FIPS 140-2 Security Policy

For

Wireless Access Point AP-7131N-44040-FGR, AP-7131N-44040-FWW, AP-7131N-44040-FIL, AP-7131N-66040-FGR, AP-7131N-66040-FWW and AP-7131N-66040-FIL

Document Version 1.6

Table of Contents

1 Module Description

The Motorola AP-7131 Access Point is a standalone device that manages inbound and outbound traffic on the wireless network. It provides security, network services, intrusion detection and system management applications. It may be used together with the Motorola RF Switch and Motorola external IDS server.

The module is used to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices, as well as to provide Wireless Intrusion Detection Functionality. The module protects data exchanged with wireless client devices using IEEE 802.11i wireless security protocol, which provides data protection using the AES-CCM cryptographic algorithm.

For the purposes of FIPS 140-2 the module is classified as multi-chip standalone module.

FIPS 140-2 conformance testing of the module was performed at Security Level 2, except for Cryptographic Module Specification and Design Assurance sections of the FIPS 140-2 standard, which were tested as Security Level 3. The following configurations were tested:

Module Name and Version	**Firmware versions**
AP-7131N-44040-FGR Access Point	AP7131N v4.0.0.0-035GR
AP-7131N-44040-FWW Access Point	AP7131N v4.0.0.0-035GR
AP-7131N-44040-FIL Access Point	AP7131N v4.0.0.0-035GR
AP-7131N-66040-FGR Access Point	AP7131N v4.0.0.0-035GRN
AP-7131N-66040-FWW Access Point	AP7131N v4.0.0.0-035GRN
AP-7131N-66040-FIL Access Point	AP7131N v4.0.0.0-035GRN

2 Cryptographic Boundary

The complete set of hardware and firmware components of the module is physically enclosed in a metal enclosure which serves as the cryptographic boundary of the module. The enclosure consists of the following two parts. The top panel can be removed from the bottom panel by unscrewing screws. The switch enclosure is opaque within the visible spectrum.

For tamper evidence the module requires tamper-evident labels to allow the detection of the opening of the top panel.

An image of the module is provided below:

Figure 1. An image of the module.

3 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

Port Name	Count	Interface(s)
Ethernet Port	2	Data Input, Data Output, Control Input, Status Output
Serial Console Port	1	Control Input, Status output, Data Output
LEDs	6	Status Output
Power Port	1	Power Input
Power Over Ethernet Port (included in the Ethernet connector)	1	Power Input
Reset Button	1	Control Input
Antenna Ports	6	Data Input/Output

4 Roles, Services and Authentication

The module provides the following roles: a User role, a Crypto Officer role.

The Crypto Officers configure the module and manage its cryptographic functionality. Users employ the cryptographic services provided by the module.

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

Role	Authentication Mechanism
User	Passwords are used for wireless connection with EAP-PEAP and EAP-TTLS authentication. The module uses passwords of at least 8 characters, therefore for each random authentication attempt the probability of success will be significantly less than one in 1,000,000. When a secure network connection is established, the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000 due to the password length and authentication process performance limitation. Client Certificates are used for wireless connection with EAP-TLS authentication. The module uses client certificates with at least 1024 bit RSA key, which corresponds to 80 bits of security, therefore for each random authentication attempt the probability of success will be significantly less than one in 1,000,000. The possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000 due to the authentication process performance limitation.
Crypto Officer	Passwords are used for connections via Command Line Interface (CLI), Web User Interface and SNMP management interface. The module uses passwords of at least 8 characters, therefore for each random authentication attempt the probability of success will be significantly less than one in 1,000,000. Upon a command line interface login attempt failure next username and password prompt is provided after 1 second interval. This ensures that a user can only make 60 or less consecutive attempts in a minute. Therefore the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000.

The module provides the following services to the operators:

Service	Role	Access to Cryptographic Keys and CSPs R- read; W – write or generate; E-execute
Installation of the Module	Crypto Officer	Password: W 802.11i pre-shared key: W SSH RSA key pair: W TLS server certificate: W TLS/EAP Certificate: W SSH keys: E ANSI X9.31 seed and key: E

Service	**Role**	**Access to Cryptographic Keys and CSPs** **R- read; W – write or generate; E-execute**
Login	Crypto Officer	Password: E SNMP secret: E SSH Keys: E TLS Keys: E ANSI X9.31 seed and key: E
Run self-test	Crypto Officer	N/A
Show status	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Update firmware	Crypto Officer	Firmware load verification HMAC SHA-1 firmware load verification key: E
Zeroize/Restore factory settings	Crypto Officer	All keys: W
IPSec/VPN configuration	Crypto Officer	IPSec/IKE pre-shared key: W SSH Keys: E TLS Keys: E ANSI X9.31 seed and key: E
Configure Secure IPSEC Connection to the Motorola WLAN switch	Crypto Officer	IPSec/IKE pre-shared key: W SSH Keys: E TLS Keys: E ANSI X9.31 seed and key: E
Configure Secure IPSEC Connection to the External Authentication, Time and Audit Servers	Crypto Officer	IPSec/IKE pre-shared key: W SSH Keys: E TLS Keys: E ANSI X9.31 seed and key: E
Wireless Security Protocol configuration (802.11i , EAP-TLS, EAP-TTLS, EAP-PEAP)	Crypto Officer	802.11i pre-shared key: W EAP-TTLS, PEAP passwords: W EAP-TLS certificates: W SSH Keys: E TLS keys: E ANSI X9.31 seed and key: E
View Wireless Intrusion Detection Logs	Crypto Officer	TLS keys: E SSH Keys: E
Password protection configuration	Crypto Officer	Password: W SNMP secret: W

Service	**Role**	**Access to Cryptographic Keys and CSPs** **R- read; W – write or generate; E-execute**
Establishment of secure network connection	User	TLS keys: E IPSec/IKE keys: E TLS/EAP Certificate: E 802.11i keys: E ANSI X9.31 seed and key: E

5 Security Functions

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

Algorithm	Certificate Number
SHS	1063, 1064
HMAC	652, 653
Triple DES	831, 832
AES	1147, 1148, 1149, 1150
RSA	543
ANSI X9.31 PRNG	635, 636

The table below lists non-Approved cryptographic algorithms employed by the module

Algorithm	Usage
MD5	Used by EAP-TLS, EAP_TTLS and EAP-PEAP protocols Used during TLS handshake Used by the SNMP protocol
HMAC-MD5	Used by the SNMP protocol
DES	Used by the SNMP protocol
AES	Used by the SNMP protocol
SHS	Used by the SNMP protocol
Diffie-Hellman	Used for key establishment in TLS, IPSec/IKE, and SSH[1] handshake. Provides 80 bits of encryption strength.
RSA encrypt/decrypt	Used for key establishment in TLS handshake. Provides 80 bits of encryption strength.

[1] SSH version 2 is used.

6 Key Management

The module uses ANSI X9.31 PRNG to generate random data.

The module provides a key zeroization command, which zeroizes all private and secret cryptographic keys and CSPs stored in flash memory. The command is followed by a reboot which zeroizes keys and CSPs stored in RAM.

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

Name and type	Usage	Storage
TLS master secret	Used to derive TLS data encryption key and TLS HMAC key	Plaintext in RAM
TLS Triple-DES or AES encryption keys	Used to encrypt data in TLS protocol	Plaintext in RAM
TLS HMAC keys	Used to protect integrity of data in TLS protocol	Plaintext in RAM
TLS/EAP server RSA certificate (including the private key)	Used to encrypt the TLS master secret during the TLS handshake	Plaintext in RAM Plaintext in flash
TLS and IPSec/IKE, and SSH Diffie-Hellman keys	Used for key establishment during the handshake	Plaintext in RAM
EAP-TLS Certification Authority RSA Certificate	Used to verify client certificate during the EAP-TLS handshake	Plaintext in RAM Plaintext in flash
SSH RSA key pair	Used to authenticate the module to the SSH client during the SSH handshake	Plaintext in RAM Plaintext in flash
SSH master secrets	Used to derive SSH encryption key and SSH HMAC key	Plaintext in RAM
SSH Triple-DES or AES encryption keys	Used to encrypt SSH data	Plaintext in RAM
SSH HMAC keys	Used to protect integrity of SSH data	Plaintext in RAM
IPSec/IKE pre-shared key	Used to derive IPSec/IKE encryption keys and IPSec/IKE HMAC keys	Plaintext in RAM Plaintext in flash
IPSec/IKE Triple-DES or AES encryption keys	Used to encrypt IPSec/IKE data	Plaintext in RAM
IPSec/IKE HMAC keys	Used to protect integrity of IPSec/IKE data	Plaintext in RAM

Name and type	Usage	Storage
ANSI X9.31 PRNG1 Seed and Seed Key	Used to initialize the PRNG to a random state	Plaintext in RAM
ANSI X9.31 PRNG2 Seed and Seed Key	Used to initialize the PRNG to a random state	Plaintext in RAM
802.11i AES-CCM Temporal Key	Used to secure unicast wireless data	Plaintext in RAM
802.11i AES-CCM Group Temporal Key	Used to secure multicast wireless data	Plaintext in RAM
802.11i pre-shared key	Used to derive 802.11i Temporal Key and 802.11i Group Temporal Key	Plaintext in RAM Plaintext in flash
Firmware load verification HMAC SHA-1 Key	Used to verify firmware components	Plaintext in RAM Plaintext in flash
Passwords	Used to authenticate users	Plaintext in RAM Plaintext in flash
SNMP secret	Used to authenticate Crypto Officers accessing SNMP management interface	Plaintext in RAM Plaintext in flash
IDS Server RSA Public Key and RSA Client Certificate	Used to establish TLS 1.0 connection to the external IDS server	Plaintext in RAM Plaintext in flash

7 Self Tests

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

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

Algorithm	Test
Firmware integrity	**Firmware integrity test using SHA-1**
For each AES implementation	Known Answer Test
For each TDES implementation	Known Answer Test
For each SHS implementation	Known Answer Test
For each HMAC implementation	Known Answer Test
For each ANSI X9.31 PRNG implementation	Known Answer Test
RSA	Pairwise Consistency Check (Sign/Verify)

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

Condition	Test
Random Number Generation	Continuous PRNG Test

Condition	Test
Firmware Load	Firmware Load Test
RSA Key Pair generation	Pairwise Consistency Check (Sign/Verify, Encrypt/Decrypt)
Bypass	Bypass Test

8 Physical Security

The module consists of production-grade components enclosed in a metal enclosure. The enclosure is opaque within the visible spectrum. The top panel of the enclosure can be removed by unscrewing screws.

The module is protected by three tamper evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements. The three tamper evident labels are applied over the panels and sides of the module at the factory to provide evidence of tampering.

An image of the module with tamper evident labels applied is provided below:

9 Secure Operation

9.1 Approved Mode of Operation

The module always operates in the Approved Mode of Operation and does not support a non-Approved mode of Operation. The following message is output to the command line interface and the Web User Interface: "This Device Is Running In FIPS Mode". Module documentation provides detailed guidance for the module users and Crypto Officers.

The Crypto Officer periodically inspects the module and the tamper evident labels. If an evidence of tampering is detected, the Crypto Officer shall immediately disable the module and notify the management.

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

When the module is received from the factory, it includes default Crypto Officer username/password. The Crypto Officer shall connect to the module using the serial interface and change the password to the non-default value before letting other users to operate the module.