# iPASOLINK AES MODEM Card （MODEM-AEH） Security Policy

FIPS 140-2 Security Level: 2

Document Number: GVT-029406-001

Document Version: 01.46

Revision Date: Sep. 11th, 2017

NEC Corporation

http://www.nec.com

# Table of Contents

# 1 INTRODUCTION

## 1.1 PURPOSE

This is a non-proprietary Cryptographic Module Security Policy for the iPASOLINK AES MODEM Card (MODEM-AEH) module from NEC Corporation. This Security Policy describes how the module meets the security requirements of Federal Information Processing Standards (FIPS 140-2) 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 (CSE) 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 140-2-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

The following is a target cryptographic module.

Module Name: iPASOLINK AES MODEM Card (MODEM-AEH)

Table 1-1 Description of Target Cryptographic Module

| Module Code | Type | FIPS 140-2 Compliance | Remark |
|---|---|---|---|
| NWA-086220 | 004 | Level-2 | |

## 1.2 REFERENCES

This document deals only with operations and capabilities of the AES MODEM Card module in the technical terms of a FIPS 140-2 cryptographic module security policy. For more information, please contact NEC Corporation.

.

# 2 iPASOLINK AES MODEM Card SECURITY POLICY

## 2.1 MODULE OVERVIEW

iPASOLINK is NEC's most advanced and comprehensive optical and radio converged transport product family, providing solution for backhaul optimization and transformation to help you achieve your business objectives such as cost efficient integration of both TDM and carrier-class Ethernet network and versatile and smooth migration from TDM to IP next generation network.

The traffic interface of iPASOLINK is a basic Drop and Insert interface card and has up to two front access universal card slots which are connected to TDM cross connect interfaces and packet switch interfaces with interface buses. These card slots are provided for radio interface (AES MODEM Card module) and additional interface to satisfy various D/I or interface and topology requirements.

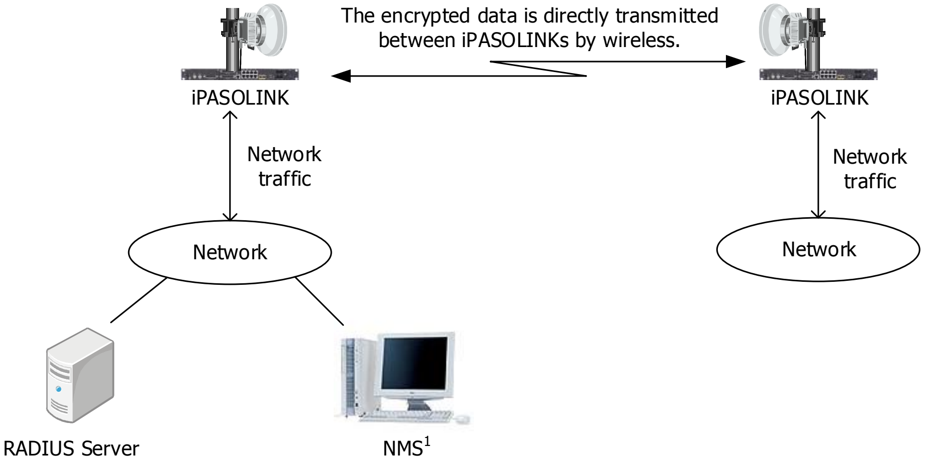

Figure 2-1 iPASOLINK System

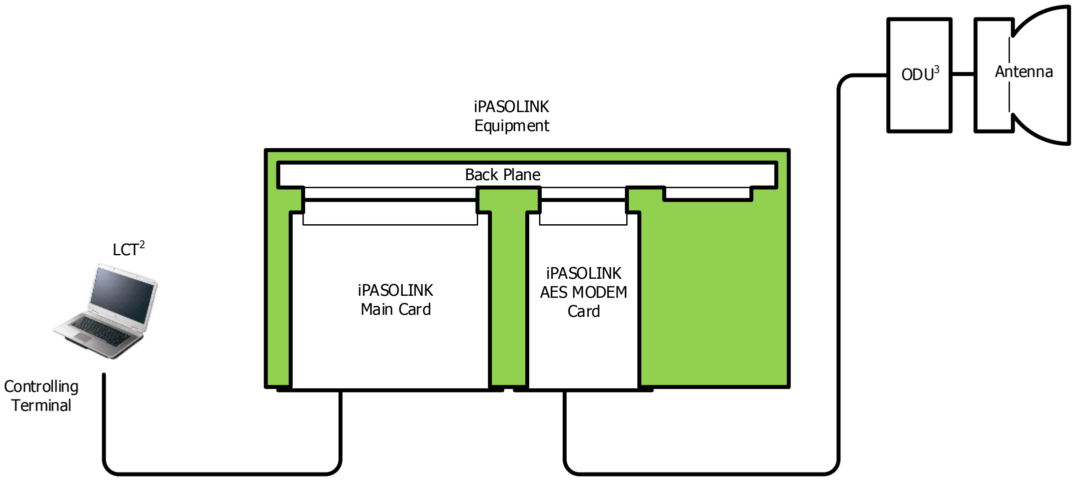

Figure 2-2 IPASOLINK Standard composition

[1] NMS - Network Management System

[2] LCT - Local Craft Terminal

[3] ODU - Out Door Units

iPASOLINK can provide the functionality of AES[4] cipher transceiver of radio data as security function. The standard composition of iPASOLINK for the security function consists of AES MODEM Card module, iPASOLINK Main Card (Main Card), Antenna and ODU.

The network traffic is forwarded to the module through the Main Card. The module encrypts and modulates the network traffic. The traffic encrypted and modulated by the module is transmitted to another iPASOLINK through ODU/Antenna.

To the contrary, the encrypted traffic that the ODU/Antenna received is forwarded to the module. The module decrypts and demodulates the traffic. The traffic decrypted by the module is transmitted to the Main Card.

The LCT is connected to the Main Card. An operator can control the functionality of AES cipher transceiver implemented in the module using LCT.

An AES cryptographic key is not generated in the module but in the Main Card.

[4] AES - Advanced Encryption Standard

## 2.2 MODULE SPECIFICATION

The AES MODEM Card module is a hardware module with a multi-chip embedded embodiment. The overall security level of the module is 2. The cryptographic boundary of the module is defined by all the hardware components which are mounted on printed circuit board, including front cover and printed circuit board. The Figures 2-3 to 2-5 depict the cryptographic module, of which Figure 2-5 provides the module's block diagram; the following components are the components of the module and surrounded with red dashed lines in the Figure 2-3 and 2-4. The other components on the circuit board are explicitly excluded from the requirements of FIPS 140-2 as they are non-security relevant and have no impact on the overall security of the module.

- FPGA
- Two Flash Memories
- CPLD
- EEPROM
- Crystal oscillators
- BWB Connector
- Heat sink
- The screws to fix the heat sink
- FPGA firmware

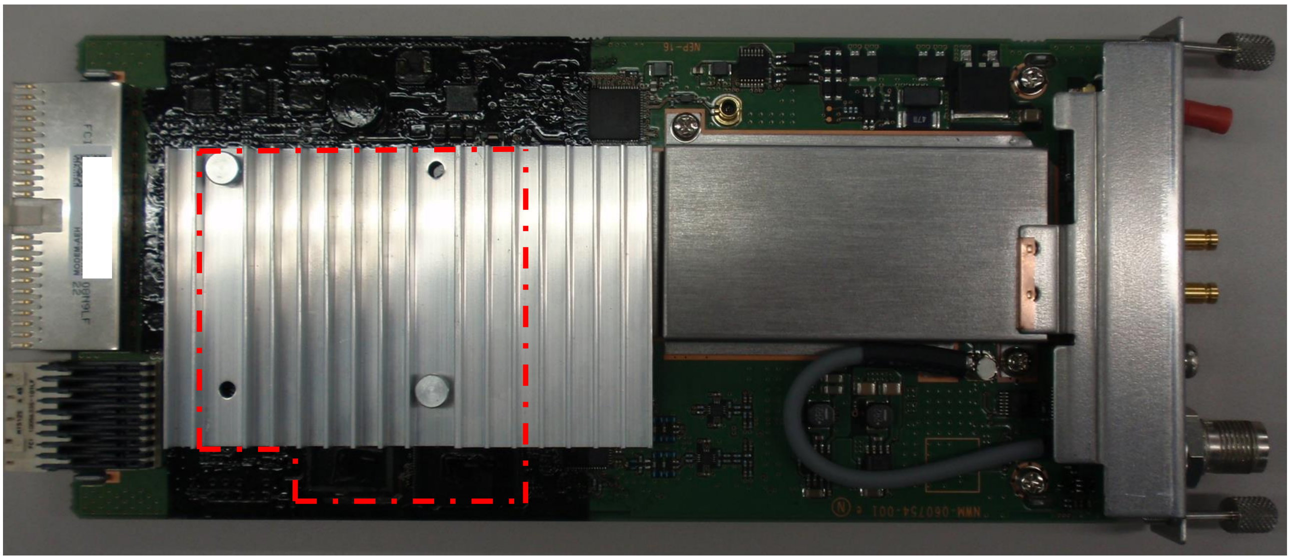

Figure 2-3 iPASOLINK AES MODEM Card Top View

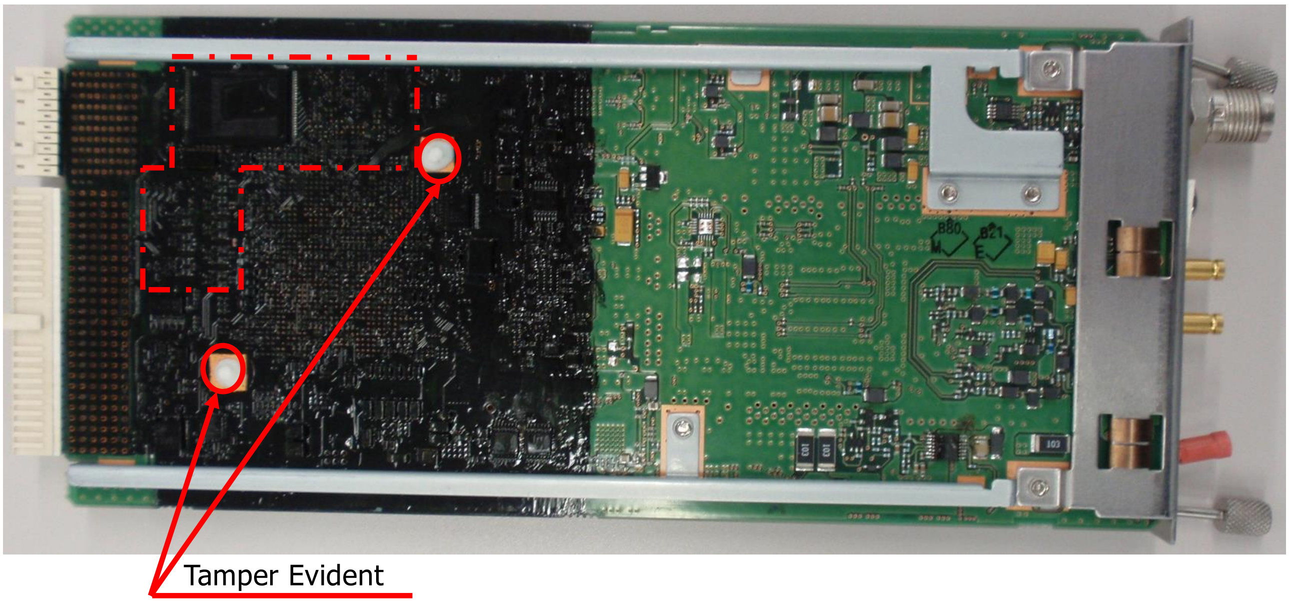

Figure 2-4 iPASOLINK AES MODEM Card Bottom View

The FPGA implements AES encryption / decryption functions, CO / User pass codes management function, modulator / demodulator functions, and control interface. The CPLD downloads the FPGA firmware to the FPGA from the flash memory when power is provided to the module. The flash memory holds the FPGA firmware. The EEPROM holds all operation parameters of the module, such as CO/User pass codes.

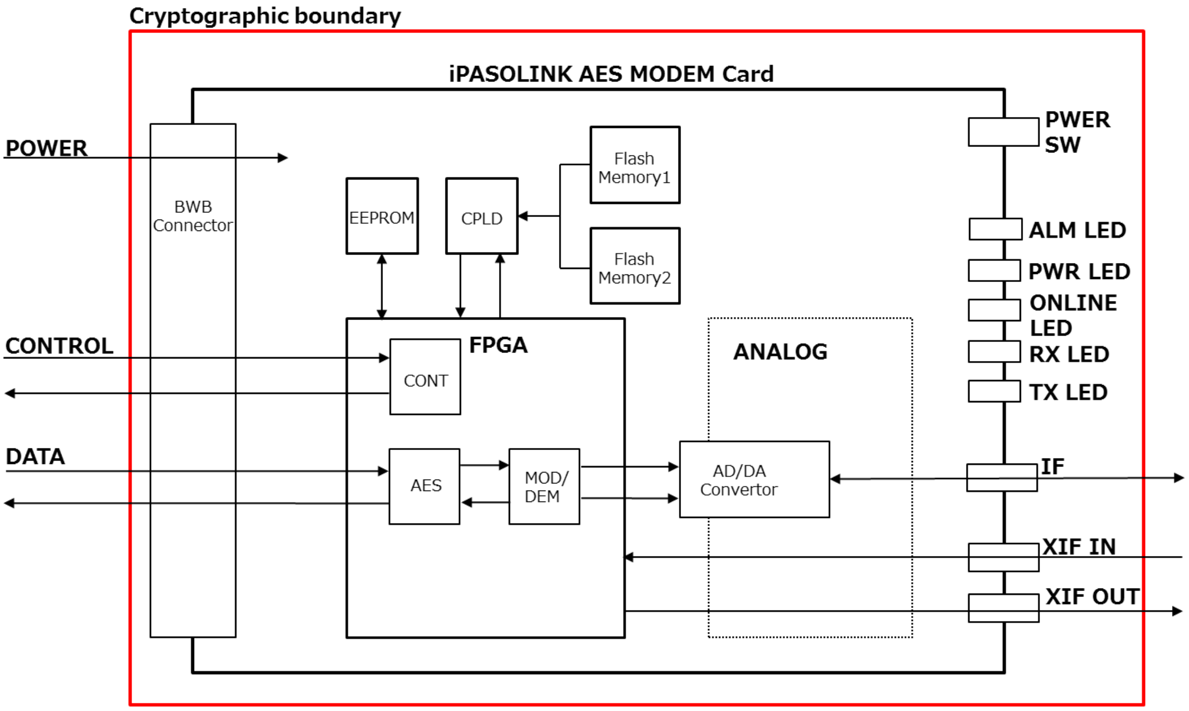

Figure 2-5 iPASOLINK AES MODEM Card Cryptographic boundary

## 2.3 PORTS AND INTERFACES

### 2.3.1 PHYSICAL PORTS

The AES MODEM Card module implements the following physical ports:

Table 2-1 FIPS 140-2 Physical Ports

| FIPS 140-2 Physical Ports | Description |
|---|---|
| IF[5] Interface Port | The IF Interface Port transmits and receives IF signals from the ODU. |
| Power Switch | The Power Switch turns the module and the ODU on or off. |
| XIF[6] Input Port | The XIF Input Port is an IF signal input port for XPIC[8]. |
| XIF Output Port | The XIF Output Port is an IF signal output port for XPIC. |
| BWB[7] Interface Port | The BWB Interface Port consists of a bidirectional data interface, control data inputs, status data outputs and power input. |
| ALM LED[9] | The ALM LED provides alarm status indications for the module. |
| PWR LED[10] | The PWR LED provides power status indications for the module. |
| ONLINE LED | The ONLINE LED provides online status indications for the module. |
| RX LED[11] | The RX LED provides status indications of data receiving. |
| TX LED[12] | The TX LED provides status indications of data transmitting. |

[5] IF Interface - Intermediate Frequency Interface

[6] XIF - XPIC Interface

[7] BWB - Back Wiring Board

[8] XPIC - Cross Polarization Interference Canceller

[9] ALM LED -Alarm Light Emitting Diode

[10] PWR LED -Power Light Emitting Diode

[11] RX LED - Receiver Light Emitting Diode

[12] TX LED - Transmitter Light Emitting Diode

### 2.3.2 LOGICAL INTERFACES

The physical ports can be mapped to the following logical interfaces defined by FIPS 140-2:

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

The AES MODEM Card module implements the following logical interfaces, which are mapped to the physical ports as indicated in Table 2-2:

Table 2-2 FIPS 140-2 Logical Interface Mappings

| FIPS 140-2 Logical Interface | Description |
|---|---|
| Data Input Interface | IF Interface Port, XIF Input Port, BWB Interface Port |
| Data Output Interface | IF Interface Port, XIF Output Port, BWB Interface Port |
| Control Input Interface | XIF Input Port, BWB Interface Port,<br>Power Switch |
| Status Output Interface | IF Interface Port, XIF Output Port, BWB Interface Port,<br>ALM LED、PWR LED、ONLINE LED、RXLED、TXLED |
| Power Interface | IF Interface Port, BWB Interface Port |

## 2.4 SECURITY LEVELS

The AES MODEM Card module meets the following security levels, as defined in FIPS140-2:

Table 2-3 Security Level per FIPS 140-2 Section

| Section | 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[13] | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

[13] EMI/EMC - Electromagnetic Interference / Electromagnetic Compatibility

## 2.5 APPROVED MODE OF OPERATION

The AES MODEM Card module implements only AES-CTR[14] mode that is the approved security function. When the power is on, the module is always in the approved mode of operation. No other mode of operation is implemented in the module.

The following manually-operated steps are required to start the approved mode of operation.

1) Turn on the iPASOLINK equipment
2) Turn on the module

In addition the module does not implement a bypass mode.

### 2.5.1 APPROVED SECURITY FUNCTION

The following approved security function is available in the approved mode of operation:

Table 2-4 FIPS 140-2 Approved Security Function

| Security Function | Purpose | Validation Certificate | Key Size |
|---|---|---|---|
| AES CTR | Encrypt or Decrypt the radio transmission signal | Advanced Encryption Standard Algorithm Validation #4546 | 128bits<br>192bits<br>256bits |

No other security function is implemented.

### 2.5.2 NON-APPROVED SECURITY FUNCTION

The AES MODEM Card module does not implement any non-approved security function.

## 2.6 OPERATORS AND ROLES

The AES MODEM Card module meets all FIPS 140-2 level 2 requirements for Roles and Services, implementing both a Crypto Officer role and a User role. The module implements role-based authentication which is accompanied by a pass code entry. Additionally, the module does not support a maintenance role or any other role.

The Crypto Officer is responsible for installing, configuring, and monitoring the module. The User role is capable of performing monitoring the module.

[14] AES-CTR - Advanced Encryption Standard Counter Mode

### 2.6.1 Crypto Officer Authentication Strength

A Crypto Officer is required to be properly authenticated by a pass code entry. A three words (96 bits) pass code shall be used for the authentication process. Since this pass code has a strength of 96 bits, the number of possible pass codes is $2^{96}$ ≒ 7.92E28. The probability that a random attempt will succeed or a false acceptance will occur is 1/(7.92E28) that is less than 1/1,000,000.

The fastest control bus supported by the AES MODEM Card module is 24.448MHz. Hence at most $24.448 \times 10^6$ bits/second x 60 seconds = 1,466,880,000 bits of data can be transmitted in one minute. The pass code is 96 bits; meaning 15,280,000 pass codes can be passed to the module (assuming no overhead) in a one minute period. Therefore, the probability of successfully authenticating to the module within one minute is $15,280,000/2^{96}$ ≒ 1/(5.18E21) that is less than 1/100,000.

### 2.6.2 User Authentication Strength

A User is required to be properly authenticated by a pass code. A two words (64 bits) pass code shall be used for the authentication process. Since this pass code has a strength of 64 bits, the number of possible pass codes is $2^{64}$ ≒ 1.84E19. The probability that a random attempt will succeed or a false acceptance will occur is 1/(1.84E19) that is less than 1/1,000,000.

The fastest control bus supported by the AES MODEM Card module is 24.448MHz. Hence at most $24.448 \times 10^6$ bits/second x 60 seconds = 1,466,880,000 bits of data can be transmitted in one minute. The pass code is 64 bits; meaning 22,920,000 pass codes can be passed to the module (assuming no overhead) in a one minute period. Therefore, the probability of successfully authenticating to the module within one minute is $22,920,000/2^{64}$ ≒ 1/(8.04E11) that is less than 1/100,000.

## 2.7 SELF TESTS

The AES MODEM Card module performs power-up self-tests. In the case of any self-test failure, the module enters a critical error state and issues a critical error indication to the ALM LED and the Main Card which is the external device and illustrated in Figure 2-2. In the critical error state, the module cannot invoke any cryptographic functions.

### 2.7.1 POWER-UP SELF-TESTS

Power-up self-tests are performed automatically under the following condition:

- When power is provided to the AES MODEM Card module.

The Power-up self-tests consist of the following tests:

- Cryptographic algorithm tests using known answer tests of AES-CTR encrypt and decrypt
- Firmware integrity tests of FPGA firmware

### 2.7.2 ON-DEMMAND SELF-TESTS

On-demand self-tests are performed automatically under the following condition:

- When power is provided to the AES MODEM Card module.

On-demand self-tests consist of the following tests:

- Cryptographic algorithm tests using known answer tests of AES-CTR encrypt and decrypt
- Firmware integrity tests of FPGA firmware

## 2.8 SERVICES

Table 2-5 presents the mapping between the services and the roles.

Setting method of keys and CSPs is indicated in 2.8.1

Table 2-5 Summary of Roles and Services (1/2)

| Role | Services | Description |
|---|---|---|
| Crypto Officer (CO) | Set common key | Setting a common key for AES-CTR encryption<br>Setting a common key for AES-CTR decryption |
| | Set pre-shared key | Setting a pre-shared key for AES-CTR encryption<br>Setting a pre-shared key for AES-CTR decryption |
| | Set AES-CTR default counter value[15] | Setting a default counter value |
| | Monitor common key | Monitoring a common key for AES-CTR encryption<br>Monitoring a common key for AES-CTR decryption |
| | Monitor pre-shared key | Monitoring a pre-shared key for AES-CTR encryption<br>Monitoring a pre-shared key for AES-CTR decryption |
| | Monitor AES-CTR default counter value | Monitoring a default counter value |
| | Change Crypto Officer pass code | Changing the current Crypto Officer pass code |
| | Set AES key size | Setting the key size (128bit, 192bit and 256bit) of the common key and pre-shared key |
| User | Monitor common key | Monitoring a common key for AES-CTR encryption<br>Monitoring a common key for AES-CTR decryption |
| | Monitor pre-shared key | Monitoring a pre-shared key for AES-CTR encryption<br>Monitoring a pre-shared key for AES-CTR decryption |
| | Monitor AES-CTR default counter value | Monitoring a default counter value |
| | Change User pass code | Changing the current User pass code |

[15] AES-CTR default counter value - Default counter value for Advanced Encryption Standard Counter Mode

Table 2-5 Summary of Roles and Services (2/2)

| Role | Services | Description |
|---|---|---|
| no authentication required | On-demand self-test | Performing the self-test for checking the AES-CTR operation |
| | Zeroization of CSPs | Zeroization of CSPs other than CO/User pass codes |
| | Crypt Officer authentication | Authenticating of the Crypt Officer |
| | User authentication | Authenticating of the User |
| | AES-CTR encryption | AES-CTR encrypts user data. Radio transmits the encrypted data. |
| | AES-CTR decryption | AES-CTR decrypts user data. Decrypt encrypted radio transmissions data. |
| | Security status monitor | Monitoring the AES-CTR operation status via LED indication and status output |
| | Transmission status monitor | Monitoring the radio transmission status and the module status via LED indication and status output |
| | Radio control | Setting of radio transmission parameter |
| | Modulation and demodulation | User data modulation and demodulation for radio transmission |
| | Analog-digital and digital-analog | User data analog-digital and digital-analog conversion for radio transmission |
| | XPIC modulation and demodulation | User data modulation and demodulation for radio transmission by XPIC mode |
| | Power supply | Supply power through iPASOLINK PS Card[16] to the AES MODEM Card module and ODU.<br>Implement DC-DC converter[17]. |

### 2.8.1 SETTING OF KEYS AND CSPs

All keys and CSPs (common keys, pre-shared keys and AES-CTR default counter value and CO/User pass codes shown in Table 2-6 in Section 2.9.1) are input to the AES MODEM Card module in plaintext from the Main Card which is the external device and illustrated in Figure 2-2.

The Crypto Officer role authentication is required to input all keys and CSPs except for the User pass code. Also, the User role authentication is required to input the User pass code.

All keys and CSPs except for CO/User pass codes are written in a volatile memory inside the module. The CO/User pass codes are written in an EEPROM inside the module.

[16] PS Card – Power Supply Card

[17] DC-DC converter – Direct Current to Direct Current converter

## 2.9 KEYS AND CRITICAL SECURITY PARAMETERS

### 2.9.1 DEFINED KEYS AND CSPs

The AES MODEM Card module supports the following Keys and Critical Security Parameters (CSPs). The module can register four kinds of keys; a common key for encryption, a common key for decryption, a pre-shared key for encryption and a pre-shared key for decryption. The common key is used to encrypt or decrypt the radio transmission data. The pre-shared key is used to the first key exchange. The CO/User pass codes are used for operator authentication in the module.

Table 2-6 Keys used by iPASOLINK AES MODEM Card (1/2)

| CSP | Purpose | Input | Output | Storage | Zeroization |
|---|---|---|---|---|---|
| AES-CTR encrypt key (common key) | A common key used to encrypt the radio transmission signal. | Externally generated and input | Output by the CO/User role after the two independent internal actions | Volatile memory within the FPGA | Turning–off or resetting the module |
| AES-CTR decrypt key (common key) | A common key used to decrypt the radio transmission signal. | Externally generated and input | Output by the CO/User role after the two independent internal actions | Volatile memory within the FPGA | Turning-off or resetting the module |
| AES-CTR encrypt key (pre-shared key) | A pre-shared key used to encrypt the radio transmission for pre-shared key-exchange. | Externally generated and input | Output by the CO/User role after the two independent internal actions | Volatile memory within the FPGA | Turning-off or resetting the module |
| AES-CTR decrypt key (pre-shared key) | A pre-shared key used to decrypt the radio transmission for pre-shared key-exchange. | Externally generated and input | Output by the CO/User role after the two independent internal actions | Volatile memory within the FPGA | Turning-off or resetting the module |

Table 2-6 Keys used by iPASOLINK AES MODEM Card (2/2)

| CSP | Purpose | Input | Output | Storage | Zeroization |
|---|---|---|---|---|---|
| AES-CTR default counter value (including nonce and initialization vector) | AES-CTR default counter value used to AES-CTR encryption and decryption. | Externally generated and input | Output by the CO/User role after the two independent internal actions | Volatile memory within the FPGA | Turning-off or resetting the module |
| CO pass code | The Crypto Officer role authentication | Externally generated and input | N/A | Non-volatile memory EEPROM | Change Crypto Officer pass code |
| User pass code | The User role authentication | Externally generated and input | N/A | Non-volatile memory EEPROM | Change User pass code |

## 2.9.2 KEY AND CSP ACCESS

The following tables define how services access Keys and CSPs. The following terminology is used:

- R : Read, the AES MODEM Card module uses the CSP without modifying it.
- W : Write, the module modifies or deletes the CSP.

Table 2-7 Key and CSP Access (CO)

| Services | AES-CTR encrypt key (common key) | AES-CTR encrypt key (pre-shared key) | AES-CTR decrypt key (common key) | AES-CTR decrypt key (pre-shared key) | AES-CTR default counter value | CO pass code | User pass code |
|---|---|---|---|---|---|---|---|
| Set common key | W | - | W | - | - | - | - |
| Set pre-shared key | - | W | - | W | - | - | - |
| Set AES-CTR default counter value | - | - | - | - | W | - | - |
| Monitor common key | R | - | R | - | - | - | - |
| Monitor pre-shared key | - | R | - | R | - | - | - |
| Monitor AES-CTR default counter value | - | - | - | - | R | - | - |
| Change Crypto Officer pass code | - | - | - | - | - | W | - |
| Set AES key size | - | - | - | - | - | - | - |

Table 2-8 Key and CSP Access (User)

| Services | AES-CTR encrypt key (common key) | AES-CTR encrypt key (pre-shared key) | AES-CTR decrypt key (common key) | AES-CTR decrypt key (pre-shared key) | AES-CTR default counter value | CO pass code | User pass code |
|---|---|---|---|---|---|---|---|
| Monitor common key | R | - | R | - | - | - | - |
| Monitor pre-shared key | - | R | - | R | - | - | - |
| Monitor AES-CTR default counter value | - | - | - | - | R | - | - |
| Change User pass code | - | - | - | - | - | - | W |

Table 2-9 Key and CSP Access (no authentication required)

| Services | AES-CTR encrypt key (common key) | AES-CTR encrypt key (pre-shared key) | AES-CTR decrypt key (common key) | AES-CTR decrypt key (pre-shared key) | AES-CTR default counter value | CO pass code | User pass code |
|---|---|---|---|---|---|---|---|
| On-demand self-test | - | - | - | - | - | - | - |
| Zeroization of CSPs | W | W | W | W | W | - | - |
| Crypt Officer authentication | - | - | - | - | - | R | - |
| User authentication | - | - | - | - | - | - | R |
| AES-CTR encryption | R | R | - | - | R | - | - |
| AES-CTR decryption | - | - | R | R | R | - | - |
| Security status monitor | - | - | - | - | - | - | - |
| Transmission status monitor | - | - | - | - | - | - | - |
| Radio control | - | - | - | - | - | - | - |
| Modulation and demodulation | - | - | - | - | - | - | - |
| Analog-digital and digital-analog | - | - | - | - | - | - | - |
| XPIC modulation and demodulation | - | - | - | - | - | - | - |
| Power supply | - | - | - | - | - | - | - |

## 2.10 ZEROIZATION

Since all CSPs except for the CO/User pass codes are stored in a volatile memory within the FPGA, they are zeroized by turning off or resetting the AES MODEM Card module. Whereas the CO/User pass codes are stored in a non-volatile memory EEPROM and zeroized by a pass code change service with all zero pass code, that is, setting all zero value in the "Change Crypto Officer pass code" or "Change User pass code" service.

Please refer to section-2.9.1.

## 2.11 PHYSICAL SECURITY AND MITIGATION OF OTHER ATTACKS

The AES MODEM Card module is a multi-chip embedded cryptographic module which utilizes production-grade components with standard passivation techniques. All security-related components are covered by either a heat sink (fixed by the screws with tamper evident) or conformal coating. Removing the heat sink by an attack, it needs to break the tamper evident on the screws that fix the heat sink on the module. The tamper-evident conformal coating covers all security-related components. Attacking these components, it need to remove the coating. Please refer to section-2.2. The module was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2. Therefore, the section; Mitigation of Other Attacks, is not applicable.

# 3 USER GUIDANCE

## 3.1 PORTS, INTERFACES AND SERVICES

The following ports, interfaces and services are available to the User role of the AES MODEM Card module.

- Physical Ports as described in section-2.3.1
  BWB Interface Port
- Logical Interfaces as described in section -2.3.2
  Control Input Interface (BWB Interface port)
  Status Output Interface (BWB Interface port)
- Services permitted to the User role as described in section -2.8

## 3.2 USER RESPONSIBILITIES

The User must not peel away the tamper-evident conformal coating on the circuit board or break the tamper-evident on the screws that fix the heat sink on the AES MODEM Card module.

# 4 CRYPTO OFFICER (CO) GUIDANCE

## 4.1 PORTS, INTERFACES AND SERVICES

The following ports, interfaces and services are available to the Crypto Officer of the AES MODEM Card module.

- Physical Ports as described in section-2.3.1
  BWB Interface Port
- Logical Interfaces as described in section-2.3.2
  Control Input Interface (BWB Interface port)
  Status Output Interface (BWB Interface port)
- Services permitted to the Crypto Officer role as described in section-2.8

## 4.2 MODULE INSTALLATION AND STARTUP

The Crypto Officer is required to periodically inspect the tamper evident on the screws that fix the heat sink and on the conformal coating.

The Crypto Officer has to install the AES MODEM Card module into the iPASOLINK equipment before starting up of the module. Therefore, the Crypto Officer must check the appropriate guidelines for ESD[18].

For further Crypto Officer actions required to startup the iPASOLINK equipment, please refer to the iPASOLINK manual.

[18] ESD - Electro Static Discharge

## 4.3 MODULE INITIALIZATION

The AES MODEM Card module is initialized with one of the following methods.

- Resetting the module
- Ejecting the module from the iPASOLINK equipment
- Switching off the module

# 5 Revision History

| Date | Revision | Description |
|---|---|---|
| Feb. 10, 2017 | 01.00 | Initial release. |
| Mar. 30, 2017 | 01.10 | Correction |
| Apr. 10, 2017 | 01.11 | Correction |
| Apr. 28, 2017 | 01.12 | Correction |
| June. 6, 2017 | 01.20 | Correction |
| June. 19, 2017 | 01.30 | Correction |
| June. 21, 2017 | 01.40 | Correction |
| June. 26, 2017 | 01.41 | Correction |
| June. 28, 2017 | 01.42 | Correction |
| Aug. 29, 2017 | 01.43 | Correction |
| Sep. 5, 2017 | 01.44 | Correction |
| Sep. 6, 2017 | 01.45 | Correction |
| Sep.11, 2017 | 01.46 | Correction |

\Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create
the ICT-enabled society of tomorrow.
We collaborate closely with partners and customers around the world,
orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to
greater safety, security, efficiency and equality,
and enable people to live brighter lives.