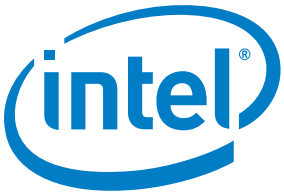

Intel® Firmware Support Package for Intel Atom® C3XXX Product Family

Release Notes

Production Validated 002

June 2018

Document Number: 335701-003US

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 Software is subject to change without notice, and should not be construed as a commitment by Intel Corporation to market, license, sell or support any product or technology. Unless otherwise provided for in the license under which this Software is provided, the Software is provided AS IS, with no warranties of any kind, express or implied.

Except as expressly permitted by the Software license, neither Intel Corporation nor its suppliers assumes any responsibility or liability for any errors or inaccuracies that may appear herein. Except as expressly permitted by the Software license, no part of the Software may be reproduced, stored in a retrieval system, transmitted in any form, or distributed by any means without the express written consent of Intel Corporation.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting: http://www.intel.com/design/literature.htm.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at http://www.intel.com/ or from the OEM or retailer.

No computer system can be absolutely secure.

Intel, the Intel logo, Atom, and Pentium are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. This Intel® Firmware Support Package ("Software") is furnished under license and may only be used or copied in accordance with the terms of that license.

Intel, Atom, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Contents

Tables

Revision History

Date	Revision	Description
June 2018	003	Production Validated 002
October 2017	002	Production Validated 001
March 2017	001	Initial release - Production Candidate 001

§

1.0 Introduction

This package contains required binary image(s) and collateral for the Intel® Firmware Support Package (Intel® FSP) for the Intel Atom® C3XXX Product Family (formerly Denverton-NS).

This Intel® Firmware Support Package (Intel® FSP) is compliant with the *Intel® FSP External Architecture Specification v2.0 (FSP EAS v2.0)*.

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	SVN r90465
Memory Reference Code Version	95042B
Reference Code Build Version	15D62

Note: Validation was done on Harcuvar B1 with Intel® Atom® C3XXX SoC B1 (QMEH) stepping only.

1.2 Bootloader Requirements

It is expected that the bootloader perform the following:

- Configure the HSUART device for the serial port. Refer to the UPD Data Region section of the *Intel Atom® C3XXX Product Family Intel® Firmware Support Package (Intel® FSP) Integration Guide*.

  Note: Intel Atom® C3XXX Product Family Intel® FSP does **NOT** support legacy serial port.

- Implement the following functions depending on specific platform requirements:
  - Addition of support for Intel Atom® C3XXX Product Family (A0/A1/B0/B1/Cx stepping) silicon
  - Addition of support for required boards/platforms
  - Setup 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
BSF	Boot Settings File
CRB	Customer Reference Board
FIA	Flexible I/O Adapter
Intel® FSP	Intel® Firmware Support Package
IBL	Intel® Business Link
MOW	Message of the Week
OS	Operating System
PCIe*	Peripheral Component Interconnect Express
RMT	Rank Margining Tool
SATA	Serial AT Attachment
SoC	System on a Chip
USB	Universal Serial Bus

1.4 Related Documentation, Tools, and Packages

Table 3 lists the Intel Atom® C3XXX Product Family Platform documentation.

Table 3. Intel® Firmware Support Package Documentation

Document Name	Reference Number
Intel® FSP External Architecture Specification v2.0 (FSP EAS v2.0)	http://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp-architecture-spec-v2.pdf
Binary Configuration Tool (BCT) for Intel® FSP	https://github.com/IntelFsp/BCT
Linux FSP for Intel Atom® C3XXX Product Family*	https://github.com/IntelFsp/FSP

Document Name	Reference Number
Intel Atom® C3XXX Product Family Intel® Firmware Support Package (Intel® FSP) Integration Guide	335702

Table 5 lists the tools applicable to this Intel® FSP release.

Table 4. Tool Versions

Tool	Version
Binary Configuration Tool (BCT)	3.3.1
SPS FW (CRB) version	04.00.04.168.0

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 Atom® C3XXX Product 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 Atom® C3XXX Product Family Product Family Intel® Firmware Support Package Integration Guide* and reference manuals. If your field representative has created an account for you, support requests can be submitted at https://premier.intel.com.

§

2.0 New in This Release

2.1 New Features

This release includes the following new features and product changes:

- Fixed invalid parameter stored in SMBIOS Memory HOB.

§

3.0 Intel Atom® C3XXX Product Family Software Issues and Limitations

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

3.1 Known Issues for Intel Atom® C3XXX Product Family Product Family

None known.

3.2 Resolved Issues for Intel Atom® C3XXX Product Family

Table 5. Resolved Issues

Description	Status
Module Part Number stored in SMBIOS Memory HOB is invalid.	Fixed

3.3 Limitations for Intel Atom® C3XXX Product Family

Table 6. Limitations

Description	Status
Denverton FSP can only support IO based serial port base address, MMIO based serial port base address is not supported.	No Planned Fix

§

4.0 Where to Find the Release

This package can be found on GitHub.com.

4.1 How to Install this Release

This release can be installed on a Linux* system.

4.1.1 For Linux*

1. Download the zipped file from https://github.com/IntelFsp /FSP.
2. Extract the contents of the .zip file.
3. Refer to the `Readme_Extract.txt` file for further instructions to complete the installation.

Note: For the guide to adding the Intel® FSP APIs into the bootloader code, refer to the *Intel Atom® C3XXX Product 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 (i.e., 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 considered to be operating out of specification.

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

The steps for converting a microcode patch to a microcode header are as follows:

1. Download the latest microcode patch. This file is in text format (i.e. *.txt or *.inc).

2. This is a sample command to reformat the microcode patch:

```
cat {name}.TXT | awk ‘{print $2}’ | sed ‘s/^/0x/’ | sed ‘s/h/,/’
> {name}.h
```

4.3 Debug

Debug messages are the primary way of debugging the Intel® FSP. There is an option to modify the Intel® FSP debug level using the BCT. The **FSP Debug Print Level** has a default value of `MEDIUM DEBUG`, which is the level below the highest debug level.

1. Start the BCT and open the `DenvertonNSFsp.bsf` file that was included with the Intel® FSP kit.
2. In the **Settings Configuration->MRC & Early SoC** section, set **Intel® FSP Debug Print Level** to the desired debug level (Range: No Debug – Verbose Debug).
3. Save the settings in an `.absf` file.
4. Apply the settings to the Intel® FSP binary file using **Binary Tools->Patch**.

4.4 Rank Margining Tool

The RMT can flag areas of concern for platform developers. The BCT tool can be used to modify the Intel® FSP binary to enable the RMT for memory testing.

1. Start the BCT and open the `DenvertonNSFsp.bsf` file that was included with the Intel® FSP kit.
2. In the **Setting Configuration->MRC & Early SoC** section:
   a. Set **Enable Rank Margin Tool** to **Enabled.**
   b. Set **RMT CPGC exp_loop_cnt** to the desired value.
   c. Set **RMT CPGC num_bursts** to the desired value.
3. Save the settings in an `.absf` file.
4. Apply the settings to the Intel® FSP binary file using **Binary Tools->Patch**.

4.5 Component Extraction

The Intel® FSP binary is released as a single binary. Use the python* script, SplitFspBin.py, to split the FD in to the different FSP components.

SplitFspBin.py is available at:
https://github.com/tianocore/edk2/tree/master/IntelFsp2Pkg/Tools

The sample command shown below creates three binaries named after the input Intel® FSP binary and appended with "_M", "_S", and "_T" respectively.

```
python IntelFsp2Pkg\Tools\SplitFspBin.py split -f <FSP Binary>
```

Example: `python IntelFsp2Pkg\Tools\SplitFspBin.py split -f DenvertonNSFsp.fd`

Example Output:

- `DenvertonNSFsp_M.fd`
- `DenvertonNSFsp_S.fd`
- `DenvertonNSFsp_T.fd`

§

5.0 Release Content

This release package contains the following contents.

Table 7. Package Contents

Description	Filename	Path
Intel® FSP Kit License File	*DenvertonNSFspKitProductionRULACLicense.pdf*	
Intel® FSP Binary File	DenvertonNSFsp.fd	DenvertonNSFspBinPkg/FspBin
Boot Setting File (BSF)	DenvertonNSFsp.bsf	DenvertonNSFspBinPkg/FspBin
Documentation	*DenvertonNSFspIntegrationGuide.pdf* *DenvertonNSFspReleaseNotes.pdf*	DenvertonNSFspBinPkg/Docs
Text File Copy of Intel® FSP Kit License File (Linux* only)	license.txt	DenvertonNSFspBinPkg/Docs
Sample File	FsptUpd.h FspmUpd.h FspsUpd.h FspUpd.h	DenvertonNSFspBinPkg/Include

§

6.0 Hardware and Software Compatibility

6.1 Supported Hardware

The Intel® FSP included in this release is specifically targeted for the Intel Atom® C3XXX Product Family Product Family System on a Chip (SoC).

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 9 on the Customer Reference Boards (CRBs) for Intel Atom® C3XXX Product Family.

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

Table 8. Operating System/Bootloader Support

Software Type	Name	Version
Bootloader	coreboot*	4.6
Payload Bootloader	UEFI Payload	PC 001
Firmware Component	SPS ME Firmware	04.00.04.168.0
Firmware Component	Intel® FSP	PV002
Operating System	Yocto*	2.0
Tool	BCT	3.3.1

Validation was done on Intel® Atom® C3XXX SoC B1 (QMEH) stepping only.

§

7.0 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 Atom® C3XXX Product Family is `0xFFF30000`).

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: `DenvertonNSFsp.fd`
4. Click **Open**. Another window will open and show the Intel® FSP binary information.
5. Click **OK** to close the window.

This FSP Release has the following Binary Description.

FSP-T Header Details:

- This FSP supports the following:
  - Deverton NS SoC
  - Build: 0015.D85
- FSP Header:
  - Signature: FSPH
  - Header Length: 0x48
  - Header Revision: 0x3
  - SpecVersion: 0x20
  - Image Revision: 0x110
  - Image ID: DNV-FSP0
  - Image Size: 0x1000
  - Image Base: 0xfff30000
  - Image Attribute: 0x10030000
  - Configuration Region Offset: 0x18c
  - Configuration Region Size: 0x80
  - API Entry Num: 0x0
  - Temp RAM Init Entry: 0x4cd
  - 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-M Header Details:

- This FSP supports the following:
  - Deverton NS SoC
  - Build: 0015.D85
- FSP Header:
  - Signature: FSPH
  - Header Length: 0x48
  - Header Revision: 0x3
  - SpecVersion: 0x20
  - Image Revision: 0x110
  - Image ID: DNV-FSP0
  - Image Size: 0x90000
  - Image Base: 0xfff32000
  - Image Attribute: 0x20030000
  - Configuration Region Offset: 0x18c
  - Configuration Region Size: 0x200
  - API Entry Num: 0x0
  - Temp RAM Init Entry: 0x0
  - FSP Init Entry: 0x0
  - Notify Phase Entry: 0x0
  - FSP Memory Init Entry: 0x460
  - Temp RAM Exit Entry: 0x46a
  - 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:
  - Deverton NS SoC
  - Build: 0015.D85
- FSP Header:
  - Signature: FSPH
  - Header Length: 0x48
  - Header Revision: 0x3
  - SpecVersion: 0x20
  - Image Revision: 0x110
  - Image ID: DNV-FSP0
  - Image Size: 0x19000
  - Image Base: 0xfffc3000
  - Image Attribute: 0x30030000
  - Configuration Region Offset: 0x18c
  - Configuration Region Size: 0x100
  - API Entry Num: 0x0
  - Temp RAM Init Entry: 0x0
  - FSP Init Entry: 0x0
  - Notify Phase Entry: 0x350
  - FSP Memory Init Entry: 0x0
  - Temp RAM Exit Entry: 0x0
  - FSP Silicon Init Entry: 0x35a
- FSP Extended Header:
  - Signature: FSPE
  - Header Length: 0x18
  - Header Revision: 0x1
  - FSP Producer Id: INTELC
  - FSP Producer Revision: 0x1

§