Intel Confidential

ACMs for Grangeville platform with the HSX-EP and BDX-EP processors.

This release includes BIOS ACM version 1.3.5 and SINIT ACM version 1.3.27 for IPU 2022.1 PV.

Note: The Security Version Number (SVN) of the 1.3.27 SINIT ACM in this release has been incremented which will result in prior versions of the ACM being revoked for protection against rolling back to an earlier version. After updating to this latest ACM, any attempts to then execute a previous ACM version will result in an ACM revocation error when attempting to perform a TXT trusted boot.

Changes for IPU 2022.1 PV Release

Common Vulnerabilities and Exposures (CVEs) Addressed	
Title	**Description**
	No additional CVEs addressed since beta release
Non-CVE related issues addressed	
Title	**Description**
SINIT SVN revocation changes	Code modifications made to enable BIOS ACM to increment SINIT SVN value stored in TPM AUX index in order to revoke SINIT ACM via BIOS ACM. This changes the way the SINIT revocation is triggered. Previously, a special ACM was needed to update the SINIT SVN value stored in the TPM AUX index. With these code modifications, the BIOS ACM updates the SINIT SVN value in the AUX index, so revocation will automatically be performed by running the BIOS ACM instead of a special revocation ACM.

Changes for IPU 2022.1 Beta Release

Common Vulnerabilities and Exposures (CVEs) Addressed	
Title	**Description**
CVE-2021-33123 CVE-2021-33124	For information on CVEs addressed in this ACM package please refer to the *IPU 2022.1 Guidance Document for NDA Customers* (Doc #640127).
Non-CVE related issues addressed	
Title	**Description**