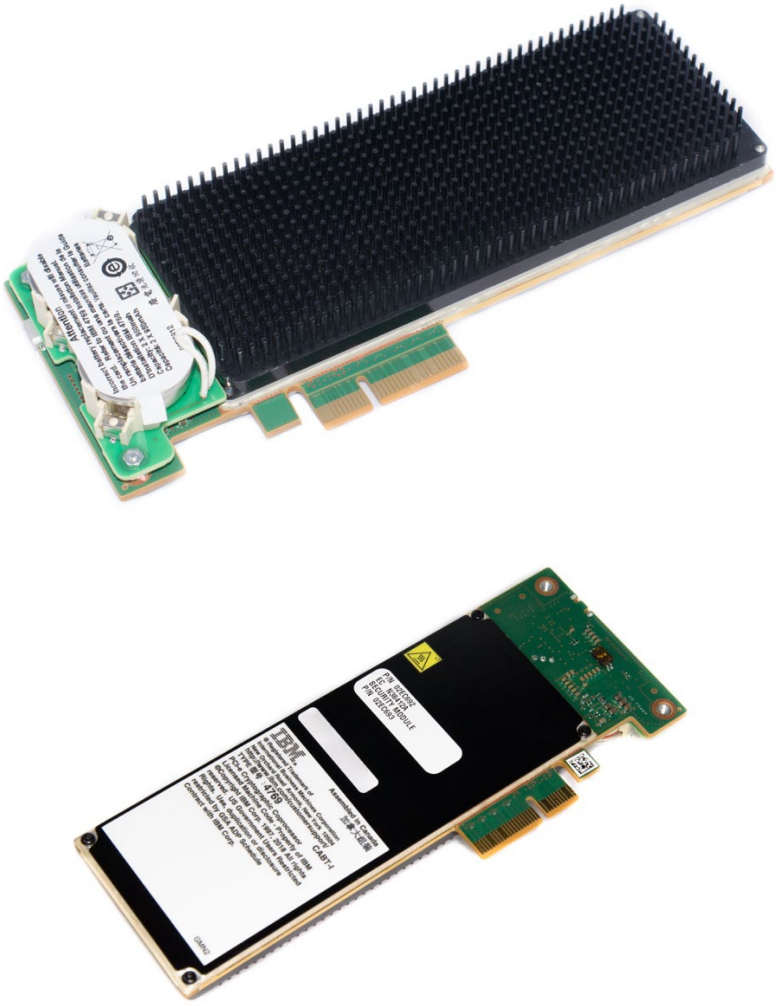
IBM Corporation
IBM 4769-001 Cryptographic Coprocessor Security Module
Non-Proprietary Security Policy



IBM Advanced Cryptographic Hardware Development
IBM Research - Zurich
IBM Development – Lexington, Poughkeepsie, Boeblingen

Table of Contents

1 Document History 5

2 Introduction 6

2.1 Hardware and Physical Cryptographic Boundary 10
2.2 Firmware and Logical Cryptographic Boundary 11
2.3 Mode of Operation 12

3 Cryptographic Functionality 13

3.1 Critical Security Parameters (CSP) 14
3.2 Public Keys 15

4 Roles, Authentication and Services 15

4.1 Assumption of Roles 15
4.2 Authentication Methods 16
4.3 Services 16
4.4 Services cross-reference table 18

5 Self-Tests 19

6 Physical Security Policy 21

7 Operational Environment 23

8 Mitigation of Other Attacks Policy 23

9 Security Rules and Guidance 23

10 References and Definitions 24

List of Tables

Table 1 – Cryptographic Module Configurations 6
Table 2 – Security Level of Security Requirements 8
Table 3 – Physical Ports and Interfaces 11
Table 4 – Approved Cryptographic Functions 13
Table 5 – Critical Security Parameters (CSPs) 14
Table 6 - Public Keys 15
Table 7 - Role Description 15
Table 8 - Authentication Method 16
Table 9 – Authenticated Services 16
Table 10 – Unauthenticated Services 17
Table 11 – Services cross-reference 18
Table 12 – Power-on Self-tests 20
Table 13 – Conditional Self-Tests 21
Table 14 – Physical Security Tamper Types and Recommended Actions 22
Table 15 – References 24
Table 16 – Acronyms and Definitions 24

List of Figures

Figure 1 – 4769-001 Module 10
Figure 2 – 4769-001 Block Diagram 12
Figure 3 – Module Software Architecture – Example Usage 12

1 Document History

Version	Date	Contents
1.00	12/30/2020	IBM Review complete
1.10	1/20/2021	Updates in response to CMVP Comments
1.11	6/16/2021	Updates in response to CMVP Comments
1.12	12/4/2021	Corrected the Module P/N and Version for Modules 1 and 2 in Table 1; added new P/Ns and versions in Table 1 (Modules #3, 4, 5, and 6)

2 Introduction

This document defines the Security Policy for the IBM 4769-001 Cryptographic Coprocessor Security Module, hereafter denoted the Module. This Module with Miniboot software resident in ROM and code flash, provides security officers, users, and the security policy governing access to those services. This policy applies to multiple members of the 4769 family of products.

A multi-chip embedded product, the Module is a cryptographic coprocessor, a general-purpose computing environment with accelerator engines, executing software and retaining secrets, despite foreseeable physical or logical attacks. End users can base high-assurance applications, such as digital signature generation or financial transaction processing, on this platform.

Firmware identifiers refer to unambiguously identifiable leading characters of Segment 1 (firmware) hash, a unique value describing firmware configuration. The actual value, a cryptographic hash of the segment image, is returned by configuration queries.

Table 1 – Cryptographic Module Configurations

	Module	Module P/N and Version	FW Version
1	4769-001	PN 02WN654-N37880 POST0 v9662 MB0 v6096 (Standard Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D 5A3B421DD38E4094547C3C3B229CC521 7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6
2	4769-001	PN 02WN652-N37880 POST0 v9662 MB0 v6096 (Low Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D

			5A3B421DD38E4094547C3C3B229CC521 7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6
3	4769-001	PN 03FM956-H07053 POST0 v8657 MB0 v6381 (Standard Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D 5A3B421DD38E4094547C3C3B229CC521 7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6
4	4769-001	PN 03FM953-H07053 POST0 v8657 MB0 v6381 (Low Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D 5A3B421DD38E4094547C3C3B229CC521 7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6
5	4769-001	PN 03JJ168-N38177 POST0 v8657 MB0 v6381 (Standard Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D 5A3B421DD38E4094547C3C3B229CC521

			7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6
6	4769-001	PN 03JJ165-N38177 POST0 v8657 MB0 v6381 (Low Power)	Segment 1 Information Name: 7.0.46z P1591 M1591 P5625 F0701 Hash data: 2B5F92F34C8FF2CDC93B794AE6F4EA44 B4C5112A5FA92156F8E67BC1F1B4F557 E9BC92F4CEE9C896C1F560D954F87354 E64F60BC28535765127CBE8985E07C06 Name: 7.0.74z P3795 M6356 P0630 F0701 Hash data: 5D4F8741EDD2403F61C33D3C190B714D 5A3B421DD38E4094547C3C3B229CC521 7F94324B4840AB98EAE7644AD87E8932 217CC15CBD045A83F33F8D48DC6E7AF6

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Level 4. End users can base high-assurance applications, such as digital signature generation or financial transaction processing, on this platform.

Note that this policy covers services of trusted, lower layers of internal firmware (Layers 0 and 1, and a stub of Layer 2). Higher layers, OS and applications (2 and 3) are not included in the current validation. Layers 2 and 3 must not be run; otherwise, it will no longer be running as a validated FIPS module. The installation of such components is out of scope and would require a separate validation to maintain FIPS 140-2 compliance. However, the security foundations do not require a cooperative or trustworthy OS/application for consistent and secure Miniboot operation.

The cryptographic boundary is the enclosure of the self-contained Module. The Module is labeled unambiguously with model and part numbers of the host PCIe card, and that of the Module itself. The correspondence between end-user product, Module, and security policy is self-explanatory. The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	4
Cryptographic Module Ports and Interfaces	4
Roles, Services, and Authentication	4
Finite State Model	4

Security Requirement	Security Level
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	4
EMI/EMC	4
Self-Tests	4
Design Assurance	4
Mitigation of Other Attacks	N/A

2.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1 for the 4769-001; the red outline depicts the physical cryptographic boundary. Figure 1 displays the physical attributes of the 4769-001 PCIe Module. The 4769-001 Module is comprised of two (2) electrical component cards with one used as a battery holder and the second one being the main functional component of the Module and part of the secure boundary. The Module relies on a host system that supplies a PCIe interface for input/output communication.

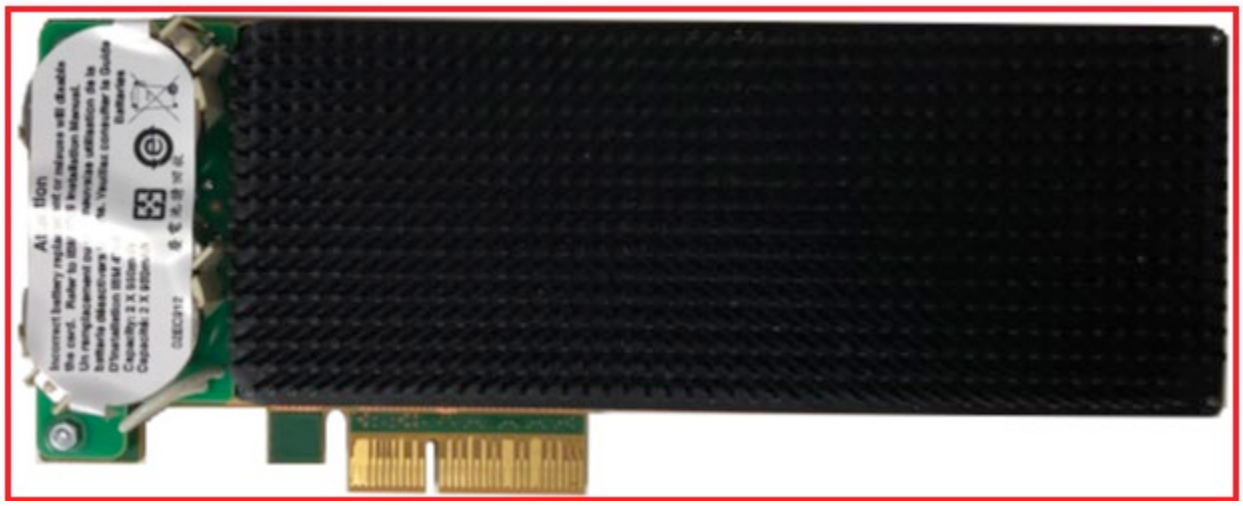


Figure 1 – 4769-001 Module

Table 3 – Physical Ports and Interfaces

Physical Port	Description	Logical Interface Type
PCI Express signals:	**4-lane (x4) external**	
PCIe data/addresses	Bidirectional	Data input Data output
PCIe control	bidirectional; PCIe v2.0 compliant “single function” device	Control input Status output
Auxiliary signals:	**tunneled over shared flexcables**	
Serial ports	only used as status output by current IBM firmware	Status out
USB port	bidirectional; may tunnel other signals (such as Ethernet-over-USB) not used by current IBM firmware	N/A (with current firmware)
PCIe power	3.3 V	Power
Battery power	variable, nominal 3.0 V	Power
External warning	host connectivity test, latching removal from host bus monitored within Module	Control input (from sensor) Status output (to host)

2.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment with the secure enclosure outlined in red.

Note: POST2 is also in scope because it is part of the signed Segment1 image (and is included as one of the named components in the Segment1 image).

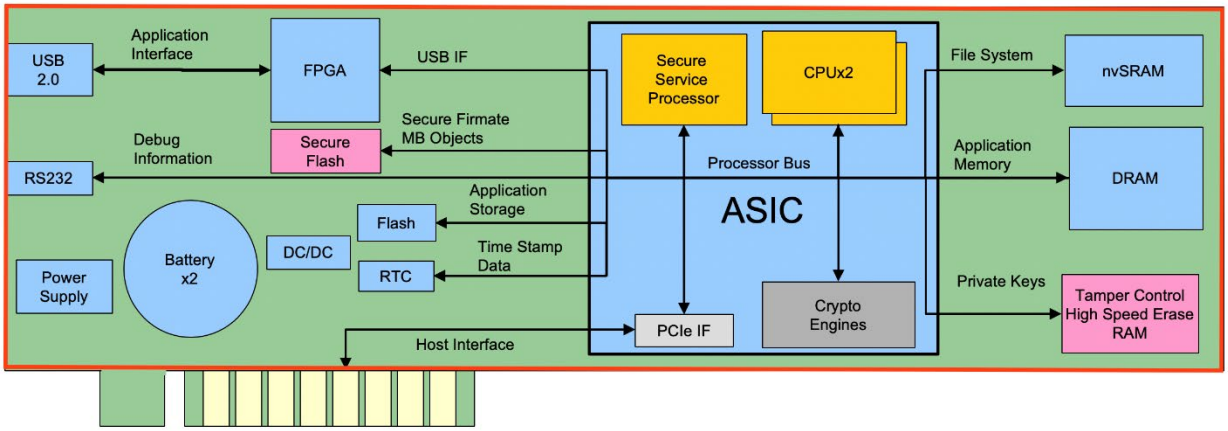


Figure 2 – 4769-001 Block Diagram

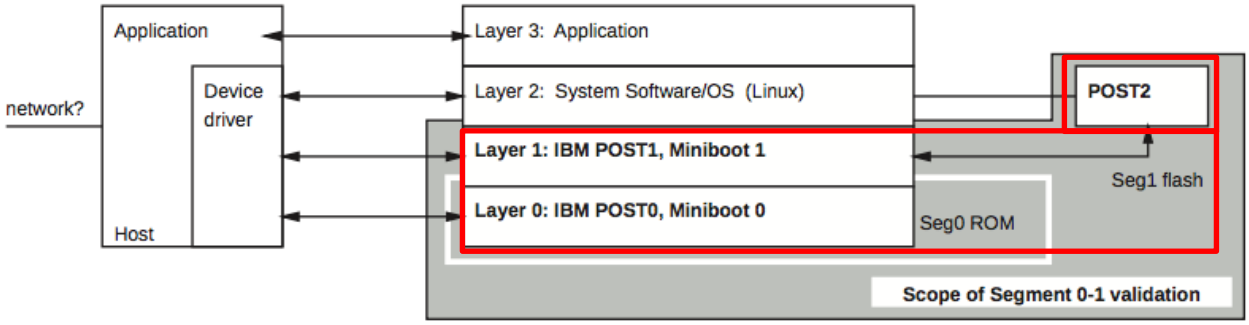


Figure 3 – Module Software Architecture – Example Usage

2.3 Mode of Operation

The Module uses only approved algorithms and modes of operation. If the Module is functional, and the validated firmware variant is loaded to a validated hardware platform(s), the Module is in FIPS mode for Segments 0 and 1. The running of Seg2 and Seg3 are outside this FIPS validation. However, the loading of Seg2 and Seg3 are inside this FIPS validation. The "Signed Health Query" (Miniboot 1), in addition to segment ownership and revision number, returns code layers' contents' SHA-512 hashes. Please see the Module P/N and Version and the FW Version Segment 1 hash being validated in Table 1 – Cryptographic Module Configurations.

3 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC Key sizes: 128, 192, and 256 bits **NOTE:** This is tested, but not used.	C1187 Low Power C1188 Standard Power
AES/CMAC	Functions: Generation and Verification Key sizes: 128, 192, and 256 bits **NOTE:** This is tested, but not used.	C1187 Low Power C1188 Standard Power
CVL ECDSA SigGen Component	[FIPS 186-4] Functions: Signature generation Curves/Key sizes: P-521 w/ SHA-512	C1249 Low Power C1250 Standard Power
DRBG	[NIST SP800-90A Rev 1] Hash DRBG based on SHA-512 Cert. C1249 DRBG uses C1247 SHA-512 and Cert. C1250 DRBG uses C1248 SHA-512 The ENT(P) NDRNG is used to seed the HASH_DRBG, which has a security strength of 256-bits.	C1249 Low Power C1250 Standard Power C1247 SHA Low Power C1248 SHA Standard Power
ECDSA	[FIPS 186-4] Functions: Key generation and signature verification Curves/Key sizes: P-521 w/ SHA 512 Per IG D.12, the asymmetric key generation method is: [133] Sections 4 and 5 Asymmetric signature key generation using unmodified DRBG output.	C1249 Low Power C1250 Standard Power
ENT(P)	[NIST SP 800-90B] Hardware generated Approved ENT(P) NDRNG Function: Physical entropy source used as seeds for the Approved DRBG.	N/A

Algorithm	Description	Cert #
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 **NOTE:** This is tested, but not used.	C1187 Low Power C1188 Standard Power
SHS	[FIPS 180-4] [FIPS 202] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-256, SHA-512 **NOTE:** These SHA sizes are tested, but not used: SHA-1, SHA-224, SHA-384, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512	C1187 Low Power C1188 Standard Power
SHS	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-512	C1247 Low Power C1248 Standard Power
Triple-DES	Function: Encryption, Decryption Modes: TECB, TCBC Key sizes: 168 bits **NOTE:** This is tested, but not used.	C1187 Low Power C1188 Standard Power
Triple-DES/CMAC	**NOTE:** This is tested, but not used.	C1187 Low Power C1188 Standard Power

3.1 Critical Security Parameters (CSP)

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 5 – Critical Security Parameters (CSPs)

Key	Description / Usage
Device keypair (DKP1) private key	Keys unique to a specific card, validated by IBM trust chain ending at the IBM Root key. Enables proof externally that card is genuine and untampered. Signs responses to Miniboot queries from host. Signs certificate for next subsequently generated device keypair. (ECC P-521)

NDRBG seed	Entropy input / seed value generated by NDRBG and used to seed the DRBG.
DRBG state	State of the hardware DRBG in the ASIC. State must be saved between uses and restored to the hardware before each use. State includes V and C.

3.2 Public Keys

Public keys are used by the module to authenticate each command request individually. Authentication is based on signature verification. For 0 < N < 4, Miniboot authenticates a command from Officer N by verifying that the public-key signature on the command came from the entity that is Officer N for that card and was acting in that capacity when the signature was produced.

Table 6 - Public Keys

Key	Description / Usage
Officer1 public key	Authenticates commands controlled by CO1, including new Seg1 or Seg2 firmware. (ECC P-521)
Officer2 public key	Authenticates commands controlled by CO2, including new Seg3 firmware. (ECC P-521)
Officer3 public key	Authenticates commands controlled by CO3. (ECC P-521)
Device keypair (DKP1) public key	Authenticates Seg1 responses. (ECC P-521)
IBM Class Root public key	Authenticates certificate for the first Device public key (DKP1 public key) to be generated. (ECC P-521)

4 Roles, Authentication and Services

4.1 Assumption of Roles

The Role descriptions are noted in the Role Description table:

Table 7 - Role Description

Role ID	Role Description	Authentication Type	Authentication Data
CO1	Cryptographic Officer 1 (FIPS 140 User role) - Owns Segment 1 and established by IBM as the base authority	Identity-based	Digital Signature ECC P-521

Role ID	Role Description	Authentication Type	Authentication Data
CO2	Cryptographic Officer 2 (FIPS 140 CO role) - Owns Segment 2 and established by CO1	Identity-based	Digital Signature ECC P-521
CO3	Cryptographic Officer 3 (FIPS 140 CO role) - Owns Segment 3 and established by CO2	Identity-based	Digital Signature ECC P-521

4.2 Authentication Methods

The authentication method and its strength of mechanism are in the Authentication Method table:

Table 8 - Authentication Method

Authentication Method	Strength of Mechanism
Digital Signature ECC P-521	ECC P-521 using SHA-512 is used for the signing and verification of digital signatures. The probability that a random attempt will succeed, or a false acceptance will occur is 1/2^256, which is less than 1/1,000,000. The Module can only perform one (1) digital signature verification per second. The probability of successfully authenticating to the Module within one minute through random attempts is 60/2^256, which is less than 1/100,000.

4.3 Services

All services implemented by the Module are listed in the table(s) below. Each service description also describes all usage of CSPs by the service.

Table 9 – Authenticated Services

Service	Description	CO1	CO2	CO3
Establish Officer 2	Register new Officer 2	X		
Establish Officer 3	Register new Officer 3		X	
Surrender Officer 2	Clear Layer 2 and 3 parameters and persistent data, and officer 2 and officer 3 public keys		X	

Service	Description	CO1	CO2	CO3
Surrender Officer 3	Clear Layer 3 parameters and persistent data and officer 3 public key			X
Ordinary Burn 1	Load Layer 1 firmware and officer 1 public key; optionally clear Layer 2 and/or 3 parameters and persistent data and officer public key, as defined by Segment 2/3 persistent object definitions	X		
Ordinary Burn 2	Use the Officer2 public key; Load (replace) layer 2 firmware; optionally clear Layer 3 parameters, persistent data, and officer public key, as defined by segment 3 persistent object definitions		X	
Emergency Burn 2	Clear Layer 2 and 3 parameters and persistent data and officer 2 and officer 3 public keys; Load layer 2 firmware and officer 2 public key	X		
Ordinary Burn 3	Use the Officer3 public key; Load (replace) layer 3 firmware			X
Emergency Burn 3	Clear Layer 3 parameters and persistent data and officer 3 public key; Load layer 3 firmware and officer 3 public key		X	
Software-induced tamper	A command that renders a card inoperable by evoking the module's tamper response mechanism. Evocation of this service destroys all CSPs residing on the card. Note: this command is not expected to be used during the lifetime of a typical deployment since it requires IBM cooperation to create (instances are unique).	X		

Table 10 – Unauthenticated Services

Service	Description
Cold Boot	Reboots the Module and performs power-on self-tests, triggered by the strobing of a bit in the HRCSR by a host device driver.
Query Status	Read infrastructure status, including layer owners. Reset the Module CPU (MCPU) (OS/application).
Query Status/Noreset	Read module status, including layer owners. Do not reset Module CPU.

Service	Description
Query Signed Health ("Get Health")	Read module status, including owner identities and officer public keys; Reset Module CPU conditionally (only if segment 2 or segment 3 has been updated since the MCPU was last reset [in practice this is only possible for segment 3])
Query Signed Health/Noreset ("Query Firmware")	Read module status, including owner identities and officer public keys. Do not reset Module CPU.
Query Certificate	Returns the entire segment 1 certificate list, one certificate at a time (repeated calls to MB1).
Query Segment 0 Hash	Returns the computed SHA512 hash of segment 0 (MB0 concatenated with POST0).
Algorithm Test (SHA-256 test)	Compute SHA-256 hash of host-supplied data as an interactive communications/infrastructure self-test; Does not access CSPs
Continue to Segment 1	Advance from Segment 0 into Segment 1 if status permits
Continue to Segment 2	Start layer 2 firmware if status permits

4.4 Services Cross-Reference Table

All services implemented by the Module are listed in the table below. Each service is cross-referenced with the Module CSPs, NDRBG seed, and DRBG state.

Cross-reference Key

- G Generates keys
- I Inputs key from outside of the Module
- O Output key
- W Write/Store key
- U Use key
- Z Zeroize

Table 11 – Services Cross-Reference

Service	Device keypair (DKP1) private key	NDRBG seed	DRBG state	Officer1 public key	Officer2 public key	Officer3 public key	Device keypair (DKP1) public key	IBM Class Root public key
Establish Officer 2	U	-	-	U	-	-	-	-

Service	Device keypair (DKP1) private key	NDRBG seed	DRBG state	Officer1 public key	Officer2 public key	Officer3 public key	Device keypair (DKP1) public key	IBM Class Root public key
Establish Officer 3	U	-	-	-	U	-	-	-
Surrender Officer 2	U	-	-	-	UZ	Z	-	-
Surrender Officer 3	U	-	-	-	-	UZ	-	-
Ordinary Burn 1	UGW	-	GUZ	IUW	-	-	GW	U
Ordinary Burn 2	U	-	GUZ	-	U	-	-	-
Emergency Burn 2	U	-	GUZ	U	IWU	-	-	-
Ordinary Burn 3	U	-	GUZ	-	-	U	-	-
Emergency Burn 3	U	-	GUZ	-	U	IWU	-	-
Software-induced tamper	Z	Z	Z	U	-	-	-	-
Cold Boot	-	GUZ	GZ	-	-	-	-	-
Query Status	-	-	-	-	-	-	-	-
Query Status/Noreset	-	-	-	-	-	-	-	-
Query Signed Health (“Get Health”)	U	-	-	O	O	O	-	-
Query Signed Health/Noreset (“Query Firmware”)	U	-	-	O	O	O	-	-
Query Certificate	U	-	GUZ	-	-	-	O	O
Query Segment 0 Hash	-	-	-	-	-	-	-	-
Algorithm Test	-	GUZ	GUZ	-	-	-	-	-
Continue to Segment 1	-	-	-	-	-	-	-	-
Continue to Segment 2	-	-	-	-	-	-	-	-

5 Self-Tests

Each time the Module is powered on, it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged. Power on self–tests are available on demand by power cycling the Module.

On power on or reset, the Module performs the self-tests described in the Power on Self-tests table below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module halts and a POST error code is generated.
In addition to startup tests, the Module executes conditional data tests.

Table 12 – Power-on Self-tests

Test Target	Description
Symmetric Algorithms	
AES	KATs: Encryption, Decryption Modes: ECB, CBC Key sizes: 256 bits
Asymmetric Algorithms	
ECDSA	PCT: Signature Generation Component, Signature Verification Curves/Key sizes: P-521 w/ SHA 512
Hash Algorithms and Derivatives	
SHA	KATs: SHA-256, SHA-512
Deterministic Random Number Generation	
DRBG Health Checks	Tested by supplying a known state to the hardware and performing the following operations in sequence at start up. 1) Instantiate without entropy XOR, zeroize key and IV 2) Reseed 3) Generate 4) Generate (again) 5) Uninstantiate
DRBG	KATs: NIST SP800-90A Rev 1
Firmware Integrity Test	
POST0 32-bit Checksum	The POST0 firmware image incorporates a 32-bit checksum computed so that when the POST0 image is treated as an array of four-byte numbers, the sum of the entries is zero. POST0 copies itself from flash to RAM and then verifies the checksum on the RAM copy.
POST1 32-bit Checksum SHA-512	The POST1 firmware image incorporates a 32-bit checksum computed so that when the POST1 image is treated as an array of four-byte numbers, the sum of the entries is zero. When POST1 runs, it verifies the checksum on the RAM copy of itself. POST1 is covered by the Persistent Memory Manager (PMM). MB0 directs the PMM to copy POST1 from flash to RAM. The PMM verifies the SHA-512 hash of POST1 at this time.
POST2 32-bit Checksum SHA-512	The POST2 firmware image incorporates a 32-bit checksum computed so that when the POST2 image is treated as an array of four-byte numbers, the sum of the entries is zero. POST2 copies itself from flash to RAM and then verifies the checksum on the RAM copy. POST2 is covered by the Persistent Memory Manager (PMM). The PMM verifies the SHA-512 hash of POST2 when POST1 directs the PMM to initialize itself.

Test Target	Description
MB0 32-bit Checksum	The MB0 firmware image incorporates a 32-bit checksum computed so that when the MB0 image is treated as an array of four-byte numbers, the sum of the entries is zero. POST0 verifies the checksum on the copy of MB0 in flash before transferring control to MB0. While MB0 copies itself from flash to RAM, it computes the checksum and verifies that the result is zero at the end.
MB1 SHA-512	MB1 is covered by the Persistent Memory Manager (PMM). POST1 directs the PMM to copy MB1 from flash to RAM. The PMM verifies the SHA-512 hash of MB1 at this time.
FPGA Proprietary integrity check SHA-512	The FPGA blob incorporates a proprietary integrity check that is verified by the controller that reads the blob and uses it to configure the FPGA. The proprietary integrity check is a 32-bit CRC of the Altera FPGA. The FPGA blob is covered by the Persistent Memory Manager (PMM). POST1 directs the PMM to read the FPGA blob into a buffer in RAM before POST1 loads the blob into the FPGA hardware. The PMM verifies the SHA-512 hash of the FPGA blob at this time.

Table 13 – Conditional Self-Tests

Test Target	Description
DRBG	Continuous Test performed when a random value is requested from the DRBG.
ENT(P) NDRNG	Continuous Test performed when a random value is requested from the ENT(P) NDRNG.
Firmware Load	ECC P-521 signature verification when the firmware is loaded onto the card. Once the firmware has been stored in the flash on the card, hashes are used to verify the image integrity prior to invoking the firmware. This is done for Segment 1 [, 2, and 3]. Officer1 keys are used for Segment 1 and some Segment 2 firmware. Officer2 keys are used for other Segment 2 and all Segment 3 firmware.
ECDSA	Self-test in place for the underlying mathematical functions used for ECDSA (e.g., Point multiply, point verify, etc.). Pairwise consistency testing on all of the ECC keys generated, which, in effect, tests ECDSA (e.g., verifies that a generated keypair can be used to sign and then verify a data item).

6 Physical Security Policy

Module physical security mechanisms are mainly automatic. Intrusions, which destroy card secrets through an internal, independent action, are host-observable as system administration events. A picture of the Module security cover is presented in Figure 1.

System administrators may notice tamper detection through unusual Module startup, such as a card failing to initialize. The details of such administrator-level logging are platform-dependent. It is recommended to investigate the tamper event type reported by the Module, possibly cross-checking

the tamper event with other logs.

The types of tamper events are listed in the following table:

Table 14 – Physical Security Tamper Types and Recommended Actions

Physical Security Mechanism	Severity/Effect	Recommended Frequency of Inspection	Test Guidance
Hard Tamper	Zeroization	N/A (Automatic)	N/A
Soft Tamper	Module Reset	N/A (Automatic)	N/A
External Warning	Warning	Module Restart	Application Discretion
Low Battery	Warning	As frequent as possible	Replace as soon as possible

Physical security is constantly monitored through a tamper detection/ response envelope with tamper response and zeroization circuitry. No external physical monitoring is required. Environmental failure protection (EFP) is included.

A hard tamper event is caused by very high overvoltage, temperature, or its rate of change out of reasonable operational range, or physical tamper (penetration of the tamper-detection matrix). Module memory-type devices (e.g., BBRAM, communication FIFOs) are actively zeroized. Module secrets are immediately destroyed: HSEB is actively cleared at microelectronic speeds (sub-milliseconds). The Module becomes permanently inoperative: Miniboot startup does not successfully terminate without secrets in HSEB.

Any of the following conditions will trigger a hard tamper response:

- Mesh sensors opens and shorts detected
- High voltage (above 4.2 Volts) detected on 3.3 Volt Power supply or 3.3 Volt battery.
- High voltage (above 6.28 Volts) detected on 5 Volt Power supply
- Dead Battery (below 2.4 Volts) detected on 3.3 Volt Battery
- Tamper controller software configuration change attempt
- Temperature detected below -38°C ±3°C or above +90°C ± 2°C limits

A soft tamper event is caused by moderate overvoltage or temperature moderately out of operational range. Reaction is instantaneous. The Module is held under reset while the soft tamper conditions persist. Secrets are not destroyed.

Any of the following conditions will trigger a soft tamper response:

- Under voltage (below 4.76V) on 5 Volt Power supply
- Over voltage (above 5.89V) on 5 Volt power supply
- Temperature detected below 0°C ± 2°C or above 83°C ± 2°C

- System Reset from Host

Tamper evidence is provided by the metal enclosure and circuit board. Attempts to tamper are made evident by a scratch or dent in the surface of the material.

7 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and require a separate FIPS 140-2 validation.

8 Mitigation of Other Attacks Policy

N/A

9 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic Module to implement the security requirements of this FIPS 140-2 Level 4 Module.

1. The Module will provide three (3) distinct operator roles: Cryptographic Officer 1 / User role, Cryptographic Officer 2, and Cryptographic Officer 3.
2. The Module will provide identity-based authentication.
3. The Module will clear previous authentications on power cycle. This is accomplished by clearing RAM and all running applications.
4. When the Module has not been placed in a valid role, the operator will not have access to any cryptographic services.
5. The operator will be capable of commanding the Module to perform the power on self-tests by cycling power or resetting the Module.
6. Power on self-tests do not require any operator action.
7. Data output will be inhibited during key generation, self-tests, zeroization, and error states. This is accomplished by the Custom Communication Hardware in the PCIe interface path.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual key entry.
13. The Module does not have any external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does not output intermediate key values.

10 References and Definitions

The following are references for this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
FIPS140-2	*Security Requirements for Cryptographic Modules*, May 25, 2001
SP800-90A Rev 1	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015*
SP800-90B	*Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018*
Annex A	Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
Annex B	Approved Protection Profiles for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
Annex C	Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
Annex D	Approved Key Establishment Techniques for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

Table 16 – Acronyms and Definitions

Acronym	Definition
CA	Certificate Authority
CCP	Card Configuration Parameters
BBRAM	Battery-Backed static RAM
CSP	Critical Security Parameters
EDC	Error Detection code
Device Keypair	Device-specific public-key keypair generated and retained by Segment 1. It is non-exportable, traceable back to the IBM factory CA through a certificate chain and may be used by external parties to verify the identity of a Module through outbound authentication (OA).
Firmware identifier	An unambiguous status identifier (“Segment 1 hash”), used to quickly summarize firmware contents. It is the SHA-256 hash of firmware contents, possibly including hardware, such as an FPGA bitfile. Segments are identified by their own segment hashes, but this document only specifies Segment 1. Modules loaded with validated Segment 2 and 3 must specify their specific validated configurations.

Acronym	Definition
FWID	Abbreviation of Firmware identifier
High Voltage	Anything above the specified voltage is considered High Voltage. For example, “High Voltage on +5 (6.28V ± 0.01V)” means anything above 6.28V is considered High Voltage with a variation/toleration of 0.01V.
HLM	Hardware Lock Microcontroller, a dedicated microcontroller which assisted previous 47xx generations with access control and management of persistent storage. While current generations no longer contain an actual HLM controller, some of the relevant functionality has been retained. Documentation refers to these features as “HLM (infrastructure)” for historical reasons.
HSEB	High-speed erase BBRAM, a dedicated BBRAM chip actively erased upon tamper. The most valuable Miniboot secrets reside within this region, which is wiped within milliseconds of detecting a tamper event.
IA	Inbound Authentication, Miniboot authenticates each command request individually.
KAT	Known Answer Test
MCPU	The Module CPU (MCPU) is a redundant embedded PowerPC 476. It is not used in the FIPS mode of operation.
Miniboot	Software component of Module firmware. Miniboot functionality, together with POST, roughly corresponds to those of a system BIOS in PCs, with obvious additions to cover cryptographic functionality, Module-specific hardware, and act as the Module security controller.
MB0	Miniboot #0 is the security bootstrap that verifies the MB0 checksum; notifies the host to start and that MB0 is ready; loads POST1 into DRAM; verifies the SHA-512 hash of POST1 in DRAM; and transitions to POST1 if status permits.
MB1	Miniboot #1 checks the health of the DRBG; notifies the host to start and that MB1 is ready; gets and processes MB1 commands; and provides the “Continue to Segment 2” service.
OA	Outbound Authentication, infrastructure capable of signing by a card-resident, non-exportable private key. External parties, including other Modules, can verify that signed content has been generated by an untampered Module firmware (Segment 1). An extension allows OA to manage private keys for OS or applications (Segment 2 or 3).
PCIe	PCI Express, the external interface of our Module (also abbreviated as PCI-E).
PN	Part Number
POST	Power-On Self-Test, infrastructure tests resident in ROM and flash.

Acronym	Definition
POST0	Power-On Self-Test #0 initializes the hardware, verifies the POST0 checksum, performs SHA-512 KATs, verifies the MB0 checksum, and transitions to MB0 if status permits.
POST1	Power-On Self-Test #1 verifies the POST1 checksum; configures and tests hardware; performs KATs; provides the “Continue to Segment 1” service; and transitions to MB1 if status permits.
POST2	Power-On Self-Test #2 is the part of the Segment 1 image that is the startup stub for Segment 2.
RAS	Abbreviation of Reliability, Availability, Serviceability
SSP	Security Service Processor (SSP), a dedicated processor executing Miniboot and most of POST (i.e., all privileged code). The SSP is an embedded PowerPC 405.
Segment 1F	Segment 1F is the rewritable part of card infrastructure, including the FPGA programming file, and POST 2, all protected as part of Segment 1. Used only when the FPGA bitfile is explicitly mentioned in Segment 1 operations.