F5® Device Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Hardware Versions:

BIG-IP i7800 and BIG-IP 10350v-F
with FIPS Kit P/N: F5-ADD-BIG-FIPS140

Firmware Version:

14.1.2

FIPS Security Level 2

Document Version 1.1

Document Revision: February 5, 2021

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

1. Cryptographic Module Specification 4
1.1. Module Description 4
1.2. FIPS 140-2 Validation Level 5
1.3. Description of modes of operation 6
1.4. Cryptographic Module Boundary 10
2. Cryptographic Module Ports and Interfaces........ 11
3. Roles, Services and Authentication........ 13
3.1. Roles 13
3.2. Authentication 14
3.3. Services 15
4. Physical Security........ 21
4.1. Tamper Label Placement 21
5. Operational Environment 23
6. Cryptographic Key Management........ 24
6.1. Key Generation 25
6.2. Key Establishment 25
6.3. Key Entry / Output 25
6.4. Key / CSP Storage 26
6.5. Key / CSP Zeroization........ 26
6.6. Random Number Generation........ 26
7. Self-Tests 27
7.1. Power-Up Tests 27
7.1.1. Integrity Tests 27
7.1.2. Cryptographic algorithm tests 27
7.2. On-Demand self-tests 28
7.3. Conditional Tests 29
8. Guidance 30
8.1. Delivery and Operation........ 30
8.2. Crypto Officer Guidance 30
8.2.1. Installing Tamper Evident Labels........ 30
8.2.2. Install Device........ 30
8.2.3. Password Strength Requirement 31
8.2.4. Additional Guidance 31
8.2.5. Version Configuration........ 32

8.3. User Guidance....32
9. Mitigation of Other Attacks....33

Figure 1 – Hardware Block Diagram....10
Figure 2 – BIG-IP i7800....12
Figure 3 – BIG-IP 10350v-F....12
Figure 4 – BIG-IP i7800 *with tamper labels shown*....22
Figure 5 – BIG-IP 10350v-F with faceplate removed....22
Figure 6 – BIG-IP 10350v-F*, with tamper labels shown .* 22

Table 1 – Tested Modules....5
Table 2 – Security Levels....6
Table 3 – Approved Cryptographic Algorithms....8
Table 4 - Non-Approved but Allowed in FIPS mode Cryptographic Algorithms....9
Table 5 – Non-Approved and Non-Compliant Cryptographic Algorithms/Modes....10
Table 6 – Ports and Interfaces....11
Table 7 – FIPS 140-2 Roles....14
Table 8 – Authentication of Roles....15
Table 9 – Non-Authenticated Services....16
Table 10 – Authenticated Management Services in FIPS mode of operation....18
Table 11 – Crypto Services in FIPS mode of operation....19
Table 12 – Services in non-FIPS mode of operation....20
Table 13 – Inspection of Tamper Evident Labels....21
Table 14 – Number of Tamper Evident Labels per hardware appliance....21
Table 15 – Life cycle of CSPs....24
Table 16 – Self-Tests....28
Table 17 – Conditional Tests....29

Copyrights and Trademarks

F5® and BIG-IP® are registered trademarks of F5 Networks, Inc.
Intel® and Xeon® are registered trademarks of Intel® Corporation.

Introduction

This document is the non-proprietary FIPS 140-2 Security Policy of F5® Device Cryptographic Module with firmware version 14.1.2 and hardware version listed in Table 1. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 2 module.

1.Cryptographic Module Specification

The following section describes the cryptographic module and how it conforms to the FIPS 140-2 specification in each of the required areas.

1.1. Module Description

The F5® Device Cryptographic Module (hereafter referred to as “the module”) is a smart evolution of Application Delivery Controller (ADC) technology. Solutions built on this platform are load balancers. They are full proxies that give visibility into, and the power to control—inspect and encrypt or decrypt—all the traffic that passes through your network.

Underlying all BIG-IP hardware and firmware is F5’s proprietary operating system, Traffic Management Operation System (TMOS), which provides unified intelligence, flexibility, and programmability. With its application control plane architecture, TMOS gives you control over the acceleration, security, and availability services your applications require. TMOS establishes a virtual, unified pool of highly scalable, resilient, and reusable services that can dynamically adapt to the changing conditions in data centers and virtual and cloud infrastructures.

The module has been tested on the hardware platforms listed in Table 1 with the firmware version 14.1.2.

Hardware	Processor	Operating System	Specifications
BIG-IP i7800	Intel® Xeon® E5-1650 v4	TMOS 14.1.2	• 1 x USB port[1] • 8 x 10GbE and 4 x 40GbE network ports • 1 x Console port • 1 x 10/100/1000-BaseT management port • 4 x LEDs • 1 x LCD Display
BIG-IP 10350v-F	Intel® Xeon® E5-2658 v2	TMOS 14.1.2	• 2 x USB port[1] • 16 x 1/10GbE; 2 x 40GbE network ports • 1 x Console port • 1 x 10/100/1000-BaseT management port • 4 x LEDs • 1 x LCD Display

Table 1 – Tested Modules

1.2. FIPS 140-2 Validation Level

For the purpose of the FIPS 140-2 validation, the F5® Device Cryptographic Module is defined as a multi-chip standalone hardware cryptographic module validated at overall security level 2. Table 2 shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standards.

[1] The USB port found on all platforms are used only for exporting the audit logs

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall Level		2

Table 2 – Security Levels

1.3. Description of modes of operation

The module must be installed in the FIPS validated configuration as stated in Section 8 –Guidance. In the operation mode the module supports two modes of operation:

- in "FIPS mode" (the FIPS Approved mode of operation) only approved or allowed security functions with sufficient security strength can be used.
- in "non-FIPS mode" (the non-Approved mode of operation) only non-approved security functions can be used.

The module enters operational mode after power-up self-tests succeed. Once the module is operational, the mode of operation is implicitly assumed depending on the security function invoked and the security strength of the cryptographic keys. Critical Security Parameters (CSPs) used or stored in FIPS mode are not used in non-FIPS mode, and vice versa.

In the FIPS Approved Mode, the cryptographic module will provide the following CAVP certified cryptographic algorithms (Table 3). Not all algorithms/ modes tested are used within the module (i.e. AES-GMAC). The Control (or Management) Plane refers to the connection from an administrator to the BIG-IP for system management. The Data Plane refers to the traffic passed between external entities and internal servers.

Standards/ Algorithm	Usage	Keys/CSPs	Certificate Number	
			Control Plane[2]	Data Plane[3]
[FIPS197] [SP800-38A] [SP800-38D] AES-ECB AES-CBC AES-GCM	Encryption and Decryption	128/192/256-bit AES key	C701	N/A
[FIPS197] [SP800-38A] [SP800-38D] AES-CBC AES-GCM		128/256-bit AES key	N/A	C1306, C1307
[SP800-90A] CTR_DRBG (with AES-256)	Random Number Generation	Entropy input string, seed, V and Key values	C701	C1306, C1307
[FIPS 186-4] RSA	RSA Key Generation	RSA public and private key pair with 2048/3072-bit modulus size	C701	N/A
PKCS#1 v1.5 RSA	RSA Signature Generation and Verification	RSA key pair with 2048/3072-bit modulus, with SHA-1 (for Sign Ver only), SHA-256 and SHA-384	C701	C1306, C1307
[FIPS 186-4] (Appendix B.4.2) ECC Key Pair Generation	ECDSA Key Pair Generation	ECDSA/ ECDH public/ private key pair for P-256 and P-384 curves	C701	C1306, C1307
[FIPS 186-4] ECDSA	ECDSA Signature Generation and Verification	ECDSA key pair (P-256 P- 384 curves) with SHA-1 (for Sign Ver only), SHA-256 and SHA-384	C701	C1306, C1307
[FIPS180-4] SHA-1 SHA-256 SHA-384	Message Digest	N/A	C701	C1306, C1307

[2] For control plane, the BIG-IP i7800 and BIG-IP 10350v-F with processors E5 share the same CAVP certificate.

[3] For data plane, the platform BIG-IP 10350v-F with E5 processor owns the CAVP certificate C1306. The platform BIG-IP i7800 with E5 processor owns the CAVP certificate C1307.

[FIPS 198] HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	Message Authentication	HMAC key (>=112-bit)	C701	C1306, C1307
[SP800-38F] KTS	Key Wrapping/ Key Transport	Modes: AES-GCM, AES-[ECB, CBC] and HMAC 128/192/256-bit AES key	C701	N/A
		Modes: AES-GCM, AES-[ECB, CBC] and HMAC 128/256-bit AES key	N/A	C1306, C1307
Standards/ Algorithm	**Usage**	**Keys/CSPs**	**Certificate Number**	
			Control Plane	**Data Plane**
[SP800-56A] Ephemeral Unified, Section 5.7.1.2 ECC CDH Primitive	Shared Secret Computation used Key Agreement Scheme (KAS)	private Key with P-256 and P-384 curves	C701 (CVL)	C1306 (CVL) C1307 (CVL)
[SP800-135] KDF in SSH[4]	Key Derivation	Session encryption and data authentication keys	C701	N/A
TLS[4] 1.0/1.1/1.2 with SHA-256 and SHA-384			C701	C1306, C1307,

Table 3 – Approved Cryptographic Algorithms

The following table lists the non-Approved algorithms that are allowed in FIPS approved mode along with their usage.

Algorithm	**Usage**	**Keys/CSPs**	**Interface**	
			Control Plane	**Data Plane**
EC Diffie-Hellman	Key Agreement	private key with P-256 and P-384 curves	Non-Approved but Allowed	
PKCS#1 v1.5 RSA Key Wrapping	Asymmetric Encryption and Decryption	RSA key pair with 2048/ 3072-bit modulus.	Non-Approved but Allowed	

[4] No parts of the SSH and TLS protocols except the KDF has been reviewed or tested by the CAVP and CMVP

NDRNG	Seeding DRBG	seed	Non-Approved but Allowed

Table 4 – Non-Approved but Allowed in FIPS mode Cryptographic Algorithms

The following table lists the non-FIPS Approved algorithms along with their usage.

Algorithm	Usage	Notes
AES	Symmetric Encryption and Decryption	using OFB, CFB, CTR, XTS[5] and KW modes
DES RC4 Triple-DES SM2 SM4		N/A
RSA	Asymmetric Encryption and Decryption	using modulus sizes less than 2048-bits or greater than 3072 bits
RSA	Asymmetric Key Generation	FIPS 186-4 less than 2048-bit modulus size or greater than 3072 bits
DSA		using any key size
ECDSA ECDH		using public/private key pair for curves other than P-256 and P-384
RSA	Digital Signature Generation and Verification	PKCS#1 v1.5 using key sizes other than 2048 and 3072 bits
		PKCS#1 v1.5 using 2048, 3072 bits modulus with SHA-1 (for Sig Gen), SHA-224 and SHA-512
		using X9.31 standard
		using Probabilistic Signature Scheme (PSS)
DSA		using any key size and SHA variant
ECDSA		FIPS 186-4 using curves other than P-256 and P-384, all SHA sizes
		FIPS 186-4 using curves P-256 and P-384 with SHA-1, SHA-224 and SHA-512
SHA-224 SHA-512 MD5 SM3	Message Digest	N/A
HMAC-SHA-224 HMAC-SHA-512	Message Authentication	N/A

[5] The AES-XTS mode shall only be used for the cryptographic protection of data on storage devices and shall not be used for other purposes such as the encryption of data in transit.

AES-CMAC Triple-DES-CMAC		
Diffie-Hellman	Key Agreement Scheme (KAS)	N/A
ECDH		using curves other than P-256 and P-384
TLS KDF	Key Derivation function	Using SHA-1/SHA-224/SHA-512
SSH KDF		
SNMP KDF		using any SHA variant
IKEv1 and IKEv2 KDF		

Table 5 – Non-Approved and Non-Compliant Cryptographic Algorithms/Modes

1.4. Cryptographic Module Boundary

The cryptographic boundary of the module is defined by the exterior surface of the appliance (red dotted line in Figure 1). The block diagram below shows the module, its interfaces with the operational environment and the delimitation of its logical boundary. Figure 1 also depicts the flow of status output (SO), control input (CI), data input (DI) and data output (DO). Description of the ports and interfaces can be found in *Table 5 – Ports and Interfaces*.

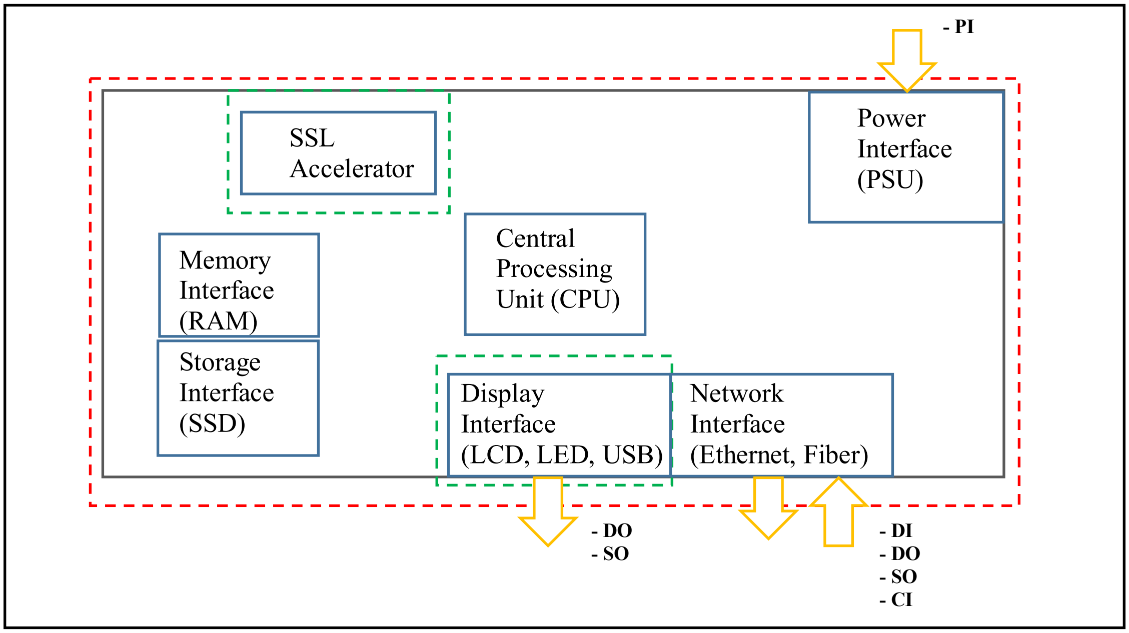

Figure 1 – Hardware Block Diagram

2. Cryptographic Module Ports and Interfaces

For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which it runs.

The logical interfaces are the commands through which users of the module request services. The following table summarizes the physical interfaces with details of the FIPS 140-2 logical interfaces they correspond to.

Logical Interface	Physical Interface	Description
Data Input	• Network Interface	Depending on module, the network interface consists SFP, SFP+, and QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 40Gbps.
Data Output	• Network Interface • Display Interface	Depending on module, the network interface consists SFP, SFP+, and QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 40Gbps. In addition, Status logs may be output to USB found in the interface.
Control Input	• Display Interface • Network Interface	The control input found in the display interface includes the power button and reset button. The control input found in the network interface includes the API which control system state (e.g. reset system, power-off system).
Status Output	• Display Interface	Depending on model, the display interface can consist of a LCD display, LEDs, and/or output to STDOUT which provides system status information.
Power Input	• Power Interface	Removable PSU (x2)

Table 6 – Ports and Interfaces

Figure 2 and Figure 3 show the various modules that were tested. Please use the images to familiarize yourself with the devices.

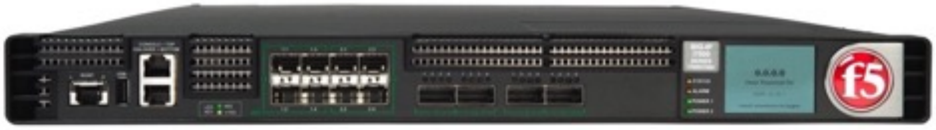

Figure 2 – BIG-IP i7800

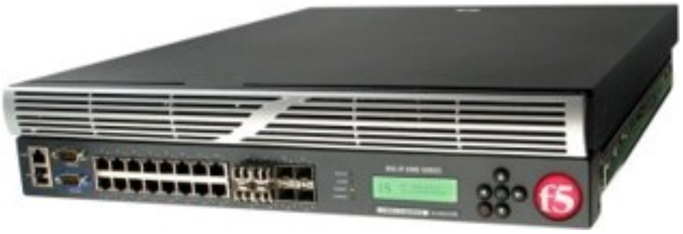

Figure 3 – BIG-IP 10350v-F

3. Roles, Services and Authentication

3.1. Roles

The module supports roles-based authentication. The FIPS 140-2 roles are defined below and purpose of role are described in the Table 7.

- User role: Performs cryptographic services (in both FIPS mode and non-FIPS mode), key zeroization, module status requests, and on-demand self-tests. The FIPS140-2 User role is mapped to multiple BIG-IP roles which are responsible for different components of the system (e.g. auditing, certificate and key management, user management, etc.). The User can access the module through Command Line Interface (CLI) or Web Interface. However, the CO can restrict User role access to the CLI. In that case the User will have access through Web Interface only.
- Crypto Officer (CO) role: Crypto officer is represented by the administrator of the BIG-IP. This entity performs module installation and initialization. This role has full access to the system and has the ability to create, delete, and manage other User roles on the system.

The module supports concurrent operators belonging to different roles (one CO role and one User role) which creates two different authenticated sessions, achieving the separation between the concurrent operators.

Two interfaces can be used to access the module:

- CLI: The module offers a CLI called traffic management shell (tmsh) which can be accessed remotely using the SSHv2 secured session over the Ethernet ports.
- Web Interface: The Web interface consists of HTTPS over TLS interface which provides a graphical interface for system management tools. The Web interface can be accessed from a TLS-enabled web browser.

Note: The module does not maintain authenticated sessions upon power cycling. Power-cycling the system requires the authentication credentials to be re-entered. Authentication data is protected against unauthorized disclosure, modification and substitution by the Operating System. Additionally, when entering authentication data through the Web interface, any character entered will be obfuscated (i.e. replace the character entered with a dot on the entry box). When entering authentication data through the CLI, the module does not display any character entered by the operator in stdin (e.g. keyboard).

FIPS 140-2 Role	BIG-IP Role	Purpose of Role
Crypto Officer	Administrator	Main administrator of the of the BIG-IP system. This role has complete access to all objects on the system. Entities with this role cannot have other roles on the system.
User	Auditor	Entity who can view all configuration data on the system, including logs.

FIPS 140-2 Role	BIG-IP Role	Purpose of Role
	Certificate Manager	Entity who manages digital certificates and Keys.
	Firewall Manager	Grants a user permission to manage all firewall rules and supporting objects. Notably, the Firewall Manager role has no permission to create, update, or delete non-network firewall configurations, including Application Security or Protocol Security policies
	iRule Manager	Grants a user permission to create, modify, view, and delete iRule. Users with this role cannot affect the way that an iRule is deployed.
	Operator	Grants a user permission to enable or disable nodes and pool members.
	Resource Manager	Grants a user access to all objects on the system except BIG-IP user accounts. With respect to user accounts, a user with this role can view a list of all user accounts on the system but cannot view or change user account properties except for their own user account. Users with this role cannot have other user roles on the system.
	User Manager	Entity who manages BIG-IP crypto officer and user accounts. Create, Modify, view, Enable or disable terminal access for any user account.

Table 7 – FIPS 140-2 Roles

3.2. Authentication

FIPS 140-2 Role	Authentication type and data	Strength of Authentication (Single Attempt)	Strength of Authentication (Multiple-Attempt)
Crypto Officer	Password based (CLI or Web Interface)	The password must consist of minimum of 6 characters with at least one from each of the three character classes. Character classes are defined as: digits (0-9), ASCII lowercase letters (a-z), ASCII uppercase letters (A-Z). Assuming a worst-case scenario where the password contains four digits, one ASCII lowercase letter and one ASCII uppercase letter. The probability to guess every character successfully is (1/10) ^4 * (1/26)^1 * (1/26)^1 = 1/6,760,000 which is much smaller than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/6,760,000 which is less than the requirement of 1/100,000.

FIPS 140-2 Role	Authentication type and data	Strength of Authentication (Single Attempt)	Strength of Authentication (Multiple-Attempt)
	Signature Verification (CLI only)	The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is 1/(2^{112}) which is less than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/(2^{112}) which is less than the requirement of 1/100,000.
User	Password based (CLI and Web Interface)	The password must consist of minimum of 6 characters with at least one from each of the three character classes. Character classes are defined as: digits (0-9), ASCII lowercase letters (a-z), ASCII uppercase letters (A-Z). Assuming a worst-case scenario where the password contains four digits, one ASCII lowercase letter and one ASCII uppercase letter. The probability to guess every character successfully is (1/10) ^4 * (1/26)^1 * (1/26)^1 = 1/6,760,000 which is much smaller than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/6,760,000 which is less than the requirement of 1/100,000.
	Signature Verification (CLI only)	The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is 1/(2^{112}) which is less than 1/1,000,000.	The maximum number of login attempts is limited to 6 after which the account is locked. This means that at worst case an attacker has the probability of guessing the password in one minute as 6/(2^{112}) which is less than the requirement of 1/100,000.

Table 8 – Authentication of Roles

3.3. Services

The module provides services to users that assume one of the available roles. All services are described in detail in the user documentation.

Table 9 lists the module’s Services that can be performed without authentication.

Service	Usage/Notes
Show Status	Displays system status information over LCD screen (e.g. network info, system operational status, etc.).
Self-Tests	When the BIG-IP system has been started, the self-tests are performed. This includes the integrity check and Known Answer Tests. On-Demand self-tests are initiated by manually power cycling the system.

Table 9 – Non-Authenticated Services

Table 10 lists the services for the management of the module available in FIPS mode of operation which are only available after the authentication has succeeded. The Services, the Roles that can request the Service and the CSPs involved and how the CSPs are accessed (Read / Write / Zeroize - R, W, Z –) are listed.

Service / Description	**Keys-CSPs**	**Access Type (R, W, Z)**	**Authorized Role**	
			Crypto Officer	**User**
User Management Services				
List Users Display list of users	N/A	N/A	✓	User Manager Resource Manager Auditor
Create additional User	password	W	✓	User Manager
Modify existing Users	N/A	N/A	✓	User Manager
Delete User	password	Z	✓	User Manager
Unlock User Remove Lock from user who has exceeded login attempts	N/A	N/A	✓	User Manager
Update own password	password	W	All Roles	
Update others password	password	W	✓	User Manager
Configure Password Policy Set password policy features	N/A	N/A	✓	None
Certificate and Keys Management Services				
Create / Delete SSL Certificate a self-signed certificate	TLS RSA/ECDSA private Key	W (for Create only)/ R (for Create only) / Z (for Delete only)	✓	Certificate Manager Resource Manager

Service / Description	Keys-CSPs	Access Type (R, W, Z)	Authorized Role	
			Crypto Officer	User
Create/ Delete SSL Key used for the SSL Certificate key file	TLS RSA/ECDSA private Key	W (for Create only)/ R (for Create only) / Z (for Delete only)	✓	Certificate Manager Resource Manager
List Certificate Display / log expiration date of installed certificates	N/A	N/A	✓	Auditor Certificate Manager Resource Manager
List private keys	N/A	N/A	✓	Auditor Certificate Manager Resource Manager
Import SSL Certificate	N/A	N/A	✓	Certificate Manager
Export Certificate File	N/A	N/A	✓	Certificate Manager
ssh-keyswap utility service utility to create or delete ssh keys	Session encryption and authentication keys, ECDH shared secret	R, W	✓	Certificate Manager
Firewall Management Services				
Configure firewall settings policy rules, and address-lists for use by firewall rules.	N/A	N/A	✓	Firewall Manager
Show firewall state the current system-wide state of firewall rules	N/A	N/A	✓	Firewall Manager
Show statistics of firewall rules on the BIG-IP system	N/A	N/A	✓	Firewall Manager
Audit Management Services				
View System Audit service logs	N/A	N/A	✓	Auditor Resource Manager
Export Analytics Logs system	N/A	N/A	✓	Auditor
Enable/ Disable Audit	N/A	N/A	✓	Auditor
System Management Services				
Configure Boot Options Enable Quit boot, manage boot locations	N/A	N/A	✓	Resource Manager

Service / Description		Keys-CSPs	Access Type (R, W, Z)	Authorized Role	
				Crypto Officer	User
Configure SSH access options	Enable/Disable SSH access, Configure IP address whitelist	N/A	N/A	✓	Resource Manager
	Update private key for user authentication	SSH RSA/ECDSA private keys	R, W	✓	User Manager Resource Manager
Configure Firewall Users		N/A	N/A	✓	Firewall Manager
Configure nodes and pool members	Enable / Disable nodes and pool members	N/A	N/A	✓	Operator
Configure iRules	create, modify, view, and delete iRules	N/A	N/A	✓	iRule Manager Resource Manager
Reboot System	Restart cryptographic module	N/A	N/A	✓	Resource Manager
Secure Erase	Full system zeroization	All CSPs in Table 15	W, Z	✓	None

Table 10 – Authenticated Management Services in FIPS mode of operation

Table 11 lists the TLS and SSH crypto Services available in FIPS mode of operation, the Roles that can request the Service, the algorithms and the CSPs involved and how the CSPs are accessed (Read/Write/Zeroize - R, W, Z).

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type	Interface	
SSH Services					Data Plane	Control Plane
Establish SSH Session	Signature generation and verification: ECDSA with SHA-256/SHA-384 and curve P-256/P-384 RSA with SHA-256/SHA-384 and 2048/3072-bit key size	User CO	RSA/ECDSA Key Pair	R		Yes

Service	Algorithms / Key Sizes	Role	Keys/CSPs	Access Type	Interface	
	Key Exchange: EC Diffie-Hellman		EC Diffie-Hellman key pair, shared secret	R, W		
	Key Derivation: SP800-135 SSH KDF		Session encryption keys EC Diffie-Hellman shared secret	R, W		
Maintain SSH Session	Data Encryption and Decryption: AES (CBC mode)	User CO	Session encryption keys	R		Yes
	Data Integrity (MAC): HMAC with SHA-1		Session data authentication keys	R, W		
Close SSH Session	N/A	User CO	Zeroize session keys and shared secret	Z		Yes
TLS Services					**Data Plane**	**Control Plane**
Establish TLS session	Signature Generation and Verification: RSA or ECDSA with SHA-256/SHA-384	User CO	RSA, ECDSA key pairs	R, W	Yes	Yes
	Key Exchange: ECDH with SP800-135 TLS KDF, RSA Key wrapping (allowed)		RSA, ECDH Key pair, TLS pre-master secret and master secret	R, W	Yes	Yes
Maintaining TLS session	Data Encryption: AES CBC, GCM Data Authentication: HMAC SHA-1/SHA-256/SHA-384	User CO	AES and HMAC Keys	R, W	Yes	Yes
Closing TLS session	N/A	User CO	Session keys, shared secret	Z	Yes	Yes

Table 11 – Crypto Services in FIPS mode of operation

Table 12 lists all of the non-Approved Services available in the non-FIPS-Approved mode of operation.

Service	Role	Usage/Notes
TLS Services		
Establishing TLS session	User/ CO	Signature generation and verification using DSA or RSA/ECDSA with SHA-1/SHA-224/SHA-512 RSA with keys less than 2048
		Key Exchange using: Diffie-Hellman RSA Key wrapping with keys less than 2048
Maintain TLS session		Data encryption using Triple-DES, AES-CTR, AES-GCM Data authentication using HMAC SHA-224/SHA-512
SSH Services		
Establish SSH session	User/ CO	Signature generation and verification using: DSA, Ed25519 RSA/ECDSA with SHA-1/SHA-224/SHA-512 RSA with key size less than 2048-bit Key exchange using Diffie-Hellman, Ed25519
Maintain SSH session		Data encryption using Triple-DES Data authentication using HMAC SHA-1/SHA-224/SHA-512
Other Services		
IPsec	User/ CO	The configuration and usage of IPsec is not approved
iControl REST access		Access to the system through REST using non-approved crypto from BouncyCastle
Configuration using SNMP		Management of the module via SNMP is not approved.

Table 12 – Services in non-FIPS mode of operation

4. Physical Security

All of the modules listed in Table 1 are enclosed in a hard-metallic production grade case that provides obscurity and prevents visual inspection of internal components. Each module is fitted with tamper evident labels to provide physical evidence of attempts to gain access inside the case. The tamper evident labels shall be installed for the module to operate in approved mode of operation. The Crypto Officer is responsible for inspecting the quality of the tamper labels on a regular basis to confirm that the modules have not been tampered with. In the event that the tamper evident labels require replacement, a kit providing 25 tamper labels is available for purchase (P/N: F5-ADD-BIG-FIPS140). The Crypto Officer shall be responsible for the storage of the label kits.

Physical Security Mechanism	Recommended Inspection Frequency	Guidance
Tamper Evident Labels	Once per month	Check the quality of the tamper evident labels for any sign of removal, replacement, tearing, etc. If any label is found to be damaged or missing, contact the system administrator immediately.

Table 13 – Inspection of Tamper Evident Labels

4.1. Tamper Label Placement

The details below show the location of all tamper evident labels for each hardware appliances. Label application instructions are provided in section 8.2 Crypto-office guidance

Hardware Appliance	# of Tamper Labels
BIG-IP i7800	4
BIG-IP 10350v-F	4

Table 14 – Number of Tamper Evident Labels per hardware appliance

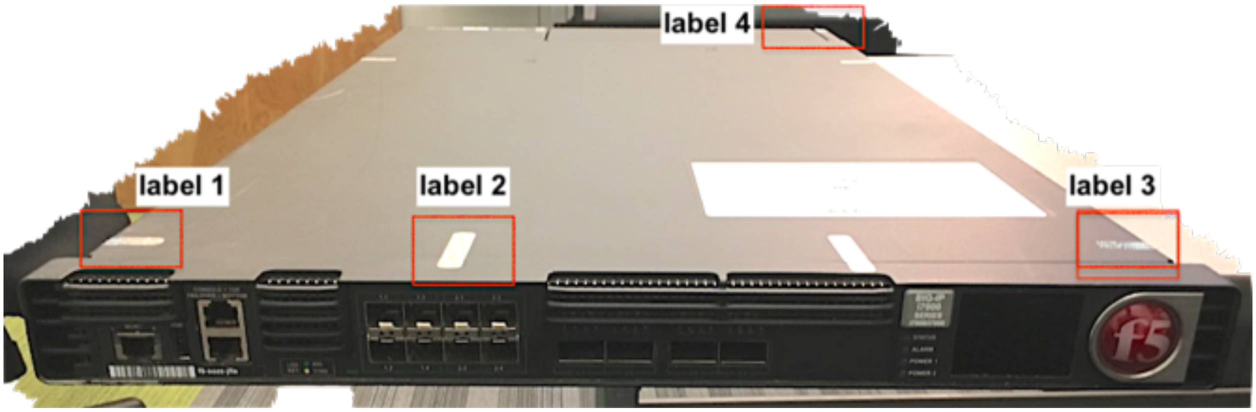

Figure 4 – BIG-IP i7800 *with tamper labels shown*

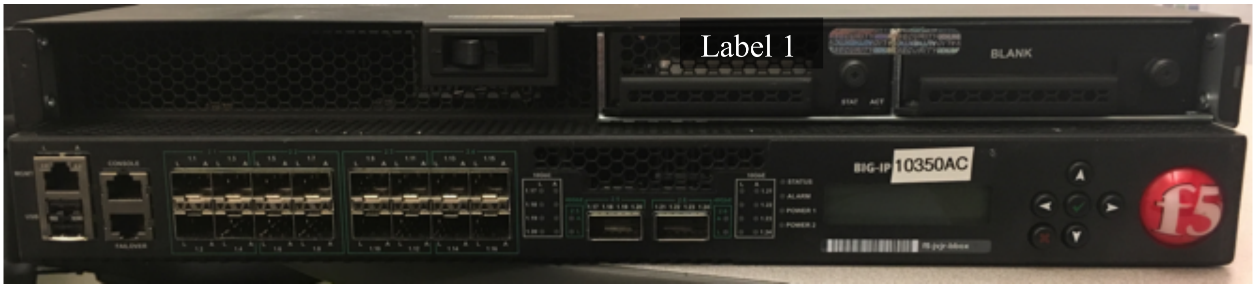

Figure 5 – *BIG-IP 10350v-F with faceplate removed*

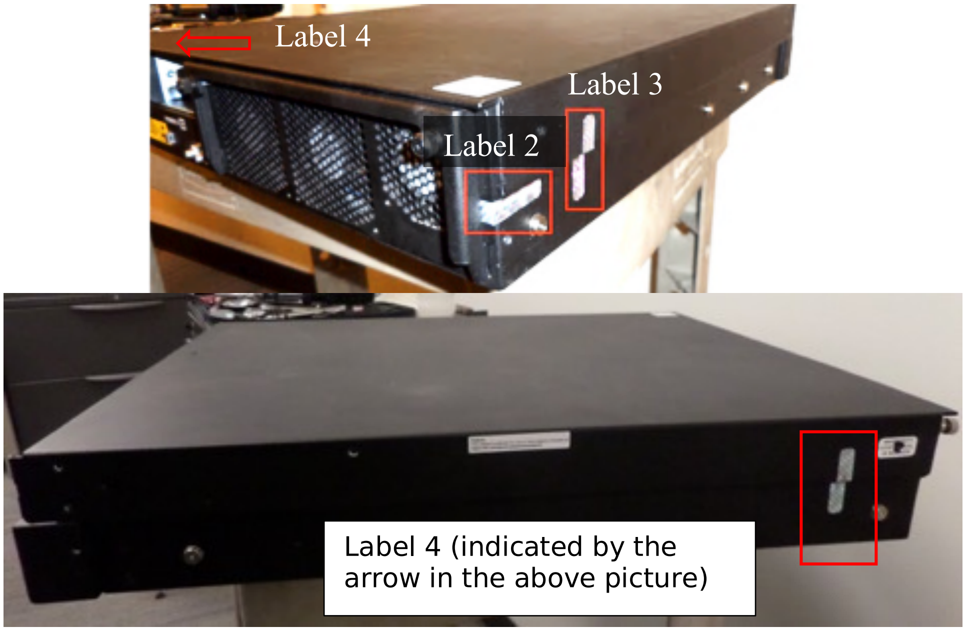

Figure 6 – BIG-IP 10350v-F, *with tamper labels shown .*

5. Operational Environment

The module operates in a non-modifiable operational environment per FIPS 140-2 level 2 specifications and as such the operational environment requirements do not apply.

6. Cryptographic Key Management

Table 15 summarizes the key and CSPs that are used by the cryptographic services implemented in the module. Sizes for the listed keys are given in Table 3 and Table 4 section 1.3.

Key / CSPs	Generation	Storage	Zeroization
DRBG entropy input string, seed	Obtained from NDRNG.	RAM	Zeroized by device reboot
DRBG V and Key values	Derived from entropy string as defined by [SP800-90A]	RAM	
TLS RSA key pair	Generated using [FIPS 186-4] Key generation method. The random value used in the key generation is generated using [SP800-90A] DRBG.	Disk	Zeroized when key file is deleted or by secure erase option at boot.
TLS ECDSA key pair			
TLS EC Diffie-Hellman key pair		RAM	Zeroized by closing TLS session or by rebooting the device.
TLS Pre-Master Secret and Master Secret	Established during the TLS handshake	RAM	Zeroized by closing TLS session or by or rebooting the device.
Derived TLS session key (AES, HMAC)	Derived from the master secret via [SP800-135] TLS KDF		
SSH Shared Secret	Established during the SSH handshake	RAM	Zeroized by closing SSH session or terminating the SSH application or rebooting the device.
Derived SSH session key (AES, HMAC)	Derived from the shared secret via [SP800-135] SSH KDF	RAM	
SSH EC Diffie-Hellman Key pair	Generated using [FIPS 186-4] Key generation method. The random value used in the key generation is generated using [SP800-90A] DRBG.	RAM	
SSH RSA Key pair		Disk	Zeroized using ssh-keyswap utility or by secure erase option at boot.
SSH ECDSA Key pair			
User Password	Entered by the user	Disk	Zeroized by secure erase option at boot or overwritten when password is changed
Crypto Officer Password	Entered by the Crypto Officer	Disk	Zeroized by secure erase option at boot or overwritten when password is changed

Table 15 – Life cycle of CSPs

The following sections describe how CSPs, in particular cryptographic keys, are managed during its life cycle.

6.1. Key Generation

The module implements RSA and EC asymmetric key generation services compliant with [FIPS186-4], and using [SP800-90A] DRBG.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP800-133r1] (vendor affirmed).

The module does not implement symmetric key generation as an explicit service. The HMAC and AES symmetric keys are derived from shared secret by applying [SP 800-135] as part of the TLS/SSH protocol. The scenario maps to the [SP 800-133r1] section 6.3 symmetric keys generated using Key Agreement Schemes.

6.2. Key Establishment

The module provides the following key establishment services:

- RSA Key wrapping scheme is used as part of TLS protocol.
- EC Diffie-Hellman key agreement scheme is used as part of the TLS and SSH Protocol with the key derivation implemented by [SP 800-135] TLS and SSH KDF.
- [SP 800-38F] key wrapping in the context of TLS and SSH protocol where a key may be within a packet or message that is encrypted and authenticated using approved authenticated encryption mode i.e. AES GCM or a combination method which includes approved symmetric encryption algorithm i.e. AES together with approved authentication method i.e. HMAC-SHA.

These schemes provide the following security strength in FIPS mode:

- RSA key wrapping provides between 112 or 128-bits of encryption strength
- EC Diffie-Hellman key agreement provides 128 or 192-bits of encryption strength
- [SP 800-38F] key wrapping using approved authenticated encryption mode (i.e. AES-GCM) provides between 128 and 256 bits of encryption strength (AES Cert. #C701)
- [SP 800-38F] key wrapping using a combination of approved AES encryption and HMAC authentication method provides between 128 and 256 bits of encryption strength (AES and HMAC Cert. #C701)
- [SP 800-38F] key wrapping using approved authenticated encryption mode (i.e. AES GCM) provides 128 or 256 bits of encryption strength (AES Certs. #C1306 and #C1307)
- [SP 800-38F] key wrapping using a combination of approved AES encryption and HMAC authentication method provides 128 or 256 bits of encryption strength (AES and HMAC Certs. #C1306 and #C1307)

6.3. Key Entry / Output

The module does not support manual key entry or intermediate key generation key output. During the TLS/SSH handshake, the keys that are entered or output to the module over the network, includes RSA/ECDSA public keys and the TLS pre-master secret encrypted with RSA key only when using the RSA key exchange with TLS. For TLS with ECDH key exchange, the TLS pre-master secret is established during key agreement and is not output from the module. Once the TLS/SSH session is established, any key or data transfer performed thereafter is protected by AES encryption.

6.4. Key / CSP Storage

As shown in Table 15. the keys stored in the volatile memory (RAM) in plaintext form and are destroyed when released by the appropriate zeroization calls or when the system is rebooted. The keys stored in plaintext in non-volatile memory (SSD) are static and will remain on the system across power cycle and are only accessible to the authenticated administrator.

6.5. Key / CSP Zeroization

The zeroization methods listed in Table 15, overwrites the memory occupied by keys with “zeros”. Additionally, the user can enforce it by performing procedural zeroization. For keys present in volatile memory, calling reboot command will clear the RAM memory. For keys present in non-volatile memory, using secure erase option (can only be triggered by the administrator during reboot of the device) will perform single pass zero write erasing the disk contents.

6.6. Random Number Generation

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800-90A] for the generation of random value used in asymmetric keys, and for providing an RNG service to calling applications. The Approved DRBG provided by the module is the CTR_DRBG with AES-256. The DRBG is initialized during module initialization. The module performs the health tests for the SP800 90A DRBG as defined per section 11.3 of SP800-90A.

The module uses a Non-Deterministic Random Number Generator (NDRNG) to seed the DRBG. A Continuous Random Number Generation Test (CRNGT) is performed on the output of the NDRNG prior to seeding the DRBG and also on the DRBG output. The NDRNG provides at least 256 bits of entropy to the DRBG during initialization (seed) and reseeding (reseed). The NDRNG is within its physical boundary.

7. Self-Tests

7.1. Power-Up Tests

The module performs power-up tests automatically during initialization when the device is booted without requiring any operator intervention; power-up tests ensure that the module's firmware is not corrupted and that the cryptographic algorithms work as expected.

During the execution of power-up tests, services are not available and input and output are inhibited. Upon successful completion of the power-up tests, the module is initialized and enters operational mode where it is accessible for use. If the module fails any of the power-up tests, it enters into the "Halt Error" state and halts the system. In this state, the module will prohibit any data outputs and cryptographic operations and will not be available for use. The module will be marked unusable and the administrator will need to reinstall the module to continue.

7.1.1. Integrity Tests

The integrity of the module is verified by comparing the MD5 checksum value of the installed binaries calculated at run time with the stored value computed at build time. If the values do not match the system enters halt error state and the device will not be accessible. In order to recover from this state, the module needs to be reinstalled.

7.1.2. Cryptographic algorithm tests

The module performs self-tests on all FIPS-Approved cryptographic algorithms supported in the approved mode of operation and is done on the Data Plane as well as Control Plane side, using the Known Answer Test (KAT) and Pair-wise Consistency Test (PCT) as listed in the following table:

Algorithm	Test
Control Plane Self-tests	
CTR_DRBG	• KAT using AES 256-bit with and without derivation function
AES	• KAT of AES encryption with GCM mode and 128-bit key • KAT of AES encryption and decryption performed separately with ECB mode and 128-bit key
RSA	• KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA-256 • KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA-256
ECDSA	• PCT of ECDSA signature generation and verification with P-256 curve

Algorithm	Test
EC Diffie-Hellman	• primitive “Z” computation KAT with P-256 curve
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	• KAT of HMAC-SHA-1 • KAT of HMAC-SHA-256 • KAT of HMAC-SHA-384
SHA-1, SHA-256, SHA-384	• Covered by respective HMAC KATs
Data Plane Self-Tests	
AES	• KAT of AES encryption with GCM mode and 128-bit key • KAT of AES encryption /decryption with CBC mode and 128-bit key
RSA	• KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA-256 • KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA-256
ECDSA	• PCT of ECDSA signature generation and verification with P-256 curve
EC Diffie-Hellman	• primitive “Z” computation KAT with P-256 curve
CTR_DRBG	• Covered by Control Plane Self-Tests. (Data Plane makes use of the same DRBG implementation provided by Control Plane)
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	• KAT of HMAC-SHA-1 • KAT of HMAC-SHA-256 • KAT of HMAC-SHA-384
SHA-1, SHA-256, SHA-384	• Covered by respective HMAC KATs

Table 16 – Self-Tests

7.2. On-Demand self-tests

The module does not explicitly provide the Self-Test service to perform on demand self-tests. On demand self-tests can be invoked by powering-off and powering-on the system in order to initiate the same cryptographic algorithm tests executed during power-up. During the execution of the on-demand self-tests, crypto services are not available, and no data output or input is possible.

7.3. Conditional Tests

The module performs conditional tests on the cryptographic algorithms shown in the following table. If the module fails any of these tests, the device reboots and enters into the “Halt Error” state prohibiting any data output or cryptographic operations and the module will be inoperable. The module must be re-installed in order to clear the error condition.

Algorithm	Test
DRBG	• CRNGT on the output of the DRBG
NDRNG	• CRNGT on the output of the NDRNG prior to seeding the CTR_DRBG
RSA key generation	• PCT using SHA-256
ECDSA key generation	• PCT using SHA-256

Table 17 – Conditional Tests

8. Guidance

8.1. Delivery and Operation

The module is distributed as a part of a BIG-IP product which includes the hardware and an installed copy of 14.1.2. The hardware devices are shipped directly from the hardware manufacturer/authorized subcontractor via trusted carrier and tracked by that carrier. The hardware is shipped in a sealed box that includes a packing slip with a list of components inside, and with labels outside printed with the product nomenclature, sales order number, and product serial number. Upon receipt of the hardware, the customer is required to perform the following verifications:

- Ensure that the shipping label exactly identifies the correct customer name and address as well as the hardware model.
- Inspect the packaging for tampering or other issues.
- Ensure that the external labels match the expected delivery and the shipped product.
- Ensure that the components in the box match those on the documentation shipped with the product.
- The hardware model can be verified by the model number given on the shipping label as well as on the hardware device itself.

For FIPS compliance, the following steps defined in section 8.2 should be completed by the Crypto Officer prior to access to the device is allowed.

8.2. Crypto Officer Guidance

8.2.1. Installing Tamper Evident Labels

Before the device is installed in the production environment, tamper-evident labels must be installed in the location identified for each module in section 4.1. The following steps should be taken when installing or replacing the tamper evident labels on the module. The instructions are also included in *F5 Platforms: FIPS Kit Installation* provided with each module.

- Use the provided alcohol wipes to clean the chassis cover and components of dirt, grease, or oil before you apply the tamper evidence seals.
- After applying the seal, run your finger over the seal multiple times using extra high pressure.
- The seals completely cure within 24 hours.

It is the responsibility of the Crypto Officer to inspect the tamper evident labels for damage or any missing labels as specified in Section 4.

8.2.2. Install Device

Follow the instructions in the "*BIG-IP System: Initial Configuration*" guide for the initial setup and configuration of the device.

- Run the Setup wizard to license and provision the BIG-IP system.
- Activate the Base Registration Key provided with the purchase of the BIG-IP platform.
- Add the FIPS license. Installing the FIPS license for the host system is required for module activation. Guidance on Licensing the BIG-IP system can be found in https://support.f5.com/csp/article/K7752 and summarized as followed: Before you can activate the license for the BIG-IP system, you must obtain a base registration key. The base registration key is pre-installed on new BIG-IP systems. When you power up the product and connect to the Configuration utility, the Licensing page opens and displays the registration key. After a license activation method is selected (activation method specifies how you want the system to communicate with the F5 License Server), the F5 product generates a dossier which is an encrypted list of key characteristics used to identify the platform. If the automated activation method is selected, the BIG-IP system automatically connects to the F5 License Server and activates the license. If the manual method is selected, the Crypto Officer shall go to the F5 Product Licensing page at secure.f5.com, paste the dossier in the “Enter Your Dossier” box which produces a license. The Crypto Officer will then copy and paste it into the “License” box in the Configuration Utility. The BIG-IP system then reloads the configuration and is ready for additional system configuration. This concludes the product licensing.

8.2.3. Password Strength Requirement

The Crypto officer must modify the BIG-IP password policy to meet or exceed the requirements defined in Table 7 – Authentication of Roles. Instructions for this can be found in the “*BIG-IP System: User Account Administration*” guide. After assuming the role for the first time, the Crypto Officer shall replace the default password with one matching the password policy.

8.2.4. Additional Guidance

The Crypto Officer should verify that the following specific configuration rules are followed in order to operate the module in the FIPS validated configuration.

- All command shells other than tmsh are not allowed. For example, bash and other user-serviceable shells are excluded.
- Management of the module via the appliance's LCD display is not allowed.
- Usage of f5-rest-node and iAppLX and provisioning of iRulesLX is not allowed.
- Only the provisioning of AFM and LTM is included.
- Remote access to the Lights Out / Always On Management capabilities of the system are not allowed.
- Serial port console should be disabled after the initial power on and communications setup of the hardware.
- Use of command *run util fips-util -f init* is not allowed. Running this command followed by a system reboot or restart will mean that the module is not operating as a FIPS validated module.

8.2.5. Version Configuration

Once the device is installed, licensed and configured, the Crypto Officer should confirm that the system is installed and licensed correctly.

8.2.5.1. Version Confirmation

The Crypto Officer should run the command "tmsh show sys version", then confirm that the provided version matches the validated version shown in Table 1 - Tested Modules. Any firmware loaded into the module other than version 14.1.2 is out of the scope of this validation and will mean that the module is not operating as a FIPS validated module.

8.2.5.2. License Confirmation

The FIPS validated module activation requires installation of the license referred as ‘FIPS license’. The Crypto Officer should run the command "tmsh show sys license", then verify that the list of license flags includes the "FIPS 140-2 Compliant Mode”.

8.3. User Guidance

The module supports two modes of operation*. Table 11 – Crypto Services in FIPS mode of* operation lists the FIPS approved services and *Table 12 – Services in non-FIPS mode of operation* lists the non-FIPS approved services. Using the non-FIPS approved algorithm or mode in *Table 5 – Non-Approved and Non-Compliant Cryptographic Algorithms/Modes* means that the module operates in non-FIPS Approved mode for the particular session of a particular service.

AES-GCM IV is constructed in accordance with SP800-38D in compliance with IG A.5 scenario 1. The implementation of the nonce_explicit management logic inside the module ensure that when the IV exhausts the maximum number of possible values for a given session key, the module triggers a new handshake request to establish a new key. In case the module’s power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-distributed. The AES GCM IV generation follows [RFC5288] and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5; thus, the module is compliant with [SP800-52r1].

9. Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
CTR	Counter Mode
CVL	Component Validation List
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feedback
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
TMOS	Traffic Management Operating System
XTS	XEX-based Tweaked-codebook mode with cipher text stealing

Appendix B. Selection of References

FIPS140-2 **FIPS PUB 140-2 - Security Requirements For Cryptographic Modules**
May 2001https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

FIPS140-2_IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
Aug 2015
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography**
https://tools.ietf.org/html/rfc8017

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

SP800-38D **NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
November 2007
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

SP800-56A **NIST Special Publication 800-56A - Recommendation for Pair-Wise Key**
Establishment Schemes Using Discrete Logarithm Cryptography
Apr 2018, rev3
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

SP800-90A **NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
Jun 2015
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

SP800-131A **NIST Special Publication 800-131A - Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths**
Mar 2019
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

SP800-133r1 **Recommendation for Cryptographic Key Generation**
July 2019
https://doi.org/10.6028/NIST.SP.800-133r1