FIPS 140-2 Security Policy

for

Motorola, Inc

Fusion 802.1X Authentication Supplicant

Software Module

Version: H_3.40.0.0.19

Document Version Number: 1.2

1. Module Description

Motorola Fusion 802.1x Authentication Supplicant is a component of Motorola Wireless Mobile Computing devices that are equipped with a WLAN radio. These devices are used for business process automation applications in a number of vertical markets like retail, manufacturing, transportation, health and government

For the purposes of FIPS 140-2 the module is classified as a software module.
This software module includes the following components:

- wpasvc.dll software component

The software module is installed into a GPC, which typically has handheld dimensions and provides wireless functionality. Since the GPC where the module is installed is a multi-chip standalone device, the module is qualified as a multi-chip standalone module.

The main purpose of the module is to function as an 802.1X authentication supplicant, and in that context to provide cryptographic services.

FIPS 140-2 conformance testing of the module was performed at Security Level 1. The following configurations were tested by the lab:

Software Component Version	**Operating System**	**Hardware Component Version**
wpasvc.dll H_3.40.0.0.19	Windows Mobile 6.5 OS OEM Version 2.31.0002	ES400 MC65

The following table summarizes FIPS 140-2 compliance claims

Security Requirements Section	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1

Security Requirements Section	Security Level
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of other attacks	N/A

2. Cryptographic Boundary

The logical cryptographic boundary of the module includes the wpasvc.dll software binary (software component).

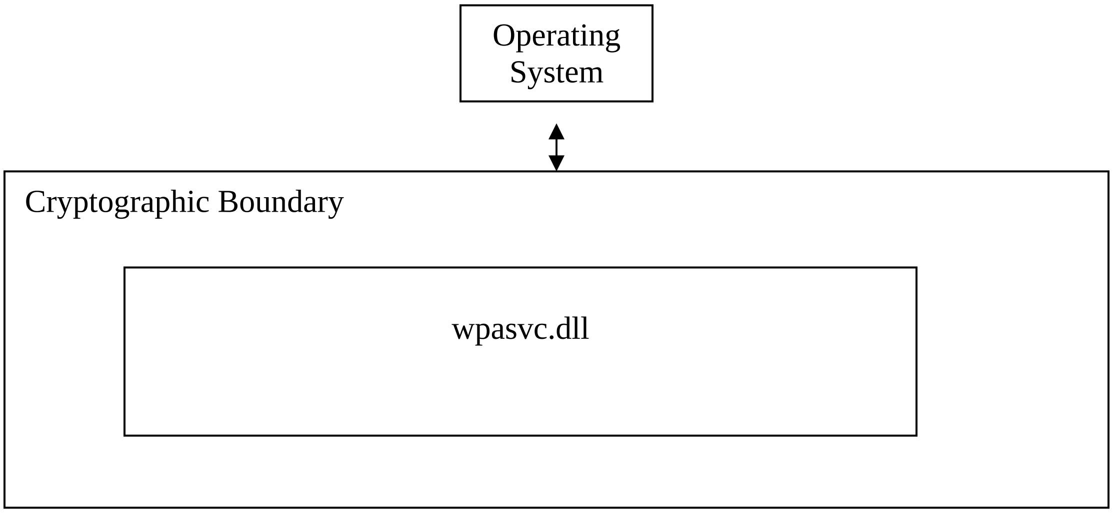
The module includes the following logical interfaces:

- Control Input Interface: software API commands and command parameters used to control and configure module operation.
- Status Output Interface: return values from software API commands used to obtain information on the status of the module.
- Data Input Interface: data inputs to the software API commands and network packets containing 802.1X authentication information sent through an OS-supplied interface.
- Data Output Interface: network packets containing 802.1X authentication information sent through an OS-supplied interface.

All module interfaces, inputs and outputs are provided by the software component.

The block diagram for the module is provided below.

Figure 1. Block Diagram



3. Roles and Services

The module provides the following roles:

1. User.
2. Crypto Officer.

The Crypto Officer configures the module and manages its cryptographic functionality. The User employs the cryptographic services provided by the module.

The module provides the following services to the User and Crypto Officer.

Service	Role	Access to Cryptographic Keys and CSPs R- read or use W – write or generate, Z – zeroize N/A – no CSPs are accessed by this service
Run-self tests	Crypto Officer	N/A
Get status of the module	Crypto Officer	N/A
Perform wireless association protocol handshake using one of the following Approved protocol implementations: EAP-TLS EAP-PEAP EAP-PEAP with EAP-TLS EAP-TTLS or one of the following non-Approved protocol implementations: EAP-FAST LEAP CCKM WAI AKMP (Chinese Government) This service will operate in a non-Approved mode unless the approved mode of operation is enabled by the Crypto Officer as specified in Section 7.	User	The following Keys and CSPs are associated with each Approved EAP-TLS, EAP-PEAP, EAP-PEAP with EAP-TLS, and EAP-TTLS protocol implementation: TLS master secret: W TLS Triple-DES or AES encryption key: W TLS HMAC key: W TLS Diffie-Hellman keys: W TLS Server Public Key: R 802.11i EAP PMK: W 802.11i pre-shared PMK: R 802.11i PTK: W 802.11i GTK: R ANSI X9.31 seed and key: W The client certificate is only associated with EAP-TTLS: Client Certificate: R
Zeroize	Crypto Officer	Z zeroizes all keys

4. Security Functions

The table below lists approved cryptographic algorithms employed by the module

Algorithm	Certificate #
AES	1853
RSA	936
DSA	578
TDES	1200
HMAC	1100
SHS	1630
RNG	971

In the non-Approved mode of operation the module implements the following non-Approved cryptographic algorithms: DES, RC4, RC2, MD5, IDEA, RSA with key length less than 1024 bit, DSA with key length less than 1024 bit, Diffie-Hellman with key length less than 1024 bit, SMS4 (Chinese Government), CCKM (Cisco proprietary)

5. Key Management

The following cryptographic keys are supported by the module

Name and Type	Generation or establishment	Usage
TLS master secret	Established during TLS handshake	Used to derive TLS data encryption keys and TLS HMAC key
TLS Triple-DES or AES encryption key	Established during TLS handshake	Used to encrypt data within TLS protocol
TLS HMAC key	Established during TLS handshake	Used to protect integrity of data within TLS protocol
TLS Diffie-Hellman keys	Established during TLS handshake	Used for key establishment during the handshake
ANSI X9.31 PRNG Seed and Seed Key	Derived from an entropy source	Used to initialize the PRNG to a random state
802.11i Protocol session keys: EAP or pre-shared Pairwise Master Key(PMK) Pairwise Temporal Key (PTK) Group Temporal Key (GTK)	The PMK, PTK, and GTK are established during the 802.11i protocol handshake The pre-shared PMK is entered by the calling application	Encryption and authentication of wireless data
RSA or DSA Client Certificate	Entered by the calling application	Used as an authentication credential
TLS Server RSA or DSA Public Key	Received over the air from the EAP server	Encryption (RSA) and digital signatures (RSA and DSA) during the EAP protocol handshake

All keys are stored inside the module in plaintext. The module does not provide functionality to output cryptographic keys.

To zeroize the keys inside the logical cryptographic boundary one shall power down the GPC, which will also power down the module. Since all keys stored in the module are stored in the volatile memory, powering down the module destroys the keys.

6. Self Tests.

If the module has been configured for FIPS mode, 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 self-test success or error status is queried from the module.

The module runs power-on self-tests for the following algorithms

Algorithm	Test
AES	Known Answer Test (encrypt/decrypt)
TDES	Known Answer Test (encrypt/decrypt)
RNG	Known Answer Test
RSA	Known Answer Test
DSA	Pairwise consistency test (sign/verify)
SHA-1	Tested during the integrity check
HMAC SHA-1	Tested during the integrity check

During the execution of the module a continuous random number generator test is performed for RNG.

7. Approved Mode of Operation

The approved mode of operation is enabled by the Crypto Officer role.

At boot-up time when the drivers are loaded, the module is transitioned into Approved mode upon receipt of a command via a text-based, OS-supplied message queue.
The exact command is “ENABLE_FIPS_MODE”.

Upon receiving this command, the module runs a Self Integrity Test (SIT) which calculates the HMAC-SHA1 digest over the module’s file (wpasvc.dll) and compares it to a digest that was pre-calculated and stored in a file. If that test succeeds, the module calls the tests for crypto algorithms.

The external application that set the module into FIPS mode polls the module for the FIPS tests result using the command “GET_FIPS_TESTS_RESULT”. The command returns “OK: passed” to the caller upon successful completion of the FIPS tests. Otherwise an error-specific message or a message indicating that the tests are still running is returned.

In order for the module to stay in the Approved mode of operation, the following protocols implemented by the module shall not be used by the operator: WEP, WPA, TKIP, SMS4, WAI AKMP, CCKM.

In order for the module to stay in the Approved mode of operation one shall not use the module with digital certificates less than 1024 bits in length.

The following 802.1X authentication protocols, used in conjunction with WPA2-Enterprise or WPA2-Personal, and AES encryption, are available in the Approved mode

1. EAP-TLS
2. EAP-PEAP with any of the tunnel types:
    a. MSCHAPv2
    b. EAP-TLS
    c. EAP-GTC
3. EAP-TTLS with any of the tunnel types:
    a. PAP
    b. CHAP

c. MSCHAP

d. MSCHAPv2

e. MD5

The following policies must be adhered to in order for the module to stay in the Approved Mode:

- use only WPA2-Enterprise setting or WPA2-Personal setting.

- use only AES encryption setting.

- use only EAP-TLS, EAP-PEAP with any tunnel type, or EAP-TTLS with any tunnel type.

- must NOT specify the use of a user certificate when EAP-TTLS is used.

- have both the “Allow Motorola HFSR” and “Allow Cisco CCKM” checkboxes unchecked.

- set up infrastructure devices (such as Access Points) to include AES in the pair-wise cipher suite, and to only offer AES for the group cipher suite.