iPASOLINK MODEM AES Card Security Policy

FIPS Security Level: 1

Document Number: NWD-131165-001

Document Version: 01.01

Revision Date: Mar. 13, 2012

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 MODEM AES Card (MODEM Card) from NEC Corporation. This Security Policy describes how the MODEM Card 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 following is a target cryptographic module.

Module Name: iPASOLINK MODEM AES Card
Version Number of the Module: NWA-055300-004, 5.00
Firmware Code of the Module: NWA-055300-004
Hardware Code of the Module: 5.00

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. For more information, please contact NEC Corporation.

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

2 iPASOLINK MODEM AES 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 optimisation 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 four (4) 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 (MODEM Card) and additional interface to satisfy various D/I or interface and topology requirements.

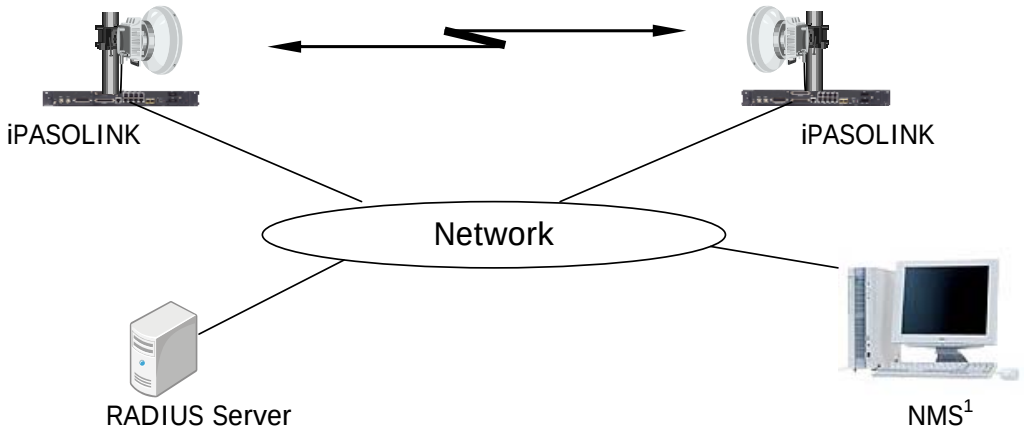

Figure 2-1 iPASOLINK System

[1]NMS - Network Management System

iPASOLINK can provide the functionality of AES[3] cipher transceiver of radio data as security function. The standard composition of iPASOLINK for the security function consists of MODEM Card, iPASOLINK Main Card (Main Card), Antenna and ODU.

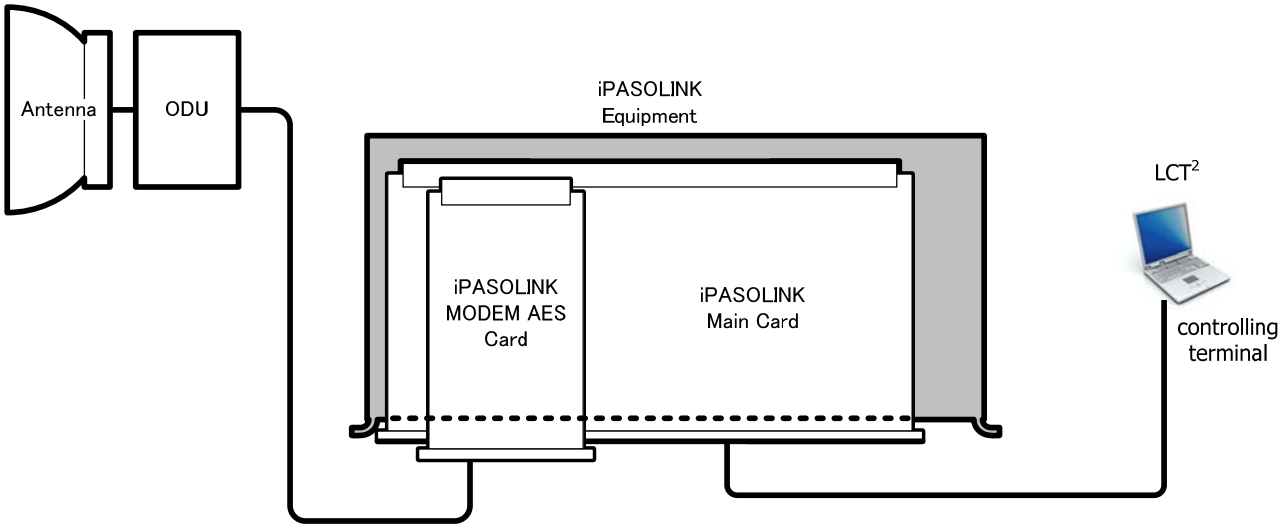

Figure 2-2 IPASOLINK Standard composition

User data is forwarded to MODEM Card through Main Card. MODEM Card processes encryption of user data and modulation of transmission signal. Encrypted data is transmitted through ODU[4]/Antenna.

To the contrary, the cipher data that ODU/Antenna received is forwarded to MODEM Card. MODEM Card processes decryption of cipher data and demodulation of transmission signal. Decrypted data is processed in Main Card as user data.

iPASOLINK Main Card is connected with LCT[2]. An operator can control the functionality of AES cipher transceiver to MODEM Card using LCT.

A key for AES cipher is generated in Main Card. Key exchange control is implemented in the Main card. Therefore a MODEM Card doesn't generate a key.

[2]LCT - Local Craft Terminal

[3]AES - Advanced Encryption Standard

[4]ODU - Out Door Units

2.2 MODULE SPECIFICATION

The MODEM Card is a hardware module with a multi-chip embedded embodiment. The overall security level of the module is 1. The cryptographic boundary of the MODEM Card is defined by all the hardware components which are mounted on printed circuit board, including Front cover and printed circuit board. The top and front of the MODEM Card images are shown in Figure 2-3 and Figure 2-4 below.

Figure 2-3 iPASOLINK MODEM AES Card Top View

Figure 2-4 iPASOLINK MODEM AES Card Front View

The Cryptographic Module consists of FPGA, Analog components, LEDs, Power control components and other components. The FPGA implements AES encryption / decryption functions, Modulator / Demodulator functions, and Control Interface. The Analog components implements Analog / digital conversion functions and Intermediate Frequency Processing.

A block diagram of The Cryptographic Module and cryptographic boundary is shown in Figure 2-5.

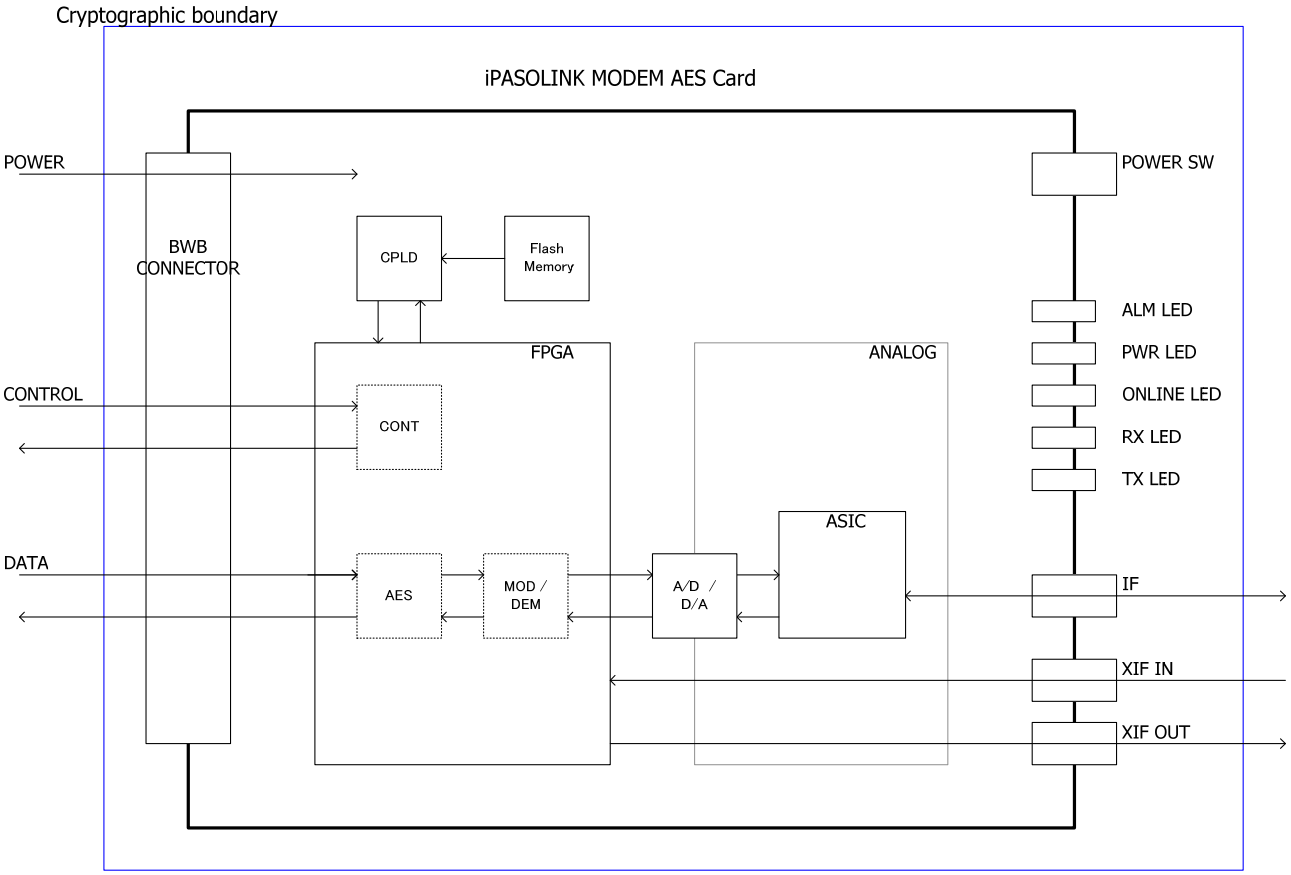

Figure 2-5 iPASOLINK MODEM AES Card Cryptographic boundary

2.3 PORTS AND INTERFACES

2.3.1 PHYSICAL PORTS

The MODEM Card FIPS140-2 Cryptographic Module implements the following physical ports:

Table 2-1 FIPS 140-2 Physical Ports

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

[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 categorized into the following logical interfaces defined by FIPS 140-2:

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

The MODEM Card FIPS140-2 Cryptographic Module implements the following logical interfaces, which map to the physical ports as indicated:

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	IF Interface port, XIF Input port, BWB Interface port, Power Switch
Status Output Interface	IF Interface port, XIF Output port, BWB Interface port, ALM LED、PWR LED、ONLINE LED、RXLED、TXLED
Power Interface	IF Interface port, BWB Interface port

2.4 SECURITY LEVELS

The MODEM Card FIPS140-2 Cryptographic 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	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[12]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

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

2.5 APPROVED MODE OF OPERATION

The mode using the AES-CTR[13] algorithm (AES-CTR algorithm is an approved security function by FIPS140-2) is FIPS approved mode.

The following manually-operated steps before the start FIPS approved mode.
The modem settings are made automatically by power supply on.

1) Turn on the iPASOLINK equipment.
2) Turn on the MODEM Card.
3) Operate AES Encryption processing using LCT.

In addition the MODEM Card FIPS140-2 Cryptographic Module does not implement bypass mode.

2.5.1 APPROVED SECURITY FUNCTION

The following approved security function is used in FIPS approved mode:

Table 2-4 FIPS 140-2 Approved Security Function

Security Function	Purpose	Validation Certificate
AES CTR	Encrypt or Decrypt the radio transmission signal	Advanced Encryption Standard Algorithm Validation No.1834

2.5.2 NON-APPROVED SECURITY FUNCTION

The MODEM Card FIPS140-2 Cryptographic Module does not implement the non-approved security function.

2.6 OPERATORS AND ROLES

The MODEM Card FIPS140-2 Cryptographic Module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both a Crypto Officer role and a User role. As the MODEM Card is a level 1 module, role-based authentication is not supported. An operator implicitly assumes the role of either Crypto Officer or User by selecting a service associated with that role. No authentication is performed. Additionally, the module does not support a Maintenance role or any other role.

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

2.7 SELF TESTS

The MODEM Card FIPS140-2 Cryptographic 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 on the LCT and ALM LED. In the critical error state, the module can not invoke any cryptographic functions and must be ejected from the iPASOLINK equipment. (The MODEM card is turned off by ejecting.) The MODEM card must be repaired as broken module.

2.7.1 POWER-UP SELF-TESTS

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

- When turn on the MODEM Card using power switch.
- When reset operation to the MODEM Card.

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

- Cryptographic algorithm tests using known answer tests of AES CTR Encrypt
- Firmware integrity tests of FPGA configuration data

2.8 SERVICES

A relation about services to each role in this module is indicated in Table 2-5.

Setting method of keys and CSPs is indicated in 2.8.1

Table 2-5 Summary of Roles and Services

Role	Services	Description	Security
Crypto Officer (CO)	Set AES Encrypt / Decrypt start-up	Setting the start-up and shutdown AES encryption Setting the start-up and shutdown AES decryption The start-up or shutdown trigger FIPS approved mode of operation.	○
	Set common key	Setting a common key for AES-CTR Encryption Setting a common key for AES-CTR Decryption	○
	Set pre-shared key	Setting a pre-shared key for AES-CTR Encryption Setting a pre-shared key for AES-CTR Decryption	○
	Set AES-CTR Default Counter[16] Value	Setting the Default Counter Value for AES-CTR Encryption Setting the Default Counter Value for AES-CTR Decryption	○
	On-demand self-test	Operate the self-test. Operating conditions are as follows: ・ Reset operation to the MODEM Card ・ Turn-on after turn-off MODEM Card	○
	Zeroize CSP	Operate the zeroize CSP Operating conditions are as follows: ・ Reset operation to the MODEM Card	○
User	AES-CTR Encryption	AES CTR Encrypt user data. Radio transmits the encrypted data.	○
	AES-CTR Decryption	AES CTR Decrypt user data. Decrypt encrypted radio transmissions data.	○
	Security status output	Notify iPASOLINK Main Card of information related to State of the cryptographic module security. Indicate the State of the cryptographic module	○

Role	Services	Description	Security
		security to ALM LED.	
	Power supply	Supply power through iPASOLINK PS[16] Card to MODEM Card and ODU. Implement DC-DC converter[15].	○

2.8.1 SETTING OF KEYS AND CSPs

All keys and CSPs (common keys, pre-shared keys and AES-CTR Default Counter Value) shown in Table 2-6 in Section 2.9.1, are generated by the Main Card which is the external device for the MODEM Card, illustrated in Figure 2-2.

When Crypto Officer executes AES Encryption function using LCT connected with iPASOLINK equipment as shown in Figure 2-2, all keys and CSPs are input to the MODEM Card in plain text through the Main Card.

All keys and CSPs are written in a volatile memory inside the MODEM Card, and used for AES cipher transceiver.

[15]DC-DC converter – direct current to direct current converter

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

2.9 KEYS AND CRITICAL SECURITY PARAMETERS

2.9.1 DEFINED KEYS AND CSPs

The MODEM Card FIPS140-2 Cryptographic Module supports the following Keys and Critical Security Parameters (CSPs).

The MODEM Card can register each 2 kinds of key for encryption and decryption. Common key is used to cryptographic communication. Pre-shared key is used to the first key exchange.

Table 2-6 Keys used by iPASOLINK MODEM AES Card

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	N/A	Volatile memory within the FPGA	Resetting MODEM Card
AES-CTR Decrypt Key (Common Key)	A common key used to decrypt the radio transmission signal.	Externally generated and input	N/A	Volatile memory within the FPGA	Resetting MODEM Card
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	N/A	Volatile memory within the FPGA	Resetting MODEM Card
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	N/A	Volatile memory within the FPGA	Resetting MODEM Card
AES-CTR Default Counter Value (Including Nonce and Initialization Vector)	AES-CTR key counter Default Value used to AES-CTR Encryption and Decryption.	Externally generated and input	N/A	Volatile memory within the FPGA	Resetting MODEM Card

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 module uses the Key / CSP without modifying it.
- W : Write, the module modifies or deletes the Key / CSP.

Table 2-7 Key and CSP Access (CO)

Services	AES ENC Key[17] (common key)	AES ENC Key (Pre-Shared Key)	AES DEC Key[18] (common key)	AES DEC Key (Pre-Shared Key)	AES-CTR Default Counter
Set AES Encrypt / Decrypt start-up	W	W	W	W	W
Set common key	W	-	W	-	-
Set pre-shared key	-	W	-	W	-
Set AES-CTR Default Counter Value	-	-	-	-	W
On-demand self-test	-	-	-	-	R
Zeroize CSP	W	W	W	W	W

Table 2-8 Key and CSP Access (User)

Services	AES ENC Key (common key)	AES ENC Key (Pre-Shared Key)	AES DEC Key (common key)	AES DEC Key (Pre-Shared Key)	AES-CTR Default Counter
AES-CTR Encryption	R	R	-	-	R
AES-CTR Decryption	-	-	R	R	R
Security status output	-	-	-	-	-
Power supply	-	-	-	-	-

※Extracted the Security-related items Section2.8.

[17]AES ENC Key - Encryption Key for Advanced Encryption Standard Encryption Key

[18]AES DEC Key - Decryption Key for Advanced Decryption Standard Encryption Key

2.10 ZEROIZATION

All CSPs are themselves stored in internal volatile memory of the FPGA. All CSPs are zeroized by resetting MODEM Card. Please refer to section-2.9.1 type of CSPs.

In addition, CSPs are stored in volatile memory. Therefore, All CSPs cleared by turn-off MODEM Card though it is not a Zeroization.

2.11 PHYSICAL SECURITY AND MITIGATION OF OTHER ATTACKS

The MODEM Card FIPS140-2 Cryptographic Module is a multi-chip Embedded Cryptographic Module which utilizes production-grade components with standard passivation techniques. Because all CSPs cleared when turned off MODEM Card, the MODEM Card will not be intercepted the CSPs information by contacting the physical terminal. Because of MODEM Card is inserted into chassis of iPASOLINK equipment when turned on, the MODEM Card will not be intercepted the CSPs information by contacting the physical terminal. The module is not designed to mitigate any other specific attacks.

3 USER GUIDANCE

3.1 PORTS, INTERFACES AND SERVICES

The MODEM Card FIPS140-2 Cryptographic Module makes available to the User:

- Physical Ports as described in section-2.3.1
- Logical Interfaces as described in section -2.3.2
- Services associated with the User role as described in section -2.8

3.2 USER RESPONSIBILITIES

To ensure the module operate in the approved FIPS mode of operation the User must only invoke Services using the approved algorithms listed in section-2.5.

4 CRYPTO OFFICER (CO) GUIDANCE

4.1 PORTS, INTERFACES AND SERVICES

The MODEM Card FIPS140-2 Cryptographic Module makes available to the CO:

- Physical Ports as described in section-2.3.1
- Logical Interfaces as described in section-2.3.2
- services associated with the CO role as described in section-2.8
- security parameters described in section-2.9.1

4.2 MODULE INSTALLATION AND STARTUP

To ensure the module operates in the approved FIPS mode of operation the User must only invoke Host Services using the approved algorithms listed in section-2.5.

An operator has to install the MODEM Card into the iPASOLINK equipment to initiate module startup. Therefore, operator must check the appropriate guidelines for ESD.

Any operator actions required by the iPASOLINK equipment to initiate module startup are beyond the scope of this document.

4.3 MODULE INITIALIZATION

The MODEM Card is initialized with the following method.

- Resetting the MODEM Card
- Ejecting the MODEM Card from the iPASOLINK equipment
- Switching off the MODEM Card

5 Revision History

Date	Revision	Description
Nov. 11, 2011	01.00	Initial release.
Mar. 2, 2012	01.01	Added the name and the hardware version of the target module to section 1.1. Added “Setting of Keys and CSPs” to section 2.8.1.

Empowered by Innovation

NEC