F5, Inc.

Device Cryptographic Module

Hardware Versions:

BIG-IP i4600, BIG-IP i4800, BIG-IP i5600, BIG-IP i5800, BIG-IP i5820-DF, BIG-IP i7600, BIG-IP i7800, BIG-IP i7820-DF, BIG-IP i10600, BIG-IP i10800, BIG-IP i11600-DS, BIG-IP i11800-DS, BIG-IP i15600, BIG-IP i15800, BIG-IP i15820-DF, VIPRION B2250, VIPRION B4450

with FIPS Kit P/N: F5-ADD-BIG-FIPS140

Firmware Version: 16.1.3.1

FIPS Security Level 2

FIPS 140-3 Non-Proprietary Security Policy

Last update: July 2024

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

Table of Contents

Copyrights and Trademarks

F5®, BIG-IP®, TMOS®, are registered trademarks of F5, Inc.

Intel® and Xeon® are registered trademarks of Intel Corporation.

1 General

This document is the non-proprietary FIPS 140-3 Security Policy for the Device Cryptographic Module with firmware version 16.1.3.1 and hardware versions listed in Table 2 below. The document contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for a Security Level 2 module.

This document provides all tables and diagrams (when applicable) required by NIST SP 800-140B.

The following describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-tests	2
11	Life-cycle Assurance	2
12	Mitigation of Other Attacks	N/A

Table 1 - Security Levels

2 Cryptographic Module Specification

2.1 Description

The Device Cryptographic Module (hereafter referred to as “the module”) is a Hardware cryptographic module with multiple-chip standalone embodiment. 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 software is F5’s proprietary operating 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.

2.2 Operating Environments

#	Model	Hardware [Part Number and Version]	Processors	Firmware Version	Distinguishing Features
1	i4600	BIG-IP iseries	Intel® Xeon® D-1518, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 1GbE; 4 x 10GbE network ports 1 x Console port 1 x 1GbE management port
2	i4800	BIG-IP iseries	Intel® Xeon® D-1518, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 1GbE; 4 x 10GbE network ports 1 x Console port 1 x 1GbE management port
3	i5600	BIG-IP iseries	Intel® Xeon® E5-1630v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 4 x 40GbE network ports 1 x Console port 1 x 1GbE management port
4	i5800	BIG-IP iseries	Intel® Xeon® E5-1630v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 4 x 40GbE network ports 1 x Console port 1 x 1GbE management port
5	i5820-DF	BIG-IP iseries	Intel® Xeon® E5-1630v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 4 x 40GbE network ports 1 x Console port 1 x 1GbE management port
6	i7600	BIG-IP iseries	Intel® Xeon® E5-1650v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE and 4 x 40GbE network ports 1 x Console port 1 x 10/100/1000-BaseT management port
7	i7800	BIG-IP iseries	Intel® Xeon® E5-1650v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE and 4 x 40GbE network ports 1 x Console port 1 x 10/100/1000-BaseT management port

#	Model	Hardware [Part Number and Version]	Processors	Firmware Version	Distinguishing Features
8	i7820-DF	BIG-IP iseries	Intel® Xeon® E5-1650v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE and 4 x 40GbE network ports 1 x Console port 1 x 10/100/1000-BaseT management port
9	i10600	BIG-IP iseries	Intel® Xeon® E5-1660v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE management port
10	i10800	BIG-IP iseries	Intel® Xeon® E5-1660v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE management port
11	i11600-DS	BIG-IP iseries	Intel® Xeon® E5-2695v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE (10/100/1000 capable) management port
12	i11800-DS	BIG-IP iseries	Intel® Xeon® E5-2695v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 10GbE; 6 x 40GbE network ports 1 x Console port 1 x 1GbE (10/100/1000 capable) management port
13	i15600	BIG-IP iseries	Intel® Xeon® E5-2680v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 40GbE; 4 x 100GbE network ports 1 x Console port 1 x 1GbE management port
14	i15800	BIG-IP iseries	Intel® Xeon® E5-2680v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 40GbE; 4 x 100GbE network ports 1 x Console port 1 x 1GbE management port
15	i15820-DF	BIG-IP iseries	Intel® Xeon® E5-2680v4, Broadwell	BIG-IP 16.1.3.1	1 x USB port 8 x 40GbE; 4 x 100GbE network ports 1 x Console port 1 x 1GbE management port
16	B2250	VIPRION	Intel® Xeon® E5-2658v2, Ivy Bridge	BIG-IP 16.1.3.1	2 x USB port 4 x 40 GbE network ports 1 x Console port 1 x GbE management port
17	B4450	VIPRION	Intel® Xeon® E5-2658v3, Haswell	BIG-IP 16.1.3.1	1 x USB port 6 x 40 GbE; 2 x 100 GbE network ports 1 x Console port 1 x GbE (10/100/1000 Ethernet) management port

Table 2 - Cryptographic Module Tested Configuration

2.3 Modes of Operation

The module supports two modes of operation:

- Approved mode of operation: Only approved or vendor affirmed security functions can be used.
- Non-Approved mode of operation: Only non-approved security functions can be used.

The module enters operational mode after pre-operational self-tests succeed. The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested. SSPs used or stored in the Approved mode are not used in the non-Approved mode, and vice versa.

In the Approved Mode, the cryptographic module provides the following cryptographic algorithms whose CAVP certificates are in Table 3 below. 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. Not all the ACVP tested capabilities are used by the module in approved mode of operation.

2.4 Algorithms

2.4.1 Approved Algorithms and Vendor Affirmed Algorithms

CAVP Cert		Algorithm and Standard	Mode / Method	Description / Key Size(s)/ Key Strength(s)	Use / Function
Control Plane	Data Plane				
A2594	N/A	AES [FIPS 197, SP800-38A, SP800-38C, SP800 38D]	ECB, CBC, GCM, CCM, CTR	128 / 192 / 256-bit keys with key strengths from 128 to 256 bits	Encryption and Decryption
A2594	A2671	KTS (AES) [FIPS 197, SP800-38D, SP800- 38F]	GCM, CCM	128 / 256-bit AES keys with key strengths 128 or 256 bits	Key Wrapping / Unwrapping
A2594	A2671		AES-CBC key and HMAC-SHA2-256, or HMAC-SHA2-384	128 / 256-bit AES and HMAC keys with key strengths 128 or 256 bits	
A2594	N/A		AES-CBC/ AES-CTR keys and HMAC-SHA-1, HMAC-SHA2-256	128 / 256-bit AES and HMAC keys with key strengths 128 or 256 bits	
A2594	N/A	AES [FIPS 197, SP800-38B, SP800 38D]	GMAC	128 / 192 / 256-bit AES keys with key strengths from 128 to 256 bits	MAC Generation and Verification
N/A	A2671	AES [FIPS 197, SP800-38A, SP800-38C, SP800 38D]	CBC, GCM, CCM	128 / 256-bit keys with key strengths 128 and 256 bits	Encryption and Decryption

CAVP Cert		Algorithm and Standard	Mode / Method	Description / Key Size(s)/ Key Strength(s)	Use / Function
Control Plane	Data Plane				
N/A	A2671	AES [FIPS 197, SP800-38B, SP800 38D]	GMAC	128 / 256-bit keys with key strengths 128 and 256 bits	MAC Generation and Verification
A2594	N/A	CTR_DRBG [SP800-90ARev1]	AES 256 in CTR mode with / without derivation function; prediction resistance disabled / enabled	Entropy input (256-bits with DF and 384-bits without DF), V (128-bits) and key (256-bits) values	Random Number Generation
N/A	A2671	CTR_DRBG [SP800-90A Rev1]	AES 256 in CTR mode with derivation function; prediction resistance disabled	Entropy input (256-bits), V (128-bits) and key (256-bits) values	Random Number Generation
A2594	N/A	RSA [FIPS 186-4]	B.3.3 Random Probable Primes	2048 and 4096-bit keys with key strengths 112 and 150-bits	Key Generation
A2594	A2671	RSA [FIPS 186-4]	PKCS#1v1.5: SHA-1 (Sig Ver only) SHA2-256, SHA2-384	2048, 3072 and 4096-bits keys with key strengths 112 to 150-bits	Signature Generation and Verification
N/A	A2671	RSA [FIPS 186-4]	PKCSPSS: SHA-1 (Sig Ver only) SHA2-256, SHA2-384	2048, 3072 and 4096-bits keys with key strengths 112 to 150-bits	Signature Generation and Verification
A2594	A2671	Safe Primes Key Generation/ Verification [SP800-56Ar3]	Safe Primes groups	ffdhe2048, ffdhe3072, and ffdhe4096 with key strengths 112 to 150-bits	Diffie-Hellman key pair generation and verification using Safe Primes
A2594	A2671	ECDSA [FIPS 186-4]	B.4.2 Testing Candidates	P-256 and P-384 with key strengths 128 and 192-bits	Key Pair Generation / Verification
A2594	A2671	ECDSA [FIPS 186-4]	SHA2-256, SHA2-384, SHA2-512	P-256 and P-384 with key strengths 128 and 192-bits	Signature Generation and Verification
A2594	A2671	SHS [FIPS180-4]	SHA-1 SHA2-256 SHA2-384 SHA2-512	N/A	Message Digest
A2594	A2671	HMAC [FIPS 198-1]	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	112 bits to 1024-bits with key strengths 112 to 256-bits	Message Authentication

CAVP Cert		Algorithm and Standard	Mode / Method	Description / Key Size(s)/ Key Strength(s)	Use / Function
Control Plane	Data Plane				
A2594	A2671	KAS-ECC-SSC [SP800-56ARev3]	Ephemeral Unified; KAS Role: initiator, responder	P-256, P-384 with key strengths 128 and 192-bits	Shared Secret Computation used in Key Agreement Scheme (KAS) IG D.F scenario 2 (path 2)
A2594	A2671	KAS-FFC-SSC [SP800-56ARev3]	dhEphem KAS Role: initiator, responder	ffdhe2048, ffdhe3072, ffdhe4096 with key strengths 112 to 150-bits	Shared Secret Computation used in Key Agreement Scheme KAS) IG D.F scenario 2 (path 2)
A2594	N/A	SSH KDF[1] [SP800-135] (CVL)	AES-128, AES-256 with SHA2-256, SHA2-384	256-bit keys with 256-bits key strength	Key Derivation
A2594	A2671	TLS KDF[1] [SP800-135] (CVL)	TLS v1.2	128 / 256-bit AES keys with key strengths from 112 and 256 bits; 112 / 256-bit HMAC keys with key strengths from 112 to 256 bits	Key Derivation
(vendor affirmed)	(vendor affirmed)	CKG [SP800-133rev2] CTR_DRBG [SP800-90Ar1] Diffie-Hellman, EC Diffie-Hellman [SP800-56Ar3] RSA, ECDSA [FIPS 186-4]	DRBG produces random numbers use for key generation of RSA, ECDSA, Diffie-Hellman and EC Diffie-Hellman	RSA Sizes: 2048 and 4096-bits key with 112 and 150-bits key strength	Key generation
				ECDSA, EC Diffie-Hellman: P-256 and P-384 with 128 and 192-bits key strength	
				Safe Primes: ffdhe2048, ffdhe3072, ffdhe4096 with 112, 128, 150-bits key strength	

Table 3 - Approved Algorithms

2.4.2 Non-Approved, Allowed Algorithms and Non-Approved, Allowed Algorithms with No Security Claimed

The module does not implement any non-approved algorithms allowed in the approved mode of operation with or without security claimed.

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

2.4.3 Non-Approved, Not Allowed Algorithms

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

Algorithm/ Functions	Use/Function
AES modes: OFB, CFB, XTS[2] and KW modes; DES RC4 Triple-DES SM2, SM4	Symmetric Encryption and Decryption
RSA	Asymmetric Encryption and Decryption
RSA Key generation	Using modulus sizes other than 2048-bit or 4096-bit; ANSI X9.31 standard with all key sizes
DSA	Domain parameter generation, domain parameter verification, key pair generation
DSA digital signature	Signature generation and verification using any key size
EdDSA digital signature	Signature generation and verification using Ed25519
ECDSA Key generation/ verification	Using curves other than P-256 and P-384
RSA digital signature	- Signature Generation: PKCS#1 v1.5 using 2048, 3072 or 4096-bits modulus with SHA-1, SHA2-224, SHA2-512 - Signature Verification PKCS#1 v1.5 using 2048, 3072 or 4096-bits modulus with SHA2-224, SHA2-512 - Signature Generation and Verification using PKCS #1 v1.5 scheme with modulus other than 2048, 3072 or 4096 bits, for all SHA sizes - Signature Generation PSS using 2048, 3072 or 4096-bits modulus with SHA-1, SHA2-224, SHA2-512 - Signature Verification PSS using 2048, 3072 or 4096-bits modulus with SHA2-224, SHA2-512 - Signature Generation and Verification using Probabilistic Signature Scheme (PSS) specified in ANSI X9.31 standard
ECDSA digital signature	- Digital Signature Generation and Verification using curves other than P-256 and P-384, all SHA sizes - Digital Signature Generation using curves P-256 and P-384 with SHA-1, SHA2-224 - Digital Signature Verification using curves P-256 and P-384 with SHA2-224
SHA2-224 SM3 MD5	Message Digest
HMAC-SHA2-224 AES-CMAC Triple-DES AES-GCM in IPsec protocol	Message Authentication

[2] 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.

Algorithm/ Functions	Use/Function
Diffie-Hellman EC Diffie-Hellman	Key Agreement Scheme: - Diffie-Hellman using groups other than ffdhe2048, ffdhe3072, ffdhe4096 - Diffie-Hellman using MODP groups in IPsec/IKE protocol - EC Diffie-Hellman ephemeral Unified using curves other than P-256 and P-384 - EC Diffie-Hellman using curves P-256 and P-384 Static Unified and OnePassDh - EC Diffie-Hellman in IPsec/IKE protocol using P-384
TLS KDF SNMP KDF, IKEv1, IKEv2 KDF	Key Derivation function in the context of: - TLS using MD5/ SHA-1/ SHA2-224 / SHA2-512 - SSH using SHA-1/ SHA2-224/ SHA2-512 - SNMP using any SHA variant - IKE using any SHA variant
TLS used in SSL Orchestrator (SSLO)	All ciphersuites algorithms implemented by f5-rest-node

Table 4 - Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.5 Hardware Module photographs

Figure 1 - BIG-IP i4600 and BIG-IP i4800

Figure 2 - BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF

Figure 3 – BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF

Figure 4 - BIG-IP i10600, BIG-IP i10800 and BIG-IP i11600-DS, BIG-IP i11800-DS

Figure 5 – BIG-IP i15600, BIG-IP i15800, BIG-IP i15820-DF

Figure 6 - B2250 blade mounted in VIPRION chassis C2400 with three blanks

Figure 7 - B4450 blade mounted in VIPRION chassis 4480 with three blanks

2.6 Block Diagram and Cryptographic Boundary Descriptions

The cryptographic boundary of the module is defined by the exterior surface of the appliance (red dotted line in Figure 8). The block diagram below shows the module, its interfaces and the delimitation of its cryptographic boundary. Figure 8 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.

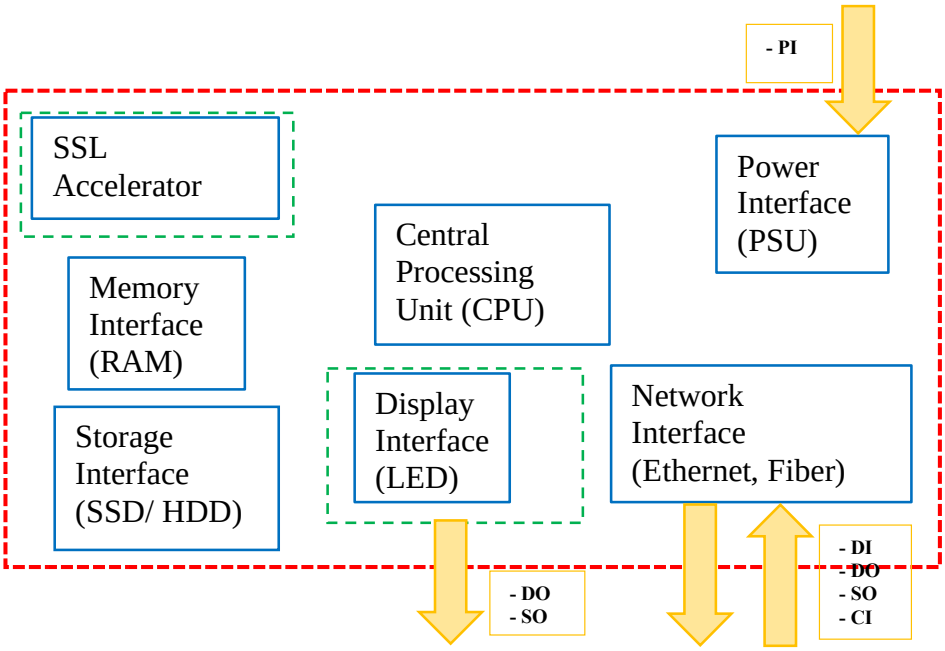

Figure 8 - Hardware Block Diagram

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The logical interfaces are the commands through which users of the module request services. There are no external input or output devices to the module can be used for data input, data output, status output or control input.

The physical ports mapping to the logical interfaces and the flow of data passing over them are described in the Table 5.

Physical port[3]	Logical Interface	Data that passes over port/interface
Network Interface (SFP, SFP+, and QSFP+ ports (Ethernet and/or Fiber Optic) which allow transfer speeds from 1Gbps up to 100Gbps.)	Data Input	TLS/SSH protocol input messages; Configuration commands for interface management
Network Interface (SFP, SFP+, and QSFP+ ports)	Data Output	TLS/SSH protocol output messages; Status logs
Network Interface (SFP, SFP+, and QSFP+ ports)	Control Input	API which control system state (e.g. reset system, power-off system).
Network Interface (SFP, SFP+, and QSFP+ ports); Display Interface (LEDs, and/or output to STDOUT)	Status Output	API which provides system status information.
Power Interface	Power Input	PSU

Table 5 - Ports and Interfaces

[3] The module does not implement Control Output interface.

4 Roles, Services, and Authentication

4.1 Roles

The module supports one CO role and one User role. Maintenance role is not supported. The FIPS 140-3 roles are defined below and corresponding service with input and output are described in Table 6.

- Crypto Officer (CO) role: The Crypto Officer is represented by the administrator of the module (administrator" is the CO). 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. At initialization of the module, the CO is the only available role. Only the CO can create the user roles.
- The FIPS140-3 User role is mapped to multiple module roles: Auditor, Certificate Manager, Firewall Manager, iRule Manager, Operator, Resource Manager and User Manager. Each of the module roles are responsible for different components of the system (e.g. auditing, certificate and key management, user management, etc.).

The list of services available to the CO and user roles are defined in Table 8 and Table 9.

FIPS 140-3 Role	Module Role	Service	Input	Output
CO User	administrator User Manager Resource Manager Auditor	List users	None	List of user accounts
CO User	administrator User Manager	Create additional User	Username / password	Confirmation of account creation
CO User	administrator User Manager	Modify existing Users	Username	Confirmation of account modification
CO User	administrator User Manager	Delete User	Username	Confirmation of deletion
CO User	administrator User Manager	Unlock User	Username	Confirmation of unlock
CO User	administrator User	Update own password	Own password	Confirmation of update of password
CO User	administrator User Manager	Update others password	Username / password	Confirmation of update
CO	administrator	Configure password policy	New password policy	Confirmation of configuration change
CO User	administrator Certificate Manager Resource Manager	Create TLS certificate	Certificate identification information	Confirmation of certificate creation
CO User	administrator Certificate Manager Resource Manager	Create TLS Key	Key identification information	Confirmation of key creation
CO User	administrator Certificate Manager Resource Manager	Delete TLS Key / Certificate	Key identification information	Confirmation of key / certificate deletion
CO User	administrator Auditor Certificate Manager Resource Manager	Display / log expiration data of installed certificates	List of certificates to display	Certificate expiration information
CO User	administrator Auditor Certificate Manager Resource Manager	List private keys	List of private keys to display	TLS private key information

FIPS 140-3 Role	Module Role	Service	Input	Output
CO User	administrator Certificate Manager	Import TLS Certificate	Certificate to import	Confirmation of import of certificate
CO User	administrator Certificate Manager	Export Certificate file	Certificate to export	Exported Certificate file
CO User	administrator Resource Manager	Create SSH-keyswap	SSH key to create	Confirmation of SSH key creation
CO User	administrator Resource Manager	Delete SSH-keyswap	SSH key to delete	Confirmation of SSH key deletion
CO User	administrator Firewall Manager	Configure Firewall	Policy rules, address lists	Confirmation of policy configuration
CO User	administrator Firewall Manager	Show firewall state	N/A	Display the current system wide state of the firewall rules.
CO User	administrator Firewall Manager	Show statistics of firewall rules on the BIG-IP system	N/A	List of statistics of firewall rules
CO User	administrator Firewall Manager	Configure Firewall Users	Firewall user and configuration information	Confirmation of configuration
CO User	administrator Auditor Resource Manager	View System Audit Log	N/A	Display of system audit logs
CO User	administrator Auditor	Export Analytics Logs System	N/A	Display System Analytics Logs
CO User	administrator Resource Manager	Enable / Disable Audit	N/A	Confirmation of enabling or disabling of audit
CO User	administrator Resource Manager	Configure Boot Options	Boot options	Confirmation of configuration of boot options
CO User	administrator Resource Manager	Configure SSH access options	SSH access / IP address list	Confirmation of configuration of SSH access options
CO User	administrator Resource Manager User Manager	Configure SSH user configuration	ssh/ authorized_keys file	Confirmation of configuration of SSH user configuration
CO User	administrator Operator	Modify nodes and pool members	Which nodes and pool members to modify	Confirmation of modification of nodes and pool members
CO User	administrator Firewall Manager Resource Manager	Configure nodes	List of nodes to create / modify / view / delete	Confirmation of creation / modification / display / deletion of nodes
CO User	administrator iRule Manager Firewall Manager Resource Manager	Configure iRules	List of iRules to create / modify / view / delete	Confirmation of creation / modification / display / deletion of iRules
CO	administrator	Reboot System	N/A	Confirmation of system reboot
CO	administrator	Secure Erase	Selected option	Confirmation of full system zeroization
CO User	administrator User	Establish SSH Session	User / address / password /	Confirmation of SSH session establishment

FIPS 140-3 Role	Module Role	Service	Input	Output
			algorithms / key sizes	
CO User	administrator User	Maintain SSH Session	SSH Derived Session key	SSH session information
CO User	administrator User	Closing SSH Session	N/A	Confirmation of SSH session closure
CO User	administrator User	Establish TLS Session	Address / algorithms/ keys / primary secret	Confirmation of establishment of TLS session
CO User	administrator User	Maintain TLS Session	TLS Derived Session key	TLS session information
CO User	administrator User	Closing TLS session	N/A	Confirmation of TLS session closure
CO User	administrator User	Show version	None	Versioning information, and module name
CO User	administrator User	Show license	None	License information
CO User	administrator User	Show status	None	Status of the specific service passed in the show status command
CO User	administrator User	Self- test	power	Pass/ fail results of self-tests

Table 6 **-** *Roles, Service Commands, Input and Output*

4.2 Authentication

The module supports role-based authentication. The module supports concurrent operators belonging to different roles (one CO role and one User role) which create different authenticated sessions, while achieving the separation between the concurrent operators.

Two interfaces can be used to access the module:

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

The User role can access the module through CLI or WebUI. However, the CO can restrict User role access to have the User accessing through WebUI only.

The module does not maintain authenticated sessions upon power cycling. Power-cycling the system requires the authentication credentials to be re-entered. When entering password 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 password authentication data through the CLI, the module does not display any character entered by the operator in stdin (e.g. keyboard).

Table *7* lists the required role-based authentication method for the Crypto Office role and the User role depending upon which interface is being used.

Role	Authentication Method	Authentication Strength
Crypto Officer User	role-based authentication with Password (CLI or WebUI)	The password must consist of a minimum of 8 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 six numerical digits, one ASCII lowercase letter and one ASCII uppercase letter. The probability of guessing every character successfully is (1/10)^6 * (1/26)^1 * (1/26)^1 = 1/676,000,000. Note: this is less than 1/1,000,000. The maximum number of login attempts is limited to 3 after which the account is locked. This means that, in the worst case, an attacker has the probability of guessing the password in one minute as 3/676,000,000. Note: This is less than 1/100,000.
Crypto Officer User	role-based authentication with SSH ECDSA key-pair (CLI only)	The ECDSA using P-256 or P-384 curves for key based authentication yields a minimum security-strength of 128 bits. The chance of a random authentication attempt falsely succeeding is at most $1/(2^{128})$ that is less than 1/1,000,000. The maximum number of login attempts is limited to 3 after which the account switch to password authentication. Then the attacker probability of succeeding to establish the connection depends on the probability of guessing the password and it is, as above, 3/676,000,000 less than 1/100,000.

Table 7 - Roles and Authentication

4.3 Approved Services

Table 8 lists the Approved services, the service name, description, the Approved security function being used by the service, the keys and SSPs accessed by the service, the roles used by the service, access rights to keys and SSPs and the FIPS 140-3 service indicator returned by the service.

The environment variable SECURITY_FIPS140_CIPHER_STRICT is exported with the cipher restriction status. If the cipher_restricted status is enabled, the status output from the service indicator is returned in the high speed login /var/log remote.log file. The output 'Service Indicator: Approved' or the 'Service Indicator: Not Approved' are listed in Table 8. If the cipher_restricted status is disabled, there is no service indicator output.

For SSH service the service indicator is implicit: when the SSH connection is established the service with the cipher selected is approved.

The following variables are used in the Access rights to keys or SSPs column:

- **G = Generate**: The module generates or derives the SSP.
- **R = Read**: The SSP is read from the module (e.g. the SSP is output).
- **W = Write**: The SSP is updated, imported, or written to the module.
- **E = Execute**: The module uses the SSP in performing a cryptographic operation.
- **Z = Zeroise**: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
User Management Services						
List users	Display list of all User accounts	N/A	N/A	CO, User Manager, Resource Manager, Auditor	N/A	None
Create additional User	Create additional User	N/A	password	CO, User Manager	W	None
Modify existing Users	Modify existing Users	N/A	N/A	CO, User Manager	N/A	None
Delete User	Delete User	N/A	N/A	CO, User Manager	N/A	None
Unlock User	Remove lock from user who has exceeded login attempts	N/A	N/A	CO, User Manager	N/A	None
Update own password	Update own password	N/A	password	CO, User	W	None
Update others password	Update others password	N/A	password	CO, User Manager	W	None
Configure Password Policy	Set password policy features	N/A	N/A	CO	N/A	None
Certificate and Keys Management Services						
Create TLS Certificate	Self-signed certificate creation	RSA / ECDSA SigGen	TLS RSA private key; TLS ECDSA private key	CO, Certificate Manager, Resource Manager	E	Service Indicator: Approved
Create TLS Key	Used for the SSL Certificate key file	RSA / ECDSA KeyGen CTR_DRBG	TLS RSA public key; TLS RSA private key; TLS ECDSA public key; TLS ECDSA private key;	CO, Certificate Manager, Resource Manager	G	Service Indicator: Approved
			DRBG seed		E	
			DRBG internal state (V and key values)		W, E	
Delete TLS Certificate /Key	Self-signed certificate / key deletion	N/A	TLS RSA public key; TLS RSA private key; TLS ECDSA public key; TLS ECDSA private key	CO, Certificate Manager, Resource Manager	Z	None
List Certificate	Display / log expiration data of installed certificates	N/A	N/A	CO, Auditor, Certificate Manager, Resource Manager	N/A	None

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
List Private Keys	List private key information	N/A	N/A	CO, Auditor, Certificate Manager, Resource Manager	N/A	None
Import TLS Certificate	Import TLS Certificate	N/A	TLS RSA public key; TLS ECDSA public key	CO, Certificate Manager	W	None
Export Certificate File	Export Certificate File	N/A	TLS RSA public key; TLS ECDSA public key	CO, Certificate Manager	R	None
Create ssh-keyswap	Utility service create ssh keys	ECDSA KeyGen CTR_DRBG	SSH ECDSA public key; SSH ECDSA private key	CO, Resource Manager	G	Service Indicator: Approved
			DRBG seed		E	
			DRBG internal state (V and key values)		W, E	
Delete ssh-keyswap	Utility service delete ssh keys	N/A	SSH ECDSA public key; SSH ECDSA private key	CO, Resource Manager	Z	None
Firewall Management Services						
Configure Firewall	Set policy rules, and address lists for use by firewall rules	N/A	N/A	CO, Firewall Manager	N/A	None
Show firewall state	Display the current system-wide state of firewall rules	N/A	N/A	CO, Firewall Manager	N/A	None
Shows statistics	Shows statistics of firewall rules on the BIG-IP system	N/A	N/A	CO, Firewall Manager	N/A	None
Configure Firewall Users	Configure firewall users	N/A	N/A	CO, Firewall Manager	N/A	None
Audit Management Services						
View System Audit Log	Display logs/files of configuration changes	N/A	N/A	CO, Auditor, Resource Manager	N/A	None
Export Analytics Logs System	Export Analytics Logs System	N/A	N/A	CO, Auditor	N/A	None
Enable/ Disable Audit	Enable/ Disable Audit	N/A	N/A	CO, Resource Manager	N/A	None
System Management Services						

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Configure Boot Options	Enable Quiet boot, Manage boot locations	N/A	N/A	CO, Resource Manager	N/A	None
Configure SSH access options	Enable / Disable SSH access, Configure IP address allow list	N/A	N/A	CO, Resource Manager	N/A	None
Configure SSH user configuration	Update ssh/ authorized_keys file for user authentication	N/A	SSH ECDSA public key	CO, Resource Manager User Manager	W	None
Configure Firewall Users	Configure Firewall Users	N/A	N/A	CO, Firewall Manager	N/A	None
Modify nodes and pool members	Enable / Disable nodes and pool members	N/A	N/A	CO Operator	N/A	None
Configure nodes	Create, modify, view, delete nodes	N/A	N/A	CO Firewall Manager, Resource Manager,	N/A	None
Configure iRules	Create, modify, view, delete, iRules	N/A	N/A	CO, iRule Manager, Firewall Manager, Resource Manager,	N/A	None
Reboot System	Restart cryptographic module	N/A	SSPs listed in Table *12*	CO	Z	None
Secure Erase	Full system zeroization	N/A	SSPs listed in Table *12*	CO	Z	None
SSH Services						
Establish SSH session	Key authentication	ECDSA with SHA2-256 / SHA2-384 curves P-256 / P-384	SSH ECDSA public key; SSH ECDSA private key	CO User	W	SSH connection successful
	Password authentication	N/A	Password	CO User	W	SSH connection successful
	Key Exchange	ECDSA KeyGen, CTR_DRBG	SSH EC Diffie-Hellman public key; SSH EC Diffie-Hellman private key	CO User	G	SSH connection successful
			DRBG Seed		E	
			DRBG internal state (V and key values)		W, E	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		KAS-ECC-SSC	SSH EC Diffie-Hellman public key (remote peer)		W	
			SSH EC Diffie-Hellman private key		E	
			SSH shared secret		G	
	Key Derivation	[SP 800-135] SSH KDF	SSH shared secret	CO User	E	SSH connection successful
			derived SSH session key (AES, HMAC)		G	
Maintain SSH Session	Data Encryption and Decryption	AES-CBC AES-CTR	derived SSH Session key (AES)	CO User	E	SSH connection successful
	Data Integrity (MAC): HMAC-with SHA-1/ SHA2-256	HMAC	derived SSH session key (HMAC)	CO User	E	SSH connection successful
Close SSH Session	Close SSH Session	N/A	SSH EC Diffie-Hellman public key; SSH EC Diffie-Hellman private key; SSH shared secret; derived SSH session key	CO User	Z	None
TLS Services						
Establish TLS Session	TLS Certificate Authentication	ECDSA / RSA	TLS RSA public key; TLS RSA private key; TLS ECDSA public key; TLS ECDSA private key	CO User	W	Service Indicator: Approved
	Key Exchange	ECDSA KeyGen, Safe Primes Key Generation and Verification, CTR_DRBG	TLS Diffie-Hellman public key; TLS Diffie-Hellman private key; TLS EC Diffie-Hellman public key; TLS EC Diffie-Hellman private key	CO User	G	Service Indicator: Approved
			DRBG Seed		E	
			DRBG internal state (V and key values)		W, E	
		KAS-ECC-SSC, KAS-FFC-SSC	TLS Diffie-Hellman public key (remote peer); TLS EC Diffie-Hellman public key (remote peer)		W	
			TLS Diffie-Hellman private key; TLS EC Diffie-Hellman private key		E	
			TLS pre-primary secret		G	
		[SP 800-135] TLS KDF	TLS pre-primary secret		E	
			TLS primary secret		G, E	
			TLS derived session keys (AES and HMAC or authentication cypher)		G	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Maintain TLS Session	Data Encryption, Data Authentication	AES-CBC with HMAC-SHA2-256 / SHA2-384 or AES-GCM, AES-CCM	TLS derived session keys (AES and HMAC or authentication cypher)	CO User	E	Service Indicator: Approved
Close TLS session	Close TLS session	N/A	TLS Diffie-Hellman public key; TLS Diffie-Hellman private key; TLS EC Diffie-Hellman public key; TLS EC Diffie-Hellman private key; TLS pre-primary secret; TLS primary secret; TLS derived session keys	CO User	Z	None
Other services						
Show version	Return the module name and versioning information	N/A	N/A	CO User	N/A	None
Show license	Return license information	N/A	N/A	CO User	N/A	None
Show status	Return the module status	N/A	N/A	CO User	N/A	None
Self- test	Execute integrity test; Execute the CASTs	All the algorithms listed in table section 10	N/A (key for self-tests are not SSPs)	CO User	N/A	None

Table 8 - Approved Services

4.4 Non-Approved Services

Table 9 shows the non-Approved services, a description, the non-Approved algorithms that are accessed, the role and service indicator, where applicable.

Service	Description	Algorithms Accessed	Role	Indicator
Establish TLS session	Signature generation and verification	Algorithms listed in Table 4 rows DSA, RSA, ECDSA, EdDSA *digital signature*	User/ CO	No indicator
	Key Exchange	- TLS KDF using MD5, SHA-1, SHA2-224, SHA2-512 - Diffie-Hellman with other curves than ffdhe2048, ffdhe3072, ffdhe4096 - RSA key wrapping with all keys - EC Diffie-Hellman ephemeral unified using curves other than P-256 and P-384 - EC Diffie-Hellman using P-256 and P-384 with Static Unified and OnePassDh	User/ CO	No indicator
Maintain TLS session	Data encryption	Triple-DES	User/ CO	No indicator
	Data authentication	HMAC SHA-1	User/ CO	No indicator

Service	Description	Algorithms Accessed	Role	Indicator
IPsec /IKEv2	configuration and usage	- Authentication: SHA2-256, SHA2-512. AES-GCM - Encryption: AES-192, AES-256, AES-GCM-128, triple-DES - Key Exchange: MODP1024, MODP2048, EC Diffie-Hellman with P-384	User/ CO	No indicator
iControl REST access	Access to the system through REST	None	User/ CO	No indicator
SSLO Configuration and usage	Management of the module protected by iApplx authentication	TLS used in SSL Orchestrator (SSLO)	User/ CO	No indicator
Configuration using SNMP	Management of the module	SHA-1, AES-ECB, RSA- signature verification	User/ CO	No indicator

Table 9 - Non-Approved Services

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module using the approved integrity technique HMAC-SHA2-384 is listed in the section 10.1.1 below. Integrity tests are performed as part of the Pre-Operational Self-Tests.

5.2 On-Demand Integrity Test

The on demand pre-operational self-tests, including the integrity test on demand, are performed by powering the module off and powering it on again.

5.3 Executable Code

The executable code is defined by the firmware version 16.1.3.1. All code belonging to this firmware version is the executable code of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The module operates in a non-modifiable operational environment provided by F5 called TMOS 16.1.3.1. The module is a hardware validated at a Security Level 2 in Physical Security. Once the module is operational, it does not allow the loading of any additional firmware.

There are no further requirements for this security area.

7 Physical Security

7.1 Mechanisms and Actions Required

The module tested in the platforms listed in Table 2 is enclosed in a hard-metallic production grade enclosure that provides opacity and prevents visual inspection of internal components. Each test platform is fitted with tamper evident labels to provide physical evidence of attempts to gain access inside the enclosure. 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 module has 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 Frequency of Inspection / Test	Inspection/Test Guidance Details
Production grade enclosure (SL1)	N/A	N/A
Opaque enclosure (SL2)	N/A	N/A
Tamper Evident Labels (SL2)	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 10 - Physical Security Inspection Guidelines

7.2 Tamper Label Placement

The pictures below show the location of all tamper evident labels for each hardware appliance. Label application instructions are provided in Section 11.2.1 of the Crypto-Officer guidance below.

Hardware Appliance	# of Tamper Labels
BIG-IP i4600, BIG-IP i4800	8
BIG-IP i5600, BIG-IP i5800 BIG-IP i5820-DF	7
BIG-IP i7600 BIG-IP i7800 BIG-IP i7820-DF	8
BIG-IP i10600 BIG-IP i10800	7
BIG-IP i11600-DS BIG-IP i11800-DS	7
BIG-IP i15600 BIG-IP i15800 BIG-IP i15800-DF	8
VIPRION B2250	1

VIPRION B4450	2

Table 11 – Number of Tamper Evident Labels per hardware appliance

The tamper labels are delineated with orange circles in the pictures below.

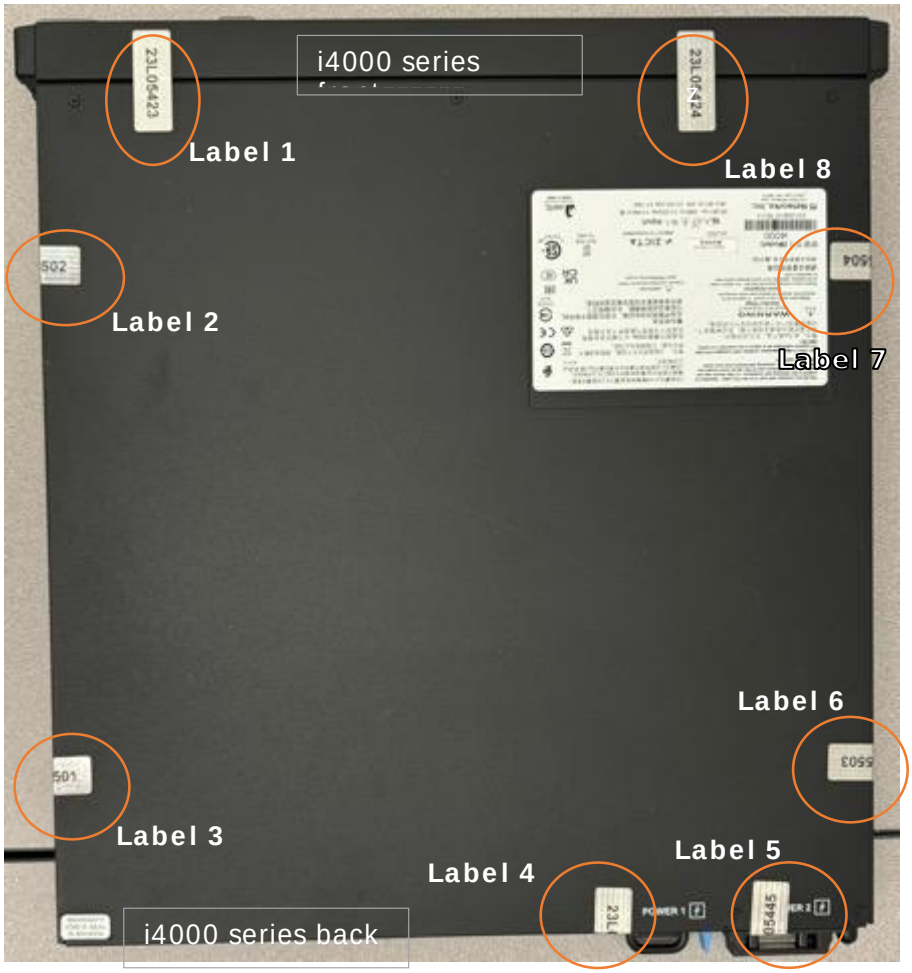

Figure 9 - Tamper labels on BIG-IP i4600 and BIG-IP i4800 (8 / 8 tamper labels)

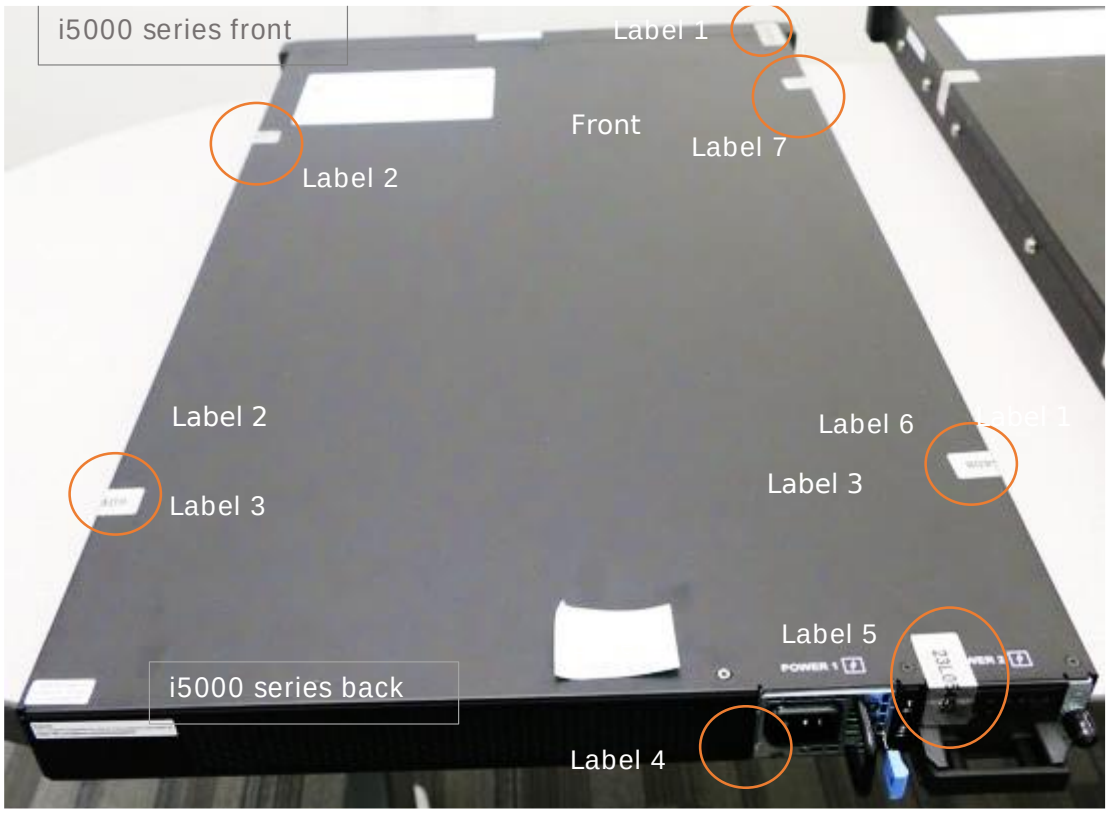

Figure 10 – Tamper labels on BIG-IP i5600, BIG-IP i5800 and BIG-IP i5820-DF (7 / 7 tamper labels)

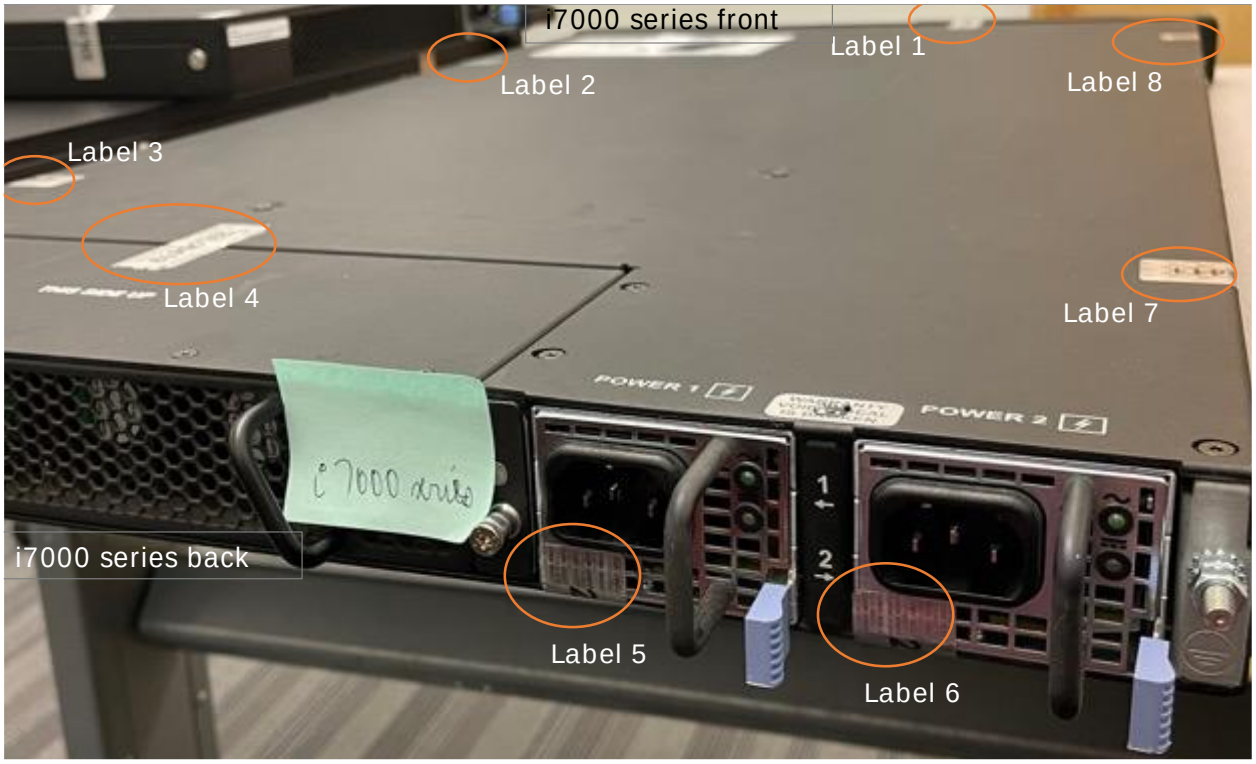

Figure 11 – Tamper labels on BIG-IP i7600, BIG-IP i7800 and BIG-IP i7820-DF. Label position is as follows: on the front side of the platform -label 1-; on the opposite lateral sides of the platform -labels 2,3,7,8; on the ventilation fan tray that allows access to SSD -label 4. On the replaceable PSUs -labels 5,6.

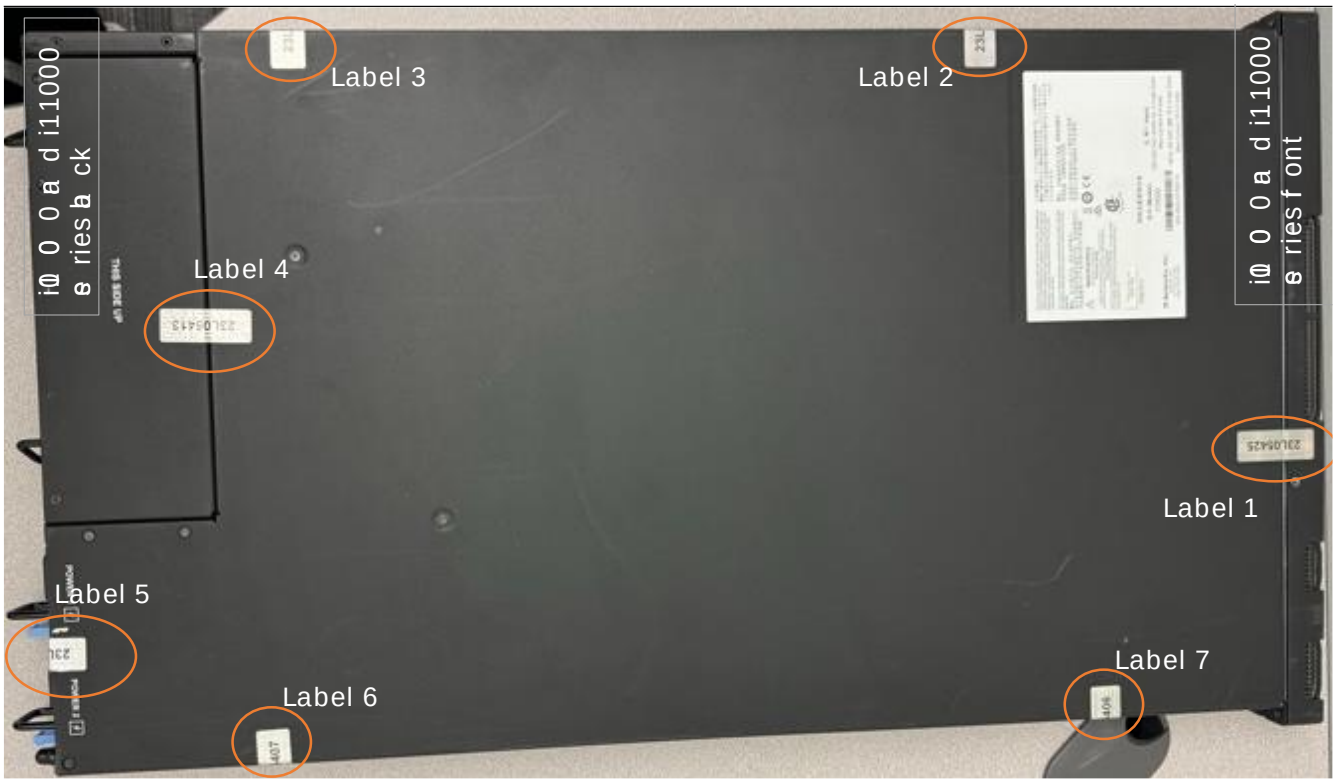

Figure 12 – Tamper labels on BIG-IP i10800, BIG-IP i10600, BIG-IP i11600-DS, BIG-IP i11800-DS (7 / 7 tamper labels shown)

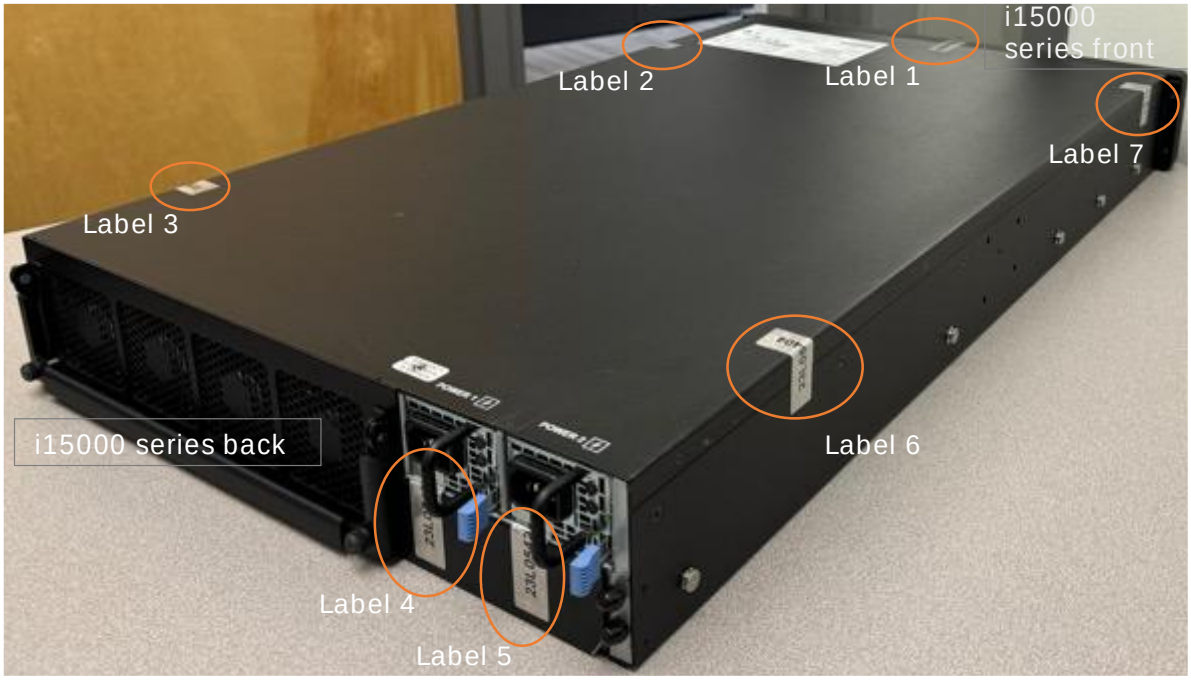

Figure 13 – Tamper labels on BIG-IP i15600, BIG-IP i15800, and BIG-IP i15820-DF. 1 label on the front, 4 labels on the sides, 2 tamper labels shown circled in orange to mark with evidence the unauthorized removal of the fan tray and PSUs (replaceable items) that give access to replaceable storage drives.

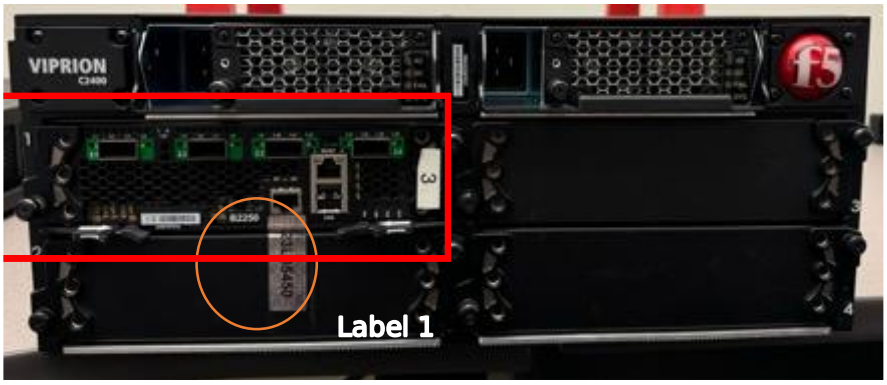

Figure 14 – Tamper labels on chassis with VIPRION B2250 blade (delineated by a red box) and three blanks (1 of 1 tamper label shown)

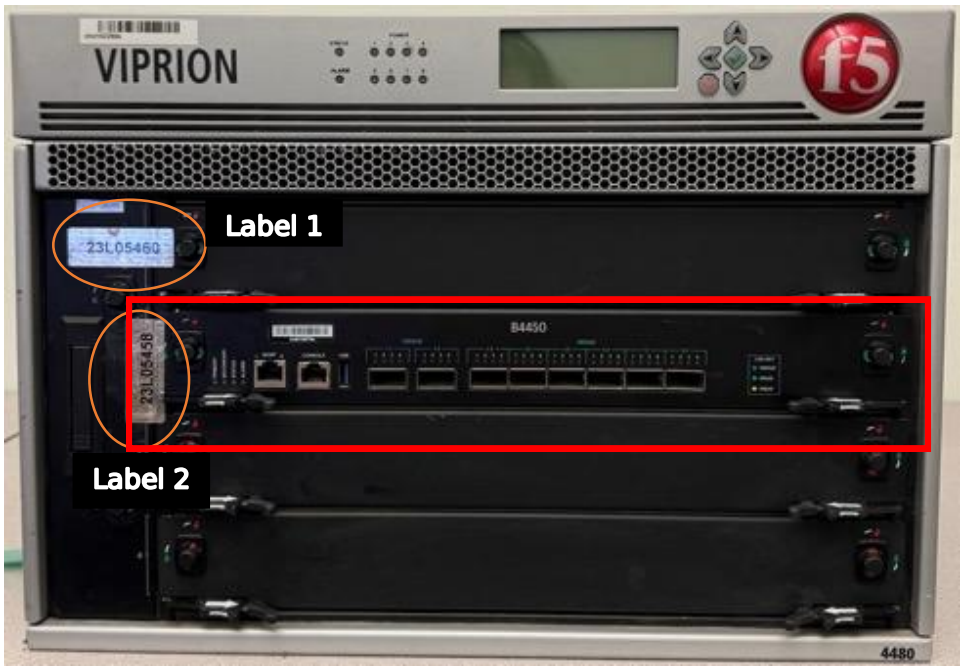

Figure 15 – Tamper labels on chassis with VIPRION B4450 blade (delineated by a red box) and three banks (2 of 2 tamper labels shown)

8 Non-Invasive Security

This section is N/A until non-invasive security is defined.

9 Sensitive Security Parameter Management

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
TLS RSA public key	112-bits to 150-bits	RSA A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key generation method; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	HDD or SSD	Zeroized by Secure Erase service at boot.	**Use**: Key Generation, Digital signature verification used in the TLS protocol **Related SSPs**: TLS RSA private key, DRBG internal state (V and key values)
TLS RSA private key	112-bits to 150-bits	RSA A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key generation method; random values are obtained using [SP 800-90ARev1] DRBG	No import No export	N/A	HDD or SSD	Zeroized by Secure Erase service at boot.	**Use**: Key Generation, Digital signature generation used in the TLS protocol **Related SSPs**: TLS RSA public key, DRBG internal state (V and key values)
TLS ECDSA public key	128-bits and 192-bits	ECDSA A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] ECDSA Key Generation method; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	HDD or SSD	Zeroized by Secure Erase service at boot.	**Use**: Key Generation, Digital signature verification used in the TLS protocol **Related SSPs**: TLS ECDSA private key, DRBG internal state (V and key values)
TLS ECDSA private key	128-bits and 192-bits	ECDSA A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] ECDSA Key Generation	No import No export	N/A	HDD or SSD	Zeroized by Secure Erase service at boot.	**Use**: Key Generation, Digital signature generation used in the TLS protocol **Related SSPs**: TLS ECDSA

[4] The " Import/Export" column also defines the distribution and entry options from IG 9.5.A e.g. Automated Distribution / Electronic Entry = AD/EE

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
			method; random values are obtained using [SP 800-90ARev1] DRBG					public key, DRBG internal state (V and key values)
TLS EC Diffie-Hellman public key	128-bits and 192-bits	KAS-ECC-SSC A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key Generation; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: Key Generation, TLS protocol key exchange **Related SSPs**: TLS EC Diffie-Hellman private key, DRBG internal state (V and key values), TLS pre-primary Secret
TLS EC Diffie-Hellman private key	128-bits and 192-bits	KAS-ECC-SSC A2594 A2671	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key Generation; random values are obtained using [SP 800-90ARev1] DRBG	No import No export	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: Key Generation, TLS protocol key exchange **Related SSPs**: TLS EC Diffie-Hellman public key, DRBG internal state (V and key values), TLS pre-primary Secret
TLS Diffie-Hellman public key	112, 128, and 150-bits	KAS-FFC-SSC A2594 A2671	Generated using Safe primes key generation method specified in SP800-56Arev3; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: Key Generation, TLS protocol key exchange **Related SSPs**: TLS EC Diffie-Hellman private key, DRBG internal state (V and key values), TLS pre-primary Secret
TLS Diffie-Hellman private key	112, 128, and 150-bits	KAS-FFC-SSC A2594 A2671	Generated using Safe primes key generation method specified in SP800-56Arev3; random values are obtained using [SP 800-	No import No export	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: Key Generation, TLS protocol key exchange **Related SSPs**: TLS Diffie-Hellman public key, DRBG internal state (V and key values),

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
			90ARev1] DRBG					TLS pre-primary Secret
TLS pre-primary Secret	Diffie-Hellman: 112, 128, 150-bits EC Diffie-Hellman: 128-bits and 192-bits	KAS-ECC-SSC or KAS-FFC-SSC A2594 A2671	N/A	No import No export	Established via SP800-56ARev3 during key agreement for Diffie-Hellman or EC Diffie-Hellman cipher suites	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: TLS protocol **Related SSPs**: TLS EC Diffie-Hellman public/private key or TLS Diffie-Hellman public/private key, TLS primary secret
TLS primary Secret	256-bits	TLS KDF A2671 A2594	Derived from TLS pre-primary Secret using SP 800-135 TLS KDF	No import No export	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: TLS protocol **Related SSPs**: TLS pre-primary secret, TLS derived session key
TLS Derived session key (AES, HMAC)	128 and 256-bits (AES) 112 and 256-bits (HMAC)	TLS KDF A2671 A2594	Derived from TLS Derived session key using SP 800-135 TLS KDF	No import No export	N/A	RAM	Zeroized by closing TLS session or by Reboot System service	**Use**: TLS protocol **Related SSPs**: TLS pre-primary secret, TLS primary secret
SSH ECDSA public key	128 and 192-bits	ECDSA A2594	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] ECDSA Key generation method; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	HDD or SSD	Zeroized using delete ssh-keyswap utility or by Secure Erase service at boot	**Use**: Key Generation; SSH key-based authentication **Related SSPs**: SSH ECDSA private key, DRBG internal state (V and key values)
SSH ECDSA private key	128 and 192-bits	ECDSA A2594	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4]	No import No export	N/A	HDD or SSD	Zeroized using delete ssh-keyswap utility or by Secure	**Use**: Key Generation, SSH key-based authentication **Related SSPs**: SSH ECDSA

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
			ECDSA Key generation method; random values are obtained using [SP 800-90ARev1] DRBG				Erase service at boot.	public key, DRBG internal state (V and key values)
SSH EC Diffie-Hellman public key	128 and 192-bits	KAS-ECC-SSC A2594	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key generation method; random values are obtained using [SP 800-90ARev1] DRBG	Can be imported/ exported from the module; AD / EE	N/A	RAM	Zeroized by closing SSH session or terminating the SSH application or Reboot System service	**Use**: SSH handshake **Related SSPs**: SSH EC Diffie-Hellman private key, SSH shared secret, DRBG internal state (V and key values)
SSH EC Diffie-Hellman private key	128 and 192-bits	KAS-ECC-SSC A2594	Generated conformant to SP800-133Rev2 (CKG) using [FIPS 186-4] Key generation method; random values are obtained using [SP 800-90ARev1] DRBG	No import No export	N/A	RAM	Zeroized by closing SSH session or terminating the SSH application or Reboot System service	**Use**: SSH handshake **Related SSPs**: SSH EC Diffie-Hellman public key, SSH shared secret, DRBG internal state (V and key values)
SSH Shared Secret	128 and 192-bits	KAS-ECC-SSC A2594	N/A	No import No export	Established via SP800-56ARev3 KAS-ECC-SSC	RAM	Zeroized by closing SSH session or terminating the SSH application or Reboot System service	**Use**: Key derivation, SSH shared secret; **Related SSPs**: SSH EC Diffie-Hellman public/private key, SSH derived key
SSH Derived session key (AES, HMAC)	128 and 256-bits (AES) 112 and 256-bits (HMAC)	SSH KDF A2594	Derived from SSH Shared Secret using SP 800-135 SSH KDF	No import No export	N/A	RAM	Zeroized by closing SSH session or terminating the SSH application or Reboot System service	**Use**: Used in data encryption / decryption and MAC calculations in SSH protocol **Related SSPs**: SSH shared secret

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
Password	1/676,000,000 (see Table 7)	N/A	N/A	Input by the User or CO invoking "create additional user" or "Update own password" or "Update others password" services No export; AD / EE	N/A	HDD or SSD as a hashed value	Zeroized by Secure Erase service at boot	**Use**: SSH authentication, WebUI login **Related SSPs**: N/A
Entropy input	256-bits with DF and 384-bits without DF	Entropy Source ESV Cert. #E16	Obtained from non-physical Entropy source	No import No export	N/A	RAM	Zeroized by Reboot System service	**Use**: random number generation **Related SSPs**: DRBG seed
DRBG seed	256 bits	CTR_DRBG A2594 A2671	Derived from the entropy string as defined by [SP 800-90ARev1]	No import No export	N/A	RAM	Zeroized by Reboot System service	**Use**: random number generation **Related SSPs**: Entropy input, DRBG internal state (V and key values)
DRBG internal state (V and key values)	256 bits	CTR_DRBG A2594 A2671	Derived from the seed as defined by [SP 800-90ARev1]	No import No export	N/A	RAM	Zeroized by Reboot System service	**Use**: random number generation **Related SSPs**: Entropy input, DRBG seed, TLS RSA public key, TLS RSA private key, TLS ECDSA public key, TLS ECDSA private key, TLS EC Diffie-Hellman public key, TLS EC Diffie-Hellman private key, TLS Diffie-Hellman public key, TLS Diffie-Hellman private key, SSH ECDSA

Key/ SSP Name / Type	Strength	Security Function / Cert. #	Generation	Import /Export[4]	Establishment	Storage	Zeroization	Use and related SSPs
								public key, SSH ECDSA private key, SSH EC Diffie-Hellman public key, SSH EC Diffie-Hellman private key

Table 12 - SSPs

9.1 Random Bit Generation - Entropy Source

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800-90ARev1] for the generation of random value used in asymmetric keys. The Approved DRBG provided by the module is the CTR_DRBG with AES-256. The module uses the SP800-90B compliant Entropy source specified in Table 13 to seed the DRBG with full entropy.

In accordance with FIPS 140-3 IG D.L, the 'Entropy input string', 'seed', 'DRBG internal state (V and key values)' are considered CSPs by the module.

No non-DRBG functions or instances are able to access the DRBG internal state.

The operator does not have the ability to modify the F5 entropy source (ES) configuration settings (see details in Public Use Document referenced in section 11.2). The F5 ES is tested in the OEs listed in Table 2.

Entropy Source	Minimum number of bits of entropy	Details
ESV #E16 (non-physical noise source)	256-bits	The CPU Jitter RNG version 3.4.0 entropy source uses jitter variations caused by executing instructions and memory accessed. The entropy source has been shown to provide full 256-bits of entropy at the output of the SHA3-256 vetted conditioning function (Cert. #A2621).

Table 13 - Non-Deterministic Random Number Generation Specification

9.2 SSP Generation

The module implements RSA, ECDSA, EC Diffie-Hellman and Diffie-Hellman asymmetric key generation services compliant with [FIPS186-4], using a [SP800-90ARev1] DRBG.

In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per [SP800-133r2] (vendor affirmed).

The RSA and ECDSA key pairs used for Digital Signature Schemes are generated in accordance with section 5.1 of [SP800-133r2] and maps specifically to [FIPS 186-4].

The ECDH and DH key pairs used for Key Establishment are generated in accordance with section 5.2 of [SP800-133r2] i.e. key generation method specified in [SP 800-56Ar3]. For this module applicable method from [SP800-56Ar3] is 5.6.1.2 ECC Key Pair Generation which actually maps to [FIPS 186-4]. and 5.6.1.1 FFC Key Pair Generation.

The module does not implement symmetric key generation as an explicit service. The HMAC and AES symmetric keys are derived from shared secrets by applying [SP 800-135] as part of the TLS/ SSH protocols. The scenario maps to the [SP 800-133r2] section 6.2.1 *Symmetric keys generated using Key Agreement Scheme*.

9.3 SSP Establishment

The module provides the following key establishment services:

- EC Diffie-Hellman key agreement scheme compliant with SP800-56A Rev3 and FIPS 140-3 IG D.F scenario 2 (path 2) is used as part of the TLS and SSH Protocols. The full EC Diffie-Hellman KAS implements a shared secret computation with the key derivation implemented by [SP 800-135] TLS KDFs and [SP 800-135] SSH KDFs.

  EC Diffie-Hellman key agreement provides 128 or 192-bits of encryption strength.

- Diffie-Hellman key agreement scheme compliant with SP800-56A Rev3 and FIPS 140-3 IG D.F scenario 2 (path 2) is used as part of the TLS Protocols. The full Diffie-Hellman KAS implements a shared secret computation with the key derivation implemented by [SP 800-135] TLS KDFs.

  Diffie-Hellman key agreement provides between 112 and 150-bits of encryption strength.

- [SP 800-38F], IG D.G key wrapping in the context of TLS protocol where a key may be within a packet or message that is encrypted and authenticated using:
  - An approved authenticated encryption mode (i.e. AES-GCM, AES-CCM) provides 128 or 256 bits of encryption strength (AES Certs. #A2594 and # A2671).
  - A combination method which includes an approved AES encryption and an approved HMAC authentication method provides 128 or 256 bits of encryption strength (AES and HMAC Certs. #A2594 and # A2671).

- [SP 800-38F], IG D.G key wrapping in the context of SSH protocol where a key may be within a packet or message that is encrypted and authenticated using:
  - A combination method which includes an approved AES-CBC or AES-CTR encryption mode and an approved HMAC authentication method provides 128 or 256 bits of encryption strength (AES and HMAC Cert. # A2594).

9.4 SSP Entry / Output

For TLS with EC Diffie-Hellman / Diffie-Hellman key exchange, the TLS pre-primary secret is established during key agreement and is not output from the module. Once the TLS session is established, any key or data transfer performed thereafter is protected by authenticated encryption mode using AES-GCM/ AES-CCM or AES encryption and HMAC authentication through a mutually agreed AES and HMAC session keys derived by applying SP 800-135 TLS KDF.

For SSH with EC Diffie-Hellman key exchange, the SSH shared secret is established during key agreement and is not output from the module. SSH ECDSA public keys can be imported into the module by the CO and User role using the "Configure SSH user configuration" service. Once the SSH session is established, any key or data transfer performed thereafter is protected by AES encryption and HMAC authentication through a mutually agreed AES and HMAC session keys derived by applying SP 800-135 SSH KDF.

There are no encrypted SSPs that are directly entered.

9.5 SSP Storage

As shown in Table 12 the keys are 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 SSPs stored in plaintext in the module's non-volatile memory (SSD/ HDD) are static and will remain on the system across power cycle.

SSPs are only accessible to the authenticated operator, to which the SSPs are associated.

9.6 SSP Zeroization

The zeroization methods listed in Table 12, overwrites the memory occupied by keys with “zeros” or pre-defined values.

The zeroization of temporary values are performed at the closing of the TLS/SSH connection.

The zeroization can be enforced by the Crypto Officer and Resource Manager role with the following services:

- Using the Delete SSH-keyswap service will perform the destruction of the selected SSH ECDSA authentication key.

The zeroization can be enforced by the Crypto Officer with the following services:

- Calling Reboot System service will clear the SSPs present in volatile memory RAM memory.
- Using Secure Erase service (which can only be triggered during reboot of the device) will perform a single pass zeroization erasing the HDD or SSD contents and the module itself.

10 Self-Tests

10.1 Pre-Operational Self-Tests

The pre-operational self-test are performed automatically whenever the module is powered on. At initialization the module performed the pre-operational self-tests (the integrity test) and the conditional cryptographic algorithm tests (CASTs). Both the pre-operational tests and conditional tests are performed without operator intervention, without any external controls, externally provided test vectors, output results and the determination of pass of fail is done by the module.

Services are not available during the pre-operational self-test and the data output interface is inhibited. On successful completion of the pre-operational self-tests, the module enters operational mode and cryptographic services are available. If the module fails any of the tests, it will return an error code and enter into the error state to prohibit any further cryptographic operations.

10.1.1 Pre-Operational Software/Firmware Integrity Test

The integrity of the module is verified by comparing the HMAC-SHA2-384 checksum values of the installed binaries calculated at run time with the stored values computed at build time. If the values do not match the system enters the error state and the device will not be accessible. Data output and cryptographic operations are inhibited while the module is in the error state. In order to recover from this state, the module needs to be reinstalled. The HMAC-SHA384 algorithm is self-tested prior to the integrity test being run.

10.2 Conditional Self-Tests

The following sub-sections describe the conditional self-tests supported by the module. The conditional self-tests are specified in Table 14. If one of the conditional self-tests fails, the module transitions to the error state and a corresponding error indication is given. The module becomes inoperable, and no services are available. Data output and cryptographic operations are inhibited while the module is in the error State.

The entropy source performs its required self-tests: RCT and APT at start-up (power-on) and runtime. If the entropy source health tests fail, then the module moves into the error state.

10.2.1 Conditional Cryptographic Algorithm Self-Tests

The module performs cryptographic algorithm self-tests (CASTs) on all Approved cryptographic algorithms. The module performs the CASTs shown in Table 14 during the power-up. The CASTs consist of Known Answer Tests for all the approved cryptographic algorithms, SP800-90B Health Tests for entropy source and SP800-90ARev1 Health Tests for DRBG.

Algorithm	Test
Control Plane (A2594 Cert.)	
non-physical entropy source	SP800-90B health test (APT and RCT) classified as CAST: • at start-up: performed on 1,024 consecutive samples. • during runtime.
CTR_DRBG	CAST KAT with AES 256 bits with and without derivation function SP800-90ARev1 section 11.3 health tests
AES	CAST KAT of AES encryption / decryption separately with AES-GCM mode and 256-bit key

Algorithm	Test
	CAST KAT of AES encryption / decryption separately with ECB mode and 128 bit-key
RSA	CAST KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA2-256 CAST KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA2-256
ECDSA	CAST KAT of ECDSA signature generation using P-256 and SHA2-256 CAST KAT of ECDSA signature verification using P-256 and SHA2-256
KAS-ECC-SSC	CAST KAT of shared secret computation with P-256 curve
KAS-FFC-SSC	CAST KAT of shared secret computation with 2048 modulus
HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	CAST KAT of HMAC-SHA-1, CAST KAT of HMAC-SHA2-256 CAST KAT of HMAC-SHA2-384 (prior integrity tests during pre-operational self-tests) CAST KAT of HMAC-SHA2-512
SHA-1, SHA2-256, SHA2-384, SHA2-512	CAST KATs for all SHA sizes are covered by the respective HMAC KATs (allowed per IG 10.3.B)
[SP800-135] KDF	SSH CAST KAT TLS1.2 CAST KAT
Data Plane (A2671 Cert.)	
AES	CAST KAT of AES encryption with GCM mode and 128-bit key CAST KAT of AES encryption /decryption performed separately with CBC mode and 128-bit key
RSA	CAST KAT of RSA PKCS#1 v1.5 signature generation with 2048 bit key and SHA2-256 CAST KAT of RSA PKCS#1 v1.5 signature verification with 2048 bit key and SHA2-256
ECDSA	CAST KATs of ECDSA signature generation and verification with P-256 curve, SHA2-256
KAS-ECC-SSC	CAST KAT of shared secret computation with P-256 curve
KAS-FFC-SSC	CAST KAT of shared secret computation with 2048 modulus
CTR_DRBG	Covered by Control Plane Self-Tests. (Data Plane makes use of the same DRBG implementation provided by Control Plane)
[SP800-135] KDF	TLS1.2 CAST KAT
HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	CAST KAT of HMAC-SHA-1 CAST KAT of HMAC-SHA2-256 CAST KAT of HMAC-SHA2-384 CAST KAT of HMAC-SHA2-512
SHA-1, SHA2-256, SHA2-384, SHA2-512	CAST KATs for all SHA sizes are covered by respective HMAC KATs (allowed per IG 10.3.B)

Table 14 – Conditional Cryptographic Algorithm Self-Tests

10.2.2 Conditional Pairwise Consistency Test

A pairwise consistency test is run whenever asymmetric keys (RSA, Diffie-Hellman, EC Diffie-Hellman or ECDSA) are generated. PCT for ECDSA (Control and Data planes) and RSA (Control Plane) Key Pair Generation used for digital signatures is tested by the calculation and verification of a digital signature. PCT for Diffie-Hellman (Control and Data planes) Key Pair Generation is performed following the SP 800-56Arev3 requirements. PCT for EC Diffie-Hellman (Control Plane) Key Pair Generation is covered by ECDSA PCT (IG 10.3.A). PCTs for EC Diffie-Hellman (Data Plane) Key Pair Generation is performed following the SP 800-56Arev3 section 5.6.2.1.4 requirements.

10.2.3 On-Demand Self-Test

On demand and periodic self-tests are performed by powering off the module and powering it on again. This service performs the same cryptographic algorithm tests executed during pre-operational self-tests and CASTs. During the execution of the periodic and on-demand self-tests, crypto services are not available and no data output or input is possible.

10.3 Error States

Error State	Cause of Error	Status Indicator
Halt Error	HMAC-SHA2-384 KAT failure or HMAC-SHA2-384 integrity test failure	Module will not load
	Failure of any of the Control Plane CAST KATs, and SP800-90rev1 Health tests and Data Plane CAST KATs	Module will not load
	Failure of any of the PCTs	Module will reboot
	Failure of the APT, RCT at restart/power-on (CAST for entropy source health test at restart)	Module will not load
Health Test Error	Failure of the APT, RCT at runtime (CAST for entropy source health test at runtime)	The module reboot in a loop

Table 15 - Error States

In any of the error states, any data output or cryptographic operations are prohibited. The module must reboot to re-loaded with a fresh image to clear the error condition.

All data output and cryptographic operations are inhibited when the module is in an error state.

11 Life-Cycle Assurance

11.1 Delivery and Operation

The module is distributed as a part of a BIG-IP product which includes the hardware and an installed copy of firmware with version 16.1.3.1. 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’s 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.
- Verify the hardware model with the model number given on the shipping label and marked on the hardware device itself.

11.2 Crypto Officer Guidance

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

The ESV Public Use Document (PUD) reference for non-physical entropy source is as follows: https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/16

11.2.1 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 7.2. 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 7.

11.2.2 Installing BIG-IP

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

- Run the Setup wizard "appliance-setup-wizard" using the CLI with the CO account and default credentials. The system will prompt you to change the password.
- License the system from the WebUI. 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.

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

11.2.2.1 Version Confirmation

The Crypto Officer should call the show version service (with command "tmsh show sys version" and "tmsh show sys hardware"), then confirm that the provided firmware and hardware versions matches the validated versions shown in Table 2. Any firmware loaded into the module other than version 16.1.3.1 is out of the scope of this validation and will mean that the module is not operating as a FIPS validated module.

11.2.2.2 License Confirmation

The FIPS validated module activation requires installation of the license referred as ‘FIPS license’. The Crypto Officer should call the show license service (with command "tmsh show sys license"), then verify that the list of license flags includes "FIPS 140-3”.

11.2.3 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 and USB port should be disabled after the initial power on and communications setup of the hardware.
- On the i11800-DS device, the Cavium Nitrox-V must be disabled using the following command since full support is not available:

```
# lspci | grep -i encryption | awk '{print "device exclude " $1;}' > /config/tmm_init.tcl
# bigstart restart tmm
```

- Use of command run util fips-util -f init is not allowed. Running this command followed by a System Reboot service or restart will mean that the module is not operating as a FIPS validated module.
- The Single Diffie-Hellman should be turned ON for the platform GUI.
- The server ssl profile shall be configured with "cert none" and "key none" option that disables client authentication.

- All the RSA keys in "PubkeyAcceptedKeyTypes" section of the sshd_config file shall be deleted. The command "service sshd restart" updates the sshd_config file.

11.3 User Guidance

The module supports two modes of operation, Approved mode and non-Approved mode. The following two tables define which services are available in each mode: Table 8 - Approved Services and Table 9 - Non-Approved Services. Using the non-approved algorithms found in Table 4 - Non-Approved Algorithms Not Allowed in the Approved Mode of Operation, means that the module operates in non- Approved mode for the particular session of a particular service.

11.3.1 AES GCM IV

The User shall consider the following requirements and restrictions when using the module. AES-GCM IV is constructed in accordance with SP800-38D in compliance with IG C.H scenario 1. The implementation of the nonce_explicit management logic inside the module ensures 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 [RFC 5288] and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-3_IG] IG C.H scenario 1; thus, the module is compliant with [SP800-52 Rev2] section 3.3.1.

11.3.2 RSA SigGen/SigVer

All the modulus sizes supported by the module have been ACVP tested (per IG C.F).

12 Mitigation of Other Attacks

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

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ESV	Entropy Source Validation
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAS	Key Agreement Schema
KAT	Known Answer Test
KW	AES Key Wrap
KWP	AES Key Wrap with Padding
MAC	Message Authentication Code
NDF	No Derivation Function
NIST	National Institute of Science and Technology
OFB	Output Feedback
PR	Prediction Resistance
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
TDES	Triple-DES
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS140-3	**FIPS PUB 140-3 - Security Requirements for Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS140-3_IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** March 2023 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS180-4	**Secure Hash Standard (SHS)** March 2012 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
FIPS186-4	**Digital Signature Standard (DSS)** July 2013 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FIPS197	**Advanced Encryption Standard** November 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 http://www.ietf.org/rfc/rfc3447.txt
SP800-38A	**NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP800-38B	**NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP800-38C	**NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** May 2004 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf
SP800-38D	**NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP800-38F	**NIST Special Publication 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP800-56Ar3	**NIST Special Publication 800-56A Revision 3 - Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://doi.org/10.6028/NIST.SP.800-56Ar3

SP800-90A	**NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://doi.org/10.6028/NIST.SP.800-90Ar1
SP800-90B	**NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation** January 2018 https://doi.org/10.6028/NIST.SP.800-90B
SP800-133	**NIST Special Publication 800-133 Revision 2 - Recommendation for Cryptographic Key Generation** June 2020 https://doi.org/10.6028/NIST.SP.800-133r2
SP800-135	**NIST Special Publication 800-135 Revision 1 - Recommendation for Existing Application-Specific Key Derivation Functions** December 2011 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
SP800-140B	**NIST Special Publication 800-140B - CMVP Security Policy Requirements** March 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf