SIIP Scripts for Elkhart Lake Platform

Release Notes

Date: October 2019

Revision: 0.7.2

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 9](#_Toc23199265)

[1.1 Purpose 9](#_Toc23199266)

[1.2 Audience 9](#_Toc23199267)

[1.3 Acronyms 9](#_Toc23199268)

[2.0 New in This Release 10](#_Toc23199269)

[2.1 New Features 10](#_Toc23199270)

[2.2 Changes to Existing Features 10](#_Toc23199271)

[2.3 Unsupported or Discontinued Features 10](#_Toc23199272)

[3.0 Fixed Issues 10](#_Toc23199273)

[3.1 Overall 10](#_Toc23199274)

[3.2 SIIP Stitch Script 10](#_Toc23199275)

[3.3 SIIP Sign Script 11](#_Toc23199276)

[3.4 Sub-Region Capsule 11](#_Toc23199277)

[4.0 Known Issues 11](#_Toc23199278)

[5.0 Related Documentation 12](#_Toc23199279)

[6.0 Where to Find the Release 12](#_Toc23199280)

[7.0 Release Content 12](#_Toc23199281)

[7.1 Component Revision Numbers 12](#_Toc23199282)

[8.0 Hardware and Software Compatibility 13](#_Toc23199283)

[8.1 BIOS/Firmware Version 13](#_Toc23199284)

[8.2 Supported Operating Systems 13](#_Toc23199285)

Tables

[Table 1 Acronyms Used in Document 9](#_Toc23199286)

[Table 2 SIIP Scripts Component Revision Numbers 12](#_Toc23199287)

***Revision History***

|  |  |  |
| --- | --- | --- |
| **Date** | **Revision** | **Description** |
| October 28, 2019 | 0.7.2 | Engineering Release corresponding to SIIP Scripts version 0.7.2 with the following changes:   1. Overall:    1. Add Linux OS support    2. Fixed RTC# 310845, [FBU] Add logger support    3. Fixed RTC# 310847, [FBU] Integrate simics tests using automation scripts 2. SIIP Stitch Script:    1. Fixed RTC #307926, SIIPStich do not have check on missing third party tool    2. Fixed RTC #311465, Refactor generate\_\* capsule script with stitch script 3. SIIP Sign Script:    1. Updated fill module type in CPD entries    2. Added a simple checksum function    3. Fixed RTC #305593, [SIIPSign] Add RSA 3072 signing support    4. Updated RTC #310218, [sign] Make RSA 3K and SHA384 as default in signing 4. Sub-Region Capsule:    1. Updated RTC #311047, Update JSON for TSN config with EHL Power On changes |
| October 3rd 2019 | 0.7.1 | Alpha Release |
| September 20th 2019 | 0.7.1 | Alpha Release Candidate2 corresponding to SIIP Scripts version 0.7.1 with the following changes:   1. Overall:    1. Fixed RTC#308211, Add FAQ to README    2. Fixed RTC#308297, Add banners to all scripts    3. Updated RTC#300610: complete release package with a single step 2. SIIP Stitch Script:    1. Fixed RTC #307926, SIIPStich do not have check on missing third party tool    2. Fixed RTC #307930, SIIPStitch tool do not have check if privatekey file is not found    3. Fixed RTC#305839, when we change the init sequence, HU will print error    4. Fixed RTC#307925, Example file on Help menu for IPNAME\_IN is not updated    5. Fixed RTC#309053, Load JSON as input to stitch subregions    6. Fixed RTC#309049, VBT stitching failed to boot with BIOS v1374    7. Fixed RTC#309545, Stitch one inputfile to merge GFX PEIM into IFWI 3. Sub-Region Capsule:    1. Fixed RTC#309024, Wrong GUID is used for OOB sub-region    2. Fixed RTC#308208, Update IP filenames to match new BIOS files. |
| September 4th 2019 | 0.7.0 | Alpha Release Candidate corresponding to SIIP Scripts version 0.7.0 with the following changes:   1. Overall:    1. Update allow scripts to run from script directory    2. Fixed RTC# 304639, Fix coding style in all scripts    3. Added RTC #300610, Created a complete release package with a single step and reorganize script and shared code into new layout: 2. scripts : entry to all scripts 3. 3rdParty : Third party code 4. common : modules and libraries 5. SIIP Sign Script:    1. Added RTC #305963, Support stitching GOP/PEIM GFX/VBT into IFWI image 6. SIIP Stitch Script:    1. Update stitching Include Gfx PEIM in OBB stitching flow    2. Fixed RTC #304918, Timeout time too short causing the failure of stitching    3. Fixed RTC #305982, Stitching not working on some systems with predefined timeout of 10 seconds    4. Fixed RTC #305321, SIIPStitch tool do not have a check file on IPNAME\_IN file size    5. Fixed RTC #305325, SIIPStitch tool do not have a check on IPNAME\_IN2 file size    6. Update RTC #306596, Update siiipstitch tool to recognize the new IP filenames with PSE instead of OSE    7. Fixed RTC #305389, SIIPStitch tool do not have a check on privatekey file size    8. Fixed RTC#305296, Unable stitch with privatekey full path    9. New feature request RTC #305460, New feature request to support GbE 3 Sub-Regions on BIOS and PSE, HSD-ES RCR: https://hsdes.intel.com/resource/1507303757 7. Sub-Region Capsule:    1. Updated sub-region examples and FV alignment    2. Update RTC #306548, Separate subregion JSON conversion to binary feature from main script    3. Fixed RTC#304497, All data is read from file even if the size set in json is less than file size |
| August 2nd , 2019 | 0.6.1 | Pre-Alpha Release. |
| July 26, 2019 | 0.6.1 | Pre-Alpha Release Candidate2 corresponding to SIIP Scripts version 0.6.1 with the following changes:   1. Overall:    1. Update Readme to match the latest code for all scripts    2. Fixed inconsistent data handling 2. SIIP Sign Script:    1. RTC#304639: Fix coding styles 3. SIIP Stitch Script:    1. Fixed #304887, Readme file is not updated based on ww29.3 Release    2. Fixed #304889, SIIPStitch tools do not have a check on missing GenFv.exe    3. Fixed #304892, Error message for missing required executable file is not updated based on latest directory name    4. Fixed #304893, Misleading error message for privatekey when stitch with invalid private key's name    5. Fixed #304918, Timeout time too short causing the failure of stitching    6. Updated siip\_stitch.py to meet flake8 and pycodestyle 4. Sub-Region Capsule:    1. Fixed #304639, Fixing coding style issues |
| July 16, 2019 | 0.6.0 | Pre-Alpha Release Candidate 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.******docx***

## 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 |
| --- | --- |
| FMMT | Intel(R) Firmware Module Management Tool |
| PSE | Intel® Programmable Services Engine |
| SIIP | SoC Independent IP |

# New in This Release

## New Features

* None in this release.

## Changes to Existing Features

* **SIIP Sign**: Updated RTC #310218, [sign] Make RSA 3K and SHA384 as default in signing.

## Unsupported or Discontinued Features

None in this release.

# Fixed Issues

## Overall

* Add Linux OS support
* Fixed RTC# 310845, [FBU] Add logger support
* Fixed RTC# 310847, [FBU] Integrate simics tests using automation scripts

## SIIP Stitch Script

* Fixed RTC #307926, SIIPStich do not have check on missing third party tool
* Fixed RTC #311465, Refactor generate\_\* capsule script with stitch scrip

## SIIP Sign Script

* Updated fill module type in CPD entries
* Added a simple checksum function
* Fixed RTC #305593, [SIIPSign] Add RSA 3072 signing support
* Updated RTC #310218, [sign] Make RSA 3K and SHA384 as default in signing

## Sub-Region Capsule

* Updated RTC #311047, Update JSON for TSN config with EHL Power On changes

# Known Issues

* [SIIP Stitch]: RTC #306596 implemented to recognize the new IP filenames with PSE instead of OSE, testing used pervious IFWI and PSE FW (before ER23 release) will cause stitching error message popup.
  + **Workaround**: Manually rename filenames with OSE (example: OseFw.bin) instead of PSE (example: PseFw.bin).

# Related Documentation

README.docx

# Where to Find the Release

Intel® Programmable Services Engine (PSE) , link: TBD

# Release Content

## Component Revision Numbers

Table 2 SIIP Scripts Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| common | common\ \_\_init\_\_.py  common\banner.py  common\configparser.py  common\firmware\_volume.py  common\ifwi.py  common\logging.py  common\siip\_constants.py  common\sub\_region\_descriptor.py  common\sub\_region\_image.py  common\tools\_path.py  common\utilities.py | N/A |
| scripts | scripts\Examples\oob\_manageability.json  scripts\Examples\pse\_fw.json  scripts\Examples\tsn\_config.json  scripts\Examples\tsn\_ip\_config.json  scripts\Examples\tsn\_mac\_address.json  scripts\\_\_init\_\_.py  scripts\siip\_sign.py  scripts\siip\_stitch.py  scripts\subregion\_capsule.py | 0.7.2 |
| thirdparty | thirdparty\Bin\\*.\*  thirdparty\edk2\_capsule\_tool\\*.\* | N/A |
| Readme Files | LICENSE  README.md  README.docx  USER\_MANUAL.html | N/A |
| Releasenote | Releasenotes.docx | 0.7.2 |

# Hardware and Software Compatibility

Elkhart Lake platform

## BIOS/Firmware Version

* TBD

## Supported Operating Systems

* Window 10
* Linux