CUBIC GLOBAL TRACKING SOLUTIONS

2560 Mission College, Suite 130
Santa Clara, CA 95054-1217

Security Policy for Cubic Managed Asset Tag (MAT) Cryptographic Module and Cubic SINK Cryptographic Module

Detailed Revision History

Issue	Description of Changes
1.4	Initial release.

Table of Contents

Table of Figures

List of Tables

1. SCOPE

This document is the Cryptographic Module Security Policy for the Cubic Managed Asset Tag Cryptographic Module and Cubic SINK Cryptographic Module (herein after referred to "the cryptographic module" or "the module"). This policy is a specification of the security rules under which the module operates and meets the overall requirements of FIPS 140-2 Level 1.

1.1 REFERENCE DOCUMENTS

Document No.	Description
FIPS PUB 140-2	Security Requirements For Cryptographic Modules [FIPS PUB 140-2] (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

Table 1 Reference Documents

2. CRYPTOGRAPHIC MODULE OVERVIEW

The cryptographic module is a single-chip cryptographic module based on the TI CC2530 SOC chip. The cryptographic module securely sends and receives information collected from peripheral sensors to/from an external Cubic Gateway in support of Cubic mist ™ mesh networking solutions. The difference in module firmware implementations is summarized in the NOTE at the bottom of Section 7 below.

2.1 VALIDATED MODULE VERSIONS

The validated module consists of the following hardware and firmware:

Cubic Managed Asset Tag Cryptographic Module

- Hardware version: 380270-1 Rev. -
- Firmware version: mat_v2_1_0

Cubic SINK Cryptographic Module

- Hardware version: 380270-1 Rev. -
- Firmware version: sink_v2_1_0

3. SECURITY LEVELS

The cryptographic module satisfies the FIPS 140-2 Security Level 1 requirements as shown in Table 2 below:

FIPS 140-2 Security Requirements	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
FIPS Overall Level	1

Table 2 FIPS 140-2 Security Levels

4. CRYPTOGRAPHIC BOUNDARY

The illustration below indicates the cryptographic boundary.

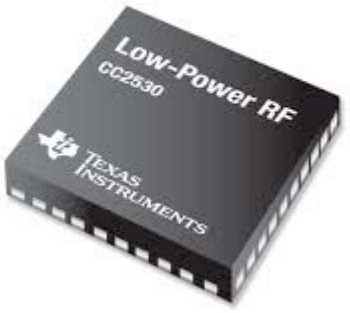

Figure 1 Isometric view of cryptographic module

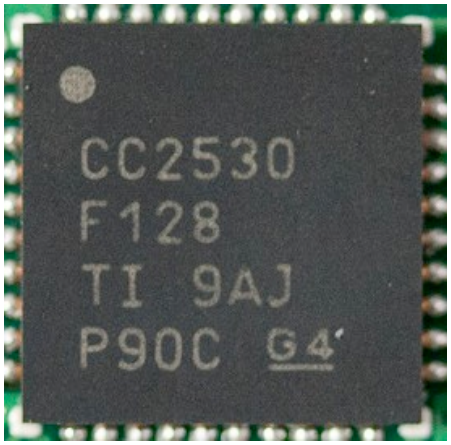

Figure 2 Top view of cryptographic module

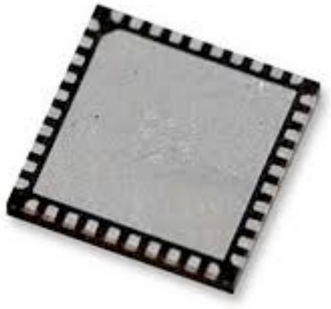

Figure 3 Bottom view of cryptographic module

5. APPROVED ALGORITHMS

The cryptographic module supports the following Approved algorithms:

- Symmetric Encryption/Decryption
  - Advanced Encryption Standard (AES)**: Cert # 1863**

- Random Number Generation (DRBG)
  - DRBG – NIST SP800-90: **Cert # 150**

6. NON-APPROVED ALGORITHMS

The cryptographic module supports the following non-Approved algorithms:

- Non-deterministic hardware RNG for seeding Approved NIST SP800-90 DRBG

7. PORTS AND INTERFACES

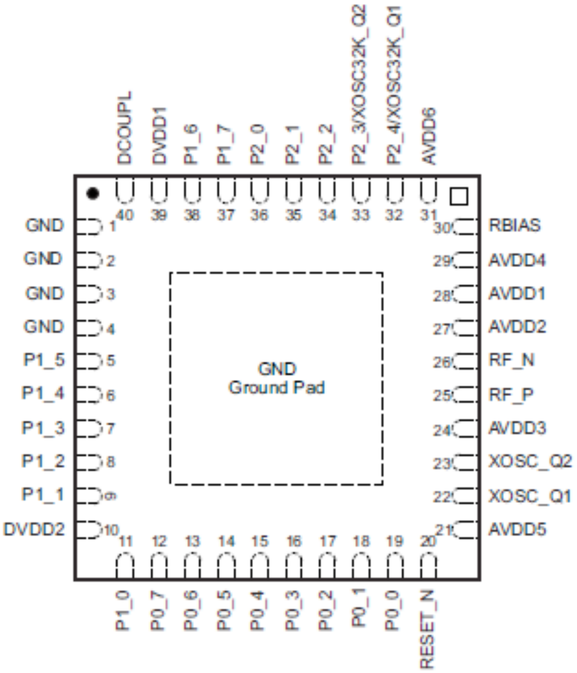

Figure 4 Cryptographic module ports and interfaces

The following table maps the cryptographic module logical interfaces to the physical ports:

Logical Interface	Pin Name	PIN	PIN Description
Data Input	P0_0	19	Light Sensor
	P0_1	18	Motion Sense
	P0_2	17	GPS serial receive
	P0_4	15	I2C Data
	P0_6	13	Acceleration sensor interrupt
	P1_0	11	Door Sensor
	P1_7	37	RTC SPI_MISO
			SFLASH SPI_ MISO
			FRAM SPI_ MISO
			Expander SPI_ MISO
	P2_1	35	Programmer Data Input
	P2_2	34	Programmer Clock
	P2_3	33	32.768 kHz crystal
	P2_4	32	
	XOSC_Q1	22	32 MHz crystal
	XOSC_Q2	23	

	RF_N	26	Negative RF input signal
	RF_P	25	Positive RF input signal
Data Output	P0_3	*16	Serial transmit
	P0_4	15	I2C Data
	P1_6	*38	RTC SPI_MOSI
			SFLASH SPI_MOSI
			FRAM SPI_MOSI
			Expander SPI_MOSI
	P2_1	35	N/A – Disabled in secure Cubic factory.
	RF_N	26	Negative RF output signal
	RF_P	25	Positive RF output signal
Control Input	Reset_N	20	Reset
	RF_N	26	Negative RF input signal
	RF_P	25	Positive RF input signal
Status Output	P0_7	12	Buzzer control
	P1_4	*6	SPI expander chip select
	P1_5	*5	SPI clock
	P2_0	36	LED
	P0_5	14	Acceleration sensor reset
	P1_1	9	RTC chip select
	P1_2	8	Serial Flash chip select
	P1_3	7	FRAM chip select
Power	AVDD1	28	2-V–3.6-V analog power-supply connection
	AVDD2	27	2-V–3.6-V analog power-supply connection
	AVDD3	24	2-V–3.6-V analog power-supply connection
	AVDD4	29	2-V–3.6-V analog power-supply connection
	AVDD5	21	2-V–3.6-V analog power-supply connection
	AVDD6	31	2-V–3.6-V analog power-supply connection
	DCOUPL	40	1.8-V digital power-supply decoupling
	DVDD1	39	2-V–3.6-V digital power-supply connection
	DVDD2	10	2-V–3.6-V digital power-supply connection
	GND	_	Ground pad connected to a solid ground plane
	GND	1, 2, 3, 4	Ground

NOTE: Ports/Interfaces differences

- *Cubic Managed Asset Tag Cryptographic Module:*
    - *Pin 16: Used for GPS Serial Transmit.*
    - *Pins 5, 6 and 38: "Secure Magnetic Wipe" service IS NOT supported.*

- *Cubic SINK Cryptographic Module:*
    - *Pin 16: Used for GPS Serial Transmit and Serial Transmit.*
    - *Pins 5, 6 and 38: Used for "Secure Magnetic Wipe" service.*

8. AUTHENTICATION

The cryptographic module supports the following distinct roles: Cryptographic Officer role, User role and Gateway role. The cryptographic module does not support a Maintenance role. The cryptographic module enforces the separation of roles using role-based authentication.

Role	Type of Authentication	Authentication Data
Cryptographic Officer	Role-based authentication	Join Keyset and Data Key
User	Role-based authentication	Data Key
Gateway	Role-based authentication	Join Keyset

Table 3 Roles and Authentication Data

Authentication Mechanism	Strength of Mechanism
Knowledge of symmetric key(s)	The authentication is based on proof of knowledge of AES CCM symmetric key(s) via encryption/authentication of commands providing 128 bits of equivalent computational resistance to attack. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{128}$ which is significantly less than 1/1,000,000. The module supports a maximum of 60 authentication attempts within a one-minute period. Therefore the probability that multiple consecutive random authentication attempts will be successful within one minute is $60/2^{128}$ which is significantly less than 1/100,000.

Table 4 Strength of Authentication Mechanism

9. ROLES AND SERVICES

9.1 CRYPTOGRAPHIC OFFICER SERVICES

Table 5 summarizes the services and associated CSP access rights that are only available to the Cryptographic Officer role.

	Services	Description	CSP(s) and Key(s)	Type(s) of Access
1.	Zeroize	Zeroizes all plaintext CSPs from RAM, Program memory and registers.	Internal Key Data Key NIST SP800-90 CTR_DRBG V and Key	Write Write Write
2.	Program CSP	Updates CSP(s).	Internal Key Key Delivery Key Data Key	Read Read Read

Table 5 Cryptographic Officer Services

User ServicesTable 6 summarizes the services and associated CSP access rights that are only available to User role.

Services		Description	CSP(s) and Key(s)	Type(s) of Access
1.	Send	Send data to the device.	Internal Key	Read
2.	Receive	Receive data from the device.	Internal Key	Read
3.	Send secure	Send data securely to the device.	Internal Key Data Key	Read Read
3.	Receive secure	Receive data securely from the device.	Internal Key Data Key	Read Read

Table 6 User Services

9.2 GATEWAY SERVICES

Table 7 summarizes the services that are only available to the Gateway role.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Join Network	Make the module part of a wireless mesh network.	Internal Key	Read
		Join Keyset	Read
		Session Key	Write
		NIST SP800-90 CTR_DRBG V and Key	Write
Choke Point Transponder (CPT)	Send/receive asset related information.	Internal Key	Read
		Choke Point Transponder (CPT) Key	Read

Table 7 Gateway Services

9.3 UNAUTHENICATED SERVICES

Table 8 summarizes the unauthenticated services that are available.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Power On Self-Tests	Required self-tests are performed at Power On.	N/A	N/A
Status LED	Status Output to external LED(s).	N/A	N/A
** Secure Magnetic Wipe	Zeroizes all plaintext CSPs from the RAM and registers.	All CSPs are actively destroyed from the RAM and registers.	Write

Table 8 Unauthenticated Services

** NOTE: The “Secure Magnetic Wipe” service is only available on the Cubic SINK Cryptographic Module (i.e. the “Secure Magnetic Wipe” service IS NOT available on the Cubic Managed Asset Tag Cryptographic Module).

The "Secure Magnetic Wipe" service is intended to take a module offline temporarily, not permanently destroy the module as is the case with the "Zeroize" service. If the timed sequence described below is not strictly adhered to (such as performing the required tasks out of order, failing to abide by the timing restrictions such as applying the magnet over the peripheral for more than 4 seconds during the initial step as per your inquiry, etc.) nothing happens.

- The Secure Magnetic Wipe service can be invoked as follows:
  - Apply the magnet to the right hand side of the MAT for 4 seconds. There will be 1 second green LED blink in the beginning of these 4 seconds.
  - Remove magnet for 4 seconds. As soon as you remove the magnet you will see sub-second green and then orange blinks.
  - Reapply magnet for 1 second you will see sub-second green and then orange blinks again.
  - Then after 1-2 seconds pause you will see orange LED going solid for ~10 seconds. This is an indication of the successful Zeroization of all plaintext CSPs from the RAM and registers.

10. CRITICAL SECURITY PARAMETERS

#	Name	Description
1.	Internal Key	AES CCM 128-bit key used for protection of data and CSPs while communicating with peripherals outside the cryptographic boundary.
2.	Join Keyset	Keyset (Qty. 2 keys) AES CCM 128-bit for joining a wireless mesh network.
3	Key Delivery Key	AES CCM 128-bit key used for key delivery.
4.	Session Key	AES CCM 128-bit key used for protection of data and CSPs in wireless communication session.
5.	Data Key	AES CCM 128-bit key for end-to-end data encryption.
6.	NIST SP800-90 CTR_DRBG V and Key	DRBG internal state.
7.	Choke Point Transponder (CPT) Key	AES CCM 128-bit key for protection of asset related information.

11. PHYSICAL SECURITY

The cryptographic module is a production-grade single-chip embodiment..

The physical security mechanism of the module is the hard, opaque and tamper-evident epoxy IC packaging. Attempts to remove the epoxy IC packaging will, with high probability, result in irreparable damage to the module to the extent that the module will no longer function.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque and tamper evident epoxy IC packaging	The Cryptographic Officer shall perform inspection upon receipt of module and as often as feasible.	The Cryptographic Officer shall visually inspect the epoxy IC packaging of the single-chip module for scratches, scrapes, gouges, rips, tears, divots, nicks, scuffs, deformations, evidence of attempts to mask or otherwise hide malicious activity, any and all other visible signs of tampering.

Table 9 Inspection/Test of Physical Security Mechanism

NOTICE: If “any” tampering of the module is observed or suspected, the Cryptographic Officer shall remove the module from service “immediately”.

12. OPERATIONAL ENVIRONMENT

The module includes a non-modifiable operational environment.

13. SELF-TESTS

The module performs the following self-tests:

- Power Up Self-Tests
  - Cryptographic algorithm tests:
    - AES encrypt/decrypt Known Answer Test
    - NIST SP800-90 DRBG Known Answer Test
  - Firmware Integrity Test (CRC-16)
  - Critical functions tests: N/A

- Conditional Self-Tests
  - Continuous Random Number Generator (RNG) tests:
    - NIST SP800-90 DRBG
    - Non-deterministic Hardware RNG
  - Manual Key Entry Test: N/A – the module does not support manual key entry.
  - Firmware Load Test: N/A – the module has a non-modifiable operational environment.
  - Pairwise Consistency Test: N/A – the module does not generate asymmetric key pairs and does not implement any asymmetric algorithms.
  - Bypass Test: N/A – the module does not support a bypass capability.

- Critical functions tests: N/A

14. MITIGATION OF OTHER ATTACKS

The cryptographic module does not mitigate any specific attacks beyond the scope of FIPS 140-2.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 10 Mitigation of Other Attacks

15. SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

- The module shall not support a bypass capability or a maintenance interface.
- The module shall support concurrent operators. However, the module shall not support more than one operator per role. The operators are not allowed to switch roles without re-authenticating and separation of roles and associated services shall be maintained for concurrent operators.
- The operator shall re-authenticate on each power-up event.
- The module shall inhibit data output during self-tests, error states, key generation and zeroization.
- The module shall provide role-based authentication.
- The module shall not provide feedback of authentication data or and CSPs.
- The module shall not support a non-FIPS mode of operation.
- The module shall only operate in an Approved mode of operation. The module shall be initialized for FIPS mode of operation within the secure Cubic factory.
- The operator may verify that the module is running in an approved mode of operation by verifying the status output to external LED(s):
  - Solid Orange: the module is performing power-up self-tests.
  - Blinking Orange rapidly: the module is in a error state following the power-up self-tests
  - Blinking Green (in 2.5 second intervals): the module has successfully performed self-tests, is connected to an external Cubic Gateway and is running in FIPS mode
  - Blinking Red (in 2.5 second intervals): the module has successfully performed self-tests, is not connected to an external Cubic Gateway and is running in FIPS mode

    NOTE: for the SINK module, the equivalent of orange is one red and one green.
- An error state may be cleared by power-cycling the module.
- The module shall provide logical separation between all the data input, control input, data output and status output interfaces.
- The module shall include a power input interface and shall not support a power output interface.
- The module protects CSPs from unauthorized disclosure, unauthorized modification and unauthorized modification.
- The module does not support manual key entry; a manual key entry test is not implemented by the module.
- The module does not support split-knowledge processes.
- The operator may perform on-demand power-on self-test by recycling power to the module.

- The status output does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- The module does not support a bypass capability and does not support a bypass test.

16. ACRONYMS

Acronym	Definition
AES	Advanced Encryption Standard
CCM	Counter with CBC MAC
SOC	System on a chip
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
IC	Integrated Circuit
KAT	Known Answer Test
N/A	Not applicable