SHA1 support removed from MTL

Dell BIOS Architecture
October 2022

PBA-4772

1.0

A CPG BIOS Architectural Document

Revisions

Version	Description	Author	Date
0.5	Initial Document Draft	JaySC Chen	10/3/2023
0.6	Modify the in scope and out of scope	JaySC Chen	10/4/2023
1.0	Modify the Impacted Internal Components to Security team only.	JaySC Chen	10/5/2023

Table of Contents

1 Solution Overview

1.1 General Overview*

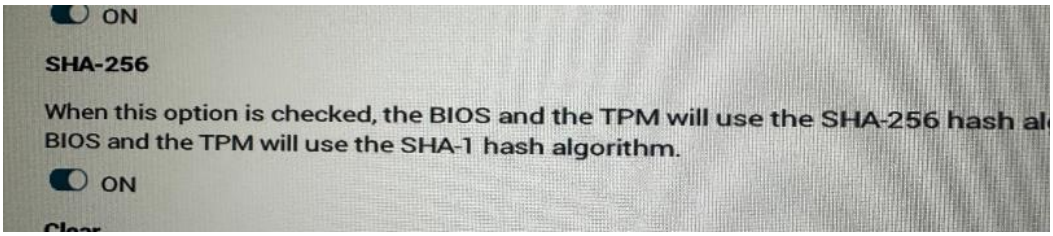
Background/History: According to the Intel document, MTL-TXT-D001_Intel® Trusted Execution Technology, starting from the MeteorLake platform, the TPM SHA-1 hash algorithm has deprecated by Intel, and the default setting controlled by a PCD – PcdDeprecatedCryptoRemove that default value is “TRUE” after Intel MeteorLake platforms.

Disable SHA1 Support

- Starting MeteorLake, we are removing SHA1 support from our code BIOS base and we have a PCD to control this setting at compile time: gPlatformModuleTokenSpaceGuid.PcdDeprecatedCryptoRemove
- In MeteorLake the PcdDeprecatedCryptoRemove PCD value defaults to TRUE. (See ./Intel/MeteorLakePlatSamplePkg/PlatformPkg.dec). This effectively strips out any linkage to HashInstanceLibSha1 and TPM 1.2 support (See ./MeteorLakeBoardPkg/BoardPkg.dsc)
- The main affected components are those related to TCG and TPM support and measurements (PeiBootGuardEventLogLib).
- BIOS defines the platform supported hash algorithms through the HashLib instances linked at compile time; these are project specific settings.

Why do we need this NUDD? As per the Dell Technologies BIOS setup menu, there is a checkbox with SHA-256 that allows customers to uncheck it to switch the hash algorithm to SHA-1, which would go against the Intel Meteor Lake design. Although we have no plans to add more strong hash algorithms now (e.g SHA-384, SHA-512), we can keep the interface and PID for the long term that we can decide to support additional hash algorithms, which means the NUDD is not asking to remove the attribute interface and PID attribute (PID_TPM_HASH_ALGORITHM).

In summary, the implementation is that we need to hide the checkbox and restrict access to attribute capabilities after 23Q4 platforms.



1.2 High-Level Requirements*

At the firmware level, the BIOS should hide the SHA-256 options and configure the default hash algorithm as SHA-256. As for the attribute interface, access to the PID_TPM_HASH_ALGORITHM must be restricted, so it will not allow the attribute to change the hash algorithm.

1.3 User Stories

Customers can't use the bios setup option to uncheck the SHA-256 option to allow the TPM to use the SHA-1 hash algorithm after 23Q4 platforms.

1.4 In Scope vs. Out-of-Scope Declaration

In Scope	Out of Scope
23Q4 platform and further platforms.	Before 23Q4 platforms.

2 Architecture Details

2.1 Architecture Overview

2.2 Description of the Architecture

2.2.1 Solution Description*

The majority of the solution should be covered by BIOS only.

2.2.2 BIOS Section

Since the MeteorLake platform has deprecated the SHA-1 hash algorithm, please ensure the PcdDeprecatedCryptoRemove is setting "TRUE" for these platforms. Meanwhile, the BIOS should hide the options for SHA-256 on VFR and configure the default hash algorithm as SHA-256. Access to the PID_TPM_HASH_ALGORITHM in the attribute interface (BIOSAttributesMgrSmm.c) must be restricted.

SecurityVfr.vfr @DellPkgs\DellPublicPkgs\DellCommonFeaturePkgs\DellSetupFormSets\Protocol\Dxe\Security

```
364: //·SHA·256
365: suppressif·((get·(SecurityData.Tpm_2.ShaPolicy.Suppress)·==·1)·OR
366: ·····|····((ideqval·CommonSetupData.Advanced·==·0)·AND·(get·(SecurityData.Tpm_2.ShaPolicy.Advanced)·==·1)));
367: disableif(get·(SecurityData.Tpm_2.ShaPolicy.Disable)·==·1);
368: ··checkbox
369: ····varid··=·SecurityData.Tpm_2.ShaPolicy.Value,
370: ····prompt·=·STRING_TOKEN(STR_TPM_2_SHA256),
371: ····help···=·STRING_TOKEN(STR_TPM_2_SHA256_HELP),
372: ····flags··=·RESET_REQUIRED,
373: ····default·value·=·get(SecurityData.Tpm_2.ShaPolicy.Default),
374: ··endcheckbox;
375: ··dell_pid·(PID_TPM_HASH_ALGORITHM)
376: endif;
377: endif;
378:
```

2.3 Hardware Dependencies*

The NUDD is HW independent.

1. *The features are not tied to specific system/platforms. Most of HW independent features could be applications or GUI.*
2. *The features readiness can ready for testing after platforms' feature complete*

2.4 Driver Dependencies*

Not needed

2.5 OS Support / Dependencies*

Not needed

2.6 User Interface Impacts

2.6.1 BIOS Setup Information*

Not create new setup option.

2.6.2 Error Messages*

Not create new error messages for this NUDD.

2.6.3 DACI Token / Attribute Usage

Not create a new DACI Token/Attribute for this NUDD.

2.6.4 Other Application User Interactions Information

Not needed

2.7 Architectural Impacts

2.7.1 Dependencies

N/A

2.7.2 Interface Changes

2.7.2.1 DACI Interface
N/A

2.7.2.2 EC-SBIOS Interface
N/A

2.7.2.3 WMI
N/A

2.7.2.4 ACPI
N/A

2.7.2.5 PD Interface
N/A

2.7.2.6 Other External Interfaces
N/A

2.7.3 Factory Implications
No

2.7.4 POC Completed?
No POC was carried out for this NUDD.

2.7.5 Design Assumptions
N/A

2.7.6 Security Evaluation*
Risk assessment questionnaire is attached in the epic PBA-4774 for this NUDD

2.7.7 Privacy Concerns*
N/A

2.7.8 Serviceability
N/A

2.8 Behavior Spec Modification*

The behavior specification may need to describe that the BIOS will hide the checkbox for SHA-256 in the BIOS setup menu if the platform has deprecated the SHA-1 hash algorithm.

3 Impacts to Critical Resources*

This section is meant to highlight any impacts to critical areas of the system as a whole. For example: If a new feature requires an extra 2MB of SPI, and adds an additional 450ms to the boot time, it should be called out in this section.

3.1 NVRAM/Boot Time Impacts

Component	Description	Impacted?	Details
BIOS Boot Time	Indicate if this feature will cause BIOS boot times to increase	No	
NVRAM (Code)	Will the changes associated with this feature require a significant increase in the amount of CODE space required?	No	
NVRAM (Data)	Will the changes associated with this feature require a significant increase in the amount of DATA space required? E.g., large .BMP files, new font sets, etc.	No	

3.2 TPPA (Thermal, Power, Performance, and Acoustic)

No impact the TPPA

4 Impacted Internal Components*

Team	Impacted?	Work Required	Effort (S, M, L, XL)
BIOS Core (AgS)			
BIOS Platform (ODM)			

BIOS Common Features			
BIOS Security Features (NUDDs/	Yes	Hidden the SHA-256 setup option and configure the default hash algorithm as SHA-256 and the attribute must be restricted.	S
EC			
Unified Drivers			
MSR/ISH			
Serviceability			
Signing			
Manageability (Attributes/PlatCfg)			
BIOS Security Solutions (Signing, POC			
iDiags			
Firmware Update/Recovery			
RCAV			
Magneto (Engine)			
Other			

Link to team owners: https://confluence.cpg.dell.com/pages/viewpage.action?pageId=163716847

5 Impacted External Components*

Team	Impacted?	Work Required	Effort (S, M, L, XL)
Factory Tools			
Dell Optimizer			
MyDell/Fusion			
Dell Peripheral Manager			
Factory			
Services			
CFI			

OEM			
Operating System			
Peripherals (e.g. Dell-branded webcams, keyboards, conference pucks)			

6 Risks*

List at least one risk associated with this feature

7 Data Instrumentation / Telemetry Recommendations

Ths NUDD does not need telemetry data.

8 Validation Recommendations*

Need to omit the SHA-256 uncheck test case if the platform is MTL and after.

57	**6. SHA-256 BIOS Option** Ensure that the SHA-256 is checked in the BIOS options for TPM. **Note:** dTPM would perform SHA-256 PCR measurements only if the SHA-256 checkbox selected on the BIOS Setup selection. In the cmd, enter the command: *reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\IntegrityServices* Ensure that the following values are seen: TPMActivePCRBanks REG_DWORD 0x3 (this value may be 0x2 for platforms that don't support Windows 7) TPMDigestAlgID REG_DWORD 0xb	Ensure that the SHA-256 is checked following values are seen: • TPMActivePCRBanks REG_DWORD 0x2 • TPMDigestAlgID REG_DWORD 0xb
58	Ensure that the SHA-256 is unchecked in the BIOS options for TPM. **Note:** dTPM would perform SHA-1 PCR measurements only if SHA-256 checkbox **de-selected** on the BIOS Setup selection. In the cmd, enter the command: *reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\IntegrityServices* Ensure that the following values are seen: TPMActivePCRBanks REG_DWORD 0x1	Ensure that the SHA-256 is unchecked following values are seen: • TPMActivePCRBanks REG_DWORD 0x1 • TPMDigestAlgID REG_DWORD 0x4

9 Open Items

Use this section to list any items which are still under investigation. **Open JIRA tickets for each open item/UI.**

10 Appendix

10.1 Terms and Definitions

Provide list of all terms or definitions needed for complete understanding of the feature to be implemented

Term	Meaning	Description

10.2 Referenced Architectures or Technical Documentation

1. MTL-TXT-D001_Foundation_Trusted_Plat_Intel_TXT_CTT_WW21_2022.pdf
2. 575623_Intel_CBnT_BWG_Rev1p2p5.pdf