Intel® Management Engine (Intel® ME) for Kabylake Platform Framework BIOS Initialization Code Version 3.7.9

Release Notes

March 2020

Revision 3.7.9

Intel Restricted Secret

.

1 Introduction

- Product: Intel® Management Engine (Intel® ME) for Kabylake Platform Framework BIOS Initialization Code
- Developed by: Intel Corporation
- Software version released date: <March 2020>

Note: This document is cumulative and includes information on previous versions. The version information is presented with the newest release first and then regressing through earlier versions.

This program was developed by Intel Corporation. The Licensee has Intel's permission to incorporate this source code into their product, royalty free. This source code may NOT be redistributed to anyone without Intel's written permission. Intel specifically disclaims all warranties, express or implied, and all liability, including consequential and other indirect damages, for the use of this code, including liability for infringement of any proprietary rights, and including the warranties of merchantability and fitness for a particular purpose. Intel does not assume any responsibility for any errors which may appear in this code or any responsibility to update it.

Note: This sample code is to be used in accordance with the DCL document that came with the samples. Refer to the DCL for intended purpose of the sample and recommendations for testing that should not be performed with these samples.

1.1 Purpose of Intel® Management Engine BIOS Initialization Code

This document accompanies Framework Intel® Management Engine for Kabylake Platform Initialization Code Spec. The purpose of this document is to describe the changes in Framework Intel® Management Engine for Kabylake Platform Initialization Code starting from Pre – Alpha 0.5 that directly impacts the Intel ME components functions and code integration to help customers better understand the changes and to help them access their validation plans for each Initialization code release after 0.5.

Note this document may doesn't cover all (line by line) the Initialization code changes but is intended to cover the main changes in ME Initialization code.

1.2 Target Customers

The ME SiC code is intended for use as part of Intel BIOS. The code is compatible with both mobile and desktop products.

1.3 Version Release History

Version	Description	Release Date
0.5.0	Initial Release	December 2015
0.6.0	Updates to all other Kabylake platforms and supported OS.	January 2016
0.6.1	Alpha update	January 2016
0.7.0	Updates to all other Kabylake platforms and supported OS.	Feburary 2016
0.7.1	Beta release update	March 2016
0.7.2	Updates to all other Kabylake platforms and supported OS.	March 2016
0.7.3	Updates to all other Kabylake platforms and supported OS.	April 2016
0.8.0	Updates to all other Kabylake platforms and supported OS.	April 2016
0.8.1	Updates to all other Kabylake platforms and supported OS.	May 2016
0.9.0	Updates to all other Kabylake platforms and supported OS.	May 2016
0.9.1	Updates to all other Kabylake platforms and supported OS.	June 2016
1.0.0	PV release update.	June 2016
1.0.1	Updates to all other Kabylake platforms and supported OS.	June 2016
1.0.2	Updates to all other Kabylake platforms and supported OS.	July 2016
1.0.3	Updates to all other Kabylake platforms and supported OS.	July 2016
1.0.4	Updates to all other Kabylake platforms and supported OS.	Augest 2016
1.0.5	Updates to all other Kabylake platforms and supported OS.	Augest 2016
1.1.0	Updates to all other Kabylake platforms and supported OS.	September 2016
1.2.0	Updates to all other Kabylake platforms and supported OS.	October 2016
1.3.0	Updates to all other Kabylake platforms and supported OS.	October 2016
1.4.0	Updates to all other Kabylake platforms and supported OS.	November 2016
1.4.1	Updates to all other Kabylake platforms and supported OS.	November 2016
1.5.0	Updates to all other Kabylake platforms and supported OS.	December 2016
1.6.0	Updates to all other Kabylake platforms and supported OS.	January 2017
1.7.0	Updates to all other Kabylake platforms and supported OS.	February 2017
1.8.0	Updates to all other Kabylake platforms and supported OS.	February 2017
1.9.0	Updates to all other Kabylake platforms and supported OS.	March 2017
2.0.0	Updates to all other Kabylake platforms and supported OS.	March 2017
2.1.0	Updates to all other Kabylake platforms and supported OS.	April 2017
2.2.0	Updates to all other Kabylake platforms and supported OS.	April 2017
2.3.0	Updates to Coffeelake with PCH Z370 platform support.	May 2017
2.4.0	Updates to Coffeelake with PCH Z370 platform support.	June 2017
2.5.0	Updates to all other Kabylake platforms and supported OS.	June 2017
2.5.1	Updates to all other Kabylake platforms and supported OS.	July 2017

2.6.0	Updates to all other Kabylake platforms and supported OS.	July 2017
2.6.1	Updates to all other Kabylake platforms and supported OS.	August 2017
2.6.2	Updates to all other Kabylake platforms and supported OS.	August 2017
2.7.0	Updates to all other Kabylake platforms and supported OS.	August 2017
2.7.1	Updates to all other Kabylake platforms and supported OS.	August 2017
2.7.2	Updates to all other Kabylake platforms and supported OS.	September 2017
2.8.0	Updates to all other Kabylake platforms and supported OS.	September 2017
2.8.1	Updates to all other Kabylake platforms and supported OS.	October 2017
2.9.0	Updates to all other Kabylake platforms and supported OS.	October 2017
2.9.2	Updates to all other Kabylake platforms and supported OS.	November 2017
3.0.0	Updates to all other Kabylake platforms and supported OS.	December 2017
3.1.0	Updates to all other Kabylake platforms and supported OS.	December 2017
3.1.1	Updates to all other Kabylake platforms and supported OS.	February 2018
3.1.2	Updates to all other Kabylake platforms and supported OS.	March 2018
3.2.0	Updates to all other Kabylake platforms and supported OS.	April 2018
3.2.1	Updates to all other Kabylake platforms and supported OS.	May 2018
3.3.0	Updates to all other Kabylake platforms and supported OS.	May 2018
3.4.0	Updates to all other Kabylake platforms and supported OS.	June 2018
3.5.0	Updates to all other Kabylake platforms and supported OS.	June 2018
3.6.0	Updates to all other Kabylake platforms and supported OS.	July 2018
3.6.1	Updates to all other Kabylake platforms and supported OS.	July 2018
3.6.2	Updates to all other Kabylake platforms and supported OS.	August 2018
3.6.3	Updates to all other Kabylake platforms and supported OS.	September 2018
3.6.4	Updates to all other Kabylake platforms and supported OS.	October 2018
3.6.5	Updates to all other Kabylake platforms and supported OS.	October 2018
3.6.6	Updates to all other Kabylake platforms and supported OS.	November 2018
3.6.7	Updates to all other Kabylake platforms and supported OS.	November 2018
3.6.7.1	Updates to all other Kabylake platforms and supported OS.	December 2018
3.6.8	Updates to all other Kabylake platforms and supported OS.	December 2018
3.6.9	Updates to all other Kabylake platforms and supported OS.	January 2019
3.7.0	Updates to all other Kabylake platforms and supported OS.	March 2019
3.7.1	Updates to all other Kabylake platforms and supported OS.	March 2019
3.7.2	Updates to all other Kabylake platforms and supported OS.	April 2019
3.7.3	Updates to all other Kabylake platforms and supported OS.	May 2019
3.7.4	Updates to all other Kabylake platforms and supported OS.	June 2019
3.7.5	Updates to all other Kabylake platforms and supported OS.	June 2019
3.7.6	Updates to all other Kabylake platforms and supported OS.	August 2019

3.7.7	Updates to all other Kabylake platforms and supported OS.	December 2019
3.7.8	Updates to all other Kabylake platforms and supported OS.	January 2020
3.7.9	Updates to all other Kabylake platforms and supported OS.	March 2020

2 Version 3.7.9 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.9

2.1 New Features

None

2.2 Fixed Bugs

None

3 Version 3.7.8 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.8

3.1 New Features

None

3.2 Fixed Bugs

None

4 Version 3.7.7 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.7

4.1 New Features

None

4.2 Fixed Bugs

4.2.1 Bug1

- **Description/Solution:**

  Memory leak without clearing data in PrepareMeBiosPayload().

- **Affected Files**
  - KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c
  - KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

5 Version 3.7.6 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.6

5.1 New Features

None

5.2 Fixed Bugs

None

6 Version 3.7.5 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.5

6.1 New Features

None

6.2 Fixed Bugs

None

7 Version 3.7.4 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.4

7.1 New Features

None

7.2 Fixed Bugs

None

8 Version 3.7.3 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.3

8.1 New Features

None

8.2 Fixed Bugs

None

9 Version 3.7.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.2

9.1 New Features

None

9.2 Fixed Bugs

None

10 Version 3.7.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.1

10.1 New Features

None

10.2 Fixed Bugs

None

11 Version 3.7.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.7.0

11.1 New Features

None

11.2 Fixed Bugs

None

12 Version 3.6.9 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.9

12.1 New Features

None

12.2 Fixed Bugs

None

13 Version 3.6.8 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.8

13.1 New Features

None

13.2 Fixed Bugs

None

14 Version 3.6.7.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.7.1

14.1 New Features

None

14.2 Fixed Bugs

None

15 Version 3.6.7 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.7

15.1 New Features

None

15.2 Fixed Bugs

None

16 Version 3.6.6 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.6

16.1 New Features

None

16.2 Fixed Bugs

16.2.1 Bug1

- **Description/Solution:**

  Return function status with corresponding MKHI status.

- **Affected Files**

  KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  KabylakeSiliconPkg/Me/Include/MkhiMsgs.h

  KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

17 Version 3.6.5 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.5

17.1 New Features

None

17.2 Fixed Bugs

None

18 Version 3.6.4 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.4

18.1 New Features

None

18.2 Fixed Bugs

None

19 Version 3.6.3 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.3

19.1 New Features

None

19.2 Fixed Bugs

19.2.1 Bug1

- **Description/Solution:**

  BIOS must send EOP in recovery with error modes. Unconditionally Allowed EoP message in HECI driver.

- **Affected Files**

  KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

  KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

20 Version 3.6.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.2

20.1 New Features

None

20.2 Fixed Bugs

None

21 Version 3.6.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.1

21.1 New Features

None

21.2 Fixed Bugs

None

22 Version 3.6.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.6.0

22.1 New Features

None

22.2 Fixed Bugs

None

23 Version 3.5.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.5.0

23.1 New Features

None

23.2 Fixed Bugs

23.2.1 Bug1

- **Description/Solution:**

  JHI validation failing on KBL-YR Pre-Production Parts.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/BeihaiPlugin.c

24 Version 3.4.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.4.0

24.1 New Features

None

24.2 Fixed Bugs

None

25 Version 3.3.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.3.0

25.1 New Features

None

25.2 Fixed Bugs

None

26 Version 3.2.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.2.1

26.1 New Features

None

26.2 Fixed Bugs

None

27 Version 3.2.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.2.0

27.1 New Features

None

27.2 Fixed Bugs

- **Description/Solution:**

  Fix JHI validation issue on KBL-Platforms(U/Y/S and H).

- **Affected Files**

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhid.c

28 Version 3.1.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.1.2

28.1 New Features

None

28.2 Fixed Bugs

None

29 Version 3.1.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.1.1

29.1 New Features

None

29.2 Fixed Bugs

None

30 Version 3.1.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.1.0

30.1 New Features

None

30.2 Fixed Bugs

30.2.1 Bug1

- **Description/Solution:**

  Fix Klocwork issues for ME BIOS.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

31 Version 3.0.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 3.0.0

31.1 New Features

None

31.2 Fixed Bugs

31.2.1 Bug1

- **Description/Solution:**

  While Bus master being disabled on HECI preventins transmission of touch data to UEFI Intel® Precise Touch driver.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

32 Version 2.9.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.9.2

32.1 New Features

None

32.2 Fixed Bugs

32.2.1 Bug1

- **Description/Solution:**

  Fixed issue Intel® Precise Touch does not work while VT-d Enabled..

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

33 Version 2.9.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.9.0

33.1 New Features

None

33.2 Fixed Bugs

None

34 Version 2.8.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.8.1

34.1 New Features

None

34.2 Fixed Bugs

34.2.1 Bug1

- **Description/Solution:**

  Touch does not work when all debug logs disabled.

- **Affected Files**

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

34.2.2 Bug2

- **Description/Solution:**

  Fix KBL ME BIOS Klocwork issue.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

34.2.3 Bug3

- **Description/Solution:**

  Added code to put PTT in idle after this command, due to BIOS doesn't set TPM goIdle bit in s3 exit. That would impact no CSME PG until first TPM driver. command.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

34.2.4 Bug4

- **Description/Solution:**

  PC will stuck while MEInfo tool exxcuted in EFI Shell with iTouch is enabled.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

34.2.5 Bug5

- **Description/Solution:**

  Buffer overflow in PeiHeciHsioMsg routing, due to buffer is to small to hold the response.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/BupMsgs.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

35 Version 2.8.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.8.0

35.1 New Features

None

35.2 Fixed Bugs

None

36 Version 2.7.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.7.2

36.1 New Features

None

36.2 Fixed Bugs

None

37 Version 2.7.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.7.1

37.1 New Features

37.1.1 Feature 1

- **Description/Solution:**

  Changed Debug Verbosity for ME BIOS.

- **Affected Files**

  KabylakeSiliconPkg/Me/ActiveManagement/Sol/Dxe/SerialOverLan.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/UsbProvision.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/FwStsSmbios.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhid.c

  /KabylakeSiliconPkg/Me/Jhi/Dxe/JhiDxe.c

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhis.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

  /KabylakeSiliconPkg/Me/Library/PeiDxeMeShowBufferLib/PeiDxeMeShowBufferLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePolicyPeiLib.c

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

37.2 Fixed Bugs

None

38 Version 2.7.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.7.0

38.1 New Features

None

38.2 Fixed Bugs

None

39 Version 2.6.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.6.2

39.1 New Features

None

39.2 Fixed Bugs

None

40 Version 2.6.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.6.1

40.1 New Features

None

40.2 Fixed Bugs

None

41 Version 2.5.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.5.1

41.1 New Features

None

41.2 Fixed Bugs

None

42 Version 2.5.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.5.0

42.1 New Features

None

42.2 Fixed Bugs

None

43 Version 2.4.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.4.0

43.1 New Features

None

43.2 Fixed Bugs

None

44 Version 2.3.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.3.0

44.1 New Features

None

44.2 Fixed Bugs

None

45 Version 2.2.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.2.0

45.1 New Features

None

45.2 Fixed Bugs

45.2.1 Bug1

- **Description/Solution:**

  Fixed the JHI handle initialization failure.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/BeihaiPlugin.c

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/DxeBeihaiLib.inf

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

46 Version 2.1.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.1.0

46.1 New Features

None

46.2 Fixed Bugs

None

47 Version 2.0.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 2.0.0

47.1 New Features

None

47.2 Fixed Bugs

47.2.1 Bug1

- **Description/Solution:**

  iTouch did not working during POST on customer platform. Changed memory allocation from pool to pages to fix.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeTouchHeciMsgsLib.h

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

47.2.2 Bug2

- **Description/Solution:**

  iTouch is not working even though BIOS code is returning "TouchSensorNotifyDevReady" and "TouchSensorGetDeviceInfo" passing status.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeTouchHeciMsgsLib.h

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

48 Version 1.9.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.9.0

48.1.1 Feature 1

- **Description/Solution:**

  Add EndOfFirmwareEvent for FSP to put all HECI devices to D0i3 state. There is an option available to set DisableD0I3SettingForHeci to 1 to skip putting HECI devices into D0i3 state.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.h

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInitFsp.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.h

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

48.2 Fixed Bugs

48.2.1 Bug1

- **Description/Solution:**

  Cleared the temporary Remote Secure Erase passwords in memory after use.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtHeciDxeLib.c

49 Version 1.8.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.8.0

49.1.1 Feature 1

- **Description/Solution:**

  Prevent the duplicate notify events in FSP wrapper mode.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

49.2 Fixed Bugs

49.2.1 Bug1

- **Description/Solution:**

  Modify KVM Query flow to avoid system hangup at BIOS POST from S4/S5, after Enter User Consent Code into VNC Viewer.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/AsfMsgs.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtHeciDxeLib.c

49.2.2 Bug2

- **Description/Solution:**

  BIOS doesn't wait for CSME FW to complete its loading after enabling ME via HECI.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

50 Version 1.7.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.7.0

50.1 New Features

None

50.2 Fixed Bugs

None

51 Version 1.6.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.6.0

51.1 New Features

51.1.1 Feature 1

- **Description/Solution:**

  ME BIOS code maintain backward compatible update.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeTouchHeciMsgsLib.h

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

  /KabylakeSiliconPkg/Me/Library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

51.2 Fixed Bugs

51.2.1 Bug1

- **Description/Solution:**

  Have MEBx to retain “ME Unconfig on RTC Clear State” settings as following BIOS settings.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeAmtPolicyLib.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeMePolicyLib.h

  /KabylakeSiliconPkg/Me/Include/Private/Library/MeInitLib.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLib/DxeAmtPolicyLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpDebugPrint.c

51.2.2 Bug2

- **Description/Solution:**

  JHI connect message was returning buffer to small, but no retry status bring up to the original caller before retry. Solution to return it to the called of HECI recieve so they can handle it accordingly.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

51.2.3 Bug3

- **Description/Solution:**

  Fix iTouch unable to commnicate with MEInfo tool.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Protocol/IntegratedTouch.h

  /KabylakeSiliconPkg/Me/Include/Protocol/IntegratedTouchHid.h

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.inf

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

51.2.4 Bug4

- **Description/Solution:**

  The length of Filename mismatch is observed with PDT unlock message in debug BIOS.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

51.2.5 Bug5

- **Description/Solution:**

  iTouch is not working during POST on customer platform.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeTouchHeciMsgsLib.h

  /KabylakeSiliconPkg/Me/Include/Protocol/IntegratedTouchHid.h

/KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

/KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

/KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

/KabylakeSiliconPkg/SiPkg.dec

51.2.6 Bug6

- **Description/Solution:**

  Fixed issue as POST time increased if ME close manuf.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/MeFwDowngrade/Dxe/MeFwDowngrade.c

51.2.7 Bug7

- **Description/Solution:**

  KBL BIOS Advertises overlapping memory resources for TPM 2.0. Create a CRS to either represent the DMA buffer and actual device resource range on the platform is configured to use the DMA buffer solution.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Ptt/Smm/Ptt.asl

51.2.8 Bug8

- **Description/Solution:**

  BIOS to implement TPM 2.0 TCG PPI 1.3 for RS2 HLK passing.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Ptt/Smm/Ptt.asl

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.h

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.inf

52 Version 1.5.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.5.0

52.1 New Features

None

52.2 Fixed Bugs

None

53 Version 1.4.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.4.1

53.1 New Features

None

53.2 Fixed Bugs

53.2.1 Bug1

- **Description/Solution:**

  Fixed error message '(A7)ME FW downgrade - Request MeSpiLock Failed.' popup on POST screen after clear CMOS. It due to ME BIOS needs to check FwInitComplete prior to proceeding HeciHmrfpoLock.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeAmtLib.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtHeciDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtPolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/MeFwDowngrade/Dxe/MeFwDowngrade.c

54 Version 1.4.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.4.0

54.1 New Features

54.1.1 Feature 1

- **Description/Solution:**

  Added Touch filter code for customization requests.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

54.1.2 Feature 2

- **Description/Solution:**

  Included UnConfigureOnRtcClearDisable Heci Message into RC policy to control.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Include/MkhiMsgs.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

54.2 Fixed Bugs

54.2.1 Bug1

- **Description/Solution:**

  Fixed Klocwork issue.

- **Affected Files**

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/JhiPlugin.c

/KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.c

54.2.2 Bug2

- **Description/Solution:**

  Fixed native RC Pkg build fail in ME due to 32bit alignment check.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/FwStsSmbios.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/Include/FwStsSmbiosTable.h

  /KabylakeSiliconPkg/Me/Include/Library/MeFwStsLib.h

54.2.3 Bug3

- **Description/Solution:**

  Fixed cold boot time increase about 400~600 ms with RVP 3,7,8 and 11 boards.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpDebugPrint.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

54.2.4 Bug4

- **Description/Solution:**

  Fixed Slow POST times if ME in ME Disable BIOS path.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/FwStsSmbios.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.h

  /KabylakeSiliconPkg/Me/Include/FwStsSmbiosTable.h

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

54.2.5 Bug5

- **Description/Solution:**

  Fixed incorrect usage of sizeof for HeciPdtUnlockMsg routine.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

54.2.6 Bug6

- **Description/Solution:**

  Fix disk information not appearing in WebUI.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

55 Version 1.3.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.3.0

55.1 New Features

None

55.2 Fixed Bugs

None

56 Version 1.2.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.2.0

56.1 New Features

None

56.2 Fixed Bugs

None

57 Version 1.1.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.1.0

57.1 New Features

None

57.2 Fixed Bugs

57.2.1 Bug1

- **Description/Solution:**

  Fix no device info display on Web-UI of M.2 NVMe device, due to wrong contents of NVME Identify Controller command.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

57.2.2 Bug2

- **Description/Solution:**

  Fix ME RC Klocwork issues.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

58 Version 1.0.5 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.5

58.1 New Features

58.1.1 Feature 1

- **Description/Solution:**

  ME code update for header file compliance.

- **Affected Files**

  /KabylakeSiliconPkg/Me/AcpiTables/MeSsdt/MeNvs.asl

  /KabylakeSiliconPkg/Me/AcpiTables/MeSsdt/MeSsdt.asl

  /KabylakeSiliconPkg/Me/Include/Private/Protocol/MeGlobalNvsArea.h

  /KabylakeSiliconPkg/Me/Include/Private/Protocol/MeNvs.h

  /KabylakeSiliconPkg/Me/Include/Private/Protocol/PttNvs.h

  /KabylakeSiliconPkg/Me/Include/Protocol/MeGlobalNvsArea.h

  /KabylakeSiliconPkg/Me/Ptt/Smm/Ptt.asl

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.h

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttNvs.asl

58.1.2 Feature 2

- **Description/Solution:**

  Clear FreePool usage in PEI clear up.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

58.2 Fixed Bugs

58.2.1 Bug1

- **Description/Solution:**

  Fix FSP GCC build boot fail issue.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

58.2.2 Bug2

- **Description/Solution:**

  Removed ASCII Character in comments.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

58.2.3 Bug3

- **Description/Solution:**

  Fix iTouch initialization code to wait ME ready event.

- **Affected Files**

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchComponentName.c

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouchPrivate.h

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.c

59 Version 1.0.4 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.4

59.1 New Features

59.1.1 Feature 1

- **Description/Solution:**

  To update ME doxygen package.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

59.1.2 Feature 2

- **Description/Solution:**

  New Heci message and function implemented

  - Provide a function MANUF_RST_HLT that can be called in PEI phase on S3 resume.
  - Provide a separate function callable at DXE stage (after DID) to poll for FWSTS values for temp_disable.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/BupMsgs.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Include/MkhiMsgs.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

59.2 Fixed Bugs

59.2.1 Bug1

- **Description/Solution:**

  Added additional check for removable device for fix ODD information not shown on AMT WebUI.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

59.2.2 Bug2

- **Description/Solution:**

  Fix incorrect usage of assert_efi_error.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

60 Version 1.0.3 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.3

60.1 New Features

None

60.2 Fixed Bugs

60.2.1 Bug1

- **Description/Solution:**

  iTouch Driver incorrectly binding supprt attaches on all PCI I/O, that will causing problem for other driver in the system.

- **Affected Files**

  KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.c

60.2.2 Bug2

- **Description/Solution:**

  USBr device should not get reported in the Hardware Asset Tables, which is AMT conpliance test issue as AMT_013 fix accordlly.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.inf

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/DxeMeLib.inf

61 Version 1.0.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.2

61.1 New Features

None

61.2 Fixed Bugs

None

62 Version 1.0.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.1

62.1 New Features

62.1.1 Feature 1

- **Description/Solution:**

  Add AMT_SUPPORT FLAG for AMT feature support.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

62.1.2 Feature 2

- **Description/Solution:**

  Added ResetSystemLib instance for SEC/PEI/DXE phase.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/DxeMeLib.inf

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.c

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.h

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.inf

62.2 Fixed Bugs

62.2.1 Bug1

- **Description/Solution:**

  Replaced Cold boot 0xCF9 write 06 with 0xCF9 write 0E and Warm boot 0xCF9 write 04 with 0xCF9 write 06 for issue fix of Active Processor Core values are not reflecting in BIOS and OS.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MeDxeLibInternals.h

62.2.2 Bug2

- **Description/Solution:**

  Fill information in ResetData and DataSize while reset type is EfiResetPlatformSpecific, to avoid we get a NULL of ResetData.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePeiLibInternals.h

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.c

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.inf

62.2.3 Bug3

- **Description/Solution:**

  Updated DeviceId's for ME devices for SOL terminal issue fix.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/MeChipset.h

62.2.4 Bug4

- **Description/Solution:**

  Change all PTT detection to use the FTIF register in the PCH which indicates whether TPM transactions are routed to fTpm or not.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

62.2.5 Bug5

- **Description/Solution:**

  Installs Efi Reset2 PeiService instead the usage of PchResetPpi to be compliant with PI 1.4 spec.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInitFsp.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePeiLibInternals.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/PeiMeLib.inf

62.2.6 Bug6

- **Description/Solution:**

  Issue fix for cannot perform reset once disable ME, then re-enable ME State.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePeiLibInternals.h

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.c

  /KabylakeSiliconPkg/Me/MePlatformReset/RuntimeDxe/MePlatformReset.inf

63 Version 1.0.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 1.0.0

63.1 New Features

None

63.2 Fixed Bugs

None

64 Version 0.9.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.9.1

64.1 New Features

64.1.1 Feature 1

- **Description/Solution:**

  Add flag to eliminate AMT configuration code if non support AMT in PEI phase.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

64.1.2 Feature 2

- **Description/Solution:**

  Solved backward compatibility issue.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/MkhiMsgs.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

64.2 Fixed Bugs

None

65 Version 0.9.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.9.0

65.1 New Features

None

65.2 Fixed Bugs

None

66 Version 0.8.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.8.1

66.1 New Features

None

66.2 Fixed Bugs

66.2.1 Bug1

- **Description/Solution:**

  Change the way BIOS identifies devices before sending data to AMT to unblock Remote Secure Erase flow for remapped drives and RAID volumes.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.h

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.inf

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.h

66.2.2 Bug2

- **Description/Solution:**

  Issue fix for "Local Fw update heci message" does not work.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/MkhiMsgs.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

66.2.3 Bug3

- **Description/Solution:**

  If PTT is in idle the TPM_CRB_CTRL_STS may contain garbage values.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/PeiDxePttPtpLib/PeiDxePttPtpLib.c

66.2.4 Bug4

- **Description/Solution:**

  Remove old HCI drivers for PTT fully PTP compliant

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/PttHciLib.h

  /KabylakeSiliconPkg/Me/Library/PeiDxePttHciLib/PeiDxePttHciLib.c

  /KabylakeSiliconPkg/Me/Library/PeiDxePttHciLib/PeiDxePttHciLib.inf

  /KabylakeSiliconPkg/SiPkgCommonLib.dsc

67 Version 0.8.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.8.0

67.1 New Features

67.1.1 Feature 1

- **Description/Solution:**

  Condition change for CSME Symmetric key distribution.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/CoreBiosMsg.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  /KabylakeSiliconPkg/Me/Include/MeBiosPayloadData.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpDebugPrint.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLib.inf

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLibFsp.inf

67.1.2 Feature 2

- **Description/Solution:**

  Changed the return value for the GET_RSE_PASSWORD in case of empty password.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtHeciDxeLib.c

67.1.3 Feature 3

- **Description/Solution:**

  To update ME doxygen package.

- **Affected Files**

/KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

67.2 Fixed Bugs

67.2.1 Bug1

- **Description/Solution:**

  End of Post Done Protocol cannot be detected properly.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

67.2.2 Bug2

- **Description/Solution:**

  Revise 32bit MMIO address restore when S3 resume flow in end of PEI. After restoring s3 boot script, BIOS should not use 64-bit MMIO address at PEI phase.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Library/MeChipsetLib.h

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Library/PeiDxeMeChipsetLib/PeiDxeMeChipsetLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePolicyPeiLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

67.2.3 Bug3

- **Description/Solution:**

  DRAM INIT data would be always set to 0 by default.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

67.2.4 Bug4

- **Description/Solution:**

  PTT ACPI structure is not aligned between ASL and C code for External BIOS.

- **Affected Files**

/KabylakeSiliconPkg/Me/Ptt/Smm/Ptt.asl

67.2.5 Bug5

- **Description/Solution:**

  Removing unnecessary header file.

- **Affected Files**

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.h

68 Version 0.7.3 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.7.3

68.1 New Features

- **Description/Solution:**

68.1.1 Feature 1

- **Description/Solution:**

  To embellish ME doxygen package.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

68.2 Fixed Bugs

None

69 Version 0.7.2 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.7.2

69.1 New Features

69.1.1 Feature 1

- **Description/Solution:**

  Add BIOS reporting of NVMe device in ME Management Media Table.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.h

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.inf

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/Inventory.h

  /KabylakeSiliconPkg/Me/Include/HeciRegs.h

69.1.2 Feature 2

- **Description/Solution:**

  To embellish include file path in slicon package.

- **Affected Files**

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

  /KabylakeSiliconPkg/Me/Include/Private/Library/DxeBeihaiLib.h

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhid.c

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhid.h

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhis.c

/KabylakeSiliconPkg/Me/Jhi/Dxe/Jhis.h

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/BeihaiPlugin.c

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/bhp_impl_admin.c

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/bhp_impl_ta.c

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/JhiPlugin.h

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

/KabylakeSiliconPkg/Me/Library/Private/DxeJhiSupportLib/File.c

/KabylakeSiliconPkg/Me/Library/Private/DxeJhiSupportLib/MsgPrintf.c

/KabylakeSiliconPkg/Me/Library/Private/DxeJhiSupportLib/StrHelper.c

/KabylakeSiliconPkg/Me/Library/Private/PeiActiveManagementLib/PeiAlertStandardFormat.h

/KabylakeSiliconPkg/Me/Library/Private/PeiDxeAlertStandardFormatLib/AlertStandardFormat.c

/KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.h

69.1.3 Feature 3

- **Description/Solution:**

  Add PostCodes to indicate 'exit' for previous 'entry' PostCodes of ME stages to improve debug capability.

- **Affected Files**

  /KabylakeSiliconPkg/DoxygenInternalOnly/DoxygenPostCode.h

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePeiLibInternals.h

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

69.1.4 Feature 4

- **Description/Solution:**

Modify DXE modules if these module use PCH config data.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInitFsp.inf

69.1.5 Feature 5

- **Description/Solution:**

  Builds a HOB to preserve the Policy data which are needed for ME RC PEI and DXE phases.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInitFsp.inf

  /KabylakeSiliconPkg/Me/Include/AmtPolicyHob.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/AmtDxeConfig.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeAmtLib.h

  /KabylakeSiliconPkg/Me/Include/MePolicyHob.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtDxeLibInternals.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtPolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/DxeAmtLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLib/DxeAmtPolicyLib.c

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLib/DxeAmtPolicyLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLib/DxeAmtPolicyLibrary.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/DxeMeLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MeDxeLibInternals.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLibrary.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLib.inf

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLibFsp.inf

69.1.6 Feature 6

- **Description/Solution:**

  Condition change for Sideband access removal due to PCH code change request.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

69.2 Fixed Bugs

69.2.1 Bug1

- **Description/Solution:**

  Fix KBL Virtual Keyboard is not functional.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

69.2.2 Bug2

- **Description/Solution:**

  Ctrl+P MEBx prompt is not seen during platform boot.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtPolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

69.2.3 Bug3

- **Description/Solution:**

  MEI driver got yellow bang and not disappear in Device manager if ME disable by HDA_SDO jumper.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

69.2.4 Bug4

- **Description/Solution:**

  Fix the warning message shows up during platform boot to EFI shell if ME State disabled.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

70 Version 0.7.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.7.1

70.1 New Features

70.1.1 Feature 1

- **Description/Solution:**

  CSME design change for the message "Set Nanufacturing ME Reset and HALT message", ME RC need to change accordingly.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

70.1.2 Feature 2

- **Description/Solution:**

  Remove useless protocol in BIOSExtensionloader driver.

- **Affected Files**

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.inf

70.1.3 Feature 3

- **Description/Solution:**

  Cosmeticize comments in definition of ME/AMT policy protocol.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Protocol/MePolicy.h

  /KabylakeSiliconPkg/Me/Include/Protocol/AmtPolicy.h

70.2 Fixed Bugs

None

71 Version 0.7.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.7.0

71.1 New Features

71.1.1 Feature 1

- **Description/Solution:**

  Remove redundant policies between PEI and DXE ConfigBlocks, and refine prototype of ME public APIs.

- **Affected Files**

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MeDxeConfig.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/HeciRegs.h

  /KabylakeSiliconPkg/Me/Include/Library/DxeMeLib.h

  /KabylakeSiliconPkg/Me/Include/Library/PeiMeLib.h

  /KabylakeSiliconPkg/Me/Include/Private/Library/HeciInitLib.h

  /KabylakeSiliconPkg/Me/Include/Protocol/HeciProtocol.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/DxeMeLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MeDxeLibInternals.h

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePeiLibInternals.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/MePolicyPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/PeiMeLib.inf

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

/KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

/KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.h

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.h

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLib.inf

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLibFsp.inf

/KabylakeSiliconPkg/SiPkg.dec

71.1.2 Feature 2

- **Description/Solution:**

  RSE requirement change to execute Secure Erase on all connected storge (SATA & NVMe) in a multi-disk configuration which includes RST configurations such as RAID/NGSA.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/AlertStandardFormat.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtHeciDxeLib.c

71.1.3 Feature 3

- **Description/Solution:**

  To prevent H_Rst bit to be set agin when HOST still working in progress.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

71.1.4 Feature 4

- **Description/Solution:**

  Remve PTT switch policy in ME ConfigBlock.

- **Affected Files**

  /KabylakeSiliconPkg/Me/AcpiTables/MeSsdt/MeSsdt.asl

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Protocol/MeGlobalNvsArea.h

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

/KabylakeSiliconPkg/Me/Ptt/Smm/Ptt.asl

71.1.5 Feature 5

- **Description/Solution:**

  Add extra POSTCodes for ME RC.

- **Affected Files**

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.c

  /KabylakeSiliconPkg/Me/BiosExtensionLoader/Dxe/BiosExtensionLoader.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/DxeMeLib.inf

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MeDxeLibInternals.h

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/PeiMeLib.inf

71.1.6 Feature 6

- **Description/Solution:**

  To allow to install HECI PPI for SPS.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.h

71.1.7 Feature 7

- **Description/Solution:**

  To add Produces/Consumes commnet for each GUID.

- **Affected Files**

  /KabylakeSiliconPkg/Me/ActiveManagement/AlertStandardFormat/Dxe/AlertStandardFormatDxe.inf

  /KabylakeSiliconPkg/Me/ActiveManagement/Sol/Dxe/SerialOverLan.inf

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInitFsp.inf

  /KabylakeSiliconPkg/Me/IntegratedTouch/IntegratedTouch.inf

  /KabylakeSiliconPkg/Me/Jhi/Dxe/JhiDxe.inf

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.inf

  /KabylakeSiliconPkg/Me/library/DxeTouchHeciMsgsLib/DxeTouchHeciMsgsLib.inf

/KabylakeSiliconPkg/Me/Library/PeiMeLib/PeiMeLib.inf

/KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.inf

71.1.8 Feature 8

- **Description/Solution:**

  To allow extra MEI messages to ME FW when FW is in recovery mode.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/Private/Library/HeciInitLib.h

  /KabylakeSiliconPkg/Me/Library/Private/PeiDxeHeciInitLib/HeciCore.c

71.2 Fixed Bugs

71.2.1 Bug1

- **Description/Solution:**

  Fix building error for GCC compiler.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

71.2.2 Bug2

- **Description/Solution:**

  Fix ME RC Klocwork issues.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Jhi/Dxe/Jhis.c

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/BeihaiPlugin.c

  /KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/JhiPlugin.c

  /KabylakeSiliconPkg/Me/Ptt/Smm/PttHciSmm.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

71.2.3 Bug3

- **Description/Solution:**

  Fix natural alignment issue for ME RC.

- **Affected Files**

/KabylakeSiliconPkg/Me/Include/AmtForcePushPetHob.h

/KabylakeSiliconPkg/Me/Include/MeBiosPayloadData.h

/KabylakeSiliconPkg/Me/Include/MeBiosPayloadHob.h

71.2.4 Bug4

- **Description/Solution:**

  Fix for the return type of "AmtConfigBlockInit" in ME RC.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeAmtLib/AmtPolicyDxeLib.c

72 Version 0.6.1 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.6.1

72.1 New Features

72.1.1 Feature 1

- **Description/Solution:**

  ME RC uses PCH PSF library and doesn't control PSF registers directly.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/PeiDxeMeChipsetLib/PeiDxeMeChipsetLib.c

  /KabylakeSiliconPkg/ /Library/PeiDxeMeChipsetLib/PeiDxeMeChipsetLib.inf

72.1.2 Feature 2

- **Description/Solution:**

  Refine doxygen syntax in ME RC for all ConfigBlocks and Policies..

- **Affected Files**

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/AmtDxeConfig.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/AmtPeiConfig.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MeDxeConfig.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Include/Protocol/AmtPolicy.h

  /KabylakeSiliconPkg/Me/Include/Protocol/MePolicy.h

72.1.3 Feature 3

- **Description/Solution:**

  To replace ME HOB by Silicon HOB for ME pre-mem ConfigBlock.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/Include/CoreBiosMsg.h

/KabylakeSiliconPkg/Me/Include/MePolicyHob.h

/KabylakeSiliconPkg/Me/Library/DxeMeLib/HeciMsgDxeLib.c

/KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

/KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.c

/KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.inf

/KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLibrary.h

/KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

/KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/DxeBeihaiLib.inf

/KabylakeSiliconPkg/Me/Library/Private/DxeBeihaiLib/Mei.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLib.inf

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PeiMeInitLibFsp.inf

/KabylakeSiliconPkg/SiPkg.dec

72.2 Fixed Bugs

None

73 Version 0.6.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.6.0

73.1 New Features

73.1.1 Feature 1

- **Description/Solution:**

  Use MeSetup to replace ME options in SetupVariable, revise and refine some unsed policies.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MeDxeConfig.h

  /KabylakeSiliconPkg/Me/Include/ConfigBlock/MePeiConfig.h

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLib/DxeAmtPolicyLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMeLib/MePolicyDxeLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/DxeMePolicyLib/DxeMePolicyLibrary.h

  /KabylakeSiliconPkg/Me/Library/PeiAmtPolicyLib/PeiAmtPolicyLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMeLib/HeciMsgPeiLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLibrary.h

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MeInitPostMem.c

  /KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

73.1.2 Feature 2

- **Description/Solution:**

  Remove FSP_FLAG build switch and relative code to accords with FSP and EFI build.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/EndOfPost.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.c

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/HeciInit.inf

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/HeciInit.h

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/MbpData.c

/KabylakeSiliconPkg/Me/Library/Private/PeiMeInitLib/PchMeUma.c

73.1.3 Feature 3

- **Description/Solution:**

  Add EOP message policy,

  - For fsp+coreboot, the EOP message will be send at End of PEI.
  - For fsp+wrapper and EDKII build, the EOP will be sent at ReadyToBoot event (DXE phase). → Default

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/PeiMePolicyLib/PeiMePolicyLib.c

73.2 Fixed Bugs

73.2.1 Bug1

- **Description/Solution:**

  Fixed EOP message in S3 resume path for FSP build.

- **Affected Files**

  /KabylakeSiliconPkg/Me/HeciInit/Dxe/MeInitFsp.c

73.2.2 Bug2

- **Description/Solution:**

  Revised PcdAmtEnable set to FALSE case was an ASSERT in platform code.

- **Affected Files**

  /KabylakeSiliconPkg/Me/Library/DxeAmtLibNull/DxeAmtLibNull.c

  /KabylakeSiliconPkg/Me/Library/DxeAmtLibNull/DxeAmtLibNull.inf

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLibNull/DxeAmtPolicyLibNull.c

  /KabylakeSiliconPkg/Me/Library/DxeAmtPolicyLibNull/DxeAmtPolicyLibNull.inf

  /KabylakeSiliconPkg/SiPkgDxeLib.dsc

74 Version 0.5.0 Details

This version is based on Intel® Management Engine Framework BIOS Initialization Code 0.5.0

74.1 New Features

None

74.2 Fixed Bugs

None

74.3 Known Issues

None