NAL Research Corporation

XM Crypto Module
1.1.0

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 1.0

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the XM Crypto Module contained in the A3LA-XM modem, figure 1, from NAL Research Corporation. This Security Policy provides detailed non-proprietary information relating to the XM Crypto Module as it relates to FIPS 140-2 Level 1 security requirements along with instructions on setting up the module in a secure FIPS 140-2 mode.

Figure 1 - A3LA-XM Modem

2 Product Overview

The A3LA-XM, figure 1 above is a standalone modem comprised of a communication board, a SIM card and the XM crypto module running on a standalone board. The cryptographic module is designed to encrypt and decrypt data using AES-ECB 256 and the communication board is used to transmit encrypted data over a communication network. The SIM card or Subscriber Identity Module is a portable memory chip with no sensitive data stored on it and not available when the crypto module is in FIPS mode. The XM crypto module runs on an internal micro-controller/processor with RAM. This micro-controller is programmed to monitor the modem‘s connectivity status, process data as it comes into the crypto module and contains a code lock to lock down the firmware so it cannot be modified. Similar to a standard landline modem, the A3LA-XM can be controlled by any DTE (data terminal equipment) capable of sending standard AT commands via an RS232 serial or a USB 2.0 port. A DTE can be a desktop computer, a

laptop computer, a PDA, or even a micro-controller. The A3LA-XM Modem works with SMS (text message), SBD (short burst data) and phone data.

When encryption is enabled, the crypto module is in FIPS mode and the A3LA-XM modem can send data between the A3LA-XM modem and another device, figure 2. The XM crypto module works in a single user/process mode of operation. The device is set with an encryption and decryption key and will perform all cryptographic operations using this single key until a new key is entered. The A3LA-XM has been certified to MIL-STD-810F standards for temperature, humidity, altitude, rain, shock, sand, dust and salt fog.

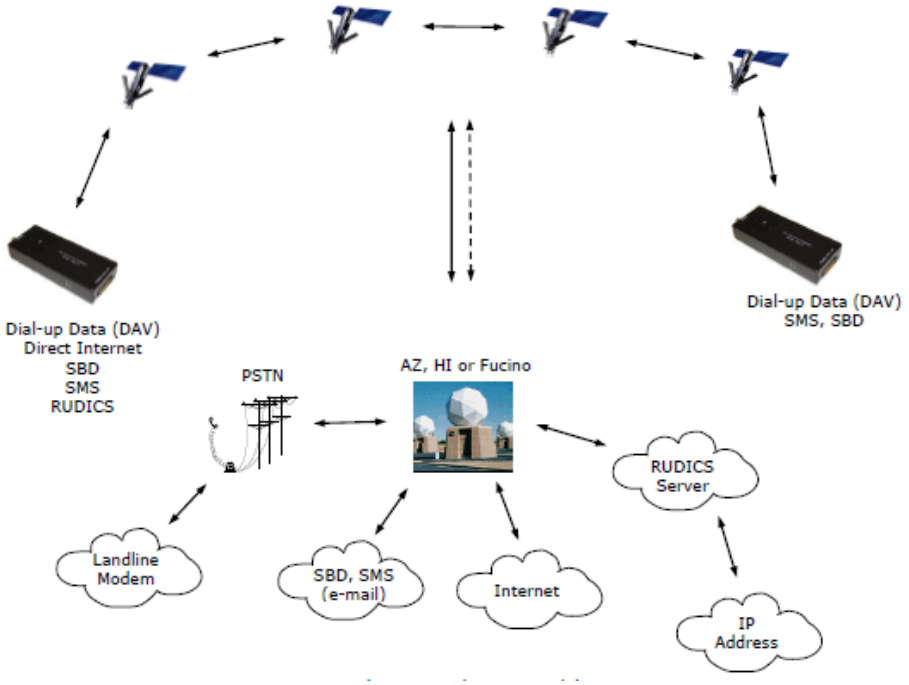

Figure 2 - A3LA-XM Network Configuration

2.1 Cryptographic Module Specification

The XM Crypto Module is a non-modifiable firmware-based cryptographic module running A3LA-XM firmware 1.1.0 with Scheduler 1.1.0 utility. The crypto module is entirely encapsulated within the cryptographic boundary indicated within red below which is further encapsulated within the physical boundary of the A3LA-XM as shown in Figure 4 below.

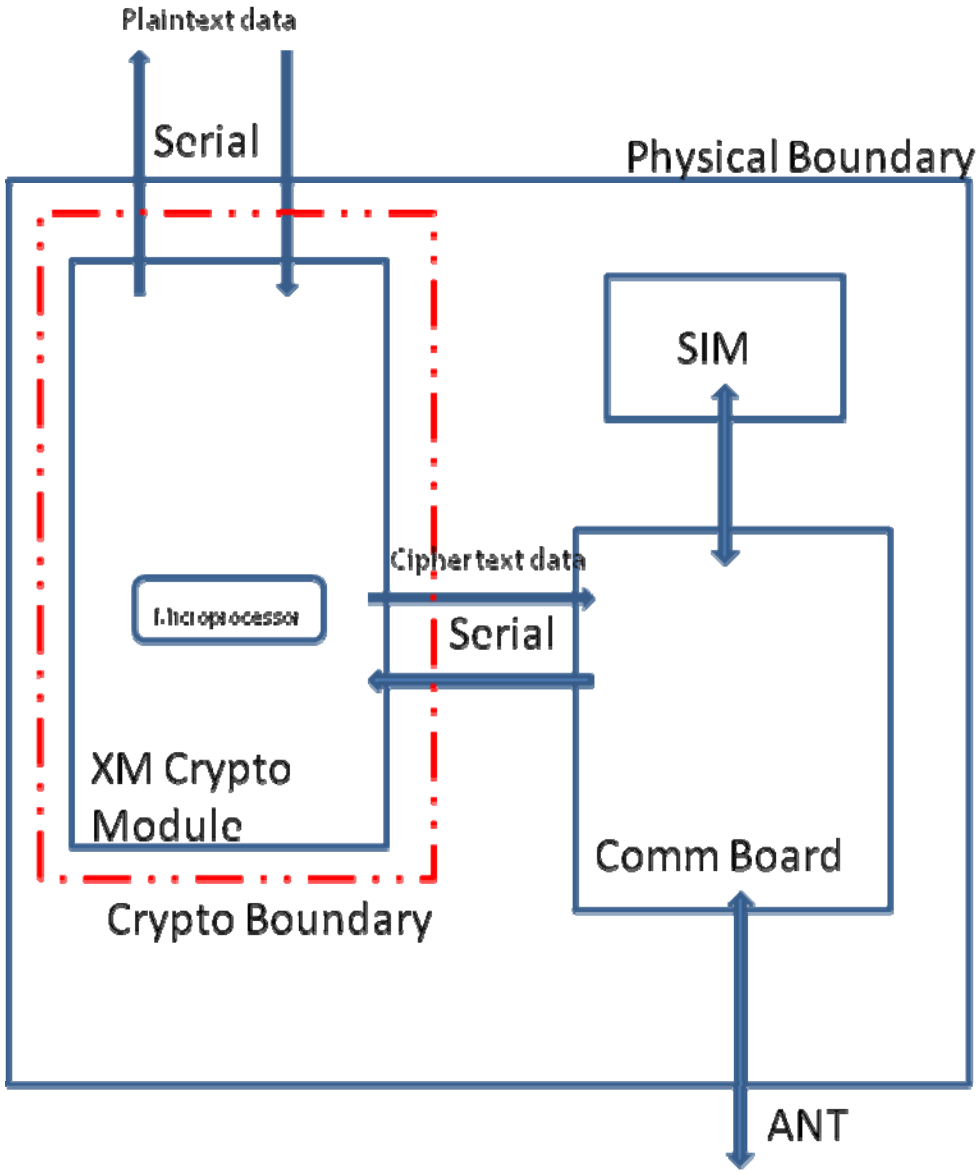

Figure 3 - Physical Block Diagram with Cryptographic Boundary

The physical device consists of a cryptographic board (Crypto Board) running the XM crypto module with a micro-processor containing RAM, a SIM card and a communication board (Comm Board). The system operates in a single user mode. The cryptographic boundary of the module is only the crypto board and everything contained on that board. The SIM card is used in the non-FIPS mode by default for storage however when FIPS is enabled the SIM card does not get used for storage. Per FIPS 140-2 terminology, the XM Crypto Module is multi-chip standalone module that meets overall level 1 FIPS 140-2 requirements. The XM Crypto Module is validated as follows:

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 1 - Security Level per FIPS 140-2 Section

2.2 Module Ports and Interfaces

The cryptographic module uses a male 25-pin miniature D-Sub type connector for a physical external serial port connection and internal serial interface between the crypto board and the comm. board. The external physical serial port is the dedicated external connection made to the A3LA-XM modem providing plaintext data input, cryptographic key input, Crypto Officer password input, power in and data output for the crypto board inside the A3LA-XM modem. All of this is handled over dedicated serial pins. Plaintext data comes into the crypto board via the external serial connection and cipher data leaves the crypto board via the internal serial data out port from the crypto board to the comm board. Ciphertext comes in to the crypto board via the internal serial connection from the comm board. The data is decrypted on the crypto board and then sent out via the external dedicated serial pin. The interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out Interface
- Data Control Interface
- Status Output Interface
- Power Interface

2.2.1 Data Input Interface

Dedicated external male 25-pin miniature D-Sub type serial connection provides a dedicated serial pin for data in. This connect is used for plaintext data input, crypto key input and Crypto Officer password.

Internal serial connection between the communication board and the crypto board within the A3LA-XM modem provides a dedicated serial pin for cipher text data into the crypto board.

2.2.2 Data out Interface

Dedicated external male 25-pin miniature D-Sub type serial connection provides a dedicated serial pin for data out. This connect is used for plaintext data out.

Internal serial connection between the communication board and the crypto board within the A3LA-XM modem providing dedicated serial pin for cipher text data out of the crypto board.

2.2.3 Data Control Interface

Dedicated external male 25-pin miniature D-Sub type serial connection provides a dedicated serial pin for control input. This connection is used for AT commands into the crypto module from external DTE (data terminal equipment).

2.2.4 Status Output Interface

Dedicated external male 25-pin miniature D-Sub type serial connection provides a dedicated serial pin for status output. This connection is used for status messages from the crypto module to the external DTE (data terminal equipment). Also three LEDs are present, P (power), I (iridium) and S (status).

2.2.5 Power Interface

Dedicated external male 25-pin miniature D-Sub type serial connection provides a dedicated serial pin for power input. This connection is used to provide power into the crypto module which is further passed onto the comm board after the power is downgraded. AN LED “P” for power is present on the side of the modem.

2.3 Roles, Services and Authentication

The XM Crypto Module has three Roles associated, a Crypto Officer, User (Human), and User (Process) roles. The operator of the module must assume either the Crypto Officer or User (Human) roles based on the operator's operation. User (Process) role is assumed based on the process of encrypted data being sent to the crypto board. All of these roles and their responsibilities are described below.

2.3.1 Crypto Officer Role

The Crypto-Officer (CO) is explicitly assumed by an operator accessing services associated with this role. The module requires the Crypto Officer to enter a password, eight to sixteen characters long made up any combination of upper case, lower case, numbers and special characters, along with setting any services.

The crypto-officer password, at minimum, will be eight charcaters in length, and can consist of any combination of 94 different characters (26 uppercase, 26 lowercase, 10 numerical and 32 special characters). Therefore, there is less than a one in 1,000,000 chance that a random attempt will be successful or that a false acceptance will occur (1/94^8 < 1/1,000,000). The module will allow one attempt to enter the correct password and then will not allow another attempt until after a ten second delay. The maximum number of attempts in a one minute time period is five attempts which means that the probability of a successful attempt in a one minute period is 5/94^8 which is less than 1/100,000.

Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Service	Description	Input	Output	CSP
Set Crypto Officer Password	Crypto Officer change default P/W Also changes any active password.	Enter new password 8-16 alpha-numerical characters. CO Password	No password is output. Module allows setting of encryption when password set correctly.	Crypto Officer password -write
Enter AES Encryption Cipher Key	AT command contains Crypto Officer password followed by encryption key. The entry is done twice and the module compares the values to make sure they are the same.	CO Password and AES-ECB 256 cipher key in HEX for encryption	Status message "Encryption Key Set" actual key cannot be output from module.	Crypto Key - write

Service	Description	Input	Output	CSP
Enter AES Decryption Cipher Key	AT command contains Crypto Officer password followed by decryption key. The entry is done twice and the module compares the values to make sure they are the same.	CO Password and AES-ECB 256 cipher key in HEX for decryption	Status message "Decryption Key Set "actual key cannot be output from module.	Crypto Key - write
Zeroize	AT command followed with Crypto Officer password which zeroize the crypto key or change Crypto Officer Password. Then system is rebooted to further clear keys in all locations within the module.	CO Password and AES-ECB Cipher Key for encryption and decryption are set to all zeros	Status message "ok"	Crypto Keys cleared or CO password changed -write
Enable/disable Crypto Service (encrypt and decrypt)	Sets or disables encryption capability within the module to perform	CO Password and Set encryption: UE = 0 to disables UE = 1 to sets	Status output message- Set to be Enabled Next Power Cycle. No msg when disabled	None

Table 2 – Mapping of CO Services to Inputs, Outputs, and CSPs

2.3.2 User Role – Human

The User role, implicitly assumed, accesses the module's cryptographic services that include encryption. No authentication is used to assume the User Role. The following table lists the services available to the User role.

Service	Description	Input	Output	CSP
Execute encryption process on data	AT command: instruct module to encrypt data	Any of following AT Commands SBDWB, SBDWT, D or CMGS followed by plaintext data	Ciphertext data	Encryption key - read

Service	Description	Input	Output	CSP
Power on/off module	Manually disconnect serial cable causes module to power off. Reconnect cable provides power	Manual connect/disconnect serial cable	Power on/off	None
Self-test	AT Command to execute on-demand self-test	STR	Pass or Power up self test FAILED	None
Show status	AT command to show status of module	UE	Encryption Currently Enabled. Encryption Currently Disabled. Set to be Enabled Next Power Cycle. Set to be Disabled Next Power Cycle. Encryption Disabled No Keys Entered.	None

Table 3 – Mapping of User Services to Inputs, Outputs, CSPs, and Type of Access

2.3.3 User Role – Process

The User role (Process) accesses the module's cryptographic services that include decryption. No authentication is used to assume the User Role (Process) The following table lists the services available to the User role (Process).

Service	Description	Input	Output	CSP
Execute decryption process on data	AT command to instruct module to decrypt following data	CMT or SBDRB followed by Ciphertext data	Plain text data	Decryption key - read

Table 4 – Mapping of User (Process) Services to Inputs, Outputs, CSPs, and Type of Access

2.4 Physical Make-up

The A3LA-XM's physical make-up consists of an aluminum case with anodized coating. The top panel comes completely off after removing 14 screws. The bottom panel has a small door covering the SIM card which is maintained by three screws. There is a serial connection on one end and an antenna connector on the other end.

The XM crypto module was tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

2.5 Cryptographic Key Management

The XM Crypto Module implements the following FIPS-approved algorithms:

- AES-ECB 256 (certificate # 1698)

The module supports the following critical security parameters:

Key	Generation / Input	Output	Storage	Zeroize	Access
AES-ECB 256 Cipher Key for encryption	AT Command followed by 32 Bytes HEX data	None	Plaintext within microcontroller (non-volatile)	AT Command sets key to zeros	CO
AES-ECB 256 Cipher Key for decryption	AT Command followed by 32 Bytes HEX data	None	Plaintext within microcontroller (non-volatile)	AT Command sets key to zeros	CO
Crypto Officer Password	8-16 alpha-numeric characters	Asterisk	Plaintext within microcontroller (non-volatile)	Manually zeroize	CO

Table 5 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

2.6 Self-Tests

The XM Crypto Module performs various self-tests to prevent any operations from continuing when components within the crypto boundary are not functioning correctly. This cryptographic module performs start-up, on-demand and conditional tests. The following is a breakdown of these self-tests:

- Power-Up Self-Tests:
  - Firmware integrity test
  - AES-ECB 256 Known Answer Tests (KATs)

- Conditional self-tests:
  - Key comparison

- On-demand self-test
    - Firmware integrity test
    - AES-ECB 256 Known Answer Tests (KATs)

Status output of power-up and on-demand self-tests display one of the following:

Running Self Test... Passed
Running Self Test... Power Up Test FAILED!

Status output of conditional self-test display the following:

Keys do not match

2.7 Design Assurance

Configuration management for all of the NAL Research Corporation source code files is provided by the program Subversion. The source code revisions are maintained in corporate controlled system with limited management access. Version number (X.Y.Z) is significant change, followed by new feature change/additions and finally by bug fix issue.

2.8 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

3 Secure Operation

The XM Crypto Module can be operated in FIPS mode or in non-FIPS mode. In non-FIPS mode no encryption is used. In FIPS mode the operator can see encryption set on the screen. The sections below describe how to configure and maintain the module in a FIPS-approved mode of operation. Operating the module without following this guidance will remove the module from the FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

3.1.1 Initial Setup

After connecting the male 25-pin miniature D-Sub type connector the module can be powered up. This in turn causes the module to go through a start-up self test. When the start-up self test is satisfactorily completed the Crypto Office must change their password from the factory default password. Then they enter in the encryption key and the decryption key followed by the AT command UE to set encryption. The Crypto Office then reboots the system by disconnecting the external serial cable and reconnecting the cable. Once the system comes up and satisfactorily completes the self-test the module is now in the FIPS mode of operation. An AT command

entered will verify. The Approved mode of operation occurs when the crypto-officer enters the crypto keys and sets the module to use encryption followed by a reboot of the system. The module is now in FIPS mode.

3.2 User Guidance

3.2.1 Setup/Operation

The User can determine if the module is in FIPS mode by entering the ^UE command. If not in FIPS mode the User shall notify the Crypto Officer to have the module placed in FIPS mode. The Users, both human and process can pass in data to the crypto module which in turn will cause the module to either encrypt or decrypt the data when in FIPS mode depending on the direction the data is traveling.

