

**Intel PSG**  
**SM Encryption**

**Test Plan**

**Version Draft**

**Yan See, Lee**

Table of Contents

[1 Overview 3](#_Toc1523722975)

[1.1 Highlight Changes 4](#_Toc1667233310)

[2 Scope and Objective 6](#_Toc1225171727)

[3 Test Requirements 9](#_Toc678770136)

[3.1. Software Requirements 9](#_Toc1880126612)

[3.2. Hardware Requirements 9](#_Toc931700576)

[3.3. Setup Requirements 9](#_Toc507179687)

[3.4. SM Encryption Landing Zone requirements 9](#_Toc1746144566)

[4 Test Strategy 11](#_Toc1091521670)

[5 Test plan documentation 11](#_Toc171692637)

[5.1. Test Coverage Overview 11](#_Toc268323101)

[Existing Test Coverage 11](#_Toc594600948)

[SDM1.5 Test Coverage 11](#_Toc1998380210)

[5.2. Positive Test 11](#_Toc1852709679)

[5.4 Recovery Test 11](#_Toc2028326348)

[6 Testing gaps 11](#_Toc694323921)

[7 Resources 11](#_Toc1861043294)

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Author** | **Summary of Changes** |
| Draft 0.1 | Sep 13, 2022 | Yan See, Lee | Initial draft version for review containing the test coverage for encryption on SM devices. |
| Draft 0.6 | Nov 17, 2022 | Yan See, Lee | * Update as per SDM1\_5\_Security\_Spec v0.6 * Added 3 new tests for OCS key |
| Draft 0.68 | Mar, 2023 | Yan See, Lee | * Added RSU test * Update as per SDM1\_5\_Security\_Spec v8.6a * Added AES ccert cancellation test |
| Draft 0.7 | May, 2023 | Yan See, Lee | * Reviewed within Team in SM Security Test Discussion Meeting Reviewed with Andy * Modified aes\_keyslot\_corruption to use eng loader flow and added one more subtest to corrupt both prog start and prog end. * Reviewed in Security VT Meeting |
| Draft 0.8 | May 30, 2023 | Yan See, Lee | * Update the flow of aes\_keyslot\_corruption to do corruption at the beginning of test |
| Draft 0.8 | August 16, 2023 | Yan See, Lee | * Update negative\_aes\_cancellation as per expectation of aes non-cancellable ccert, it should allow reprogram of same aes key after the aes key is cancelled. * Added the requirement needed for test mode, especially BBRAM. Need erase BBRAM before pubkey program and reload provision * Update Figure 22 as UDS test mode now supports 6 instead of 4 prefix value. |

# Overview

This document describes the test plan for Security – encryption based on system-level view with reference to the following documents:

1. [SDM1\_5\_Security\_Spec](https://swarm61.devtools.intel.com:6161/files/depot/docs/pgm/nadder/nadder_programmer_support_fd.docx)
2. [Mailbox\_command\_and\_response.docx](https://swarm61.devtools.intel.com:6161/files/depot/docs/firmware/mas/mailbox_command_and_response.docx)
3. [Provision FW Spec.docx](https://swarm61.devtools.intel.com:6161/files/depot/docs/firmware/mas/Provision%20FW%20Spec.docx)
4. [Glen Pass Project FW Spec.docx](https://swarm61.devtools.intel.com:6161/files/depot/docs/firmware/mas/Glen%20Pass%20Project%20FW%20Spec.docx)
5. [nadder\_iid\_puf\_and\_bbram\_key\_scrambling\_pgm\_fd.docx](https://swarm61.devtools.intel.com:6161/files/depot/docs/pgm/nadder/nadder_iid_puf_and_bbram_key_scrambling_pgm_fd.docx)

Bitstream Encryption feature was first introduced in 19.1+ in Stratix 10 and 19.4+ in Agilex but was first released in FM6 RevB0 SFE board to the public in 20.4.1.

In 21.1, firmware is being rearchitected and the method for programming the AES Root Key to decrypt the bitstream has changed to CCERT based method. In 21.2, the metal key scrambling for BBRAM is supported and BBRAM clear key is obsoleted. User AES Root Key CCERT is generated using programmer tool and programmed into BBRAM key storage via using the SDM command CERTIFICATE[0xB].

Moving forward for SDM1.5 devices such as Agilex Edge, encryption feature no longer utilize DIMK algorithm to wrap the encryption key. It is replaced by fuse wrapping base repeat-N key deriving from EFUSE UDS value. The other major changes are the increase of the AES key slot in EFUSE from 1 to 6. AES key programming is expected to fail when all the 6 IFP key slot is blown. Virtual EFUSE flow is expected to behave the same as physical EFUSE flow, where the previous AES key programmed will be cancel until there is no more available slot. In virtual flow, a power cycle will be able to reset the AES key slot and allow AES key programming again.

## 1.1 Highlight Changes

**Before 21.2:**

BBRAM Key storage only supports plaintext. In future releases, firmware will support different key wrapping selection for BBRAM. The user AES root key can also be programmed into a flash chip called PUF AES Key. Highlight fields are the possible combination for Key Wrapping and Key Storage.

Table 1‑2 Valid key wrapping-storage selection before 21.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Key Destination** | **Wrapping Key Selection** | | | |
| No-Wrap | Internal | User IID PUF | Intel PUF (FM) |
| BBRAM | Yes | No | No | Future |
| EFUSE | No | Yes | Future | Future |
| OFF-CHIP | N/A | N/A | Yes | Future |

**After 21.2:**

BBRAM clear key AES key programming is no longer supported in 21.2. Decryption flow with clear key in BBRAM will still be supported although BBRAM clear key wrapping is obsoleted. Highlight fields are the possible combination for BBRAM Key Wrapping.

Table 1‑3 Valid key wrapping-storage selection from 21.2 onwards

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Key Destination** | **Wrapping Key Selection** | | | |
| No-Wrap | Internal | User IID PUF | Intel PUF |
| BBRAM | No | Yes | Yes | Future |
| EFUSE | No | Yes | Future | Future |
| OFF-CHIP | N/A | N/A | Yes | Future |

**In SDM1.5:**

Support Intel PUF as one of the wrapping key selections. For internal wrapping selection, DIMK is no longer used to derive wrapping key and is replaced by FUSE wrapping base N. UDS Intel PUF can only be selected when UDS\_IntelPUF fuse is blown. However, User IID PUF and UDS IID PUF will be disable in production SM. It is encouraged to use UDS Intel PUF which has the highest security level among the key wrapping options.

Table 1‑4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Key Destination** |  | | | | |
| No-Wrap | Internal | User IID PUF | UDS IID PUF | UDS Intel PUF |
| BBRAM | No | Yes | Yes | Yes | Yes |
| EFUSE | No | Yes | No | No | Yes |
| OFF-CHIP | N/A | Yes | Yes | Yes | Yes |

# Scope and Objective

This test plan will focus on the testing of AES key programming and target JTAG configuration mode, unless stated otherwise.

The overall test plan for SM can be found here:

* [SDM1.5\_TestPlan](https://intel.sharepoint.com/:w:/s/psgswval/ETKD1rcQQs5Ambw3BxgK9JcBgOx9vL4ns16ifWYx0JsTEA?e=8chK4I&CID=E975B5AD-B2F9-4405-B31A-C2FF5E333DBC&wdLOR=c58D1A781-BE17-4C10-B182-DE4AC189D334)

The basic configurations, positive and negative legacy tests for BBRAM key can be found here:

* [19.1 FWVAL\_TestPlan ND\_FM Bitstream Encryption Updating\_as\_per\_14013191759.docx](https://intel.sharepoint.com/sites/psgswval/Shared%20Documents/Val%20Documents/Test%20Plan/19.1/19.1%20FWVAL_TestPlan%20ND_FM%20Bitstream%20Encryption%20Updating_as_per_14013191759%20rev0.5.docx)
* [21.1 FWVAL\_TestPlan ND\_FM AES CCERT Encryption](https://intel.sharepoint.com/sites/psgswval/_layouts/15/Doc.aspx?sourcedoc=%7BB4FDD930-F5C3-4DB9-986C-3F1BA35E802F%7D&file=21.1%20FWVAL_TestPlan%20ND_FM%20AES%20CCERT%20Encryption%20rev0.1.docx&action=default&mobileredirect=true&cid=57980db1-5399-4f8d-bfe6-d73b12b04741&CID=9798EDBB-6E62-4D6E-8F76-6FD8E6FA92A1&wdLOR=c82729FE6-20F0-4A4C-953F-2902C2EC4FF4)

This document discusses the test scenarios and procedures that are broadly classified into two different categories to validate the functionality and capability of the firmware with regards to AES root key programming SDM1.5 features. Below is the category of testing.

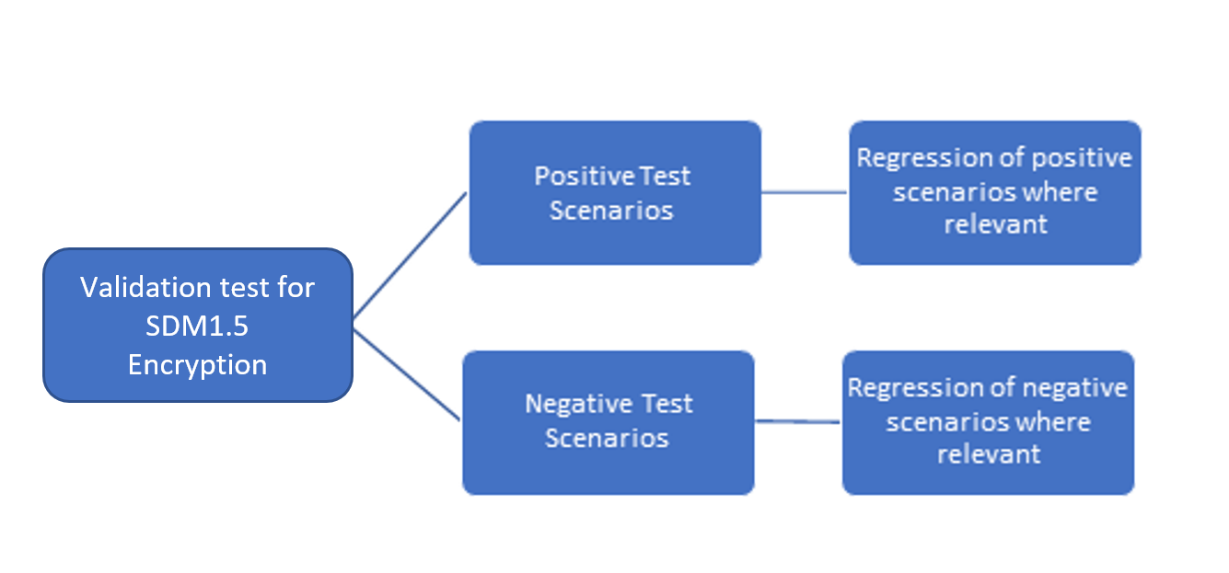


Figure 2‑1 Test Validation Category and coverage overview

1. Positive Tests
   * Test happy scenarios that are intended for usual usage i.e. programming AES Root Key CCERT with features such as AES test mode and AES cancellation, it shall pass in any configuration type including JTAG and QSPI. The test plan focuses on AES key rolling for EFUSE and OFFCHIP storage, to ensure the functionality of IFP key slot.
2. Negative Tests
   * Test corner cases/scenarios/security/areas within firmware that would need enhancement with invalid input, trying to perform configuration i.e. AES key programming shall fail when more than 6 IFP key slots are occupied.

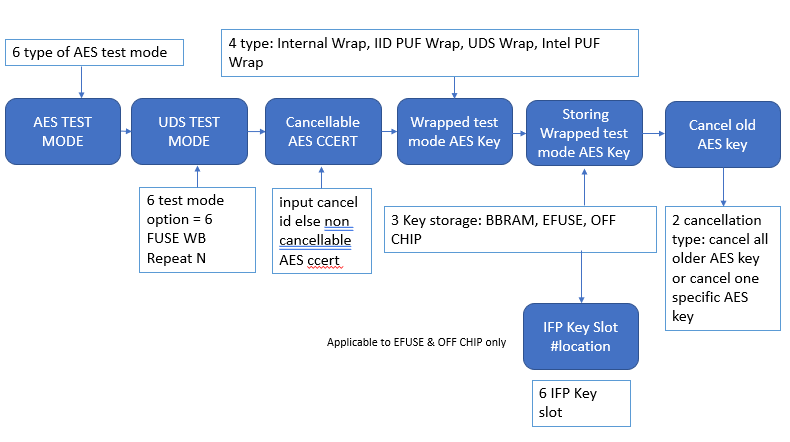


Figure 22 Overview of the possible combination and flow of all AES key options

The above diagram shows all the AES key options involved in SDM1.5 encryption flow. First, when user generate an AES key they can specify if they would like to use test mode for AES key. There is 6 fixed value of test mode to choose from. By default, the AES key generated is non test mode.

User can select 6 types of UDS test mode through the SDM command EFUSE\_WRITE\_DISABLE to pick fixed value of UDS variable to use. UDS test mode 0 means real UDS value will be use while 1-6 is a set of prefixed fake UDS values. This will later influence the generation of FUSE Wrap Base Repeat N value. Note that non test mode flow shall only be used with SFE device, it is expected to fail on non-SFE device as no UDS value is written on the bank 9 efuse.

The additional step required by AES test mode flow is reloading the provision firmware after sending efuse write disable command to trigger an ARB which prompt ARB to produce “Fuse WB Repeat N” or “WB Repeat n” using Test Mode UDS value. For test mode with BBRAM, BBRAM need to be erase before programming the public key. Note that non AES test mode encryption key programming is expected to fail in UDS test mode environment, so AES test mode encryption key should be use in this case.

During AES key programming, user can select the AES ccert cancel id, key wrapping and key storage options. A warning message will display to remind user that the AES ccert will be non-cancellable if no cancel id is input. The cancellation here only applies to the certificate, in other words the AES key will always be cancellable regardless of this input. AES key programmed can be cancel by sending CERTIFICATE command (0x0B) with Cancel Old User AES Key(s) Certificate. IFP Key Slot allocated based on first come first serve basis, means the first AES/OCS key programmed will be store in keyslot#0. For the available combination of key wrapping and key storage, refer to Section 1 table 14.