Apollo Lake Platform - Intel® Trusted Execution Engine (Intel® TXE) 3.1 Firmware

Release Notes - NDA

Revision 3.1.75.2351– Maintenance Release
March 2020

Intel Confidential

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

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

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.

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.

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

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

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

Revision History

Revision Number	Description	Revision Date
3.1.75.2351	Maintenance Release	March 2020
3.1.70.2334	IPU 2019.2 PV Release	August 2019
3.1.70.2331	Hot Fix Release	June 2019
3.1.70.2325	Maintenance Release	May 2019
3.1.65.2318 Version 2	Hot Fix Release	May 2019
3.1.65.2318	Hot Fix Release	April 2019
3.1.65.2317	QSR 2019.1 PV	April 2019
3.1.60.2280 Version 2	HR Release	February 2019
3.1.65.2284	QSR 2019.1 Beta Release	January 2019
3.1.60.2280	QSR 2018.4 PV Release	November 2018
3.1.60.2275	QSR 2018.4 Beta Release	October 2018
3.1.55.2269	QSR 2018.2 PV Release	July 2018
3.1.50.2244 Version 2	Hot Fix Release	May 2018
3.1.50.2244	Hot Fix Release	May 2018
3.1.50.2238 Version 2	Hot Fix Release	February 2018
3.1.50.2238	Hot Fix Release	January 2018
3.1.50.2231	Hot Fix Release	January 2018
3.1.50.2229	Hot Fix Release	November 2017
3.1.50.2222	Point Release	October 2017
3.0.13.1144	Hot Fix Release	January 2017
3.0.12.1138	Hot Fix Release	November 2016
3.0.11.1131	Hot Fix Release	October 2016
3.0.10.1129	PV Release – RS1	September 2016
3.0.2.1108	Hot Fix Release	August 2016
3.0.1.1107	Hot Fix Release	July 2016
3.0.1.1105	PV / RS1-Beta Release	July 2016
3.0.0.1078	Beta Release	February 2016
3.0.0.1058	Alpha Release	December 2015

Contents

1 Introduction

This document covers Intel® Trusted Execution Engine firmware for the Apollo Lake platforms.

1.1 Glossary

Acronym/ Terminology	Definition
BIOS	Basic Input Output System
BUP	Bring Up
EC	Embedded Controller
EDK	EFI Development Kits
EOM	End of Manufacturing
EOP	End of Post
FW	Firmware
Intel® DAL	Intel® Dynamic Application Loader
Intel® DnX	Intel® Download and Execute
Intel® FIT	Intel® Flash Image Tool
Intel® FPT	Intel® Flash Programming Tool
Intel® MEU	Intel® Manifest Extension Utility
Intel® PFT	Intel® Platform Flash Tool
Intel® SPD	Intel® Storage Proxy Driver
Intel® TXE	Intel® Trusted Execution Engine
Intel® TXEI	Intel® Trusted Execution Engine Interface
Intel® TXEInfo	Intel® Trusted Execution Engine Info tool
Intel® TXEManuf	Intel® Trusted Execution Engine Manufacturing tool
MCA	Manufacturing Configuration App
MSU	Mobile Signing Utility
OS	Operating System
PAVP	Protected Audio Video Path
RCR	Requirements Change Request
SMIP	Signed Master Image Profile
SPI	Serial Peripheral Interface
SW	Software
USB	Universal Serial Bus

1.2 Important Notes

- Intel® TXE has been updated to include functional and security updates. Users should update to the latest version.
- This Firmware Kit includes an updated version of the Intel® Content License Service (iCLS) Client Software version 1.59.241.0 which must be deployed with the firmware update.
- Please notes that this Intel® CSE 3.1.75.2351 version includes some implemented RCR . Refer here for more details
- Intel® TXE 3.1.50.2238 version 2 HF release included an updated fusing process to solve Apollo Lake fusing issue on the manufacturing line:
    - Intel strongly recommends that all OxMs still in manufacturing move immediately to Intel® TXE 3.1.50.2238 and above FW versions.
    - Starting WW11'18 and onward, Intel no longer provides technical support or allows RMA on any materials being programmed with Intel® TXE FW older than 3.1.50.2238.
- The predecessor of this version was issued as a Point Release, moving from 3.0.x.x to 3.1.x.x. A Point Release indicates that new features and/or changes to existing features have been introduced.
- Based on an in-depth comprehensive security review, the Intel® TXE 3.1 baseline brings architectural security enhancements, improved firmware resilience, and enhancements to Trusted Compute Base recovery.
- Support for Intel® TXE FW 3.0 has been discontinued. All future corrections and/or changes requested will only be built using Intel® TXE FW 3.1 as a base.
- Given the new firmware's baseline changes, Intel recommends performing a full regression validation cycle.
- Customers are requested to always adopt Intel® TXE FW, Intel® TXE Drivers and Intel® TXE tools versions from the same kit. A mix between kits is not supported and might cause unexpected issues.

§§

2 Release Kit Details

The kit can be downloaded from VIP (https://platformsw.intel.com/). See the supported OS(s) and details on kit content below.

2.1 Supported Operating Systems

- Windows* 10 64 bit RS3.
  Please talk to the Intel representative about other OS support.

2.2 VCN Firmware Upgrade / Downgrade Table

Intel® TXE FW Version	SVN #	VCN #	PV (1 or 0)
3.1.75.2351	3	69	1
3.1.70.2334	3	67	1
3.1.70.2331	3	67	1
3.1.70.2325	3	67	1
3.1.65.2318 *version 2*	3	66	1
3.1.65.2318	3	66	1
3.1.65.2317	3	66	1
3.1.60.2280 *version 2*	3	65	1
3.1.60.2280	3	65	1
3.1.60.2275	3	65	1
3.1.55.2269	3	64	1
3.1.50.2244 *version 2*	3	63	1
3.1.50.2244	3	63	1
3.1.50.2238 *Version 2*	3	62	1
3.1.50.2238	3	62	1
3.1.50.2231	3	62	1
3.1.50.2229	3	62	1
3.1.50.2222	3	62	1

- In this Intel® TXE 3.1.75.2351 version, VCN (Version Control Number) has been increased to 69, which prohibits downgrading to earlier Intel® TXE FW .

2.3 Kit content

2.3.1 Documents

- Intel® TXE FW Bring Up Guide – Revision 1.1
- System Tools User Guide – Revision 1.04

- VSCCommn_bin Content – Revision 5.0.2
- Signing and Manifesting Guide – Revision 1.3
- Secure Tokens Guide – Revision 1.1
- SMIP and SPI Programming Guide – Revision 1.0
- Intel® TXE FW 3.1.75.2351 Release Notes

2.3.2 Firmware and Installers

Type	Version
Intel® TXE Firmware	3.1.75.2351
MSI/DCH SW Installer	3.1.50.8284
MUP Specification Version	2.4.4
Intel® Trusted Execution Engine Interface (Intel® TXEI) driver 64b	3.0.0.1115 **Submission ID:** 1152921504627916394 **Shared Product ID:** 1152921504607639069
Intel® Storage Proxy Driver (Intel® SPD) 64b	3.0.0.1104 **Submission ID:** 1152921504626062049 **Shared Product ID:** 1152921504606990879
Intel® Content License Service (Intel® iCLS)	1.59.241.0 **Submission ID:** 1152921504628273045 **Shared Product ID:** 1152921504607863002
Intel® JHI Driver	1915.4.0.1049 **Submission ID:** 1152921504628006168 **Shared Product ID:** 1152921504607685416
Intel® OEM Extension	1811.12.0.1115 **Submission ID:** 1152921504627522255 **Shared Product ID:** 1152921504607441890

2.3.3 Tools

Tool	Version	Description
Intel® FIT	3.1.75.2352	• Provided as both, a GUI and a command line tool • Flash Image Creation Tool • OS Support: Windows* 7 (32-bit) and above

Tool	Version	Description
Intel® FPT	3.1.75.2352	• Command line tool • Writes the flash image into the SPI flash device • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® TXEInfo	3.1.75.2352	• Command line tool • Provides FW version information • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® TXEManuf	3.1.75.2352	• Command line tool • Validates Intel® TXE functionality on the manufacturing line • OS Support: Windows* 7 (32-bit) and above/ EFI
Intel® MEU	3.1.75.2352	• Command line tool • Generates binaries that generates manifests
Intel® PFT	5.9.5.0	• Provided as both, a GUI and a command line tool • Injects tokens and able to update FW on DnX enabled platforms • OS Support: Windows* 7 (32-bit) and above/ Ubuntu
Mobile Signing Utility (MSU)	1.1.2	• Command line tool • Allows PFT to sign secure tokens • OS Support: Windows* 7 (32-bit) and above/ Ubuntu

§§

2.4 iCLS SW Change Log

Intel® Capability License Service (iCLS) Client is included as part of the Intel® TXEI Driver Software installer package within the TXE FW Kits.

Intel® Capability License Service (iCLS) requires internet connectivity over TCP/IP port 443; if the port is blocked by the network, iCLS cannot communicate with the iCLS Service Servers.

iCLS SW Version	Intel® TXE SW Version	Introduced in Intel® TXE FW Kit Version	Changes
1.59.241.0	3.1.50.8284	3.1.75.2351	• TSS updated to 2.3.1 • OpenSSL updated to 1.1.1d • gSoap updated to 2.8.95
1.56.87.0	3.1.50.8276	3.1.70.2334	• OpenSSL updated to 1.1.1c • gSoap updated to 2.8.84 • TSS updated to 2.2.3
1.55.66.0	3.1.50.2316	3.1.70.2325	• gSoap updated to 2.8.83 • SDK/WDK/ADK updated to 19H1 10.0.18362.0 (RTM) • UWD INF installer certified for RS3,RS4,RS5&19H1 • PTT timeout of iCLSClient extended in Linux version (https://hsdes.intel.com/resource/1807335620)

3 Fixed Issues in This Release

Issue #	Title	Details
1307025629	Flash log is filled out with irrelevant error logs in coinless designs	**Description:** In coinless designs, an RTC reset happens on each G3 resume flow causing Flog to be filled out with error messages of RTC reset **Affected Component:** Intel® TXE tools
1306506759	Intel® FPT tool failed to work with iqv interface	**Description:** Intel® FPT tool failed to work with iqv interface in Intel® CSE 3.1.66.2328 version. **Affected Component:** Intel® FPT tool
1307236184	Intel PTT enters failure mode when saving HMAC sequence	**Description:** Due to intel PTT data size being larger than the buffer size, and this leads to the PTT entering in failure mode when using HMAC sequence. **Affected Component:** Intel® TXE FW
1307090460	Maximum allowed ARB FPFs cannot be committed properly	**Description:** Sending command to commit ARB FPFs done successfully but no actual commit is being done. **Affected Component:** Intel® TXE FW

3.1 Mitigated Security Vulnerabilities

This section describes security issue mitigations in Intel® TXE in this Intel Release.

Release	Technical Advisory (TA)	Doc #	Reference Details
Maintenance	PSIRT-TA- PSIRT-TA-2019-10-001	615340	2020.1 MR – Intel® CSME, SPS, TXE, AMT and DAL, PSIRT-TA-2019-10-001
IPU 2019.2	PRIRT-TA-201905	611730	Intel® CSME, Server Platform Services, Trusted Execution Engine, Intel® Active Management Technology and Dynamic Application Loader 2019.2 IPU Advisory, PSIRT-TA-201905-011
2019.1	PSIRT-TA-201901-002	607858	Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology 2019.1 QSR Advisory, PSIRT-TA-201901-002
2018.4	PSIRT-TA-201810-004	603440	Intel® CSME, Server Platform Services, Trusted Execution Engine and Intel® Active Management Technology 2018.4 QSR Advisory, PSIRT-TA-201810-004
2018.2	PSIRT-TA-201805-001	597108	Intel® Converged Security Management Engine (Intel® CSME) Q2’2018 Security Release

3.2 Validation Guidance

This document provides detailed validation guidance associated with this Intel Release.

Release	Doc #	Reference Details
Maintenance	618465	Intel® CSME Firmware and Intel® TXE Firmware Intel Platform Update Security Update Beta
IPU 2019.2	612251	Intel® CSME Firmware and Intel® TXE Firmware Intel Platform Update (IPU) 2019.2
2019.1	608852	Intel® CSME Firmware and Intel® TXE Firmware QSR 2019.1 Validation Guidance
2018.4	604339	Intel® CSME Firmware and Intel® TXE Firmware QSR 2018.4 Validation Guidance

§§

4 Implemented RCRs in This Release

RCR #	Details
1306993589	**Title** Restrict access to USB3 DbC after EOM **Background** ● This RCR aims to enhance the SoC security by adding some restrictions for debug using USB3 DbC. • Currently Intel® CSE supports debug capabilities for the platform before and after the EOM flow with no limitations. **Change Details** ● DCI devices, including BSSB (CCA) and Dbc, will not be able to connect when the platform is locked after EOM. • In order to enable USB3 DbC, customers will need to first unlock the platform using an Intel or OEM token Please refer to ARB doc communication (617164) for more details
2207636724	**Background** The purpose of this RCR is to have a HW based ARB solution for Intel® CSE core modules and loadable modules which can later be extended,To prevent Intel® CSE runtime FW with old ARB SVN from running on a platform where newer ARB SVN has been written to FPF. **Change Details** ▪ Intel® CSE provides direct HW Based ARB protection through dedicated FPF and is controlled by Intel® OEM via FPF enabling/disabling setting. Default is permanently disabled ▪ MEInfo shall display this configuration ▪ Intel® CSE is configured with FPF based SVN verification : ▪ for OEM KM . Intel® CSE shall verify OEM KM manifest SVN value against the FPF stored SVN value.Intel® CSE shall continue to boot only in case the SVN in manifest is greater or equal to the value in FPF. ▪ when loading ucode patch, Intel® CSE shall verify ucode patch SVN value against the FPF stored SVN value. ▪ Tools changes: ▪ Intel® FIT shall have a single enable/disable for HW based ARB as a whole. ▪ Intel® MEInfo shall display the value in the FPFs.

§§

5 Intel® TXE Known Issues

Issue #	Title	Description/ Affected component
N/A	N/A	N/A

§§

6 Intel® TXE Tools Open Issues

Issue #	Title	Description/ Affected component
N/A	N/A	N/A

§§

7 Archive

7.1 Fixed Issues in Previous Releases

Issue #	Title	Details
1607379724	System shows an error when using Intel® FPT tool	**Description: The** system shows an error "Setting Global Reset fail" **Affected Component:** Intel® TXE tools
1507142160	CVT Tool Check fails with software from Intel ® TXE 4.0.15.1295	**Description:** CVT Tool shows a red error message for failure in driver MUP Check. **Affected Component:** Intel® TXE SW
1409308277/ 1507181322	Uninstalling Intel® TXE driver is not working properly.	**Description:** Uninstalling Intel® TXE driver ends successfully, however an error message is being displayed. **Affected Component:** Intel® TXE SW
2207693697/ 1507265550	Intel® TXE software components are not found in control panel after performing software upgrade	**Description**: This is observed when Upgrading from intel® TXE software 3.1.50.2222 to 3.1.50.2284 or to 3.1.50.2307 **Affected Component**: Intel® TXE SW
1306348633	Intel® FPT –CLOSEMNF fails due to incorrect BIOS Lock check on APL	**Description:** N/A **Affected Component:** Intel® TXE Tools
1306260930	Updating NVARs and FPFs with Intel® FPT config file fails.	**Description:** executing "FPT –u –in fpt2.cfg -verbose" to update NVARs and FPFs fails. **Affected Component:** SW.MFG_TOOLS.FPT
1305876457	Platform fails to update a new image after checking the "UPDATE_IMAGE_CHECK" API with "Logical Partition Error" being displayed.	**Description:** platform should be able to update the new "update image" after checking "UPATE_IMAGE_CHECK" API without any error. **Affected Component:** FW

7.2 Implemented RCR in Previous Releases

RCR #	Details
1806691264	**Title:** IPs authentication shall be disabled when OEM unlock token is injected in a fused platform **Background:** Currently, OEM token processing and DFx configuration according to token are performed in the same stage in FW. There is an ordering requirement forcing SMIP authentication to be performed before delivery of PMC payloads, and another ordering requirement for delivering PMC payloads before DFx configuration. **Change Details:** Perform the processing of the unlock token before the authentication of the IPs in the boot flow is done (including SMIP). In case unlock token is present and valid, authentication of all the IPs in the boot flow shall be skipped.