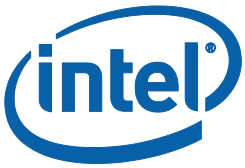


Gemini Lake Platform – Intel® Trusted Execution Engine (Intel® TXE) Firmware Bring-up Guide – A "Quick Start" guide into GLK

Quick Start Guide

July 2017

Revision 1.0

Intel Confidential

Contents

Figures

1 Introduction

This document covers the quick start procedure for Gemini Lake Platform (GLK) Intel® Trusted Execution Engine (Intel®TXE) Firmware.

IMPORTANT NOTE: This guide only contains the SMIP configuration procedure for the basic boot of any Gemini Lake platform. This document is NOT intended to serve as a guidance on any of the used tools or as a manipulation guide on how to edit or sign images, create manifests, or enable any components or regions that are irrelevant to a normal basic boot. It also does not include booting using DnX (Download and Execute) as it is solely intended for SPI flash and basic boot.

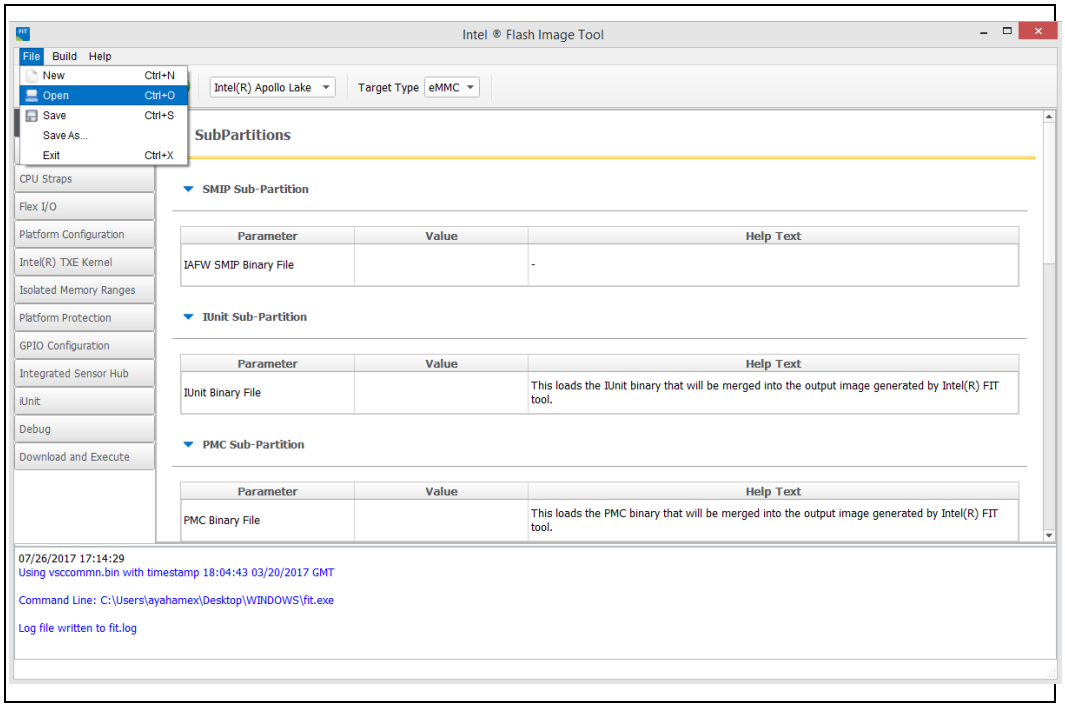
Please note that the purpose of this document is to enable its' readers to quick start and boot a GLK platform to OS by walking-through the image creation and flashing using Intel® Flash Image Tool and Dediprog tools.
For the complete guide for the platform Signed Master Image Profile "SMIP" configurations please refer to "Gemini Lake Intel® TXE Firmware Bring-up guide_V1_0" and "Gemini Lake SoC SPI and SMIP programming guide".

2 Image Creation & Flashing

2.1 Building the image using Intel® FIT

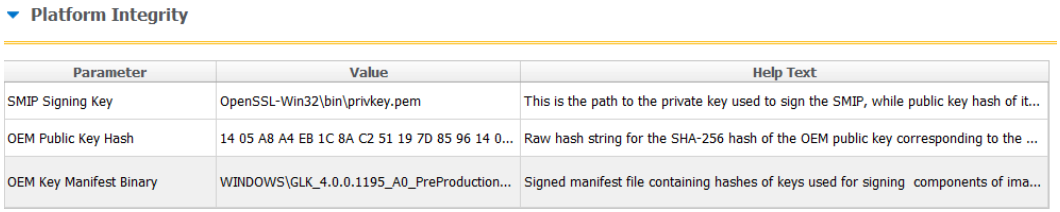
- Start the Intel® FIT tool.
- Drag and drop the IFWI (Integrated Firmware Image) into the Intel® FIT tool (or using the upper ribbon → File → Open, and then selecting the image as shown in the figure below)

Figure 1 – Opening image through FIT



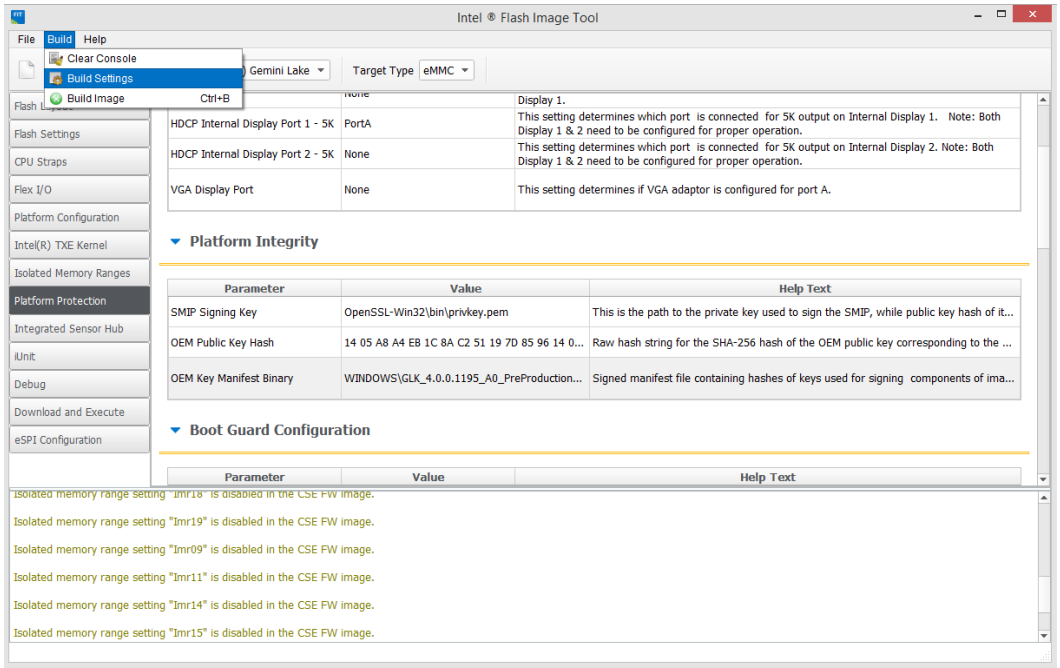
- Loading the image into Intel® FIT will decompose all the various components and update all GUI elements of Intel® FIT.
- Users can change pre-defined regions and any of the components or sub-partitions as desired prior to building the image.
- In the Platform Protection tab in Intel® FIT and under platform Integrity section, users must add the path to the private key created using the OpenSSL tool. However, users can choose not to enable OEM signing and hence editing this field would not be required.

Figure 2 – Editing the SMIP Signing Key Field



After editing all the required fields and regions. Users should configure the build settings, clicking on the build settings icon or through Build → Build Settings as shown below.

Figure 3 – Build Settings



In the Build Settings window, the user must configure three important fields:

1. Region Order: This should contain the order in which the regions will be sorted.
2. Intel® Manifest Extension Utility: This should contain the path to the accompanying Intel® MEU tool.
3. Signing Tool Path: This should contain the path to the signing tool used earlier to create the required keys.

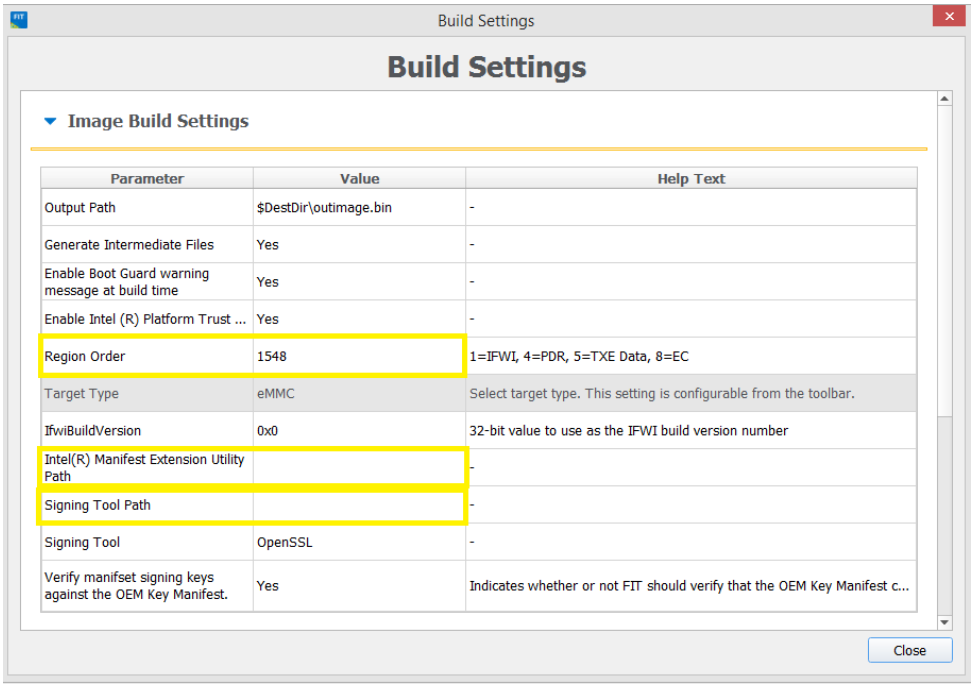
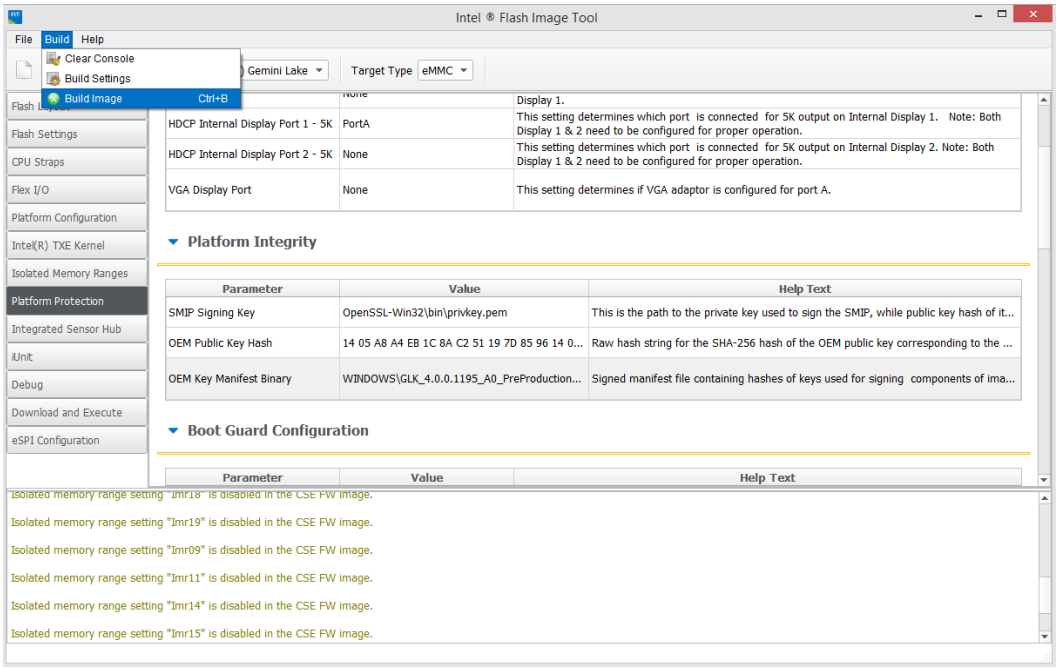


Figure 4 – Configuring Build Settings

The next step, after configuring all required fields and regions, would be building the image. This is done by clicking on the green Build icon in Intel® FIT or by going through "Build → Build Image" as shown below. The result, if not changed in the build configuration, would be an image under the name "outimage.bin" located in the Intel® FIT folder unless specified otherwise by the user. A successful build message can be seen typed in the console at the bottom of the tool.

Figure 5 – Building the image



2.2 Flashing the image & ROM Bypass

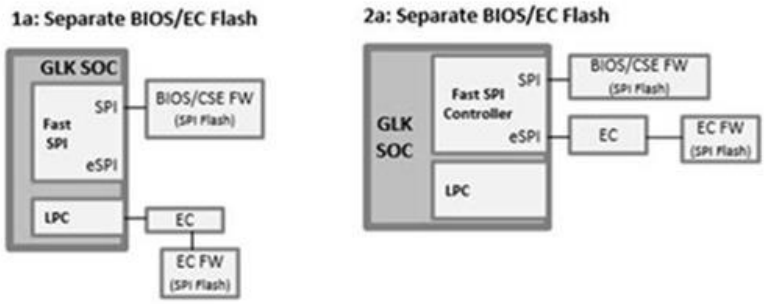
ROM bypass needs to be flashed to the platform prior to the bring-up procedure using the image built for GLK platforms.

The ROM bypass SPI (Serial Peripheral Interface) image can be found in the Intel® TXE FW kit, under “Image_Components\TXE” or can be the outimage.bin created earlier using Intel® FIT tool.

2.2.1 Flashing the ROM bypass

Depending on the applied configuration option on the platform, which can be either 1a or 2a (shown in the figure below), the user must connect the Dediprog to the suitable port.

Figure 6 – BIOS & EC (Embedded Controller) Configurations



- Connect the Dediprog to the EC pins (marked in yellow below) on the platform and run the Dediprog software to burn the proper KSC (Keyboard System Controller). The KSC is required prior to the ROM Bypass and can be found in the relevant GLK kit.

Figure 7 – EC pins for KSC flashing

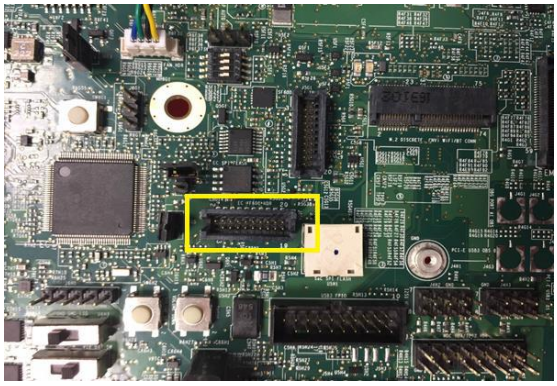
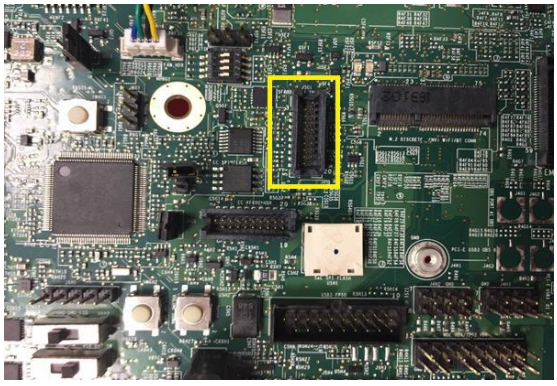
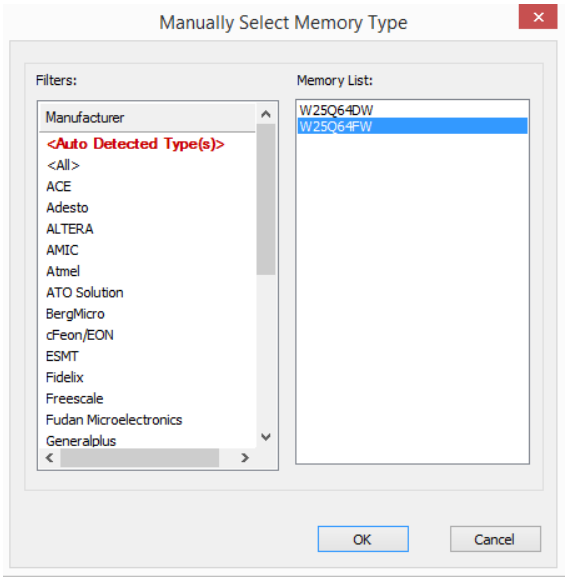


Figure 8 – SF600 pins for SPI flashing



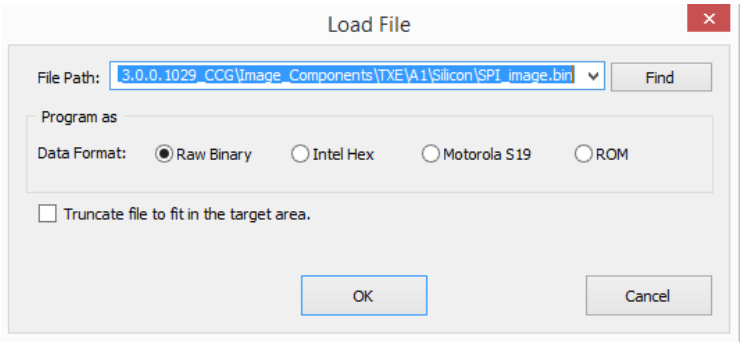
- Connect the Dediprog to the SF600 pins (marked in yellow in the below image) on the platform and run the Dediprog software.
- Click "Detect".
- In the "Manually Select Memory Type" window, select the SPI flash and click OK
  Note: on Intel RVP choose: "W25Q64FW"

Figure 9 – Selecting the SPI Component



- Click "File", select the SPI image that was built in section 2.1.

Figure 10 – Load File Settings



- Click "Batch" to flash the file, when the procedure is over, click "Verify" to verify that the flashing was performed correctly