

Ice Lake Signing and Manifesting Guide

User Guide

Revision 1.0

June 2019

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>

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

Copyright © 2019, Intel Corporation. All rights reserved.

Contents

1	Introduction	6
1.1	Tools Used In This Document	6
1.2	Terminology	6
1.3	Pre-Requisites.....	7
2	OEM Key Manifest (OEM KM)	8
2.1	Introduction	8
2.2	OEM Key Manifest Creation	9
2.3	Opting out of the OEM KM.....	9
2.4	Creation of OEM Key Manifest	10
2.5	Versioning	12
3	Manifesting and Signing OEM Components.....	15
3.1	High level signing of OEM components.....	15
3.2	Signing commands	15
4	Creating PKI Key Pairs	17
4.1	Introduction	17
4.2	Generating Key Pair for Signing	17
4.3	Creating the Public Key Hash:	17
4.3.1	Creating a Public Key Hash Using Intel® MEU.....	17
4.3.2	Creating Public Key Hash Manually.....	18
4.4	Key Security	19
5	Intel® Manifest Extension Utility (Intel® MEU)	20
5.1	Usage	20
5.2	Examples	21
5.2.1	Generate Configuration XML Template	21
5.2.2	Generate Code partition XML.....	22
5.2.3	Generate Compressed and Signed Partition	22
6	Using Intel® MEU to Manifest & Sign	24
6.1	Introduction	24
6.2	Binary Manifesting Signing Overview	24
6.3	Intel® MEU Configuration	25
6.4	Intel® MEU Binlist.....	25
6.4.1	Bin-list usage.....	26
6.5	Intel® MEU Decomposition	26
6.6	Intel® MEU Re-sign	27
6.7	Different Binary Types Supported By Intel® MEU.....	27
6.7.1	ISH FW	28
6.7.2	IUnit / aDSP	29
6.7.3	Secure Tokens (OEM Unlock Tokens).....	30
7	Add Components to Intel® FIT	33
7.1	Introduction	33
7.2	Include each production signed binary	33
7.3	Add the OEM Key Manifest	33
7.4	Add the Public Key Hash for OEM Key Manifest	34
7.5	Change the Key Manifest ID	34



	7.6	FIT Manifest Version Validation.....	36
	§	36	
8		Production Signing	37
	8.1	Introduction	37
	8.2	Production signing high-level.....	37
	8.3	Export Manifests	38
	8.4	Manifest structures	39
		8.4.1 Manifest Header	40
		8.4.2 Signed Package Info Extension	41
		8.4.3 Metadata extensions	42
		8.4.4 OEM Key Manifest.....	43
	8.5	Import Manifest	44
9		Boot Flow Authentication.....	45
	9.1	OEM KM Precedence & Key usage relationships	45
10		Common Bring Up Issues and Troubleshooting Table.....	46
	10.1	Common Bring Up Issues and Troubleshooting Table	46

Revision History

Revision Number	Description	Revision Date
0.6	Initial Release	September 2017
0.7	Update Figure-5 in section 6.3 – New figure includes the removal of the default Signing Tool path.	March, 2018
0.8	Added two subsections to chapter 7. (IP loading precedence and IP versioning) Removed table and image from table of content, since they were off.	May 2018
0.9	Updated chapter 8.5 on Intel® FIT manifest version verification	September 2018
1.0	Changes introduced since CML: Stronger signing with RSA – 3072 and SHA 356 Header layout	June 2019



1 Introduction

This document gives an overview of the process of manifesting and signing OEM components to be included in the IFWI image for Ice Lake platforms using ME13 FW.

When a platform boots, it is critical to ensure the FW loaded is from a trusted source. OEMs are encouraged to enable OEM KM usage to extend platform root of trust from the Intel ME ROM.

The goal of this guide is to train the user to:

1. Manifest and sign OEM components
2. Include data on all signatures in the IFWI image
3. Build the production IFWI image

This guide also offers some background about the IP loading flow.

1.1 Tools Used In This Document

The following tools are referenced this document:

- Intel® Flash Image Tool (Intel® FIT): Found in the Intel® ME FW Kit
- Intel® Manifest Extension Utility (Intel® MEU): Found in the Intel® ME FW Kit
- OpenSSL: Open Source

1.2 Terminology

Term	Description
Intel® FIT	Intel® Flash Image Tool
IBB	Initial Boot Block
IBBL	Initial Boot Block Loader
IFWI	Integrated Firmware Image (System FW Image on SPI)
ISH	Integrated Sensor Hub
OBB	OEM Boot Block
Intel® MEU	Intel® Manifest Extension Utility
SUT	System Under Test
CNL	Cannon Lake
ICL	Ice Lake



Term	Description
OEM KM	OEM Key Manifest
EOM	End of Manufacturing
ROT KM	Root of Trust Key Manifest (containing Intel public key hashes to authenticate Intel signed FW components).

1.3 Pre-Requisites

The user should download and install the following kit.

- Latest Intel® ME FW kit: The kit can be downloaded from the following location:

<https://platformsw.intel.com/>

- ICL Firmware Bring-Up Guide: The overall platform bring-up procedure is described in this guide which can be found in the ME FW kit.
- ICL System Tools User Guide: The System Tools User Guide gives further detail on the usage of all the firmware manufacturing tools and is the definitive guide to the details of each tool's usage.

2 **OEM Key Manifest (OEM KM)**

2.1 **Introduction**

The OEM Key Manifest is the central part of the entire signing mechanism. It lists the public key hashes of all the OEM-created binaries within the IFWI as well as other binaries and manifests that can be loaded at a later date (such as audio and camera binaries, OS Kernel and OS Boot loader, and secure tokens).

If the IFWI image will not be signed, the OEM can skip the creation of an OEM Key Manifest.

The OEM Key Manifest itself, once created, is signed with a key whose public key hash will be entered into Intel FIT. When the platform manufacture is complete, this public key hash will be burned into a fuse (FPF) that can never be changed. Thus we create a secure verification mechanism: firmware is able to verify that the OEM Key Manifest on the platform is the same one whose hash is burned into a hardware fuse, and each hash within the manifest allows firmware to verify the binary or manifest components it plans to load.

Important!

Since the hash burned into the platform hardware can never be changed, it is critical to secure the private key used to sign the OEM Key Manifest. If at any stage a new image needs to be burned onto the platform (e.g. via flash gang programmer), it must be signed with this key.

The Intel ME Authentication infrastructure is important to the OEMs platform because OEM can take advantage of Intel HW Root of Trust (ME ROM) to extend the chain of trust to the BIOS and even to the OS.

Platform Chain of trust extended from Intel HW Root of Trust (ME ROM)



The OEM KM is a key manifest containing the OEM's public key hashes for authenticating the OEM's components. The OEM KM is authenticated by the ME FW against the "OEM Public Key Hash" FPF that is provisioned during OEM/ODM manufacturing flow. Once the OEM KM binary is authenticated, the keys contained in it are subsequently used to authenticate various OEM components based on the key usages enabled. The OEM KM can be used to authenticate OEM signed components such as ISH FW, Audio FW, iUnit FW, ISI FW etc.

OEM Key Manifest (OEM KM)

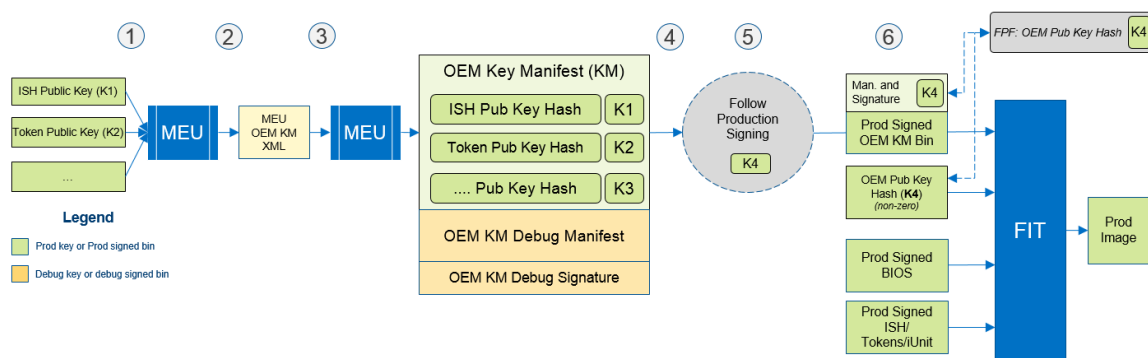
There are three main use case for the OEM KM:

1. Dedicate separate key for each OEM component team (i.e. 1 key for ISH team, another for Audio FW, another for iUnit, etc.).
2. OEM outsourcing to Multiple ODMs using the same OEM KM keys. OEMs may differentiate between the ODMs by using different KM IDs while using the same keys for OEM KM.

2.2 OEM Key Manifest High Level Overview

The diagram below demonstrates high-level flow of OEM KM creation.

Figure 2: OEM KM Creation Process



Procedure:

1. To authenticate OEM components using the OEM KM, input each of their public keys into MEU to produce public key hashes
2. Add the public key hash binaries to MEU XML
3. Input the MEU XML to MEU to generate the OEM KM binary
4. MEU outputs manifest, extensions, hash, debug signature in the OEM KM binary
5. Perform production signing on the OEM KM binary.
6. Input the production signed components into FIT (including the OEM KM signed binary) & OEM Public Key hash

(Commands are listed under Manifesting and Signing chapter)

2.3 Opting out of the OEM KM

OEMs who do not wish to utilize the OEM KM should:

1. Not create nor include OEM KM binary into FIT. FIT will set an FPF value to indicate OEM KM is not present. This is FPF that will be **permanently** set in the FPF HW at time of EOM flow, indicating that platform can never contain an OEM KM.
2. If using ISH, iUnit, or Audio FW, use Intel signed ISH, iUnit and Audio. Intel signed FW is authenticated by Intel ROT KM (Root of



Trust Key Manifest) which is part of the Intel signed ME FW. Make sure to use pre-production ISH/Audio/iUnit with pre-production ME FW & production ISH/Audio/iUnit to make sure keys match and verified per keys in the appropriate ME FW.

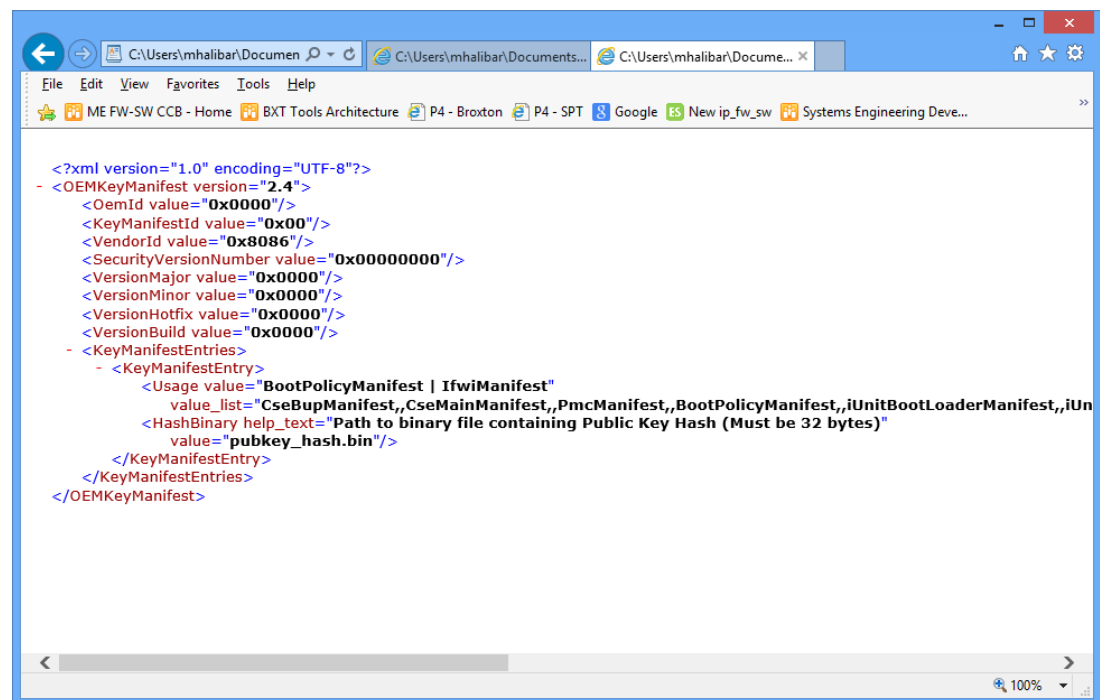
2.4 Creation of OEM Key Manifest

The manifest file xml template can be generated using the following command:

```
# meu -gen OEMKeyManifest
```

This generates an xml template with a single KeyManifestEntry node, which lists the file type, and the path to its public key hash.

Figure 1. Default OEM Key Manifest XML



The KeyManifestId field must not be left with its default value of 0x1 (must be given some non-zero value). It is critical that the matching field in FIT is also changed to match the non-zero value, as this field will be burned into an FPF and used to validate the OEM Key Manifest on platform boot.

Extra 'KeyManifestEntry' nodes should be added for each file that has a unique key hash to be entered. If several files share the same key, they can be included within the same node, as in the default xml template.

So, for example, if the OEM Key Manifest wants to have

- IshManifest, iUnitBootLoaderManifest & iUnitMainFwManifest with key 1

OEM Key Manifest (OEM KM)

It would appear as follows:

Figure 2. OEM Key Manifest with 1 key for multiple manifests

```
<?xml version="1.0" encoding="UTF-8"?>
- <OEMKeyManifest version="2.4">
  <OemId value="0x0000"/>
  <KeyManifestId value="0x1"/>
  <VendorId value="0x8086"/>
  <SecurityVersionNumber value="0x00000000"/>
  <VersionMajor value="0x0000"/>
  <VersionMinor value="0x0000"/>
  <VersionHotfix value="0x0000"/>
  <VersionBuild value="0x0000"/>
  - <KeyManifestEntries>
    - <KeyManifestEntry>
      <Usage value="IshManifest | iUnitBootLoaderManifest | iUnitMainFwManifest"
        value_list="BootPolicyManifest,,iUnitBootLoaderManifest,,iUnitMainFwManifest,,cAvsImage0M
        <HashBinary value="pubkey_hash1.bin" help_text="Path to binary file containing Public Key Hash
        (Must be 32 bytes)"/>
      </KeyManifestEntry>
    </KeyManifestEntries>
  </OEMKeyManifest>
```

If the OEM Key Manifest wants to have

- IshManifest with key 1
- iUnitBootLoaderManifest & iUnitMainFwManifest with key 2

It would appear as follows:



Figure 3. OEM Key Manifest with 2 key for multiple manifests

```
<?xml version="1.0" encoding="UTF-8"?>
- <OEMKeyManifest version="2.4">
  <OemId value="0x0000"/>
  <KeyManifestId value="0x1"/>
  <VendorId value="0x8086"/>
  <SecurityVersionNumber value="0x00000000"/>
  <VersionMajor value="0x0000"/>
  <VersionMinor value="0x0000"/>
  <VersionHotfix value="0x0000"/>
  <VersionBuild value="0x0000"/>
  - <KeyManifestEntries>
    - <KeyManifestEntry>
      <Usage value="IshManifest"
        value_list="BootPolicyManifest,,iUnitBootLoaderManifest,,iUnitMainFwManifest,,cAvsImage0Manifest"
        <HashBinary value="pubkey_hash1.bin" help_text="Path to binary file containing Public Key Hash
          (Must be 32 bytes)"/>
      </KeyManifestEntry>
    - <KeyManifestEntry>
      <Usage value="iUnitBootLoaderManifest | iUnitMainFwManifest"
        value_list="BootPolicyManifest,,iUnitBootLoaderManifest,,iUnitMainFwManifest,,cAvsImage0Manifest"
        <HashBinary value="pubkey_hash2.bin" help_text="Path to binary file containing Public Key Hash
          (Must be 32 bytes)"/>
      </KeyManifestEntry>
    </KeyManifestEntries>
  </OEMKeyManifest>
```

Once the OEM Key Manifest xml has been edited to include all the required hashes, the MEU can be run with the xml as input to manifest and sign the with the private key created for this purpose (private key to be used here will require to have its public key hash set in the "OEM Pub Key Hash" FPF in FIT. This hash will be **permanently** committed to the FPF HW at EOM/Closemfnf):

```
# meu.exe -f <OEMKeyManifest.xml> -o < OEMKeyManifest.bin> -
key <privatekey.pem>
```

It is only necessary to override the private key for signing (as in the example) if the key is different than that defined in the default Intel MEU configuration xml.

2.5 Versioning

The OEM KM XML contains fields for setting the version of the IP component to be signed. This chapter holds true for other XMLs described in this document as well.

Figure 13. OEM Key Manifest Version Fields

```

<?xml version="1.0" encoding="UTF-8"?>
- <OEMKeyManifest version="2.4">
  <OemId value="0x0000"/>
  <KeyManifestId value="0x1"/>
  <VendorId value="0x8086"/>
  <SecurityVersionNumber value="0x00000000"/>
  <VersionMajor value="0x0000"/>
  <VersionMinor value="0x0000"/>
  <VersionHotfix value="0x0000"/>
  <VersionBuild value="0x0000"/>
  <KeyManifestEntries>
    - <KeyManifestEntry>
      <Usage value="IshManifest | iUnitBootLoaderManifest | iUnitMainFwManifest"
        value_list="BootPolicyManifest,,iUnitBootLoaderManifest,,iUnitMainFwManifest,,cAvsImage0M
      <HashBinary value="pubkey_hash1.bin" help_text="Path to binary file containing Public Key Hash
        (Must be 32 bytes)"/>
      </KeyManifestEntry>
    </KeyManifestEntries>
  </OEMKeyManifest>

```

OEMs are required to define these versions so the component can be identified by its version. Versions are updated based on the changes made, with the following rule of thumb in mind:

Major	A major change in the component or design
Minor	A minor change to the component
Hotfix	If the new component is basically the same as before, but includes a hotfix
Build	Incremented any time the component is rebuilt again for whatever reason

Here is the breakdown of the versioning as an examples taken from CSME:

VersionMajor: 11 (when CSME version **11**.8.50.3399)

VersionMinor: 8 (when CSME version 11.**8**.50.3399)

VersionHotfix: 50 (when CSME version 11.8.**50**.3399)

VersionBuild: 3399 (when CSME version 11.8.50.**3399**)

The security version number (SVN) starts at 1 for production IPs. It is used as a security measure to block the loading of versions with security vulnerabilities. On a platform which contains an IP with SVN = x, upgrade is allowed to versions with SVN=x or SVN= x+1.

Therefore:

- To allow downgrade to the previous IP versions, keep SVN the same value as the previous version.
- To block downgrade to the previous IP versions, increase the SVN.



OEM Key Manifest (OEM KM)

For example, in machine that has a component with version 1.1.0.2 and SVN 2, the following applies:

Version	SVN Value	Can it be updated?
1.0.0.1	1	No, the SVN value is lower
1.1.0.1	2	Yes, same SVN value
1.2.0.0	3	Yes, higher SVN value

§



3 Manifesting and Signing OEM Components

3.1 High level signing of OEM components

1. Generate PKI key pairs and the public key hash for:
 - a. Each entry in the OEM Key Manifest. These are enumerated in Section 2.4.
 - b. The OEM Key Manifest
2. Use the Intel® MEU tool to add to each binary a manifest, signature, and where relevant also add metadata, stitch and/or compress the binary.
3. Create an OEM Key Manifest¹, including within it the public key hash of each of the created keys, and use the Intel MEU to manifest/sign it. Note: The order in which steps 2 and 3 are executed does not matter.
 - a. Signing the "OEM KM" binary may be done by performing the normal OEM proprietary production signing flow. Refer to the production signing section for more details.
4. Add each binary component to the Intel FIT.
5. Add to Intel FIT the OEM Key Manifest created in step 3.
6. Add to Intel FIT the public key hash for the key used to sign the OEM KM. At EOM (End of Manufacturing)/closemfn process, this value of the OEM Public Key hash will be committed/burned into the HW FPFs permanently.
7. For debug use-cases, you may add an OEM debug token to Intel FIT.

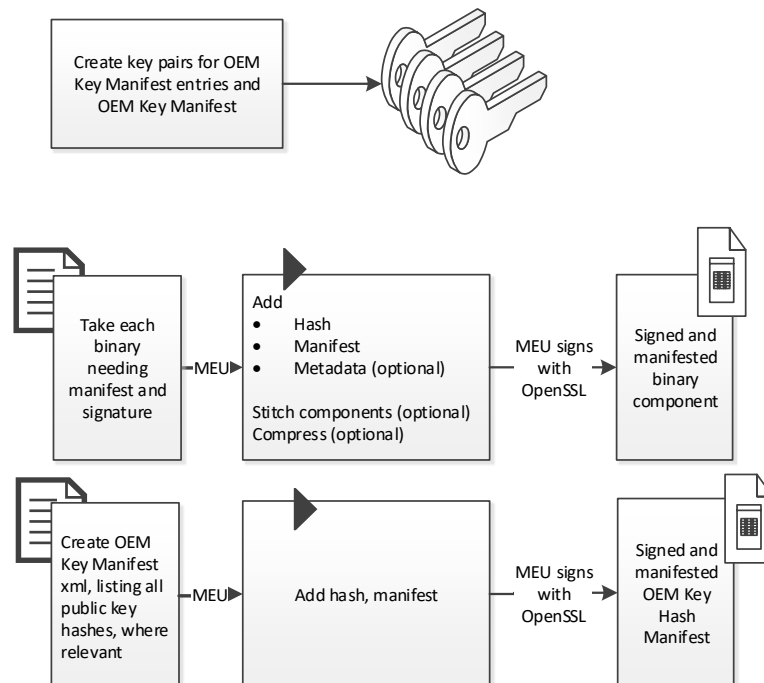
3.2 Signing commands

3. Generate a local private/public key pair
 - a. Generate privateKey.pem: `Openssl.exe genrsa -out <privateKey.pem> 3072`
 - b. Generate publicKey.pem: `Openssl.exe rsa -in <privateKey.pem> -pubout -out <publicKey.pem>`
Note: Generate a key pair for each component to be signed, as well as for OEMKeyManifest. Or sign all with the same key pair.
4. Generate meu_config.xml: `meu.exe -gen meu_config`
 - a. Update path to openssl.exe
 - b. Update path to privateKey.pem
 - c. Update path to LZMA (If signing ISH)

¹ OEM KM is optional. OEMs who do not wish to use OEM KM may keep OEM Public Key hash as zeros in FIT tool.
If flashing an image without OEM KM at the time of EOM, the platform will never be able to contain an OEM KM.

- (LZMA tool can be downloaded from [here](#))
5. Generate PubKeyHash.bin: `meu.exe -keyhash <pubKeyHash> -key <publicKey.pem>`
 6. Generate Codepartition.xml: `meu.exe -gen codepartition`
(Need a separate code partition file for each IUP)
 - a. Update the value field under (1)Name, (2)Usage (taken from value_list), (3)Version and (4)InputFile (raw bin)
 7. Generate OEMKeyManifest.xml: `meu.exe -gen OEMKeyManifest`
 - a. Update value field under ⁽¹⁾KeyManifestId, ⁽²⁾SecurityVersionNumber, ⁽³⁾Usage, ⁽⁴⁾HashBinary
 8. Generate CodePartition_signed.bin:
`meu.exe -f CodePartition.xml -o <CodePartition_signed.bin> -key <privateKey.pem>`
(Signs the Codepartition.xml)
 9. Generate OEMKeyManifest_signed.bin:
`meu.exe -f OEMKeyManifest.xml -o <OEMKeyManifest_signed.bin> -key <privateKey.pem>`
(Signs the OEMKeyManifest.xml)

Figure 4. High Level Overview of Manifesting and Signing OEM Components in the IFWI Image





4 Creating PKI Key Pairs

4.1 Introduction

If creating a signed IFWI image, you will need to create PKI key pairs, as well as the public key hash for:

10. Each entry in the OEM Key Manifest. See Creation of OEM Key Manifest for full list of entries in the OEM KM.
11. The OEM Key Manifest

4.2 Generating Key Pair for Signing

The Intel tools are designed to work together with the open source OpenSSL tool (version 1.0.2b), which generates key pairs in the RSA-3072 PKCS-1.5 format. **This is the only key format which is supported for the Intel IFWI image signing flow!** Although other tools which generate key pairs in this format can be used for signing, Intel tools currently do not interface with any other tool, and if you choose to use a different tool, Intel cannot provide support.

The OpenSSL tool is not provided by Intel, it must be installed separately. One source for the OpenSSL binaries is [Shining Light Productions](#), the "Light" version is sufficient. Ensure that OpenSSL.exe can be run in the directory in which it is installed, and it is able to create output files there as well, otherwise you may see errors when executing some of the commands.

You can generate a private key by running the following command from the CLI:

```
# openssl.exe genrsa -out privkey.pem 3072
```

A public key can be extracted from the private key using:

```
# openssl.exe rsa -in privkey.pem -pubout -out pubkey.pem
```

4.3 Creating the Public Key Hash:

A public key hash is a binary file containing the modulus and exponent of the public key in little endian format. You can create it using the Intel® MEU, or manually.

4.3.1 Creating a Public Key Hash Using Intel® MEU

You can create the public key hash using the Intel® MEU in one of 3 different ways:

12. Extraction from an already signed binary:

```
# meu.exe -keyhash <output hashfile> -f <input.bin>
```



13. Extraction from a public or private key in PEM format

```
# meu.exe -keyhash <output hashfile> -key <inputkey.pem>
```

14. Creation when building or signing a binary

```
# meu.exe -keyhash <output hashfile> -f <input.xml> -o  
<output.bin>
```

The public key hash is a readable string, and can be copied and pasted from the text file as needed.

Here is an example of generating the public key hash from a signed binary:

```
# meu.exe -keyhash temp/hash -f iunp.bin  
=====
```

Intel(R) Manifest Extension Utility. Version: 12.0.0.xxxx
Copyright (c) 2013 - 2017, Intel Corporation. All rights reserved.
7/12/2017 - 10:16:35 am
=====

Command Line: meu -keyhash temp/hash -f iunp.bin
Log file written to meu.log
Loading XML file: C:/Users/meu_config.xml
Public Key Hash Value:
14 05 A8 A4 EB 1C 8A C2 51 19 7D 85 96 14 09 FF 15 FD CD
23 D3 25 CC DD 88 D2 17 5C DE 3B 27 36

Public Key Hash Saved to:
temp\hash.bin
temp\hash.txt
Program terminated.

4.3.2 Creating Public Key Hash Manually

You can create a public key hash manually in one of two different ways:

15. Extraction from the public or private key:

- a. Using OpenSSL, dump the key details:
If using the public key:

```
openssl.exe rsa -in public.pem -text -noout -pubin
```

If using the private key:

```
openssl.exe rsa -in private.pem -text -noout
```

- b. Copy the modulus (excluding any leading bytes that are all 0s)
- c. Reverse the modulus byte order (Use excel to paste all the bytes on different rows into a column, then put ascending numbers in another column and do a reverse sort on the numbers)

- d. Paste the reverse byte modulus into a new file <new file> in a hex editor
- e. Copy the exponent following the modulus into the new file (make sure it is little endian)

Hash the new file using

```
openssl.exe dgst -sha256 <new file>
```

16. Extraction from a manifest signed with the keys, by MEU

- a. Open a signed file that MEU has created in a hex editor
- b. Search for the string "\$MN2", then move 100 bytes after the start of "\$MN2" (this will be the start of the modulus + exponent)
- c. Extract the following 260 bytes to a new file <new file>
- d. Hash the new file using openssl:

```
openssl.exe dgst -sha256 <new file>
```

The public key hash is a readable string, and can be copied and pasted from the text file as needed.

4.4 Key Security

Although the same key may be used for signing each entry in the OEM Key Manifest, and indeed for signing the manifest itself, Intel recommends using separate key pairs for signing each component. Using the same key for signing multiple components is less secure, as if the key is compromised, the entire package is compromised.

Private keys should always be stored securely and kept secret to provide a robust secure boot flow and firmware load. If the keys escape to 3rd parties, they may be used to create and sign unofficial versions of the binaries which can then be loaded onto the platform.

Keys may be needed again if there is a need to re-sign a future version of a binary.

OEMs need to take special steps to ensure that the private keys are kept secure while allowing restricted/audited access to them for manifesting/signing components and building the image. For example, MEU could be run on a secure server which houses the keys or OEMs may use the MEU export function for production signing if MEU does not run on the OEM's signing server (see production signing chapter).

OEMs should use a separate set of keys during the development process and creating production images. This will ensure that on production platforms only the production OEM Key Manifest with signatures for production components can be run.

§



5 Intel® Manifest Extension Utility (Intel® MEU)

The Intel® Manifest Extension Utility (MEU) inputs a firmware binary created by a 3rd party and outputs an independent-updateable partition (IUP) that is compressed and signed. After completing this process the signed binary can be added to the SPI flash image using the Intel® FIT tool.

The Intel® Manifest Extension Utility (MEU) requires administrator privileges to run under Windows* OS. The user needs to use the Run as Administrator option to open the CLI in Windows* 7 64/32 bit and Windows* 8.1 64/32 bit.

The Intel® MEU tool completes the following steps:

- Creates an Independent Updatable Partition (IUP) by adding manifest and meta-data information to the firmware.
- Calls an external LZMA tool for compression of the firmware binary
- Calls the signing infrastructure tool to sign the partition.

5.1 Usage

The executable can be invoked by:

```
MEU.exe [-exp] [-h|?] [-3rdparty] [-version|ver] [-binlist]
[-o] [-f]

[-gen] [-cfg] [-decomp] [-save] [-w] [-s] [-d] [-u1] [-u2]
[-u3]

[-mnver] [-mndebug] [-st] [-stp] [-key] [-noverify] [-
keyhash] [-resign]

[-export] [-import] [-printman]
```

Table 5-1. Options

Option	Description
-H or -?:	Displays the list of command line options supported by the Intel® MEU tool.
-3rdparty	Displays 3rd party software credits.
-EXP	Shows examples about how to use the tools.
-VER	Shows the version of the tools.
-binlist	Displays a list of supported binary types.
-o <filename>	Overrides the output file path.
-f <filename>	Specifies input XML file.



Option	Description
-gen <type>	Specifies the binary type for which to generate a template XML file.
-cfg <filename>	Overrides the path to the tool config XML file.
-decomp <type>	Specifies the binary type to use for decomposition.
-save <filename>	Specifies the output XML path.
-w <path>	Overrides the \$WorkingDir environment variable.
-s <path>	Overrides the \$SourceDir environment variable.
-d <path>	Overrides the \$DestDir environment variable.
-u1 <path>	Overrides the \$UserVar1 environment variable.
-u2 <path>	Overrides the \$UserVar2 environment variable.
-u3 <path>	Overrides the \$UserVar3 environment variable.
-mnver <value>	Overrides the version of the output binary. (Format: Major.Minor.Hotfix.Build)
-mndebug <true false>	Overrides the debug flag in the output binary's manifest(s).
-key <path>	Overrides the signing key in the tool config XML file.
-st <tool>	Overrides SigningTool in the tool config XML file.
-stp <path>	Overrides SigningToolPath in the tool config XML file.
-noverify	Skips verification of generated manifest signature.
-keyhash <path>	Exports the public key hash to a directory.
-resign <indices 'all'>	Resigns manifest(s) in a binary.
-export <indices 'all'>	Exports manifest(s) from a binary.
-import <path>	Imports manifest(s) into a binary.
-printman <indices 'all'>	Prints manifest(s) information from a binary

5.2 Examples

5.2.1 Generate Configuration XML Template

This command will generate the configuration XML template file using MEU.

Windows / WinPE:

```
MEU.exe -gen meu_config
```



```
=====
=====
Intel(R) Manifest Extension Utility. Version: 12.0.0.xxxx
Copyright (c) 2013 - 2017, Intel Corporation. All rights
reserved.
7/12/2017 - 10:16:35 am
=====
=====
Command Line: meu.exe -gen meu_config

Log file written to meu.log

Saving XML ...

XML file written to meu_config.xml
```

5.2.2 Generate Code partition XML

This command will generate the Code partition XML file using MEU.

Windows / WinPE:

```
MEU.exe -gen CodePartition
```

```
=====
=====
Intel(R) Manifest Extension Utility. Version: 12.0.0.xxxx
Copyright (c) 2013 - 2017, Intel Corporation. All rights
reserved.
7/12/2017 - 10:16:35 am
=====
=====

Command Line: meu.exe -gen CodePartition

Saving XML ...

XML file written to CodePartition.xml
```

5.2.3 Generate Compressed and Signed Partition

This command will create the compressed and signed partition using MEU.

Windows / WinPE:

```
MEU.exe -f CodePartition.xml -o ISHC_MEU.bin
```

```
=====
=====
Intel(R) Manifest Extension Utility. Version: 12.0.0.xxxx
Copyright (c) 2013 - 2017, Intel Corporation. All rights
reserved.
7/12/2017 - 10:16:35 am
=====
=====

Command Line: meu.exe -f CodePartition.xml -o ISHC_MEU.bin

Executing pre-build actions
```



Intel® Manifest Extension Utility (Intel® MEU)

Building objects

Processing attribute: CodePartition

Executing post-build actions

Full Flash image written to C:\...\ISHC_MEU.bin



6 Using Intel® MEU to Manifest & Sign

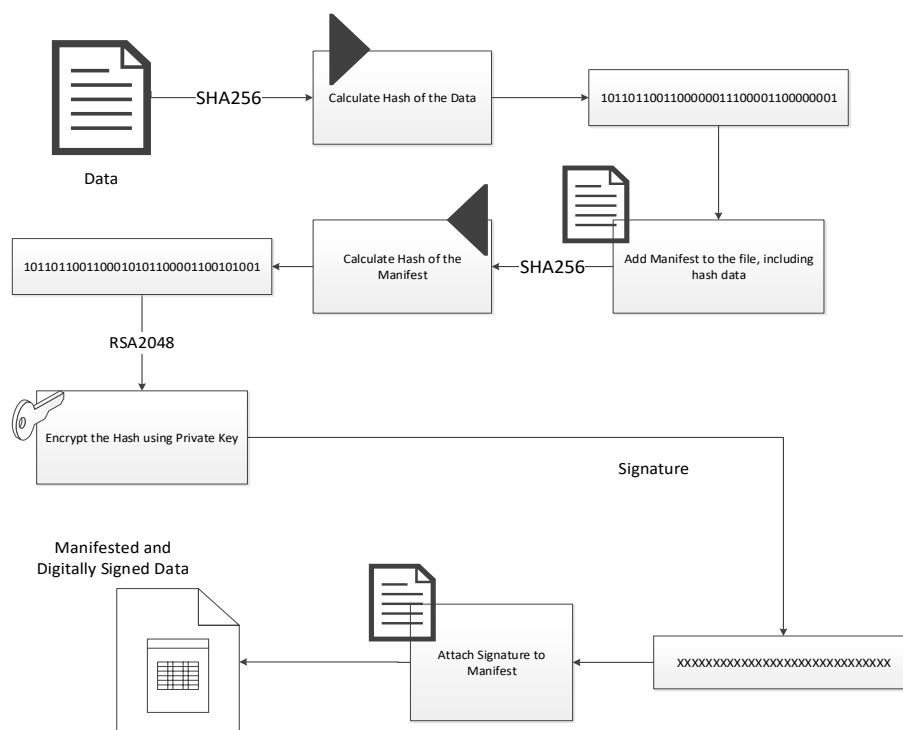
6.1 Introduction

All of the components to be authenticated by keys in the OEM Key Manifest owned by an OEM are expected to have a signed manifest added to them.

6.2 Binary Manifesting Signing Overview

Intel signing for ICL platforms employs an RSA 2048 public key infrastructure (PKI) mechanism to sign and verify components of the IFWI image. The private key is used to sign the image components as shown in Figure 2 below. The Intel MEU is used to create the manifests and interfaces with OpenSSL to add signatures to the manifest.

Figure 5. Schematic View of Manifesting and Signing Process



6.3 Intel® MEU Configuration

To get started using Intel MEU you must first configure the tool. To do this, run the following command:

```
# meu -gen meu_config
```

This will generate a default configuration xml file:

Figure 6. Intel MEU Configuration xml

```
<?xml version="1.0" encoding="UTF-8"?>
- <MeuConfig version="2.4">
- <PathVars label="Path Variables">
  <WorkingDir label="$WorkingDir" help_text="Path for environment variable $WorkingDir" value="." />
  <SourceDir label="$SourceDir" help_text="Path for environment variable $SourceDir" value="." />
  <DestDir label="$DestDir" help_text="Path for environment variable $DestDir" value="." />
  <UserVar1 label="$UserVar1" help_text="Path for environment variable $UserVar1" value="." />
  <UserVar2 label="$UserVar2" help_text="Path for environment variable $UserVar2" value="." />
  <UserVar3 label="$UserVar3" help_text="Path for environment variable $UserVar3" value="." />
</PathVars>
- <SigningConfig label="Signing Configuration">
  <SigningTool label="Signing Tool" help_text="Select tool to be used for signing, or disable signing." value="OpenSSL"
    value_list="Disabled,OpenSSL,MobileSigningUtil"/>
  <SigningToolPath label="Signing Tool Path" help_text="Provide the path to your signing tool executable, such as /usr/bin/openssl or C:\OpenSSL-
    Win32\bin\openssl.exe" value="" />
  <PrivateKeyPath label="Private Key Path" help_text="Path to private RSA key (in PEM format) to be used for signing. Key is required if using
    OpenSSL. If using MSU, and value is not-empty, this will override the key in the Signing Tool Config XML."
    value="$WorkingDir\private.pem" />
  <SigningToolXmlPath label="Signing Tool Config XML Path" help_text="Configuration XML template for MobileSigningUtil. Leave blank if not using
    MSU." value="" />
  <SigningToolExecPath label="Signing Tool Execution Path" help_text="Specify a directory from which the signing tool should be executed. This can
    be useful if relative paths are used in the Signing Tool Config XML. If no path is provided, the signing tool will be executed from the same
    directory as this tool was executed. Leave blank if not using MSU." value="" />
</SigningConfig>
- <CompressionConfig label="Compression Configuration">
  <LzmaToolPath label="LZMA Tool Path" help_text="Path to lzma tool executable." value="" />
</CompressionConfig>
</MeuConfig>
```

If you will not be signing the manifests, then change the 'SigningTool' node to 'Disabled'.

```
<SigningTool label="Disabled"
value_list="Disabled,,OpenSSL,, MobileSigningUtil"
label="Signing Tool" help_text="Select tool to be used for
signing, or disable signing." />
```

If you will be signing the manifests, the xml should be edited to ensure the 'SigningToolPath' node correctly points to the OpenSSL executable file and that the path to the private key used for signing is correct. You are free to edit the other fields if appropriate.

6.4 Intel® MEU Binlist

Intel MEU supports manifesting and signing a large number of different file types. To see the full list, run the following:

```
# meu.exe -binlist
```



Figure 7. Intel MEU list of Supported Binary Types

```
Intel(R) Manifest Extension Utility. Version: 12.0.0.1006
Copyright (c) 2013 - 2017, Intel Corporation. All rights reserved.
7/12/2017 - 10:54:40 am
=====

Command Line: meu.exe -binlist

The following binary types can be generated by this tool. A template XML file
can be generated for a given type using the -gen switch.

Type          : Description
-----
meu_config    - Template tool config file (meu_config.xml)
CodePartition - Generic Updateable Code Partition
CodePartitionMeta - Updateable Code Partition with user-provided Metadata
OEMKeyManifest - OEM Key Manifest
OemUnlockToken - OEM Unlock Token

Program terminated.
=====
```

6.4.1 Bin-list usage

Each of the items in the above binlist is supported by MEU for manifesting & signing. For each file that needs to be manifested and signed you use the Intel MEU to generate an xml for that file type and then edit the xml to ensure the data is correct – in particular:

- i. Update xml with targeted FW usage
- ii. Update xml with targeted FW path

You then call the MEU with the edited xml as input, and pass in the name of the required output file, it will create the manifested and signed output file:

```
# meu.exe -f <input.xml> -o <output.bin>
```

It is recommended practice to sign each file with a different private key. An easy way to do this is to use the configuration xml without changing it and override the private key used for signing on the command line (otherwise the private key in the MEU config would be used to sign all the components):

```
# meu.exe -f <input.xml> -o <output.bin> -key
<privatekey.pem>
```

6.5 Intel® MEU Decomposition

Intel MEU is able to decompose a manifested and signed binary returning it to the original state it was in before the Intel MEU added a manifest and/or signature while providing an xml detailing the decomposition. This xml can later be used as input to the Intel® MEU to recreate the full binary with manifest and signature. The `-decomp` command also requires the binary type as its first parameter. So, for example, to decompose an OEM Key Manifest binary, you can call:



```
# meu -decomp OEMKeyManifest -f <input.bin> -save
<decomp.xml>
```

6.6 Intel® MEU Re-sign

Intel® MEU is able to re-sign a binary that has already been signed. This is very useful when changing the signing keys – the relevant binary files just need to be re-signed.

```
# meu.exe -resign -f <input.bin> -o <output.bin> -key
<privatekey.pem>
```

It is only necessary to override the private key for signing (as in the example) if the key is different than that defined in the default Intel® MEU configuration xml.

Some binaries – such as full IFWI images, include multiple manifests. When calling the `-resign` option on such binaries, you need to include the index of the manifest to be re-signed, or 'all' if all are to be re-signed (using the new key). If the index, or 'all' is not included, the Intel® MEU will show a full list of the manifests included in the binary:

More than one manifest was found in this file. Please provide a comma-separated list of the manifest indices you want to resign. (ex. `-resign "0,3,5"`) or specify "all" (ex. `-resign "all"`)

The following manifests were detected:

Index	Offset	Size	Name (if available)
0	0x000084058	0x000000378	RBEP.man
1	0x000094058	0x000000378	PMCP.man
2	0x0000A4580	0x000001750	FTPR.man
3	0x0000A9000	0x000000330	rot.key
4	0x0001F4000	0x000000330	oem.key
5	0x0001FB058	0x000000378	ISHC.man
6	0x00023B070	0x000000378	IUNP.man
7	0x00023D0E8	0x0000004B0	WCOD.man
8	0x0002BD0B8	0x000000448	LOCL.man
9	0x000342448	0x000000C00	NFTP.man

Error 24: Failed to resign manifest(s). Missing manifest indices list.

The Intel® MEU can then be called again including the index desired. Following the above example if the OEM KM is to be re-signed, call:

```
# meu.exe -resign 4 -f <input.bin> -o <output.bin> -key
<privatekey.pem>
```

6.7 Different Binary Types Supported By Intel® MEU

Intel MEU is able to add manifests and sign several types of files, as enumerated below.



Note: All binaries provided by Intel will have a manifest and signature. OEMs do not need any further processing on these binaries.

6.7.1 ISH FW

The ISH FW binary is regarded as a 'code partition' by the Intel® MEU. Intel signed ISH FW is authenticated by the Intel® ME FW, but if the OEM wishes to have their own custom ISH FW instead of the Intel signed version, the OEM may do so by customizing the FW then signing with their private key and including the public key hash in the OEM KM. To sign such FW, the OEM needs to generate the code partition xml template using the following command:

```
# meu -gen CodePartition
```

The xml generated will need to be edited to enter version information about the code partition, as well as the path to the binary. If compression is required the path to the LZMA compression file also needs to be entered. Note that the Intel MEU tool only supports the LZMA tool provided by Intel to compress binaries. The ISH binary requires compression.

Figure 8. Code Partition xml

```
<?xml version="1.0" encoding="UTF-8"?>
- <CodePartition version="2.4">
  <Name help_text="Name to use in the output binary's directory. Maximum length is 4 characters." value="ISHC"/>
  <Length help_text="Length of output binary, extra space will be filled with 0xFF's. If length is smaller than required, an error will be reported. If set to 0, the length will be computed as needed by the tool." value="0x0"/>
  <Usage help_text="Indicates the type of data contained in this binary. This value is used during signature verification to validate the public key." value="IshManifest" value_list="CseBupManifest,,CseMainManifest,,PmcManifest,,UsbTypeCIOMManifest,,UsbTypeCMGManifest,,UsbTypeCTBTManifest,,IshManifest"/>
  <VendorId value="0x0000"/>
  <InstanceId value="0x1"/>
  <PartitionFlags value="0x00000000"/>
  <PartitionVersion value="0x10000000"/>
  <VersionControlNumber value="0x00000000"/>
  <SecurityVersionNumber value="0x00000000"/>
  <VersionMajor help_text="Used to manually set the Major Version field in the manifest" value="0x0" label="Version Major"/>
  <VersionMinor help_text="Used to manually set the Minor Version field in the manifest" value="0x0" label="Version Minor"/>
  <VersionHotfix help_text="Used to manually set the Hotfix Version field in the manifest" value="0x0" label="Version Hotfix"/>
  <VersionBuild help_text="Used to manually set the Build Version field in the manifest" value="0x0" label="Version Build"/>
  <VersionExtraction>
    <Enabled help_text="If enabled, the version details will be extracted from the InputFile binary at the offsets specified. If disabled, the version must be specified manually." value="false" value_list="true,,false"/>
    <InputFile help_text="Binary file from which to extract the version details." value=""/>
    <VersionMajorByte0Offset help_text="Offset of Major Version number's LSB in InputFile." value="0"/>
    <VersionMajorByte1Offset help_text="Offset of Major Version number's MSB in InputFile." value="0"/>
    <VersionMinorByte0Offset help_text="Offset of Minor Version number's LSB in InputFile." value="0"/>
    <VersionMinorByte1Offset help_text="Offset of Minor Version number's MSB in InputFile." value="0"/>
    <VersionHotfixByte0Offset help_text="Offset of Hotfix Version number's LSB in InputFile." value="0"/>
    <VersionHotfixByte1Offset help_text="Offset of Hotfix Version number's MSB in InputFile." value="0"/>
    <VersionBuildByte0Offset help_text="Offset of Build Version number's LSB in InputFile." value="0"/>
    <VersionBuildByte1Offset help_text="Offset of Build Version number's MSB in InputFile." value="0"/>
  </VersionExtraction>
  <CPModules>
    <CPDataModule name="ish_main">
      <InputFile help_text="Path to binary file to load for this module's data." value="ish_main.bin"/>
      <CompressionType help_text="Select compression type for this module." value="LZMA" value_list="NOT_COMPRESSED,,LZMA"/>
      <ProcessId value="0xf6"/>
    </CPDataModule>
  </CPModules>
</CodePartition>
```

Once the Code Partition xml has been edited to include all the required input files, the MEU can be run with the xml as input to manifest and sign the Code Partition with the private key created for this purpose.



```
# meu.exe -f <CodePartition.xml> -o <ISH.bin> -  
key<privatekey.pem>
```

It is only necessary to override the private key for signing (as in the example) if the key is different than that defined in the default Intel MEU configuration xml.

6.7.2 IUnit / aDSP

The IUnit and aDSP (Audio) FW binaries are regarded as 'code partition metadata' by the Intel MEU. Intel signed iUnit & aDSP (Audio) FW is authenticated by the Intel ME FW, but if the OEM wishes to substitute their own custom iUnit/aDSP FW the OEM may do so by customizing the FW, signing it with their private key and including the public key hash in the OEM KM. To sign such FW, the OEM needs to generate xml for it using the following command:

```
# meu -gen CodePartitionMeta
```

The xml generated will need to be edited to enter the path to the binary and the path to a metadata binary file.

Figure 9. Code Partition Metadata xml



Once the Code Partition Metadata xml has been edited to include all the required input files the MEU can be run with the xml as input to manifest and sign it with the private key created for this purpose.

It is only necessary to override the private key for signing (as in the example) if the key is different than that defined in the default Intel MEU configuration xml.

The OEMUnlockToken binary is authenticated by the Intel ME FW. OEMs who wish to use this feature need to create token, sign it with OEM private key and include the public key hash in the OEM KM for OemUnlockToken. To create such token, the OEM needs to generate xml for it using the following command:

The xml generated will need to be edited to enter the path to the part ID binary

Figure 10. OEMUnlockToken xml

```
<?xml version="1.0" encoding="UTF-8"?>
- <OemUnlockToken version="2.4">
  <ExpirationSeconds help_text="Time from Part ID generation to Token expiration (in seconds)."
    value="0x00278D00"/>
  <PartIdsPath help_text="Path to directory containing Part ID binaries." value=""/>
  - <TokenFlags>
    <PartRestricted value="Yes" value_list="Yes,,No"/>
    <AntiReplayProtected value="Yes" value_list="Yes,,No"/>
    <TimeLimited value="Yes" value_list="Yes,,No"/>
  </TokenFlags>
  - <TokenKnobs>
    <OemUnlockKnob value="OemUnlockEnabled"
      value_list="OemUnlockDisabled,,OemUnlockEnabled"/>
    <IshGdbDebugKnob value="IshGdbSupportEnabled"
      value_list="IshGdbSupportDisabled,,IshGdbSupportEnabled"/>
    <AllowVisaOverrideKnob value="VisaOverrideDisabled"
      value_list="VisaOverrideDisabled,,VisaOverrideEnabled"/>
    <DisableBiosSecureBootKnob value="SecureBootEnforced"
      value_list="SecureBootEnforced,,AllowRnDKeys,,SecureBootDisabled"/>
    <DisableAudioFwAuthenticationKnob value="AuthenticationEnforced"
      value_list="AuthenticationEnforced,,AllowRnDKeys,,AuthenticationDisabled"/>
    <DisableIshFwAuthenticationKnob value="AuthenticationEnforced"
      value_list="AuthenticationEnforced,,AllowRnDKeys,,AuthenticationDisabled"/>
    <DisableIunitFwAuthenticationKnob value="AuthenticationEnforced"
      value_list="AuthenticationEnforced,,AllowRnDKeys,,AuthenticationDisabled"/>
  </TokenKnobs>
</OemUnlockToken>
```

There are multiple flags that can now be set for the token as following:

In the **TokenFlags** tag, you can set following values to yes

- **PartRestricted:** This means that the token can be used on any platform whose token key hash matches that of the token, and tied to a particular platform ID when value is set to yes.
- **Anti-Replay Protected.** Anti-Replay protection stops a token being re-used on the same device after new token is created for device. This option is only relevant for tokens tied to a particular platform ID.
- **TimeLimited.** This means that the token has time limit. Anti-Replay Protected must be set for token with time expiration, because otherwise you can re-use the token after RTC clear.

It is recommended to use to secure token with time expiration and Anti-reply flag.

In the root node you can set:

- **Expiration timeout** (if relevant)
- **Part ID path.** You can retrieve the Part ID data using Intel® FPT, by calling
FPT.exe -GETPID <file>

This will retrieve the part ID into a file. Provide the path to the directory that contains PID.bin or multiple PID binaries.

Note: Executing this command will invalidate all secure tokens with Anti-replay protection set generated earlier for the given platform



Using Intel® MEU to Manifest & Sign

In the TokenKnobs section, you can set the 'Knobs' for the token. These define what the token allows/disables on the platform. The knobs available vary depending on the token being created. Here is an explanation of the various knobs:

Knob	Meaning
OEM Unlock	Allow an OEM (Orange) unlock. For CNP it will enable debug interfaces to ISH and Audio
ISH GDB Debug	Enable ISH GDB support

Note: VISA override, DisableSecureBootknob, DisableIshFwAuthenticationKnob, DisableIunitFwAuthenticationKnob, DisableAudioFwAuthenticationKnob are not supported with OEM Secure Token and should be set to disabled

Once the OEMUnlockToken xml has been edited to include all the required input files the MEU can be run with the xml as input to manifest and sign it with the private key created for this purpose.

```
# meu.exe -f <OEMUnlockToken.xml> -o <OEMtoken.bin> -key  
<privatekey.pem>
```

It is only necessary to override the private key for signing (as in the example) if the key is different than that defined in the default Intel MEU configuration xml.

§



7 Add Components to Intel® FIT

7.1 Introduction

Intel FIT is a tool provided to OEMs to stitch together multiple binary files, configuration data and other input into a full SPI image. This document will only discuss the usage of the tool as relevant to the signing mechanism. The full image creation procedure & FIT functionalities are detailed in the Ice Lake - Intel® ME Firmware Bring-Up Guide & System Tools User Guide.

7.2 Include each production signed binary

FIT includes input fields allowing the input of binary files. Most are available in the Flash Layout tab.

7.3 Add the OEM Key Manifest

Add the signed OEM KM binary into FIT.

Important Note: The OEM KM is optional. OEMs who do not wish to use the OEM KM may keep out the OEM KM binary. By excluding or including OEM KM binary, the given platform will be **permanently** set to require/not-require OEM KM per the configuration set in FIT. This choice will only be **permanently committed** to FPF HW at the time the platform undergoes closemnf/end-of-manufacturing process. This cannot be reversed after closemnf/EOM. This will be done by an FPF value called OEM_KM_Presence. This FPF value can be viewed by MEInfo.



Intel(R) AMT

Isolated Memory Ranges

Platform Protection

Integrated Clock Controller

Networking & Connectivity

Internal PCH Buses

Power

Integrated Sensor Hub

Camera

Debug

CPU Straps

Flow 1/n

PAVP Supported	Yes	This setting determines if the Protected Audio Video Path (PAVP) fea...
Content Encryption Key		This option is for entering the raw hash 256 bit string or certificate fil...
LSPCON Internal Displa...	None	This setting determines which port for LSPCON will be connected to t...
HDCP Internal Display P...	PortA	This setting determines which port is connected for 5K output on In...

▼ **Platform Integrity**

Parameter	Value	Help Text
OEM Public Key Hash	14 05 A8 A4 EB 1C 8A ...	Raw hash string for the SHA-256 hash of the OEM public key corresp...
OEM Key Manifest Binary	...\oemkeymn2.bin	Signed manifest file containing hashes of keys used for signing comp...

Add to Intel FIT the public key hash for the OEM Key Manifest. This field is available in the Platform Protection tab.

This hash will be burned into an FPF in the FPF HW when the system closes manufacture (closemnf/EOM), and can never be changed after this stage.

Platform Protection	Content Encryption Key		This option is for entering the raw hash 256 bit string or certificate fil...
	LSPCON Internal Displa...	None	This setting determines which port for LSPCON will be connected to t...
	HDCP Internal Display P...	PortA	This setting determines which port is connected for 5K output on In...
	▼ Platform Integrity		
Platform Protection	Parameter	Value	Help Text
	OEM Public Key Hash	14 05 A8 A4 EB 1C 8A ...	Raw hash string for the SHA-256 hash of the OEM public key corresp...
	OEM Key Manifest Binary	... oemkeymn2.bin	Signed manifest file containing hashes of keys used for signing comp...

The Key Manifest ID field must be changed from 0x0 to match the value set in the OEM Key Manifest.



Figure 13. Key Manifest ID

Platform Configuration	▼ Boot Guard Configuration		
Intel (R) ME Kernel			
Intel(R) AMT			
Isolated Memory Ranges			
Platform Protection			
Integrated Clock Controller			
Networking & Connectivity			
Internal PCH Buses			
	Parameter	Value	Help Text
	Key Manifest ID	0	ODM identifier used during the Key manifest authentication process. ...
	Boot Profile	Boot Guard Profile 0 - N...	Boot Guard Profile 0 - Legacy is for platforms that do not wish to ena...
	CPU Debugging	Enabled	This setting determines if CPU debug modes will be displayed. When...
	BSP Initialization	Enabled	This setting determines BSP behavior when it receives an INIT signal...



7.6 FIT Manifest Version Validation

In order to prevent issues in the final image due to use of an incorrect MEU tool, ICL MEU inserts the MEU version into the IUP manifest during the signing process. FIT uses that data to verify that the end result image will be compatible for the image FIT is going to create.

The following checks are in place:

Test Title	Test Logic	Upon Failure
IUP manifest version is supported by CSE FW	IUP Manifest version (from IUP manifest) == FIT supported manifest version	FIT will not stitch the image. The IUP team must update MEU and resign the IUP.
MEU and FIT are from the same project	MEU version major.minor (from IUP manifest) == FIT version major.minor.	FIT will not stitch the image. The IUP team must update MEU and resign the IUP.
CSE FW version is the same as the FIT version	FIT version major.minor.hotfix.build == CSE FW version major.minor.hotfix.build	FIT will issue a warning in the log, and stitch the IFWI. Use FIT and FW from the same CSE kit.



8 Production Signing

8.1 Introduction

Some OEMs will have already existing signing tools and systems and will want to use Intel® MEU together with them without having to integrate with OpenSSL. In order to do that the OEM needs to use the MEU to create the manifests required and then perform production signing separately.

The purpose of this section is to allow customers to perform production signing without requiring MEU to run on the signing server. The OEM may use MEU to debug/dummy signing first and then export the given manifest to a signing server to perform the OEM proprietary signing flow.

8.2 Production signing high-level

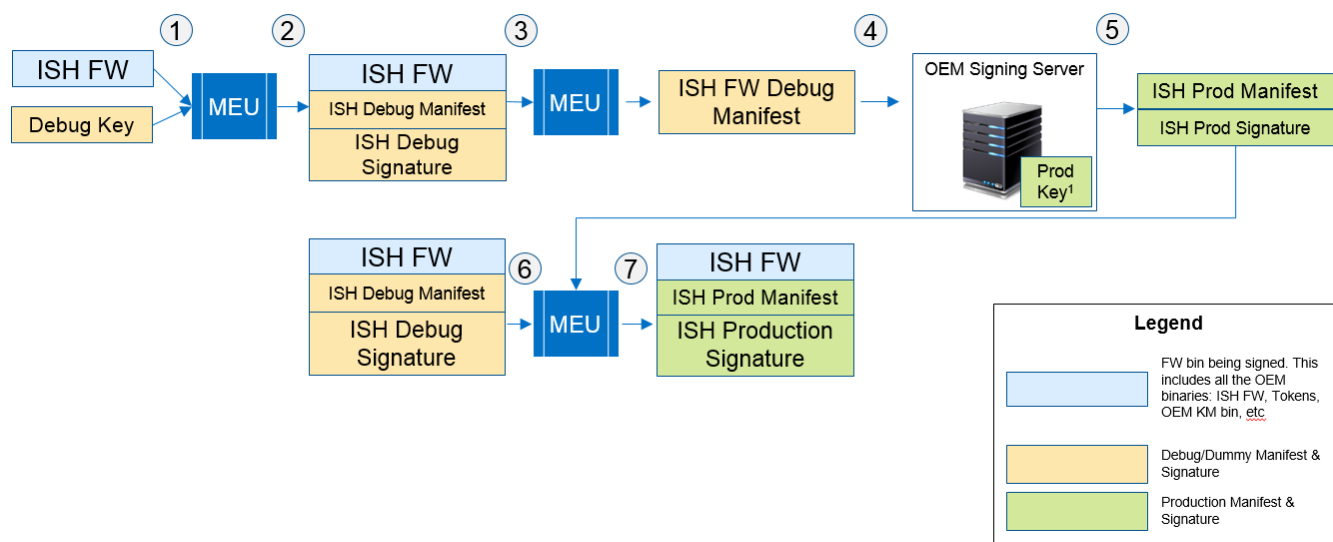


Figure 14: Production Signing Flow for OEM FW Binaries

High-level production signing process:

1. Pass the FW binary to be manifested & signed by the MEU (integrating with OpenSSL)
2. MEU adds manifest, extensions, hash, debug signature
3. Use MEU to extract debug signed manifest via export function
4. Pass the debug signed manifest to OEM signing infrastructure
5. Remove the debug signature + debug public key + sign the exported manifest with OEM signing infrastructure by inserting the production manifest + production public key



6. Pass production signed manifest and debug signed manifest+binary to MEU
7. MEU swaps the production signed manifest in place of debug signed manifest

Note: The OEM "Production Key" is the key the wish to use for the given bin for platforms in the field. They may define this key to be pre-production or production per the needs (i.e. during R&D dedicate a "Pre-production" key and for launched platforms, use "Production" key.)

8.3 Export Manifests

Use the MEU `-export` function to export the manifest from binaries who need signatures added or changed. The manifest is exported to a directory.

```
# meu -export -f <binary.bin> -o  
<directory_containing_manifests>
```

If the binary includes multiple manifests, you must specify the index of the desired manifest, e.g.

```
# meu -export 0 -f <binary.bin> -o  
<directory_containing_manifests>
```

If you do not supply an index or include `all` with the `-export` flag, MEU will output a list of all the manifests, including their indices:

More than one manifest was found in this file. Please provide a comma-separated list of the manifest indices you want to export. (ex. `-export "0,3,5"`) or specify `"all"` (ex. `-export "all"`)

The following manifests were detected:

Index	Offset	Size	Name (if available)
-------	--------	------	---------------------

0	0x000001130	0x000000D9C	FTPR.man
1	0x000053000	0x000000330	rot.key
2	0x000094058	0x000000378	RBEP.man
3	0x0000A1748	0x000001280	NFTP.man

Error 26: Failed to export manifest(s). Missing manifest indices list.

8.4 Manifest structures

In order to perform production signing on the OEM server, the OEM needs to re-sign the portion of the manifest, replace the signature and insert the production public key. This section details the manifest layout to enable this process.

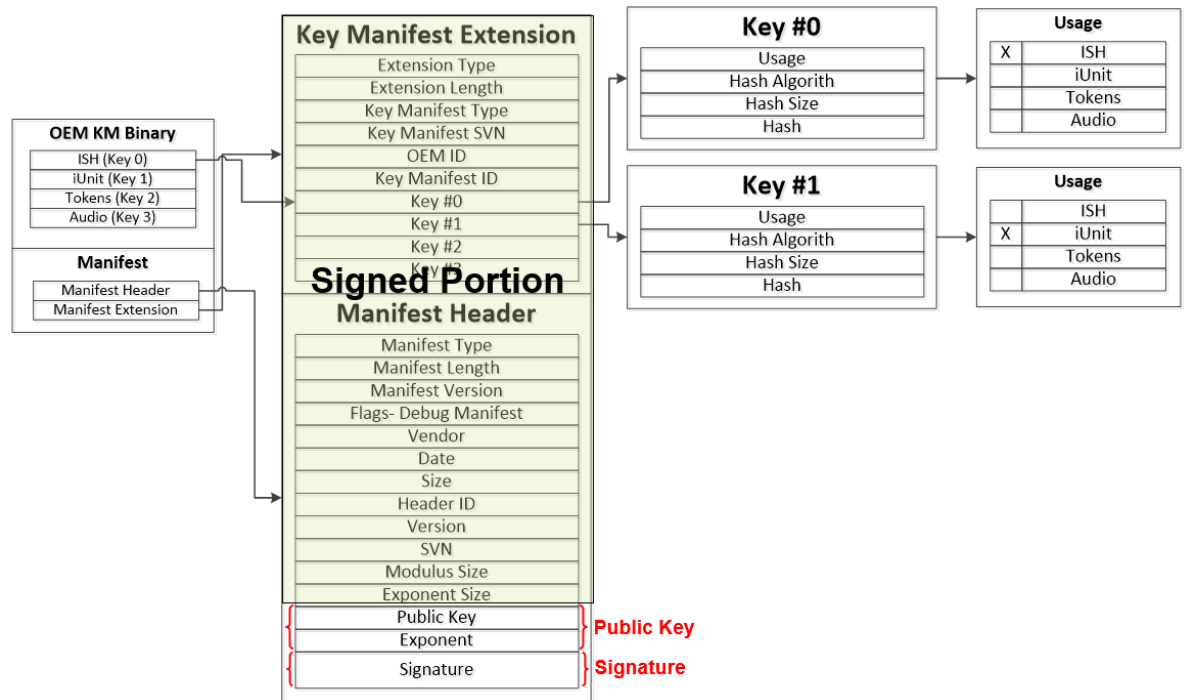


Figure 15: OEM KM Manifest Structure

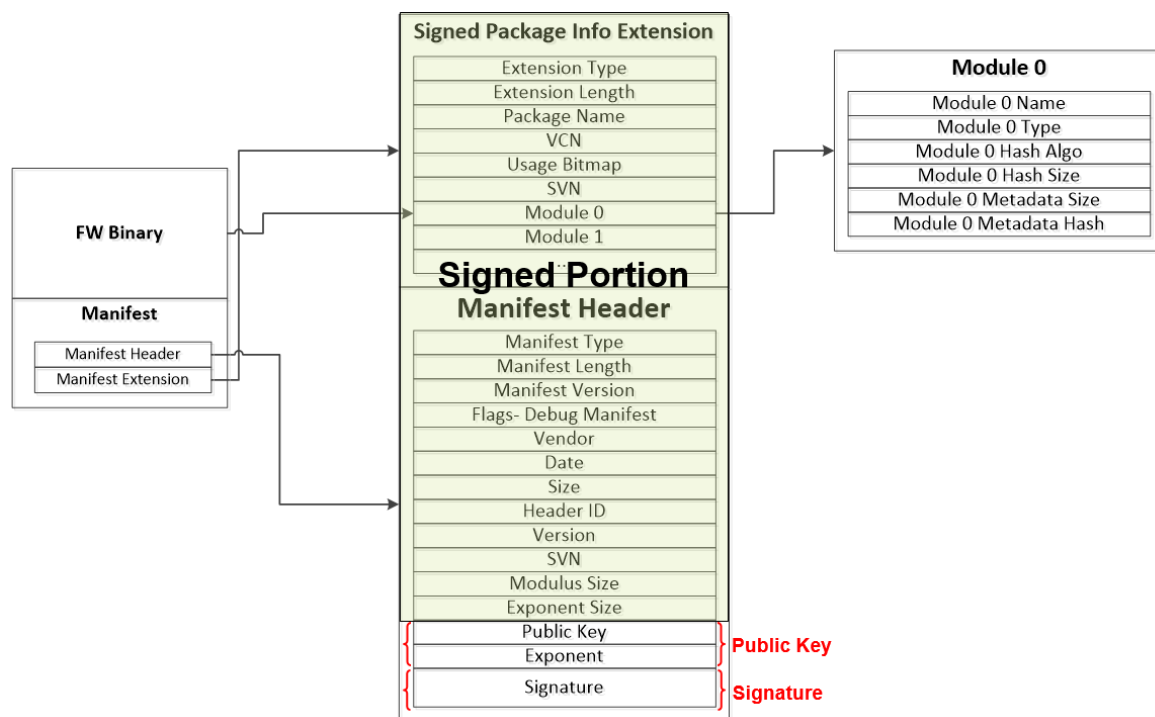


Figure 16: Code Partition Manifest Structure

8.4.1 Manifest Header

In order to use an alternate signing tool, the OEM needs to:

1. Take the "Signed Portion" section of the above shown manifests and re-sign with the production signing key.
2. Change the "Signature" and "Public Key" section with the production signature and production public key used.

Structure of manifest header:

Table 2: Manifest Header

Entry Name	Size	Description
Type	4B	Must be 0x4
Length	4B	In Dwords. - PKCSv1.5 version - 225 for SHA-384, SSA-PSS version.
Version	4B	- PKCSv1.5 version - 0x21000 for SHA-384,SSA-PSS version
Flags	4B	Manifest Flags
Flags_debug	4B	Debug flag
Vendor	4B	Vendor ID

Date	4B	yyymmdd in BCD format
Size	4B	in Dwords size of the entire manifest. Maximum size is 2K DWORDS (8KB)
Header_id	4B	Magic number. Equals \$MN2 for this version
internal_data	4B	Must be 0x4 for all headers
version_major	2B	Major Version
version_minor	2B	Minor Version
version_hotfix	2B	Hotfix
version_build	2B	Build number
Svn	4B	Secure Version Number
meu_kit_version	8B	MEU Kit Version
meu_manifest_version	4B	Manifest Version - increased each fix/change that break backward compatibility. Last word is reserved for future use
reserved	60B	will be set to 0
modulus_size	4B	In DWORDs; 64 for pkcs 1.5-2048, 96 for SSA-PSS - 3072
exponent_size	4B	In DWORDs; 1 for pkcs 1.5-2048 and for SSA-PSS - 3072

There may be multiple extensions after this manifest header making up the rest of the manifest binary.

The entire manifest binary must be hashed without the 3 'crypto' fields in the header: Public Key (offset 128, size 256), Exponent (offset 384, size 4) and Signature (offset 388, size 256). The hash must be performed using SHA-384, then be encrypted with PKCS #1-v1_5 to create the signature followed by the 3 'crypto' fields in the manifest header populated with the key, exponent and signature.

No other fields in the manifest should be changed.

8.4.2 Signed Package Info Extension

For authenticating the various platform firmware components such as aDSP, iUnit, ISH FW, etc. This structure will appear after manifest header for codepartitions as shown in Figure 16.



Table 3: Signed Package Info Extension

Name	Offset (Dec)	Offset (Hex)	Size (bytes)	Description
Extension Type	0	0	4	= 15 for Signed Pkg Info Extension
Extension Length	4	4	4	In bytes; equals $(52 + 52*n)$ for this version, where 'n' is the number of modules in the manifest
Package Name	8	8	4	Name of the package
Version Control Number (VCN)	12	C	4	The version control number (VCN) is incremented whenever a change is made to the FW that makes it incompatible from an update perspective with previously released versions of the FW
Usage Bitmap	16	10	16	Bitmap of usages depicted by this manifest, indicating which key is used to sign the manifest
SVN	32	20	4	SVN of this signed image
Reserved	36	24	16	Must be 0
Module 0 Name	52	34	12	Character array; if name length is shorter than field size, the name is padded with 0 bytes.
Module 0 Type	64	40	1	0 – Process 1 – Shared Library 2 – Data 3 – Reserved...
Module 0 Hash Algorithm	65	41	1	3 = SHA384
Module 0 Hash Size	66	42	2	Size of Hash in bytes = N. N = 32
Module 0 Metadata Size	68	44	4	Size of metadata file
Module 0 Metadata Hash	72	48	32	The SHA2 of the module metadata file
...				

8.4.3 Metadata extensions

Name	Offset	Size (bytes)	Description
Extension Type	0	4	= 10 for module attribute extension
Extension Length	4	4	In bytes; equals 56 for this version

Compression Type	8	1	0 – Uncompressed 1 – Huffman compressed 2 – LZMA compressed
Reserved	9	3	Must be 0
Uncompressed Size	12	4	Uncompressed image size, must be divisible by 4K
Compressed Size	16	4	Compressed image size. This is applicable for LZMA compressed modules only. For other modules, should be the same as “Uncompressed size” field.
Global Module Identifier	20	4	A globally unique identifier for the module. Bits 0-15: Module number, unique in the scope of the vendor: Bits 16-31: Vendor ID (PCI style)
Image hash	24	32	SHA2 Hash of uncompressed image

8.4.4 OEM Key Manifest

After Manifest Header for OEM KM, there will be Key Manifest Extension that is used for OEM KM as shown in Figure 15.

Table 4: Key Manifest Extension

Name	Offset (Dec)	Offset (Hex)	Size (bytes)	Description
Extension Type	0	0	4	= 14 for Key Manifest Extension
Extension Length	4	4	4	In bytes; equals $(36 + 68*n)$ for this version, where 'n' is the number of keys in the OEM KM manifest
Key Manifest Type	8	8	4	2 = OEM Key Manifest
Key Manifest Security Version Number (KMSVN)	12	C	4	The security version number for the OEM Key Manifest
Reserved	16	10	2	0 – Reserved
Key Manifest ID	18	12	1	ID number of the Key Manifest. This is matched by the verifier against the value stored in the platform in FPF. This is typically used as an ODM ID – to enable an OEM to assign IDs to its various ODMs and generate Key Manifests specific to each ODM.
Reserved	19	13	1	Must be 0
Reserved	20	14	16	Must be 0



Key 0 Usage	36	24	16	Bitmap of usages; allows for 128 usages. Bits 0-31 are allocated for Intel usages; bits 32-127 are allocated for OEM usages Bit 0-31: Reserved for Intel usage Bit 32: Reserved Bit 33: iUnit BootLoader Manifest Bit 34: iUnit Main FW Manifest Bit 35: cAVS Image #0 Manifest Bit 36: cAVS Image #1 Manifest Bit 37: Reserved Bit 38: OS Boot Loader Manifest Bit 39: OS Kernel manifest Bit 40: Reserved Bit 41: ISH manifest 1 (ISH Main) Bit 42: ISH manifest 2 (ISH BUP) Bit 43: OEM Debug Tokens Manifest Bit 44: Reserved Bit 45: Reserved Bit 46: Reserved Bit 47: OEM Key Attestation Bit 48: OEM DAL Manifest Bit 49 - 127: Reserved for future OEM usages
Key 0 Reserved	52	34	16	
Key 0 Reserved	68	44	1	
Key 0 Hash Algorithm	69	45	1	3 = SHA384
Key 0 Hash Size	70	46	2	Size of Hash in bytes = N. N = 32
Key 0 Hash	72	48	N (32)	The hash of the key.

8.5 Import Manifest

Use the MEU -import function to import the signed manifest back into the binary. The signed manifest must be in a separate directory passed as an input parameter. If the binary supports multiple manifests (e.g. a full SPI binary), and the folder has multiple manifests, the command will be able to import them all back into the binary.

```
# meu.exe -import <directory_containing_manifests> -f  
<input_binary.bin> -o <output_binary.bin>
```

§

9 Boot Flow Authentication

9.1 OEM KM Precedence & Key usage relationships

OEM KM contains the key hashes of the components owned/customized by the OEM.

During the authentication process, where relevant, the ME engine first checks the OEM KM to see if the desired component is listed. If the component is listed in OEM KM, the associated key hash will be used for authenticating the component and determine whether it should load.

If the component is not listed by the OEM as a desired usage in the OEM KM, the ME engine will look up the key hash in the ROT KM, and determine whether the component can load based on whether it authenticates. See table below showing the components which can be listed in the OEM KM, and what the precedence is if they are listed.

FW Component	ROT KM	OEM KM	Precedence	ME authentication behavior during FW loading
ME BUP	Y	N	ROT KM.	1. Authenticate using key in ROT KM, if no key or authentication fails, fail to boot.
ME Main	Y	N		
PMC	Y	N		
ISH BUP	Y	N		
ISH Main FW	Y	Y	OEM KM, then ROT KM.	1. Authenticate using key in OEM KM, if authenticate fails, fail to load component & exit flow. Otherwise if no key usage marked for component in OEM KM then proceed to #2 2. Authenticate using key in ROT KM if no key or authenticate fails, fail to load component.
iUnit Boot Loader	Y	Y		
iUnit Main FW	Y	Y		
Audio (cAVS) Image #0	Y	Y		
IsiOemManifest	Y	Y		
OS Boot Loader	N	Y	OEM KM Only.	1. If key usage marked for component in OEM KM, authenticate using key in OEM KM, if authenticate fails, fail to load component & exit flow.
OS Kernel	N	Y		
OEM Debug Tokens	N	Y		



10 Common Bring Up Issues and Troubleshooting Table

10.1 Common Bring Up Issues and Troubleshooting Table

Problem / Issue	Solution / Workaround
Intel MEU tool fails to run	Confirm that the MEU_Config and template xml files are present in the same folder as the Intel MEU tool. Confirm that both files have been modified properly.
Audio component fails to load although signed and entered into image as instructed	Check in OEM KM, that the OEM audio component uses the cAVS0 key in OEM KM, not cAVS1.

§