CS67PLUS Cryptographic Module

Hardware Version 004F014840-1

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.1

Date: 09/13/2022

Comtech Systems, Inc.
212 Outlook Point Drive, Suite 100
Orlando, FL 32809
Telephone: +1-407-854-1950
Fax: +1-407-851-6960
https://www.comtech.com/systems.html

Table of Contents

List of Tables

List of Figures

1. Introduction

Comtech Systems designs, develops, and produces communication systems which support line-of-sight ("LOS") and troposcatter beyond-line-of-sight ("BLOS") communications. These systems are designed for a variety of applications, including lightweight tactical communication systems, and stationary redundant fixed installations. These systems feature data encryption to secure over-the-air communications.

The CS67PLUS is a software-defined adaptive troposcatter radio assembly, packaged in a compact sealed enclosure. Within this assembly resides an FPGA containing a CS67PLUS Cryptographic Module cryptographic subsystem. The module is defined as a sub-chip cryptographic subsystem, within a single-chip hardware module, that provide data encryption and decryption, with the ability to bypass the encryption and decryption and pass plaintext data instead.

The cryptographic module resides within the CS67PLUS radio assemblies listed in the table below.

Hardware Version	Radio Firmware Version	Distinguishing Features
004F014840-1	659F014840-1	FPGA 10AS066H3F34I2SG

Table 1 - Cryptographic Module Configuration

The following table lists the level of validation for each area in FIPS 140-2:

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

Table 2 - Security Level Detail

2. Cryptographic Module Specification

2.1 Hardware and Physical Cryptographic Boundary

The CS67PLUS radio assembly contains an FPGA, SDRAM, non-volatile memory storage (FLASH), and other devices and controllers that interface to the FPGA. Only the sub-chip cryptographic subsystem within the Intel Arria 10 SoC FPGA resides within the cryptographic boundary. All other ICs, memories, I/O controllers, and interfaces residing outside of the cryptographic boundary, including the onboard dual core ARM Cortex-A9 processor residing on the SoC and FLASH memory storage

containing the firmware used by the ARM processor and the radio assembly firmware are excluded components. Note the FPGA is manufactured by Intel, which purchased Altera after the Arria 10 FPGA was designed, hence why the silkscreen on the FPGA is labeled Altera while the current manufacturer is Intel.

Figure 1 – Physical boundary (Arria 10 FPGA)

Within the cryptographic boundary, the module encrypts and decrypts Ethernet data traffic. The clock, hard reset, data input, and data output ports signals are generated outside of the FPGA. The module is managed by an onboard 32-bit ARM processor, which accesses the module via the register read/write and soft reset ports.

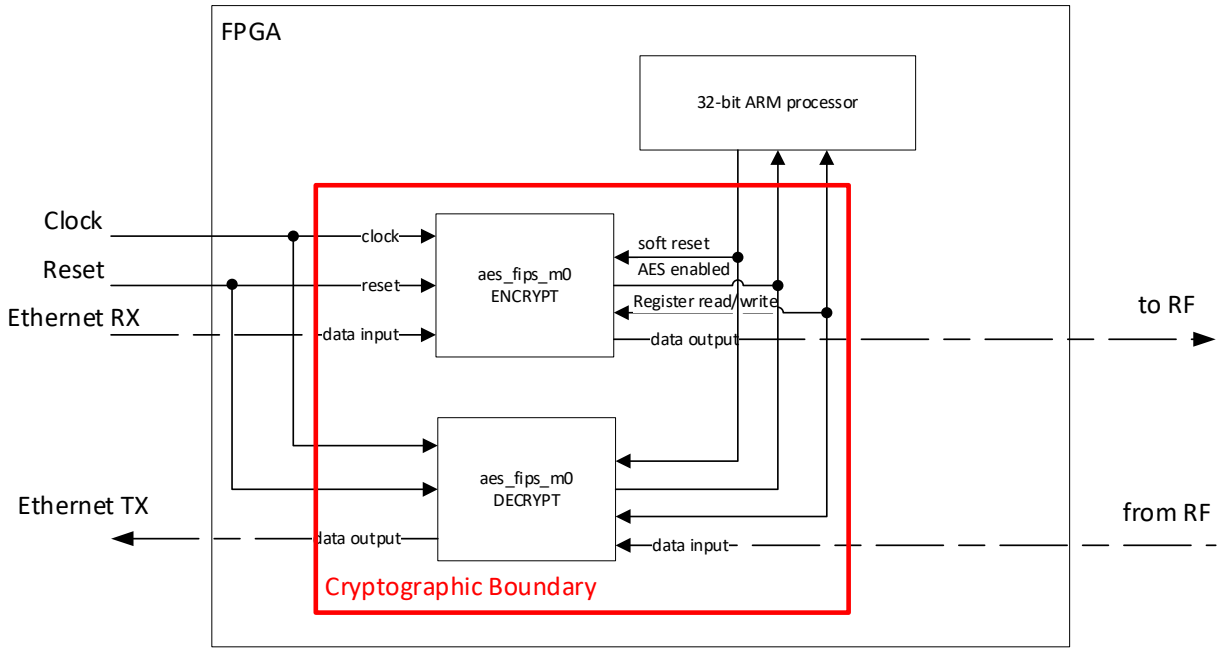

Figure 2 – Sub-chip Cryptographic subsystem

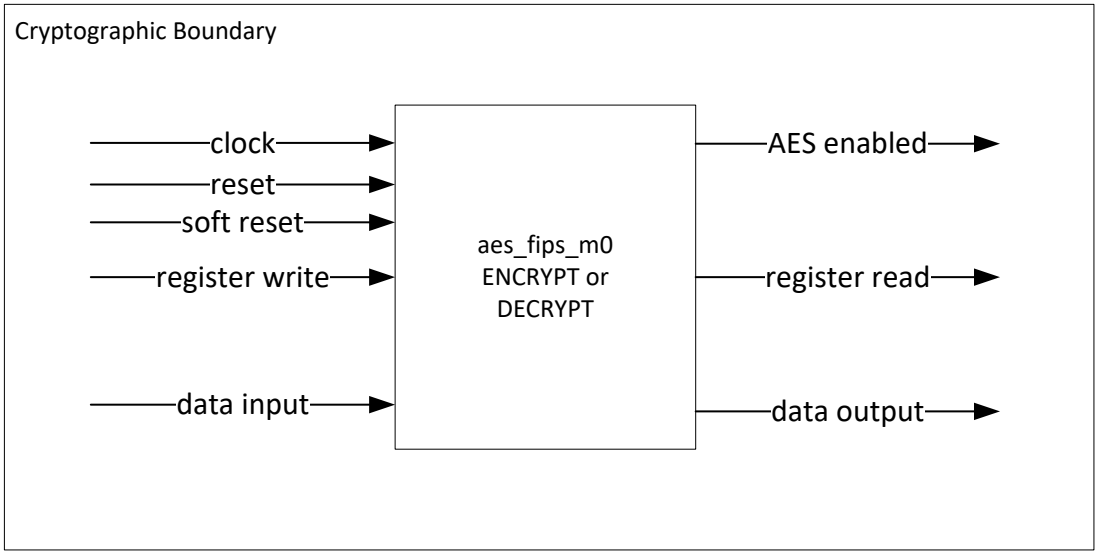

Figure 3 - Block diagram of Cryptographic Subsystem

2.2 Ports and Interfaces

Physical Port	Description	Logical Interface
Clk	Clock signal	Data Input
Reset	Reset signal to FPGA	Data Input
Soft Reset	Reset signal from within FPGA	Data Input
Data Input	128 bit data bus	Data Input
Data Output	128 bit data bus	Data Output
Register Read	32 bit data bus / addressable with 6 address lines	Status Output
Register Write	32 bit data bus / addressable with 6 address lines	Control Input
AES Enabled	Discrete signal	Status Output

Table 3 - Ports and Interfaces

2.3 Mode of Operation

The module has a single mode of operation, FIPS Mode.

2.4 Zeroization

The authentication password is zeroized by erasing the FLASH image. The module must be shipped to the manufacturer for zeroization.

3. Cryptographic Algorithms & Key Management

The module implements the FIPS Approved cryptographic functions listed in the following tables.

3.1 Approved Cryptographic Algorithms

CAVP Cert	Algorithm [Standard]	Mode/Method	Key Size(s)	Use / Function
#A1700	AES [FIPS 197, SP 800-38A]	CTR, ECB*	256-bit	Encrypt or Decrypt Data Input

Table 4 - Approved Algorithms and CAVP Certificates

*Note: ECB was CAVP tested as a prerequisite for CTR but not used by the module.

3.2 Cryptographic Key Management

The table below provides a complete list of the Secret Key and CSP used by the module:

Key / CSP Name	Key / CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES traffic key / Nonce	AES-CTR 256-bit key / 128-bit nonce	Generated externally; input in plaintext	Never output from module	Located in FPGA RAM in plaintext	Reset	Encrypts / decrypts traffic data
Password	User Authentication password	Generated externally; input in plaintext	Never output from module	Stored in FLASH in plaintext	Erase FLASH image (module disposition)	User authentication

Table 5 - Secret Key and CSP

3.2.1 Key Generation

The Traffic key is generated externally to the module.

3.2.2 Key Storage

The Traffic key is stored in FPGA RAM in plaintext. The authentication password is stored on the FPGA binary image residing within a FLASH module.

3.2.3 Key Zeroization

The Traffic Key is zeroized by performing a reset (hard or soft).

4. Roles, Authentication and Services

4.1 Roles and Authentication of Operators to Roles

The module supports two separate roles, the Cryptographic Officer (or Crypto Officer), and the User. The user role authenticates to the module. Note 'User' refers to the system outside of the Cryptographic Boundary and not the end user. The Crypto Officer is responsible for the building of the

module(s) to the FPGA image and the deployment of the created image to the FLASH module of the CS67PLUS radio assembly. See section 8.1 for details.

4.2 Authentication Methods

The user role authenticates using a fixed password. The module accepts passwords from 8 to 15 alphanumeric digits and will only authenticate if the password matches the corresponding password designated to the module revision.

Comtech Systems provides the fixed password through an internal secure mechanism to the user. The password is written to the hardware assembly which is protected by the physical enclosure of the single chip module embodiment of this sub-chip module.

Authentication Type	Strength
Password	The password is between eight and fifteen alphanumeric characters. Alphanumeric characters include numbers 0 – 9 and the letters A – Z, both uppercase and lowercase. Given 62 possible alphanumeric character combinations, the single attempt guessing probability is 62^{-8}, which is less than 1 in 1,000,000. Due to the access speed of the register read/write ports, the maximum number of trials possible is less than $250e^6/(N+1)$ trials per second, where N is the number of characters in the password. The probability of a successful random attempt during a one-minute period is (1 / 62^8) * 60 * (250e6 / 9) = 7.63e-6, which is less than 1:100,000. Note the password buffer must be cleared before transmitting a new password sequence. The clearing of the password buffer with the value of 0x100 is considered an extra register access, hence why the maximum number of trials formula above uses N+1 instead of N as a divisor.

Table 6 – Password Restrictions

4.3 Services

All services implemented by the module are listed in the tables below. Note Show status service is invalid before Log In service first attempt.

Service Name	User	Crypto Officer	CSP access
Log in	X		Password (I/X)
Encrypt / Decrypt	X		AES key (X)
Bypass	X		n/a
Load Key / Nonce	X		AES key (I)
Self-Test	X	X	n/a
Reset		X	AES key (Z)
Show Status	X		n/a
Zeroize Module	X		(Z)

Table 7 – Services and CSP Access Rights

I or Input: Input to the module

X or Execute: Use of the Critical Security Parameter

G or Generate: Generation of module password

Z or Zeroize: Zeroization of module

5. Self tests

5.1 Power-On Self Tests

The module performs the following self-tests upon a hard or soft reset:

- Known Answer Tests (KATs)
    - Encrypt AES CTR KAT
    - Decrypt AES CTR KAT

5.2 Conditional Self Tests

The module also performs the following conditional self-tests:

- When entering bypass mode
- When exiting bypass mode

5.3 Status

A register read from address 0 denotes the following status information:

- Bit 29 denotes the result of the self-test and is set if the self-test failed
- Bit 30 denotes the status of the bypass mode and is reset if the module is in bypass mode

See *CS67PLUS Cryptographic Module Register Map* for more information.

6. Physical Security

The module resides on an opaque commercial chip package. Attempting to penetrate the device will leave visible evidence of tampering.

7. Operational Environment

The operational environment requirements do not apply since the module operates in a non-modifiable environment. The sub-chip module operates within an Intel Arria 10 FPGA and does not make use of an operating system or function as a general purpose CPU.

8. Guidance and Secure Operation

8.1 Security Rules and Guidance

The module is intended to be used by Comtech's software developers for creating the firmware residing within the CS67PLUS radio assembly.

To generate the firmware, the Crypto Officer retrieves the VHDL source files stored within the internal GIT repository tagged with the proper revision found in this document. The firmware is created by first compiling the design using the Intel Arria 10 FPGA synthesis tool software. Once compiled, a post synthesis step is performed which prepares the image to be uploaded to the radio module via a JTAG interface found on the within the radio assembly circuit board assembly. Further details may be found in internal build description document (BDD) 069F014840-1.

To load the cryptographic key, the user loads the 256 bit encryption key to registers 0x20 – 0x3C and the 128 bit encryption NONCE to registers 0x40 – 0x4C via the module's register write interface. It is the responsibility of the user to load a FIPS 140-2 compliant 256 bit AES-CTR cryptographic key and NONCE.

To load the module password, the user loads the password serially into register 0x10 via the module's register write interface. Once the correct password has been loaded in the module, the module's status register 0x0 will denote validity. Operator shall regenerate the nonce at every system startup to protect against replay attacks. See the operator's manual for more details.

Further details may be found in the BDD document.

To change the hardcoded module password, the Crypto Officer would modify the 'PASSWORD_STR' constant located within the VHDL source files and recreate the firmware. It is the responsibility of the Crypto Officer to choose a password which meets the password restrictions found in Table 6 – Password Restrictions. Further details may be found in the BDD document.

9. Mitigation of other Attacks

The module does not mitigate against any other attacks.

10. References and Standards

The following Standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Table 8 - References

11. Acronyms and Definitions

The following Acronyms are referred to in this Security Policy.

Acronym	Definition
AES	Advanced Encryption Standard
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter-mode
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
NONCE	Number user ONCE
KAT	Known Answer Test
N/A	Not Applicable

Table 9 - Acronyms