SIIP Scripts for Elkhart Lake Platform

Releasenote

Date: July 2019

Revision: 0.6.0

Intel Confidential

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

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

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.

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

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, Intel brands, and the Intel logo 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.

Copyright © 2019, Intel Corporation. All rights reserved.

Contents

[1.0 Introduction 6](#_Toc14265461)

[1.1 Purpose 6](#_Toc14265462)

[1.2 Audience 6](#_Toc14265463)

[1.3 Acronyms 6](#_Toc14265464)

[2.0 New in This Release 7](#_Toc14265465)

[2.1 New Features 7](#_Toc14265466)

[2.2 Changes to Existing Features 7](#_Toc14265467)

[2.3 Unsupported or Discontinued Features 7](#_Toc14265468)

[3.0 Fixed Issues 7](#_Toc14265469)

[3.1 SIIP Stitch Script 7](#_Toc14265470)

[3.2 SIIP Sign Script 7](#_Toc14265471)

[4.0 Known Issues 8](#_Toc14265472)

[5.0 Related Documentation 9](#_Toc14265473)

[6.0 Where to Find the Release 9](#_Toc14265474)

[7.0 Release Content 9](#_Toc14265475)

[7.1 Component Revision Numbers 9](#_Toc14265476)

[8.0 Hardware and Software Compatibility 11](#_Toc14265477)

[8.1 BIOS/Firmware Version 11](#_Toc14265478)

[8.2 Supported Operating Systems 11](#_Toc14265479)

Tables

[Table 1 Acronyms Used in Document 8](#_Toc14255841)

[Table 2 SIIP Scripts Component Revision Numbers 11](#_Toc14255842)

[Table 3 SIIP Stitch Script Component Revision Numbers 12](#_Toc14255843)

[Table 4 SIIP Sign Script Component Revision Numbers 12](#_Toc14255844)

[Table 5 Sub-Region Capsule Script Component Revision Numbers 12](#_Toc14255845)

[Table 6 SIIP Scripts Support Component Revision Numbers 12](#_Toc14255846)

***Revision History***

|  |  |  |
| --- | --- | --- |
| **Date** | **Revision** | **Description** |
| July 16, 2019 | 0.6.0 | Pre-Alpha Release corresponding to SIIP Scripts version 0.6.0 with the following changes:   1. SIIP Sign Script:    1. Fixed #29951, previous fix was not complete to handle verify subcommand when two keys are provided from command line and removed dead bash script 'test\_me'    2. Update: separated FKM as a separate file    3. Fixed coding style (PEP8 and Flake8)    4. Fix script per security review feedback:       1. SHA1 shall not be allowed as hashing option       2. RSA key size shall not be less than 2048 bits long    5. Fixed signing issue for GOP/GFX/VBT    6. Fixed bug in stitching PEIM GFX driver, PEIM GFX driver should be compressed using PI\_STD flag, instead of PI\_NONE 2. SIIP Stitch Script: 3. Added stitching feature for GOP, PEM GFX and VBT images to BIOS, fixed signing as GOP image required to be signed before stitching 4. Fixed #303203 Stitch passed but temporary working directory unable to remove when we switch the suggested root path to the other path 5. Fixed #302775 Typo in README.md and SIIPStitch.py file for version description |
| June 21, 2019 | 0.2.0 | Engineering Drop Release corresponding to SIIP Scripts version 0.2.0 with the following changes:   1. Overall: 2. Add a top level README as user guide document 3. Sub-Region Capsule: 4. Add Print output message 5. Fixed STDIN input to return bytes array 6. Fixed #299938 STDIN input to return bytes array 7. Fixed #299937 and #299569 Typo in readme file 8. Removed unused files and tools 9. Removed the 2 from IntelOob2Config 10. Updated README.md consistent with the code 11. SIIP Stitch: 12. Updated check valid IP names from a list 13. Removed GUID tool Rsa2048Sah256Sign 14. Removed debug code 15. Fixed #299330 Stitch failed with error "Error using FMMT.exe" when input file in half path 16. Fixed #299322 Stitch failed with error "Error base\_tool is not located: GenSec" when manually set EDK\_TOOLS\_BIN path 17. Fixed #300930 SIIPStitch should return a error when it does not find the firmware volume that match the requirement file to replace. 18. Fixed #300551 Stitch tool hang without error message prompt out when input empty bios 19. Fixed #300553 Stich tool hang without error message prompt out when input random gen binary file as BIOS 20. Fixed #300554 Stitch tool successfully stitch empty OseFw without error 21. Fixed #299943 Wrong Command to check OpenSSL is located in README file 22. Fixed #299945 Wrong Path for siipSupport folder in README file 23. SIIP Sign:     1. Fixed #299515 Sign and verify function not able to completed successfully if input files path consists of semicolon |
| May 24, 2019 | 0.1.0 | Engineering Drop Release corresponding to SIIP Scripts version 0.1.0 with the following changes:   1. This package consists of three scripts:    1. SIIP Stitch Script ( SIIPStitch.py ): Stitch a signed image into a full IFWI image    2. New Release: SIIP Sign Script ( SIIPSign.py ): Sign a payload image according to SIIP specification    3. New Release: Sub-region Capsule Script ( GenerateSubRegionCapsule.py ): Create a UEFI capsule image containing the signed image 2. Update BSD 2 Clause Licenses for release. 3. SIIP Stitch Script:    1. Correct SIIPStitch version control from v0.6.0 to v0.5.2 for engineering drop release.    2. Fixed stitching IFWI error. 4. SIIP Sign Script: New release, version v0.2.0 5. Sub-Region Capsule Script: New release, version 0.1.0 |

# Introduction

## Purpose

This document provides system requirements, installation instructions, issues and limitations, and legal information.

To learn more about this product, see:

* New features listed in the [New in this Release](#_What's_New) section below, or in the help.
* Reference documentation listed in the [Related Documentation](#_Related_Documentation) section below
* Installation instructions can be found at ***README.md.html***

## Audience

The audience for this document is developers and product design teams who are creating system running on the Elkhart Lake platform.

## Acronyms

The following acronyms are used in this document (arranged in alphabetical order).

Table 1 Acronyms Used in Document

| Acronym | Description |
| --- | --- |
| PSE | Intel® Programmable Services Engine |
| SIIP | SoC Independent IP |

# New in This Release

## New Features

* Added stitching feature for GOP, PEM GFX and VBT images to BIOS, fixed signing as GOP image required to be signed before stitching

## Changes to Existing Features

* Update: separated FKM as a separate file

## Unsupported or Discontinued Features

* None in this release.

# Fixed Issues

## SIIP Stitch Script

* Fixed #303203 Stitch passed but temporary working directory unable to remove when we switch the suggested root path to the other path
* Fixed #302775 Typo in README.md and SIIPStitch.py file for version description

## SIIP Sign Script

* Fixed #29951, previous fix was not complete to handle verify subcommand when two keys are provided from command line and removed dead bash script 'test\_me'
* Fixed coding style (PEP8 and Flake8)
* Fix script per security review feedback:
* SHA1 shall not be allowed as hashing option
* RSA key size shall not be less than 2048 bits long
* Fixed signing issue for GOP/GFX/VBT
* Fixed bug in stitching PEIM GFX driver, PEIM GFX driver should be compressed using PI\_STD flag, instead of PI\_NONE

# Known Issues

Does not support Linux

# Related Documentation

README.md.html

# Where to Find the Release

Intel® Programmable Services Engine (PSE)

# Release Content

## Component Revision Numbers

Table 2 SIIP Scripts Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Scripts | SIIP\_Scripts\siipSign  SIIP\_Scripts\siipStitch  SIIP\_Scripts\siipSupport  SIIP\_Scripts\SubRegionCapsule  SIIP\_Scripts\SIIPSupport.py  SIIP\_Scripts\siip\_constants.py | N/A |
| Readme Files | README.md.html  README.md | N/A |
| Releasenote | Releasenotes.docx | 0.6.0 |

Table 3 SIIP Stitch Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Stitch Script Files | siipStitch\README.md  siipStitch\README.md.html  siipStitch\SIIPStitch.py | 0.6.0 |

Table 4 SIIP Sign Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Sign Script Files | siipSign\README.md  siipSign\README.md.html  siipSign\SIIPSign.py | 0.6.0 |

Table 5 Sub-Region Capsule Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| Sub-Region Capsule Script Files | SubRegionCapsule\GenerateCapsule.py  SubRegionCapsule\GenerateSubRegionCapsule.py  SubRegionCapsule\README.md  SubRegionCapsule\README.md.html  SubRegionCapsule\SubRegionDescriptor.py  SubRegionCapsule\SubRegionImage.py | 0.6.0 |
| Common Tools and Files | SubRegionCapsule\Common  SubRegionCapsule\CommonDataClass  SubRegionCapsule\Examples | N/A |

Table 6 SIIP Scripts Support Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Scripts Support Files | siipSupport\Bin\Win32\FMMT.exe  siipSupport\Bin\Win32\FmmtConf.ini  siipSupport\Bin\Win32\GenFfs.exe  siipSupport\Bin\Win32\GenFv.exe  siipSupport\Bin\Win32\GenSec.exe  siipSupport\Bin\Win32\LzmaCompress.exe  siipSupport\Bin\Win32\rsa\_helper.py | N/A |

# Hardware and Software Compatibility

Elkhart Lake platform

## BIOS/Firmware Version

* TBD

## Supported Operating Systems

* Window 10