Tintri Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Document Revision: 1.3
S.W. Version: 1.0

REVISION HISTORY

Author(s)	Version	Updates
Farzam Tajbakhsh	1.0	Initial release
Thomas Clifford	1.1	Update
Thomas Clifford	1.2	Addition of T7080 and T7060
Thomas Clifford	1.3	T7060 CPU correction

Table of Contents

INTRODUCTION

The following summarizes key features of the Tintri Cryptographic Module (Software Version 1.0). Hereinafter, the Tintri Cryptographic Module may be referred to as "the cryptographic module" or "the module". The module is a multi-chip standalone software-only cryptographic module.

The module is tested under the configurations below:

Platform	Operating System	Processor	Optimization
T1000	Tintri OS 4.5	Intel Xeon E5-2609 @ 1699MHZ	AES-NI
		Intel Xeon E5-2609 @ 1699MHZ	None
EC6030	Tintri OS 4.5	Intel Xeon E5-2609 @ 1699MHZ	AES-NI
		Intel Xeon E5-2609 @ 1699MHZ	None
EC6050	Tintri OS 4.5	Intel Xeon E5-2609 @ 1699MHZ	AES-NI
		Intel Xeon E5-2609 @ 1699MHz	None
EC6070	Tintri OS 4.5	Intel Xeon E5-2620 @ 2100MHz	AES-NI
		Intel Xeon E5-2620 @ 2100MHz	None
EC6090	Tintri OS 4.5	Intel Xeon E5-2680 @ 2399MHz	AES-NI
		Intel Xeon E5-2680 @ 2399MHz	None
T7060	Tintri OS 5.2	Intel(R) Xeon(R) Gold 5218T CPU @ 2.10 GHz	with AES-NI
		Intel(R) Xeon(R) Gold 5218T CPU @ 2.10 GHz	None
T7080	Tintri OS 5.2	Intel(R) Xeon(R) Gold 6230 CPU @ 2.10 GHz	with AES-NI
		Intel(R) Xeon(R) Gold 6230 CPU @ 2.10 GHz	None

Exhibit 1 – *Tested Configurations*

NOTE: The CMVP allows porting of this cryptographic module from the operational environment specified on the validation certificate to an operational environment which was not included as part of the validation testing as long as the porting rules of FIPS 140-2 Implementation Guidance G.5 are followed. As per FIPS 140-2 Implementation Guidance G.5, no claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed above in Exhibit 1.

CRYPTOGRAPHIC BOUNDARY

The following diagram defines the cryptographic boundary of Tintri Cryptographic Module 1.0:

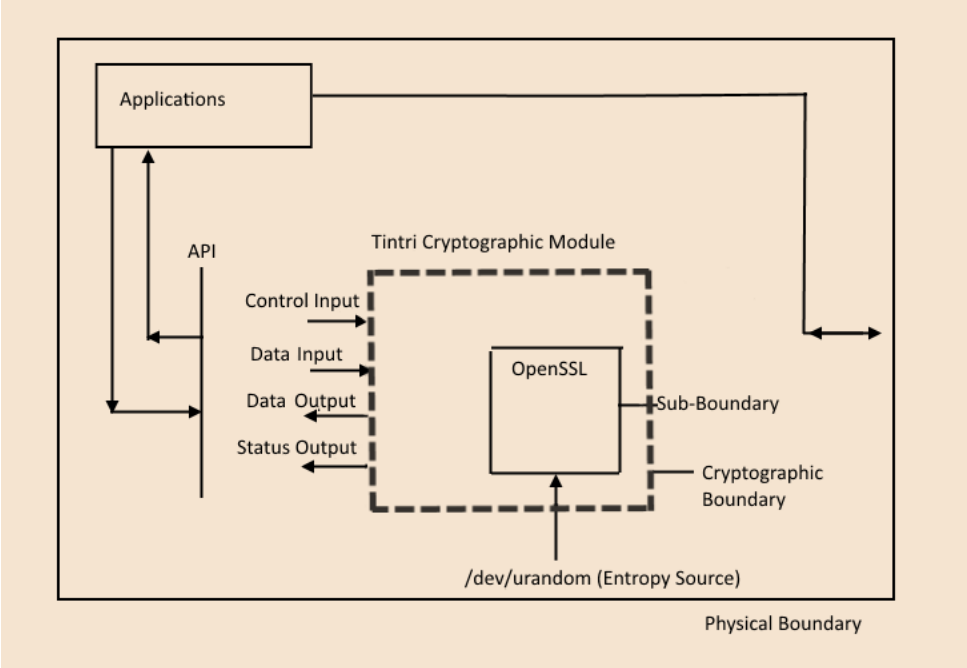

Exhibit 2 – *Specification of Cryptographic Boundary of Tintri Cryptographic Module 1.0*

ACRONYMS

Acronyms related to the cryptographic module that will be referenced in this document:

TERM	DESCRIPTION
AES	Advanced Encryption Standard (FIPS-197)
API	Application Programming Interface
CBC	Cipher Block Chaining
CTR	Counter
CO	Crypto Officer
DRBG	Deterministic Random Bit Generator (SP800-90Ar1)
ECB	Electronic Codebook
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standards
FIPS 140-2 IG	Federal Information Processing Standards 140-2 Implementation Guidance
GCM	Galois/Counter Mode
HMAC	Keyed-hash Message Authentication Code (FIPS 198-1)
IV	Initialization Vector
KAT	Known Answer Test
N/A	Not Applicable
NDRNG	Non-deterministic random number generator
RAM	Random-access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
SHA-1	Secure Hash Algorithm 1 (FIPS 180-4)
USB	Universal Serial Bus
VGA	Video Graphics Array

Exhibit 3 – *Specification of acronyms and their descriptions*

SECURITY LEVEL SPECIFICATION

FIPS 140-2 SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Exhibit 4 – *Security Level Specification Table.*

PHYSICAL PORTS AND LOGICAL INTERFACES

The module runs on a general-purpose computer with physical ports. The tested configurations include the following physical ports:

- Power Port
- Ethernet Port
- Serial Port
- USB Port
- VGA Port

The module does not include a maintenance interface. Given that the cryptographic module is software-only the logical interfaces into the module are via its API.

LOGICAL INTERFACE	DESCRIPTION
Data Input	API Data Input Parameters
Control Input	API Control Input Parameters
Data Output	Return statements from API
Status Output	Status statements returned from API

Exhibit 5 – *Specification of Cryptographic Module Logical Interfaces*

SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

1. Installation of the cryptographic module is the responsibility of the Crypto Officer. The Crypto Officer shall install the cryptographic module as follows:
    A. Install the software-only cryptographic module (libtcrypto.so and libtcrypto.so.sha1) onto the general purpose computing platform.

    NOTE: The Crypto Officer shall verify the message authentication code in file libtcrypto.so.sha1 containing the publicly available HMAC-SHA-1 of the cryptographic module. This can be accomplished by opening the file in a HEX editor and inspecting the contents of the file; the HEX value to be verified is: b0c6c7477903c4760cc203c4aef958b8aca5a971

    B. Upon successful installation the cryptographic module is now available for use.

    C. The calling application can now invoke the cryptographic module. Upon invocation, the module will perform power-up self-tests and output the following status output if successful:

    libtcrypto.so HMAC-SHA1 verified!
    TCRYPTO library self test validated!

2. The module enforces logical separation between all data inputs, data outputs, control inputs, and status outputs via the cryptographic module API.
3. The cryptographic module inhibits all data output during self-tests and error states. The data output interface is logically disconnected from the processes performing self-tests and zeroization.
4. The cryptographic module is designed to satisfy the requirements of FIPS 140-2 Level 1, therefore the cryptographic module does not provide authentication mechanisms.
5. The cryptographic module runs on a general-purpose computing platform that conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e. for Home use) which vacuously satisfies Class A.
6. Power-up self-tests do not require any operator intervention (i.e. the cryptographic module includes a default entry point as per FIPS 140-2 Implementation Guidance 9.10).

7. The cryptographic module protects CSPs from unauthorized disclosure, unauthorized modification, and unauthorized substitution. The cryptographic module does not utilize public/private keys.
8. The cryptographic module does not support a maintenance interface or maintenance role.
9. The cryptographic module does not support manual key entry.
10. The cryptographic module does not support a bypass capability.
11. FIPS 140-2, Section 7.7 is applicable to this software module. As per the guidance, the module under tests falls under category “CM Software to/from App Software via GPC INT Path”, whereby the key entry/output requirements of FIPS 140-2 Area 7 are not applicable.
12. The general-purpose computing platform includes a power port.
13. Roles are implicitly assumed based upon the service requested.
14. When performing zeroization, the operator of the cryptographic module shall reboot the cryptographic module and shall reformat and overwrite the hard drive.
15. As per FIPS 140-2 Implementation Guidance 6.1, the server application is the single-user of the cryptographic module.
16. Power cycle the module in order to exit the error states and resume normal operation. Otherwise, reinstall the software-only cryptographic module onto the general-purpose computing platform.

17. The cryptographic module supports a FIPS Approved mode of operation and a non-FIPS Approved mode of operation. The module will be in FIPS-Approved Mode when invoking Approved services and algorithms (see Exhibit 6 and Exhibit 11), and the module will be in non-FIPS Approved mode when invoking non-Approved services and algorithms (see Exhibit 7 and Exhibit 8).

MODES OF OPERATION

The module supports two modes of operation: FIPS Approved mode and non-Approved mode.

FIPS APPROVED MODE OF OPERATION

The module supports the following Approved Security Functions in FIPS Approved mode:

APPROVED ALGORITHMS AVAILABLE IN FIPS MODE

CAVP CERT#	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS	USE
4856, 4857, 4858, 4859, 4860, 4861, A2046	AES	FIPS 197, SP800-38A	ECB, CBC	128, 192, 256	Data Encryption/ Decryption
3252, 3253, 3254, 3255, 3257, 3258, A2046	HMAC	FIPS 198-1	HMAC-SHA-1	112 < bits ≤ 256	Message Authentication
3993, 3994, 3995, 3996, 3998, 3999, A2046	SHS	FIPS 180-4	SHA-1	N/A	Hashing

Exhibit 6 – *Table of Approved Algorithms Available in FIPS Mode*

For additional information on transitions associated with the use of cryptography refer to NIST Special Publication SP800-131Ar2. This document can be located on the CMVP website at: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf)

The data in the tables will inform Users of the risks associated with using a particular algorithm and a given key length.

NON-APPROVED MODE OF OPERATION

The following non-FIPS approved algorithms are provided only in non-Approved mode of operation.

NON-APPROVED ALGORITHMS AVAILABLE IN NON-FIPS MODE

ALGORITHM	MODE/METHOD	KEY LENGTHS	USE
NDRNG (Note: /dev/urandom is outside of the cryptographic module's logical boundary but inside of the physical boundary)	N/A	N/A	Seeding for the Non-Approved DRBG
AES (Non-Compliant)	GCM (Non-Compliant)	128, 192, 256	Non-Approved Authenticated Encryption
DRBG (Non-Compliant)	CTR_DRBG (with Derivation Function) (Non-Compliant)	N/A	Non-Approved Deterministic Random Bit Generation

Exhibit 7 – *Table of Non-Approved Algorithms Available in Non-FIPS Mode*

The following table lists services implemented by the cryptographic module that shall not be used when operating in the FIPS Approved mode of operation. If any of these services are used, the cryptographic module is no longer considered to be in the FIPS Approved mode of operation.

Service	ROLE	ALGORITHM(S)	MODE
Non-Approved Random Number Generation	CO, User	NDRNG, DRBG (Non-Compliant)	CTR_DRBG (with Derivation Function) (Non-Compliant)
Non-Approved Authenticated Encryption	CO, User	AES (Non-Compliant)	GCM (Non-Compliant) (with 128, 192, or 256 bit keys)

Exhibit 8 –*Table of Services Available in Non-Approved Mode*

IDENTIFICATION AND AUTHENTICATION POLICY

The cryptographic module supports a Crypto Officer role and a User role. A role is implicitly assumed based upon the service that is invoked.

ROLE	AUTHENTICATION TYPE	AUTHENTICATION DATA
Crypto Officer	N/A	N/A
User	N/A	N/A

Exhibit 9 - *Roles and required Identification and Authentication (FIPS 140-2 Table C1)*

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM
N/A	N/A

Exhibit 10 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

ACCESS CONTROL POLICY

The following table describes the services of the module available in FIPS Approved Mode along with which role, cryptographic keys and CSPs, and type of access it corresponds to.

SERVICE	ROLE	CRYPTOGRAPHIC KEYS & CSPs	TYPE(S) OF ACCESS
Install/Initialize	CO	None	-
Self-test	CO, User	None	-
Show Status	CO, User	None	-
Zeroize	CO, User	All CSPs	D
Symmetric encrypt/decrypt	CO, User	Data Encryption Key	R, W
Keyed Hash	CO, User	HMAC Key	C, D, R, W
Utility	CO, User	None	-

Exhibit 11 - *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4)*

Exhibit 11 above describes how the services performed by each role access each CSP. A letter is placed in the Type(s) of Access column when a service can create (C), destroy (D), read (R) or write (W) a CSP.

SELF-TESTS

Power-Up Tests:

1. Software Integrity Test
    a. HMAC-SHA-1
2. Known Answer Tests:
    a. AES (128-bit) key size KAT (encrypt) in CBC Mode
    b. AES (128-bit) key size KAT (decrypt) in CBC Mode
    c. AES (192-bit) key size KAT (encrypt) in CBC Mode
    d. AES (192-bit) key size KAT (decrypt) in CBC Mode
    e. AES (256-bit) key size KAT (encrypt) in CBC Mode
    f. AES (256-bit) key size KAT (decrypt) in CBC Mode
    g. HMAC SHA-1 KAT
3. Critical Functions Tests:
    a. N/A

Conditional Tests: N/A

Status messages for success/failure of self-tests:

1. Success:
    a. HMAC-SHA-1 Software Integrity Test:
    Libtcrypto.so HMAC-SHA1 Verified!

    b. All known answer tests(encrypt/decrypt):
    TCRYPTO library self test validated!

2. Failure:
    a. HMAC-SHA-1 Software Integrity Test:
    HMAC doesn't match!
    Failed: libtcrypto.so HMAC-SHA1 verification!

    b. AES (128-bit) key size KAT(encrypt/decrypt) in CBC Mode:
    Failed: FIPS_selftest_aes_cbc_128

    c. AES (192-bit) key size KAT(encrypt/decrypt) in CBC Mode:
    Failed: FIPS_selftest_aes_cbc_192

    d. AES (256-bit) key size KAT(encrypt/decrypt) in CBC Mode:
    Failed: FIPS_selftest_aes_cbc_256

e. HMAC SHA-1 KAT :
Failed: FIPS_selftest_hmac

PHYSICAL SECURITY POLICY

The cryptographic module is a software-only module, so the physical security requirements of FIPS 140-2 Area 5 are not applicable.

PHYSICAL SECURITY MECHANISMS	RECOMMENDED FREQUENCY OF INSEPCTION/TEST	INSPECTON/TEST GUIDANCE DETAILS
N/A	N/A	N/A

Exhibit 12 - *Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)*

MITIGATION OF OTHER ATTACKS POLICY

The cryptographic module is not designed to mitigate any other attacks beyond the specific scope of FIPS 140-2.

OTHER ATTACKS	MITIGATION MECHANISM	SPECIFIC LIMITATIONS
N/A	N/A	N/A

Exhibit 13 – *Table of Mitigation of Other Attacks (FIPS 140-2 Table C6)*

APPENDIX A: CRITICAL SECURITY PARAMETERS

1. Data Encryption Key (128-bit, 192-bit and 256-bit)
   - Description: 128-bit, 192-bit and 256-bit AES secret keys used in CBC mode to encrypt user data locally
   - Generation: N/A
   - Establishment: N/A
   - Storage: RAM
   - Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable
   - Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable
   - Entity: via process
   - Zeroization: Overwrite with zeroes in RAM

2. HMAC Key (112 < bits ≤ 256)
   - Description: HMAC key used for “Keyed Hash” service
   - Generation: N/A
   - Establishment: N/A
   - Storage: RAM
   - Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable
   - Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable
   - Entity: via process
   - Zeroization: Overwrite with zeroes in RAM

(END OF DOCUMENT)