FIPS 140-2 Level 2 Security Policy

For

MOTOROLA

WS5100 Wireless Switch

Document Version 0.4

Table of Contents

1 Module Description

The Motorola WS5100 Wireless Switch is a rack-mountable device that manages all inbound and outbound traffic on the wireless network. It provides security, network services, and system management applications. The switch uses centralized, policy-based management to apply sets of rules or actions to all devices on the wireless network. Management "intelligence" is collected from individual access points, and the collected information is moved into the centralized wireless switch.

The module is used to control operation of multiple wireless access points and to provide secure Wireless Local Area Network (WLAN) connectivity to a set of wireless client devices. The module is installed at a wired network location, and is connected to a set of wireless access point devices over a wired Ethernet network. Wireless access point devices are hardware radio devices, which do not provide security functionalities and are used to tunnel wireless network traffic between the module and wireless client devices. 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 WS5100 Wireless Switch is classified as multi-chip standalone module.

FIPS 140-2 conformance testing of the module was performed at Security Level 2. The following configurations were tested:

Module Name and Version	**Firmware versions**
WS5100 Wireless Switch	WS5100-3.0.0.0-020GR

2 Cryptographic Boundary

The complete set of hardware and firmware components of the WS5100 Wireless Switch is physically enclosed in a metal and hard plastic enclosure which serves as the cryptographic boundary of the module. The enclosure consists of the following parts: top, front, left, right, rear, and bottom panels of the case. The top panel can be removed 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:

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	2	Status Output
Power Switch	1	Control Input
Power Port	1	Power Input

4 Roles, Services and Authentication

The module provides the following roles: a User role, a Crypto Officer role, a System Administrator role, and a Monitor User role.

The Crypto Officers and System Administrators configure the module and manage its cryptographic functionality. The Monitor Users monitor the operation of the module. 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 System Administrator Monitor User	Passwords are used for connections via Command Line Interface (CLI). 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 System Administrator	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 System Administrator Monitor User	Password: E SSH Keys: E ANSI X9.31 seed and key: E
Run self-test	Crypto Officer System Administrator Monitor User	N/A
Show status	Crypto Officer System Administrator Monitor User	N/A
Reboot	Crypto Officer System Administrator Monitor User	N/A
Update firmware	Crypto Officer System Administrator	Firmware load verification RSA Public Key: E
Zeroize/Restore factory settings	Crypto Officer System Administrator	All keys: W
IPSec/VPN configuration	Crypto Officer	IPSec/IKE pre-shared key: W SSH Keys: E ANSI X9.31 seed and key: E
802.11i configuration	Crypto Officer	802.11i pre-shared key: W SSH Keys: E ANSI X9.31 seed and key: E
Password protection configuration	Crypto Officer System Administrator	Password: E
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	744, 745
HMAC	392, 393
Triple DES	648, 649
AES[1]	726, 727, 772

[1] The maximum effective AES key length is 232 bits.

Algorithm	Certificate Number
RSA Sign/verify	341
ANSI X9.31 PRNG	423, 424
DSA	274

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

Algorithm	Usage
MD5	Used by inner TTLS protocol Used during TLS handshake
Diffie-Hellman	Used for key establishment in TLS, IPSec/IKE, and SSH[2] handshake. Provides between 80 and 112 bits of encryption strength.
RSA encrypt/decrypt	Used for key establishment in TLS handshake. Provides 80 bits of encryption strength.

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 key	Used to encrypt data in TLS protocol	Plaintext in RAM
TLS HMAC key	Used to protect integrity of data in TLS protocol	Plaintext in RAM
TLS/EAP server RSA certificate[3] (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

[2] SSH version 2 is used.

[3] The same certificate is shared by EAP-TLS, EAP-PEAP and EAP-TTLS protocols.

Name and type	Usage	Storage
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 secret	Used to derive SSH encryption key and SSH HMAC key	Plaintext in RAM
SSH Triple-DES or AES encryption key	Used to encrypt SSH data	Plaintext in RAM
SSH HMAC key	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
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 RSA Public Key	Used to verify firmware components	Plaintext in RAM Plaintext in flash
Passwords	Used to authenticate users	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
AES	Known Answer Test
TDES	Known Answer Test
SHS	Known Answer Test
HMAC	Known Answer Test
ANSI X9.31 PRNG	Known Answer Test
RSA	Pairwise Consistency Check (Sign/Verify)
DSA	Pairwise Consistency Check (Sign/Verify)

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

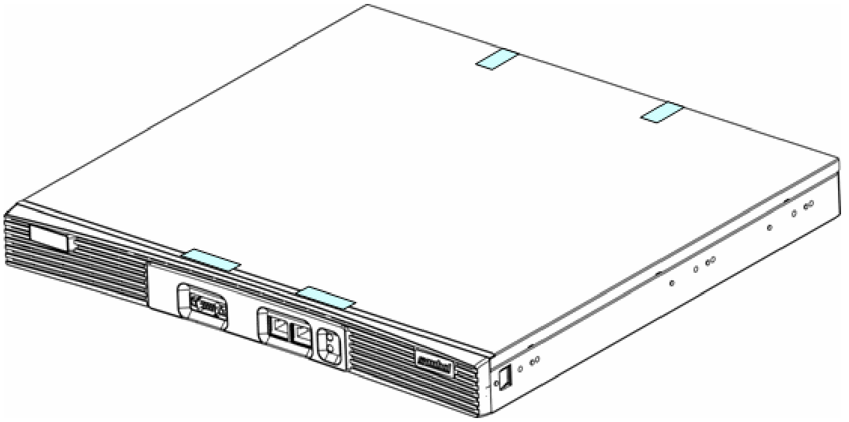
Condition	Test
Random Number Generation	Continuous PRNG Test
Firmware Load	Firmware Load Test
RSA Key Pair generation	Pairwise Consistency Check (Sign/Verify, Encrypt/Decrypt)
Bypass	Bypass Test

8 Physical Security

The module consists of production-grade components enclosed in a metal and hard plastic 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 tamper evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements. The tamper evident labels are applied over the top panel and a side of the module at the factory to provide evidence of tampering if the top panel is removed.

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. Module documentation provides detailed guidance for the module users and administrators.

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 administrators shall keep all authentication data confidential and shall not allow access to the module to unauthorized persons.