server Platform Services Manageability Engine Firmware for the Icelake D Product Line.

The product name is abbreviated to SPS in the remainder of this document.

SPS Firmware for Idaville platform can be configured in SKUs: NM, SiEn. Please refer to Intel® SPS External Product Specification [572822] for information regarding the Firmware SKU definition.

1.1. Revision Numbers of SPS Package Components

Table 1.1: Revision numbers of Power-On release components included in SPS_SoC-X_05.00.00.048.0.zip package.

Subproject (component)	Location	Revision
Intel(R) SPS ME Firmware	/MeRegion.bin	SPS_SoC-X_05.00.00.048.0
Intel Flash Image Tool for Server Platform Services only	/Tools/FlashImageTool	SPS_SoC-X_05.00.00.048.0
Intel® Flash Programming Tool	/Tools/FlashProgrammingTool	SPS_Tools_4.2.97.235
SPS ME SMBus Diagnostic Console	/Tools/MeDiagnosticConsole	SPS_Tools_4.2.97.235
SPS ME SMBus Diagnostic Console	/Tools /MeDiagnosticConsoleAgent	SPS_Tools_4.2.97.235
Intel® ME Info with support for SPS	/Tools/SpsInfo	SPS_Tools_4.2.97.235
SPS FW Manufacturing Tool	/Tools/SpsManuf	SPS_Tools_4.2.97.235
Sample Update Tool for SPS	/Tools/SampleUpdateTool	SPS_Tools_4.2.97.235
NULL Heci Driver	/Tools/NullHeciDriver	SPS_Tools_4.2.97.235
Compliance Tests IPMI Tool Scripts	/Tools/ComplianceTestsScripts	SPS_Tools_4.2.97.235

Table 1.2: Revision numbers visible in component properties, on the console, or over IPMI included in SPS_SoC-X_05.00.00.048.0.zip package.

Console-Component	Revision
ME SPS Firmware Get Device Id response	50 01 05 00 02 21 57 01 00 11 0B 05 04 80 01
ME SPS Recovery Boot Loader Get Device Id response	50 01 85 00 02 20 57 01 00 11 0B 00 04 80 00
HECI MKHI_GET_FW_VERSION response	05.00.00.048
spsFITc.exe	5.0.0.48
spsFPTW64.exe, spsFPT.efi	SPS_Tools_4.2.97.235
MESDC.exe	SPS_Tools_4.2.97.235
RemoteAgentLinux64, RemoteAgentWin64.exe	SPS_Tools_4.2.97.235
spsInfoWin64.exe, spsInfoLinux64, spsInfo.efi	SPS_Tools_4.2.97.235
spsManufWin64.exe, spsManuf.efi, spsManufLinux64	SPS_Tools_4.2.97.235

2. SPS Package Contents

Table 2.1 lists the contents of the release package.

Note: All of this software needs Intel® compatible PC with Microsoft Windows 7® x64, Microsoft Windows 8.1® x86/x64, Microsoft Windows 10® x64, Microsoft Windows Server 2012® R2 SP1 x64 or Microsoft Windows Server 10® x64 operating system installed depending on the specific tool requirements listed below.

Note: The release package contains one license file placed in the main directory. This license is specified for Power-On release firmware.

Table 2.1: Software package

No.	Package	Contents
1	ReleaseNotes.pdf	This file.
2	SPS_SoC-X_05.00.00.048.0	This is a release package with Intel SPS ME Firmware and Tools for Icelake D SoC platform. Uncompress the package. The package will uncompress into SPS_SoC-X_05.00.00.048.0 directory. MeRegion.bin - Uncompressed SPS firmware binary for Snow Ridge SoC silicon located in the main directory. Intel Flash Image Tool for Server Platform Services only - Microsoft Windows* tool: This is a tool to create SPI Flash image and to modify SPS Firmware factory configuration. This tool is unpacked into the /Tools/FlashImageTool directory. Oemsptkeymn2.bin - sample OEM signing hashes. Should be replaced with actual OEM signing hashes when available. Flash Programming Tool - Microsoft Windows* tool: Flash Programming Tool for SoC attached SPI Flash. This tool is unpacked into the /Tools/FlashProgrammingTool directory.

Table 2.1: Software package

No.	Package	Contents
		ME SMBus Diagnostic Console Application. This tool is used to diagnose ME Firmware through SMBus interface. The main purpose of this tool is to provide live feedback from ME FW. ME SMBus Diagnostic Console Application is unpacked into the /Tools/MeDiagnosticConsole directory. MESDC Agent. This tool is a proxy application for MESDC. It connects MESDC using the LAN connection with the SPS FW using the HECI connection. MESDC Agent is unpacked into the /Tools/MeDiagnosticConsoleAgent directory. SPS Info tool for checking basic ME health and supported features list in /Tools/SpsInfo directory. SPS Manuf tool for validation ME on the manufacturing line in /Tools/SpsManuf directory. Compliance Tests IPMI Tool Scripts in /Tools/ComplianceTestsScripts directory.

3. New/Changed Features

3.1. New/Changed Features

Release for Idaville platforms (SiEn) introduces the following new features:
New ME firmware version SPS_SoC-X_05.00.00.048.0 is provided
spsRecovery.bin and spsOperational.bin were replaced with one meBinary.bin

3.2. Limitations

The following list describes all the limitations for this SPS release
This code was tested in the following configuration:

This release was tested with the following operating systems:

- RHEL74.craff
- Windows Server 2019
- EFI

This release was tested with:

- ROM version: ME-ROM A0 frozen: ROM_CDF_A0_MC_SERV_SI_REL_21_NOV_2017
- BIOS version: IDVLCRB.86B.WR.64.2020.13.3.03.1540_0114.P36_P_LCC_CDF_PO
- PMC patch version: PMCP_VER CDFH_B0_PMC_FW_000.02.10.1002_DebugSigned_pmcp
- mPhy table version: CdfPchHsioAxSvpV111ChipsetInit
- CCA version: JVL_IDV_SoftStraps_rev2.8_Master_WIP_WW17
- iRC IRCP_VER irc_fw_4.034.css_mu_r2.signed
- NM PTU: N/A

3.3. XML Changes

Initial version of Firmware.

3.4. Documentation Updates

Table 3.1: Current SPS Firmware Documentation.

Document Title	Revision	Ref.
SPS 5.0 External Product Specification	1.2	572822
SPS 5.0 Platform Integration Guide	1.0	574653
SPS 5.0 Services Integration Guide	1.0	575469
NM 5.0 External Interface Specification	1.2	575576
SPS 5.0 ME-to-BIOS Specification	1.7	575642
SPS 5.0 Services Compliance Guide	1.0	575752

4. Known Issues

Table 4.1: Disposition field definition.

State	Definition
Under Investigation	The sighting is being investigated.
Root Cause Identified	The root cause for the defect is identified.
Workaround Available	A temporary solution to the defect is provided until the defect is fixed.

Table 4.2: Known Issues.

Issue Id	Description
18011471052	**Delayed Authentication Mode is always enabled**
Description	In order to make the fused part verification, Delayed Authenication Mode is always enabled. Corresponding DAM setting in spsFITc tool do not allow to disable DAM feature.
Root Cause	Unknown
Status	Under Investigation

5. Fixed Issues

Table 5.1: Disposition field definition.

State	Definition
As Designed	The issue reported is not a defect and the behavior will not be modified.
Closed no repro	The situation was not observed anymore and no further investigation is scheduled.
Fixed	Already fixed.

Table 5.2: Fixed Issues.

Issue Id	Description
18011402357	**Intel PTT Configuration tab in spsFITc is hide**
Description	Configuration / Platform Security / Intel PTT Configuration is hide in spsFITc GUI.
Root Cause	spsFITc GUI issue
Status	Fixed