TI SimpleLink WiFi MCU HW Crypto Engines Module

version 4.0.0.5

Chip ID: 0x311001

Non-Proprietary FIPS 140-2 Security Policy

Version 1.1

2018-08-07

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1. Cryptographic Module Specification

This document is the non-proprietary FIPS 140-2 Security Policy for the TI SimpleLink WiFi MCU HW Crypto Engines Module version 4.0.0.5, Chip ID 0x311001. It contains the security rules under which the module must operate 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. Description of Module

The SimpleLink WiFi CC3235 and CC3135 are internet-on-a-chip Wi-Fi solutions that allow the connection of any low-cost, low power microcontroller unit (MCU) to the Internet of Things (IoT). It is a self-contained network processor with a dedicated ARM MCU and embedded TCP/IP stack that completely offloads Wi-Fi and internet protocols for the Host MCU. It consists of a Wi-Fi network processor subsystem, a Wi-Fi driver, multiple internet protocols in ROM, an ARM Cortex-M4 application microcontroller and peripherals.

Figure 1 demonstrates the physical look of the SimpleLink CC3235 and CC3135 chips.

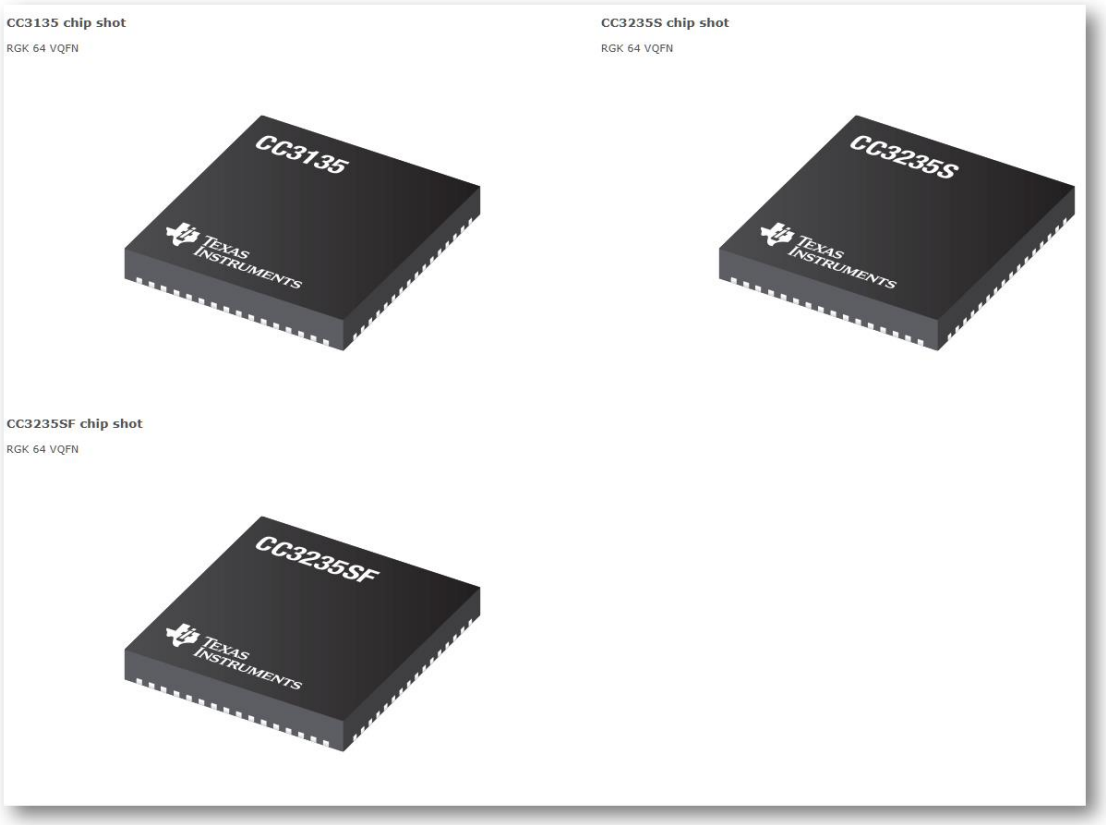

Figure 1: Physical representation of the CC3135 and CC3235 chips.

The TI SimpleLink WiFi MCU HW Crypto Engines Module (hereafter referred to as "the crypto engines module", "the crypto module" or "the module") is a sub-chip cryptographic subsystem that resides within SimpleLink CC3235 and CC3135 chips. The physical enclosure of these chips is the physical boundary of the crypto engines sub-chip module.

The crypto engines module is one of the two sub-chip modules on the same single chip subject to the FIPS 140-2 validation (this module is bound to the other sub-chip module, TI SimpleLink WiFi Networking Subsystem Crypto Module, validated under its own FIPS 140-2 certificate). The crypto engines module contains embedded hardware cryptographic engines and firmware NWP Boot code stored in ROM. It provides cryptographic services for the integrity check on the second sub-chip module, verifies the RSA signatures of TI-signed Service Packs during their programming operation, and encrypts the file system using AES when the file system is established early at the boot time.

The logical boundary of the module is the yellow component blocks in Figure 2 and Figure 3. The orange blocks indicate the components belonging to the logical boundary of the bound sub-chip module, TI SimpleLink WiFi Networking Subsystem Crypto Module. Blocks of another color do not belong to any logical boundary.

SimpleLink CC31XX represents CC31XX family chips including CC3135. Likewise, CC32XX includes CC3235 as a specific chip model within this family.

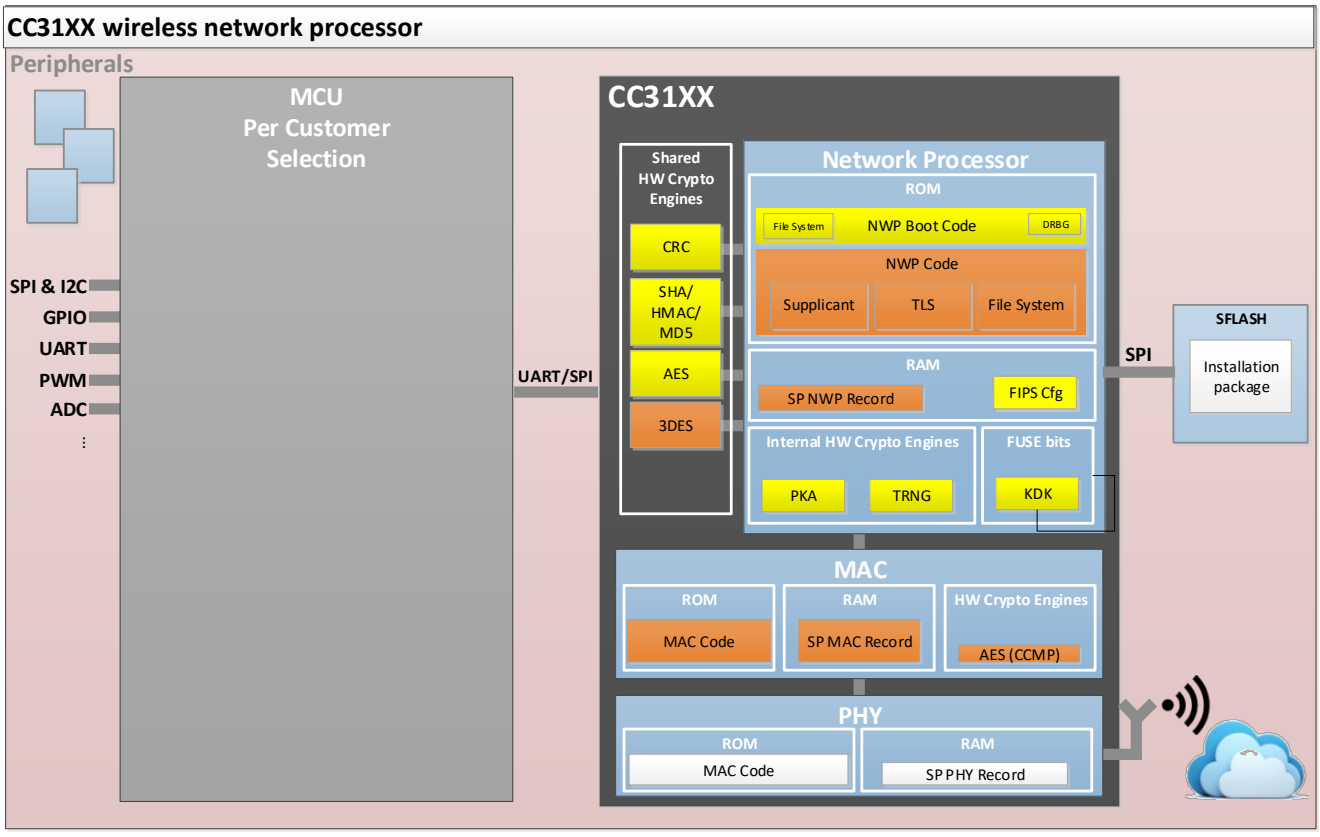

Figure 2: Logical Boundary of the module on SimpleLink CC31XX chip.

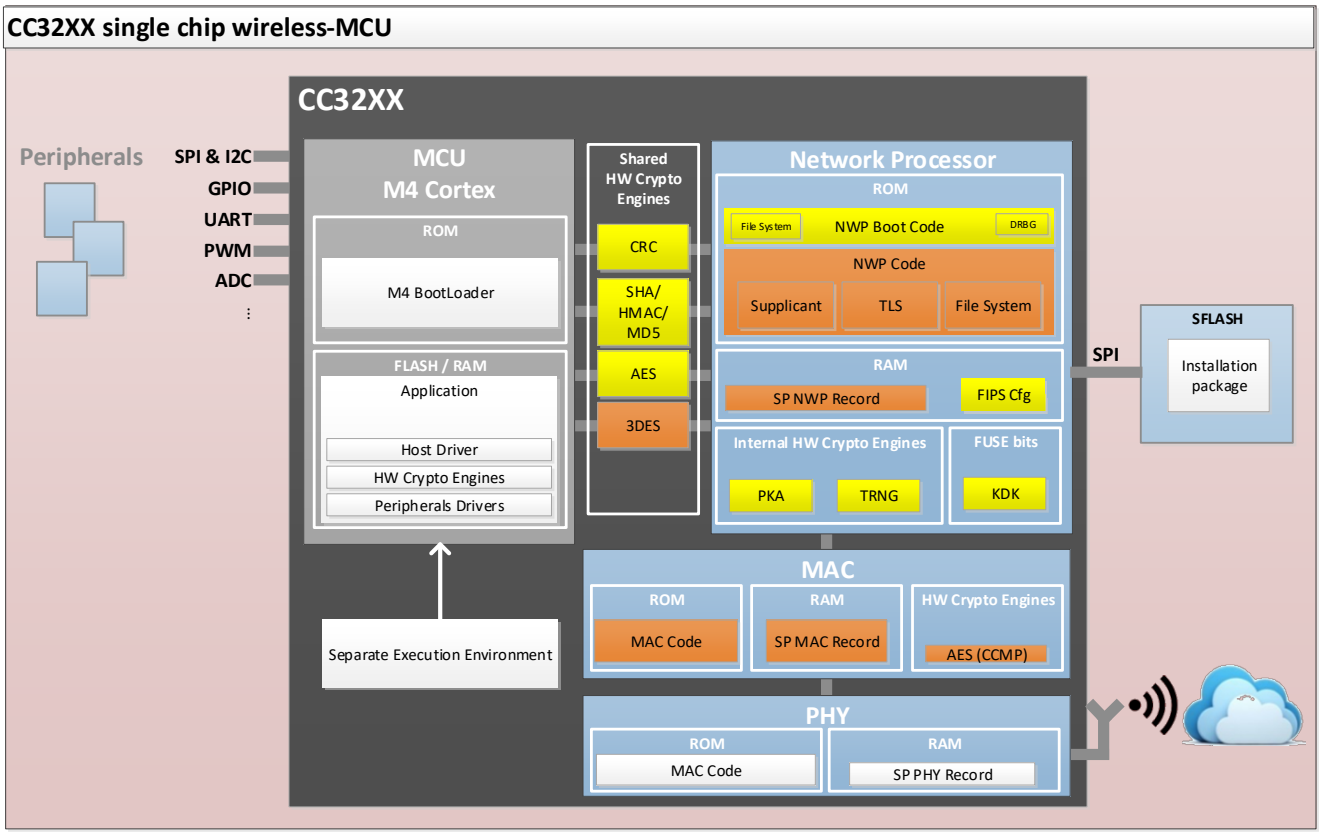

Figure 3: Logical Boundary of the module on SimpleLink CC32XX chip.

The components within the logical boundary of the HW Crypto Engines Module are listed in Table 1.

1.2. Version

The module version is 4.0.0.5, Chip ID 0x311001. These numbers comprise all components of the module, including the FIPS Configuration (Cfg) file. The Chip ID refers to the hardware chip component of the module and the FIPS Cfg file, wherein the 5 digits after the "0x" prefix identify the chip, and the last digit uniquely identifies the FIPS Cfg file.

Any extra digits after the 6 digits in the Chip ID are not relevant for the module version.

Table 1: Components of TI SimpleLink WiFi MCU HW Crypto Engines Module.

Component	Type
NWP Boot Code	Firmware version 4.0.0.5, Chip ID 0x311001
FIPS Configuration (FIPS Cfg) file	A file present in RAM during execution time
SHA/HMAC/MD5 Engine	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips
AES Engine	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips
PKA Engine (RSA)	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips
TRNG Engine	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips
CRC Engine	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips
CRC value for integrity check on HW Crypto Engine Module	Hardware component in SimpleLink Wifi CC3235 and CC3135
FUSE ROM bits to store KDK (128 bits)	Hardware component in SimpleLink Wifi CC3235 and CC3135 chips

1.3. FIPS 140-2 Validation

For the purpose of the FIPS 140-2 validation, the module is defined as a sub-chip hardware cryptographic module with a single chip embodiment validated at overall security level 1. Table 2 shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard.

Table 2: Security levels for each section of FIPS 140-2 standard.

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**

The module has been tested on the platforms specified in Table 3.

Table 3: Tested platforms.

Test Platform (SoC Reference)	MCU
CC3135R	Outside the physical boundary of the chip
CC3235S	ARM Cortex M4
CC3235SF	ARM Cortex M4

1.4. Modes of operation

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

The POST is executed automatically without any operator intervention. If the POST fails during power-up, the module goes into the error state. The status of the module can be determined by the availability of the module. If the module is available, then it has passed all self-tests. If it is unavailable, it is because the POST procedure failed and the module has transitioned to the error state.

2. Cryptographic Module Ports and Interfaces

The module provides cryptographic services and an application program interface (API). The physical ports are registers within the logical boundary of the sub-chip module. These registers hold the data for API parameters. Table 4 summarizes the four logical interfaces and their mappings to physical ports.

Table 4: Ports and Interfaces.

Logical Interface	Physical Ports	Description
Data Input	Registers	API input parameters for data
Data Output	Registers	API output parameters for data
Control Input	Registers, Interrupts	API function calls, API input parameters for control.
Status Output	Registers, Interrupts	API return codes, API output parameters for status.
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.

The Data Input interface consists of the registers that hold the data for the input parameters of the API functions. The input data is received from the Serial Peripheral Interface (SPI) or Universal Asynchronous Receiver/Transmitter (UART) of the SimpleLink chip on which the sub-chip module resides.

The Data Output interface consists of registers that hold the data for the output parameters of the API functions. The output data leaves the physical boundary of the SimpleLink chip via its SPI or UART interfaces.

The Control Input interface consists of the API function calls as interrupts and the input parameters used to control the behavior of the module. The control input enters the sub-chip module via registers.

The Status Output interface includes the return code of the API functions via interrupts and the status sent through output parameters. The status output is sent through the registers.

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. The module does not support concurrent operators.

3.2. Services

The module provides services to users who assume one of the available roles. Table 5 shows the approved and the non-approved-but-allowed services in FIPS mode of operation, the cryptographic algorithms supported for each service (and their CAVP certificate numbers), the roles that can perform each service, and the Critical Security Parameters (CSPs) involved and how these CSPs are accessed. Since the module always operates in FIPS mode, Table 5 includes all services offered by the module. There are no offered services in non-FIPS mode.

Table 5: Cryptographic Services in FIPS mode of operation.

Service	Algorithms, CAVP certificate	Role	Access to Keys/CSPs	Keys/CSPs
Symmetric Encryption and Decryption	AES (ECB, CBC, CTR, CFB, GCM, and CCM) #5428 (CC3135R) #5429 (CC3235S) #5430 (CC3235SF)	User	Read	AES 128-bit, 192-bit and 256-bit keys
RSA digital signature verification	RSA SigVer with SHA-1 and SHA-256 #2907 (CC3135R) #2909 (CC3235S) #2908 (CC3235SF)	User	Read	RSA public key with 1024-bit and 2048-bit modulus sizes
Message digest	SHA-1, SHA-256 #4354 (CC3135R) #4355 (CC3235S) #4356 (CC3235SF)	User	n/a	none
Message Authentication Code (MAC)	HMAC-SHA-1, HMAC-SHA-256 #3592 (CC3135R) #3593 (CC3235S) #3594 (CC3235SF)	User	Read	HMAC key of size at least 112 bits

Service	Algorithms, CAVP certificate	Role	Access to Keys/CSPs	Keys/CSPs
Random Number Generation	Hash-DRBG #2118 (CC3135R) #2120 (CC3235S) #2119 (CC3235SF)	User	Read, Write	Seed (384-bit length) Internal state
Key Derivation	Key Derivation Function in Counter Mode (KDF in CTR mode) [SP800-108]. #204 (CC3135R) #206 (CC3235S) #205 (CC3235SF)	User	Read, Write	KDK and derived keys. (Derive HMAC keys from KDK, using DRBG as context string.)
NDRNG	N/A	User	Read, Write	Seed to DRBG (minimum 301 bits of entropy – Section 6.6)
Show status	N/A	User	n/a	none
Self-Tests	N/A	User	Read	HMAC key (for module integrity test)
Zeroization by power-cycle	N/A	User	Zeroize	All CSPs but KDK
Zeroization of KDK	N/A	Crypto Officer	Blow FUSE ROM	KDK
Module Installation	N/A	Crypto Officer	n/a	none

3.3. Operator Authentication

There is no operator authentication; assumption of role is implicit in the used service(s).

4. Physical Security

The module is a sub-chip module implemented as part of the TI SimpleLink CC3235 and CC3135 chips. The TI SimpleLink family 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 operates in a non-modifiable operational environment per FIPS 140-2 level 1 specifications. As such the operational environment is considered as not applicable to the FIPS rules.

6. Cryptographic Key Management

Table 6 summarizes the keys and CSPs that are used by the cryptographic services implemented in the module.

Table 6: Life cycle of Keys and Critical Security Parameters (CSPs).

Name	Generation	Entry/Exit	Storage	Zeroization	Usage
AES keys	Externally generated	Entered via API parameter. No exit.	RAM	Zeroized during cold-boot of the module.	File/data Encryption/decryption
HMAC keys	Derived from KDK	N/A	RAM	Zeroized during cold-boot of the module.	File/data integrity protection
RSA public key	Externally generated	Enter during manufacture process	ROM	N/A	Signature verification of installation package
KDK	Externally generated	Enter during the manufacture process	ROM	Blow KDK FUSE ROM	Per-chip root key from which HMAC keys are derived
Seed	Generated by the NDRNG	N/A	RAM	Zeroized during cold-boot of the module.	Seed SP 800-90A DRBG
DRBG internal state (V, C, Key)	Generated by the DRBG	Exit module encrypted by AES and then stored encrypted on an external SFLASH memory along with SHA-256 value	RAM	Zeroized during cold-boot of the module	Generate random bit strings

The following sections describe how the module manages the life cycle of its keys and other CSPs.

6.1. Key Generation

The module does not have internally generated keys.

6.2. Key Derivation

The module has one root key, named by TI as KDK, that is provisioned as part of TI manufacture process. The module uses the KDK and the DRBG output as context string to derive HMAC keys.

6.3. Key Entry / Output

The module does not support manual key entry or intermediate key output. In addition, the module does not produce key output in plaintext format. The output of NIST SP800-90A DRBG exits the module boundary under the AES encryption. The DRBG outputs are not used as keys by the modules. It is used as a context string in the KDF in CTR mode to derive HMAC keys from KDK.

6.4. Key / CSP Storage

The KDK is stored in persistent one-time programmable memory (FUSE ROM). All other keys and CSPs only exist in the volatile RAM during the runtime. These other keys and CSPs are not preserved over the power cycles.

6.5. Key / CSP Zeroization

The KDK can be zeroized by blowing the KDK FUSE ROM, which irreversibly alters the electrical properties of the FUSE ROM. This operation can only be performed by the crypto officer. The zeroization of the KDK will render the module useless and hence decommission the module.

Zeroization of all other keys and CSPs in RAM is obtained by powering off the module, and then powering the module back on (power cycle).

The zeroization process results in a key or CSP being overwritten with zeroes.

6.6. Random Number Generation

The module employs a Deterministic Random Bit Generator (DRBG) based on [SP800-90A]. The output of DRBG is used as a context string for SP800-108 CTR KDF.

The DRBG implements a Hash_DRBG mechanism. The DRBG is initialized during module initialization and seeded by an on-chip Non-Deterministic Random Number Generator (NDRNG). The min-entropy estimate rate of this entropy source (per tested platform as indicated in Table 3) is demonstrated in Table 7. The length of the entropy_input string that forms the DRBG seed is 384 bits. Considering the lowest bit/bit entropy value in Table 7 (CC3135S), the NDRNG provides a 384-bit seed with at least 301 (truncated to an integer) bits of entropy to the DRBG during initialization (seed) and reseeding (reseed). The entropy of 301 bits is computed per the equation below.

$$MinEntropy = 0.785 \cdot 384 \cong 301$$

The module performs continuous tests on the output of the NDRNG to ensure that consecutive random numbers do not repeat.

Table 7: Minimum entropy of the on-chip NDRNG per tested platform.

Test Platform (SoC Reference)	Min. Entropy (bits/byte)	Min. Entropy (bit/bit)
CC3135R	6.47	0.809
CC3235S	6.28	0.785
CC3235SF	6.46	0.808

7. Self Tests

7.1. Power-Up Tests

The module performs power-up tests automatically when the module is powered on; These self-tests are performed without requiring operator intervention. These power-up tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

While the module is executing the power-up tests, cryptographic services are not available, and data output are inhibited. The module's cryptographic services are not available until the power-up tests are completed.

7.1.1. Integrity Tests

The integrity of the ROM code of module is verified by comparing a CRC-16 value calculated at run time with the checksum value stored in the module that was computed at build time.

7.1.2. Cryptographic algorithm tests

The module performs self-tests on all FIPS-Approved cryptographic algorithms supported in the approved mode of operation, using the known answer tests (KAT) shown in Table 8.

Table 8: Self-tests.

Algorithm	Test
AES	• KAT AES ECB, encrypt • KAT AES ECB, decrypt
HMAC	• KAT HMAC-SHA-1 • KAT HMAC-SHA-256
RSA	• KAT RSA 2048-bit key (PKCS#1 v1.5) with SHA-256 signature verification
DRBG	• KAT Hash_DRBG

7.2. On-Demand self-tests

The on-demand Self-Test is achieved by power cycling. The self-tests initiated on demand perform the same cryptographic algorithm tests as those executed during power-up. While the on-demand self-tests are running, cryptographic services are not available and data output is inhibited.

7.3. Conditional Tests

The module performs conditional tests on the NDRNG, that is, NDRNG Continuous Test.

8. Guidance

8.1. Crypto Officer Guidance

In order to install the FIPS validated module, the subsequent steps must be followed:

- The chip and the serial flash must be physically assembled on the PCB.
- The chip must be programmed with an image and the Image Creator tool provided by the vendor. The image contains the FIPS140-2 installation package, and programming must be done by checking the proper checkbox in the Image Creator tool to enable the FIPS Cfg file to be programmed. The Image Creator tool verifies the digital signature of the installation package, and will not program the image if the signature verification fails.

For more information please refer to the Uniflash guide: http://www.ti.com/lit/pdf/swru469.

8.2. User Guidance

Upon the correct installation of the FIPS validated module, the module always operates in the FIPS approved mode. There is no action expected from the user.

8.2.1. AES-GCM IV

To comply with the IV construction requirements for FIPS 140-2, the AES GCM encryption and decryption are to be used in the context of the TLS protocol version 1.2 that is implemented in the bound module TI SimpleLink WiFi Networking Subsystem Crypto Module. Under this usage, the module is compliant with [SP 800-52] GCM ciphersuites and the mechanism for IV generation is compliant with [RFC5288]. The IV constructed according to the TLS v1.2 protocol may only be used in the context of the AES-GCM mode encryption within the TLS v1.2 protocol. The operations of one of the two parties involved in the TLS key establishment scheme are performed entirely within the cryptographic boundary of the module, including the setting of the counter portion of the IV.

When the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module (acting as server or client) triggers a handshake to establish a new encryption key per Section 7.4.1.1 and Section 7.4.1.2 in [RFC5246] and compliant to [FIPS140-2_IG] A.5.

In case the module's power is lost and then restored, the key used for AES GCM encryption or decryption shall be re-distributed.

For additional information please refer to

- Product page: http://www.ti.com/product/CC3235

9. Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

10. 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.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation Scheme
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DF	Derivation Function
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
MCU	Microcontroller Unit
NIST	National Institute of Science and Technology
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feedback
PKA	Public Key Algorithm
PR	Prediction Resistance
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
TDES	Triple-DES
TI	Texas Instruments
UART	Universal Asynchronous Receiver/Transmitter

Appendix B. References

FIPS140-2 **FIPS PUB 140-2 - Security Requirements For Cryptographic Modules**
May 2001
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

FIPS140-2_IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
May 25, 2018
https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402IG.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

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

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography**
Specifications Version 2.1
February 2003
http://www.ietf.org/rfc/rfc3447.txt

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

SP800-38C **NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
May 2004
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

SP800-38D **NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
November 2007
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

SP800-57	**NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management Part 1: General** January 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
SP800-67	**NIST Special Publication 800-67 Revision 2- Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher** November 2017 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf
SP800-90A	**NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-131Ar1	**NIST Special Publication 800-131A Revision 1- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths** November 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
SP800-108	**NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions** October 2009 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf