FIPS 140-2 Level 2 Security Policy

For

Thunder by A10 Networks, Inc.

Versions TH1040, TH3350S, TH6655S, and TH7655S

Document Version 1.4

This security policy describes the FIPS 140-2 compliance of the module

Table of Contents

1 Module Description

A10 Networks, Inc.'s Thunders are an outgrowth or evolution of Traffic Manager and Application Delivery Controller (ADC) systems and technologies. These Thunder systems are advanced load balancers for ADC needs and sophisticated address translators for IPv6 migration, while being able to secure and control the traffic directed through the system for enterprise, ISP, and mobile networks. These systems include full proxies able to encrypt, decrypt, and inspect traffic for these networks.

The foundation of the Thunder systems is the A10 Networks, Inc's proprietary A10 Core Operating System (ACOS). ACOS is a software framework for maximized networks traffic processing performance that supports a common management and control plane architecture across a range of infrastructures; from data centers to cloud to multi-cloud.

These systems (subsequently referred to as "the module") support SSH, HTTPS, and console management interfaces. For the purposes of FIPS 140-2 the Thunder is classified as multi-chip standalone module.

FIPS 140-2 conformance testing of the module was performed at Security Level 2. The following configurations were tested:

Table 1: Configurations tested by the lab

Module Name	Hardware versions	Processor	Firmware versions
Thunder by A10 Networks, Inc.	TH1040	Intel Atom C3958 with AES-NI	5.2.1-P5
	TH3350S	Intel Xeon D-2177NT with AES-NI	5.2.1-P5
	TH6655S	Intel Xeon Gold 6258R with AES-NI	5.2.1-P5
	TH7655S	Intel Xeon Gold 6258R with AES-NI	5.2.1-P5

Table 2: Module Security Level Statement

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

2 Cryptographic Boundary

The hardware and firmware components of the module are enclosed in a metal enclosure which is the cryptographic boundary of the module. The removable panels of the enclosure are protected by tamper-evident labels. The enclosure is opaque within the visible spectrum.

Images of the module is provided below:

Figure 1. Thunder TH1040

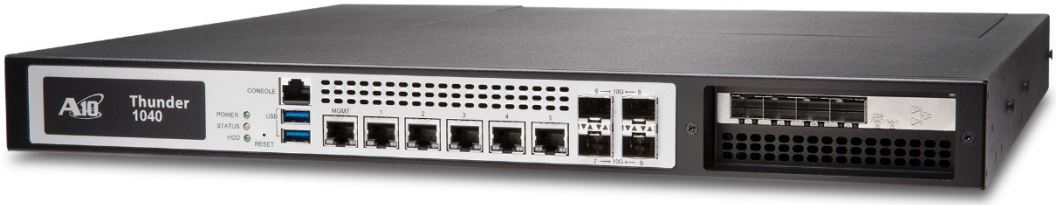

Figure 2. Thunder TH3350S

Figure 3. Thunder TH6655S

Figure 4. Thunder TH7655S

3 Security Functions

The table below lists approved cryptographic algorithms employed by the module.

Table 3: Approved Cryptographic Functions

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1940 A1305	A10 Networks SSL FIPS Library	AES	FIPS 197, SP 800-38D	ECB, CBC, CTR, GCM[1]	128, 192, 256	Data Encryption/ Decryption KTS[4]
A2499	A10 Networks Data Plane FIPS Library-1			CBC, GCM[1]		
A2500	A10 Networks Data Plane FIPS Library-2					
A1181	A10 Networks IPsec FIPS Library					
A2493	A10 Networks Data Plane FIPS Software Library			CBC		
C1940 A1305	A10 Networks SSL FIPS Library	DRBG	SP 800-90A	CTR_DRBG		Deterministic Random Bit Generation[2]
A2493	A10 Networks Data Plane FIPS Software Library					
A2499	A10 Networks Data Plane FIPS Library-1	KAS-ECC-SSC	SP 800-56Ar3	ECC Ephemeral Unified Scheme	P-256, P-384 (corresponding to 128 or 192 bits of security)	TLS Shared Secret Computation
A2500	A10 Networks Data Plane FIPS Library-2					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2499	A10 Networks Data Plane FIPS Library-1	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC- SHA-512	160, 256, 384, 512	Message Authentication KTS[4]
A2500	A10 Networks Data Plane FIPS Library-2					
C1940	A10 Networks SSL FIPS Library					
A1305						
A1181	A10 Networks IPsec FIPS Library					
A2493	A10 Networks Data Plane FIPS Software Library			HMAC-SHA-256, HMAC-SHA-384, HMAC- SHA-512	256, 384, 512	
A2493	A10 Networks Data Plane FIPS Software Library	SHS	FIPS 180-4	SHA-256, SHA-384 SHA-512		Message Digest
A1181	A10 Networks IPsec FIPS Library			SHA-1, SHA-256, SHA-384, SHA-512		
A2499	A10 Networks Data Plane FIPS Library-1					
A2500	A10 Networks Data Plane FIPS Library-2					
C1940	A10 Networks SSL FIPS Library					
A1305						

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A1305 C1940	A10 Networks SSL FIPS Library	RSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 3072	Digital Signature Generation and Verification; Key Generation
A2499	A10 Networks Data Plane FIPS Library-1		FIPS 186-4	SHA-256, SHA-384, SHA-512, PKCS1 v1.5	2048	Digital Signature Generation and Verification
A2500	A10 Networks Data Plane FIPS Library-2					
C1940 A1305	A10 Networks SSL FIPS Library	ECDSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512	P-256, P-384, P-521	Digital Signature Generation and Verification; Key Generation and Verification
A2499	A10 Networks Data Plane FIPS Library-1			SHA-256, SHA-384, SHA-512	P-256, P-384	
A2500	A10 Networks Data Plane FIPS Library-2					
A1305	A10 Networks SSL FIPS Library	DSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512	1024 (verification only), 2048, 3072	Digital Signature Generation and Verification; Key Generation and Key Verification

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A1305	A10 Networks SSL FIPS Library	KAS-FFC-SSC and Safe Primes	SP 800-56Ar3	Ephemeral Scheme	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)	Shared Secret Computation
A1305		KAS-ECC-SSC		ECC Ephemeral Unified Scheme	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)	
A2499 A2500 A2493	A10 Networks Data Plane FIPS Library-1 A10 Networks Data Plane FIPS Library-2 A10 Networks Data Plane FIPS Software Library	KAS	SP 800-56Ar3 and SP 800-135	ECC Ephemeral Unified Scheme	P-256, P-384 (corresponding to 128 or 192 bits of security)	TLS Shared Secret Computation and TLS Key Derivation
A1305 C1940	A10 Networks SSL FIPS Library	KAS	SP 800-56Ar3 and SP 800-135	Ephemeral Scheme	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)	TLS, IKE v2, SSH Shared Secret Computation and TLS, IKE v2, SSH Key Derivation
				ECC Ephemeral Unified Scheme	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)	

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2493	A10 Networks Data Plane FIPS Software Library	CVL TLS 1.2	SP 800-135			Key Derivation[3]
C1940	A10 Networks SSL FIPS Library	CVL SNMP, TLS 1.2, SSH				
A1305		CVL SNMP, IKE v.2, TLS 1.2, SSH				
CKG (vendor affirmed)	A10 Networks SSL FIPS Library A10 Networks Data Plane FIPS Software Library	Cryptographic Key Generation	SP 800-133			Key generation[2]

Note 1: Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Note 2: not all CAVS tested modes of the algorithms are used in this module.

[1] The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from SP 800-52, Section 3.3.1. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.

[2] CKG is only used to generate asymmetric keys. The module directly uses the output of the DRBG. The generated seed used in the asymmetric key generation is an unmodified output from DRBG. Section 4, example 1, of SP800-133r2 "Using the Output of a Random Bit Generator" is applicable.

[3] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[4] KTS (AES-GCM Certs. #C1940 and #A1305; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (AES-CBC and CTR Certs. #C1940 and #A1305 and HMAC Certs. #C1940 and #A1305; key establishment methodology provides 128 or 256 bits of encryption strength).

The module also implements other cryptographic algorithms:

Table 4.1: Non-Approved, Not Allowed Cryptographic Algorithms *

Algorithm	Usage
MD5	Used by RADIUS
TLS 1.3	Used by TLS
GCM	Used by IPsec

* Note: These algorithms must not be used in the Approved Mode of Operation.

Table 4.2: Non-Approved, Not Allowed Cryptographic Algorithms (disabled by 'system fips enable' command)

Algorithm	Usage
RSA Encryption/Decryption	Used by TLS
TLS 1.0/1.1 KDF	Used by TLS
GMSSL	Used by TLS
Chacha20-Poly1305	Used by TLS
3DES	Used by TLS and IPsec
DES	Used by IPsec
MD5	Used by IPsec
Not Approved Diffe-Hellman	Used by TLS and IPsec

4 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

Table 5: Ports and Interfaces

Port Name	Count	Interface(s)
Ethernet Port	TH1040:10 1 GE Copper: 6 1/10 GE Fiber (SFP+): 4	Data Input, Data Output, Control Input, Status Output
	TH3350S: 21 1 GE Copper: 7 1 GE Fiber (SFP): 2 1/10 GE Fiber (SFP+): 8 10 GE Fiber (SFP+): 4	
	TH6655S/TH7655S: 18 1 GE Copper: 2 100 GE Fiber (QSFP28): 16	
Serial Console Port	TH1040/TH3350S: 1	Control Input, Status output, Data Output
	TH6655S: 1	
	TH7655S: 2	
USB Ports	2	Disabled
Power Switch	1	Control Input
Power Port	TH1040/TH3350S: 2	Power Input
	TH6655S: 2	
	TH7655S: 2	
LEDs[1]	3	Status Output

[1] Also each Ethernet port uses 2 LEDs

5 Roles, Services and Authentication

The module provides the following roles: a User role and Crypto Officer role. The Crypto Officers initialize and manage the module. Users employ the cryptographic services provided by the module.

The table below provides information on authentication mechanisms employed by each role.

Table 6.1: Authentication Mechanisms

Role	Authentication Mechanism
User	User authentication is certificate based with an RSA key of at least 2048 bits, which corresponds to 112-bit security or a probability of one successful attempt equal to 2^{-112} or ca. $2*10^{-34}$ probability of success. The modules support the maximum of 200,000 user connections per second, even assuming that authentication occurs instantly, this translates to 12,000,000 authentication attempts per minute, and the maximum probability of success is $2.4*10^{-27}$.
Crypto Officer	The minimum requirement for the password strength is eight characters. Any of the 89 characters can be used in any place. Thus, the probability of successfully guessing the password is 89^{-8} or ca. $3*10^{-16}$ per attempt. The modules support three interfaces for password authentication: console and remote (SSH and GUI/HTTPS). In the worst-case scenario console attack can be combined with the most efficient of the two remote interfaces. The probability of succeeding after 1 minute of attempts is computed as the number of guesses within one minute divided by the total number of possible password combinations (still using the minimum password requirements as the reference). *Console access*: console bandwidth is 9600bps (1200Bps). Given an 8-bite password length, this translates to, 150 (=1200/8) guesses per second or *9,000* (=150*60) guesses per minute. *GUI/HTTPS*: the port supports 1Gbps (1,073,741,824bps). One password GUI transaction consumes at least 8,322 bytes (66,576 bits). Thus, the bandwidth supports 967,684 password guesses per minute (1,073,741,824*60/66,576). However, if we

Role	Authentication Mechanism
	take the time of transactions into consideration, we find that each password transaction in testing took at least .29 seconds. Even assuming a 1000 times faster processing rate, the number of transactions per minute is limited to 206,896 attempts (60/.00029). Thus, GUI/HTTPS can handle at most *206,896* attempts per minute. *SSH*: one SSH session takes at least 6,614 bytes. SSH forces termination after three bad attempts at most in a single session. SSH protocol goes over 1Gbps connection. The maximum number of password attempts per minute is 3,652,735 (=1,073,741,824*60*3/(6,614*8)). *The overall number of attempts per minute* is at most 3,661,735 (3,652,735+9,000) using simultaneously console and SSH authentication. The overall 1-minute probability is at most $3{,}661{,}735*89^{-8}$ or ca. $9.3*10^{-10}$. *IPSec PSK*: The module uses IPSec PSK of at least 8 printable characters. The total number of IPSec PSK character combinations is at least 62^8= 218,340,105,584,896. IPSec can also use RSA key of at least 2048 bits, which corresponds to 112-bit security or a probability of one successful attempt equal to 2^{-112} or ca. $2*10^{-34}$ probability of success. IPSec can also use ECDSA key of at least a P-256, which corresponds to 128-bit security or a probability of one successful attempt equal to 2^{-128} or ca. $3*10^{-39}$ probability of success. Therefore, the probability is less than one in 1,000,000 that a random attempt will succeed, or a false acceptance will occur. The time necessary for one IKE handshake limits the number of IKE handshakes in 1 minute to about 60000. Thus, for multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed, or a false acceptance will occur.

The module provides the following services to the operators:

Table 6.2: Roles and Services

Service	Role	Access to Cryptographic Keys and CSPs R- read; W – write or generate; E-execute
Installation of the Module	Crypto Officer	Password: W TLS server certificate: W SSH keys: E DRBG seed: E
Login	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E
Device Management	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E
SSH [1]	Crypto Officer	Password: E SSH Keys: E DRBG seed: E
HTTPS [1]	Crypto Officer	Password: E TLS Keys: E DRBG seed: E
Run self-test [2]	Crypto Officer	N/A
Show status [3]	Crypto Officer	N/A
Reboot [4]	Crypto Officer	N/A
Update firmware	Crypto Officer	Firmware load verification ECDSA SHA-256 firmware load verification key: E
Zeroize	Crypto Officer	All keys: W
Establishment of secure TLS network connection	User	TLS keys: E TLS Certificate: E DRBG seed: E
Establishment of secure IPsec network connection	User	IPsec keys: E DRBG seed: E

[1] KTS is supported in the module via HTTPS and SSH services.
[2] Run self-test by physically power cycling the module or by rebooting the module using its user interface.
[3] Show status by observation of LEDs or by observation of status in the user interface.
[4] Reboot by physically power cycling the module or by rebooting the module using its user interface.

6 Key Management

The following cryptographic keys and CSPs are supported by the module.

Table 7: Cryptographic Keys and CSPs

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
TLS pre-master secret Established using KAS-ECC-SSC	Used to derive TLS master secret	Plaintext in RAM	Never input or output.	
TLS master secret Established using KDF TLS	Used to derive TLS AES encryption key and TLS HMAC key	Plaintext in RAM	Never input or output.	
TLS AES encryption key Established using KDF TLS [3]	Used to encrypt data in TLS protocol	Plaintext in RAM	Never input or output.	128, 256 bits of security
TLS HMAC key Established using KDF TLS [3]	Used to protect integrity of data in TLS protocol	Plaintext in RAM	Never input or output.	160, 256, 384, 512 bits of security
TLS server RSA private key Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
TLS server RSA public key Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
TLS server ECDSA private key Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS server ECDSA public key Established using DRBG or set by operators	Used in TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS EC Diffie-Hellman private key Established using DRBG	Used for key establishment during the TLS handshake	Plaintext in RAM	Never input or output.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
TLS EC Diffie-Hellman public key Established using DRBG	Used for key establishment during the TLS handshake	Plaintext in RAM	Never input. Can be output from the module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
SSH AES encryption key Established using KDF SSH [3]	Used to encrypt SSH data	Plaintext in RAM	Never input or output.	128, 256 bits of security
SSH HMAC key Established using KDF SSH [3]	Used to protect integrity of SSH data	Plaintext in RAM	Never input or output.	160, 256, 512 bits of security

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
SSH RSA private key Established using DRBG or set by operators	Used in SSH handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048 (corresponding to 112 bits of security)
SSH RSA public key Established using DRBG or set by operators	Used in SSH handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048 (corresponding to 112 bits of security)
SSH Diffie-Hellman Private key Established using DRBG	Used for key establishment during the SSH handshake	Plaintext in RAM	Never input or output.	2048 (corresponding to 112 bits of security)
SSH Diffie-Hellman Public key Established using DRBG	Used for key establishment during the SSH handshake	Plaintext in RAM	Never input. Can be output from the module.	2048 (corresponding to 112 bits of security)
IPSec AES encryption key Established using KDF IKE	Used during encryption and decryption of data within the IPSec protocol	Plaintext in RAM	Never input or output.	128, 192, 256 bits of security
IPSec HMAC key Established using KDF IKE	Used to protect integrity of data within the IPSec protocol	Plaintext in RAM	Never input or output.	160, 256, 384, 512 bits of security
IPSec PSK Set by operators	Used for operator authentication	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	>= 8 characters

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
IPsec RSA private key Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of Security)
IPsec RSA public key Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
IPsec ECDSA private key Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
IPsec ECDSA public key Established using DRBG or set by operators	Used in IPsec handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	P-256, P-384, P-521 (corresponding to between 128 and 256 bits of security)
IPSec Diffie-Hellman private key Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input or output.	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)
IPSec Diffie-Hellman public key Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input. Can be output from the module.	MODP-2048, MODP-3072, MODP-4096, MODP-8192 (corresponding to between 112 and 201 bits of security)

Name and type	Usage	Storage	Input/Output	Key Lengths, Curves, or Moduli
IPSec EC Diffie-Hellman private key Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input or output.	P-256, P-384 (corresponding to 128 or 192 bits of security)
IPSec EC Diffie-Hellman public key Established using DRBG	Used during the IPSec handshake to establish the shared secret	Plaintext in RAM	Never input. Can be output from the module.	P-256, P-384 (corresponding to 128 or 192 bits of security)
Certification Authority RSA Certificate Set by operators	Used to verify user certificate during the TLS handshake	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	2048, 3072 (corresponding to 112 or 128 bits of security)
CTR_DRBG CSPs: entropy input, V and Key	Used for generation of random numbers	Plaintext in RAM	Entropy is loaded externally and never output.	Minimum length of the entropy field is 256 bits
Firmware load verification ECDSA public key	Used for firmware load test	Plaintext in RAM Plaintext in flash	Set at the factory. Never output.	P-256 (corresponding to 128 bits of security)
Passwords Set by operators	Used to authenticate operators	Plaintext in RAM Plaintext in flash	Can be input into the module. Never output.	>= 8 characters
SNMP Secret Set by operators	Used to authenticate Crypto Officers accessing SNMP management interface	Plaintext in RAM Plaintext in flash	Can be input into or output from module.	

[1] Entropy is loaded externally. The minimum length of the entropy field is 256 bits. Assuming that the entropy source provides full entropy, the module receives 256 bits of entropy.

[2] Public keys are not considered to be CSPs.

[3] SSH and TLS HMAC and AES keys can be used in key-wrapping.

[4] Input or output for all CSPs is electronic.

[5] Zeroization is performed using “security-reset” command.

7 Self Tests

The module runs a set of self-tests on power-up. If one of the self-tests fails, the module transitions into an error state where all data output and cryptographic operations are disabled.

The module runs power-up self-tests for the following algorithms:

Table 8.1: Power-up Self-Tests

Library/Area	Test
Firmware Integrity Power-up Self Test	Firmware integrity test is performed using MD5 (128-bit) verification.
Power-up Self Test for A10 Networks SSL FIPS Library	For the SSL FIPS Library, tests performed are: 1. AES (with separate encryption and decryption and indicated key sizes) a. CBC, ECB (128-bit) b. GCM (256-bit) 2. SHA a. SHA-1 3. HMAC a. HMAC-SHA-1 b. HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 4. SP800-90A DRBG KAT a. CTR_DRBG: AES 5. RSA KAT (2048-bit key, using SHA-256) 6. ECDSA Pairwise Consistency Test (sign/verify) using P-224, P-256, K-233 and SHA-512 7. KAS-FFC-SSC Primitive "Z" Computation KAT per implementation guidance using 2048-bit key 8. KAS-ECC-SSC Primitive "Z" Computation KAT per implementation guidance using P-256 9. DSA Pairwise Consistency Test (sign/verify) with 2048-bit key and using SHA-384 10. KDF KAT a. KDF-135-SNMP b. KDF-135-TLS c. KDF-135-SSH d. KDF-135-IPsec

Library/Area	Test
Power-up Self Test for A10 Networks Data Plane FIPS Library 1 and 2	For the Data Plane FIPS Libraries, tests performed are: 1. AES (with separate encryption and decryption and indicated key sizes) a. CBC (128-bit) b. GCM (256-bit) 2. SHA a. SHA-1, b. SHA-256, SHA-512 3. HMAC a. HMAC-SHA-1 b. HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 4. RSA KAT (2048-bit key, using SHA-256) 5. ECDSA Pairwise Consistency Test (sign/verify) using P-256 and SHA-512 6. KAS-ECC-SSC Primitive "Z" Computation KAT per implementation guidance using P-256 and P-384
Power-up Self Test for A10 Networks Data Plane FIPS Software Library	For the Data Plane FIPS Software Library, tests performed are: 1. SP800-90A DRBG KAT a. CTR_DRBG: AES 2. KDF KAT a. KDF-135-TLS
Power-up Self Test for A10 Networks IPsec FIPS Library	For the IPsec FIPS Library, tests performed are: 1. AES (with encryption and decryption and indicated key sizes) a. CBC (128, 192, 256-bit) 2. SHA a. SHA-1 b. SHA-256 c. SHA-384 d. SHA-512 3. HMAC a. HMAC-SHA-1 b. HMAC-SHA-256 c. HMAC-SHA-384 d. HMAC-SHA-512

During the module operation the following conditional self-tests are performed:

Table 8.2: Conditional Self-Tests

Library/Area	Condition	Test
Firmware Update	Firmware Load	Firmware Load Test using ECDSA with P-256 and SHA-256
Conditional Self Test for A10 Networks SSL FIPS Library	Random Number Generation /DRBG	Continuous RNG Test
	RSA	Pairwise Consistency Test
	ECDSA	Pairwise Consistency Test
	DSA	Pairwise Consistency Test
	DH Private/Public Key Validation	DH Private/Public Key Validation tests as per SP800-56Ar3 including FFC Full Public-Key Validation Routine
	ECDH Private/Public Key Validation	ECDH Private/Public Key Validation tests as per SP800-56Ar3 including ECC Full Public-Key Validation Routine
	DRBG Health Test	Performed per SP 800-90A Section 11.3
Conditional Self Test for A10 Networks Data Plane FIPS Library 1 and 2	ECDH Private/Public Key Validation	ECDH Private/Public Key Validation tests as per SP800-56Ar3 including ECC Full Public-Key Validation Routine
Conditional Self Test for A10 Networks Data Plane FIPS Software Library	Random Number Generation /DRBG	Continuous RNG Test
	DRBG Health Test	Performed per SP 800-90A Section 11.3

8 Physical Security

The module consists of production-grade components enclosed in a metal enclosure. The enclosure is opaque within the visible spectrum. Sealed containers are used during the shipping of the module. The integrity of the firmware is protected.

The module is protected by tamper evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements. The tamper evident labels are applied at the factory to provide evidence of tampering if a panel is removed.

The Crypto Officer must note the locations of the tamper evidence labels upon receipt of the module. The Crypto Officer must check the integrity of the tamper evident labels periodically thereafter. Upon discovery of tampering the Crypto Officer must immediately disable the module and return the module to the manufacturer.

9 Secure Operation

9.1 Approved Mode of Operation

The module is intended to always operate in the Approved Mode of Operation. Module documentation provides detailed setup procedures and guidance for the users and administrators.

Crypto Officer must execute the following command to enable the approved mode of operation

- system fips enable

Crypto Officer must change its password during the installation.

Configuring any of the following features causes the module to operate in the Non-Approved Mode of Operation.

- RADIUS for administrator authentication
- TLS 1.3
- GCM for IPsec
- “system fips disable” configuration command

Module users and administrators shall keep all authentication data confidential and shall not allow unauthorized access to the module.

10 References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications

Reference	Specification
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions