



Elkhart Lake Intel® Converged Security Engine (Intel® CSE) 15.40 Firmware Release

Release Notes - NDA

August 2021

Revision 15.40.15.2416 [MR1 Release]

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm%20>

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

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

© Intel Corporation

Contents

1	Introduction	6
1.1	Scope of Document	6
1.2	Acronyms	6
2	Release Kit Summary	7
2.1	Release Kit Details	7
2.2	Kit Overview	7
2.3	Contents of Downloaded Kit	7
2.3.1	Image Components.....	8
2.3.2	SW Components.....	9
2.3.3	System Tools	9
2.3.4	DnX Tool	10
2.4	Intel® CSE Release Version Numbering Information.....	11
2.4.1	Intel® CSE Supplemental Versioning Addendum	11
2.5	PMC Release Version Numbering Information	11
2.6	Firmware Update Information	12
2.6.1	Firmware Update Terminology.....	12
2.6.2	Intel® CSE Firmware Upgrade / Downgrade Table.....	13
2.6.3	PMC Firmware Upgrade / Downgrade Table.....	13
2.6.4	PCHC Firmware Upgrade / Downgrade Table	14
2.6.5	Intel® SI Firmware Upgrade / Downgrade Table	14
3	General Information	15
3.1	Important Notes	15
3.2	Hardware Configurations.....	15
3.3	Supported Operating Systems	16
3.4	Best Known Configuration	16
4	Kit Details.....	17
4.1	Build Details.....	17
4.2	PMC Change Log	18
4.3	PCHC Change Log	19
4.4	Intel® Platform Flash Tool Change Log	20
4.4.1	Intel® Flash Image Tool Changes.....	20
5	Intel® CSE New Features - RCR's.....	24
6	Issue Status Definitions.....	25
7	Intel® CSE Fixed Issues	26
8	Intel® CSE Open Issues	27
9	Archive – Fixed Issues.....	28
9.1	Intel® CSE 15.40.10.2252 Version 3.....	28
9.2	Intel® CSE 15.40.10.2204.....	28
9.3	Intel® CSE 15.40.0.2066	28
9.4	Intel® CSE 15.40.2010	30
9.5	Intel® CSE 15.40.0.1005	30
10	Archive – RCRs.....	32



Revision History

Revision Number	Description	Revision Date
15.40.15.2416	MR1 Release	August 2021
15.40.10.2252 V3.2	PR1 Release	May 2021
15.40.10.2252 V3.1	PV Release Supporting FuSa SKU	April 2021
15.40.10.2252 (V3)	B0 BKC Release	April 2021
15.40.10.2252 (V3)	B1 PV Release	March 2021
15.40.10.2204	BKC Release	February 2021
15.40.10.2146	BKC Beta Release	December 2020
15.40.0.2066	BKC Beta Release	September 2020
15.40.0.2010	BKC Release	July 2020
15.40.0.1017	BKC Release	May 2020
15.40.0.1005	BKC Release	April 2020
15.40.0.1000	Alpha Release for BKC	March 2020
15.40.0.7043	BKC Release	December 2019

1 Introduction

1.1 Scope of Document

This document provides component level details of the downloaded kit and the contents of each folder in the kit.

1.2 Acronyms

Term	Description
BIOS	Basic Input Output System
CCM	Client Control Mode (See: HPC)
CIM	Common Information Model
CRB	Intel® Customer Reference Board
FW	Firmware
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
Intel® DAL	Intel® Dynamic Application Loader (Intel® DAL)
Intel® FIT	Intel® Flash Image Tool
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® MEI	Intel® Converged Security Engine Interface (interface between the Management Engine and the Host system)
Intel® PETS	Intel® Platform Enablement Test Suite
Intel® PFT	Platform Flash Tool. This tool supports DnX use case / functionality over USB
Intel® PTT	Intel® Platform Trust Technology
Intel® SI	Intel® Safety Island
IUP	Independently Updatable Partitions
MRC	Memory Reference Code
OS	Operating System
PCH	Platform Control Hub
PMC	power management controller
SPI	Serial Peripheral Interface
SUT	System Under Test
SVN	Security Version Number. Used in Firmware Upgrade / Downgrade capabilities
VCN	Version Control Number. Used in Firmware Upgrade / Downgrade capabilities

2 Release Kit Summary

2.1 Release Kit Details

Intel® CSE Firmware Support	This Firmware supports boot from SPI. Features Supported: Loading and Authentication of firmware partitions like PMC FW, PCHC FW, and Intel® SI FW Intel® ICCS, Intel® Device Protection Technology with Boot Guard, Intel® PTT, PAVP, FuSa, DnX, RPMC, Power Flows
Kit Release	Build Number – 15.40.15.2416
Target Platform	Elkhart Lake Series Platform

2.2 Kit Overview

The kit can be downloaded from Intel® Resource and Design Center (RDC).

Note: A username and password are required to access the website and to log in. User must have an account created for access.

1. After logging in, click on the link 'View All Kits' on the left side of the web page.
2. Click on the corresponding kit number that is to be downloaded.
3. Select and open the appropriate kit component.
4. The Supporting Documentation folder under the selected component contains the following supporting documentation:
 - Release Notes – This document gives an overview of the contents of the entire downloaded component. Also provides the details on closed and open Sightings and bugs with this kit release.
5. Click on the Installation Files folder under the selected component and extract the .zip kit into a folder (Example: C:\).

2.3 Contents of Downloaded Kit

Download the kit, as previously specified, into the directory (C:\). The details of the contents and directory structure are listed below:

2.3.1 Image Components

Image	Description
Intel® CSE	- The Intel® Converged Security Engine firmware contains code and configuration data for Intel® Converged Security Engine functions. - This is one of the regions that are integrated into the final flash image that is built using the Flash Image Tool and is then programmed into the flash. Note: - For more details on building the flash image, please refer to FW Bring up Guide included in the downloaded kit.
DnX	- DnX_Module – A binary file signed by Intel. This file has the DnX logic ME ROM will run. - DnX is Intel's proprietary solution to download Integrated Flash Image (IFWI) to a target machine from a host machine by means of USB cable. DnX flows are executed over fixed USB 2 port
PMC	- The pmc firmware contains code for power management controller functions. - This is one of the regions that is integrated into the final flash image that is built using the Intel® FIT tool and is then programmed into the SPI flash. Note: For more details on the pmc related issues, please refer to pmc changes section of this document.
PCHC	- PCHC – A binary signed by Intel. This file binary is responsible for handling the configuration of PCH clock parameters. Note: - For more details on the PCHC FW related issues, please refer to PCHC changes section of this document.
Intel® SI	- Intel® Safety Island FW. Note: - For more details on the ISI FW related issues, please refer to ISI release notes inside this kit.

2.3.2 SW Components

Additional information can be found in the software installation guide document within this kit.

Installers	Description
ME_SW_DCH	- Intel® MEI driver is installed by running: C:\[skuName_x.x.xxxx]\Installers\ME_SW_DCH\SetupME.exe - To view the installer options, enter the following in a Command window: setup.exe -? And the help dialog should appear.
Intel® MEI Driver	- Intel® MEI is the interface between the host and the Intel® Converged Security Engine. - Drivers and applications on the host that wish to interact with Intel® Converged Security Engine through the host interface use the Intel® MEI host Windows* driver.
Intel® DAL JHI Driver	- This driver is capable of loading and executing code (Intel® DAL Application) in a build-in isolated VM environment. - This driver can utilize Intel® CSE capabilities.

2.3.3 System Tools

Refer to the **System Tools User Guide** for details on tool usage.

Tool	Description
Intel® Flash Image Tool	- Used to assemble the different elements of the SPI flash Descriptor, Intel Reference System BIOS, Intel® CSE, PMC, PCHC and ISI into a single binary image. - Provided as a GUI tool.
Intel® Flash Programming Tool	- Used to write the flash image into the SPI flash device. - EFI, Linux*, and Windows* command line tools provided.
FWUpdate	- Used to update the Intel® Converged Security Engine firmware. - EFI, Linux*, and Windows* command line tools provided. - Reduced Sized Intel® FWUpdate API Library is available under Tools/System_Tools/FWUpdate_RS
Intel® ME Info	- Verifies that Intel® Converged Security Engine (Intel® CSE) firmware is alive and returns data about Intel® CSE. - EFI, Linux*, and Windows* command line tools provided.

Tool	Description
Intel® ME Manuf	- Used on the manufacturing line to validate platform is configured properly. - EFI, Linux*, and Windows* command line tools provided.
Intel® MEU	- Signing and Manifesting tool - For usage instructions refer to the Signing and Manifesting Guide included in the downloaded kit.
Intel® ICC SDK	ICC Software development kit: Intel® ICC SDK library contains data structures and APIs for clock manipulation.

2.3.4 DnX Tool

Tool	Description
Intel® Platform Flash Tool (Intel® PFT)	- Intel implementation of DnX. - For usage instructions refer to the PFT DnX user Guide included in the downloaded kit. Note: Secure Token flows are supported.
Intel® Mobile Signing Utility (Intel® MSU)	Intel® PFT can call Intel® MSU to sign secure tokens.

2.4 Intel® CSE Release Version Numbering Information

Typical release version numbering is as follows,

15.40.y.z (for example: 15.40.0.zzzz) where:

'15' refers to the Intel® Converged Security Engine IP.

'40' represents the associated platform program.

[0-9] – Client platform programs

[10-19] - *Falls Workstations and HEDT

[20-29] - *leys Workstations

[30-99] – Reserved for certain program needs, where

40 – Elkhart Lake

'y' refers to Maintenance and Hot Fix release designations.

'z' refers to firmware release revision.

2.4.1 Intel® CSE Supplemental Versioning Addendum

Intel® CSE firmware kits posted on RDC will use the following versioning format to indicate package updates for components other than Intel® CSE:

The package version will be displayed as **Intel® CSE 15.40.y.z Version X.Y**, where:

X is used for Intel® CSE kit version

Y indicates change to other components (i.e. PCHC, PMC, ISI)

Example for CSE 15.40.10.2252 **Version 3.1**, which includes Version 3 of Intel® CSE SW/Tools and changes to one or more of the IFWI components when compared to previous release of Intel® CSE 15.40.10.2252 **Version 3**.

2.5 PMC Release Version Numbering Information

PMC FW is PCH Sku as well as PCH stepping dependent. For EHL, the pmc, follows this versioning scheme:

Major.Minor.HF.Build (EHL example: **154.01.yy.zzzz**), where:

- **Major = 154 for Elkhart Lake chipset**
- **Minor = PCH SKU Type (Values= 0 for SoC, 1 for LP, and 2 for H)**
- **HF = CVN# -Compatibility/Maintenance Version number**
 - Aligned with PMC Engineering branch.
 - 'yy' refers to the Compatibility/Maintenance build. This field indicates when PMC FW is updated to comply with new requirements, i.e.: HW support or features.
 - 01 = Initial branch support
 - 11 = Maintenance branch with new stepping support

- **Build# -Release version**
 - Use 4 digit # mechanism to align it with CSE FW build#
 - Start build # with 1xx1 for official release
 - Increment last digit to indicate patch's compatibility with HW stepping; if new stepping comes up which needs new patch, re-start it with 1xx1.
 - For any Eng. Release, start build# with 7xxx to differentiate between official vs. debug/Eng. Drop.

2.6 Firmware Update Information

Intel® CSE Firmware Update (either upgrade or downgrade) is evaluated based on the SVN value, the VCN value, or the PV values. These values work in unison and can impose restrictions at the same time.

2.6.1 Firmware Update Terminology

SVN (Security Version Number): will be incremented if there is a high or critical security fix in Intel® CSME Firmware. A downgrade to a lower SVN value will be prohibited:

- **ARB_SVN:** SVN used to prevent rollback of code protecting the system from using known vulnerable code versions.
- **TCB_SVN:** SVN used prevent exposure of user data where data is encrypted with latest SVN on the flash.
- For more details, refer to *Intel® CSME Cumulative Security Enhancements Pass-Through Message*, document ID [608943](#).

VCN (Version Control Number): will be incremented if there is a security fix, a significant firmware change or a new feature addition. A downgrade to lower VCN value will be prohibited.

PV (Production Version): Intel® CSE Firmware will have a PV bit set. Upgrade to a non-PV firmware is not allowed. An update from non-PV version to a PV is allowed.

Update rules:

- If the system is at PV (Production Version) quality firmware that has PV bit set, update to non-PV firmware is not allowed. Only Non-PV to PV is allowed.
 - Example: 14.0.0.zzzz PV cannot upgrade to 15.0.0.zzzz Alpha
- Update to firmware that has lower SVN (Security Version Number) is not allowed.
- Update to firmware that has lower VCN (Version control number) is not allowed.
- Update across major point release is not allowed for example 14.x to 15.x.

2.6.2 Intel® CSE Firmware Upgrade / Downgrade Table

Intel® CSE FW Version	TCB SVN	ARB SVN	VCN	PV (1 or 0)
15.40.15.2416	1	4	16	1
15.40.10.2252 (v3)	1	1	2	1
15.40.10.2204	1	1	2	1
15.40.10.2146	1	1	1	0
15.40.0.2066	1	1	1	0
15.40.0.2010	1	1	1	0
15.40.0.1017	1	1	1	0
15.40.0.1005	1	1	1	0
15.40.0.1000	1	1	1	0
15.40.0.7043	1	1	1	0

2.6.3 PMC Firmware Upgrade / Downgrade Table

PMC FW Version	ARB SVN	PV (1 or 0)
154.01.10.1024	0	1
154.01.10.1021	0	1
154.01.10.1020	0	1
154.01.10.1019	0	1
154.01.10.1015	0	1
154.01.10.1012	0	0
154.01.10.1008	0	0
154.01.01.1018	0	0
154.01.01.1015	0	0
154.01.01.1013	0	0
154.01.01.1012	0	0
154.01.01.7008	0	0

2.6.4 PCHC Firmware Upgrade / Downgrade Table

PCHC FW Version	ARB SVN	PV (1 or 0)
15.40.0.1001	0	1
15.40.0.1000	0	1
15.0.0.7008	0	0
01	0	0

2.6.5 Intel® SI Firmware Upgrade / Downgrade Table

ISI FW Version	ARB SVN	PV (1 or 0)
R55_V1.6	0	1
R053B_V1.4	0	1
R048B	0	1
045A	0	0
042	0	0
036A	0	0

3 General Information

3.1 Important Notes

- This Intel® CSE release mainly targets changes in SW & FW, additional infrastructure and functional updates may be included that are not specifically called out in these release notes.
- The VCN number is increased to '16' and the ARB SVN is increased to '4' in Intel® CSE 15.40.15.2416 release. Update to releases prior to Intel® CSE 15.40.15.2416 are not supported.
- Intel® PFT in this kit requires installation of the DnX Driver. Customers can refer to kit [642344](#) to get the driver.
- Please refer to the communication for Elkhart Lake HSIO Configurations Dependencies. Document # [645826](#). This document provides guidance and reference to relevant resources for HSIO lane configurations
- Customers interested in enabling the Intel® DnX technology, please note the following while fusing the DnX settings during End of Manufacturing (EOM),
 - Starting PV for EHL CSE FW, the default settings for DnX fuse in the FIT tool will be disabled. That is,
 - Intel® FIT Tool-> Download and Execute-> DnxEnabled – set to 'NO' by DEFAULT.
 - If Customer wants to have DnX operations like OEM Debug tokens and Re-Enabling Image Recovery operations available after End-Of-Manufacturing, they **MUST** set this setting to 'YES'.
 - Intel® FIT Tool-> Download and Execute-> DnxEnabled – set to 'YES'
 - Failing to do so will disable DnX fuse on their platform and no DnX operations will be available. All details regarding Intel® DnX technology are covered in the Intel® DnX PFT User guide.
 - **There are no functional changes or restrictions for DnX related to this change.**
- The FWUpdate binary in the image components folder should be used with FWUpdateLcl tool. Run FWupdlcl -f FWUpdate.bin to update the below binaries from the same kit:
 - Intel® CSE FW from this kit
 - Intel® PMC FW from this kit
 - Intel® PCHC FW from this kit
 - Intel® SI FW from this kit

3.2 Hardware Configurations

This release supports the following HW configurations: EHL (QS)

3.3 Supported Operating Systems

- Windows* 10 IoT Enterprise
- Linux* Yocto*

3.4 Best Known Configuration

For the latest Elkhart Lake Series Platforms Best Known Configuration (BKC), please contact the Intel CE.

§

4 Kit Details

4.1 Build Details

Component	Version#
Intel® CSE	15.40.15.2416
PMC	154.01.10.1024
PCHC	15.40.0.1001
Intel® SI	R055_V1.6
DCH SW Installer	2121.15.40.1540
Intel® MEI Driver	2108.100.0.1053 Windows* 10 Submission ID: 1152921505693227861 Windows* 10 Shared Product ID: 400511237
JHI Driver	1.41.2021.0121 Windows* 10 Submission ID: 1152921505692967792 Windows* 10 Shared Product ID: 400490106
System Tools	15.40.15.2417
Intel® PFT	5.10.7.0
Intel® MSU	1.2.0

4.2 PMC Change Log

PMC version	Changes	CSE Release	Stepping
154.01.10.1024	Fixed Issues: OOB System hang while transitioning from S0i2.0 to power down / Reboot state	15.40.15.2416	B
154.01.10.1021	- PMC FW woraround for decoupling certain clock req/ack - PMC FW workaround for LCPLL	15.40.10.2252 v3.2	B
154.01.10.1020	Fixed Issues: PCH temperature will keep a value with production SoC	15.40.10.2252 v3.1	B
154.01.10.1019	Fixed issues: - Resolve CATTRIP during Sx/S0ix Cycles - Vccst Iccmax value used for S0ix exit set incorrectly on C10 Entry - PMC to move V1p05 & Vnn FIVR from PS2 to PS0 before deasserting CPU_C10_Gate signal - xHCI is not de-asserting sidePOK due to PMC enabling fast path for PSF, but not clearing in Sx/HPR/S0ix entry leading to Sx/WR hang - CSE Fast clock requirement handling condition need to be corrected in PMC to prevent hangs in Sx cycle	15.40.10.2252 v3	B
154.01.10.1015	Production signed binary Fixed issues: - Sx is not working while Intel® CSE is running with fast clock - PBO during S5 RTC wake causes to wake from S5 without a pwrbtn press	15.40.10.2204	B
154.01.10.1012	Fixed issues: - During S3/CS/WR Cycling System gets stuck in the S5 state with S5 LED On and cannot wake with PB pressed - isCLK XTAL bringup hang after s0i3	15.40.10.2146	B
154.01.10.1008	B0 Support	15.40.0.2066	B
154.01.01.1018	Updates: - PMC patch w/a UFS lane 8/9 by raising VNN voltage for MCC A0 only - Request PMC FW to handle new PMDOWN message as w/a to Display (P2D) Fixed Issues: - Not able to run SX cycles with platform debug consent "DCI_OOB/Manual/" enabled in BIOS(DAM enabled IFWI)	15.40.0.2010	A0
154.01.01.1015	Updates: - Remove the Spread inversion patch. Fixed Issues: - PMC FW WA for decoupling the IOSF_PRIM clock req/ack. - PMC FW returns incorrect value when queried for CPU crash log address over SB.	15.40.0.1017	A0

PMC version	Changes	CSE Release	Stepping
	- PMC FW should disable SDCARD/EMMC RCOMP flow when SDCARD/EMMC statically disabled. - PMC FW to change RGMII GPIOs' PadResetCfg, for these GPIOs to survive Host Reset and Sx Reset flows (soft-strap update). - PMC FW using incorrect clock frequency define used for time calculations.		
154.01.01.1013	Fixed Issues: - Implemented workaround to enable eSPI on EHL ES0 silicon. - PMC FW to service modPHY handshaking while in DAP polling loop. - Allow reading ISI/PCH Diag Enable Status from SCI endpoint.	15.40.0.1000	A0
154.01.01.1012	Fixed issues: - PMC FW to retain 4us delay for XTAL_FORCE_ON = 1 irrespective of the Fast reset mode or Normal mode of operation. - PMC chipsetinit changes.	15.40.0.1000	A0
154.01.01.7008	Initial release	15.40.0.7043	A0

4.3 PCHC Change Log

PCHC version	Changes	CSE Release	Stepping
15.40.0.1001	PLL settings update	15.40.15.2416	B0
15.40.0.1000	Official release, ready for production	15.40.10.2146	B0
15.0.0.7008	Fixed Issue for Sporadic interface communication errors	15.40.0.2066	B0
V01	Initial release	15.40.0.7043	A0

4.4 Intel® Platform Flash Tool Change Log

Intel® PFT Version	Changes
5.10.7.0	- Fixed 3k signing via CLI - Added DAM support in Intel and OEM Unlock Tokens - Added BIOS Payload Editor GUI for selecting BIOS Payload bits - Upgraded DnX API version to 16.0.0.1268 - Added feature to cancel the intel unlock via the new intel token - Added feature to cancel the OEM key manifest present on the platform - Upgraded openssl version to 1.1.1k - Integrated dldrapi version 18.0.0.7199 - Upgraded adb fastboot version to 30.0.2
5.10.3.5	Removed ISH GDB Debug support from EHL
5.10.0.1	Support for Intel® MSU 1.2.0 with 3k Signing
5.10.0	- Upgraded OpenSSL to 1.1.1d - Ubuntu: Upgrading openssl to 1.1.1g - Adding support for 3k signing in CLI using a key-size switch - Aligned EHL token knobs - Updated FlashUsbDriver to version 1.0.3.0 - Added options in the DnX Capabilities knob
5.9.5	Initial Release

4.4.1 Intel® Flash Image Tool Changes

4.4.1.1 Intel® FIT XML Change Log

Summary of Changes	Intel® CSE Release
- Removed PSE settings - Updated help text	15.40.15.2416
- Updated default values for: - TSN Enable Value - SGMII Host 0 - PD Mode - DnX Enable	15.40.10.2252 v3
Updated default value for PCIeMltVcCont1Conf	15.40.10.2204
- Removed DefaultDataPartitionEnabled - Renamed ISI to Intel® SI - Restructure Intel® SI subpartition - Updated default value for RSA1KSupport - Added PseGbe1obEnable , and PseGbeOobEnable - Removed SMBUSLINKCONFIG and some pmc straps - Added GppC13voltSelect	15.40.10.2146
- Removed All EC region settings - Renamed GBST to Fusa Proof Test - Added PSE Subpartition. FOR TESTING PURPOSES ONLY. Refer to Important notes - Added Software Rebinding option - Removed MCTP Configuration - Removed Intel® AMT Tab	15.40.0.2066

Summary of Changes	Intel® CSE Release
- Added RSA1K Support parameter - Removed Intel® TXT Configurations - Updated the values for CLKReqMapSRC pins - Removed networkingConfigurations settings related vPro platform - Updated TimeSensitiveNetworkingConfigurations - Updated eSPI Configurations - Removed Camera Tab - removed merstcapclrstenabled parameter - Updated DirectConnect Inerg=face (DCI) Configurations - Renamed CPU straps to compute die straps tab - Updated Compute Die straps - Updated pciectrlreversal and pciecontrollerconfig parameters - Updated FlexIO Settings - Updated GPP numbering - Updated values for the following paramters - HostCPUReadAccessIntelRecommended - TopSwapOverride	
- Updated default option for Signing tool in build setting - Updated Descriptor Signing Label - Removed BTGS3Optimize parameter - Updates SmXSupport Label - Updated default value for PCHThrmIRprtngEn - Updated PCH Straps - Updated values for USB3 Port Connector Type Select - Updated Values for USB2 Port Connector Type Select - Removed Intel® Precise Touch AND Stylus Tab - Removed DnXOEMID and OEMVendorID parameters	15.40.0.2010
- Added Descriptor Configuration Settings - Added SmxSupport parameter	15.40.0.1017
- Updated values for FlashComponentsSize - Updated values for HostCPUWriteAccess - Updates under network connectivity tab: Removed TSNGBEPort settings and replaced with SGMII settings - Removed OSEGbE2MAC settings, MGbE Configuration, and OPI/DMI Configuration - Updated values for eSPI/EC Slave 3 frequencies - Updated PMC straps - Updated the values for PCIe Multi VC Controller 1, 2 , and SATA / PCIe Combo Port 0, 1	15.40.0.1005
- Updated clock frequencies - Removed Processor Emulation from Intel® ME Kernel Tab - Added parameter < SkipOemKeysCheck> - Updated Default values for multiple parameters - Removed BCLK Max frequencies - Added TsnGbePortSelectHost - Added EspiEcBusfreq - Updated parameters for Intel® Precise touch and Stylus Tab	15.40.0.1000

4.4.1.2 Intel® FIT XML Compare Against Previous Release

Intel® CSE 15.40.10.2252 v3	Intel® CSE 15.40.15.2416
N/A	<pre> <PseSubPartitionData label="PSE Configuration Sub-Partition"> <InputFile value="" label="PSE Configuration File" help_text="This loads the PSE binary that will be merged into the output image generated by Intel(R) FIT tool." /> </pre>

Intel® CSE 15.40.10.2252 v3	Intel® CSE 15.40.15.2416
<pre> <HostCpuWriteAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,0x000A,,0x001A,,Custom" label="Host CPU / BIOS Write Access Intel Recommended" help_text="This setting determines Host CPU / BIOS write access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see the SPI Programming guide." /> <HostCpuWriteAccessCustom value="0x0" label="Host CPU / BIOS Write Access Custom" help_text="This setting determines Host CPU / BIOS write access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see the SPI Programming guide." /> <HostCpuReadAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,0x000F,,0x001F,,Custom" label="Host CPU / BIOS Read Access Intel Recommended" help_text="This setting determines Host CPU / BIOS read access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see the SPI Programming guide." /> <HostCpuReadAccessCustom value="0x0" label="Host CPU / BIOS Read Access Custom" help_text="This setting determines Host CPU / BIOS read access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see the SPI Programming guide." /> </pre>	<pre> <Length value="0x180000" /> </PseSubPartitionData> <HostCpuWriteAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,,0x000A,,0x001A,,Custom" label="Host CPU / BIOS Write Access Intel Recommended" help_text="This setting determines write access control for the Host CPU / BIOS. For further details on Region Access Control see the Elkheart Lake SPI Programming Guide." /> <HostCpuWriteAccessCustom value="0x0000" label="Host CPU / BIOS Write Access Custom" help_text="This setting determines write access control for the Host CPU / BIOS. For further details on Region Access Control see the SPI and SMIP Programming Guide" /> <HostCpuReadAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,,0x000F,,0x001F,,Custom" label="Host CPU / BIOS Read Access Intel Recommended" help_text="This setting determines read access control for the Host CPU / BIOS. For further details on Region Access Control see the Elkheart Lake SPI Programming Guide." /> <HostCpuReadAccessCustom value="0x0000" label="Host CPU / BIOS Read Access Custom" help_text="This setting determines read access control for the Host CPU / BIOS. For further details on Region Access Control see the SPI and SMIP Programming Guide" /> </pre>
<pre> <MeWriteAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,0x0004,,Custom" label="Intel(R) ME Write Access Intel Recommended" help_text="This setting determines ME write access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see SPI Programming guide." /> <MeWriteAccessCustom value="0x0" label="Intel(R) ME Write Access Custom" help_text="This setting determines ME write access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see SPI Programming guide." /> <MeReadAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,0x000D,,Custom" label="Intel(R) ME Read Access Intel Recommended" help_text="This setting determines ME read access to the other regions. Note: If pre-locking is not set, closemfn will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see SPI Programming guide." /> <MeReadAccessCustom value="0x0" label="Intel(R) ME Read Access Custom" help_text="This </pre>	<pre> <MeWriteAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,,0x0004,,Custom" label="Intel(R) ME Write Access Intel Recommended" help_text="This setting determines write access control for the ME region. For further details on Region Access Control see Elkheart Lake SPI Programming guide further details." /> <MeWriteAccessCustom value="0x0000" label="Intel(R) CSE Write Access Custom" help_text="This setting determines read access control for the ME region. For further details on Region Access Control see Canonlake H / LP SPI Programming guide further details." /> <MeReadAccessIntelRecommended value="0xFFFF" value_list="0xFFFF,,0x000D,,Custom" label="Intel(R) ME Read Access Intel Recommended" help_text="This setting determines read access control for the ME region. For further details on Region Access Control see Elkheart Lake SPI Programming guide further details." /> <MeReadAccessCustom value="0x0000" label="Intel(R) CSE Read Access Custom" help_text="This setting determines read access control for the ME region. For further details on Region Access Control see Canonlake H / LP SPI Programming guide further details." /> </pre>

Intel® CSE 15.40.10.2252 v3	Intel® CSE 15.40.15.2416
setting determines ME read access to the other regions. Note: If pre-locking is not set, closemnf will revert back master access settings to 'golden master access settings'. For further details on Region Access Control see SPI Programming guide." />	
N/A	<pre> <FWPseRegion label="PSE Image"> <Enabled value="Enabled" value_list="Disabled,,Enabled" label="PSE Enable" help_text="This setting Enables / Disables PSE Config in the FWUpdate image." /> <MaxLength value="0x180000" label="PSE Max Length" /> <InputFile value="" label="PSE File" help_text="This loads the PSE Condifuration binary merged into the output image generated by the Intel(R) FIT tool." /> </FWPseRegion> </pre>

5 Intel® CSE New Features - RCR's

RCR #	Change Info
1308149767	Title: DnX flow to support several OEM keys to sign OEM KM Background: Following Intel® CSE support for several OEM keys (refer to OEM Key revocation RCR) , DnX flows need to have support for use cases where the OEM KM is not signed by a single key Change Details: DnX FW module to support several OEM keys Reason: Support DnX flash operations and debug token operations for OEMs using several keys in the OEM KM.
1308003000	Title: Drop support of LMS SW Background: Currently, the DCH SW installer, installs the LMS service which has no use cases on consumer SKU. Change Details: Remove LMS service from Intel® CSE consumer SKU software installer Reason: For efficient development and support of Intel® CSE SW. Customer Action: After upgrading to the new Intel® CSE SW, customers are recommended to uninstall LMS to remove its services from the system
1808525680	Title: Allow for OEM KM and boot critical partitions to be independently updateable through FT partial FW Update Background: - Currently, a full FWUpdate using a full image is required to update the OEM_KM. - Not all boot critical partitions are updated with fault tolerant behavior support. - This RCR requests that OEM KM and boot critical IPs can be independently updateable with Fault-Tolerant (FT) guarantee Change Details: - FWUpdate process shall support Fault Tolerant (FT) on all boot critical IUPs. - FWUpdate shall support updating the OEM_KM independently. - Note: FT PFU is not supported for PMC and PCHC partitions. Reason: Simplify FWUpdate operation. Customer Action: Refer to updated Intel® CSE System tools User Guide.
1308027834	Title: Intel® PTT to comply with TCG Errata for 21H1 Windows TPM Device HLK Background: - TCG periodically publishes Errata updates to the TPM library specification. TCG also publish the PC Client TPM Profile which defines the set of algorithms and commands required for a PC TPM. - The TPM needs to report the versions supported by TCG. Currently, Intel® PTT reports PC client TPM profile version 1.03 and Errata version 1.10 Change Details: Intel® PTT to comply with PC client TPM profile version 1.04 and Errata Version 1.11 for Trusted Platform Module Library Specification, Family "2.0", Revision 01.38 Reason: Comply with latest TCG Errata

6 *Issue Status Definitions*

This document provides sightings and bugs report for Intel® CSE Firmware 15.40 for Elkhart Lake Platform.

Closed Issues: This category will only display closed issues within the current Intel® CSE Kit release. After each release, old issues will be dropped down to the "Archive" section and then new closed issues will take its place back up top for the next release. If an issue is posted in this section, it will indicate that the issue has been verified and fixed within the kit that is being released.

Known Issues: This category will display all Known Issues since the Alpha release and will remain in this section until fixed or noted otherwise. "Known Issues" are still under investigation and may or may not be root caused.

Archive: Fixes in Previous Kits: This category will display all closed issues that were closed in their respective kit#. This section will serve as a history of fixed issues.

7 *Intel® CSE Fixed Issues*

Issue #		Description	Details
N/A	N/A		N/A

8 *Intel® CSE Open Issues*

Issue #	Description	Details	Found in Intel® CSE Build #

9 Archive – Fixed Issues

9.1 Intel® CSE 15.40.10.2252 Version 3

Issue #	Description	Details
22012276690	XML file open failed with Intel® FIT tool version 15.40.10.2204	Component: sw.mfg_tools.fit Root Cause: wrong implementation. Symptoms: Failure to reload XML Workaround: N/A Affected OS: All

9.2 Intel® CSE 15.40.10.2204

Issue #	Description	Details
1308073305	Intel® MEU missing an option to set the "single boot" field in OEM unlock token	Component: sw.mfg_tools.meu Root Cause: wrong implementation. Symptoms: SingleBoot token flag is missing from Intel® MEU generated OEMUnlockToken XML Workaround: N/A Affected OS: All
1308180528	Need to display more informative error message when trying to add SHA1 certificate HASH	Component: sw.mfg_tools.fit Root Cause: wrong implementation. Symptoms: When trying to add SHA1 certificate hash, "Unable to set value" error is displayed Workaround: N/A Affected OS: All

9.3 Intel® CSE 15.40.0.2066

Issue #	Description	Details	Found in CSE Build #
22010466009	GPP settings are missing	Component: sw.mfg_tools.fit Root Cause: wrong implementation. Symptoms: The following GPP settings are missing or duplicated in "GPIO VCCIO Voltage Control" - GPP_D6 has duplicated settings, - GPP_D5 is missing - GPP_E5 is missing	15.40.0.1000

Issue #	Description	Details	Found in CSE Build #
		- GPP_F16 is duplicated, F15 is missing. - GPP_H6 is duplicated, H5 is missing - GPP_T5 is missing - GPP_T0 is mentioned twice Workaround: N/A Affected OS: All	
1307804231/ 22010759904	Mismatching soft strap values in the descriptor region	Component: sw.mfg_tools.fit Root Cause: Definition Gap. Symptoms: decompose IFWI in the same Intel® FIT and then rebuild the image, the descriptor region has mismatches Workaround: N/A Affected OS: All	15.40.0.1017
1508037570	BIOS capsule update hangs after power up when power failure applied around 50-70% capsule update.	Component: sw.mfg_tools.fit & FW.BIOS Root Cause: This issue is partially fixed in Bios and partially in Intel® CSE FIT. Symptoms: Top Swap Boot Size values did not support 4MB. Workaround: N/A Affected OS: All	15.40.0.1017
18011561327	USB3/PCIe Combo Port Setting blocks wrong DCI BSSB USB port	Component: sw.mfg_tools.fit Root Cause: Definition Gap. Symptoms: DCI BSSB over USB3 Port1 Enabled is greyed out Workaround: N/A Affected OS: All	15.40.0.1017
22010674834	PCH GBE ping issues observed	Component: sw.mfg_tools.fit Root Cause: Intel® FIT does not support all possible soft strap configuration RVP/CRB. Symptoms: Fail to Ping. Workaround: N/A Affected OS: All	15.40.0.1017
22010689393	PCIex2 device cannot identification when install to M.2 B Key.	Component: sw.mfg_tools.fit Root Cause: Definition Gap. Symptoms: the PCIe x2 topology will grey out the LOSL selection for M.2 Workaround: N/A Affected OS: All	15.40.0.1017

Issue #	Description	Details	Found in CSE Build #
22010962497 / 1307759179	PCIe CLKREQ Intel® FIT Tool pin name correction	Component: sw.mfg_tools.fit Root Cause: wrong implementation. Symptoms: Pin name needs correction Workaround: N/A Affected OS: All	15.40.0.2010
1508204521	Missing Voltage settings from Intel® FIT	Component: sw.mfg_tools.fit Root Cause: Definition Gap. Symptoms: Intel® HAD voltage setting is removed and is replaced by "GP_R[7:0] Voltage Tolerance" Workaround: N/A Affected OS: All	15.40.0.2010
22010955817	RPCFG (Offset 0x174, 0x178, 0x17c) will show that it is not 0x4. 0x4 is the only validated configuration	Component: sw.mfg_tools.fit Root Cause: wrong implementation. Symptoms: PCH Descriptor Record 110 bit 3:1 has wrong value Workaround: N/A Affected OS: All	15.40.0.2010

9.4 Intel® CSE 15.40.2010

Issue #	Description	Details	Found in CSE Build #
1507897252/ 1507897145	TSN IFWI unable to decompose in Intel® FIT	Component: sw.mfg_tools.fit Root Cause: PSE 0 and PCIe MVC1 are set to FIA Lane 7. Symptoms: Error shows: [Fit Actions] Invalid settings combination. Unable to set "SGMI PSE 0" to "Lane 7". "PCIe Multi VC Controller 1" is already set to "x1 PCIe on Lane 7" Workaround: N/A Affected OS: All	15.40.0.1005

9.5 Intel® CSE 15.40.0.1005

Issue #	Description	Details	Found in CSE Build #
22010142564	FSPI Frequency setting does not generate correct SPI frequency on the EHL CRB	Component: sw.mfg_tools.fit Root Cause: Definition gap. Symptoms: If 50Mhz is set in Intel® FIT UI, IFWI produced only could generate 40MHz on the CRB. Workaround: Use a hex editor to change the values for following soft straps from 0x2 to 0x1: - Fast read clock frequency - Read ID read status clock frequency - Write erase clock frequency Affected OS: All	15.40.0.7043
22010142564 / 1507753051	HSIO Configuration Issue in Intel® FIT Flex I/O tab	Component: sw.mfg_tools.fit Root Cause: Definition gap. Symptoms: USB3PCIeComboPort0 and USB3PCIeComboPort1 are always greyed out and PCIe cannot be configured. Workaround: N/A Affected OS: All	15.40.0.7043
18010029372	Unable to change MAC address using Intel® FIT tool	Component: sw.mfg_tools.fit Root Cause: Definition gap. Symptoms: Unable to assign MAC addresses for any of the 3 Ethernet interfaces on EHL using Intel® FIT tool. Workaround: Do not use the settings in Intel® FIT UI. Affected OS: All	15.40.0.7043

10 Archive – RCRs

RCR #	Change Info	Implemented in CSE Build#
1306375399	Title: OEM Key Revocation Support Background: This RCR aims to support a full key revocation flow for invalidating an old key hash and using a new one before EOM . Change Details • The key revocation feature is enabled for FW Image Signing with 3072-bit RSA and SHA384. • Allow to enable/disable key revocation feature prior to EOM • The key revocation enable/disable FPF shall be burnt and locked at EOM flow • Intel® FIT to show error when key revocation is enabled but only one key is entered • Intel® MEU tool to support revocation_extension • Intel® ME Info too to present the key revocation feature status • Intel® ME Manuf tool to verify fuse content as part of its tests and skip unconfigured key hashes in its tests. Please note that the customer must make sure to input two distinct keys in Intel® FIT when OEM key revocation feature is enabled	15.40.10.2252 Version 3
22011101884	Title: Enable DAM via Token Background: Using a Token o to enable DAM provides a predictable enablement experience. Tokens offer the opportunity to easily prepare multiple systems (64) for debug/testing. Change Details: Support enabling DAM as a separate token knob	15.40.10.2204
1809998754	Title: Deprecation of EPID and replacement with ODCA on Supporting Platforms Background: This RCR aims to remove the support for EPID on the relevant platforms which have ODCA support and make the remote attestation solution implemented solely by On Die CA Change Details: Remove EPID based code from FW and tools: • CLS and TCB processes • EPID based code from sigma process • PTT - EK rekey code based on iCLS • PAVP - EPID based session establishment • DAL - EPID based sigma support • Remove EPID content from Intel® ME Info • Remove CLS supported bit from SKU manager	15.40.10.2146
1606948908	Title: Support Unsigned SCI Configuration Data Background: Intel® CSE firmware and tools support the creation and loading of SCI Configuration data. The initial solution was to save it as a code sub partition called Intel® Safety Island Config (ISIC), but the updated solution is to support unsigned Intel® SI OEM configuration as NVAR Changes: • Remove support for ISIC sub partition from Intel® CSE firmware and tools. • Support a new NVAR in Intel® FIT for optional input of Intel® SI OEM configuration.	15.40.10.2146

RCR #	Change Info	Implemented in CSE Build#
	Intel® FPT shall support updating ISI OEM data based on binary input from the user. Intel® ME Info and ME Manuf shall support displaying and testing Intel® SI OEM Configuration file	
1307561615	Title: Manuf_lock State Shall Be Presented in FWSTS Register Background: Following the changes introduced by the Flexible Manufacturing RCR, the EOM flow was broken down to three levels, each level having its own indication. The indication of level 3, setting the OEM configurations, is an NVAR state "Manuf_Lock" that can be read by using a HECI command. This RCR aims to present Manuf_lock in a FWSTS along with the SOC_Cofig_Lock and Flash Protection Mode Change Details: Add a FWSTS indication for Manuf_lock.	15.40.0.2066
1307631115	Title: Intel® PTT to Comply with TCG EK Credential Profile (Phase 1) Background: Currently, Intel® PTT Endorsement Keys (EKs) are generated and signed by the Intel® CSE On-Die Certificate Authority (CA). Therefore, these EK are SVN based and changed on SVN update. The Trusted Computing Group (TCG) EK Credentials profile defines the requirements on the Trusted Platform Module (TPM) EK and EK credentials. Intel® PTT EK should align to the following definitions for the lifetime of the EK: 1. In TPM 2.0, the lifetime of EK is tied to the Endorsement Policy Seeds (EPS). So long as the EPS does not change, EKs can be recreated with their public area templates. 2. The TPM 2.0 Library provides a means to prevent EKs from being replaced. The command to change the EPS requires Platform Authorization. Change Details: 1. As a first phase for Intel® PTT to comply with the TCG EK Credential Profile, Intel® PTT will store the EK private keys and update the cached keys only in the event of EPS change (while using the same Intel® CSE FW SVN). 2. The second phase is for Intel® PTT to allow regenerating the cached keys after SVN update. This change is submitted as part of another RCR	15.40.0.2066
1409617099	Title: Firmware Update Library Changes Background: The Fwupdate Library is a SW library that supplies APIs for OxMs to write FWUpdate; it wraps HECI commands and FW Update flow not handled by OxMs. Reduced Size Library is used in EFI environment for performing FW update in BIOS.	15.40.0.2066

RCR #	Change Info	Implemented in CSE Build#
	- Full Size Library is used in Windows* and EFI environments though FWUpdLcl tool. Change Details: Add APIs to both FWUpdate libraries for the functions specified below. These checks are relevant only for a full FW update, not for partial FW updates (i.e., updating a single IUP). - Get the type of the PCH SKU from the FWUpdate binary. - Get the type of the Intel® CSE firmware SKU from the FWUpdate binary. - Get the product segment from the FWUpdate binary and from the flash image in the SPI. - Check if downgrade/update is possible by comparing the TCB SVN, ARB SVN, and VCN of all the updatable partitions in the FWUpdate binary and the Flash Image.	
1409600819	Title: Allow OEM-Signed Debug Token to Disable IP FW Authentication Background: Currently, OEMs must sign their FW even during the development stage of their FW because FW authentication is enabled by default on the platform. Without the ability to disable FW authentication, the OEMs must go through the process of signing even for debug or R&D FW. Change Details: Intel® CSE FW to support an option to disable the FW authentication of OEM signed IUPs on the target device by using an OEM-Signed debug token. Intel® MEU and PFT tools will support a new knob "Cancel OEM authentication" for the OEM token.	15.40.0.2066
14011027215	Title: Intel® CSE to Expose Additional Trace Messages without Tokens Background: This RCR aims to facilitate debug for working models without tokens. Change Details: Enable customers to take North Peak traces using a special token from Intel. Intel teams will use the part ID to create and sign this token with trace knobs and send it to the customer. When the token is injected to the flash, customers can take the trace messages including extended white decoder messages	15.40.0.2010
1307182923	Title: Add NVAR to Enable/Disable Support for SMx Algorithms in Intel® PTT Background: This RCR aims to provide customers the ability to enable or disable SMx support in the IFWI. Change Details: - Intel® CSE will support a new Intel® PTT NVAR to enable/ disable SMx algorithms called PTT_SMX_DISABLE. Modifying this NVAR is allowed only before EOM and BIOS EOP. - Intel® CSE System tools will support the PTT_SMX_DISABLE NVAR as follows:	15.40.0.2010

RCR #	Change Info	Implemented in CSE Build#
	- Intel® FIT will support modifying the NVAR value in the IFWI. - Intel® FPT tool will support modifying the NVAR. - Intel® ME Info will support displaying the current value of this NVAR. - Intel® ME Manuf will support this NVAR in EOL VAR testing	
1407223553	Title: On-die Certificate Authority (CA) Background: On-die Certificate Authority enables Intel® CSE to generate and renew application certificates on-die. This feature will provide enhanced performance and reduce costs. Change Details: - Intel® PTT EK certificates to use the On-Die chain - Replace EPID with ECC/ASMF for PAVP - Add support to Sigma 2.1 - Intel® DAL to expose a ECDSA API and sigma 2.1	15.40.0.2010
1406634551	Title: Intel® CSE Needs to Provide Measurements of itself and FW Background: Intel® CSE was computing measurements and writing them to Intel® FIT tool so that BIOS could use them during measured boot. Change Details: - Intel® CSE measurements feature provides trusted boot - The Intel® CSE Measurement code in Intel® CSE ROM and firmware will measure the Intel® CSE firmware binaries in the system flash to the Extend Registers of the PCI MEI device. It allows the host software to measure Intel® CSE firmware, so that the system can meet the requirements of TCG PC Client Specific Implementation Specification.	15.40.0.2010
1507465681	Title: Tools Support for Signature Check for SPI Flash Descriptor Background: This RCR aims to have Intel® CSE tools support the signing of the Intel® CSE descriptor region as well as verification of that signature on boot. Change Details: - Intel® FIT will support signing of the descriptor region - Intel® FIT will support "Exclusion Ranges" for specified offsets within the descriptor region to be excluded from signing protection - Intel® MEU should support the new entry in Intel® OEM key manifest - Intel® FPT tool will check if the descriptor signing is enabled before flashing a new image. If enabled, Intel® FPT will display warning to the user. - Intel® ME Info will display an FPF indicating descriptor signing Intel® ME Manuf and Intel® FPT will support the above FPF as any other FPF.	15.40.0.2010

RCR #	Change Info	Implemented in CSE Build#
1504726115	Title: SPI Full Recovery Over DnX Background: DnX programming is limited to the CSE region only. This RCR aims to extend this capability and enable full programming of SPI image. Change Details: Support programming to SPI the entire DnX image created by Intel® FIT.	15.40.0.2010
1208728849	Title: Intel® PTT Support for SMx Algorithms Background: SMx is a suite of cryptographic algorithms similar to the NIST B-Suite that is approved by the PRC: • SM2 is ECC with a specific curve • SM3 is equivalent to SHA2 • SM4 is equivalent to AES Change Details: Intel® PTT shall include support for the SMx suite of algorithms.	15.40.0.2010
1608117663	Title: Increase ChipsetInit Table Max Size Background: Currently, the maximum chipsetInit size is defined as 8 KB. This is a limitation against enabling all 3 Time Sensitive Networks (TSN) for EHL, since BIOS data is sent as part of chipsetinit and it is larger than the allowed size. Change Details: Change the chipsetinit maximum size to 12KB to accommodate future use.	15.40.0.1000
1306273607	Title: EOM Flow Flexibility Background: The flexible EOM enables performing each level separately with the limitation on the timing of the execution of the 1st level as Fusing & Storage provisioning must occur at the factory as considered to be HW RoT operations. The 2nd and 3rd Levels are not sequential and can be run in any order as designed by the OEMs. The design of the flow is built by customers by using Intel® FIT or Intel® FPT tools. Change Details • Irrelevant features (not supported on current SKU) will not be displayed in Intel® ME Info Tool. • Restructuring Intel® ME Info output into sections where relevant entries are grouped. • "ME FW" column in the PPFs description will be dropped from Intel® ME Info. • Introducing NoReset flag in Intel® FPT to allow postponing a reset upon running -commit commands. • Intel® FPT -closemnf command will only support the -No flag. Other flags are no longer supported. • Intel® FPT no longer supports fparts.txt file. • Intel® FPT no longer supports the following commands: -p, -List, -SPIBAR, -Hashed, & -comparefpf. • Intel® ME Manuf LAN/NOLAN configurations will become part of the config file.	15.40.0.1000

RCR #	Change Info	Implemented in CSE Build#
	Support full comparison of FPFs in Intel® ME Manuf.	
1306690230	Title: Allow FWUpdate to the Same HF Number with a Higher SVN Background: Currently, there is a check that blocks FW Update to a higher SVN if the hot fix number is unchanged. In this case, the customer is required to reflash the SPI image. - Example: Update from 15.40.2.xxxx(SVN3) to 15.40.2.xxxx(SVN4) is prohibited. Change Details - Allow FW Update to a bigger ARB SVN of FTPR sub-partition, regardless of the Hot Fix number in the version. - Allow FW Update to a bigger ARB SVN of FTPR sub-partition, regardless if it is Upgrade (bigger version number) or downgrade (smaller version number). - Other restrictions will remain. For example, update to lower VCN will still be blocked in this case.	15.40.0.1000
1405412646	Title: FuSa - Proof test / Key off support by CSE Background: Safety enhancements are required to meet SIL/ ASIL requirements Change Details - Intel® CSE is invoking pre-BIOS HW test flow, that is triggered by Intel® SI - As part of this test, PCH/CPU HW tests are executed - platform reset is required - This support is configurable in FIT and should be aligned with Intel® SI configuration	15.40.0.1000
1405837097	Title: IBB Redundancy and Fall back mechanism Background: This RCR requires Intel® CSE change for assisting BIOS with redundancy and recovery. Change Details - BIOS Redundancy Mechanism: BIOS has access to top swap configuration, hence can control the setting during BIOS FW update. Intel® CSE assistance is relevant in the following cases: - Coin battery power loss - BIOS setting can be wiped - If BIOS redundancy is enabled, Intel® CSE shall toggle top-swap value change in case Boot Guard failure is detected. - Intel® FIT shall set the configuration of BIOS redundancy support in the IFWI. - Intel® ME Info to display BIOS redundancy configuration.	15.40.0.1000
1209082922	Title: 64-byte unique platform SEEDS (SVN-based and Fixed) Background: This RCR aims to provide platform unique Seed to Host/BIOS. The seed can be used by different SW components to derive various keys used for storage, encryption, and others by doing the following:	15.40.0.7043

RCR #	Change Info	Implemented in CSE Build#
	Change Details - Intel® CSE shall provide an Intel® MEI API for BIOS to retrieve a unique 64-byte random Seed that is generated from platform keys and are bound to Intel® CSE SVN. - Intel® CSE MEI API shall provide BIOS with up to 3 previous seeds that were generated for previous CSE SVNs to allow the host to migrate from old seed to new seed. - in case BtG is disabled only seeds that were generated while BtG was disabled should be returned. - The seed shall also be bound to the Boot Guard Boot Policy Manifest SVN and change when this SVN is updated.	
1306099629	Title: Intel® CSE Firmware Boot Resilience Background: This RCR aims to achieve Intel® CSE FW boot resilience against single bit flash corruption. Single bit flash corruption in critical code area of Intel® CSE FW may result in failure to boot the platform. Change Details - Intel® CSE firmware and tools shall allow configuration with a redundant copy of the Fault Tolerant Partition (FTP) marked as Boot Critical 1 & 2 (BC1/2). - Intel® CSE FW with redundancy will result in an increased flash size. - Configuration option is available in Intel® FIT to enable redundancy (default is disabled). - Intel® ME Info tool shall display whether the platform is configured with redundancy. - Intel® CSE engine will fall back to back-up redundant copy (BC2) only when primary boot critical partition (BC1) experiences corruption failure - Intel® CSE Firmware Status (FWSTS) shall indicate when using BC2 (FWSTS1.bit10) - Intel® CSE shall boot to full normal mode when falling back to BC2 while indicating BC1 requires repair - Intel Platform BIOS sample code to initiate FWUpdate to repair a faulty Intel® CSE BC1/BC2 code.	15.40.0.7043
1306260551	Title: Clean-up Intel® ICC SDK APIs Background: This RCR aims to remove some APIs and some API fields for Intel® ICC SDK. Change Details - Remove the following APIs: GetRegister and SetRegister. - Drop support for the following API fields: "API version" from every HECI call. "HW family" field from "get clock capabilities". "FW version" field from "get clock capabilities".	15.40.0.7043
1306294603	Title: Physical Anti Rollback (ARB) Background: This RCR aims to prevent firmware downgrade based on FW security version (SVN). Change Details	15.40.0.7043

RCR #	Change Info	Implemented in CSE Build#
	• HW ARB protection: Permanent storage of minimal SVN in Field Programmable Fuses (FPFs). • Intel® CSE verifies its SVN against Intel® FPF during boot ◦ Allow Intel® CSE boot only when Intel® CSE FW SVN $\geq$ SVN FPF value ◦ When FPF SVN > FW SVN, the platform will not boot. Recovering requires physical re-flashing. • FPF SVN value update ◦ Triggered by explicit host request via HECI (BIOS or OS) ◦ No self-triggered FPF update by CSE FW ◦ Allows the OEM / IT / owner to have confirmation period/conditions prior to committing ◦ FPF value is defined by CSE based on verified good known SVN value (not provided by SW) • Intel® CSE supports SVN verification for additional components ◦ Boot Guard. DnX module, Root of trust (ROT) and OEM Key Manifest (KM), IDLM	
1407610505	Title: Support FW Update Function to Block End-users from Successfully Doing a Firmware Update of FW/ Any IUPs Background: This RCR aims to extend the ability to block FW update by host, also for Independent Updatable Partitions (IUPs). Change Details • Complete FWU update shall be blocked in this state. • Partial FWU shall be blocked unless the IUP has a policy to ignore the rule. • FWUpdate Library (Full Size and Reduced Size) and Intel® ME Info shall be updated. All supported FW update Enable/ Disable values shall be: ◦ Enable: Full Update enabled. Partial Update enabled. ◦ Disable: Full Update disabled. Partial Update enabled. ◦ Disable: Full and Partial: Full Update disabled. Partial Update disabled. (New Value)	15.40.0.7043