



SOLSDR NETNode Security Module

Firmware Version 1.0

FIPS 140-2 Level 1
Non-Proprietary Security Policy

0. Preface

0.1 Trademarks

All trademarks or registered trademarks that appear in this document are the property of their respective owners.

© Domo Tactical Communications (DTC) Limited.

Domo Tactical Communications (DTC) Limited owns the copyright of this document. Copying and distribution is allowed without the prior permission of DTC.

Contents

0. Preface.....	0-1
0.1 Trademarks.....	0-1
0.2 Document History.....	Error! Bookmark not defined.
1. Product Overview	1-1
1.1 Purpose	1-1
1.2 References.....	1-1
2. SOLSDR NETNode Security Module.....	2-2
2.1 Overview	2-2
2.2 DTC NETNode IP Mesh Radio.....	2-3
2.3 SOLSDR NETNode Security Module	2-4
2.4 Module Type.....	2-5
2.5 Xilinx Zynq-7000 FPGA.....	2-5
2.6 SOLSDR NETNode Security Module Overview	2-6
3. Module Interfaces.....	3-8
4. Roles and Services.....	4-9
4.1 Overview	4-9
4.2 Crypto Officer Role	4-10
4.3 User Role	4-11
5. Physical Security.....	5-13
6. Operational Environment.....	6-14
7. Cryptographic Key Management.....	7-15
8. EMI/EMC.....	8-17
9. Self-Tests.....	9-18
9.1 Introduction.....	9-18
9.2 Power-Up Self Tests.....	9-18
9.3 Critical Functions Self-Tests.....	9-18
9.4 Reconfiguration from One Approved Mode to Another	9-19
10. Mitigation of Other Attacks.....	10-20
11. Secure Operation	11-21
11.1 Introduction.....	11-21
11.2 Crypto Officer Guidance	11-21
11.3 User Guidance	11-22

12. Appendix A – Acronyms 12-24

1. Product Overview

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for a cryptographic module incorporated within the DTC IP Mesh Product Families. Specifically, this document details the security policy that is applicable to the SOLSDR NETNode Security Module used by both the DTC NETNode Phase 5 family of products and the SOL8SDR IP Mesh application. This Security Policy describes how the SOLSDR NETNode Security Module housed within the Xilinx FPGA Xilinx Zynq 7030 Programmable System-On-Chip XC7Z030 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 Canadian Centre for Cyber Security (CCCS) 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 SOLSDR NETNode Security 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 DTC website (<http://domotactical.com>) contains information on the full line of products from DTC.
- 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.

This Security Policy and the other validation submission documentation were produced by Domo Tactical Communications (DTC). The FIPS 140-2 Submission Package is proprietary to DTC and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact DTC.

2. SOLSDR NETNode Security Module

2.1 Overview

Within wireless communication Security and Defence industries, Domo Tactical Communications (DTC) offers a range of technologies and services to solve challenging problems across commercial, defence, and security markets. DTC products include audio, video, and data communication codecs and modems, defence electronics and surveillance products. The offered services are primarily airtime management and systems design services for major government clients.

DTC divisions include:

- Security
 - Video, IP Mesh and COFDM Radio Equipment
 - Covert Audio and Video
 - Command and Control Software products used primarily in the 'Tracking' market

The DTC group specializes in providing military radios, surveillance and communication technologies for successful operation in demanding environments.

2.2 DTC NETNode IP Mesh Radio

The DTC NETNode IP Mesh Radios are designed and manufactured by the DTC group. The DTC 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) modulation and are ideal for use in mobile surveillance applications, command and control, or advanced robotics.

The mesh architecture can contain over 64 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 receivers and cameras.

Figure 2-1 depicts a typical DTC NETNode IP Mesh Radio deployment scenario.

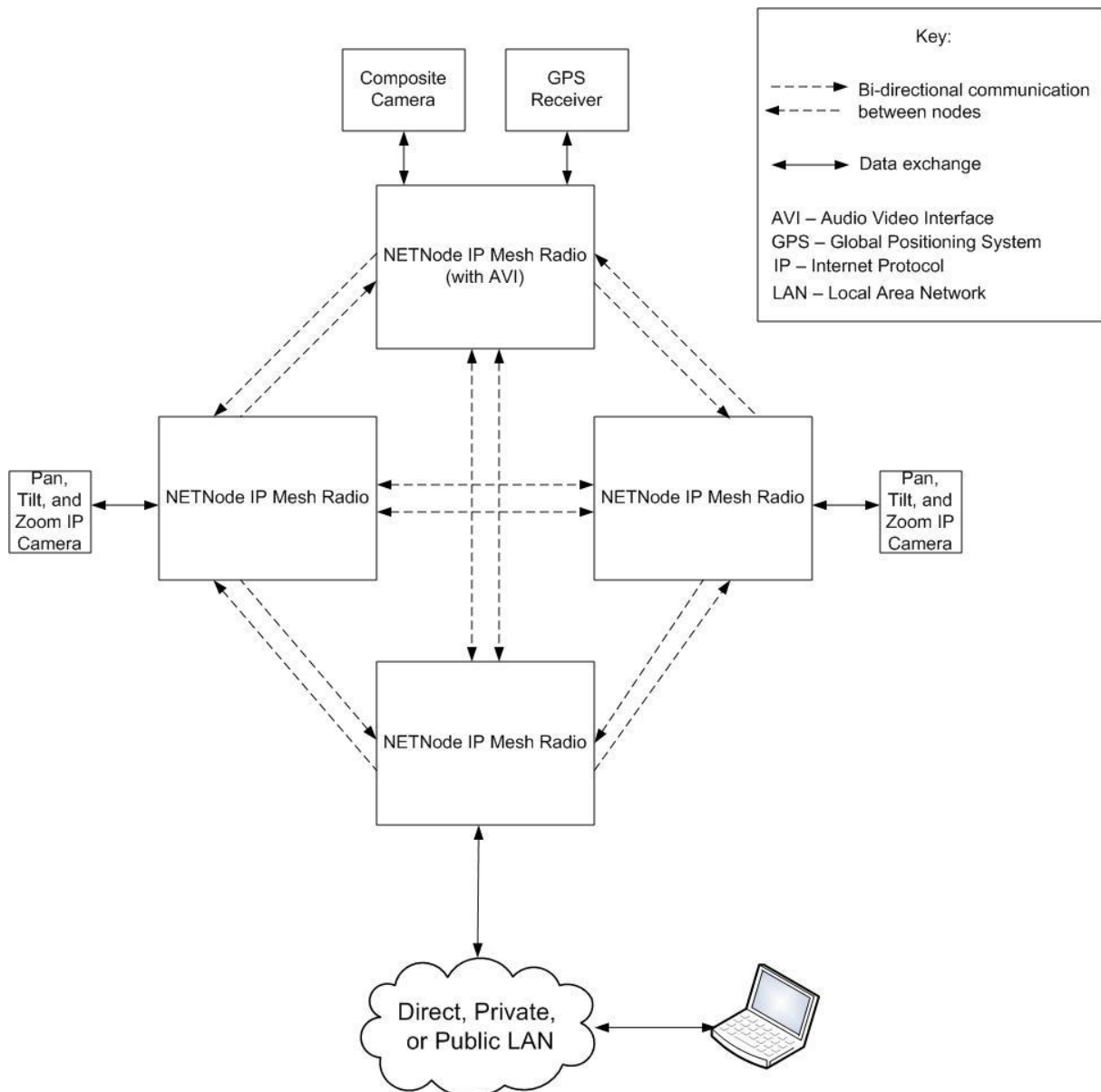


Figure 2-1 – DTC NETNode IP Mesh Radio Deployment Diagram

2.3 SOLSDR NETNode Security Module

The SOLSDR NETNode Security Module is located within the Xilinx FPGA Xilinx Zynq 7030 Programmable System-On-Chip XC7Z030. The programmable Zynq 7030 chip is located on both the DTC NETNode IP Mesh Radio D1800 TX/RX PCB and DTC NETNode IP Mesh Radio D1740 TX/RX PCB.

The module is stored in flash memory and loaded upon boot of the chip. The SOLSDR NETNode Security Module is defined as a firmware module that implements encryption/decryption, hashing and key-hash operations that are loaded upon boot in one of two DTC IP Mesh approved modes of operation. The operational environment the module executes in is considered non-modifiable and not accessible by operators.

The module includes implementations of the following FIPS-approved security functions:

- Encryption and decryption using AES; and
- Hashing and keyed-hashing functions using SHA and HMAC SHA

The SOLSDR NETNode Security Module is validated at the FIPS 140-2 section levels shown in *Table 2-1*:

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	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 2-1 – Security Level as per FIPS 140-2

2.4 Module Type

The module is a firmware module with a single-chip embodiment. The overall security level of the module is 1.

The Xilinx Zynq 7030 FPGA device integrates dual ARM processor cores offering both microprocessor CPU interfaces and inbuilt RAM, flash memory, FPGA logic, and interface connections to external interfaces.

As previously described, the module operates in two approved modes of operation. In the first mode, the encryption process is undertaken entirely in firmware running on a non-modifiable OS which executes on the embedded ARM processor in the FPGA. This module does not use any FPGA hardware acceleration in the encryption process. This mode is defined as the firmware-only or “<30Mbps mode” (also referred to as MIMO20 or Single Mesh mode) of operation. In addition to this mode, the module also supports a high-speed mode or “>30Mbps mode” (also referred to as “Mesh Ultra mode”) when the system uses FPGA logic as a hardware accelerator in the encryption process. To be more precise in the >30Mbps mode, the module uses Programmable Algorithmic Implementation (PAI) in the FPGA. The PAI is considered a full implementation of AES as defined by FIPS 140-2 IG 1.21.

A brief outline of the associated FPGA processing silicon device is given in *Section 2.5* below.

2.5 Xilinx Zynq-7000 FPGA

The module as designed will run on the Zynq-7030 FPGA device. The Zynq®-7000 family is based on the Xilinx All Programmable SoC architecture. These products integrate a feature-rich dual-core or single-core ARM® Cortex™-A9 based processing system (PS) based on an ARM v7 architecture and 28nm Xilinx programmable logic (PL) in a single device. The ARM Cortex-A9 CPUs are the heart of the PS and include on-chip memory, external memory interfaces, and a rich set of peripheral connectivity interfaces.

2.6 SOLSDR NETNode Security Module Overview

The SOLSDR NETNode Security Module cryptographic boundary is illustrated in *Figure 2-2* below. The logical cryptographic boundary is defined as the libmcrypto and the runapp components. The module executes in a non-modifiable operational environment.

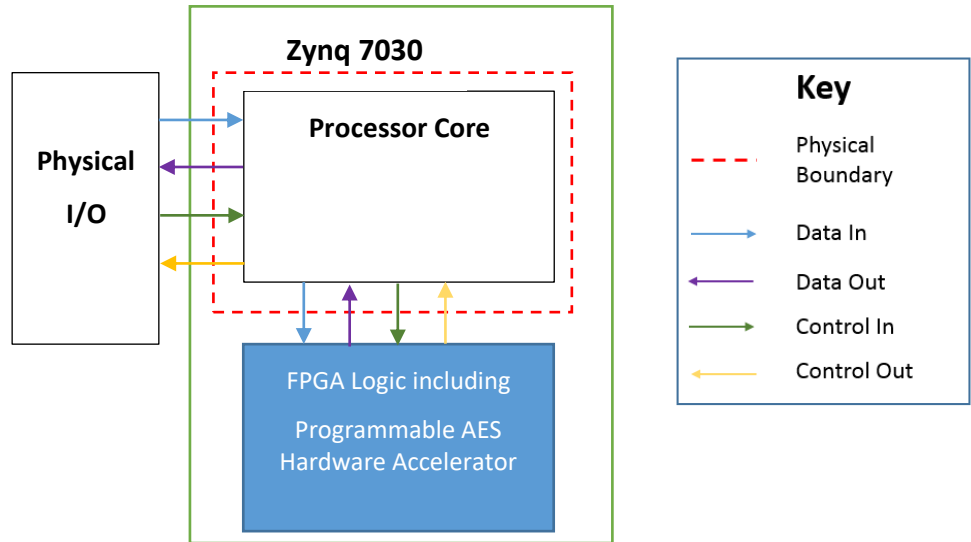


Figure 2-2 – Illustrative Physical Crypto Boundary Diagram

The module supports two approved modes of operation. The first “<30Mbps” executes in firmware-only. The second “>30Mbps mode” mode or high-speed mode makes use of a disjoint PAI hardware AES implementation in the FPGA logic within the Zynq device.

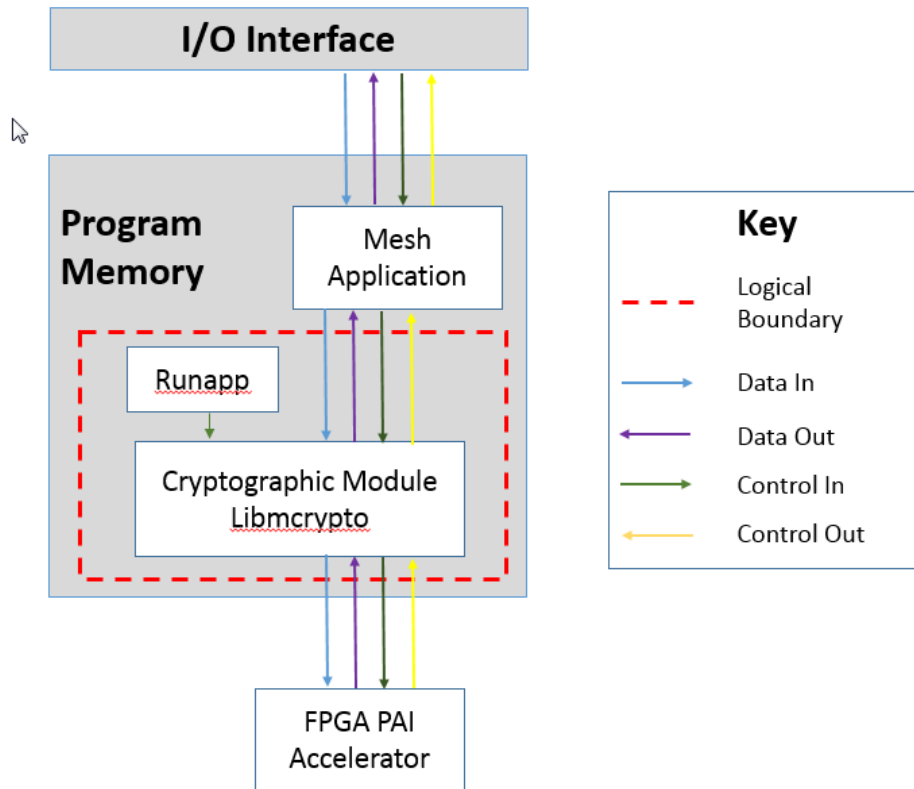


Figure 2-3 – Illustrative Logical Crypto Boundary Diagram

Plaintext data interfaces to the physical radio device via the programmable logic interface pins and via dedicated Ethernet and USB drivers on the FPGA. In the PAI mode the ARM processor uses the 'Zynq Accelerator Coherency Port (ACP Port) to transfer data between the ARM core and the PAI logic. The ACP interface allows the hardware accelerator to issue coherent accesses to the processor memory space.

Libmcrypto is responsible for performing the AES, SHA and HMAC operations. The calling application (Mesh Application) will call into the module using its API. The module's external interfaces are limited to the API function calls that provide data input, data output, status output and control input. The module only operates with references to parameters and CSPs stored in stack memory of the FPGA. Runapp component performs the required FIPS 140-2 integrity tests at power-up and instantiates libmcrypto.

3. Module Interfaces

The module's logical interfaces exist at a low level in firmware 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 mapping of the FIPS 140-2 logical interfaces and the module interfaces can be found in *Table 3-1* below.

FIPS Logical Interface	Physical Port/Interface	Module Interface (API)
Data Input	Function calls into the shared object module Ethernet, USB and serial data Interfaces to the Zynq 7030 chip. Digital video inputs to Zynq 7030. Digital IF interfaces from the Zynq 7030 to the RF input and output. When operating in the PAI mode (>30Mbps mode) the Zynq ACP port is used to transfer data between the processor and the PAI Logic.	Encryption mode function call that inputs the plaintext into the module Decryption mode function call that inputs the ciphertext into the module
Data Output	Function calls into the shared object module Ethernet, USB and serial data interfaces to the Zynq 7030 chip. Digital IF interfaces from the Zynq 7030 to the RF input and output. When operating in the PAI mode (>30Mbps mode) the Zynq ACP port is used to transfer data between the processor and the PAI Logic.	Encryption mode function call that returns the ciphertext Decryption mode function call that returns the plaintext
Control Input	Function calls into the shared object module Ethernet, USB, Serial, Digital IF and ACP interface to the Zynq 7030 chip	Defined API functions that configure the module
Status Output	Function calls into the shared object module Ethernet USB, Serial, Digital IF and ACP interface to the Zynq 7030 chip	Defined API function calls with defined returns to indicate the status
Power Input	Power to the Zynq 7030 chip from host PCB	N/A

Table 3-1 – FIPS 140-2 Logical Interface Mappings for the Module

4. Roles and Services

4.1 Overview

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. Authentication is not implemented by the module. Roles are assumed implicitly by an operator based on the selection of cryptographic functions to be performed.

Note 1: 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 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.

4.2 Crypto Officer Role

The CO is responsible for installing, configuring, and managing the module. The module is configured into the FIPS-approved modes automatically by making the API calls to operate with AES encryption. The steps to configure a FIPS-approved mode of operation on the module have been listed in *Section 11.2.1, Initial Setup* of the document.

Descriptions of the services available to the Crypto Officer role are provided in *Table 4-1* below. These services are common to both approved modes of operation.

Service	Description	Input	Output	CSP/Key and Type of Access
ConfigAESScrambling	This function configures the AES encryption. It undertakes the critical function test on the CRC values, keys provided and generates the key schedules when the keys are valid.	API call parameters (CRC values, Keys and Key schedules are passed to the module as parameters)	Status message	AES CBC key (RX)
TestCryptoCore	This function runs the power-on cryptographic self-tests on-demand.	API call parameters, power cycle	Status message, hash	N/A
Initialization	Runapp component instantiates the module runs integrity tests.	API call parameters	Status message	N/A
Zeroization	Power-cycling or rebooting the FPGA zeroizes all keys in memory	Control Input	N/A	N/A

Table 4-1 – Crypto Officer Services

4.3 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 4-2* below. All the services are available in both approved modes of operation except the AES_CBC_encrypt, and AES_CBC_decrypt which are only used in the firmware only approved mode of operation, and the AES_CBC_encrypt_read and AES_CBC_decrypt-read services which are only used in the hardware accelerated (PAI) approved mode of operation. Where a service is only available in one approved mode of operation it is also declared in *Table 4-2*.

Service	Description	Input	Output	CSP/key and Type of Access
AES_encrypt	Performs AES ECB 128 or 256-bit encryption.	Plaintext data	Ciphertext data	AES ECB key (X)
AES_decrypt	Performs the AES ECB 128 or 256-bit decryption.	Ciphertext data	Plaintext data	AES ECB key (X)
AES_CBC_encrypt	Performs the AES CBC 128 or 256-bit encryption.	Plaintext data	Ciphertext data in <30Mbps mode	AES CBC key (X)
AES_CBC_decrypt	Performs the AES ECB 128 or 256-bit decryption.	Ciphertext data	Plaintext data in <30Mbps mode	AES CBC key (X)
AES_CBC_encrypt_read	In hardware >30Mbps mode this function reads the encrypted data from the PAI implementation.	Control Input to PAI component via ACP	Returns ciphertext data when using PAI hardware accelerator in >30Mbps mode	N/A
AES_CBC_decrypt_read	In hardware >30Mbps mode this function reads the decrypted data from the PAI implementation.	Control Input to PAI component via ACP	Returns plaintext data when using PAI hardware accelerator in >30Mbps mode	N/A
SHA256 (SHA256-Init, SHA256_Bytes and SHA256_Final)	Compute SHA-256 digest on a given input.	Plaintext data	Hash	N/A

Service	Description	Input	Output	CSP/key and Type of Access
HMAC SHA-256 (SHA256_HMAC_Init, SHA256_HMAC_Bytes and SHA256_HMAC_Final)	Compute HMAC SHA-256 message authentication code on a given input.	API call parameters (Plaintext data and a fixed HMAC key passed as parameters)	Message authentication code	HMAC key (X)

Table 4-2 – User Services

5. Physical Security

The SOLSDR NETNode Security Module has a single-chip firmware module embodiment. The physical cryptographic boundary is the Zynq 7030 FPGA device. All physical components are made of production-grade materials.

6. Operational Environment

The module executes in a non-modifiable operating environment. The module (firmware version 1.0) is executed by the module's ARM microprocessor.

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.

The module is embedded into the non-modifiable operating system during the manufacturing process in the factory. The operating system is not user accessible.

7. Cryptographic Key Management

The module implements the FIPS-approved algorithms listed in *Table 7-1* below. The security module uses all the algorithms listed in both approved modes of operation.

Approved Mode of operation	Algorithm	Certificate Numbers
Firmware-only	AES-ECB encryption/decryption with 128- and 256-bit keys	C1533
Firmware-only and >30Mbps mode	AES-CBC encryption/decryption with 128- and 256-bit keys	C1534, C1533
Firmware-only	HMAC SHA-256	C1533
Firmware-only	SHA-256 ¹	C1533

Table 7-1 – FIPS-Approved Algorithm Implementations

All secret keys and CSPs are protected against unauthorized disclosure, modification, and substitution. All keys enter the module electronically in plaintext via the platform's internal path from the application firmware. 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 AES-ECB cryptographic functions are only used to scramble the Initialization Vector (IV) in the AES-CBC function.

The module includes the following non-approved but allowed algorithms; which are used as an Error Detection Code (EDC) in power-up self-tests in the FIPS-approved mode:

- MD5
- CRC-32

¹ HMAC-SHA and SHS always execute in firmware. They do not utilize PAI in the FPGA

The module supports the CSPs listed in *Table 7-2*. All the CSPs listed are available in the security module in both approved modes of operation.

CSP/key	CSP/Key Type	Generation/Input	Output	Storage	Zeroization	Use
AES ECB key	128-bit, 256-bit	Generated externally, electronically input in plaintext.	Never	Plaintext in FLASH memory with CRC-32 checksum appended	By command	Used as input into ECB Encryption/Decryption operation in <30Mbps mode (firmware only)
AES CBC key	128-bit, 256-bit	Generated externally, electronically input in plaintext.	Never	Plaintext in FLASH memory with CRC-32 checksum appended	By command	Used as input into CBC Encryption/Decryption operation in >30Mbps mode (FPGA PAI Accelerator) and in <30Mbps mode (firmware only)
HMAC key	4-byte to 128-byte key	Generated one time only with the source code and never electronically input.	Never	Plaintext in FLASH	Not applicable	Used only as an internal integrity test

Table 7-2 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

8. EMI/EMC

The SOLSDR NETNode Security Module is a Class A device and was tested and verified to conform to the EMI/EMC requirements found in the following regulations:

- FCC 47 CFR Part 90 (2014)
- FCC 47 CFR Part 2 (2014)

Physical Enclosure	PCB Number	FCC ID
SOL8SDR-C	D1800	XRFSOL8SDR-C 1.98-2.7GHz
Phase 5 NETNode-5R	D1740	XRFNETNODE-5R

Table 8-1 – Physical Enclosure List

9. Self-Tests

9.1 Introduction

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.

9.2 Power-Up Self Tests

The SOLSDR NETNode Security Module performs the following self-tests at power-up:

Power-Up Test	Description
Firmware Integrity Test (runapp)	CRC-32 EDC integrity test on runapp at power-up
Firmware Integrity Test (libmcrypto)	MD5 EDC integrity test on libmcrypto at power-up
Hardware Integrity Test on FPGA PAI Accelerator	CRC-32 EDC integrity test on VHDL block of FPGA PAI Accelerator at power-up
Firmware AES ECB KAT (encrypt/decrypt)	Encryption/decryption KAT performed when module is loaded prior to any cryptographic functions. This test is run in both Approved modes of operation (<30Mbps mode and >30Mbps mode) using both 128 and 256-bit sizes.
Hardware AES CBC KAT (encrypt/decrypt)	Encryption/decryption KAT performed when module is loaded prior to any cryptographic functions. This test is run in >30Mbps mode on FPGA PAI Accelerator using both 128 and 256-bit sizes.
SHA-256 KAT	SHA-256 KAT performed when module is loaded prior to any cryptographic functions.
HMAC-SHA-256 KAT	HMAC-SHA-256 KAT performed when module is loaded prior to any cryptographic functions.

Table 9-1 – Power-Up Self-Tests

All data output (except status information) is inhibited while the module is performing its power-up self-tests. The module only provides cryptographic functions 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 enters a critical error state and the process is halted by the operating system.

While the module is in this state, all data output is inhibited (except status information) until the CO power cycles the host device. Power cycling the host device can also be used to run power-up self-tests on demand.

9.3 Critical Functions Self-Tests

The SOLSDR NETNode Security Module performs the following critical self-tests in *Table 9-2*:

Critical Functions Test	Critical Function Tested
Key Validation Test	This test checks that the provided CRC matches the CRC of a corresponding key value.

Table 9-2 – Critical Functions Self-Tests

If the critical function test fails, 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. The module will remain in the soft error state until valid keys are passed as a parameter into the module.

9.4 Reconfiguration from One Approved Mode to Another

When the security module is reconfigured from one approved mode of operation to the other approved mode of operation, the Zynq processor device (that hosts the module) re-boots and the power-up self-tests are always performed as part of the reconfiguration process.

10. Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any other attacks.

11. Secure Operation

11.1 Introduction

The SOLSDR NETNode Security 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.

11.2 Crypto Officer Guidance

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

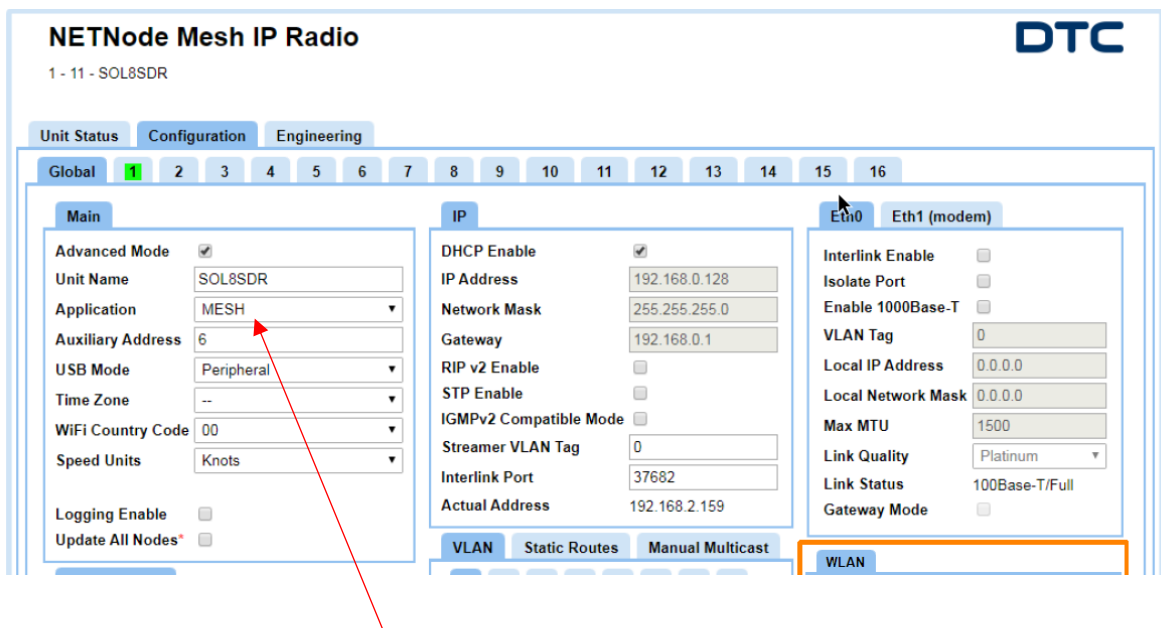
11.2.1 Initial Setup

The SOLSDR NETNode Security Module executes in the DTC NETNode IP Mesh Radios and SOL8SDR Radios only when placed in Mesh operation mode using the Web GUI Configuration. It is the Crypto Officer's responsibility to configure the device(s) to utilize the SOLSDR NETNode Security Module. This is achieved by selecting either AES128 or AES256 encryption via the user interfaces as shown below.

This document assumes that the Crypto Officer has performed initial setup of the DTC IP Mesh Radio (e.g. antennas and data connection setup, initial configuration, configuring radio talkback and GPS settings). This document also assumes that the radio has been mounted appropriately.

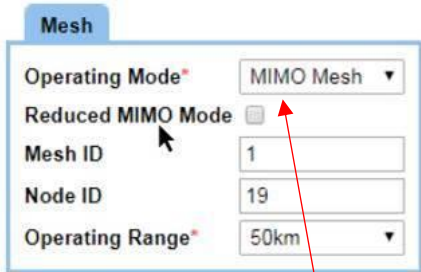
To configure the use of the SOLSDR NETNode Security Module FIPS mode, follow the steps below:

1. Power on the module
2. Approximate 30 seconds waiting period for Operating Environment/FPGA to boot
3. If the FIPS power up self-tests pass the Web GUI will be accessible and unit can be configured into either of the approved FIPS modes
4. The unit must first be configured to Mesh mode via the Web GUI Configuration > Global tab



The application must be set to MESH.

- Configuring into either the Firmware only or the Hardware Accelerated FIPS mode is performed by selecting the Mesh Operating mode via the Web Interface. The configuration is selected via the Configuration > Mesh Tab in the Web GUI.



Property	Range	Description
Operating Mode	Single Mesh MIMO Mesh MeshUltra	<p>MIMO Mesh will double the data rate over Single Mesh.</p> <p>Note: Please ensure MIMO antennas are used in MIMO Mesh modes.</p> <p>MeshUltra is dedicated to the Mesh network and will not encode video. Bandwidths up to 20MHz are possible. Refer to <i>Section 4.12</i>.</p> <p>For information on data rates, please read <i>Sections 5.4</i>.</p>

By selecting the appropriate Mesh Operating mode, either the hardware accelerated or the Firmware-only approved mode of operation operates within the security module (Standard Mesh mode and MIMO20 mode utilise the security module in firmware only mode, whilst Mesh Ultra mode utilise the security module in hardware accelerator mode).

- The unit module automatically configures into the last known operating state unless commanded to change the mode. If the mode is changed then the FPGA reboots, as part of the mode change.
- The AES128 or AES256 selection is made via either web or serial command API calls

11.2.2 Management

The Crypto Officer is responsible for ensuring that the module is running in FIPS-approved mode of operation.

11.2.3 Zeroization

The CO can manually zeroize keys and CSPs used by commanding the host FPGA device to cycle its power. When power is lost all material in RAM is zeroized immediately.

11.2.4 Module Secure Delivery

The module will be delivered as part of the embedded firmware within the product. There is no ability for the Crypto Officer or the User to access or upgrade the module independently from the entire product.

11.3 User Guidance

The SOLSDR NETNode Security Module is designed for use by the DTC 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 4-2*. The User is responsible for reporting to the CO if any irregular activity is noticed.

12. Appendix A – Acronyms

The following table provides a list of acronyms used in this document. It does not serve as a glossary of terms.

Acronym	Definition
ACP	Zynq Accelerator Coherency Port
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
CCCS	Canadian Centre for Cyber Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DDR	Double Data Rate
DES	Data Encryption Standard
DTC	Domo Tactical Communications
ECB	Electronic Code Book
EDC	Error Detection Code
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
IV	Initialization Vector

Acronym	Definition
KAT	Known Answer Test
LAN	Local Area Network
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input Multiple Output
NIST	National Institute of Standards and Technology
PAI	Programmable Algorithmic Implementation
PCB	Printed Circuit Board
PS	Processing System
PL	Programmable Logic
RAM	Random-Access Memory
RF	Radio Frequency
RX	Receiver
OS	Operating System
RF	Radio Frequency
SRAM	Synchronous Random-Access Memory
SHA	Secure Hash Algorithm
SoC	System on a Chip
TX	Transmitter
TX/RX	Transmitter/Receiver
USB	Universal Serial Bus

Table 12-1 – Acronym List