Motorola Solutions, Inc.

RFS7000 SERIES Wireless Controller

FIPS 140-2 Cryptographic Module Security Policy

Version: R1.2

Date: November 3, 2014

CHANGE RECORD

Revision	*Date*	*Author*	*Description of Change*
R1.0	April 16, 2014	Motorola Solutions	Initial release
R1.1	May 16, 2014	Motorola Solutions	Updates from lab review
R1.2	November 3, 2014	Motorola Solutions	Updates from lab review

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Motorola Solutions RFS7000 Series Controller Cryptographic modules, hereafter denoted the Module. The Module, validated to FIPS 140-2 overall Level 2. The Module incorporates an integrated router, gateway, firewall, DHCP and AAA RADIUS server, VPN, and hot-spot gateway.

HW Model	FW Version
RFS-7010	4.1.4.0-0030GR

Table 1 – Module Configuration Table

Once the firmware is installed, the resulting Module supports only the FIPS-Approved mode of operation. The FIPS-Approved mode of operation is explicitly indicated in the banner message.

RFS7000 login: cli
This device is running in Common Criteria mode.
Attention:
This is a protected and private wireless system. No unauthorized access allowed.
You must have proper rights to access and manage this system from the authorized personnel.
Do you want to proceed? (y/n):

The cryptographic boundary is the enclosure that encloses all hardware and firmware components not including external antennas. The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Security Level of Security Requirements

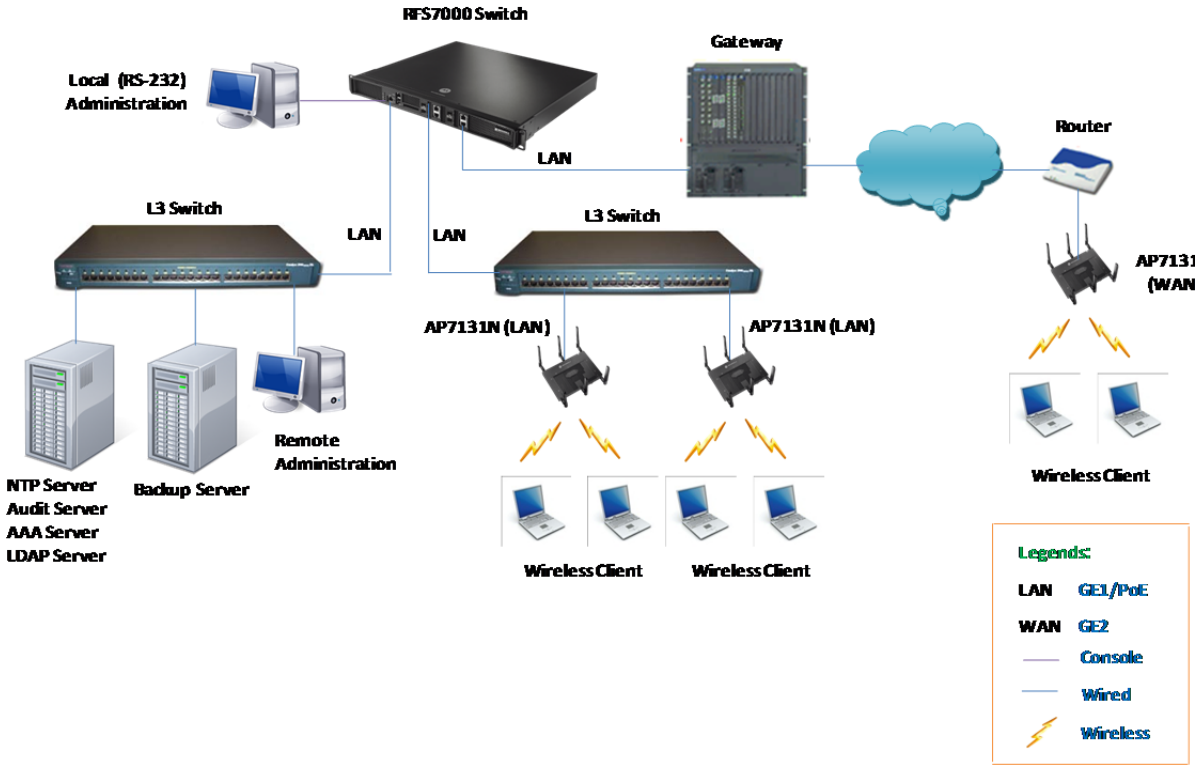

Figure 1 – Operational Context

1.1 RFS7K Controller Physical, Ports and Interfaces

The RFS-7010 GR is shipped with tamper evident seals over seams and covering the Out-of-Band Management port, USB ports, and the Compact Flash slot.

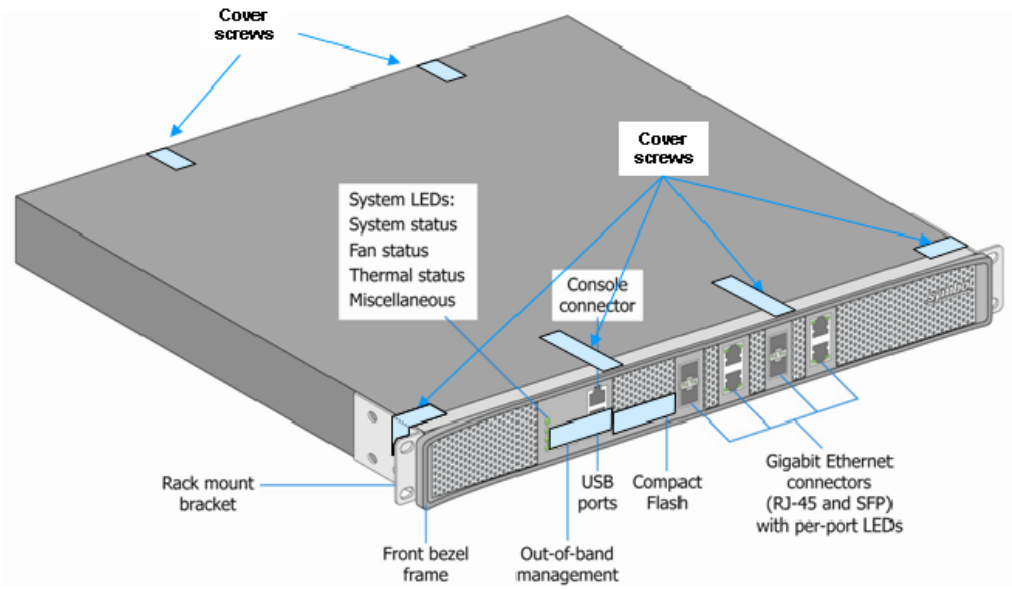

Figure 2 – RFS7K Controller

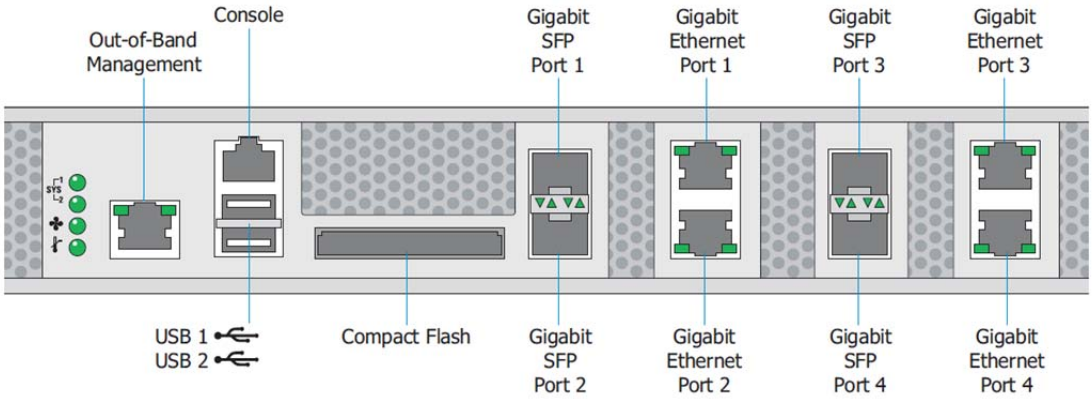

Figure 3 – RFS7K Controller Port Descriptions

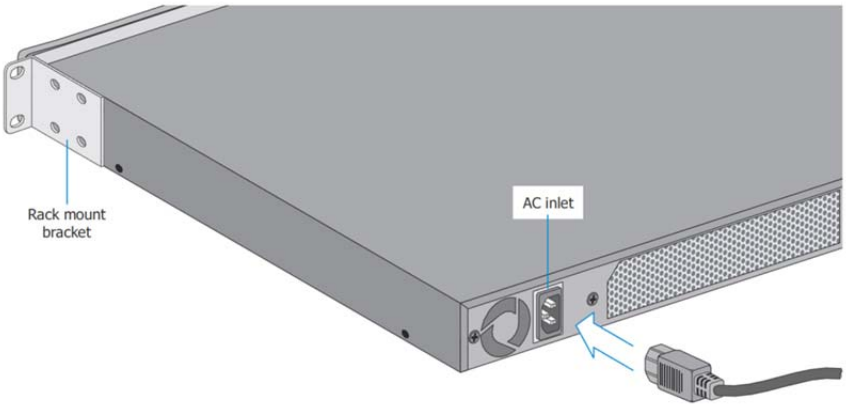

Figure 4 – RFS7K Controller Power Port

Port	Description	Logical Interface Type
Power	120V AC	Power
Management	Out-of-Band Management (Ethernet) port	This port is covered by a tamper seal.
Fiber	Four Gigabit Fiber SFP ports	Control in; Status out; Data in; Data out.
GE	Four Gigabit Ethernet ports	Control in; Status out; Data in; Data out.
Console	RJ45 Console Port (serial)	Control in; Status out; Data in; Data out.
Status LEDs	Cluster of 4 green/amber LEDs for System, Fan and Temperature status	Status out
Comm LEDs	LEDs integral to RJ45 connectors to indicate port speed and status	Status out
Flash	Compact Flash memory slot	This port is covered by a tamper seal.
USB	Two USB Ports	This port is covered by a tamper seal.

Table 3 – RFS7K Controller Ports and Interfaces

2 Cryptographic Functionality

The Module implements the *FIPS Approved* and *Non-Approved but Allowed* cryptographic functions listed in Table 4 and Table 5 below. The notation #*n* indicates multiple implementations of an algorithm or protocol; for example, "AES #1" is one implementation of the AES algorithm; "AES #2" is a second implementation of AES.

Algorithm	Description	Cert #
AES #1	[FIPS 197, SP 800-38A] Modes: ECB, CBC; Key sizes: 128, 192, 256 bits and CFB 128 mode Key size 128 bits Encryption and decryption used for RADIUS, SSHv2, SNMP and TLS.	2752
AES #2	[FIPS 197, SP 800-38A] Modes: CBC; Key sizes: 128, 192, 256 bits. Encryption and decryption used for IPsec/IKE functionality.	2765
HMAC #1	[FIPS 198-1] HMAC-SHA-1, HMAC-SHA-256 Generation and Verification used for RADIUS, SSHv2, SNMP and TLS	1726
HMAC #2	[FIPS 198-1] HMAC-SHA-1, HMAC-SHA-256 Generation and Verification used for IPsec functionality.	1731
TLS KDF	[SP 800-135] TLS key derivation function.	191
SSH KDF	[SP 800-135] SSHv2 key derivation function.	192
IKE KDF	[SP 800-135] IKEv1 key derivation function.	193
SNMP KDF	[SP 800-135] SNMP key derivation function.	190
RNG #1	[ANSI X9.31-1998] Random number generation for use with RADIUS, SSHv2, SNMP and TLS.	1268
RNG #2	[ANSI X9.31-1998] Random number generation for use with IPSec.	1270
RSA	[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PKCS1.5)] Key sizes: 2048 bits RSA Key Pair Generation, Signature Generation, and Signature Verification used for IKE, TLS, SSHv2.	1443
SHA #1	[FIPS 180-3] SHA sizes: SHA-1, SHA-256 Secure hashing used for firmware integrity checking, RADIUS, SSHv2 and TLS.	2321
SHA #2	[FIPS 180-3] SHA sizes: SHA-1, SHA-256 Secure hashing used for IKE.	2326
Triple-DES #1	[SP 800-20] Modes: TECB, TCBC; Key sizes: 3-Key Encryption and decryption used for PEAP-TLS.	1656
Triple-DES #2	[SP 800-20] Modes: TECB; Key sizes: 3-Key This implementation provides encryption and decryption for use with IPSec.	1658

Table 4 –Approved Cryptographic Functions

Algorithm	Description
Non-Compliant SP 800-56A	[IG D.2] Diffie-Hellman (group 14). Key agreement; key establishment methodology provides 112 bits of encryption strength.
Non- Compliant SP 800-56B	[IG D.2] 2048-bit RSA Key Transport. Key wrapping; key establishment methodology provides 112 bits of encryption strength.

Algorithm	Description
NDRNG	[Annex C] Hardware Non-Deterministic RNG; 4096 bits per access, used only to seed the FIPS Approved RNG.
MD5	[IG D.8] Used during TLS handshake.

Table 5 – Non-Approved But Allowed Cryptographic Functions

Algorithm	Description
IKEv1	[IG D.2] IKEv1 and IPsec supported cryptography: AES-CBC-128, AES- CBC-192, AES- CBC-256, SHA1, DH (2048)
SSHv2	[IG D.2] The SSHv2 Cipher Suites implemented by the Module are: Cipher: aes128-cbc, aes192-cbc and aes256-cbc MAC: hmac-sha1, hmac-sha1-96 KEX: diffie-hellman-group14-sha1 Hostkey-algorithms: ssh-rsa
TLS	[IG D.2] The TLS Cipher Suites implemented by the Module are: TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
RADIUS	EAP-TLS, EAP-TTLS, PEAP-TLS

Table 6 – High Level Protocols and Associated Cryptographic Functionality

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module is described in the services detailed in Section 4.

CSP	Description / Usage
RNG-SM	RNG Seed Material: 64-bit seed; Two 64 bit 2-key Triple-DES seed key for the Approved RNG. The Module ensures that the seed and seed key are not equal.
RNG-STATE	The current values of the Approved X9.31 (2-key Triple-DES) RNG instance.
RNG-QS-SM	RNG Seed Material: 64-bit seed; Three 64 bit 3-key Triple-DES seed key for the Approved RNG. The Module ensures that the seed and seed key are not equal.
RNG-QS-STATE	The current values of the Approved X9.31 (3-key Triple-DES) RNG instance.
DH-KEK	Diffie-Hellman Key Establishment Key: DH Group 14 (2048 bit) private key for TLS, IKE and SSH key establishment.
DEV-PRI	Device Private key: RSA 2048 private keys used for TLS, SSH, and EAP authentication methods.
IKE-PSS	IKE Pre-Shared Secret: 64 byte secret value used for IKEv1 authentication.
IPS-SDEK	IPsec Session Data Encryption Key: AES-128/192/256 key used to encrypt and decrypt IPsec messages.
IPS-SAK	IPsec Session Authentication Key: HMAC-SHA-1 (160 bit) key used for IPsec message authentication.
RAD-SEC	Radius Secret: 8 byte minimum, 32 byte maximum secret value used for RADIUS server authentication.
SNMP-SEC	SNMP Secret: 8 byte minimum (no maximum) secret value used for SNMP authentication.
SNMP-DEK	SNMP Data Encryption Key: AES-128 bit key used to encrypt and decrypt SNMP messages.
SSH-DEK	SSH Encryption Key: AES-128/192/256 key used to encrypt and decrypt SSH messages.
SSH-HMAC	SSH HMAC Key: HMAC-SHA1, HMAC-SHA1-96 key used to protect TLS message integrity.
TLS-SDEK	TLS Session Data Encryption Key: AES-128/256 used to encrypt and decrypt TLS messages.
TLS-HKEK	TLS Handshake Key Encryption Key: RSA-2048 private key establishment key, used in the TLS and EAP handshakes.
TLS-HMAC	TLS HMAC Key: HMAC-SHA-1 (160 bit) key used for TLS message authentication.
WL-PSK	64 byte pre-shared key for use in 802.11i (SP 800-108) Key Derivation. WL-PSK is not used directly on device; only stored on device, and sent to adopted access points during configuration.
PW	8 byte minimum (no maximum) value used for local user authentication.

Table 7 – Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
CA-PUB	Certificate authority RSA-1024 or RSA-2048 public key, used for path validation.
DEV-PUB	Device RSA-2048 public key, used for SSH or TLS authentication.
PC-PUB	Peer or client RSA-2048 public key, used for SSH or TLS authentication.
FW-PUB	Device RSA-1024 public key, used for firmware load.

Table 8 – Public Keys

The Module zeroizes all plaintext CSPs by overwriting the storage area three (3) times with three (3) different patterns. After zeroization, the Module assumes factory default settings on reboot.

3 Roles, Authentication and Services

3.1 Roles

Table 9 lists all operator roles supported by the module. The Admin and User roles are human operator roles; the remaining roles are for machine to machine interaction. The Module does not support a maintenance role, state or interface.

ID	Role Description	Authentication Method
Admin	An administrative user, inclusive of the following defined groups with varying levels of access to Module functionality: *Web Admin*: Create guest Hot Spot users and printout a voucher with their credentials. *Monitor*: Read only access to statistics and configuration information. *Security Admin*: Modify access to WLAN keys. Allows troubleshooting tasks such as clear statistics, reboot. *Crypto Officer*: Manage Layer 2, Layer 3, Wireless, RADIUS Server, DHCP Server, SMART-RF; and all SEC role services. *System Administrator*: Upgrade image, change boot partition, set time, manage admin access; and all CO role services. *Super User*: Full access including halt and delete startup configuration; and all SYS role services. This role satisfies the FIPS 140-2 Cryptographic Officer role requirement.	Passphrase verification
User	Wireless User (FIPS 140-2 “User” role): Engage the wireless cryptographic services provided by the module. This role satisfies the FIPS 140-2 User role requirement.	Passphrase verification
NMSU	An SNMP Network Management System User, inclusive of the following: *SNMP Manager*: Non-security related configuration, status monitoring. *SNMP Operator*: Read only access and status monitoring *SNMP Trap*: Read only access and status monitoring through SNMP trap messages	Passphrase verification
TLSC	TLS Client entity, inclusive of the following: https client for Web GUI administration; Air Defense Services Platform (ADSP) communications. (Uses RSA authentication exclusively)	RSA
IPSP	IPsec Peer (uses IKEv1 and the shared secret authentication method exclusively)	Passphrase verification
SSHC	SSHv2 Client (Uses RSA authentication exclusively)	RSA

Table 9 – Roles Description

The Module enforces the separation of roles using an internal access control and groups for associating specific operator credentials with operator roles.

3.2 Authentication Methods

The module implements the following authentication methods. Probability of false authentication and probability of false authentication in a one minute period are shown along with derivation information.

Authentication Method	Probability of false authentication (1.0E-06 required)	Probability of false authentication in a one-minute period (1.0E-05 required)
Passphrase verification	Minimum length: 8 characters Character set: ASCII printable (95) 1/(95^8) = 1.5E-16	Failed authentication imposes 1 second delay (60 attempts/minute). 60/(95^8)=9.0E-15
RSA	Client certificates using RSA-1024 provide 80 bit equivalent strength. 1/(2^80) = 8.3E-25	Failed authentication imposes 1 second delay (60 attempts/minute). 60/(2^80) = 5.0E-23

Table 10 – Authentication Methods and Strengths

The *Passphrase verification* method is a generalization of passwords, SNMP community strings and IKE shared secrets. This calculation uses the worst case scenario to describe minimum strength: 8 bytes minimum and a restricted character set.

3.3 Services

All services implemented by the Module are listed in the tables below.

Service	Description
Local Reset	Power cycle the Module.

Table 11 – Unauthenticated Services

Service	Description	IPSP	SSHC	TLSC	User	NMSU
Connect (IPsec)	Establish and use IPsec connection, used for VPN connection between Motorola devices, RADIUS, syslog, NTP server, etc.	X				
Connect (SSH)	Establish and use connection with SSH client, used to connect Motorola device for management and monitoring purpose.		X			
Connect (TLS)	Establish and use TLS connection, used for Web GUI, establishment of captive portal connection.			X		
Wireless Traffic	802.11 network communications by end User.				X	
SNMP Traffic	SNMP MIB communications.					X

Table 12 – Authenticated Secure Communications Services

Service	Description	Admin
Login	Authentication via CLI or web GUI for administrative use.	X
Configure	Configure device parameters, non-security relevant: routing, quality of service, radio function, etc.	X
Configure security	Configure IPsec, TLS, SSH, 802.11, operator accounts, SNMP access, and RADIUS.	X
Monitor	View intrusion detection and prevention logs.	X
Show status	Show status and configuration information.	X
Remote reset	Trigger a module reset and reboot, inclusive of Power-On Self-Test.	X
Update firmware	Load and manage a new firmware image.	X
Zeroize	Destroys the Module's CSPs and restore the module to factory settings (the Restore Factory Setting operation).	X

Table 13 – Admin Role Services

Table 14 defines access to CSPs by Module services.

	CSPs																	
Service	RNG-SM	RNG-STATE	RNG-QS-SM	RNG-QS-STATE	DH-KEK	DEV-PRI	IKE-PSS	IPS-SDEK	IPS-SAK	RAD-SEC	SNMP-SEC	SNMP-DEK	SSH-DEK	SSH-HMAC	TLS-SDEK	TLS-HKEK	TLS-HMAC	WL-PSK	PW
Configure	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	R	-
Configure Security	-	-	-	-	-	-	E W	-	-	E W	E W	-	-	-	-	-	-	R W	W
Connect (IPsec)	-	W	-	W	G	-	E	G E	G E	-	-	-	-	-	-	-	-	-	-
Connect (SSH)	-	W	-	W	-	-	-	-	-	-	-	G E	-	-	-	-	-	-	-
Connect (TLS)	-	W	-	W	-	-	-	-	-	-	-	-	G E	G E	G E	G E	G E	-	-
SNMP Traffic	-	-	-	-	-	-	-	-	-	-	E	G E	-	-	-	-	-	-	-
Login	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	E
Monitor	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Show status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Remote reset	G Z	Z	G Z	Z	Z	Z	-	Z	Z	-	-	Z	Z	Z	Z	Z	Z	-	-
Update firmware	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Zeroize	-	-	-	-	-	-	Z	-	-	Z	Z	-	-	-	-	-	-	Z	Z
Local Reset	G Z	Z	G Z	Z	Z	Z	-	Z	Z	-	-	Z	Z	Z	Z	Z	Z	-	-

Table 14 – CSP Access Rights within Services

- - = No access to the CSP by the service.
- G = Generate: The Module generates the CSP.
- R = Read: The Module exports the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP.
- Z = Zeroize: The Module zeroizes the CSP.

4 Self-test

4.1 Power Up Self-tests

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

On power up or reset, the Module performs the self-tests described in Table 15 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters an error state. The module will output a status message to the external console stating the module is in error state. Additionally, when an error state is entered the System LED 1 will blink red. The System LED 2 will be off.

Test Target	Description
Firmware Integrity	SHA-256 performed over all code stored in the Module, when the module is initialized after power-up or a soft-reset.
AES #1 ECB Encrypt	AES-128 ECB Encryption KAT
AES #1 ECB Decrypt	AES-128 ECB Decryption KAT
AES #1 CBC Encrypt	AES-128 CBC Encryption KAT
AES #1 CBC Decrypt	AES-128 CBC Decryption KAT
AES #2 CBC Encrypt	AES-128 CBC Encryption KAT
AES #2 CBC Decrypt	AES-128 CBC Decryption KAT
HMAC #1	HMAC-SHA-1 KAT
HMAC #2	HMAC-SHA-256 KAT
RNG#1	ANSI X9.31-1998 RNG (2-key Triple-DES) KAT with fixed seed, seed key and date/time input.
RNG#2	ANSI X9.31-1998 RNG (3-key Triple-DES) KAT with fixed seed, seed key and date/time input.
RSA SigGen	RSA 2048-bit Signature Generation KAT
RSA SigVer	RSA 2048-bit Signature Verification KAT
SHA-1 #1	SHA-1 KAT
SHA-256 #1	SHA-256 KAT
SHA-1 #2	SHA-1 KAT
SHA-256 #2	SHA-256 KAT
Triple-DES#1 Encrypt	3-Key TECB Encryption KAT
Triple-DES#1 Decrypt	3-Key TECB Decryption KAT
Triple-DES#2 Encrypt	3-Key TECB Encryption KAT
Triple-DES#2 Decrypt	3-Key TECB Decryption KAT
SP 800-135 KDF (TLS)	Power-on KDF self-test for TLS keys.
SP 800-135 (SSH)	Power-on KDF self-test for SSH keys.
SP 800-135 (IKE)	Power-on KDF self-test for IKE v1 keys.
SP 800-135 (SNMP)	Power-on KDF self-test for SNMP keys.

Table 15 – Power Up Self-tests

4.2 Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test in accordance with AS09.42, performed when a random value is requested from the NDRNG.
RNG#1	RNG Continuous Test in accordance with AS09.42, performed when a random value is requested from the Approved RNG.
RNG#2	RNG Continuous Test in accordance with AS09.42, performed when a random value is requested from the Approved RNG.
RSA PCT	RSA Pairwise Consistency Test performed on every RSA key pair generation.
Image integrity	The Module performs a SHA-256 test over all data storage.
Firmware Load	RSA 2048 signature verification performed when firmware is loaded.

Table 16 – Conditional Self-tests

4.3 Critical Function Tests

Test Target	Description
Kernel space self-test	This test includes memory test, DRAM test, data and address bus walk and PCI test.
CCM Generate	AES-CCM Generation KAT using AES-128
CCM Verify	AES-CCM Verification KAT using AES-128
SP 800-108 KDF	Power-on KDF self-tests for 802.11i keys.
AES#3 Encrypt	AES-128 Encryption KAT

Table 17 – Critical Function Tests

5 Physical Security Policy

The Module is housed in an industrial quality enclosure.

Motorola Solutions uses production grade components and materials in the manufacture of this product. In addition to the requirements for Level 1, the module provides evidence of tampering when physical access to the module is attempted.

The product contains eight (8) tamper-evident seals as depicted in Figure 5. The tamper evident seals are applied by Motorola Solutions during the manufacturing process. The tamper-evident seals shall be inspected every six months. Tamper seals should be inspected along the entire seal's perimeter, its surface (see Figure 6), and the area immediately surrounding the seal for scratches, scrapes, gouges, cuts and any other signs of tampering. The unit should be removed from service when any such markings are found.

Figure 5 - Tamper Seal Locations

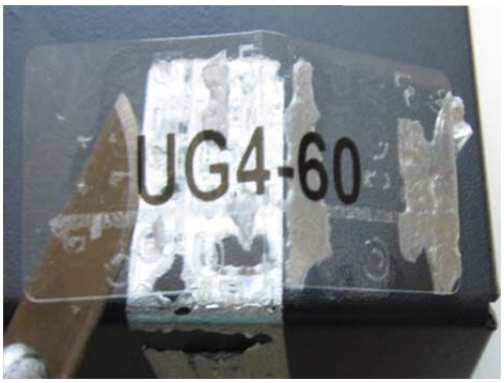

Figure 6 – Example of Tampered Seal

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Module does not implement mitigation for any other attacks.

8 Security Rules and Guidance

The following security rules are enforced by the Module:

1. The Module clears previous authentications on power cycle.
2. The Module does not perform any cryptographic functions until an operator (human or proxy) authenticates to the module, with the exception of cryptographic functions used in the authentication process.
3. Operators can perform the power up self-tests by cycling power or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output is inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module ensures that the seed and seed key inputs to the Approved RNGs are not equal.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not have any external input/output devices used for entry/output of data.
12. The module does not output intermediate key values.

Guidance for first time usage or post factory default reset usage of the Module is provided in the Module's *Secure Installation Guide*, and summarized below:

1. On first use after delivery from the factory, or after zeroization, an authorized administrator shall access the Module with the default password and create a new password.
2. The Firmware version listed in Table 1 shall be loaded onto the module.

9 References

The following documents are referenced in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[RFC3268]	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) http://www.ietf.org/rfc/rfc3268.txt
[RFC2571]	SNMPv3
[RFC2574]	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

Table 18 – References

10 Acronyms and Definitions

Acronym	Definition
ADSP	Air Defense Services Platform
Captive portal	A web page hosted by the module to authenticate wireless users. An attempt to access the device for network access redirects the user to the login web page.
CLI	Command Line Interface
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
GE	Gigabit Ethernet
GUI	Graphical User Interface
IDS	Intrusion Detection System
MIB	Management Information Base
PCI	Peripheral Component Interconnect
POE	Power Over Ethernet
TLS	Transport Layer Security
TTLS	Tunneled TLS

Table 19 – Acronyms and Definitions