SIIP Scripts for Elkhart Lake Platform

Releasenote

Date: June 2019

Revision: 0.2.0

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 5](#_Toc9645521)

[1.1 Purpose 5](#_Toc9645522)

[1.2 Audience 5](#_Toc9645523)

[1.3 Acronyms 5](#_Toc9645524)

[2.0 New in This Release 6](#_Toc9645525)

[2.1 New Features 6](#_Toc9645526)

[2.2 Changes to Existing Features 6](#_Toc9645527)

[2.3 Unsupported or Discontinued Features 6](#_Toc9645528)

[3.0 Fixed Issues 6](#_Toc9645529)

[3.1 SIIP Stitch Script 6](#_Toc9645530)

[4.0 Known Issues 6](#_Toc9645531)

[5.0 Related Documentation 7](#_Toc9645532)

[6.0 Where to Find the Release 7](#_Toc9645533)

[7.0 Release Content 7](#_Toc9645534)

[7.1 Component Revision Numbers 7](#_Toc9645535)

[8.0 Hardware and Software Compatibility 9](#_Toc9645536)

[8.1 BIOS/Firmware Version 9](#_Toc9645537)

[8.2 Supported Operating Systems 9](#_Toc9645538)

Tables

[Table 1 Acronyms Used in Document 5](#_Toc9645497)

[Table 2 SIIP Scripts Component Revision Numbers 7](#_Toc9645498)

[Table 3 SIIP Stitch Script Component Revision Numbers 8](#_Toc9645499)

[Table 4 SIIP Sign Script Component Revision Numbers 8](#_Toc9645500)

[Table 5 Sub-Region Capsule Script Component Revision Numbers 8](#_Toc9645501)

[Table 6 SIIP Scripts Support Component Revision Numbers 8](#_Toc9645502)

Revision History

| Date | Revision | Description |
| --- | --- | --- |
| June 21, 2019 | 0.2.0 | Engineering Drop Release corresponding to SIIP Scripts version 0.2.0 with the following changes:   1. Overall:    1. Add a top level README as user guide document 2. Sub-Region Capsule:    1. Add Print output message    2. Fixed STDIN input to return bytes array    3. Fixed #299938 STDIN input to return bytes array    4. Fixed #299937 and #299569 Typo in readme file    5. Removed unused files and tools    6. Removed the 2 from IntelOob2Config    7. Updated README.md consistent with the co 3. SIIP Stitch:    1. Updated check valid IP names from a list    2. Removed GUID tool Rsa2048Sah256Sign    3. Removed debug code    4. Fixed #299330 Stitch failed with error "Error using FMMT.exe" when input file in half path    5. Fixed #299322 Stitch failed with error "Error base\_tool is not located: GenSec" when manually set EDK\_TOOLS\_BIN path    6. Fixed #300930 SIIPStitch should return a error when it does not find the firmware volume that match the requirement file to replace.    7. Fixed #300551 Stitch tool hang without error message prompt out when input empty bios    8. Fixed #300553 Stich tool hang without error message prompt out when input random gen binary file as BIOS    9. Fixed #300554 Stitch tool successfully stitch empty OseFw without error    10. Fixed #299943 Wrong Command to check OpenSSL is located in README file    11. Fixed #299945 Wrong Path for siipSupport folder in README file 4. 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

* None in this release

## Changes to Existing Features

* None in this release

## Unsupported or Discontinued Features

* None in this release.

# Fixed Issues

## SIIP Stitch Script

* Fixed #299330 Stitch failed with error "Error using FMMT.exe" when input file in half path
* Fixed #299322 Stitch failed with error "Error base\_tool is not located: GenSec" when manually set EDK\_TOOLS\_BIN path
* Fixed #300930 SIIPStitch should return a error when it does not find the firmware volume that match the requirement file to replace.
* Fixed #300551 Stitch tool hang without error message prompt out when input empty bios
* Fixed #300553 Stich tool hang without error message prompt out when input random gen binary file as BIOS
* Fixed #300554 Stitch tool successfully stitch empty OseFw without error
* Fixed #299943 Wrong Command to check OpenSSL is located in README file
* Fixed #299945 Wrong Path for siipSupport folder in README file

## SIIP Sign Script

* Fixed #299515 Sign and verify function not able to completed successfully if input files path consists of semicolon

## Sub-Region Capsule Script

* Fixed #299938 STDIN input to return bytes array
* Fixed #299937 and #299569 Typo in readme file

# 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 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 | N/A |
| Test Data Files | test\_data\BIOS.BIN  test\_data\OseFw.bin  test\_data\privkey.pem  test\_data\TestCert.pem  test\_data\TestRoot.pub.pem  test\_data\TestSub.pub.pem  test\_data\TsnMacAddressDescExample.json | N/A |
| Readme Files | README.md.html  README.md | N/A |
| Releasenote | Releasenotes.docx | 0.2.0 |

Table SIIP Stitch Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Stitch Script Files | siipStitch\README.md  siipStitch\SIIPStitch.py | 0.5.3 |

Table SIIP Sign Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| SIIP Sign Script Files | siipSign\README.md  siipSign\SIIPSign.py | 0.3.0 |

Table Sub-Region Capsule Script Component Revision Numbers

| Subproject (Component) | Location | Revision |
| --- | --- | --- |
| Sub-Region Capsule Script Files | SubRegionCapsule\\_\_init\_\_.py  SubRegionCapsule\GenerateCapsule.py  SubRegionCapsule\GenerateSubRegionCapsule.py  SubRegionCapsule\README.md  SubRegionCapsule\SubRegionDescriptor.py  SubRegionCapsule\SubRegionImage.py | 0.2.0 |
| Common Tools and Files | SubRegionCapsule\Common  SubRegionCapsule\CommonDataClass  SubRegionCapsule\Examples | N/A |

Table 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\StripSignature.py | 0.2.0 |

# Hardware and Software Compatibility

Elkhart Lake platform

## BIOS/Firmware Version

* TBD

## Supported Operating Systems

* Window 10