®Sypher AES-256-bit Encryption FPGA Module

version 1.0

FIPS 140-2 Non-Proprietary Security Policy

Version 1.3

Last update: 2018-07-09

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

Copyrights and Trademarks

Contact Information

America:
Analog Devices, Inc.
One Technology Way
Norwood, MA 02062-9106
www.analog.com

1. Cryptographic Module Specification

This document is the non-proprietary FIPS 140-2 Security Policy for version 1.00 of the ®Sypher AES-256-bit Encryption FPGA Module Cryptographic Module. It 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 Sypher AES-256-bit Encryption FPGA Module (hereafter referred to as “the module”, “the FPGA” or “the FPGA module”) is developed by Analog Devices’ Trusted Security Solutions. It is a crypto sub-system contained within a Microsemi IGLOO2 Field Programmable Gate Array (FPGA) device programmed with the loadable Sypher AES 256-bit Encryption firmware. The programmed FPGA module provides key management and radio audio traffic encryption/decryption.

The FPGA module is used in Axnes’ Polycon Next Generation (PNG) system, which is a wireless Intercom System (ICS) extension for use in both rotary and fixed wing aircraft that integrates with any vendors’ existing ICS. The system includes the MP50 PNG Transceiver, BST50 Base Station, CP50 PNG Control Panel, CHG50/55 PNG Charger, and associated cables. The MP50 PNG Transceiver and BST50 Base Station utilizes 256-bit AES for communication encryption.

Figure 1 is a simplified overview of the FPGA in relation to other devices in the radio. The Red side interfaces to the Main microcontroller. The Black side interfaces to the Software Defined Radio (SDR) Digital Signal Processor (DSP). The FPGA encrypts ‘Red’ data into ‘Black’ and decrypts ‘Black’ data into ‘Red.’

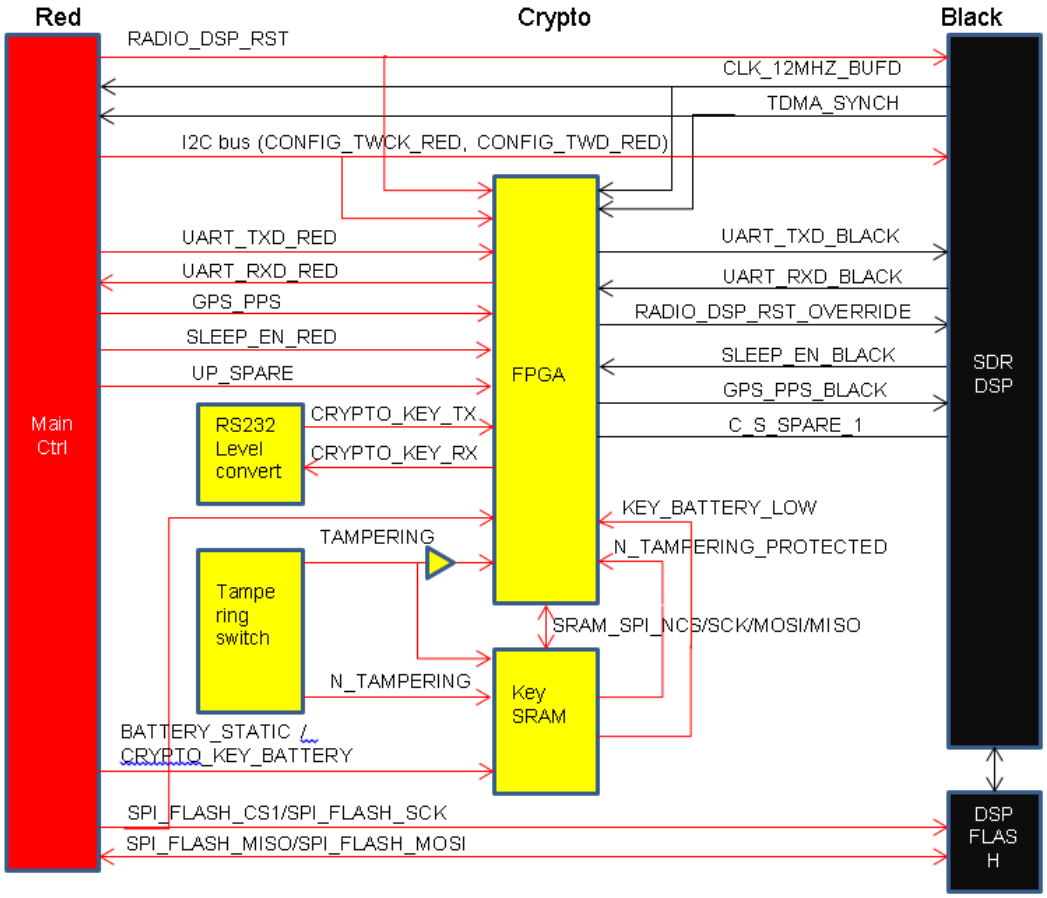

Figure 1 – Radio Block Diagram

Figure 2 shows the internal organization of the FPGA device at the top-most level. It has separate blocks dedicated to specific functionality. The physical boundary of the FPGA module under test is the continuous enclosure of the FPGA device. The logical boundary of the FPGA module consists of the Crypto Processing block and the Key Processing block. For the purpose of the FIPS 140-2 validation, this is a hard circuitry core sub-chip module per FIPS 140-2 IG 1.20.

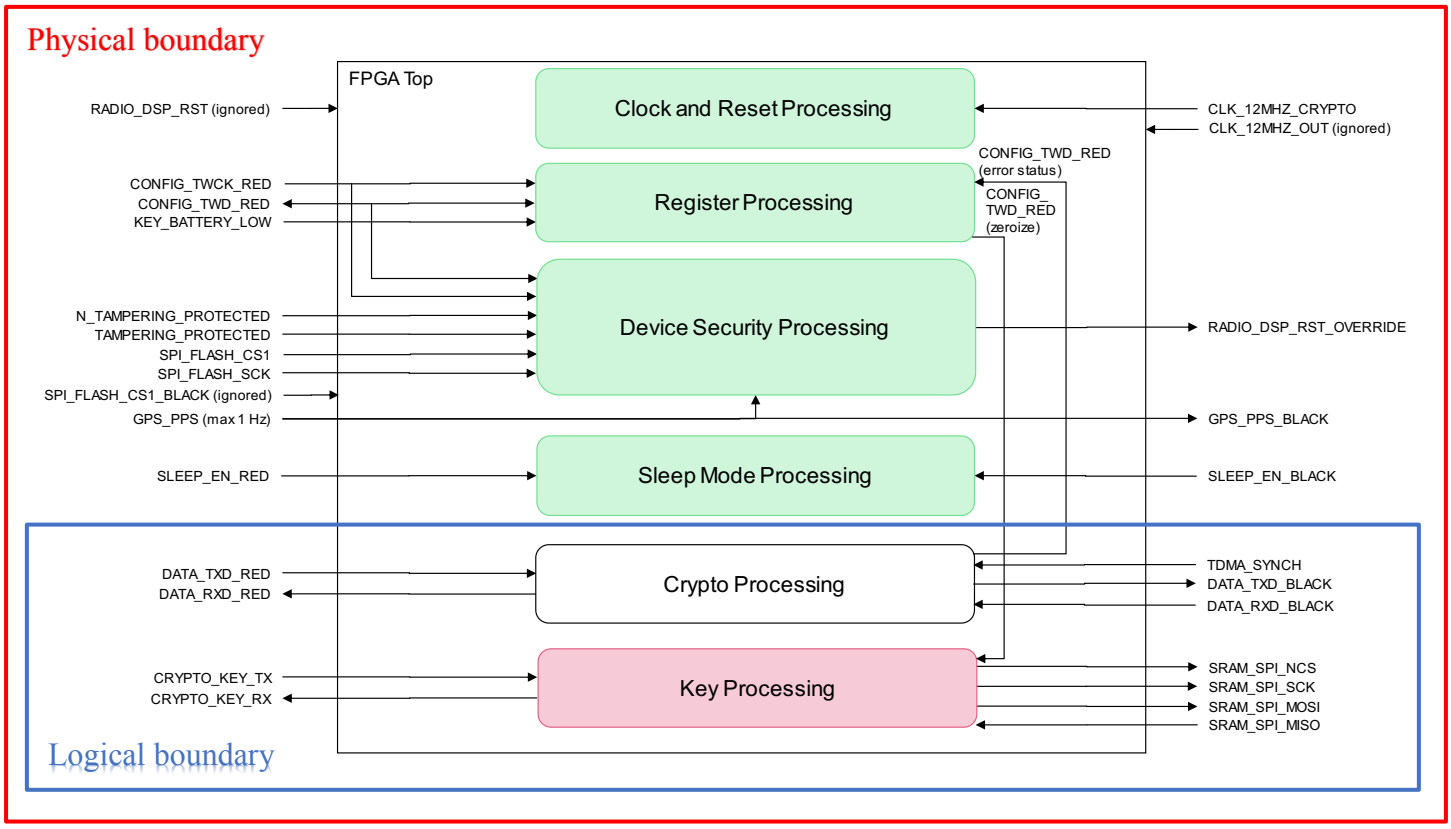

Figure 2 – Physical and Logical Boundary of the FPGA Module

1.2. FIPS 140-2 Validation

For the purpose of the FIPS 140-2 validation, the module is a hardware single-chip, sub-chip module that resides within an FPGA device. It is to be validated at an overall Security Level 1. The table below shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2 standard:

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	3
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	3
11	Mitigation of Other Attacks	N/A
Overall Level		1

Table 1 - Security Levels

1.3. Modes of operation

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

2. Cryptographic Module Ports and Interfaces

The following table summarizes the mapping between the four logical interfaces required by the FIPS 140-2 and the physical ports of the FPGA module:

Logical Interface	Physical Port	Description
Data Input	DATA_TXD_RED DATA_RXD_BLACK CRYPTO_KEY_TX SRAM_SPI_MISO	Data input to Crypto Processing block Data input to Crypto Processing block Key input to Key Processing block Key obfuscation data input to Key Processing block
Data Output	DATA_RXD_RED DATA_TXD_BLACK CRYPTO_KEY_RX SRAM_SPI_MOSI SRAM_SPI_NCS SRAM_SPI_SCK	Data output from Crypto Processing block Data output from Crypto Processing block Key output from the Key Processing block to the Crypto Processing block Key obfuscation data output from Key Processing block Key obfuscation control output from Key Processing block Key obfuscation clock output from Key Processing block
Control Input	TDMA_SYNCH CONFIG_TWD_RED	Data frame pulse input Zeroizes keys
Status Output	CONFIG_TWD_RED	Error status received from the Crypto Processing Block
Power input	Power Supply Port	Not applicable for the sub-chip FPGA module. The module gets power from the FPGA device.

Table 2 - Ports and Interfaces

.

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 users.

3.2. Services

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

Service	Algorithms	Role	Access	Keys
Cryptographic Library Services				
Symmetric encryption and decryption	AES	User	Read	AES keys
Other FIPS-related Services				
Show status	n/a	User	n/a	None
Self-Tests	AES	User	Read	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
Reset	n/a	User	n/a	None

Table 3 - Services in FIPS mode of operation

3.3. Algorithms

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

CAVP Cert#	Algorithm	Standard	Mode / Method	Key size	Use
#5177	AES	[FIPS197] [SP800-38A]	ECB, CTR	256 bits	Data Encryption and Decryption

Table 4 - FIPS-Approved Cryptographic Algorithms

3.4. Operator Authentication

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

3.5. Bypass Capability

The module does not have a Bypass capability.

4. Physical Security

The module is a sub-chip module implemented as part of the Microsemi IGLOO2 FPGA device, which is the physical boundary of the sub-chip module. The Microsemi IGLOO2 FPGA device is a sub-chip FPGA within a single-chip physical embodiment with a production grade enclosure and hence conforms to the Level 1 requirements for physical security. Below is an image of the FPGA.

Image 1 - Microsemi IGLOO2 FPGA

5. Operational Environment

The module is a hardware sub-chip FPGA module as part of an FPGA device. The procurement, build and configuring procedure are controlled. Therefore, the operational environment is considered non-modifiable.

6. Cryptographic Key Management

The following table summarizes the keys that are used by the cryptographic services implemented in the module:

Name	Generation	Entry and Output	Storage	Zeroization
AES keys	Keys are generated externally by an authorized source and manually distributed using a key load device.	Keys enter into the FPGA module via the dedicated key load interface. There is no key output.	Stored in plaintext in the FPGA's internal flash	The module provides key zeroization in response to a tamper event, on-demand zeroization on a selected key slot or on all key slots.

Table 5 - Life cycle of AES Keys

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. The keys are provided to the module via the dedicated key load interface (i.e. CRYPTO_KEY_TX), which is a serial port. PYFilling is the python application used for loading keys over the RS-232 serial interface. The module does not output keys in plaintext format outside its physical boundary.

6.3. Key Storage

Up to 16 AES-256-bit keys can be stored in the internal FPGA flash. Keys are obfuscated by a random number. The obfuscation method is not a FIPS-Approved cryptographic function. Therefore, the keys are considered as stored in plaintext from the perspective of FIPS 140-2.

.

6.4. Key Zeroization

There are three ways that keys stored in the FPGA flash are zeroized:

1. Upon a tamper event, the FPGA overwrites all 16 key slots in non-volatile flash memory with zeroes.
2. Zeroizing the selected slot bit in control register zeroes the key in the selected slot in the FPGA flash memory.
3. Zeroizing all bits in the control register zeroes all 16 key slots in the FPGA flash memory.

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

The sub-chip FPGA 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 is a hardware module and hence the integrity check requirement does not apply. The module only implements one FIPS-Approved cryptographic algorithm, AES. It performs a Known Answer Tests (KAT) for AES shown in the following table:

Algorithm	Test
AES	• KAT for AES-CTR with 256-bit key, encryption • KAT for AES-CTR with 256-bit key, decryption

Table 6- Self-Tests

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

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

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

8.2. On-Demand Self-test

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-test.

8.3. Error State

When an error occurs, the module transitions to the Error state and becomes non-operational. In the Error state, services are not available and no data output is possible with the exception of the System Info and Reset services. The module can transition to this state under the following conditions:

- Failure of the power-up self-tests (AES Known answer tests).

9. Guidance

9.1. Configuration Management

SVN is used for the configuration management of the cryptographic module.

9.2. Delivery and Operation

The cryptographic module comes preinstalled on the Axnes PNG appliance. Product information is available at https://www.axnes.com/png.

9.3. Crypto Officer Guidance

The module contains 16 key slots in internal flash memory for storing the AES keys. The Crypto Officer has the ability to zeroize all loaded keys by selecting the Zero-All bit in the menu. Each key will be stored in a register that corresponds to the bit selected. Each key will normally be used for up to 1 to 3 days at a time or when a new operation occurs.

9.4. Module installation

The module is pre-installed during product manufacturing. The crypto officer will use a key loader to load the module with a new key. The user can check that they are using the correct product by verifying the product number on the label. Below are the instructions for the key-loading procedure:

1. Connect a key loader to unit to be loaded, Base Station or Hand Held.
2. Turn on the unit
3. Put the unit in the Key Load Mode:
   Base Station
   - Press “Menu” button on Control Panel
   - Highlight “Cryptography” using the scroll knob
   - Press scroll knob to select
   - Highlight “Start Key Fill” using the scroll knob
   - Press scroll knob to select
   - BS is now ready to receive a key

   Hand Held
   - Press “Menu” button and “OK” button simultaneously to unlock (HH will audibly report “unlocked”)
   - Press “Menu” button to enter menu
   - Press down arrow repeatedly until Cryptography Menu (CM on display)
   - Press “OK” button to enter CM
   - Press “OK” again to enter “Key Fill Mode” (Scrolling key icon shown on display)
4. Select FILL on the key loader to send a key.

9.5. User Guidance

To activate a unit the user confirms a valid key is loaded in the correct key slot, selects the key slot and activates the key. The user role is assumed by the key type that has been loaded onto the device. Key zeroization can be initiated by the user.

10. Mitigation of Other Attacks

There are no mitigations from other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards Publication
KAT	Known Answer Test
NIST	National Institute of Science and Technology
PNG	Polycon Next Generation
POST	Power-On Self-Test
SDR	Software Defined Radio
SVN	Subversion

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** January 19, 2018 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 Techniques** December 2001 http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf