

Intel® CSME Runtime Verification

Release Notes

Revision 1.1.0 - 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.

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
1.1.0	Official release	April 2020
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 Runtime Verification 1.1.0	7
4 Open / Known Issues – to Date	8
5 Archive	9
5.1 Intel® CSME Runtime Verification 1.0.0	9



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
TGL	1.7
CML	1.6



3 Updates in This Release

3.1 Intel[®] CSME Runtime Verification 1.1.0

- Extending logging information for argument details.
- Enhancing product quality by adding input validation.



4 Open / Known Issues – to Date

5.1 Intel® CSME Runtime Verification 1.0.0

5.1.1 Feature Updates:

Feature	Notes
Image Information	Fields: <ul style="list-style-type: none"> FW version FW SKU Type PCH Type PCH Name
Layout Parsing	IFWI layout parsing: <ul style="list-style-type: none"> For each sub-partition directory entry <ul style="list-style-type: none"> Start and end offsets Sub partitions name

5.1.2 Usage Updates

Feature	Notes
Supported Image Inputs	Image types: <ul style="list-style-type: none"> Full image CSE Region <p>Note: pertains to <i>CSE Region.bin</i> binary file created by Intel® FIT decompose folder.</p> <ul style="list-style-type: none">
Arguments	Arguments list: <ul style="list-style-type: none"> <code>--help/-h</code> Provides help details for each argument. <code>--layout/-l</code> Required argument, the layout of the image. Possible values: 1.7 or 1.6. <code>--image/-img</code> Required argument, binary image path. <code>--CSERegionOnly/-cse</code> Optional argument, defines the input image as a CSE Image type. The default image type is full image.