Cobham TCS Limited

Cobham AES Cryptographic Firmware-Hybrid Module

Hardware Version: Freescale ColdFire Microprocessor (MCF54453)
Firmware Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.9

Prepared for:

COBHAM

Cobham TCS Limited
The Cobham Centre Solent, Fusion 2, 1100 Parkway
Whiteley, Hampshire
United Kingdom

Phone: +44 (0) 1489 566 750
Email: info@cobham.com
http://www.cobham.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cobham AES Cryptographic Firmware-Hybrid Module from Cobham TCS Limited. This Security Policy describes how the Cobham AES Cryptographic Firmware-Hybrid Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Cobham AES Cryptographic Firmware-Hybrid Module is also referred to in this document as simply, "the module".

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Cobham website (http://www.cobham.com/) contains information on the full line of products from Cobham.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Cobham. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Cobham and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cobham.

2 AES Cryptographic Firmware-Hybrid Module

2.1 Overview

Within the Aerospace and Defense industry, Cobham offers a range of technologies and services to solve challenging problems across commercial, defense, and security markets. Their products include audio, video, and data communications, defense electronics, life support, and mission equipment. The offered services are primarily aviation services such as electronic warfare training, special mission operations, and aerospace engineering.

Cobham divisions include:

- **Aerospace and Security**
  - Aerospace Communications
  - Antenna Systems
  - Commercial Systems
  - SATCOM[1]
  - Tactical Communications and Surveillance (TCS)
- **Defense Systems**
  - Defense Electronics
- **Mission Systems**
  - Aviation Services
  - Life Support
  - Mission Equipment

The TCS group specializes in providing surveillance and communication technologies for successful operation in demanding environments.

2.1.1 Cobham NETNode IP Mesh Radios

The Cobham NETNode IP Mesh Radios are designed and manufactured by the TCS group within the Aerospace and Security division. The Cobham NETNode IP Mesh Radios offer secure IP communication capabilities over a robust, self-forming, self-healing mesh architecture. They also provide genuine non-line-of-sight coverage with Coded Orthogonal Frequency-Division Multiplexing (COFDM) and are ideal for use in mobile surveillance applications, command and control, or advanced robotics.

The mesh architecture can contain up to 16 radios that automatically form a network as soon as they are powered up. These radios can also be connected to computers or attached to GPS[2] receivers and cameras. Figure 1 below depicts a typical Cobham NETNode IP Mesh Radio deployment scenario.

[1] SATCOM – Satellite Communications
[2] GPS – Global Positioning System

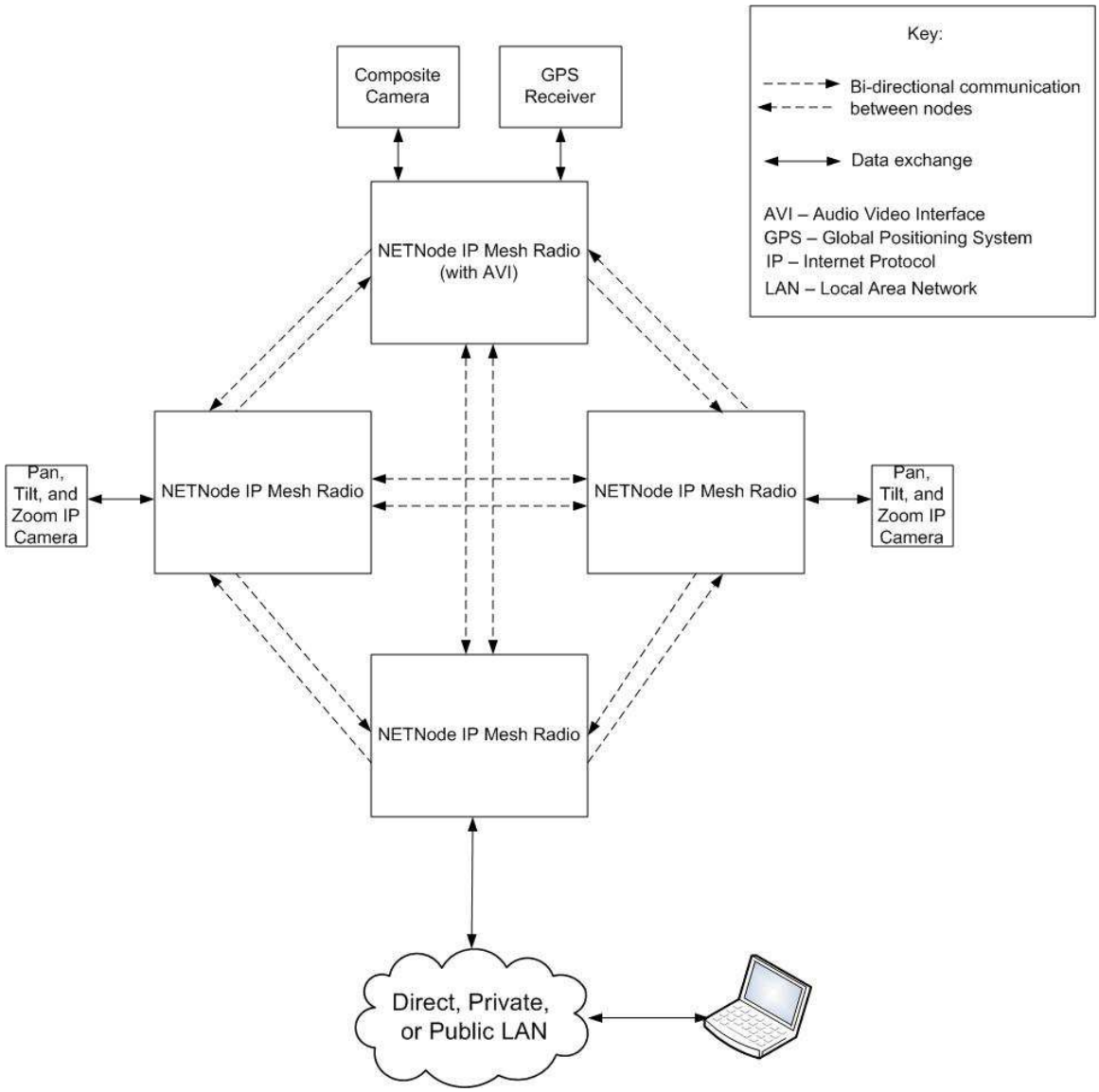

Figure 1 – Cobham NETNode IP Mesh Radio Deployment Diagram

2.1.2 AES Cryptographic Firmware-Hybrid Module

The module consists of a single cryptographic firmware library running on the Cobham NETNode IP Mesh Radio D1705D TX[3] PCB[4]'s Freescale ColdFire Microprocessor, in addition to the processor's cryptographic acceleration support. The firmware is stored in the flash memory of the D1705D TX PCB. The module includes implementations of the following FIPS-Approved security functions:

- Encryption and decryption using AES[5]
- Hashing functions using HMAC[6] SHA[7]

[3] TX – Transmitter
[4] PCB – Printed Circuit Board
[5] AES – Advanced Encryption Standard
[6] HMAC – (keyed-) Hashed Message Authentication Code
[7] SHA – Secure Hash Algorithm

The Cobham AES Cryptographic Firmware-Hybrid Module is validated at the FIPS 140-2 Section levels shown in Table 1:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	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[8]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The module is a multi-chip embedded embodiment with firmware-hybrid module type. The overall security level of the module is 1.

The Freescale Microprocessor interfaces with the DDR[9] SDRAM[10], flash memory, an FPGA[11], and interface connectors on the PCB (depicted in Figure 2 below). The red, dotted lines shown in the following block diagram represent the physical cryptographic boundary of the module, which is the Cobham D1705D TX PCB.

[8] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[9] DDR – Double Data Rate
[10] SDRAM - Synchronous Dynamic Random Access Memory
[11] FPGA – Field-Programmable Gate Array

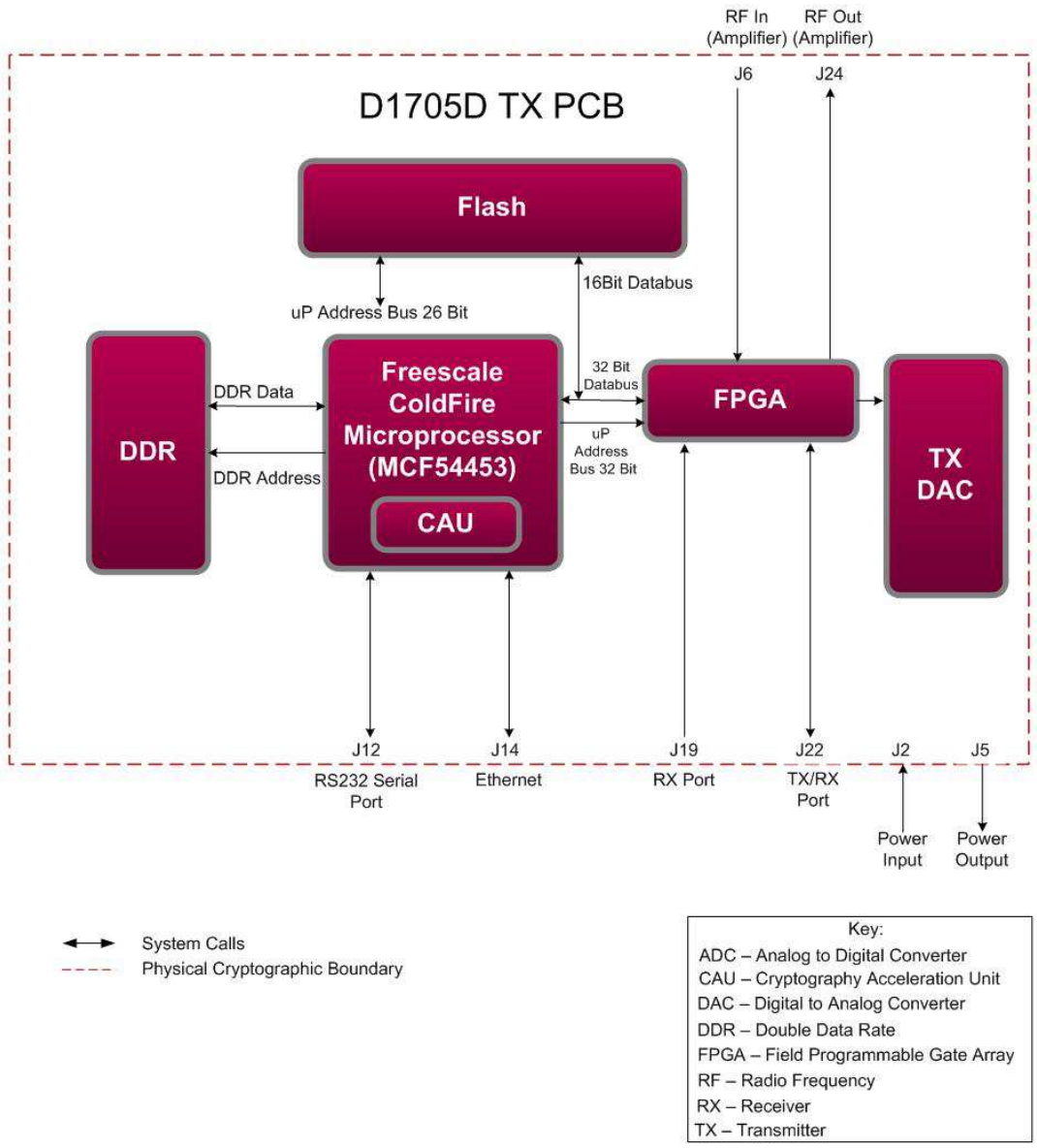

Figure 2 – Cobham D1705D TX PCB Physical Block Diagram

Figure 3 depicts the logical cryptographic boundary for the module that surrounds the single Cobham NETNode IP Mesh Radio cryptographic firmware library, e.g."FIPS Firmware" and the Freescale processor's cryptographic acceleration unit (CAU), e.g. "FIPS Hardware". The firmware library is the only component of the firmware included in the logical boundary, while the CAU is the only component of the processor hardware which is included in the logical boundary.

The colored arrows indicate the logical information flows into and out of the module. The controlling firmware component makes system calls to the cryptography acceleration unit which includes the Critical Security Parameters (CSPs) being controlled by the firmware. The two components of the module exchange information with each other and all other exchanges happen between the firmware and the external ports and interfaces. The module's cryptographic firmware library is accessed by the Cobham NETNode IP Mesh Radio's application software.

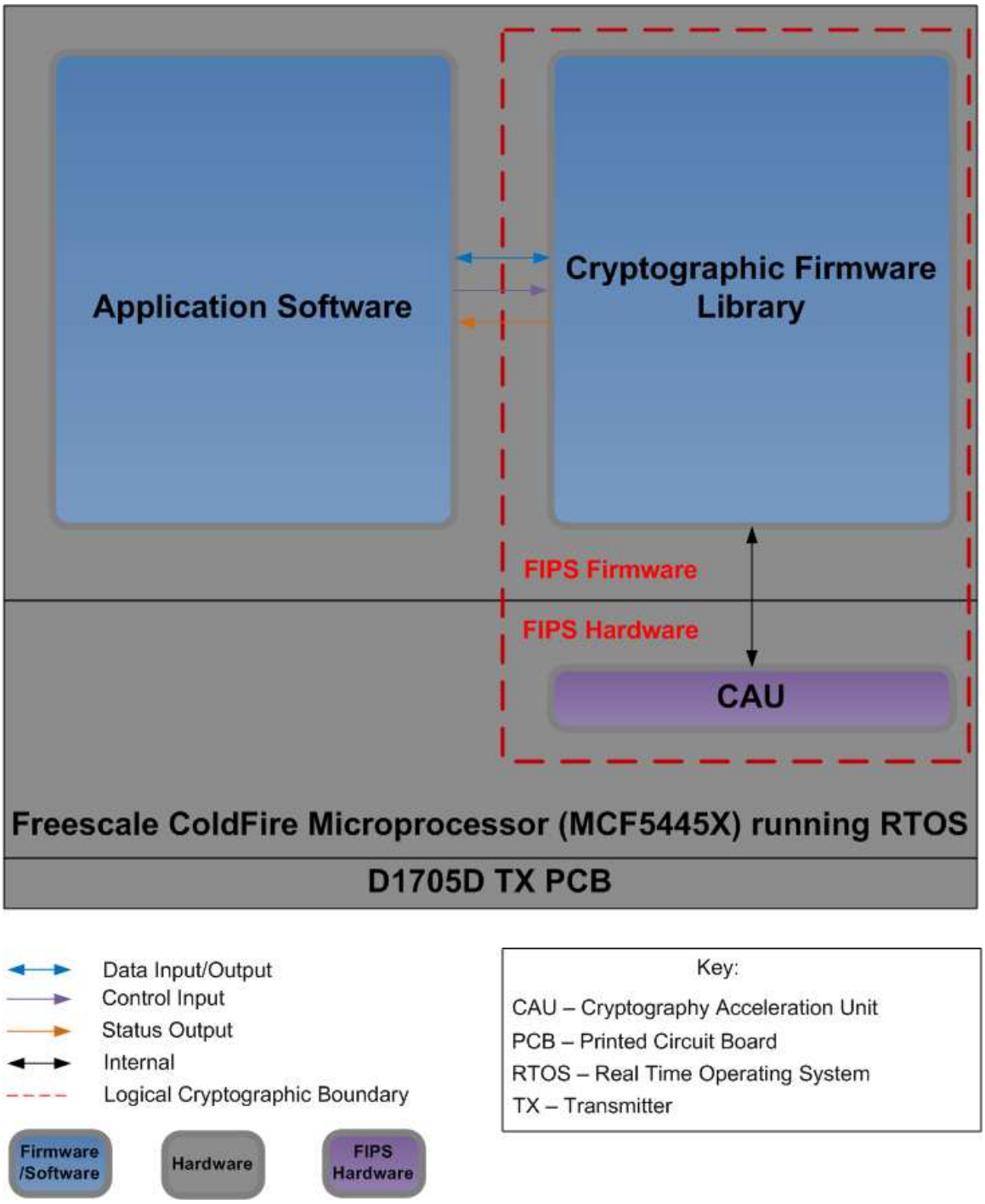

Figure 3 – Cobham D1705D TX PCB Logical Block Diagram

The cryptographic module was tested and found compliant on the following platform:

- Cobham D1705D TX PCB

Figure 4 below depicts the Freescale ColdFire Microprocessor (MCF54453) hardware component of the module.

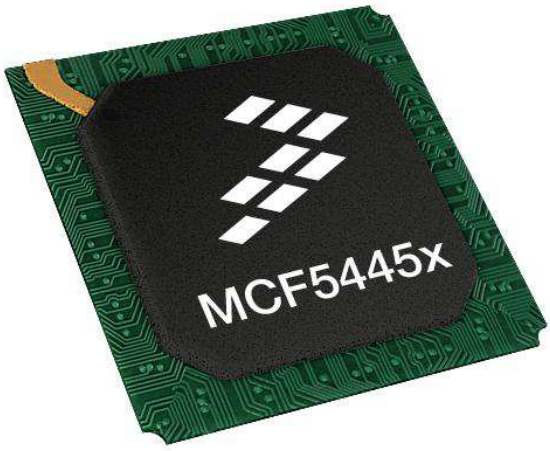

Figure 4 – Freescale ColdFire Microprocessor (MCF5445X Family)

2.3 Module Interfaces

The module's logical interfaces exist at a low level in the software as an Application Programming Interface (API). Both the API and physical interfaces can be categorized into the following interfaces defined by FIPS 140-2:

- Data Input
- Data Output
- Control Input
- Status Output

The Power Supply, External Power Adapter Supply, RS232 Serial, and Ethernet ports have JST[12] connectors. The RX[13] Port (SMP[14] coaxial connector) is located within the Cobham NETNode IP Mesh Radio to interface the TX PCB with the RX PCB. The remaining ports all have SMP coaxial connectors. Note that, as required by FIPS Implementation Guidance 1.9, all status and control ports and interfaces of the hybrid module are directed through the firmware component logical interfaces. The mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module interfaces can be found in Table 2 below.

[12] JST – Japan Solderless Terminal
[13] RX – Receiver
[14] SMP – Sub-Miniature Push-On

Table 2 – FIPS 140-2 Logical Interface Mappings for the D1705D TX PCB

FIPS Logical Interface	Physical Port/Interface	Module Interface (API)
Data Input	• J6 (RF[15] In – Amplifier Port) • J12 (RS232 Serial Port) • J14 (Ethernet Port) • J19 (RX Port) • J22 (TX/RX Switch Port)	The firmware library's API calls that accept input data for processing through their arguments.
Data Output	• J12 (RS232 Serial Port) • J14 (Ethernet Port) • J22 (TX/RX Switch Port) • J24 (RF Out – Amplifier Port)	The firmware library's API calls that return by means of their return codes, arguments generated, or processed data back to the caller.
Control Input	• J12 (RS232 Serial Port) • J14 (Ethernet Port)	The firmware library's API calls that are used to initialize and control the operation of the module.
Status Output	• J12 (RS232 Serial Port) • J14 (Ethernet Port)	Return values for the firmware library's API calls.
Power	• J2 (Power Supply Port) • J5 (External Power Adapter Supply Port)	N/A

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer (CO) role and a User role. Roles are assumed implicitly by an operator based on the selection of cryptographic functions to be performed. All services and requests are provided via the firmware library's API calls. The Freescale ColdFire Microprocessor's CAU does not provide any direct user services or subservices.

Note 1: Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Note 2: Input parameters of an API call that are not specifically a signature, hash, message, plaintext, ciphertext, or a key are NOT itemized in the "Input" column, since it is assumed that most API calls will have such parameters.

Note 3: The "Input" and "Output" columns are with respect to the module's logical boundary.

2.4.1 Crypto Officer Role

The CO is responsible for installing, configuring, and managing the module. Descriptions of the services available to the Crypto Officer role are provided in Table 3 below.

[15] RF – Radio Frequency

Table 3 – Crypto Officer Services

Service	Description	Input	Output	CSP and Type of Access
ConfigAESScrambling	This function performs the critical function tests on the keys provided and writes key schedules when keys are valid	API Call Parameters, AES key	Status Message	AES key (RX)
CryptoVersion	This function returns the firmware module version	API Call	Status Message	N/A
TestCryptoCore	This function runs the power-on self-tests and the module integrity test using the HMAC SHA-256 algorithm	API Call Parameters, Hash, HMAC key, Power Cycle	Status Message, Hash	HMAC key (X)
Zeroize keys	Zeroize keys utilized by the module	Power Cycle	Status Message	AES key (W) HMAC Key (W)
Show Status	The status of the module is observed over the serial interface during the initial power-on of the module and by issuing the "CryptoVersion" and "TestCryptoCore" API calls.	Power Cycle, API Call	Status Message	N/A

2.4.2 User Role

The User role has the ability to perform the cryptographic services offered by the module. Descriptions of the services available to the User role are provided in Table 4 below.

Table 4 – User Services

Service	Description	Input	Output	CSP and Type of Access
AESScramblePacket	Pass unencrypted data to be encrypted by the module	Plaintext data	Ciphertext data	AES key (X)
AESDescramblePacket	Pass encrypted data to be decrypted by the module	Ciphertext data	Plaintext data	AES key (X)
Generate Keyed Hash	Compute HMAC SHA-256 message authentication code on a given input	Plaintext data and HMAC key	Message authentication code	HMAC key (X)
Generate Hash	Compute SHA-256 digest on a given input	Plaintext data	Hash	N/A

Table 5 – Non-Approved Services

Role	Service	Non-Approved/Non-Compliant Algorithms
CO	ConfigDESScrambling	DES[16]
CO	Key Validation Test	CRC[17]
User	DESScramblePacket (Encryption) Non-Compliant	DES
User	DESDescramblePacket (Decryption) Non-Compliant	DES

2.5 Physical Security

The Cobham AES Cryptographic Firmware-Hybrid Module has a multi-chip embedded embodiment. The physical cryptographic boundary is the border of the D1705D TX PCB of the radio. All physical components are made of production-grade materials, and all integrated circuits (ICs) in the module are coated with commercial standard passivation.

All keys, intermediate values, and other CSPs remain in the process space of a single operator. The operating system protects memory and process space from unauthorized access. No non-cryptographic processes may interrupt the module during execution.

2.6 Operational Environment

The module employs a non-modifiable operating environment. The module's firmware (Firmware Version: 1.0) is executed by the module's Freescale ColdFire Microprocessor. The module runs on a FreeRTOS[18] (version 6.0.5).

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 6 below.

Table 6 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES-CBC[19] encryption/decryption with 128- and 256-bit keys	3211
HMAC SHA-256	2024
SHA-256	2658

The module includes the following non-compliant algorithms; which are not used in the FIPS-Approved mode of operation:

- Single-DES (Encryption & Decryption)
- CRC-32

[16] DES – Data Encryption Standard
[17] CRC – Cyclic Redundancy Check
[18] RTOS – Real-Time Operating System
[19] CBC – Cipher Block Chaining

All secret keys and CSPs are protected against unauthorized disclosure, modification, and substitution. Only AES and HMAC keys enter the module electronically in plaintext via the platform's internal path from the application software. The module only operates with references to parameters and CSPs stored in stack memory. When a service completes (either Approved or non-Approved), the reference to the location where the CSP is stored is invalidated, thus the module can no longer access it.

The module supports the CSPs listed below in Table 7.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES 128 key	128-bit AES key	Generated externally, Electronically input in plaintext	Never	Plaintext in volatile memory	Power cycle	Used as input into CBC Encryption/Decryption operation
AES 256 key	256-bit AES key	Generated externally, Electronically input in plaintext	Never	Plaintext in volatile memory	Power cycle	Used as input into CBC Encryption/Decryption operation
HMAC key	HMAC SHA-256 key	Generated externally, Electronically input in plaintext	Never	Plaintext in volatile memory	Power cycle	Passed to the module as part of a keyed hash operation

2.8 EMI/EMC

The Cobham AES Cryptographic Firmware-Hybrid Module is a "Class A" device and was tested and verified to conform to the EMI/EMC requirements found in the following regulations:

- FCC[20] Subpart 15A Rule Section 15.21
- FCC Subpart 15B Rule section 15.105
- FCC Subpart 15A Rule section 15.19(a)(3)

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and loaded into memory. The following sections list the self-tests performed by the module, their expected error status, and error resolutions.

2.9.1 Power-On Self-Tests

The Cobham AES Cryptographic Firmware-Hybrid Module performs the following self-tests at power-on:

Table 8 – List of Power-On Self-Tests

Power-On Test	Description
Firmware Integrity Test	HMAC SHA-256 integrity test performed on the module image
SHA-256 KAT[21]	SHA-256 KAT performed when module is loaded
HMAC SHA-256 KAT	HMAC SHA-256 KAT performed when module is loaded
AES 128 Encryption/Decryption KAT	AES 128 encryption/decryption KAT performed when module is loaded
AES 256 Encryption/Decryption KAT	AES 256 encryption/decryption KAT performed when module is loaded

All data output (except status information) is inhibited while the module is performing its power-on self-tests. The module only provides services only after all tests have passed. If any of the tests fail, a flag is set that prevents any calls from being made to the module. When this flag is set, the module returns the flag value, enters a critical error state, and the process is halted by the RTOS. While the module is in this state, all data output is inhibited (except status information), the user interface is inaccessible, and no user services are available until the CO power cycles the host device. Power cycling the host device can also be used to run power-on self-tests on demand.

2.9.2 Critical Functions Self-Tests

The Cobham AES Cryptographic Firmware-Hybrid Module performs the following critical self-tests in Table 9:

[20] FCC – Federal Communications Commission
[21] KAT – Known Answer Test

Table 9 – List of Critical Functions Self-Tests

Critical Functions Test	Critical Function Tested
Key Validation Test	This test checks that the provided CRC matches the CRC of the 128-bit key for AES 128 or to each 128-bit key half for AES 256.
Zero Keys Test	This test checks that the 128-bit key for AES 128 or each 128-bit key half for AES 256 is not all zeros.

If any of the critical functions tests fail the associated key schedule is invalidated by setting the key_ok flag to false. This will block the processing of packets that are due for encryption/decryption in the AESScramblePacket and AESDescramblePacket functions and place the module in a 'soft-error' state. In the 'soft-error' state, the module will remain functional but will return the false key_ok flag value and user services will be inhibited until valid keys are loaded into the module.

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Cobham AES Cryptographic Firmware-Hybrid Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Crypto Officer Guidance

This section details the CO guidance for secure initialization and management of the module.

3.1.1 Initial Setup

The Cobham AES Cryptographic Firmware-Hybrid Module is embedded on the PCB of the Cobham NETNode IP Mesh Radios. This document assumes that the Crypto Officer has performed initial setup of the Cobham NETNode IP Mesh Radio (e.g., antennae & data connection setup, initial configuration, and configuring radio Talkback and GPS settings). This document also assumes that the radio has been mounted appropriately. It is the Crypto Officer's responsibility to configure the module to use the FIPS-Approved algorithms listed in Table 6 above.

3.1.2 Monitoring Status

The CO should monitor the module's status by viewing the status output via the serial interface during the initial power-on of the unit. The CO can view the status output by power-cycling the unit in order to witness all the power-on self-tests execute and the module report that it is in its FIPS-Approved mode of operation. If the power-on self-tests fail, the module is disabled and will not accept cryptographic service requests.

The CO can also obtain the module status by issuing the "TestCryptoCore" and "CryptoVersion" API calls. The "TestCryptoCore" API call will check the module's "crypto_core_health" global variable. If this flag is set to anything other than "0" (healthy), it will not accept any requests for cryptographic services from applications or services residing in the firmware. The "CryptoVersion" API call returns the module version which is used by the CO to verify that the correct FIPS-Approved module is in use.

3.1.3 Zeroization

The CO can manually zeroize keys and CSPs used by the module by power cycling the radio.

3.2 User Guidance

The Cobham AES Cryptographic Firmware-Hybrid Module is designed for use by software application of the Cobham NETNode IP Mesh Radio. The User shall adhere to the guidelines of this Security Policy. The User does not have any ability to install or configure the module. Operators in the User role are able to use the services available to the User role listed in Table 4. The User is responsible for reporting to the CO if any irregular activity is noticed.

3.3 FIPS-Approved Mode of Operation

The module is in a FIPS-Approved mode of operation when using a FIPS-Approved algorithm (Table 6) and its associated services. The use of non-Approved algorithms with their associated services leads the module to operate in the non-Approved mode of operation. The services available in the non-Approved mode of operation are listed in Table 5 above.

When an operator uses an API call to use a non-Approved service, there is no access to any CSPs of FIPS-Approved algorithms. The module will only return to a FIPS-Approved mode of operation when the operator completes the non-Approved service and applies a FIPS-Approved service via an API call. The microprocessor on the module is single-threaded and only performs one service at a time.

4 Acronyms

Table 10 provides definitions for the acronyms used in this document.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
API	Application Programming Interface
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
COFDM	Coded Orthogonal Frequency-Division Multiplexing
CRC	Cyclic Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DDR	Double Data Rate
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
GPS	Global Positioning System
HMAC	(keyed-) Hash Message Authentication Code
IC	Integrated Circuits
IP	Internet Protocol
JST	Japan Solderless Terminal
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
PCB	Printed Circuit Board
RF	Radio Frequency
RX	Receiver
RTOS	Real-Time Operating System
SATCOM	Satellite Communications
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm

Acronym	Definition
SMP	Sub-Miniature Push-On
TCS	Tactical Communications and Surveillance
TX	Transmitter

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 (703) 267 6050
Email: info@corsec.com
http://www.corsec.com