

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

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described 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.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel, the Intel logo, Intel® TXE, Intel® FIT, Intel® ISS, Intel® PTT, are trademarks of Intel Corporation in the U.S. and/or other countries.

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

© 2017 Intel Corporation. All rights reserved.

Intel Confidential



Contents

1	Introdu	uction 4	r
2	Image	Creation & Flashing	,
	2.1	Building the image using Intel® FIT5	;
	2.2	Flashing the image & ROM Bypass8	3
		2.2.1 Flashing the ROM bypass	;

Figures

Figure 1 – Opening image through FIT	
Figure 2 – Editing the SMIP Signing Key Field	
Figure 3 – Build Settings	
Figure 4 – Configuring Build Settings	7
Figure 5 – Building the image	
Figure 6 - BIOS & EC (Embedded Controller) Config	urations
Figure 7 – EC pins for KSC flashing	Figure 8 – SF600 pins for SPI flashing9
Figure 9 - Selecting the SPI Component	
Figure 10 – Load File Settings	

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

		Intel ® F	lash Image Tool –	
Build Help				
New Ctrl+ Open Ctrl+	N Intel(R) Apollo Lake 🔻	Target Type eMMC 👻		
Save Ctrl+	s			_
Save As	SubPartitions			
Exit Ctrl+	x			_
Straps	- CHID Cub Partition			
1/0				
orm Configuration	Deservator	Malua	Itala Taut	
	Parameter	value	Heip Text	-
(R) TXE Kernel	IAFW SMIP Binary File			
ted Memory Ranges				-
orm Protection	 IUnit Sub-Partition 			
Configuration				-
arated Sensor Hub	Parameter	Value	Help Text	
graceu Sensor Hub	IUnit Binary File		This loads the IUnit binary that will be merged into the output image generated by $Intel(R)$ FIT tool.	
ug mload and Execute	 PMC Sub-Partition 			
	Parameter	Value	Help Text	
	PMC Binary File		This loads the PMC binary that will be merged into the output image generated by $\ensuremath{Intel}(\ensuremath{R})$ FIT tool.	
16/2017 17:14:29 g vsccommn.bin with time imand Line: C:\Users\aya file written to fit.log	rstamp 18:04:43 03/20/2017 GMT hamex\Desktop\WINDOWS\fit.exe			

- 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 subpartitions 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

Platform Integrity

Parameter	Value	Help Text
SMIP Signing Key	OpenSSL-Win32\bin\privkey.pem	This is the path to the private key used to sign the SMIP, while public key hash of it
OEM Public Key Hash	14 05 A8 A4 EB 1C 8A C2 51 19 7D 85 96 14 0	Raw hash string for the SHA-256 hash of the OEM public key corresponding to the \dots
OEM Key Manifest Binary	WINDOWS\GLK_4.0.0.1195_A0_PreProduction	Signed manifest file containing hashes of keys used for signing components of ima

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

Figure 3 – Build Settings

(11	Intel ® Flash Image Tool 🛛 🔷 🗖 🗙						
File Build Help							
Clear Console) Ger	mini Lake 🔻	Target Type eMMC 💌				
Ebch I 💿 Build Image	Ctrl+B		None	Display 1.			-
Flash Settings	HDCP Internal Displ	lay Port 1 - 5K	PortA	This setting de Display 1 & 2	termines which port is connected for 5K output on Internal Display 1. Note: Both need to be configured for proper operation.		1
CPU Straps	HDCP Internal Displ	lay Port 2 - 5K	None	This setting de Display 1 & 2	termines which port is connected for 5K output on Internal Display 2. Note: Both eed to be configured for proper operation.		1
Flex I/O	VGA Display Port		None	This setting de	termines if VGA adaptor is configured for port A.		
Platform Configuration						-	
Intel(R) TXE Kernel	 Platform In 	ntegrity					
Isolated Memory Ranges						_	
Distance Destantion	Parame	eter	Value		Help Text		
Platform Protection	SMIP Signing Key		OpenSSL-Win32\bin\privkey.pem		This is the path to the private key used to sign the SMIP, while public key hash of it		
Integrated Sensor Hub	OEM Public Key Has	sh	14 05 A8 A4 EB 1C 8A C2 51 19 70	85 96 14 0	Raw hash string for the SHA-256 hash of the OEM public key corresponding to the		
iUnit							
Debug	OEM Key Manifest E	Binary	WINDOWS\GLK_4.0.0.1195_A0_Pr	eProduction	Signed manifest file containing hashes of keys used for signing components of ima		
Download and Execute							
eSPI Configuration	 Boot Guard 	d Configura	tion				
	Parame	eter	Value		Help Text		*
Isolated memory range setting	g "Imr18" is disabled	In the CSE FW I	image.				1
Isolated memory range setting	g "Imr19" is disabled	in the CSE FW	image.				
Isolated memory range setting	g "Imr09" is disabled	in the CSE FW i	image.				
Isolated memory range setting	g "Imr11" is disabled	in the CSE FW i	image.				1
Isolated memory range setting	g "Imr14" is disabled	in the CSE FW i	image.				
Isolated memory range setting	g "Imr15" is disabled	in the CSE FW i	image.			-	Ŧ

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
				occurgo

1

Build Settings ×							
Build Settings							
 Image Build Settings 							
Parameter	Value	Help Text					
Output Path	\$DestDir\outimage.bin	-					
Generate Intermediate Files	Yes	-					
Enable Boot Guard warning message at build time	Yes	-					
Enable Intel (R) Platform Trust	Yes	-					
Region Order	1548	1=IFWI, 4=PDR, 5=TXE Data, 8=EC					
Target Type	eMMC	Select target type. This setting is configurable from the toolbar.					
IfwiBuildVersion	0x0	32-bit value to use as the IFWI build version number					
Intel(R) Manifest Extension Utility Path		-					
Signing Tool Path		· .					
Signing Tool	OpenSSL	-					
Verify manifset signing keys against the OEM Key Manifest.	Yes	Indicates whether or not FIT should verify that the OEM Key Manifest c					

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 \rightarrow 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

			Intel ® FI	ash Image To	ol – 🗆	
e Build Help) Gemini Lake 🔻	Target Type eMMC 💌			
🔐 🚱 Build Image	Ctrl+B		NOLIE	Display 1.		
sh Settings	HDCP Internal	Display Port 1 - 5K	PortA	This setting d Display 1 & 2	etermines which port is connected for 5K output on Internal Display 1. Note: Both need to be configured for proper operation.	
U Straps	HDCP Internal	Display Port 2 - 5K	None	This setting d Display 1 & 2	etermines which port is connected for 5K output on Internal Display 2. Note: Both need to be configured for proper operation.	
x I/O	VGA Display P	ort	None	This setting d	etermines if VGA adaptor is configured for port A.	
tform Configuration						
tel(R) TXE Kernel	Platfor	m Integrity				
plated Memory Ranges						
atform Protection	Pa	rameter	Value		Help Text	
egrated Sensor Hub	SMIP Signing	Key	OpenSSL-Win32\bin\privkey.pem	n This is the path to the private key used to sign the SMIP, while public key hash		
j.	OEM Public Ke	y Hash	14 05 A8 A4 EB 1C 8A C2 51 19 7	D 85 96 14 0	Raw hash string for the SHA-256 hash of the OEM public key corresponding to the	
bug	OEM Key Mani	M Key Manifest Binary WINDOWS\GLK_4.0.0.1195_A0_		0_PreProduction Signed manifest file containing hashes of keys used for signing components of		
wnload and Execute	1					
PI Configuration	Boot Generation	uard Configura	ation			
	Pa	rameter	Value		Help Text	
plated memory range set	ting "Imr18" is also	DIED IN THE CSE FW	image.			
lated memory range set	ting "Imr19" is disa	bled in the CSE FW	image.			
plated memory range set	ting "Imr09" is disa	bled in the CSE FW	image.			
plated memory range set	ting "Imr11" is disa	bled in the CSE FW	image.			
olated memory range set	ting "Imr14" is disa	bled in the CSE FW	image.			
plated memory range set	ting "Imr15" is disa	bled in the CSE FW	image.			
.,			<u> </u>			

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



2a: Separate BIOS/EC Flash



• 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

iters.		Memory List.
Manufacturer	^	W25Q64DW
<auto detected="" type(s)=""></auto>		
<all></all>		
ACE		
Adesto		
ALTERA		
AMIC		
Atmel		
ATO Solution		
BergMicro		
cFeon/EON		
ESMT		
Fidelix		
Freescale		
Fudan Microelectronics		
Generalplus	~	
<	>	

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

Figure 10 – Load File Settings

	Load Fil	e		×
File Path: 3.0.0.1029_CCG\Image	e_Components\TX	E\A1\Silicon\SPI_image.	bin 🗸 Find	
Program as	0	0	0	
Data Format: (Raw Binary	O Intel Hex	O Motorola S19	O ROM	
Truncate file to fit in the target	area.			
	ОК		Cancel	
Data Format:	O Intel Hex area.	O Motorola S19	Cancel	

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