FIPS 140-1 Non-Proprietary Security Policy

for

Level 1 Validation

of

NEXCOM MDR/MDT Interface Security Card (MMISC)

August 5, 2002

ITT Aerospace/Communications Division
1919 W. Cook Road
P.O. Box 3700
Fort Wayne, IN 46801-3700

Table of Contents

1 Purpose

This document describes the non-proprietary FIPS 140-1 security policy for ITT's NEXCOM MDR/MDT Interface Security Card (MMISC) cryptographic module. This Security Policy details the secure operation of the MMISC as required in Federal Information Processing Standards Publication 140-1 (FIPS 140-1). The cryptographic module is designed to attain a Level 1 overall validation.

2 References

FAA-E-2938	Subsystem Specification – Multi-Mode Digital Radio (MDR), July 23, 2001, V4.0
NAS-IC-41033502	Interface Control Document – Multi-Mode Digital Radio / Radio Interface Unit, July 23, 2001, V3.0
ITT MMISC ICD v1	MDT – MDR Interface Security Card Interface Control Document (MMISC ICD) For Next Generation Air/Ground Communications (NEXCOM)
AMPRO 5001131e2	CoreModule™/3SXi Technical Manual, P/N: 5001131, Revision: E
FIPS PUB 140-1	Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, January 11, 1994
FIPS PUB 186-2	Federal Information Processing Standards Publication, Specifications for Digital Signature Standard (DSS), National Institute of Standards and Technology, January 27, 2000
FIPS PUB 180-1	Federal Information Processing Standards Publication, Specifications for Secure Hash Standard, April 17, 1995

3 Glossary of Acronyms

AM-DSB – Amplitude Modulation Dual Side Band
CMT – Cryptographic Module Testing

FAA – Federal Aviation Administration
FIPS – Federal Information Procession Standards
ICD – Interface Control Drawing
MDR – Multi-Mode Digital Radio
MDT – Maintenance Data Terminal
MMISC – MDR/MDT Interface Security Card
NEXCOM – NEXt generation air/ground (A/G) COMmunications
RCP – Radio Control Processor
RF – Radio Frequency
RIU – Radio Interface Unit
VDL-3 – VHF Digital Link Mode 3

4 Introduction and MMISC Overview

4.1 MDR Background

Developed under the FAA's NEXCOM program, the MDR (Multi-Mode Digital Radio) is the next generation Air Traffic Control radio that provides communication services to the growing number of Air Traffic Control sectors. It supports the existing VHF AM-DSB voice ground-to-air communications, and it also provides a new digital waveform (VHDL-3) that will provide both digital voice and data services. The MDR's critical settings and functions can be controlled locally via a Maintenance Data Terminal (MDT) or remotely via a Radio Interface Unit (RIU). The MDT and RIU control interfaces are provided by the MDR's RS-232 and T1 interfaces respectively. The MDR is required to establish an authenticated control session with either of these controlling devices. In addition, the MDR can be reprogrammed from the MDT or RIU interface. The MDR is required to provide only authentication (and not encryption) with public keys provided by the user. The MDR security policy assures that an only an authorized operator possessing a valid security token can control the MDR or reprogram it with a new software upload.

4.2 MMISC

The agent within the MDR that provides the public key authentication functionality is the MDR/MDT Interface Security Card (MMISC). The MMISC security module authenticates the security token supplied by the operator during a login request to the MDR. Once a security token supplied by an operator via MDT or RIU interface is successfully authenticated, a secure control session is established with that interface (either MDT or RIU, as the case may be). While this secure control session is in progress, any login or radio control attempt made via the other interface is rejected. Any software uploaded during the secure control session is also authenticated, by verifying the digital signature received with the software. The MMISC implements a FIPS-approved Digital Signature Verification algorithm to validate the security token and software upload. The security implementation of the MMISC is required to provide level-1 security, as defined in the FIPS PUB 140-1.

The MMISC itself is a 80386-based, commercial Single Board Computer (SBC) manufactured by Ampro Computers Inc. The MMISC is classified as a multi-chip embedded module as per FIPS 140-1. The MMISC is primarily dedicated to the security functions within the MDR. It also directly provides the MDT interface, maintains an Event Log of internal radio events, and manages the software reprogramming for the entire MDR. Nearly all of the MMISC's functionality is provided by the software that is hosted on it. The MMISC runs with the VxWorks real-time operating system and ITT-developed application software written in C++. The MMISC provides just three interfaces. An RS-232 interface supports the MDT. Another RS-232 interface provides communication with the MDR's main controller processor. The third interface is input power to the MMISC.

5 Security Policy Rules

Overall, the MMISC acts as the gatekeeper of the MDR as a whole, providing both user authentication and secure software upgrades. The MDR radio relies entirely upon the MMISC (enclosed within MDR) to ensure that only valid software and valid users have access to the MDR. The following subsections provide all of the actual MDR security-related requirements that have been allocated to the MMISC. These requirements are taken directly from the FAA's Subsystem Specification – Multi-Mode Digital Radio, FAA-E-2938. These requirements essentially provide the "security policy rules" under which the MMISC must perform it security functions.

5.1 Verification

a) The MDR **shall$_{(513)}$** verify the authenticity, integrity and time validity of the digital signed information received via the MDT or RIU interfaces.
b) The MMISC (MDT – MDR Interface Security Card) performs the Digital Signature Verification algorithm as defined by the 'PKCS#1 RSA Cryptographic Standard (v1_5) and performs SHA-1 hash algorithm as defined in FIPS PUB 180-1.
c) The digital signature function **shall$_{(515)}$** meet or exceed security level 1 as defined in FIPS 140-1.
d) The digital signature function **shall$_{(516)}$** be validated according to FIPS 140-1 by an accredited FIPS 140-1 testing laboratory. ITT Industry has chosen Atlan Laboratory, an accredited CMT (Cryptographic Module Testing) laboratory, to validate its design and meet the intent of this FAA requirement.

5.2 Keys

a) The MDR **shall$_{(517)}$** provide storage for 10 public key certificates, any of which may be used in verifying the digital signature as defined in section 1 of the FAA specification, FAA-E-2938.

b) The storage for public keys **shall**$_{(518)}$ be in non-volatile memory and be maintained through power loss and restoral. The public keys are stored in the Flash memory.
c) The MDR **shall**$_{(519)}$ provide a mechanism to add and delete public keys as instructed via the MDT or RIU interface.

5.3 Security Procedures

a) All control parameter commands, except ID#30 Request Read-back, **shall**$_{(520)}$ be accepted only if the requesting device establishes a Control session, by providing a valid digitally signed authorization token ("security token").

Note: The Request Read-back control parameter is the only control parameter that the MDR will accept when no Control session has been established. This parameter facilitates a monitoring capability whereby an operator can read (but not change) any of the MDR's control settings, the MDR's internal Event Log, Public Keys (the public key data, not the key itself is read back), and some real-time performance parameters. For instance the operator can "read back" the current squelch setting or operating frequency of the MDR. He can also utilize this parameter for monitoring the MDR's current receive signal strength or reading back the Public Keys presently stored within the MDR.

Note: The "security token" will consist of the MDT- or RIU-supplied, FAA-generated digital signature of an FAA-selected data field. Data field selected FAA may be unique to each User Terminal.

b) All control parameter commands, except ID#30 Request Read-back, received without establishment of, or outside of, a Control session, or are associated with a security token that fails digital signature verification, **shall**$_{(523)}$ be rejected.

c) The MDR **shall**$_{(521)}$ receive and authenticate the security token each time an RIU or MDT logs in.

Note: Security procedures apply to Control sessions only. These security requirements apply to the MDR processing of control parameters, not to the MDR transmitter's processing of messages intended only for the RF transmission, nor to the MDR receiver's output of received RF information to the RIU.

d) Validation of the security token contained in the Log-In **shall**$_{(660)}$ be performed using only non-null public keys with any one of the 10 public keys as specified by the user.

5.4 Software Upload Security

a) Software uploads that are not digitally signed or contain an invalid digital signature **shall**$_{(522)}$ be rejected.

Note: The Software Upload control parameter (ID#38) message will contain, in the last delivered program binary block, a digital signature appended to the software binary image as a signature specifically for the software image contained in the program binary blocks.

b) Validation of the software binary image and digital signature contained in the Software upload **shall**$_{(661)}$ be performed using only non-null public keys with any one of the ten public keys as specified by the user.

5.5 Control Session

a) The MDR **shall**$_{(669)}$ initiate a control session upon successful authentication of RIU or MDT log on / security token.
b) As long as a valid session is active on one control interface, the MDR **shall**$_{(526)}$ reject all control parameters from the other control interface.
c) The MDR **shall**$_{(527)}$ terminate the control session upon log-out, MDT disconnection or after no control parameter is received within 30 minutes.

Note: An RIU or MDT will log in to initiate a Control session. A session is initiated after receipt of a Log-In and authentication of a security token. A session ends with a log-out, physical disconnection of an MDT, or when no Control Parameters are received within 30 minutes. A session is used by the RIU or MDT to convey control parameters, and receive both control replies and solicited radio monitoring messages. A control session is not required for unsolicited radio monitoring messages. The RIU will automatically log out (discontinue the control session) when it has completed sending control parameters.

5.6 Boot Cycle

The MDR boot cycle or equivalent **shall**$_{(528)}$ be secured such that the possibility of an illegitimate reconfiguration of the MDR operating software during the boot cycle or equivalent is extremely low.

6 Module Interfaces

6.1 Physical Interfaces

The MMISC's physical interfaces include two RS-232 ports through which the MMISC interfaces with the MDT and the MDR's Radio Control Processor (RCP). These serial interfaces (i.e. the MMISC/MDT interface and the MMISC/RCP interface) are used to pass commands and accept responses. Both of these interfaces operate at 38400 baud, 8 bits, no parity, 1 stop bit, and no flow control. The MMISC/MDT interface also provides a discrete signaling line (CTS) that allows the MMISC to detect the physical disconnection of the MDT.

6.2 Logical Interfaces

There are seven logical interfaces that are designated by message type and/or physical interface as follows:

1. "Forwarding" interface for MDT-to-RCP messages: An interface where the MMISC simply passes certain messages originating from the MDT on to the RCP.
2. "Forwarding" interface for RCP-to-MDT messages: An interface where the MMISC simply passes certain messages originating from the RCP on to the MDT.
3. MMISC-to-RCP query/reply interface: This is the interface upon which the MMISC may request needed data from the RCP (e.g. the MMISC requests time from the RCP so that it may time-stamp logged events).
4. Control/Request Input Interface: This interface supports messages that are targeted for the MMISC for action. All of the security related request messages (e.g. a Login Request or a SW upload) use this interface. Security benign messages such as an Event Log Download Request or a Software Version Request also use this interface.
5. Reply Output Interface: This interface handles all the replies resulting from requests on the Control/Request logical interface.
6. Event Informing Input Interface: This interface handles only Event messages coming from the RCP. The MMISC creates an Event Log entry for every incoming Event message.
7. Status Output Interface: This logical interface supports all outgoing unsolicited status messages from the MMISC. Messages on this interface include Alert/Alarm messages, failure/warning messages, control session status messages, etc.

7 Roles and Services

7.1 Roles

The MMISC defines two roles: the User role and Crypto-Officer role. The User role does not require the operator to authenticate and allows the operator to perform only non-authenticated services such as monitoring the MDR's frequency, time, and reading back the Event Log. The Crypto-Officer role has access to all of the module's services and requires the operator to authenticate and thus establish a control session with the MMISC from one of the two interfaces.

Authentication is performed by providing a valid (signed) security token. The MMISC verifies the validity of the signature before establishing a control session and granting access to control requests. The Crypto-Officer role allows the operator to perform all available functions including all control requests like key management functions, software upload, and radio configuration.

7.2 Services

The MMISC provides the following security critical functions that can only be performed by the Crypto-Officer:

Login: Allows a user to authenticate to the module by providing a valid security token.
Add key: Allows a user to load a public key on the module.
Delete key: Allows a user to delete a public key already stored on the module.
Software upload: Allows a user to load digitally signed software on the module.
Software Upload Enable/Disable: Allows a user to enable or disable the software upload function.

Self-Tests, which include a CRC-based, Software Integrity test and a Known Answer Test against the RSA signature verification function, are automatically performed at power-up. The Crypto-Officer can invoke these tests by simply power cycling the MDR.

In addition to the above-mentioned security functions the MMISC supports a variety of MDR status functions such as the monitoring functions (time, frequency, RF Power, etc.), status check functions (online/offline, software version, etc.), maintaining the MDR's Event Log, and managing the actual MDR reprogramming process. See the MMISC ICD for a complete list of all MMISC services and the corresponding role in which they can performed.

8 Authentication

8.1 Crypto-Officer

The MDR/MMISC authenticates Crypto-Officers by using the appropriate public key to verify the signed security tokens provided by the Crypto-Officer. The MMISC authenticates the security token supplied, and if successfully authenticated, establishes a secure control session for the interface from which the token originated (either MDT or RIU interface, as the case may be). While this secure control session is in progress, any additional authentication attempts made via the other interface are rejected. The MMISC will terminate the control session upon a Crypto-Officer logout request, MDT disconnection, or after a 30-minute, inactivity timeout.

8.2 Software Upload

The MMISC also additionally authenticates incoming Software Upload messages (Software Uploads contain new operating software for the MDR to support local and remote reprogramming of the MDR). Software uploads are signed, and the MMISC uses the appropriate public key to authenticate them. Software Uploads are only accepted by the MMISC for authentication within the context of an already established secure control

session. Software Uploads are rejected if they are received outside of a control session or if the authentication fails.

9 Key Management

The MMISC can persistently store up to ten 1024-bit RSA public keys used to authenticate Crypto-Officers and to verify the integrity of Software Uploads. In addition, the MMISC also contains an additional default/factory public key that is used during the manufacturing process.

The module's default or "factory" key is imbedded with the MMISC software/firmware image and is only active/valid (for use in authentication or validation of Software Uploads) when no public keys are loaded. Thus the factory key is "present" when first assembled at the factory, after a Crypto-Officer deletes all stored public keys, or after the Crypto-Officer issues a Factory Reset to the MDR. So long as one or more a public keys are being stored in any of the ten key slots, the default/factory public key can no longer be used. The Factory Key cannot be deleted by the Crypto-Officer.

The MMISC authenticates Crypto-Officers and Software Uploads; thus, it does not provide any key generation, key distribution, key output, or key archiving services. Furthermore, the module contains no secret keys, private keys or other critical security parameters. It only contains RSA public keys.

The remaining aspects of key management are discussed below:

a) Key entry/output: RSA public keys can be entered and output by the Crypto-Officer because the keys are public keys. They are transmitted in plain text.
b) Key storage: The MMISC stores public keys in non-volatile memory and stores the default public key (factory key) in its image.
c) Key zeroization: Key Zeroization is not applicable as the module does not contain any secret keys, private keys, or unprotected critical security parameters.

There is no distinct relationship between a Crypto-Officer and the public keys stored in the MMISC. Each Crypto-Officer has complete authority over all the keys (except the default factory key) stored within the MMISC, and there is no unique association between a key and its user.

10 Cryptographic Algorithms

The MMISC performs the following FIPS-approved algorithms:

a) RSA: Digital Signature Verification algorithm as defined by the "PKCS#1 RSA Cryptographic Standard (v1_5)".
b) The SHA-1 hashing algorithm as defined in FIPS PUB 180-1.

11 Self-Tests

The MMISC provides all of the FIPS-required self-tests:

Power-up tests:

- Software Integrity test: The MMISC verifies the integrity of all its software by performing a CRC over all of its software and comparing it to the stored CRC value.
- Known Answer Test for RSA signature verification.

Conditional tests:

- Software/Firmware Load Test: The MMISC validates the authenticity and integrity of all loaded software by verifying the RSA signature attached and will reject any software image that fails this test.

The user can initiate power-up self-tests upon demand by simply cycling the module's power. The module has no statistical random number generator and does not perform any optional tests.