|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Revision # | Date of Issue | Creator or Reviser | Report type (draft vs. final) | Description of Changes |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |



FIPS Guide Tool User Manual

FIPS 140-2 Revalidation Change Summary

Hardware Version: #

Security Level 3+EFP

Report #

Month Day, Year

Copyright 2017 Penumbra Security, Inc.

This document is proprietary to Penumbra Security, Inc. This document is distributed to CMVP with the understanding that it will not be disclosed or used, in whole or part, for any other purpose than for what it is intended, without the prior written consent of Penumbra Security, Inc.

# Executive Summary

Penumbra Security, Inc. (Penumbra) has reviewed the complete list of assertions for the Customer Name Module Name (*Part Numbers: Part A: #, and Part B: #; Hardware Versions: Hardware A#, and Hardware B: #; Firmware Versions: Firmware A: #, and Firmware B: #*) and found that the module fully complies with the requirements of FIPS 140-2.

The central purpose of the module is X. The module uses a number of strong identity based authentication mechanisms to provide authentication, integrity, and, when necessary, non-repudiation.

The Customer has [done X to update the module]. The updates affects less than 30% of the module’s security relevant features. The module’s hardware and underlying cryptographic functionality remain unchanged [or other reasons the effects are less than 30%].

Reopened and changed ASs and TEs are shown in Table 1, below. Modified TEs are shown in red, while those in black have passed revalidation with no change.

Table 1 – FIPS 140-2 Applicable Modification Summary

| **Section** | **Security Requirement** | **Modifications** | **Affected TEs** (TEs in red have been modified, TEs in black have passed revalidation with no change) |
| --- | --- | --- | --- |
| 1 | Cryptographic Module Specification | Summarize Modifications  (Refer to Section 1 for further details) | TE.01.03.01  *TE.01.03.02 TE.01.06.03  TE.01.08.01  TE.01.12.02* |
| 2 | Cryptographic Module Ports and Interfaces | Summarize Modifications (Refer to Section 2 for further details) | *TE.02.01.01*  *TE.02.05.01*  TE.02.06.02  TE.02.06.04  TE.02.13.03  TE.02.14.02 (N/A)  TE.02.16.02 (N/A)  TE.02.17.02 (N/A) |
| 3 | Roles, Services and Authentication | Summarize Modifications  (Refer to Section 3 for further details) | *TE.03.02.02 (N/A)*  *TE.03.02.03 (N/A)*  *TE.03.03.01*  TE.03.03.02  TE.03.03.03  TE.03.12.03  TE.03.13.02  TE.03.14.02  TE.03.15.02  TE.03.17.02  TE.03.17.03  *TE.03.19.01*  TE.03.19.02  TE.03.19.03 (N/A)  TE.03.21.02  TE.03.22.02  TE.03.23.02  *TE.03.25.01*  *TE.03.26.01* |
| 4 | Finite State Model | Summarize Modifications  (Refer to Section 4 for further details) | TE.04.03.01  TE.04.05.08 |
| 5 | Physical Security | No Change/ Summarize Modifications | None/as required |
| 6 | Operational Environment | No Change/Summarize Modifications | None TE.06.05.01 TE.06.06.01 TE.06.07.01 TE.06.08.02 TE.06.11.02 TE.06.11.03 TE.06.12.02 TE.06.12.03 TE.06.13.02 TE.06.13.03 TE.06.14.02 TE.06.14.03 TE.06.15.02 TE.06.16.02 TE.06.17.02 TE.06.22.02 TE.06.22.03 TE.06.24.02 TE.06.24.03 TE.06.22.02 |
| 7 | Cryptographic Key Management | Summarize Modifications  (Refer to Section 7 for further details) | TE.07.01.02  TE.07.02.02  *TE.07.03.01*  TE.07.15.02 (N/A)  TE.07.15.03  TE.07.15.04  TE.07.25.02  TE.07.27.02 (N/A)  TE.07.28.02 (N/A)  TE.07.29.02  *TE.07.31.02 (N/A)*  *TE.07.31.03 (N/A)*  TE.07.31.04 (N/A)  TE.07.39.02  TE.07.41.02 |
| 8 | EMI/EMC | No Change/ Summarize Modifications | None/as required |
| 9 | Self-Tests | No Change/ Summarize Modifications  (Refer to Section 9 for further details) | TE.09.04.03 TE.09.05.03 TE.09.09.02 TE.09.10.02 TE.09.12.02 TE.09.22.07 TE.09.35.05 TE.09.40.03 (N/A) TE.09.40.04 (N/A) TE.09.45.03 TE.09.46.03 |
| 10 | Design Assurance | No Change/ Summarize Modifications  (Refer to Section 10 for further details) | TE.10.03.02  *TE.10.04.01* |
| 11 | Mitigation of Other Attacks | No Change/Summarize Modifications | None/as required |

## Area 1 – Cryptographic Module Specification

Specify any updates

*Hardware Versions:*

* *Hardware A (No Change/Updated)*
* *Hardware B (No Change/Updated)*

*Firmware Versions:*

* *Firmware A (No Change/Updated)*
* *Firmware B (No Change/Updated)*

*Software Versions:*

* *Software A (No Change/Updated)*
* *Software B (No Change/Updated)*

## Area 2 – Cryptographic Module Ports and Interfaces

Penumbra verified that the cryptographic module conforms to the requirements of FIPS 140-2 Level 3 *Area 2 – Cryptographic Module Ports and Interfaces*.

A maintenance interface is not supported. Vendor documentation and conformance testing demonstrated that logical separation of all interfaces is achieved. It was also demonstrated that the data output interface is inhibited during zeroization, key generation, self-tests, and error states.

Specify any changes

## Area 3 – Roles, Services, and Authentication

Specify any changes to roles.

#### Roles, Services, and Authentication for the Updated Module

1. Role A (Authenticated Services)

Role A is responsible for X. This role’s primary functions are Y [e.g. to load keys into the module and to authorize the generation and use of keys]. Authentication is via the Z.

The services allocated to this role are as follows:

* Service A
* Service B

1. Role B (Authenticated Services)

Role B is responsible for X. This role’s primary functions are Y [e.g. to load keys into the module and to authorize the generation and use of keys]. Authentication is via the Z.

The services allocated to this role are as follows:

* Service A
* Service B

1. Unauthenticated services:

The services of the module that can be performed without an authenticated role are as follows:

* Service C
* Service D

#### Roles, Services, and Authentication for the Previous Module Validation

Specify any changes to roles.

1. Role A (Authenticated Services)

Role A is responsible for X. This role’s primary functions are Y [e.g. to load keys into the module and to authorize the generation and use of keys]. Authentication is via the Z.

The services allocated to this role are as follows:

* Service A
* Service B

1. Role B (Authenticated Services)

Role B is responsible for X. This role’s primary functions are Y [e.g. to load keys into the module and to authorize the generation and use of keys]. Authentication is via the Z.

The services allocated to this role are as follows:

* Service A
* Service B

1. Unauthenticated services:

The services of the module that can be performed without an authenticated role are as follows:

* Service C
* Service D

## Area 4 – Finite State Model (FSM)

Penumbra verified that the cryptographic module conforms to the requirements of FIPS 140-2 Level 3 *Area 4 – Finite State Model (FSM).*

The FSM defines each of the module’s finite states. The new FSM was examined and tested against the module’s source code and other supporting documentation. In addition, operational testing verified that the module’s behavior is consistent with the FSM, state descriptions, and state transitions.

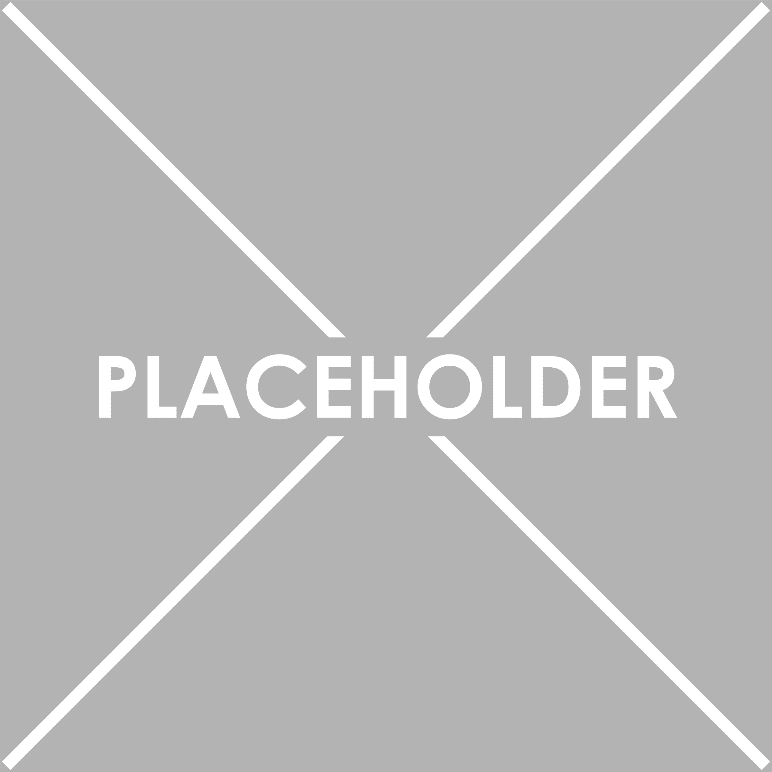


Figure 1 - FSM

## Area 5 – Physical Security

No changes/specify updates

## Area 6 – Operational Environment

No changes/specify updates

The FIPS 140-2 Area 6 (Operational Environment) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

## Area 7 – Cryptographic Key Management

#### Cryptographic Keys and CSPs

##### Cryptographic Keys and CSPs Supported by the Updated Module

Private/Secret Keys:

* Key A
* Key B

Public Keys:

* Key C
* Key D

##### Cryptographic Keys and CSPs Supported by the Previous Module Validation

Private/Secret Keys:

* Key A
* Key B

Public Keys

* Key C
* Key D

### Algorithms

List any changes in Approved, Allowed, or Non-Approved Algorithms.

## Area 8 – EMI/EMC

No changes/specify updates

## Area 9 – Self-Tests

No changes/specify updates

#### Self-Tests for the Updated Module

Power-up/Conditional/By-Pass/Critical Functions

#### Self-Tests for the Previous Module validation

Power-up/Conditional/By-Pass/Critical Functions

## Area 10 – Design Assurance

No changes/specify updates

## Area 11 – Mitigation of Other Attacks

No changes/specify updates