WiLink™ 8 Cryptographic Engine

Part Number(HW): WL1837MOD

Firmware Version 100860185

Non-proprietary FIPS 140-2 Security Policy

Version 1.2

2021-09-14

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1. Cryptographic Module Specification 4
1.1. Module Overview 4
1.2. FIPS 140-2 Validation 5
1.3. Modes of operation 6
2. Cryptographic Module Ports and Interfaces 7
3. Roles, Services and Authentication 9
3.1. Roles 9
3.2. Services 9
3.3. Algorithms 9
3.4. Operator Authentication 10
4. Physical Security 11
5. Operational Environment 12
6. Cryptographic Key Management 13
6.1. Key Generation 13
6.2. Key Entry / Output 13
6.3. Key Storage 13
6.4. Key Zeroization 13
7. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) 14
8. Self Tests 15
8.1. Power-Up Tests 15
8.2. On-Demand Self-Tests 15
9. Guidance 16
9.1. Crypto Officer Guidance 16
9.1.1. Prerequisites 16
9.1.2. Module installation 16
9.2. User Guidance 16
9.2.1. API Functions 16
10. Mitigation of Other Attacks 17

Copyrights and Trademarks

IMPORTANT NOTICE

Texas Instruments Incorporated (TI) reserves the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

TI's published terms of sale for semiconductor products (http://www.ti.com/sc/docs/stdterms.htm) apply to the sale of packaged integrated circuit products that TI has qualified and released to market. Additional terms may apply to the use or sale of other types of TI products and services.

Reproduction of significant portions of TI information in TI data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such reproduced documentation. Information of third parties may be subject to additional restrictions. Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyers and others who are developing systems that incorporate TI products (collectively, "Designers") understand and agree that Designers remain responsible for using their independent analysis, evaluation and judgment in designing their applications and that Designers have
full and exclusive responsibility to assure the safety of Designers' applications and compliance of their applications (and of all TI products used in or for Designers' applications) with all applicable regulations, laws and other applicable requirements. Designer represents that, with respect to their applications, Designer has all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. Designer agrees that prior to using or distributing any applications that include TI products, Designer will
thoroughly test such applications and the functionality of such TI products as used in such applications.

TI's provision of technical, application or other design advice, quality characterization, reliability data or other services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using TI Resources in any way, Designer (individually or, if Designer is acting on behalf of a company, Designer's company) agrees to use any particular TI Resource solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

Designer is authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS. TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY DESIGNER AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Unless TI has explicitly designated an individual product as meeting the requirements of a particular industry standard (e.g., ISO/TS 16949 and ISO 26262), TI is not responsible for any failure to meet such industry standard requirements.

Where TI specifically promotes products as facilitating functional safety or as compliant with industry functional safety standards, such products are intended to help enable customers to design and create their own applications that meet applicable functional safety standards and requirements. Using products in an application does not by itself establish any safety features in the application. Designers must
ensure compliance with safety-related requirements and standards applicable to their applications. Designer may not use any TI products in life-critical medical equipment unless authorized officers of the parties have executed a special contract specifically governing such use.
Life-critical medical equipment is medical equipment where failure of such equipment would cause serious bodily injury or death (e.g., life support, pacemakers, defibrillators, heart pumps, neurostimulators, and implantables). Such equipment includes, without limitation, all medical devices identified by the U.S. Food and Drug Administration as Class III devices and equivalent classifications outside the U.S.

TI may expressly designate certain products as completing a particular qualification (e.g., Q100, Military Grade, or Enhanced Product). Designers agree that it has the necessary expertise to select the product with the appropriate qualification designation for their applications and that proper product selection is at Designers' own risk. Designers are solely responsible for compliance with all legal and regulatory requirements in connection with such selection.

Designer will fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of Designer's non- compliance with the terms and provisions of this Notice.

1. Cryptographic Module Specification

This document is the non-proprietary FIPS 140-2 Security Policy for WL1837MOD of the TI WiLink™ 8 Wi-Fi/BT Combo. This Security Policy contains the security rules under which the module must be operated and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level **1** module. The following sections describe the cryptographic module and how it conforms to the FIPS 140-2 specification in each of the required areas.

1.1. Module Overview

The WiLink™ 8 Cryptographic Engine (hereafter referred to as "the WiLink™ module" or "the module") provides IEEE 802.11i compliant AES-CCM mode encryption and decryption functionality for use in the WLAN MAC platform. It is optimized for 802.11 CCMP protocol and supports this mode only. The CCM mode is wrapped by a hardware (HW) accelerator which translates the WLAN packets into the required CCM parameters (nonce/IV, AAD payload).

Figure 1 is the high-level block diagram and shows the main components of the WiLink™ 8 chip. The physical boundary of the module under test is the continuous enclosure of the WiLink™ 8 chip indicated by the red rectangle. The Logical boundary of the module is indicated by the blue rectangle.

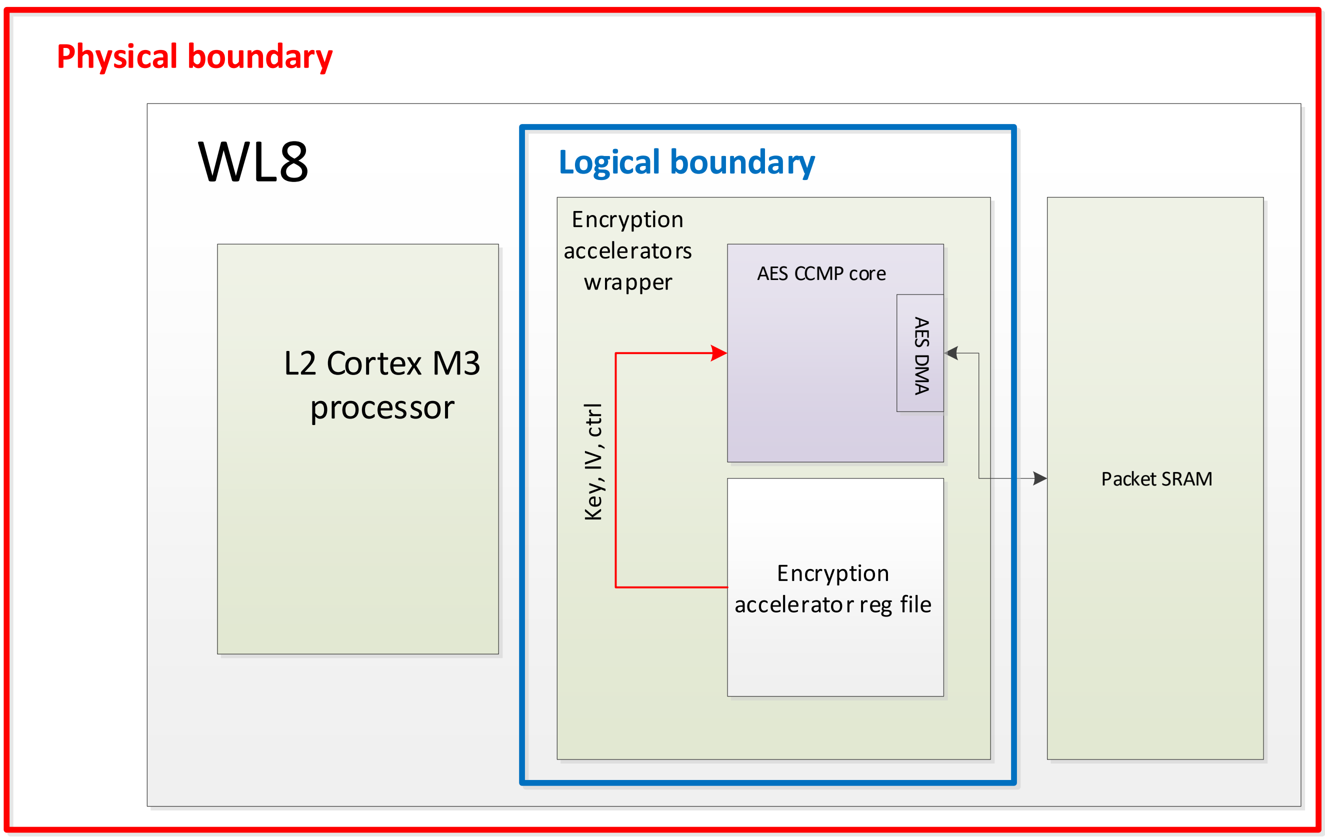

Figure 1 – Physical and Logical Boundaries of the module

The logical boundary of the module consists of the hardware implementation of AES-CCMP, the encryption accelerator register files and the firmware that runs and drives the AES hardware engine. The version of the firmware is 100860185.

For the purpose of the FIPS 140-2 validation, this is a hard circuitry core sub-chip module in a single-chip embodiment per FIPS 140-2 IG 1.20. Figure 2 shows the front and back view of the TI WiLink™ 8 chip.

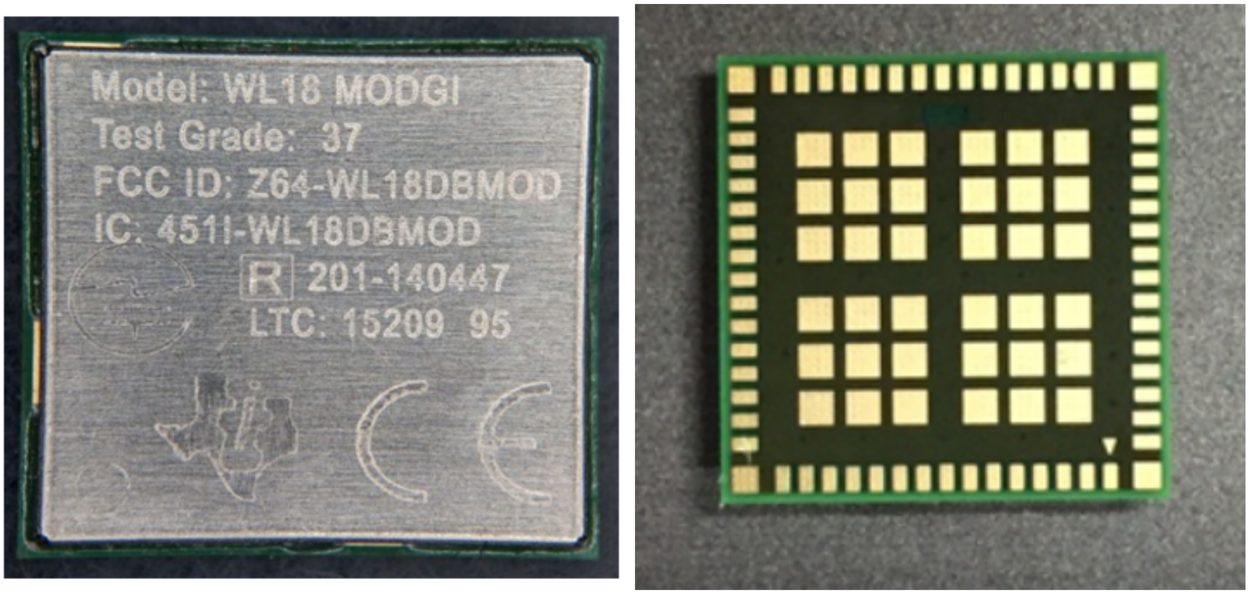

Figure 2 – Front and back views of the TI WiLink™ 8 chip.

1.2. FIPS 140-2 Validation

For the purpose of the FIPS 140-2 validation, the module is a hardware sub-chip module that resides on a TI WiLink™ 8 chip. It is to be validated at overall Security Level **1**. Table 1 shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard:

Table 1 - Security levels of each FIPS 140-2 sections.

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
Overall Level		**1**

1.3. Modes of operation

The module only supports the FIPS mode of operation. It enters the FIPS mode after the successful completion of Power-On Self-Test (POST).

2. Cryptographic Module Ports and Interfaces

Figure 3 is the elaborated diagram of the components of the module within the module's logical boundary (see Figure 1 for the depiction of the logical boundary).

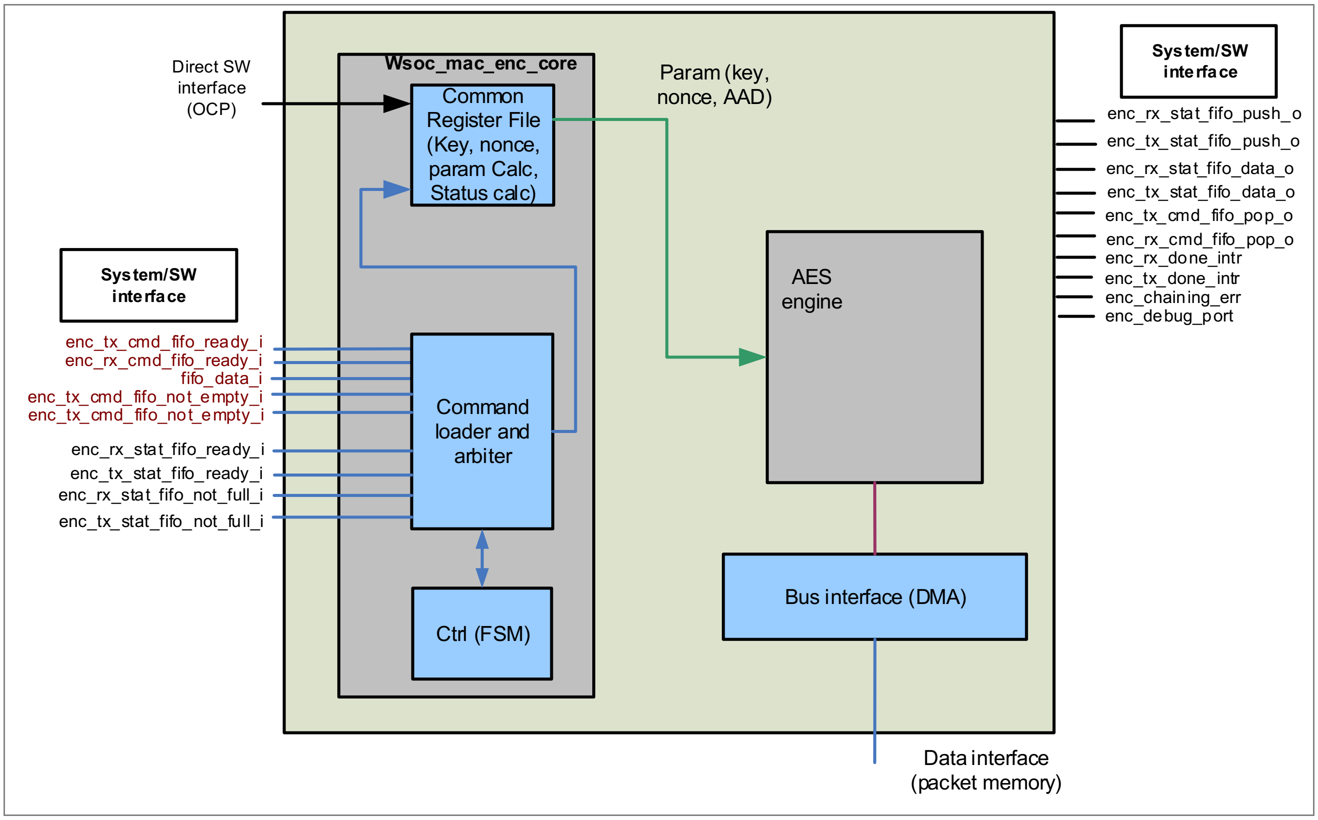

Figure 3 – Ports and interfaces of the module.

Table 2 summarizes the mapping between the four logical interfaces required by the FIPS 140-2 and the physical ports of the module:

Table 2 - Ports and interfaces of the module.

Logical Interface	Physical Port	Description
Data Input	OCP fifo_data_i DMA	SW (Software) interface – command word (command is comprised of 5 such words)
Data Output	OCP fifo_data_o DMA	HW response word (status of operation – pass/fail/bus_err)
Control Input	enc_tx_cmd_fifo_ready_i enc_rx_cmd_fifo_ready_i enc_tx_cmd_fifo_not_empty_i enc_rx_cmd_fifo_not_empty_i enc_tx_cmd_fifo_pop_o enc_rx_cmd_fifo_pop_o	Control interface to command fifo (SW interface fifo) The enc_debug_port does not contain or export the key, and this port is not used in the production module.

Logical Interface	Physical Port	Description
	enc_debug_port	
Status Output	enc_rx_stat_fifo_ready_i enc_tx_stat_fifo_ready_i enc_rx_stat_fifo_not_full_i enc_tx_stat_fifo_not_full_i enc_rx_stat_fifo_push_o enc_tx_stat_fifo_push_o enc_rx_stat_fifo_data_o enc_tx_stat_fifo_data_o enc_rx_done_intr enc_tx_done_intr enc_chaining_err	Control interface to status fifo (SW interface fifo) Interrupt signals exist but are not directly used (status fifo not empty is used to signal completion)
Power input	Power Supply Port	Not applicable for the sub-chip module. The module receives power from the device in which the module is embedded.

3. Roles, Services and Authentication

3.1. Roles

The module supports the following roles:

- **User role**: performs all services, except module installation and configuration.
- **Crypto Officer role**: performs module installation and configuration.

The User and Crypto Officer roles are implicitly assumed by the entity accessing the module services.

3.2. Services

The module provides services to users who assume one of the available roles. Table 3 shows the approved services in FIPS mode of operation, the cryptographic algorithms supported for each service, the roles that can perform each service, and the keys involved and how they are accessed. Since the module always operates in FIPS mode, Table 3 includes all services. The details about the AES algorithm supported by the module are found in Section 3.3.

Table 3 - Services in the FIPS mode of operation.

Service	Algorithms	Role	Access	Keys
Cryptographic Library Services				
Symmetric encryption and decryption	AES (ECB[1], CCM)	User	Read	AES keys
Other FIPS-related Services				
Show status	n/a	User	N/A	None
Self-Tests	AES	User	N/A	None
Module installation (e.g., importing AES keys)	n/a	Crypto Officer	Write	AES keys
Module configuration (e.g., updating AES keys)	n/a	Crypto Officer	Write	AES keys
Zeroization	n/a	Crypto Officer	Write	AES keys

3.3. Algorithms

The AES algorithm that is implemented in the module and approved to be used in FIPS mode of operation is tested and validated by the CAVP. Table 4 shows the cryptographic algorithms that are approved in FIPS mode of operation.

[1] AES CCM service uses AES-ECB encryption internally.

Table 4 - FIPS-Approved cryptographic algorithms.

CAVP Cert#	Algorithm	Standard	Mode / Method	Key size	Use
#5324	AES	[FIPS197] [SP800-38A]	ECB, CCM	128 bits	Data Encryption and Decryption[2]

3.4. Operator Authentication

The module does not implement user authentication. The role of the user is implicitly assumed based on the service that is requested.

[2]For AES-ECB the module only implements the encrypt function and hence only encryption operation is CAVP tested

4. Physical Security

The module is a sub-chip module implemented as part of the TI WiLink™ 8 chip. The TI WiLink™ 8 chip defines the physical boundary of the sub-chip module.

The TI WiLink™ 8 chip is a single chip with a production-grade enclosure and hence conforms to the Level 1 requirements for physical security.

5. Operational Environment

The module is a hardware sub-chip module as part of TI WiLink™ 8 chip. The procurement, build and configuring procedures are controlled. Therefore, the operational environment is considered non-modifiable.

6. Cryptographic Key Management

Table 5 summarizes the keys that are used by the cryptographic services implemented in the module:

Table 5 - Life-cycle of AES keys.

Name	Generation	Entry and Output	Storage	Zeroization
AES keys	N/A. Keys are externally generated.	Keys enter the module via the data input interface as shown in Section 2. There is no key output.	Stored in register within the module	The on-demand zeroization is done via power-off and then power-on again. Key zeroization can also be done by explicitly setting the ‘Key’ registers in the ‘wsoc_mac_enc’ to 0 by the SW (Software).

6.1. Key Generation

The module does not generate any keys or Critical Security Parameters (CSPs).

6.2. Key Entry / Output

The module does not support manual key entry or intermediate key output. AES keys are generated outside of the cryptographic logical boundary of the device, e.g., via the IEEE 802.11i 4-way handshake process that generates the Temporal Key (TK) utilized by the AES-CCMP. In this process, an operator typically enters a pre-shared key (PSK) via a user interface (e.g., in the case of WPA2-PSK). The PSK is utilized in the 4-way handshake to finally derive the AES keys, again outside of the cryptographic boundary of the module. The AES keys are then provided to the module via the dedicated data input interface.

The module does not output keys in plaintext format outside its physical boundary.

6.3. Key Storage

The AES key is stored in the register within the module. The module does not provide persistent key storage.

6.4. Key Zeroization

The AES key is zeroized when the module is powered off. An alternative method consists in setting the ‘key’ registers in the ‘wsoc_mac_enc’ to 0 by the SW (Software).

7. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The sub-chip module is not a standalone device. As a hardware component, it cannot be certified by the FCC. It is rather intended to be used within a larger device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the module is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment with the module embedded prior to further marketing to a vendor or to a user.

8. Self Tests

8.1. Power-Up Tests

The module performs the integrity check on its firmware via a CRC-16 checksum. The CRC-16 values are part of the module and computed upon production of the module by the vendor.

The module only implements one FIPS-Approved cryptographic algorithm, AES. It performs a Known-Answer Test (KAT) for AES as shown in Table 6:

Table 6 - Self-Tests performed by the module.

Algorithm	Test
AES	• KAT for AES-CCM with 128-bit key, encryption • KAT for AES-CCM with 128-bit key, decryption

For KAT, the module calculates the result of a cryptographic operation and compares it with the known value of the answer. If the computed answer does not match the known answer, the KAT fails and the module enters the Error state, wherein no cryptographic services are available and data output is prohibited.

The module performs the power-up self-tests when it is powered-on, without any operator intervention. The power-up self-tests ensure that the AES algorithm implementation works as expected.

While the module is executing the power-up self-tests, cryptographic services are not available, and data input and output are inhibited. The module is not available to be used until the power-up self-test are completed successfully.

8.2. On-Demand Self-Tests

On-Demand self-tests can be invoked by powering-off and powering-on the module again, thus forcing the module to run the power-up self-tests.

9. Guidance

9.1. Crypto Officer Guidance

The module is delivered as part of the firmware binary that is installed in the hardware device that utilizes the TI WiLink™ 8 chip. The vendor provides the TI WiLink™ 8 chip to OEM integrators who integrate the TI WiLink™ 8 chip into their hardware devices.

The firmware includes the module and other components that drive the hardware device, such as PHY and MAC network layer functions, etc. The firmware binary is not available for direct download to the general public, nor is its source code.

9.1.1. Prerequisites

The OEM integrators obtain the firmware binary from a version-controlled GIT repository hosted by the vendor. Access to the TI-hosted repository is granted after the OEM integrators register via a registration webpage.

The module's version can be verified via the repository logs and information.

9.1.2. Module installation

The OEM integrators store the firmware binary into an appropriate storage within the hardware device, also known as host device.

Upon boot, the host device's processor, or host processor, transfers the firmware binary to the module's memory space. The module will then load the binary and commence the POST operations as specified in this Security Policy document. After the POST operations are successfully completed, the module is ready to operate in FIPS mode only.

AES keys are generated outside the logical boundary of the module, e.g., through the IEEE 802.11i 4-way handshake process that generates the Temporal Key (TK) utilized by the AES-CCMP. The AES keys enter the module under the Crypto Officer role via the appropriate interface as specified in Section 2 and Section 3.

9.2. User Guidance

When the module is in the ready state, it only runs in FIPS Approved mode of operation.

Consonant with Sections 1.1, 3.2 and 3.3, the module offers the AES-ECB and AES-CCM engines to provide the 802.11 CCMP protocol. Access to the provided module functions is done through calls to API functions.

9.2.1. API Functions

The on-demand zeroization is done via power-off and then power-on again. Key zeroization can also be done by explicitly setting the 'Key' registers in the 'wsoc_mac_enc' to 0 by the SW.
The module's version can be verified by calling the `ReadRevision` function.

10. Mitigation of Other Attacks

There are no mitigations from other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
AAD	Additional Authentication Data
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CCM	Counter with CBC-MAC
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol, or CCM mode Protocol
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards Publication
HW	Hardware
KAT	Known-Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OCP	Open Core Protocol
POST	Power-On Self-Test
SDR	Software-Defined Radio
SW	Software
WLAN	Wireless Local Area Network

Appendix B. References

FIPS140-2 **FIPS PUB 140-2 - Security Requirements For Cryptographic Modules**
May 2001
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS140-2_IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
December 4, 2017
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Technique**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

