Motorola Solutions, Inc.
Fusion Wireless LAN Cryptographic Module for Android

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.07

Date: September 10, 2014

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Fusion Wireless LAN Cryptographic Module for Android, hereafter denoted the Module. The Module is used for encrypting/decrypting Wireless LAN data in Motorola Solutions' mobile computers running Android Jelly Bean 4.1.1 Operating System. The Module meets FIPS 140-2 overall Level 1 requirements.

For the purposes of FIPS 140-2, the Module is classified as a software hybrid module.

This hybrid module includes the following components:

Table 1 – Cryptographic Module Configurations

Software Component Version	**HW Component P/N and Version**	**FW Version** (FIPS component of firmware_fips.bin)	**OE**	**Platform**
libfirmware_loader.so Version: 1.02	WL1283CYFVR (Rev C)	1.01	Android Jelly Bean 4.1.1 on TI OMAP4 (processor)	MC40N0

The Module is integrated into Motorola Solutions' Mobile Computers and provides Wireless LAN cryptographic functionality. The Module is classified as a multi-chip standalone embodiment; the cryptographic boundary includes a software and firmware component as well as a hardware component that handles cryptographic functionality.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.1 Hardware and Physical Cryptographic Boundary

Physical Cryptographic Boundary is the mobile computer that integrates the Module. The module's hardware component is depicted in Figure 1. Figure 2 shows two (2) different connectivity chips that integrates Texas Instruments' WL1283 chipset (The module's hardware component), highlighted in red. Mobile Computers using TI OMAP4 Android Jelly Bean 4.1.1 based platform use one of the below connectivity chips shown in Figure 2.

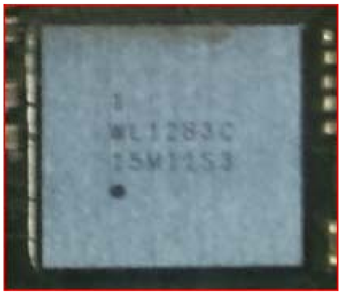

Figure 1 – Module Hardware Component

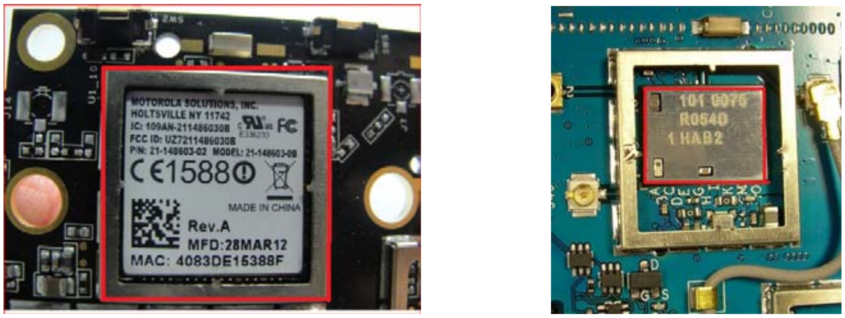

Figure 2 – Module Hardware Component Integrated to Connectivity Chip

Table 3 – Ports and Interfaces

Description	Logical Interface Type
Software/Firmware APIs to provide parameters for controlling and configuring the Module.	Control in
Return values from Software/Firmware APIs that indicates the status of the Module.	Status out
APIs to pass data to the Module	Data in
Data output from the APIs	Data out

1.2 Logical Cryptographic Boundary

Figure 3 depicts the Module’s operational environment.

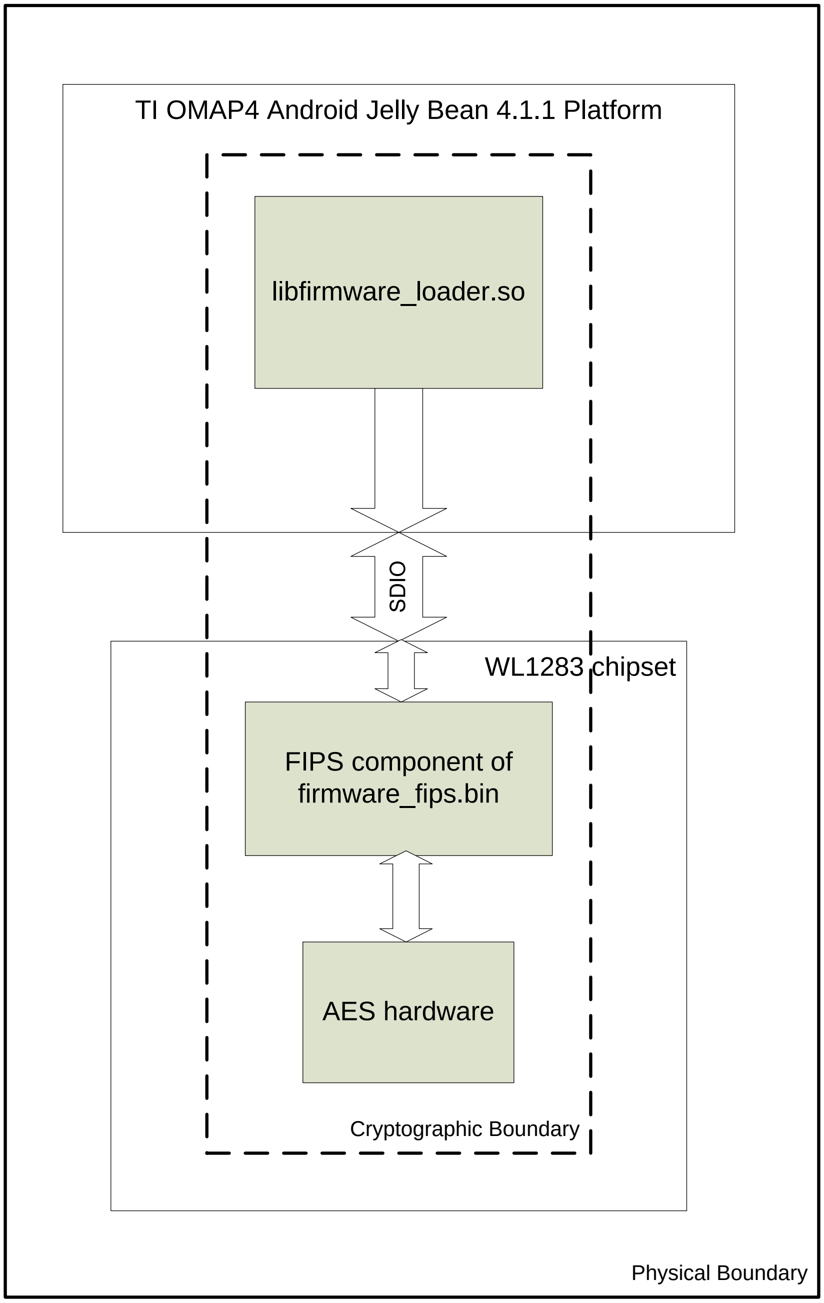

Figure 3 – Module Block Diagram

The logical cryptographic boundary only includes the components shown within Cryptographic Boundary in Figure 3. The software library (libfirmware_loader.so) will load the firmware to host processor memory which in turn gets downloaded to the WL1283 chipset. The FIPS component of the firmware file will drive the cryptographic hardware component. The AES hardware shown in Figure 3 does AES-CCMP encryption and decryption. The logical boundary only includes the AES-CCMP core inside the WL1283 chipset.

1.3 Modes of Operation

The Module operates in FIPS Approved mode when FIPS mode is enabled in the software and the FIPS firmware is loaded to WL1283 chipset.

Wi-Fi must be enabled on the OMAP4 based Android mobile device to use the module. When Wi-Fi is enabled, the firmware loader (libfirmware_loader.so) loads firmware_fips.bin to WL1283 chipset after running necessary integrity tests. The module's software API command AES_POST_STATUS will return the status of Power on Self Tests. The firmware loader library provides a software API to check the integrity test status.

2 Cryptographic Functionality

The Module implements the FIPS Approved cryptographic functions listed in the Table 4 below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption Modes: ECB Key sizes: 128	2812
CCM	[SP 800-38C] Functions: Generation, Verification Key sizes: 128	2812
HMAC	[FIPS 198-1] Functions: HMAC-SHA256 is used for the integrity test of the firmware loader and the FIPS component of the firmware. SHA sizes: SHA-256	1763
SHA	[FIPS 180-4] Functions: HMAC-SHA256 is used for the integrity test of the firmware loader and the FIPS component of the firmware. SHA sizes: SHA-256	2360

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
AES_KEY	128-bit AES key used for CCM encryption or decryption

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two (2) distinct operator roles, User and Cryptographic Officer (CO). The Module does not employ authentication mechanisms to control access. The roles are implicitly selected when Module is operated. Table 6 lists all operator roles supported by the module. The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators.

Table 6 – Roles Description

Role ID	Role Description
CO	Cryptographic Officer – Configures the module by setting the key.
User	User – Uses the cryptographic services provided by the module.

3.2 Services

All services implemented by the Module are listed in the table below. Each service description also describes all usage of CSPs by the service.

Table 7 – Services

Service	Description	CO	U
Module reset (Self-test)	Reset the module by power cycling the WLAN radio. The Self-tests are run when this service is invoked.	X	
Get status	Provides the Self Integrity Test status and Power On Self Test status (API)	X	
Get Version	Provides the version of components (API)	X	
Set key	Provide AES key to the module	X	
Encrypt/decrypt data	Encrypts or decrypts data (API)		X
Zeroize	Zeroizes the key	X	

Table 8 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 8 – CSP Access Rights within Services

Service	CSPs
	AES_KEY
Module reset	Z
Get status	-
Get version	-
Set key	W
Encrypt/decrypt data	E
Zeroize	Z

4 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 9 below. All integrity tests and KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the integrity tests or KATs fails, the Module enters the SOFT_ERROR error state. Module will indicate self-test failure by returning failure status code for Get Status API. As a result of the Module entering the error state, the WLAN stack on the platform will keep the radio in a disabled state.

Table 9 – Power Up Self-tests

Test Target	Description
Firmware loader integrity	HMAC-SHA256 integrity check is performed when the Mobile Device is configured to operate in FIPS Approved mode.
Firmware Integrity	HMAC-SHA256 integrity check is performed when the firmware is loaded onto the WL1283 chip.
CCM	KATs: Generation, Verification Key size: 128

5 Physical Security Policy

The module is housed in a production grade enclosure. Motorola Solutions uses production grade components in the manufacturing of the module and Mobile Device.

6 Operational Environment

The Module is designated as a modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware loader software library that reads the firmware and loads it into the hardware. The Module is integrated into Mobile Devices that uses the OMAP4 based Android Jelly Bean 4.1.1 platform. The software library (libfirmware_loader.so) runs in the context of Android Jelly Bean 4.1.1 Operating System. Only a single user can operate the Module at a time.

7 Mitigation of Other Attacks Policy

The module does not implement mitigation for any other attacks.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The operator can command the module to perform the power up self-tests by cycling power or resetting the module.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not have any external input/output devices used for entry/output of data.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 10 – References

Abbreviation	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
[FIPS 197, SP 800-38A]	ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001. Recommendation for Block Cipher Modes of Operation, December 2001.
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC), July 2008
[FIPS 180-4]	Secure Hash Standard (SHS), March 2012

Table 11 – Acronyms and Definitions

Acronym	Definition
API	Application Program Interface
LAN	Local Area Network
OMAP	Open Multimedia Applications Platform
TI	Texas Instruments
WLAN	Wireless Local Area Network