

Motorola Solutions, Inc.
AP 71xx Series Wireless Access Points – AP 7131N, AP 7131N-GR, AP 7161, AP 7181

FIPS 140-2 Cryptographic Module Security Policy

Version: 1.1

Date: December 16, 2013



CHANGE RECORD

<i>Revision</i>	<i>Date</i>	<i>Author</i>	<i>Description of Change</i>
1.0	June 12, 2013	Motorola Solutions	Initial release
1.1	December 16, 2013	Motorola Solutions	Updated FW version

Table of Contents

1	Introduction	5
1.1	AP 7131 Physical, Ports and Interfaces	7
1.2	AP 7161 Physical Representation, Ports and Interfaces	9
1.3	AP 7181 Physical Representation, Ports and Interfaces	10
2	Cryptographic Functionality.....	11
2.1	Critical Security Parameters	13
2.2	Public Keys.....	14
3	Roles, Authentication and Services.....	15
3.1	Roles	15
3.2	Authentication Methods	16
3.3	Services.....	17
4	Self-test	20
4.1	Power Up Self-tests	20
4.2	Conditional Self-tests	21
4.3	Critical Function Tests	21
5	Physical Security Policy.....	22
6	Operational Environment	22
7	Mitigation of Other Attacks Policy	22
8	Security Rules and Guidance.....	22
9	References.....	23
10	Acronyms and Definitions.....	23

List of Tables

Table 1 – Module Configuration Table	5
Table 2 – Security Level of Security Requirements.....	5
Table 3 – AP 7131 Ports and Interfaces	8
Table 4 – AP 7161 Ports and Interfaces	9
Table 5 – AP 7181 Ports and Interfaces	10
Table 6 –Approved Cryptographic Functions.....	11
Table 7 – Non-Approved But Allowed Cryptographic Functions	12
Table 8 – High Level Protocols and Associated Cryptographic Functionality	12
Table 9 – Critical Security Parameters	13
Table 10 – Public Keys.....	14
Table 11 – Roles Description.....	15
Table 12 – Authentication Methods and Strengths.....	16
Table 13 – Unauthenticated Services	17
Table 14 – Authenticated Secure Communications Services.....	17
Table 15 – Admin Role Services	18
Table 16 – CSP Access Rights within Services	19
Table 17 – Power Up Self-tests	20
Table 18 – Conditional Self-tests	21
Table 19 – Critical Function Tests	21
Table 20 – References.....	23
Table 21 – Acronyms and Definitions	23

List of Figures

Figure 1 – Operational Context.....	6
Figure 2 – AP 7131 with plastic shroud and antennas removed	7
Figure 3 – AP 7161 views with antennas removed.....	9
Figure 4 – AP 7181 views	10

1 Introduction

This document defines the Security Policy for the Motorola Solutions AP 71xx Series Wireless Access Points – AP 7131N, AP 7131N-GR, AP 7161, and AP 7181, hereafter denoted the Module. The Module, validated to FIPS 140-2 overall Level 1, is a common platform for multiple access points and wireless switches in the Motorola Solutions portfolio that satisfies the needs of centrally managed single and multi-cell 802.11a/b/g/n wireless deployments. The Module incorporates an integrated router, gateway, firewall, DHCP and AAA RADIUS server, VPN, and hot-spot gateway. The dashed line boxes in Figure 1 depict the Module in its operational context.

For the purposes of FIPS 140-2, the Module is classified as a multi-chip standalone embodiment, in three configurations as shown in Table 1..

HW P/N	FW Version
AP7131N, AP7131N-GR	5.4.10.0-050GR
AP7161	5.4.10.0-050GR
AP7181	5.4.10.0-050GR

Table 1 – Module Configuration Table

The Module firmware, license and secure installation instructions are delivered as an option for installation on any of the hardware part numbers listed in Table 1. 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 by the leading characters “[G]” in the shell prompt when using the Login service, for example “[G]ap7131-OF1AE6>”. The remaining characters in the prompt indicate configuration and the last 3 octets of the MAC address.

The cryptographic boundary for each configuration 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	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Security Level of Security Requirements

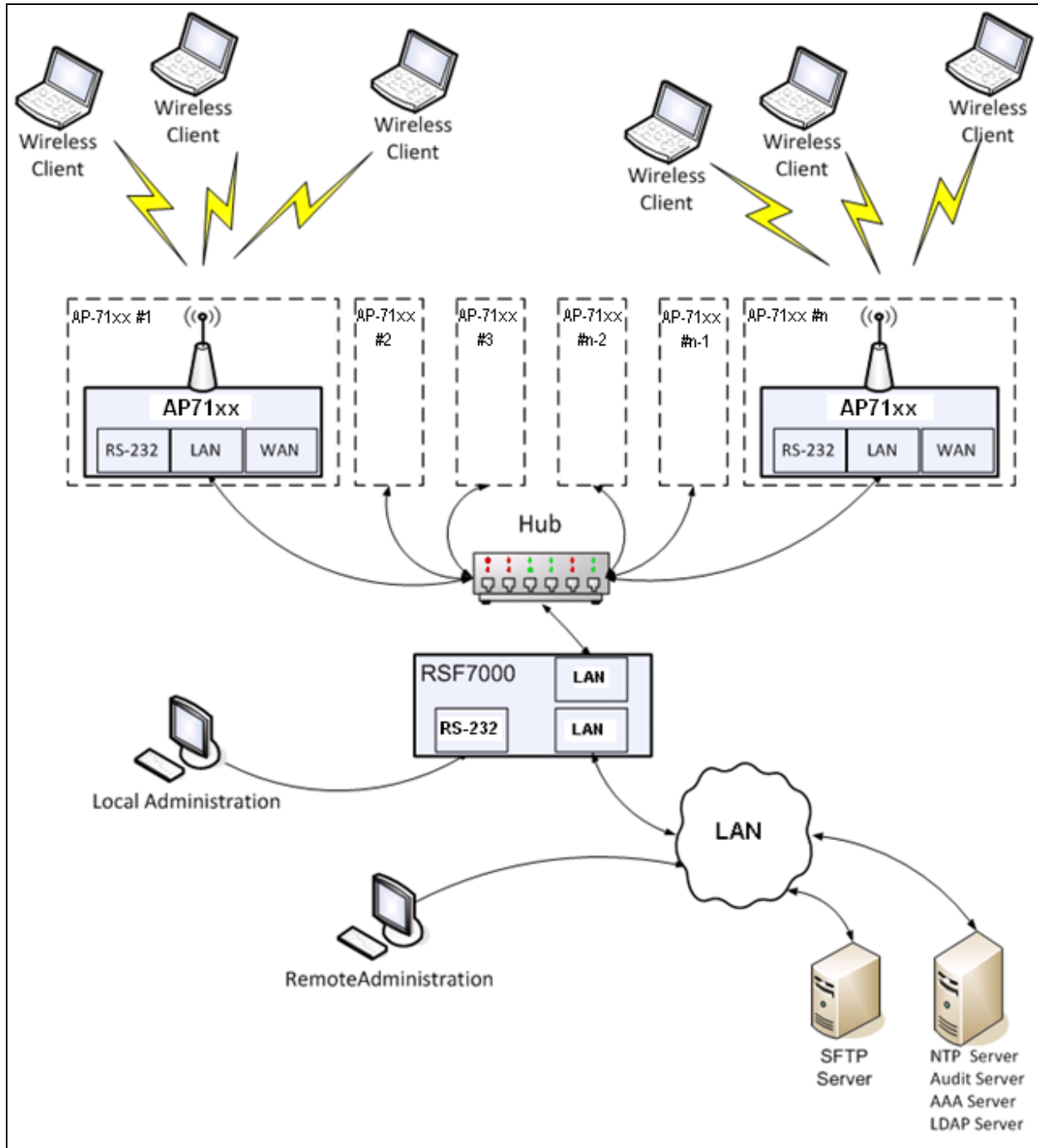


Figure 1 – Operational Context

1.1 AP 7131 Physical, Ports and Interfaces

Figure 2 depicts the AP 7131N-GR – antennas are not shown but connect to the 3 antenna ports on each side of the Module (covered by caps in the figures below). The AP 7131N is the same hardware but without the tamper evident seals. Table 3 describes the AP 7131 ports and interfaces.



Figure 2 – AP 7131 with plastic shroud and antennas removed

Port	Description	Logical Interface Type
PWR	36-57V DC	Power
GE1/POE	LAN port (Gigabit Ethernet/Power Over Ethernet)	Control in; Status out; Data in; Data out; Power (optional)
GE2	WAN port (Gigabit Ethernet)	Control in; Status out; Data in; Data out.
CONSOLE	RJ45 Console Port (serial)	Control in; Status out; Data in; Data out.
R1/2-A/B/C	2-6 antennas for 2.4 GHz and 5 GHz radios	Control in; Data in; Data out; Status out
LEDs	Six LEDs (via light tubes) providing status indicators for: 1) boot/diagnostic mode/normal operation 2) GE1 operation 3) GE2 operation 4) 5 GHz radio operation 5) 2.4 GHz radio operation 6) Unused in this model	Status out

Table 3 – AP 7131 Ports and Interfaces

The convention “R1/2-A/B/C” indicates multiple antenna connections for multiple radios. For example “R1-A” is radio one antenna A; “R2-C” is radio two antenna C.

1.2 AP 7161 Physical Representation, Ports and Interfaces

Figure 3 depicts the AP7161 without the external antennas. Table 4 describes the AP7161 ports and interfaces.

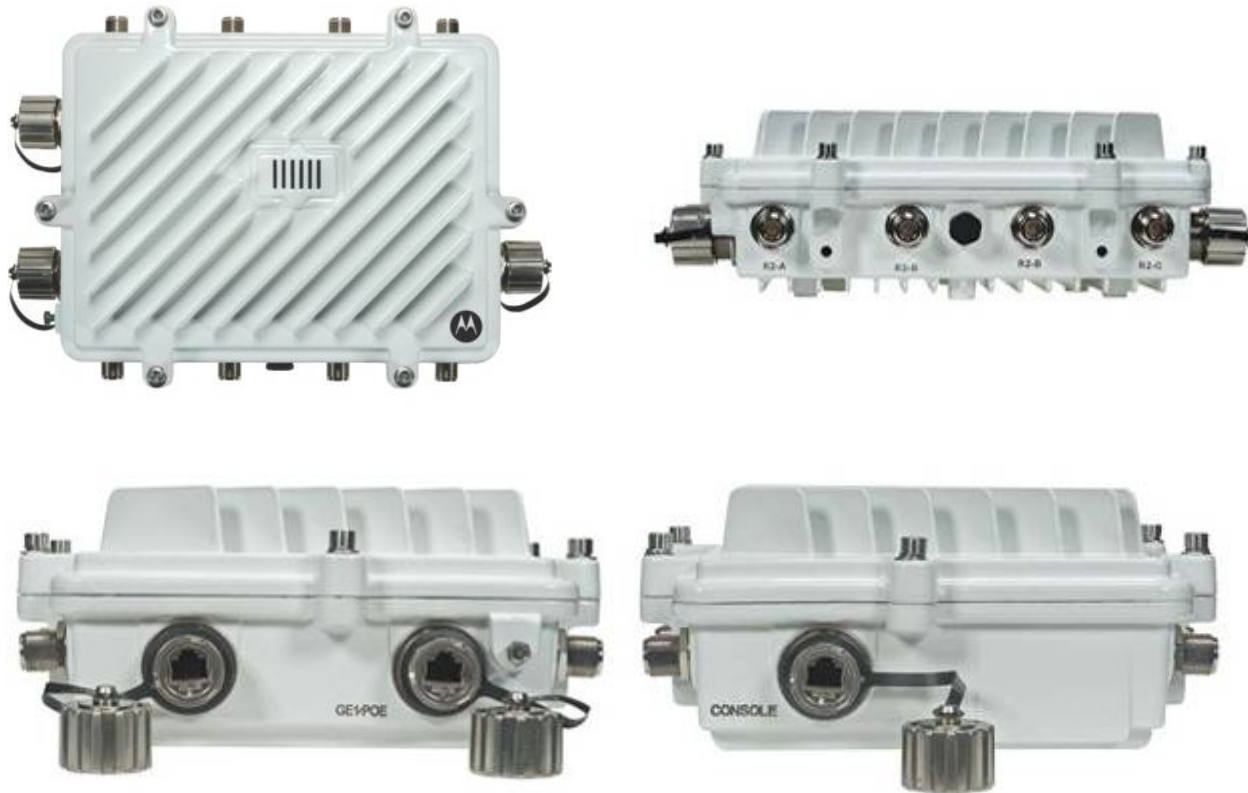


Figure 3 – AP 7161 views with antennas removed

Port	Description	Logical Interface Type
PWR	36-57V DC	Power
GE1/POE	LAN port (Gigabit Ethernet/Power Over Ethernet)	Control in; Status out; Data in; Data out; Power (optional)
GE2	WAN port (Gigabit Ethernet)	Control in; Status out; Data in; Data out.
CONSOLE	RJ 45 Console Port (serial)	Control in; Status out; Data in; Data out.
R1/2-A/B/C/D	2-8 antennas for 2.4 GHz and 5 GHz radios	Control in; Data in; Data out; Status out
LEDs	Six LEDs (via light tubes) providing status indicators for: 1) boot/diagnostic mode/normal operation 2) GE1 operation 3) GE2 operation 4) 5 GHz radio operation 5) 2.4 GHz radio operation 6) Unused in this model	Status out

Table 4 – AP 7161 Ports and Interfaces

1.3 AP 7181 Physical Representation, Ports and Interfaces

Figure 4 depicts the AP7181. Table 5 describes the AP7181 ports and interfaces.



Figure 4 – AP 7181 views

Port	Description	Logical Interface Type
PWR	100-240 VAC and 48V DC	Power
GE1/POE	LAN port (Gigabit Ethernet/Power Over Ethernet)	Control in; Status out; Data in; Data out; Power (optional)
GE2	WAN port (Gigabit Ethernet)	Control in; Status out; Data in; Data out.
CONSOLE	RJ 45 Console Port	Control in; Status out; Data in; Data out.
R1/2-A/B/C/D	8 internal antennas for 2.4 GHz and 5 GHz radios	Control in; Data in; Data out; Status out
LEDs	Six LEDs providing status indicators for: 1) boot/diagnostic mode/normal operation 2) GE1 operation 3) GE2 operation 4) 5 GHz radio operation 5) 2.4 GHz radio operation 6) Unused in this model	Status out

Table 5 – AP 7181 Ports and Interfaces

2 Cryptographic Functionality

The Module implements the *FIPS Approved* and *Non-Approved but Allowed* cryptographic functions listed in Table 6 and Table 7 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.	2377
AES #2	[FIPS 197, SP 800-38A] Modes: CBC; Key sizes: 128, 192, 256 bits. Encryption and decryption used for IPsec and MeshConnex functionality. The ECB mode included in Cert. #1114 is not used by the Module.	1114
AES #3	[FIPS 197, SP 800-38A] Modes: ECB, Key sizes: 128 bits. Encryption used for 802.11i wireless communications.	2378
CCM	[IG 7.2, SP 800-38C] Key sizes: 128-bits AES-CCM generation and verification used for 802.11i wireless communications.	861
HMAC	[FIPS 198-1] HMAC-SHA-1, HMAC-SHA-256 Generation and Verification.	1478
KDF (802.11i)	[IG 7.2, IG 7.10, SP 800-108] 802.11i shared key derivation.	10
TLS KDF	[SP 800-135] TLS key derivation function.	66
SSH KDF	[SP 800-135] SSHv2 key derivation function.	67
IKE KDF	[SP 800-135] IKEv1/IKEv2 key derivation function.	68
SNMP KDF	[SP 800-135] SNMP key derivation function.	69
RNG	[ANSI X9.31-1998] Random number generation.	1180
RSA	[FIPS 186-2, ANSI X9.31-1998, and PKCS #1 v2.1 (PKCS1.5)] Key sizes: 1024, 2048 bits RSA Key Pair Generation, Signature Generation, and Signature Verification used for IKE, TLS, SSHv2.	1231
SHA #1	[FIPS 180-3] SHA sizes: SHA-1, SHA-256 Secure hashing used for firmware integrity checking, RADIUS, SSHv2 and TLS.	2048
SHA #2	[FIPS 180-3] SHA sizes: SHA-1, SHA-256 Secure hashing used for IKE, MeshConnex.	1037
Triple-DES	[SP 800-20] Modes: TEBC, TCBC; Key sizes: 3-Key Encryption and decryption used for TLS, SSHv2.	1487

Table 6 –Approved Cryptographic Functions

Algorithm	Description
Non-Compliant SP 800-56A	[IG D.2] Diffie-Hellman (group 2 5). Key agreement; key establishment methodology provides 80 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.
NDRNG	[Annex C] Hardware Non-Deterministic RNG; 64 bits per access, used only to seed the FIPS Approved RNG.
MD5	[IG D.8] Used during TLS handshake.

Table 7 – Non-Approved But Allowed Cryptographic Functions

Algorithm	Description
IKE v1/v2	[IG D.2] IKE v1/v2 and IPsec supported cryptography: AES-CBC-128, AES- CBC-192, AES- CBC-256, SHA1, DH (1024-1536)
SSHv2	[IG D.2] The SSHv2 Cipher Suites implemented by the Module are: Cipher: 3des-cbc, aes128-cbc, aes256-cbc MAC: hmac-sha1, hmac-sha2 KEX: diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, Hostkey-algorithms: ssh-rsa
TLS	[IG D.2] The TLS Cipher Suites implemented by the Module are: TLS_DH_RSA_WITH_AES_128_CBC_SHA256 TLS_DH_RSA_WITH_AES_128_CBC_SHA TLS_DH_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 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 8 – 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: 128-bit seed; AES-256 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 (AES-256) RNG instance.
DH-KEK	Diffie-Hellman Key Establishment Key: DH Group 2 (1024 bit) or Group 5 (1536 bit) private key for TLS, IKE and SSH key establishment.
DEV-PRI	Device Private key: RSA 1024/2048 private keys used for TLS, SSH, and EAP authentication methods.
IKE-PSS	IKE Pre-Shared Secret: 64 byte secret value used for IKEv1/IKEv2 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-128/256 or 3-Key Triple-DES key used to encrypt and decrypt SSH messages.
SSH-HMAC	SSH HMAC Key: HMAC-SHA-1 (160 bit) or HMAC-SHA-256 (256 bit) key used to protect TLS message integrity.
TLS-SDEK	TLS Session Data Encryption Key: AES-128/256 or 3-Key Triple-DES 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) or HMAC-SHA-256 (256 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-TK	802.11i Temporal Key: AES-128 key for unicast wireless data encryption/decryption.
WL-GTK	802.11i Group Temporal Key: AES-128 key for multicast wireless data encryption/decryption.
WL-KCK	802.11i Key Confirmation Key: AES-128 key used for authentication / key confirmation.
WL-KEK	802.11i Key Encryption Key: AES-128 key used for sensitive data encryption.
PW	8 byte minimum (no maximum) value used for local user authentication.
MC-PSK	MeshConnex Pre-shared Key: 8 byte minimum (no maximum) value used for mesh point authentication.
MC-GTK	MeshConnex Group Transient Key: AES-128 session key used to encrypt/decrypt secure multicast routing messages.
MC-PTK	MeshConnex Pairwise Transient Key: AES-128 session key used to encrypt/decrypt secure unicast broadcast routing messages.
MC-GMK	MeshConnex Group Master Key: AES-128 key used to derive MC-GTK (SP 800-108).
MC-PMK	MeshConnex Pairwise Master Key: AES-128 key used to derive MC-PTK (SP 800-108).

Table 9 – 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-1024 or RSA-2048 public key, used for SSH or TLS authentication.
PC-PUB	Peer or client RSA-1024 or RSA-2048 public key, used for SSH or TLS authentication.

Table 10 – Public Keys

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

3 Roles, Authentication and Services

3.1 Roles

Table 11 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	<p>An administrative user, inclusive of the following defined groups with varying levels of access to Module functionality:</p> <p><i>Web Admin</i>: Create guest Hot Spot users and printout a voucher with their credentials.</p> <p><i>Monitor</i>: Read only access to statistics and configuration information.</p> <p><i>Security Admin</i>: Modify access to WLAN and meshpoint keys. Allows troubleshooting tasks such as clear statistics, reboot.</p> <p><i>Crypto Officer</i>: Manage Layer 2, Layer 3, Wireless, RADIUS Server, DHCP Server, SMART-RF; and all SEC role services.</p> <p><i>System Administrator</i>: Upgrade image, change boot partition, set time, manage admin access; and all CO role services.</p> <p><i>Super User</i>: Full access including halt and delete startup configuration; and all SYS role services.</p> <p>This role satisfies the FIPS 140-2 Cryptographic Officer role requirement.</p>	Passphrase verification
User	<p>Wireless User (FIPS 140-2 "User" role): Engage the wireless cryptographic services provided by the module.</p> <p>This role satisfies the FIPS 140-2 User role requirement.</p>	Passphrase verification
MP	Mesh Peer: Connect wirelessly to another AP in a mesh	802.11i Auth
NMSU	<p>An SNMP Network Management System User, inclusive of the following:</p> <p><i>SNMP Manager</i>: Non-security related configuration, status monitoring.</p> <p><i>SNMP Operator</i>: Read only access and status monitoring</p> <p><i>SNMP Trap</i>: Read only access and status monitoring through SNMP trap messages</p>	Passphrase verification
TLSC	<p>TLS Client entity, inclusive of the following:</p> <p>https client for Web GUI administration; Air Defense Services Platform (ADSP) communications. (Uses RSA authentication exclusively)</p>	RSA
IPSP	IPsec Peer (uses IKEv1/v2 and the shared secret authentication method exclusively)	Passphrase verification
SSHC	SSHv2 Client (Uses RSA authentication exclusively)	RSA
WC	Wireless Client	802.11i Auth

Table 11 – 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). $60/(2^80) = 5.0E-23$
802.11i Auth	AES-128 authentication of secrets derived in 802.11i handshake. $1/(2^128) = 2.9E-39$	Failed authentication imposes 1 second delay (60 attempts/minute). $60/(2^128) = 1.8E-37$

Table 12 – 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 Table 13, 14 and 15 below.

Service	Description
Local Reset	Power cycle the Module.

Table 13 – Unauthenticated Services

Service	Description	IPSP	MP	SSHC	TLSC	WC	User	NMSU
Connect (IPsec)	Establish and use IPsec connection, used for VPN connection between Motorola devices, RADIUS, syslog, NTP server, etc.	X						
Connect (Mesh)	Establish and use mesh peer connection, used for wirelessly connecting two Motorola devices.		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			
Connect (Wireless)	Establish and use connection with wireless clients.					X		
Wireless Traffic	802.11 network communications by end User.						X	
SNMP Traffic	SNMP MIB communications.							X

Table 14 – 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, MeshConnex, 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 15 – Admin Role Services

Table 16 defines access to CSPs by Module services.

Service	CSPs																									
	RNG-SM	RNG-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	WL-TK	WL-GTK	WL-KCK	WL-KEK	PW	MC-PSK	MC-GTK	MC-PTK	MC-GMK	MC-PMK
Configure	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure Security	-	-	-	-	E W	-	-	E W	E W	-	-	-	-	-	-	E W	-	-	-	-	W	E W	-	-	-	-
Connect (IPsec)	-	W	G	-	E	G E	G E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Connect (Mesh)	-	W	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	E	G E	G E	G E	G E
Connect (SSH)	-	W	-	-	-	-	-	-	-	G E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Connect (TLS)	-	W	-	-	-	-	-	-	-	G E	G E	G E	G E	G E	-	-	-	-	-	-	-	-	-	-	-	
Connect (Wireless)	-	W	-	-	-	-	-	-	-	-	-	-	-	-	E	G E	G E	G	G	G	-	-	-	-	-	
Wireless Traffic	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	E	E	-	-	-	-	-	-	
SNMP Traffic	-	-	-	-	-	-	-	-	E	G E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Login	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	E	-	-	-	-	
Monitor	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Show status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Remote reset	G Z	Z	Z	Z	-	Z	Z	-	-	Z	Z	Z	Z	Z	Z	-	Z	Z	Z	Z	-	-	Z	Z	Z	
Update firmware	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Zeroize	-	-	-	-	Z	-	-	Z	Z	-	-	-	-	-	-	Z	-	-	-	-	Z	Z	-	-	-	
Local Reset	G Z	Z	Z	Z	-	Z	Z	-	-	Z	Z	Z	Z	Z	Z	-	Z	Z	Z	-	-	-	Z	Z	Z	

Table 16 – 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 17 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.

Test Target	Description
Firmware Integrity	HMAC-SHA-256 performed over all code stored in the Module, when the module is initialized after power-up or a soft-reset.
AES #1 Encrypt	AES-128 ECB Encryption KAT
AES #1 Decrypt	AES-128 ECB Decryption KAT
AES #2 Encrypt	AES-128 ECB Encryption KAT
AES #2 Decrypt	AES-128 ECB Decryption KAT
AES #3 Encrypt	AES-128 ECB Encryption KAT
CCM Generate	AES-CCM Generation KAT using AES-128
CCM Verify	AES-CCM Verification KAT using AES-128
HMAC	HMAC-SHA-1 KAT
RNG	ANSI X9.31-1998 RNG 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 Encrypt	3-Key TEBC Encryption KAT
Triple-DES Decrypt	3-Key TEBC Decryption KAT
SP 800-108 KDF	Power-on KDF self-test for 802.11i keys.
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/v2 keys.
SP 800-135 (SNMP)	Power-on KDF self-test for SNMP keys.

Table 17 – 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	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 18 – 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.

Table 19 – 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 these products.

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 RNG 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]	<i>Security Requirements for Cryptographic Modules</i> , May 25, 2001
[SP800-131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , 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 20 – 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 21 – Acronyms and Definitions