# Intel® CSME Runtime Verification

*Release Notes*

---

*Revision 1.0.0 - Official Release*

*April 2020*

**Intel Confidential**

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. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

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.

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](http://www.intel.com/design/literature.htm).

Intel, 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.

© 2020 Intel Corporation. All rights reserved

# *Revision History*

| Version # | Description | Release Date |
|---|---|---|
| 1.0.0 | Official Release | April 2020 |

# Contents

**1 Introduction .......... 5**

1.1 Scope of Document .......... 5

1.2 Acronyms .......... 5

**2 Supported Configuration .......... 6**

**3 Updates in This Release .......... 7**

3.1 Intel ® CSME 1.0.0 Runtime Verification Features Updates .......... 7

3.2 Intel ® CSME 1.0.0 Runtime Verification Usage Updates .......... 7

**4 Open / Known Issues – to Date .......... 8**

# 1 Introduction

## 1.1 Scope of Document

This document provides release notes details of the Intel® CSME Runtime Verification for supported Intel® CSME FW based platforms.

## 1.2 Acronyms

| Term | Description |
|---|---|
| FW | Firmware |
| IFWI | Integrated Firmware Image |
| Intel® CSME | Intel ® Converged Security and Manageability Engine |
| PCH | Platform Control Hub |
| TGL | Tiger Lake |
| CML | Comet Lake |
| Intel® FIT | Intel® Flash Image Tool |

# 2 Supported Configuration

The Intel® CSME Runtime Verification supports the following configurations:

| Platform Code Name | Intel® CSME Layout Version | Comments |
|---|---|---|
| TGL | 1.7 | |
| CML | 1.6 | The feature was implemented, validation did not start yet. |

# *3 Updates in This Release*

## 3.1 Intel ® CSME 1.0.0 Runtime Verification Features Updates

| Feature | Notes |
|---|---|
| **Image Information** | **Fields:**<br>• FW version<br>• FW SKU Type<br>• PCH Type<br>• PCH Name |
| **Layout Parsing** | **IFWI layout parsing:**<br>• For each sub-partition directory entry<br>o Start and end offsets<br>o Sub partitions name |

## 3.2 Intel ® CSME 1.0.0 Runtime Verification Usage Updates

| Feature | Notes |
|---|---|
| **Supported Image Inputs** | **Image types:**<br>• Full image<br>• CSE Region<br>**Note:** pertains to `CSE Region.bin` binary file created by Intel® FIT decompose folder.<br>• |
| **Arguments** | **Arguments list:**<br>• `--help/-h`<br>Provides help details for each argument.<br>• `--layout/-l`<br>**Required** argument, the layout of the image. Possible values: 1.7 or 1.6.<br>• `--image/-img`<br>**Required** argument, binary image path.<br>• `--CSERegionOnly/-cse`<br>**Optional** argument, defines the input image as a CSE Image type. The default image type is full image. |

# 4 Open / Known Issues – to Date