Intel® Xeon® D-1700 Processor Family Intel® Firmware Support Package (Intel® FSP)

Release Notes

February 2024

Revision 003US

Notice: This document contains information on products in the design phase of development. The information here is subject to change without notice. Do not finalize a design with this information.

Intel technologies may require enabled hardware, software or service activation.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Performance varies by use, configuration, and other factors. Learn more on the Performance Index site.

Your costs and results may vary.

“Conflict-free" refers to products, suppliers, supply chains, smelters, and refiners that, based on our due diligence, do not contain or source tantalum, tin, tungsten or gold (referred to as “conflict minerals" by the U.S. Securities and Exchange Commission) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or adjoining countries.

All product plans and roadmaps are subject to change without notice.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Results have been estimated or simulated.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel contributes to the development of benchmarks by participating in, sponsoring, and/or contributing technical support to various benchmarking groups, including the BenchmarkXPRT Development Community administered by Principled Technologies.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visiting the Intel Resource and Document Center.

Contents

Tables

Revision History

Revision Number	Description	Date
001US	• Initial release of the document	September 2022
002US	• Release notes for Intel® Firmware Support Package (Intel® FSP) Intel® Software Guard Extensions (Intel® SGX) Flex Release	December 2022
003US	• Introduction of new Intel FSP-M UPDs for enablement and configuration of spread spectrum: PciePllSsc and SpsIccClkSscSetting	February 2024

1 Introduction

This package contains required binary image(s) and collateral for the Intel® Xeon® D-1700 processor family Intel® Firmware Support Package (Intel® FSP).

This Intel® Firmware Support Package (Intel® FSP) is compliant with the *Intel® Firmware Support Package External Architecture Specification v2.1*.

This document provides system requirements, installation instructions, issues and limitations, and legal information.

To learn more about this product, refer to:

- New features listed in Section 2.0 or in the help.
- Reference documentation listed in Section 1.4.
- Installation instructions listed in Section 4.1.

1.1 Component Information

The software in this release has been developed and validated using the following information as shown in Table 1.

Table 1. Intel® FSP Component Information

Component	Version
Code Base	EDKII
Core Version	edk2_stable_202208
Memory Reference Code Version	
Reference Code Build Version	0027.D84

1.2 Bootloader Requirements

It is expected that the bootloader performs the following:

- Configure the HSUART device for the serial port. Refer to the UPD Data Region section of the *Intel® Xeon® D-1700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide*.

Note: Intel® Xeon® D-1700 processor family Intel FSP does NOT support a legacy serial port.

- Implement the following functions depending on the specific platform requirements:
    - — Addition of support for the (A0 stepping) silicon
    - — Addition of support for required boards/platforms

- Set up of the operating environment for the Intel FSP Application Programming Interfaces (APIs) that includes, but is not limited to, the following:
    - CPU initialization
    - Loading microcode
    - Board-specific initialization including PCI enumeration and post-PCI enumeration initialization
    - Serial AT Attachment (SATA) initialization
    - Peripheral Component Interconnect Express* (PCIe*) initialization
    - Universal Serial Bus (USB) initialization
    - Power management initialization (S-states, P-states, wake events, and thermal)
    - Advanced Configuration and Power Interface (ACPI) support
    - Payload to load/boot the OS
    - Port 80 display
    - Fast boot support
    - Booting from USB2/USB3 storage devices
    - Booting from eMMC* storage device
    - IA64 mode support

1.3 Acronyms and Terms

Table 2 lists the acronyms and terms used in this document (in alphabetic order).

Table 2. Terminology

Term	Description
ACPI	Advanced Configuration and Power Interface
API	Application Programming Interface
BCT	Binary Configuration Tool
BIOS	Basic Input Output System
BKC	Best Know Configuration
BSF	Boot Settings File
CPU	Central Processing Unit
CRB	Customer Reference Board
eMMC	embedded Multi-Media-Card
FIA	Flexible I/O Adapter
Intel® FSP	Intel® Firmware Support Package
IBL	Intel® Business Link
MOW	Message of the Week
NS	Network Solutions

Term	Description
OS	Operating System
PCD	Platform Configuration Database
PCIe*	Peripheral Component Interconnect Express
RMT	Rank Margining Tool
SATA	Serial AT Attachment
SoC	System on a Chip
UPD	Updatable Product Data
USB	Universal Serial Bus

1.4 Related Documentation, Tools, and Packages

Table 3 lists the processor family documentation.

Table 3. Intel Firmware Support Package Documentation

Document Name	Reference Number
Intel® FSP External Architecture Specification v2.1 https://www.intel.com/content/www/us/en/intelligent-systems/intel-firmware-support-package/intel-fsp-overview.html	
Boot Setting File (BSF) Specification *https://software.intel.com/content/www/us/en/develop/download/boot-setting-file-specification-release-10.html*	
Binary Configuration Tool (BCT) for Intel® FSP *https://github.com/IntelFsp/BCT*	
Intel® Xeon® D-1700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide	742660

Table 4 lists the tools applicable to this Intel FSP release.

Table 4. Tool Versions

Tool	Version
EDKII BaseTools	edk2_stable_202208
Binary Configuration Tool (BCT)	3.4.4
Intel® Server Platform Services (Intel® SPS) FW (CRB) version	SPS_SoC-X_05.00.04.100.0

1.5 Intended Audience

This document is for platform and system developers who intend to use an Intel FSP based bootloader for the firmware solution for their overall design based on the Intel® Xeon® D-1700 processor family. This group includes system BIOS developers, bootloader developers, and system integrators.

1.6 Customer Support

Intel offers support for this software at the API level only, defined in the *Intel® Xeon® D-1700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide*. If your field representative has created an account for you, support requests can be submitted at https://premiersupport.intel.com.

2 New in This Release

2.1 New Features

This release includes the following new feature and product changes:

- Build version 0027.D84

- Introduction of new Intel FSP-M UPDs for enablement and configuration of spread spectrum:
  - PcdSpsIccClkSscSetting
  - PchPciePllSsc

3 Software Issues and Limitations

Known and resolved issues relating to the Intel Firmware Support Package are described in this section.

3.1 Known Issues

None

3.2 Resolved Issues

None

3.3 Limitations

None

4 Where to Find the Release

This package can be found at https://github.com/intel/FSP.

4.1 How to Unpack This Release

This release can be unpacked on a Linux* or Windows* system.

4.1.1 For Linux*

1. Clone IdavilleFspBinPkg from GitHub*.

Note: For guidance on how to add the Intel FSP APIs into the bootloader code, refer to the *Intel® Xeon® D-1700 Processor Family Intel® Firmware Support Package (Intel® FSP) Integration Guide* (refer to Table 3 for more information).

4.2 Microcode Update

The IA-32 processors have the capability to correct specific errata through the loading of an Intel supplied data block. This data block is referred to as a microcode update or system configuration data.

Each unique processor stepping/package combination has an associated microcode update that, when applied, constitutes a supported processor (that is, Specified Processor = Processor Stepping + Microcode Update). The proper microcode update must be loaded on each processor in a system. The proper microcode update is defined as the latest microcode update available from Intel for a given family, model, and stepping of the processor. Any processor that does not have the correct microcode update loaded is operating out of specification.

Intel recommends that future microcode updates are done as soon as the latest ones are released.

4.3 Debug

Debug messages are the primary way of debugging the Intel FSP. Debug messages are suppressed for production binary and enabled by default in the debug binary.

4.4 BIOS Shared Software Architecture (BSSA) Rank Margining Tool (RMT)

The RMT can flag areas of concern for platform developers and is disabled by default in this Intel FSP release.

4.5 Component Extraction

The Intel FSP binary is released as a single binary. Use the Python* script, SplitFspBin.py, to split the binary into the different components.

SplitFspBin.py is available at:
https://github.com/IntelFsp/FSP/blob/master/Tools/SplitFspBin.py

The sample command shown next creates three binaries named after the inputting the Intel FSP binary and appending with "_M", "_S", and "_T", respectively.

```
python SplitFspBin.py split -f <FSP Binary>
```

Example: `python IntelFsp2Pkg\Tools\SplitFspBin.py split -f FspRel.bin`

Example output:

- `FspRel_M.bin`
- `FspRel_S.bin`
- `FspRel_T.bin`

5 Release Content

This release package contains the following contents.

Table 5. Package Contents

Description	Filename	Path
Intel FSP Binary File	`FspRel.bin`	`ICELAKE-D_FSP_KIT/` `IdavilleFspBinPkg/Lcc/FspBin`
Boot Setting File (BSF)	`FspRel.bsf`	`ICELAKE-D_FSP_KIT/` `IdavilleFspBinPkg/Lcc/FspBin`

Documents	`IcelakeDEFsp IntegrationGuide.pdf`
	`IcelakeDEFsp ReleaseNotes.pdf`
		`ICELAKE-D_FSP_KIT/`
		`IdavilleFspBinPkg/Lcc/Docs`

Sample File	`FsptUpd.h`
	`FspmUpd.h`
	`FspsUpd.h`
	`FspUpd.h`
		`ICELAKE-D_FSP_KIT/ IdavilleFspBinPkg/Lcc/Include`

6 Hardware and Software Compatibility

6.1 Supported Hardware

The Intel FSP included in this release is specifically targeted for the Intel® Xeon® D-1700 processor family.

6.2 Supported Operating Systems

This release installs on either a Windows* or a Linux* system. However, the Intel FSP binary itself can be used with any software development environment to generate a complete bootloader solution.

The software in this release has been validated against the operating systems given in Table 6 on the Customer Reference Boards (CRBs) for the Intel® Xeon® D-1700 processor family.

Note: While the Intel FSP is validated on the slim bootloader and Fedora* operating systems on the respective platforms, it is designed to work without any changes on some other bootloader and operating systems.

Table 6. Operating System/Bootloader Support

Software Type	Name	Version
Bootloader	Slim Boot	SBID: SB_IDV ISVN: 001 IVER: 001.000.001.002.00016
Firmware Component	Intel® Server Platform Services (Intel® SPS) Intel® Management Engine (Intel® ME) Firmware	SPS_SoC-X_05.00.04.100.0
Firmware Component	Intel FSP	0027.D84
Operating System	Yocto*	Yocto version
Tool	BCT	3.4.4

NOTE: Validation was done on Brighton City with the Intel® Xeon® D-1700 processor family QYDX and QYDZ QDFs only. ***

7 Configuration

A Binary Configuration Tool (BCT) for the Intel FSP is provided as a companion tool and is intended to be used to:

- Customize the Intel FSP binary configuration options based on the Boot Setting File (BSF).
- Rebase the Intel FSP binary to a different base address (the default base address of the Intel FSP for Intel® Xeon® D-1700 processor family is 0xFFF85000 for FSP-T, 0xFFDA8000 for FSP-M and 0xFFD3A000 for FSP-S).

Intel recommends using the latest BCT with this release.

Refer to the *BCT User Guide* for usage instructions. Refer to Section 1.4 to obtain the BCT.

7.1 Intel Firmware Support Package Information

To obtain the Intel FSP binary information:

1. Run the Binary Configuration Tool.
2. Click the Show Binary Description command button.
3. Select the Intel FSP binary. For this release, the binary included is named as:

   FspRel.bin (release version)
4. Click Open. Another window will open and show the Intel FSP binary information.
5. Click OK to close the window.

The following information is displayed in the tool:

```
FSP-M Header Details................
This FSP supports the following:
ICXD


Build: 0027.D84
FSP Version: 0.0.27.84
FSP Header:
  Signature: FSPH
  Header Length: 0x58
  Header Revision: 0x4
  SpecVersion: 0x21
  Image Revision: 0x2784
  Image ID: ICXD-FSP
  Image Size: 0x1e5000
  Image Base: 0xffdb1000
  Image Attribute: 0x20030002
  Configuration Region Offset: 0x18c
  Configuration Region Size: 0x230
  API Entry Num: 0x0
  Temp RAM Init Entry: 0x0
  FSP Init Entry: 0x0
  Notify Phase Entry: 0x0
  FSP Memory Init Entry: 0x4b0
  Temp RAM Exit Entry: 0x4ba
  FSP Silicon Init Entry: 0x0

FSP Extended Header:
  Signature: FSPE
  Header Length: 0x18
  Header Revision: 0x1
  FSP Producer Id: INTELC
  FSP Producer Revision: 0x1

FSP-T Header Details................
This FSP supports the following:
ICXD

Build: 0027.D84
FSP Version: 0.0.27.84
FSP Header:
  Signature: FSPH
  Header Length: 0x58
  Header Revision: 0x4
  SpecVersion: 0x21
  Image Revision: 0x2784
  Image ID: ICXD-FSP
  Image Size: 0x6000
  Image Base: 0xfff96000
  Image Attribute: 0x10030002
  Configuration Region Offset: 0x18c
  Configuration Region Size: 0x80
  API Entry Num: 0x0
  Temp RAM Init Entry: 0x551
  FSP Init Entry: 0x0
  Notify Phase Entry: 0x0
  FSP Memory Init Entry: 0x0
  Temp RAM Exit Entry: 0x0
  FSP Silicon Init Entry: 0x0

FSP Extended Header:
  Signature: FSPE
  Header Length: 0x18
  Header Revision: 0x1
  FSP Producer Id: INTELC
  FSP Producer Revision: 0x1
```

```
FSP-S Header Details................
This FSP supports the following:
ICXD

Build: 0027.D84
FSP Version: 0.0.27.84
FSP Header:
  Signature: FSPH
  Header Length: 0x58
  Header Revision: 0x4
  SpecVersion: 0x21
  Image Revision: 0x2784
  Image ID: ICXD-FSP
  Image Size: 0x91000
  Image Base: 0xffd20000
  Image Attribute: 0x30030002
  Configuration Region Offset: 0x18c
  Configuration Region Size: 0x125
  API Entry Num: 0x0
  Temp RAM Init Entry: 0x0
  FSP Init Entry: 0x0
  Notify Phase Entry: 0x378
  FSP Memory Init Entry: 0x0
  Temp RAM Exit Entry: 0x0
  FSP Silicon Init Entry: 0x382

FSP Extended Header:
  Signature: FSPE
  Header Length: 0x18
  Header Revision: 0x1
  FSP Producer Id: INTELC
  FSP Producer Revision: 0x1
```