Release Notes for Intel® TXT and BtG BIOS AC 1.13.19 and SINIT AC 1.13.19 for Comet Lake S Platform

---

April 2020

Intel Confidential

Disclaimer By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

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.

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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.

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.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see here

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.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Revision History

Date	Revision	Changes
September 10th, 2019	1.11.1	Initial Release
October 5th , 2019	1.12.2	WW39 BKC
January 2020	BIOSAC: 1.12.34 & SINIT: 1.12.35	PV Release
January 2020	1.13.0	See Release Notes
February 2020	1.13.11	See Release Notes
March 2020	1.13.15	See Release Notes
March 2020	1.13.16	See Release Notes
March 2020	1.13.17	See Release Notes
March 2020	1.13.18	See Release Notes
April 2020	1.13.19	See Release Notes

ACM Details

Name:	CML_S_BIOSAC_v1.13.19 CML_S_SINIT_v1.13.19
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch or newer for CML-S
Release Information	
BIOS ACM Rev: 1.13.19	Sighting fixed this revision: • Memory unlock failed after clear CMOS with BtG Profile 0T Crashcode Tool: crash_1.3.zip – Password “I accept” Notes: • Memory unlock failed after clear CMOS with BtG Profile 0T • Added special handling for profile-0T with CMOS clear and tpmestablishment=0, • ACM will force txtenabled=1, so that IBB can be verified
SINIT ACM Rev: 1.13.19	Sighting fixed this revision: • Added more Debug output for Trace ACMs. Crashcode Tool: crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.18 CML_S_SINIT_v1.13.15
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch or newer for CML-S
Release Information	

BIOS ACM Rev: 1.13.18	Sighting fixed this revision: • Fix memory lock down issue Crashcode Tool: crash_1.3.zip – Password “I accept” Notes: • If tpmestablishment=0, send LT-CMD-NO-SECRETS before determining txtenabled flag, this will clear BLOCK-MEM-STS which will prevent incorrect determination of RTC clear. • Fixed various other issues related with this to prevent ACM to enter incorrectly into power down flow. Before ACM exit, make sure WAKE-ERROR-STS = 0 to prevent memory lock.
SINIT ACM Rev: 1.13.15	Sighting fixed this revision: • ACM forces PS attributes to be same as legacy platform for vendor WA Crashcode Tool: crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.17 CML_S_SINIT_v1.13.15
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S
Release Information	
BIOS ACM Rev: 1.13.17	Sighting fixed this revision: • Fixed issues regarding PCR extend • Fixed Measurement issue with profile0T/4T Crashcode Tool: • crash_1.3.zip – Password “I accept”

SINIT ACM Rev: 1.13.15	Sighting fixed this revision: • ACM forces PS attributes to be same as legacy platform for vendor WA Crashcode Tool: • crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.16 CML_S_SINIT_v1.13.15
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S
Release Information	
BIOS ACM Rev: 1.13.16	Sighting fixed this revision: • Fix issue with platform reset during S4 Crashcode Tool: • crash_1.3.zip – Password “I accept”
SINIT ACM Rev: 1.13.15	Sighting fixed this revision: • ACM forces PS attributes to be same as legacy platform for vendor WA Crashcode Tool: • crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.15 CML_S_SINIT_v1.13.15
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S
Release Information	

BIOS ACM Rev: 1.13.15	Sighting fixed this revision: • Adding workaround for Setting PCR18_EXTEND bit based on incoming Policy Digest Crashcode Tool: • crash_1.3.zip – Password “I accept”
SINIT ACM Rev: 1.13.15	Sighting fixed this revision: • ACM forces PS attributes to be same as legacy platform for vendor WA Crashcode Tool: • crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.11 CML_S_SINIT_v1.13.0
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S
Release Information	
BIOS ACM Rev: 1.13.11	Sighting fixed this revision: • Observing WinPSEM Error - Minidump - WHEA un correctable error, Bug check 124 , GenuineIntel during S4 / WR cycles Crashcode Tool: • crash_1.3.zip – Password “I accept”
SINIT ACM Rev: 1.13.0	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.13.0

	CML_S_SINIT_v1.13.0
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S
Release Information	
BIOS ACM Rev: 1.13.0	Sighting fixed this revision: • Implement SINIT code changes to support PCR18 extend of SINIT SVN value Crashcode Tool: • crash_1.3.zip – Password "I accept"
SINIT ACM Rev: 1.13.0	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password "I accept"
Name:	CML_S_BIOSAC_v1.12.34_DBG.bin CML_S_BIOSAC_v1.12.34_PW.bin CML_S_SINIT_v1.12.35_DBG.bin CML_S_SINIT_v1.12.35_PW.bin
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • Must have 0xCA MCU Patch for CML-S • Must have this BIOS Change, LINK.
Release Information	

BIOS ACM Rev: 1.12.34	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password “I accept”
SINIT ACM Rev: 1.12.36	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password “I accept”
Name:	CML_S_BIOSAC_v1.12.2_DBG.bin CML_S_SINIT_v1.12.2_DBG.bin
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • N/A
Release Information	
BIOS ACM Rev: 1.12.2	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password “I accept” Notes: • Initial Release

SINIT ACM Rev: 1.12.2	Sighting fixed this revision: • Updated ACM to support all CML CPUIDs Crashcode Tool: • crash_1.3.zip – Password “I accept” Notes: • Initial Release
Name:	CML_S_BIOSAC_v1.11.1_DBG.bin CML_S_BIOSAC_v1.11.1_NPW.bin CML_S_SINIT_v1.11.1_DBG.bin CML_S_SINIT_v1.11.1_NPW.bin
Description:	Startup-ACM for Intel Comet Lake Platforms
Requirements:	Important notes: • N/A
Release Information	
BIOS ACM Rev: 1.11.1	Sighting fixed this revision: • N/A. Crashcode Tool: • crash_1.3.zip – Password “I accept” Notes: • Initial Release
SINIT ACM Rev: 1.11.1	Sighting fixed this revision: • N/A. Crashcode Tool: • crash_1.3.zip – Password “I accept” Notes: • Initial Release

§