Release Notes for Intel® TXT SINIT ACM 1.7.10 & BIOS ACM 1.7.2 for Coffee Lake, Whiskey Lake & Comet Lake U/H Platforms

---

March 2020

Intel Confidential

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
August 1, 2017	0.5.0	**Rev:** 20170726
September 21, 2017	0.5.1	**Rev:** 20170912
November 21, 2017	0.6.0	**Rev:** 20170919
January 11, 2018	1.1.0 BIOSAC & 1.2.0 SINIT	**Rev:** 20180103 & **Rev:** 20171208
May 31, 2018	1.3.0	**Rev:** 20180416 & **Rev:** 20180511
June 14th, 2018	1.4.0 SINIT	**Rev:** 20180611
August 9th, 2018	1.5.0	**Rev:** 20180711
September, 2018	SINIT: 1.6.0	**Rev:** 20180904
July 2019	BIOSAC: 1.6.0 & SINIT: 1.6.1	**Rev:** 20190603
September 2019	BIOSAC: 1.6.0 & SINIT: 1.7.3	**Rev:** 20190603 **Rev:** 20190703
November 2019	BIOSAC: 1.7.0	**Rev:** 20190905
January 2020	BIOSAC: 1.7.1 SINIT: 1.7.8	**Rev:** 20191213 **Rev:** 20191220
January 2020	BIOSAC: 1.7.2 SINIT: 1.7.8	**Rev:** 20200114 **Rev:** 20191220
February 2020	BIOSAC: 1.7.2, BIOSAC 0.7.0(V2) SINIT: 1.7.9	**Rev:** 20200114 **Rev:** 20191213 **Rev:** 20200102
March 2020	BIOSAC: 1.7.2, BIOSAC 0.7.0(V2) SINIT: 1.7.10	**Rev:** 20200114 **Rev:** 20191213 **Rev:** 20200221

SINIT & BIOS ACM Details

	Release Information
Name:	CFL_BIOSAC_20200114_DEBUG_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_NPW_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_1.7.2.BIN CMLV2_BIOSAC_20191213_REL_NT_DEBUG_O1_0.7.0.bin CMLV2_BIOSAC_20191213_REL_NT_PRODUCTION_NPW_O1_0.7.0.bin CMLV2_BIOSAC_20191213_REL_NT_PRODUCTION_O1_0.7.0.bin CFL_SINIT_20200221_DEBUG_REL_NT_O1_1.7.10.bin CFL_SINIT_20200221_PRODUCTION_NPW_REL_NT_O1_1.7.10.bin CFL_SINIT_20200221_PRODUCTION_ REL_NT_O1_1.7.10.bin
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev: 20200102	**SINIT:** Sightings fixed this revision: • Changes related to CVE-2019-0151

	Updated ACM version number to: • 0x4f (for the debug-signed module) • 0x4c (for the NPW-signed module) • 0x4f (for the PW-signed module) SE_SVN • 0x9 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20200114	**BIOSAC CFL/WHL/CML U V1/CML-H:** Sightings fixed this revision: • [22010071911] [CML] Update SCLEAN memory scrubber to MRC v0.0.0.63 Updated ACM version number to: • 0x2b (for the debug-signed module) • 0x28 (for the NPW-signed module) • 0x2b (for the PW-signed module) SE_SVN • 0x8 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
Rev: 20191213	**BIOSAC CML U V2:** Sightings fixed this revision: • Initial Release Updated ACM version number to: • 0x1f (for the debug-signed module) • 0x1c (for the NPW-signed module) • 0x1f (for the PW-signed module) SE_SVN • 0x5 Crashcode Tool: • crash_1.3.zip

	Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20200114_DEBUG_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_NPW_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_1.7.2.BIN CMLV2_BIOSAC_20191213_REL_NT_DEBUG_O1_0.7.0.bin CMLV2_BIOSAC_20191213_REL_NT_PRODUCTION_NPW_O1_0.7.0.bin CMLV2_BIOSAC_20191213_REL_NT_PRODUCTION_O1_0.7.0.bin CFL_SINIT_20200102_DEBUG_1.7.9.BIN CFL_SINIT_20200102_PRODUCTION_NPW_1.7.9.BIN CFL_SINIT_20200102_PRODUCTION_1.7.9.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	

Rev: 20200102	**SINIT:** Sightings fixed this revision: • Updated ACM SVN to 3 • Updated to support more CML Processors affected by CVE-20190124. Updated ACM version number to: • 0x4b (for the debug-signed module) • 0x48 (for the NPW-signed module) • 0x4b (for the PW-signed module) SE_SVN • 0x8 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20200114	**BIOSAC CFL/WHL/CML U V1/CML-H:** Sightings fixed this revision: • [22010071911] [CML] Update SCLEAN memory scrubber to MRC v0.0.0.63 Updated ACM version number to: • 0x2b (for the debug-signed module) • 0x28 (for the NPW-signed module) • 0x2b (for the PW-signed module) SE_SVN • 0x8 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
Rev: 20191213	**BIOSAC CML U V2:** Sightings fixed this revision: • Initial Release Updated ACM version number to: • 0x1f (for the debug-signed module) • 0x1c (for the NPW-signed module) • 0x1f (for the PW-signed module)

	SE_SVN • 0x5 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20200114_DEBUG_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_NPW_1.7.2.BIN CFL_BIOSAC_20200114_PRODUCTION_1.7.2.BIN CFL_SINIT_20191220_DEBUG_1.7.8.BIN CFL_SINIT_20191220_PRODUCTION_NPW_1.7.8.BIN CFL_SINIT_20191220_PRODUCTION_1.7.8.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	

Rev: 20191220	**SINIT:** Sightings fixed this revision: • Fixed TXT failure with Intel 10GB x550 LAN installed. • Fix for failure seen with SINIT 1.7.3 on CFL/WHL/CML platform. Updated algorithm for Vtd quiesce IWD. Updated ACM version number to: • 0x47 (for the debug-signed module) • 0x44 (for the NPW-signed module) • 0x47 (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20200114	**BIOSAC:** Sightings fixed this revision: • [22010071911] [CML] Update SCLEAN memory scrubber to MRC v0.0.0.63 Updated ACM version number to: • 0x2b (for the debug-signed module) • 0x28 (for the NPW-signed module) • 0x2b (for the PW-signed module) SE_SVN • 0x7 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20191213_DEBUG_1.7.1.BIN CFL_BIOSAC_20191213_PRODUCTION_NPW_1.7.1.BIN CFL_BIOSAC_20191213_PRODUCTION_1.7.1.BIN CFL_SINIT_20191220_DEBUG_1.7.8.BIN CFL_SINIT_20191220_PRODUCTION_NPW_1.7.8.BIN CFL_SINIT_20191220_PRODUCTION_1.7.8.BIN

Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev: 20191220	**SINIT:** Sightings fixed this revision: • Fixed TXT failure with Intel 10GB x550 LAN installed. Updated ACM version number to: • 0x47 (for the debug-signed module) • 0x44 (for the NPW-signed module) • 0x47 (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20190905	**BIOSAC:** Sightings fixed this revision: • Update SCLEAN memory scrubber to support additional CML SKUs Updated ACM version number to: • 0x27 (for the debug-signed module) • 0x24 (for the NPW-signed module) • 0x27 (for the PW-signed module)

	SE_SVN • 0x6 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20190905_DEBUG_1.7.0.BIN CFL_BIOSAC_20190905_PRODUCTION_NPW_1.7.0.BIN CFL_BIOSAC_20190905_PRODUCTION_1.7.0.BIN CFL_SINIT_20190703_DEBUG_1.7.3.BIN CFL_SINIT_20190703_PRODUCTION_NPW_1.7.3.BIN CFL_SINIT_20190703_PRODUCTION_1.7.3.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	

Rev: 20190703	**SINIT:** Sightings fixed this revision: • IPU Updates Updated ACM version number to: • 0x33 (for the debug-signed module) • 0x30 (for the NPW-signed module) • 0x33 (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20190905	**BIOSAC:** Sightings fixed this revision: • Added support for CML-H82 • Update SCLEAN memory scrubber to MRC v0.7.1.108 Updated ACM version number to: • 0x23 (for the debug-signed module) • 0x20 (for the NPW-signed module) • 0x23 (for the PW-signed module) SE_SVN • 0x6 Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20190603_DEBUG_1.6.0.BIN CFL_BIOSAC_20190603_PRODUCTION_NPW_1.6.0.BIN CFL_BIOSAC_20190603_PRODUCTION_1.6.0.BIN CFL_SINIT_20190703_DEBUG_1.7.3.BIN CFL_SINIT_20190703_PRODUCTION_NPW_1.7.3.BIN CFL_SINIT_20190703_PRODUCTION_1.7.3.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev: 20190703	**SINIT:** Sightings fixed this revision: • IPU Updates Updated ACM version number to: • 0x33 (for the debug-signed module) • 0x30 (for the NPW-signed module) • 0x33 (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20190603	**BIOSAC:** Sightings fixed this revision: • Added support for CPUID 0xA0660 (CML U62) • [2207532335] Support ACM located in upper 16MB of address space Updated ACM version number to: • 0x1b (for the debug-signed module) • 0x18 (for the NPW-signed module) • 0x1b (for the PW-signed module) Crashcode Tool:

	• crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20190603_DEBUG_1.6.0.BIN CFL_BIOSAC_20190603_PRODUCTION_NPW_1.6.0.BIN CFL_BIOSAC_20190603_PRODUCTION_1.6.0.BIN CFL_SINIT_20190603_DEBUG_1.6.1.BIN CFL_SINIT_20190603_PRODUCTION_NPW_1.6.1.BIN CFL_SINIT_20190603_PRODUCTION_1.6.1.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL/WHL/CML) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev: 20190603	**SINIT:** Sightings fixed this revision: • Added support for CPUID 0xA0660 (CML U62). • [1408648222] Remove previous solution to handle PCR randomization since new one is in place. • [1408747397] Fix initialization of Benchmark data. Updated ACM version number to:

	• 0x33 (for the debug-signed module) • 0x30 (for the NPW-signed module) • 0x33 (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with Infineon TPM 2.0
Rev: 20190603	**BIOSAC:** Sightings fixed this revision: • Added support for CPUID 0xA0660 (CML U62) • [2207532335] Support ACM located in upper 16MB of address space Updated ACM version number to: • 0x1b (for the debug-signed module) • 0x18 (for the NPW-signed module) • 0x1b (for the PW-signed module) Crashcode Tool: • crash_1.3.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with Infineon TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20180711_DEBUG_1.5.0.BIN CFL_BIOSAC_20180711_PRODUCTION_NPW_1.5.0.BIN CFL_BIOSAC_20180711_PRODUCTION_1.5.0.BIN CFL_SINIT_20180904_DEBUG_1.6.0.BIN CFL_SINIT_20180904_PRODUCTION_NPW_1.6.0.BIN CFL_SINIT_20180904_PRODUCTION_1.6.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME

	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev:20180904	**SINIT:** Sightings fixed this revision: • [2205159022] Read public key hash from CPU instead of PCH • [2205369335] Added support for benchmarking all TPM 2.0 commands in SINIT. Updated ACM version number to: • 0x2f (for the debug-signed module) • 0x2c (for the NPW-signed module) • 0x2f(for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0
Rev: 20180711	**BIOSAC:** Sightings fixed this revision: • Added Support for CFL-S82 • Updated SCLEAN Memory Scrubber to MRC v0.7.1.74 • General SINIT Optimizations • Performance optimizations for PCR handling for SNIT • Enabled Benchmarking for Debugging SINIT. Updated ACM version number to: • 0x17 (for the debug-signed module) • 0x14 (for the NPW-signed module) • 0x17 (for the PW-signed module) Crashcode Tool: • crash_1.1.zip

	Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow Tested with STMicro TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20180511_DEBUG_1.3.0.BIN CFL_BIOSAC_20180511_PRODUCTION_NPW_1.3.0.BIN CFL_BIOSAC_20180511_PRODUCTION_1.3.0.BIN CFL_SINIT_20180611_DEBUG_1.4.0.BIN CFL_SINIT_20180611_PRODUCTION_NPW_1.4.0.BIN CFL_SINIT_20180611_PRODUCTION_1.4.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev:20180611	Sightings fixed this revision: • [1407164951] Determine LCP signed or unsigned list based on SignAlg. Use correct offset to calculate the size of digest. • [1407221403] Fix errors with computing digest for LCP authorities Updated ACM version number to: • 0x27 (for the debug-signed module)

	• 0x24 (for the NPW-signed module) • 0x27 (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0
Rev: 20180511	Sightings fixed this revision: • [1407065628, 1505649881] Update SCLEAN memory scrubber to CFL MRC v0.7.1.66 Updated ACM version number to: • 0x13 (for the debug-signed module) • 0x10 (for the NPW-signed module) • 0x13 (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20180511_DEBUG_1.3.0.BIN CFL_BIOSAC_20180511_PRODUCTION_NPW_1.3.0.BIN CFL_BIOSAC_20180511_PRODUCTION_1.3.0.BIN CFL_SINIT_20180416_DEBUG_1.3.0.BIN CFL_SINIT_20180416_PRODUCTION_NPW_1.3.0.BIN CFL_SINIT_20180416_PRODUCTION_1.3.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake and Whisky Lake Processors on Coffee Lake and Whisky Lake Platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL/WHL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE

	○ Boot Guard Profile 5 – FVME • Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused • TXT-enabled processor (CFL) and Chipset (CNP) be present. • TPM must be enabled and activated. • TPM to have AUX and PS indexes defined. • TPM must be provisioned properly before enabling TXT in BIOS setup ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989 ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613 ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229 • All Processor cores & threads, VT-d and TXT must be enabled
Release Information	
Rev:20180416	Sightings fixed this revision: • Added CFL-S82 Support Updated ACM version number to: • 0x23 (for the debug-signed module) • 0x20 (for the NPW-signed module) • 0x23 (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0
Rev: 20180511	Sightings fixed this revision: • [1407065628, 1505649881] Update SCLEAN memory scrubber to CFL MRC v0.7.1.66 Updated ACM version number to: • 0x13 (for the debug-signed module) • 0x10 (for the NPW-signed module) • 0x13 (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0

	Release Information
Name:	CFL_BIOSAC_20171208_DEBUG_1.1.0.BIN CFL_SINITAC_20180103_DEBUG_1.2.0.BIN CFL_BIOSAC_20171208_PRODUCTION_NPW_1.1.0.BIN CFL_SINITAC_20180103_PRODUCTION_NPW_1.2.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake Processors on Coffee Lake platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	  ○ For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	  ○ For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	  ○ For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev:20171208	Sightings fixed this revision: • Updated SE_SVN value to 0x4 Updated ACM version number to: • 0x0b (for the debug-signed module) • 0x08 (for the NPW-signed module) • 0x0b (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0

Rev: 20180103	Sightings fixed this revision: • [1604611571] TPM NV read failures observed during TBOOT • [1604602986] ProcessorSCRTMStatus is showing as 0x0 with BtG Enabled Updated ACM version number to: • 0x1f (for the debug-signed module) • 0x1c (for the NPW-signed module) • 0x1f (for the PW-signed module) Crashcode Tool: • crash_1.1.zip Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with STMicro TPM 2.0
	Release Information
Name:	CFL_BIOSAC_20170919_DEBUG_0.6.0.BIN CFL_SINITAC_20170919_DEBUG_0.6.0.BIN CFL_BIOSAC_20170919_PRODUCTION_NPW_0.6.0.BIN CFL_SINITAC_20170919_PRODUCTION_NPW_0.6.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake Processors on Coffee Lake platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL) and Chipset (CNP) be present.
	• TPM must be enabled and activated.

	• TPM to have AUX and PS indexes defined. • TPM must be provisioned properly before enabling TXT in BIOS setup • All Processor cores & threads, VT-d and TXT must be enabled
Release Information	

Rev: 20170726	Sighting fixed this revision:
	• Updated ACM to use New TPM NV Indexes
	• Please use updated Provisioning tools (See below)
	`// "old" TPM index numbers`
	`TPM20_INDEX_AUX 0x1800003`
	`TPM20_INDEX_LCP_SUP 0x1800001`
	`TPM20_INDEX_LCP_OWN 0x1400001`
	`// "new" TPM index numbers`
	`TPM20_INDEX_AUX 0x01C10102`
	`TPM20_INDEX_LCP_SUP 0x01C10103`
	`TPM20_INDEX_LCP_OWN 0x01C10106`
	o For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	o For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	o For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	o Training was given at CFL Workshop and Training material is available on CDI at Doc #575284
	Updated SINIT ACM version number to:
	• 0x13 (for the debug-signed module)
	• 0x10 (for the NPW-signed module)
	• 0x13 (for the PW-signed module)
	Updated BIOS ACM version number to:
	• 0x03 (for the debug-signed module)
	• 0x00 (for the NPW-signed module)
	• 0x03 (for the PW-signed module)
	Provision Tools:
	• For TPM 2.0 - TPM2 Provisioning Tools. CDI Kit #563989
	• For TPM 1.2 - TPM 1.2 Provisioning Tool. CDI Kit #519613
	• For more information about these command line parameters, refer to provisioning documentation in CDI Kit #543229
	Crashcode Tool:
	• crash_1.1.zip
	Notes:

	• Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with TPM 2.0
Name:	CFL_BIOSAC_20170726_DEBUG_0.5.0.BIN CFL_SINITAC_20170726_DEBUG_0.5.0.BIN
Description:	SINIT & BIOS-AC Module for Intel TXT capable Coffee Lake Processors on Coffee Lake platforms

Requirements:	Important notes:
	• Debug-signed ACM requires TXT-enabled platform with Processor and PCH parts both TXT Debug fused.
	• On CFL platform, ensure one of the following TXT-supported Boot Guard Profile is configured:
	  ○ Boot Guard Profile 0 - No_FVME
	  ○ Boot Guard Profile 4 - FVE
	  ○ Boot Guard Profile 5 – FVME
	• Production-signed ACMs (with or without NPW bit set) require TXT-enabled platform with Processor and Chipset parts both TXT Production fused
	• TXT-enabled processor (CFL) and Chipset (CNP) be present.
	• TPM must be enabled and activated.
	• TPM to have AUX and PS indexes defined.
	• TPM must be provisioned properly before enabling TXT in BIOS setup
	• All Processor cores & threads, VT-d and TXT must be enabled

Release Information	
Rev: 20170726	Sighting fixed this revision: • N/A Updated SINIT ACM version number to: • 0x13 (for the debug-signed module) Updated BIOS ACM version number to: • 0x03 (for the debug-signed module) Provision Tools: • TPM 1.2 – Use BIN.zip (DOS utility) • TPM 2.0 – Use TPM2Prov.efi (EFI64 utility) Crashcode Tool: • crash_1.1.zip

	Notes: • Tested with the TXT EFI tools • Tested SCLEAN flow • Tested with TPM 2.0

§