SiCore
technologies inc

SHIELD Secure Coprocessor
FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.2
Date: August 24, 2015

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the SHIELD Secure Coprocessor module, hereafter denoted the SHIELD. The SHIELD, validated to FIPS 140-2 overall Level 3, is a high performance secure foundation of hardware and trusted firmware on which sensitive applications (denoted System Level functionality herein) can be loaded and executed by future partners or end user developers. The scope of this validation is the SHIELD platform with no System Level functionality. Additional documentation, testing and a separate validation is required to obtain FIPS 140-2 validation of System Level functionality.

The FIPS 140-2 security levels for the SHIELD are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	4
Mitigation of Other Attacks	3

Table 1 – Security Levels of Security Requirements

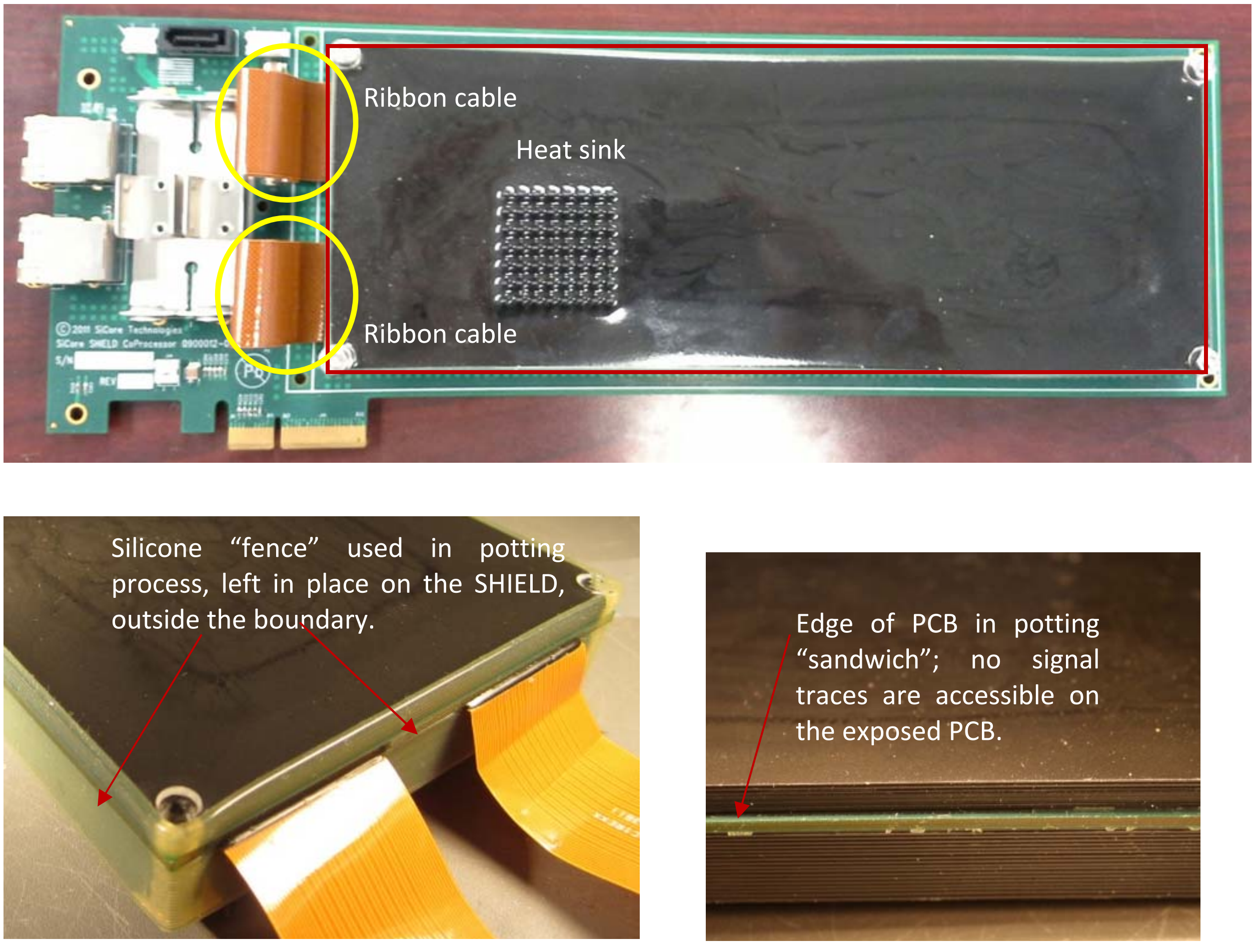
Note that CMVP program guidance requires any area that has no distinguishing factors between levels to be listed at the overall level – Level 3 in this case. For this module, only Physical Security and Design Assurance differ between Level 3 and Level 4; as such, all other Levels must be listed at Level 3.

The module's design includes a formal model of the module's function, confirmed during the FIPS 140-2 validation process by a combination of formal and informal proof processes using the B Method and the Atelier B toolkit.

1.1 Hardware and Physical Cryptographic Boundary

The SHIELD is a multi-chip embedded embodiment (see Figure 1). The cryptographic boundary is the surfaces and edges of the epoxy encapsulant (red), the exposed PCB at the center sides of the module and the protruding ribbon cables (yellow circles). The physical form of the SHIELD is depicted in Figure 1, with the red outline indicating the cryptographic boundary.

The SHIELD requires the PCIe carrier board, also shown in Figure 1 for physical connection to the ribbon connectors. The heat sink can be seen protruding from the epoxy. The image at lower left shows the ribbon cables (which are the physical ports that cross the boundary) and the image on the lower right shows the exposed PCB. The potting process uses a silicone fence and epoxy is poured onto both sides of the board to form a "sandwich" with the edge of the PCB exposed. No signal traces are accessible outside the potting. The image at the top shows the SHIELD mounted on the carrier board, for context.



Silicone "fence" used in potting process, left in place on the SHIELD, outside the boundary.

Edge of PCB in potting "sandwich"; no signal traces are accessible on the exposed PCB.

Figure 1 – Physical Form of the Module

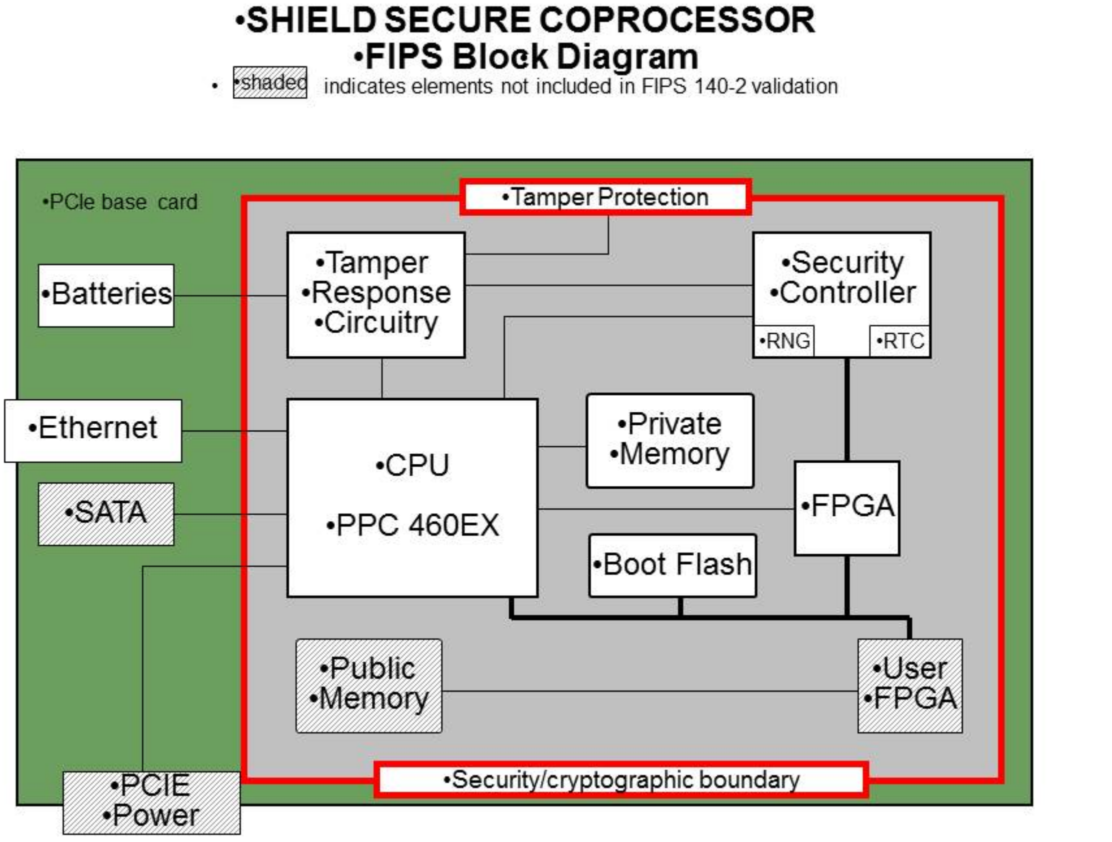
The SHIELD has two physical connectors, the two ribbon cables shown in the figure above. In the table below, RC1 refers to Ribbon Cable 1, and RC 2 refers to Ribbon Cable 2.

Port	Description	Logical Interface Type
RC1: Ethernet (2x)	10/100/1000 BaseT IEEE 802.3	Control in, Status out, Data in, Data out
RC1: Power	Power	Power (+5.0V)
RC1: Battery	External battery backup power	Power (+3.0V nominal)
RC1: SATA	Future interface expansion option	Not connected, non-functional
RC2: PCIe	Future interface expansion option	Not connected, non-functional
RC2: Power	Power	Power (+3.3V)

Table 2 – Ports and Interfaces

1.2 *Firmware and Logical Cryptographic Boundary*

Figure 2 depicts the SHIELD secure coprocessor architecture.



•_SiCore\5-Certification\SHIELD Security Policy\SSD OSD 110502

Figure 2 – Module block diagram in a typical operational context

CPU – the PowerPC master controller for the SHIELD; executes Module Foundation Firmware (MFF), manages external (Ethernet) communications, manages the Security Controller and FPGA.

FPGA – buffered communications between the CPU and the security controller.

Security Controller – hardware optimized for management of sensitive data and cryptographic functionality. Includes a non-volatile memory for CSP storage designed for fast erasure triggered by a tamper event or command. The MAX-Q1103 processor provides key storage and confirmation of the FIPS-approved mode. It stores the SHA-256 hash of the PowerPC code that is stored in flash and compares it to values calculated by the CPU during boot up.

Boot Flash - contains the boot load code in a locked sector and partitions to support User (System Level) applications.

Private Memory – provides communication buffering between the host computer and the secure coprocessor. Only the CPU can read from or write to private memory.

Tamper response circuitry – sensors to trigger fast erasure and hold the processor in a reset state.

The SATA interface, PCI-e, User FPGA and Public Memory are options for future expansion, and are unused in this version of the SHIELD.

1.3 Versions and Mode of Operation

Hardware: SHIELD Secure CoProcessor V1.0

Firmware: MFF V1.0, FPGA V1.0, SC V1.0

The SHIELD as delivered by SiCore is always in the FIPS 140-2 Approved mode of operation.

To verify that SHIELD is in an Approved mode of operation and obtain the indicator of Approved mode required for FIPS 140-2 Level 3 and higher, a Get Mode command is sent to the SHIELD card. A return value of 1 indicates that the module is in the Approved mode; any other value indicates a non-functioning module.

2 Cryptographic Functionality

The SHIELD implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Table 3 and Table 4 below.

Algorithm	Description	Cert #
AES	[FIPS 197] AES-256 ECB Encrypt/Decrypt.	2195
RSA	[FIPS 186-4] RSA 3072-bit Signature Verification.	1131
SHA	[FIPS 180-3] SHA-256 secure hash algorithm.	1901

Table 3 –Approved Cryptographic Functions

Algorithm	Description
RSA Key Transport	RSA 3072 key wrapping; key establishment methodology provides 128 bits of encryption strength. No claim of conformance to SP 800-56B is made.

Table 4 – Non-Approved But Allowed Cryptographic Functions

2.1 Critical Security Parameters

The SHIELD implements the following critical security parameters:

CSP	Description / Usage
Flash-KEK	AES-256 Master key used to encrypt all User (System Level) data stored in the Boot Flash.
Admin-KUK	Private component of an RSA key pair (3072-bit), used to decrypt an AES-256 key.
Session-DEK	AES-256 data encryption / decryption key. The lifetime of this key is approximate to the Install Application service time.

Table 5 – Critical Security Parameters

2.2 *Public Keys*

Key	Description / Usage
Admin-KWK	Public component of an RSA key pair (3072-bit). This key is present on the module, but is not used by the module except to provide to the external user for Session-DEK encapsulation, outside the SHIELD scope.
Auth-SVK	0-10 instances of an RSA 3072-bit public key used by the SHIELD to verify the signature of any authenticated command sent to the SHIELD. The index 0 instance is associated with the Administrator operator role. Any additional instances are associated with User role instances.

Table 6 – Public Keys

3 Roles, Authentication and Services

The SHIELD supports two distinct operator roles, Administrator (A) and User (U), as shown in Table 7. The SHIELD supports a single Administrator role (equivalent to the Crypto Officer role in FIPS 140-2 terminology), and 0-10 instances of the User role. Each authenticated command is accompanied by a security domain identifier and command signature, signed by an external device (out of the scope of this validation) using the operator's private key. No authenticated services are permitted until an Administrative user public key has been successfully registered using the Register Security Domain command. The SHIELD does not maintain an authenticated state; rather, an authenticated command is only executed if the command signature is verified with the public key corresponding to the identified operator.

The Administrator Security Domain (Auth-SVK 0) is registered only during initialization as an un-authenticated command. It cannot be overwritten or deleted during deployment by the REGISTER_SD and DELETE_SD commands. In order to re-register it, the card would need to be re-initialized, which destroys the keys located in the MAXQ zeroizable memory. The card cannot be re-initialized in the FIPS 140-2 configuration, with epoxy and anti-tamper mechanisms in place and functional.

ID	Role Description	Authentication Type	Authentication Data
A	Administrator (see above and services)	Identity-based authentication, using signature verification.	Command signature
U	User (see above and services)	Identity-based authentication, using signature verification.	Command signature

Table 7 – Roles/Authentication Description

The probability of false authentication is 1/(2^128) based on the equivalent strength of RSA 3072 bit signature verification, expressed in scientific notation as 2.94E-39. A conservative lower bound for command execution time is 10 ms, therefore the probability of false authentication in a one minute period is (6x10^3)/(2^128), expressed in scientific notation as 1.76E-35.

3.1 Services

Table 9 and Table 9 list unauthenticated and authenticated SHIELD services, respectively. Table 10 describes the usage of CSPs by each service.

Service	Description
HW Reset	Power cycle or tamper response circuit initiated reset, invoking all power-on self-tests.
Get Mode	Returns a 1 if the module is functional and in the Approved mode.

Table 8 – Unauthenticated Services

Service	Description	A	U
Register Security Domain	Registers a new Security Domain (User).	X	
Zeroize	Destroys all SHIELD CSPs.	X	
Delete Security Domain	Disassociates a registered security domain / user.	X	X
Install Application	Installs an application to be run by a security domain.	X	X
Delete Application	Deletes an application.	X	X
Run Application	Runs a security domain's application.		X
Reset	Initiates a software reset of the card (inclusive of self-test initiation).	X	X

Table 9 – Authenticated Services

Service	Flash-KEK	Admin-KUK	Session-DEK
HW Reset	N/A	N/A	N/A
Get Mode	N/A	N/A	N/A
Register Security Domain	N/A	N/A	N/A
Zeroize	Z	Z	Z
Delete Security Domain	N/A	N/A	N/A
Install Application	E	E	W, E
Delete Application	N/A	N/A	N/A
Run Application	E	N/A	N/A
Reset	N/A	N/A	N/A

Table 10 – Usage of CSPs by Services (E = Execute; W = Write; Z = Zeroize)

4 Self-test

4.1 Power Up Self-tests

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

On power-up or reset, the SHIELD performs the self-tests described in Table 11 below. All KATs must be completed successfully prior to any other use of cryptography by the SHIELD. If one of the KATs fails, the SHIELD enters the *KATS FAILED* error state.

Test Target	Description
Firmware Integrity	SHA-256 performed over Security Controller and CPU (PowerPC) code in separate steps. The FPGA CRC is checked internally by the device.
AES	Separate encrypt and decrypt KATs using AES-256 ECB.
RSA	RSA 3072-bit Signature Verification KAT.
SHA	The SHA-256 is self-tested as an embedded algorithm of the RSA KAT.

Table 11 – Power Up Self-tests

4.2 Conditional Self-tests

Test Target	Description
Firmware Load	RSA 3072-bit signature verification performed when firmware is loaded by the Install Application service.

Table 12 – Conditional Self-tests

4.3 Critical Function Tests

Test Target	Description
MAXQ	Communications and basic function test

Table 13 – Critical Function Tests

5 Physical Security Policy

The SHIELD PCB assembly is encapsulated in a hard, opaque epoxy encapsulant. The SHIELD is inspected for tamper evidence during the manufacturing process. The SHIELD should be inspected periodically for signs of tamper evidence. If evidence of tamper is detected, the module should be returned to SiCore Technologies, Inc.

6 Operational Environment

The SHIELD is designated as a limited operational environment under the FIPS 140-2 definitions. The SHIELD includes the Install Application service to load System Level functionality. 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.

7 Mitigation of Other Attacks Policy

- A tamper event will be triggered by the following sensors if their limits are violated.
- Plus 5 Volt Window Comparator (<4.5V >5.5V).
- Plus 3.3 Volt Window Comparator (<3.0V >3.6V).
- A Temperature Sensor (< -20C >125C).
- A Light/Radiation Sensor.

8 Security Rules and Guidance

The SHIELD does not require any specific external input/output devices, and does not implement:

- Bypass
- Maintenance role, state or interface
- Concurrent operators
- Manual key entry
- Plaintext CSP entry or output, or output of any intermediate key values
- Key generation or random number generation

The SHIELD enforces all rules necessary for secure operation of the module, assuring that:

- Data output is inhibited during self-tests, zeroization, and error states
- Status information does not contain CSPs
- Errors or failures of any level of firmware will not compromise the integrity of any lower layers.
- All CSPs are zeroized by the Zeroize service
- All sensitive data is zeroized on a tamper event detected by the tamper detect subsystem, or by invocation of the Zeroize service.
- Command signature verification is performed for every authenticated service request prior to performing an authenticated service, including all re-authentication scenarios.

Administrator and User operator responsibilities and guidance:

- The operator is responsible for protection of private keys external to the module scope (e.g., the private component associated with the Auth-SVK public key held in the module), and for correct association of operators to public keys registered to the SHIELD.
- The operator is required to encrypt Session-DEK with the public key before transmission to the card.

No trusted couriers or on-site security officers are needed to operate the secure coprocessor. No database or copy of device secrets is maintained by SiCore Technologies and there is no mechanism for unauthorized access to services, critical security parameters or protected data. The module does not retain Session-DEK keys.

9 References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[IG]	NIST FIPS 140-2 Implementation Guidance

Table 14 – References

10 Acronyms and Definitions

Acronym	Definition
MFF	Module Foundation Firmware
FPGA	Field Programmable Gate Array (FPGA)
CPLD	Complex Programmable Logic Device
SATA	Serial Advanced Technology Attachment – a bus interface specification.
SC	Security Controller – the MAX-Q1103 part in this design.

Table 15 – Acronyms and Definitions