Common Crypto Circuit Card Assembly
Rockwell Collins

Commercial Crypto Contract (CCC)

FIPS 140-2 Non-Proprietary
Security Policy

Level 1 Validation

Revision D

Date: 04 April, 2005

This page intentionally left blank.

REVISION RECORD		
{PRIVATE} REV	DESCRIPTION	APPROVAL AND DATE
-	Initial	06/05/03
1	Extensively Revised	11/13/03
2	Extensively Revised	02/13/04
3	Revised	03/11/04
4	Revised per CygnaCom Comments	04/28/04
5	Revised per CygnaCom Comments	06/01/04
6	Revised per CygnaCom Comments	07/23/04
7	Revised per CygnaCom Comments	09/24/04
8	Revised per CygnaCom Comments	04/04/05

TABLE OF CONTENTS

1.0 INTRODUCTION 1

1.1 SCOPE OF DOCUMENT 1
1.2 SECURITY LEVEL 1

2.0 REFERENCE DOCUMENTS 2

3.0 SECURITY MODULE OVERVIEW 3

3.1 COMMON CRYPTO MODULE 3
3.2 MODULE DESCRIPTION 4
3.3 MODULE PORTS AND INTERFACES 5
3.4 ROLES, SERVICES AND AUTHENTICATION 6
3.5 FINITE STATE MODEL 8
3.6 PHYSICAL SECURITY 8
3.7 CRYPTOGRAPHIC KEY MANAGEMENT 8
3.7.1 Traffic Encryption Keys 8
3.7.2 Key Management Summary 8
3.8 EMI/EMC 9
3.9 SELF-TEST 9
3.10 DESIGN ASSURANCE 9
3.11 MODES OF OPERATION 12
3.11.1 Approved Modes 12
3.11.2 Unapproved Modes 14

4.0 ACRONYMS AND ABBREVIATIONS 16

LIST OF FIGURES

FIGURE 1 CRYPTO MODULE COMPONENT LAYOUT 4
FIGURE 2 CRYPTO MODULE BLOCK DIAGRAM 5
FIGURE 3 RC-TCP V MODEL 12

LIST OF TABLES

TABLE 1 SECURITY REQUIREMENTS 1
TABLE 2 MAPPING BETWEEN PHYSICAL AND LOGICAL INTERFACES 6
TABLE 3 ROLES AND SERVICES 7
TABLE 4 ACCESS GRANTED WITH EACH SERVICE 7

1.0 INTRODUCTION

1.1 SCOPE OF DOCUMENT

This is a non-proprietary FIPS 140-2 Security Policy for the Commercial Crypto Contract (CCC) Common Crypto Circuit Card Assembly, hardware version 944-2541-002 / software version 091-3186-001. This Security Policy describes how this module meets the requirements as specified in the FIPS PUB 140-2 Security Requirements for Cryptographic Modules document. This Security Policy forms a part of the submission package to the test lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four (4) security levels for cryptographic modules this standard identifies requirements in eleven sections.

1.2 SECURITY LEVEL

The cryptographic module meets the overall requirements applicable to level 1 security of FIPS 140-2.

Table 1 Security Requirements

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

2.0 REFERENCE DOCUMENTS

Document Number	Title	Date
FIPS 140-2	Security Requirements for Cryptographic Modules	03 December 2002
N/A	Implementation Guide for FIPS PUB 140-2 and the Cryptographic Module Validation Program	22 September 2004
N/A	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules	24 March 2004
N/A	Statement of Work: Development, Evaluation and Certification of Programmable Cryptographic Devices for Link 16 Terminals	9 July 2002
963-2636-001	Module Specification, Common Crypto CCA	16 April 2003

3.0 SECURITY MODULE OVERVIEW

3.1 COMMON CRYPTO MODULE

The Common Crypto Circuit Card Assembly (CCA), or module, when mated with the appropriate interface card, comprises a data encryption/decryption card with selectable algorithms. The module is capable of storing and using up to eight keys. The Cryptographic Module has the following characteristics:

- The Cryptographic Module is a single channel device.
- The Cryptographic Module is half-duplex only.
- The Cryptographic Module is capable of utilizing four commercial algorithms, one at a time.
- The AES algorithm operates in a FIPS Approved mode.

The Common Crypto Circuit Card Assembly implements four (4) commercial cryptographic algorithms in an FPGA format. Each of the four commercial cryptographic algorithms are implemented using 128 bit Block length and 128 bit key length. In addition, a proprietary method is implemented in software and is used for the obfuscation of traffic keys. The commercial cryptographic algorithms are:

- Twofish
- Serpent
- Triple-DES*
- AES Rijndael**

*Note: Triple-DES is implemented in a non-standard manner as two Triple-DES instantiations in a side by side fashion with bit padding to create a 128 bit key. In addition, known answer tests are not performed on the Triple-DES instantiations during the power up self-tests.

**Note: AES Rijndael is implemented in an approved mode.

The Crypto Module is a factory programmable module. Cryptographic algorithms/equipments are installed in the module during production and are user selectable in the field.

The boundary is defined as the entire Common Crypto Circuit Card Assembly and there are no exclusions from the Card. The block diagram for the module is as shown in Figure 2 with all the interconnections between the components of the module.

The module implements AES in the approved mode and, Triple-DES, Twofish, Serpent in unapproved algorithm modes. The AES, Triple-DES, Twofish and Serpent algorithms are stored in memory and when selected for use, are loaded into the FPGA for operation. The Module component layout is shown in Figure 1.

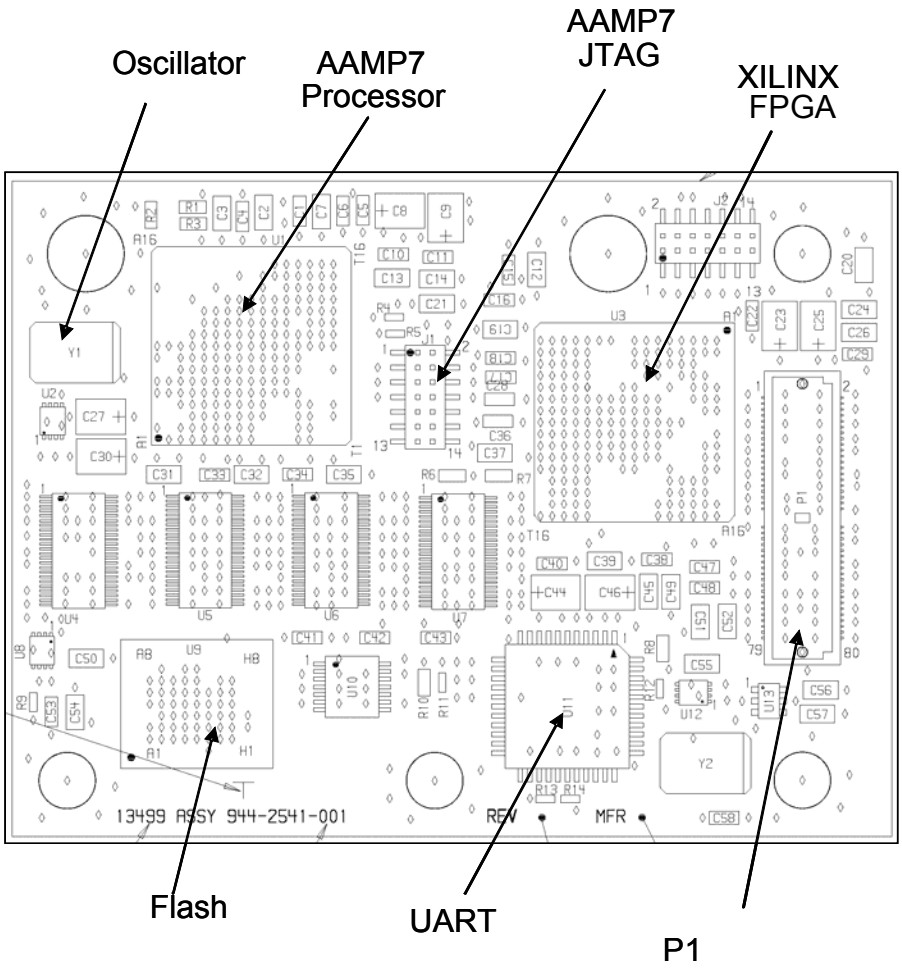

Figure 1 Crypto Module Component Layout

3.2 MODULE DESCRIPTION

The Cryptographic Module is a cryptographic Circuit Card Assembly (CCA) as seen in Figure 2. The card assembly is approximately 2.2 x 3.0" and contains the AAMP7r1 micro processor packaged in a 256-pin FPGA, a 50.000MHz clock oscillator, a UART for the serial fill port, a 3.6864MHz clock oscillator for the UART, a Xilinx XC2V1000-5FG256I FPGA (which is the programmable crypto device), a watchdog timer, and 4M x 16 FLASH. The FLASH is addressed by Chip Select 0 (CS0). The UART is addressed by Chip Select 6 (CS6).

The FPGA I/O registers are addressed by Chip Select 12 (CS12). The watchdog timer is addressed by Chip Select 15 (CS15). The watchdog timer device also generates a power up reset. Chip Select 14 (CS14) is ANDed in with the other interrupts and connected to the Non-Maskable Interrupt (NMI) inputs. The power to the board is divided so that the AAMP7 and fill port can operate in standby mode with the FPGA powered down. Chip Select 13 (CS13) is used to load the configuration into the FPGA.

Figure 2 depicts the microprocessor data bus and Input/Output destinations. The bus consists of a 32-bit data bus and a 24-bit address bus. The external FLASH hosts the four pre-programmed algorithms. The UART provides capability for Key Fill, algorithm selection, zeroization and status. This path is the only control and status port available due to the legacy terminal design.

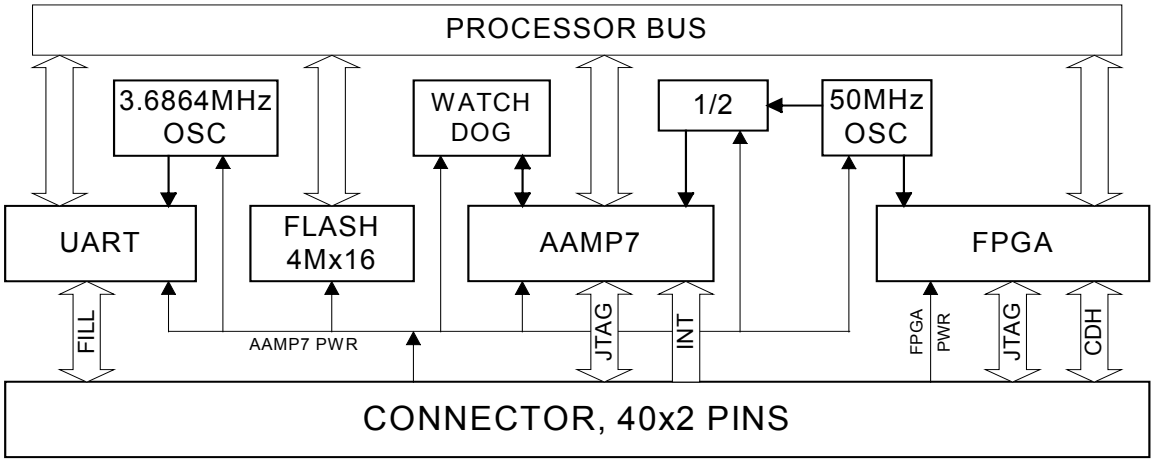

Figure 2 Crypto Module Block Diagram

The algorithms are run in a Xilinx FPGA (XC2V1000) and each is loaded into the FPGA on command from the handheld key fill device. The AAMP7 processor controls loading of the algorithms and handles key management functions within the crypto module. The AAMP7 also collects status information and reports status to the handheld key fill device upon command. The key fill device is an external custom device which interfaces to the CCA through the RXD and TXD signals on the P1 connector.

3.3 MODULE PORTS AND INTERFACES

For purposes of this discussion, the Common Crypto Circuit Card Assembly is considered to be a multiple chip embedded cryptographic module. A single physical connector is used during normal operation to host the following logical interfaces:

- Data Input Interface is defined as the data input interface through which data is input to the module.
- Data Output Interface is defined as the data output interface.

- Control Input Interface is defined as the data input interface through which control data is input to the module.

- Status Output Interface is defined as the status output interface.

At the factory, two J1 or JTAG connectors are used for programming the AAMP7 and the FPGA for initial board testing and removed after the initial testing. These connectors are made unavailable after the CCA is potted using an opaque epoxy coating to inhibit access to board components and provide tamper evidence.

Table 2 describes the relationship between the logical and physical interfaces.

Table 2 Mapping Between Physical and Logical Interfaces

Logical Interface	Physical Interface
Data Input Interface	P1, J1
Data Output Interface	P1, J1
Control Input Interface	P1, J1
Status Output Interface	P1, J1
Power Interface	P1, J1

3.4 ROLES, SERVICES AND AUTHENTICATION

The Common Crypto Circuit Card Assembly supports a Crypto Officer and a User role. The module implements no authentication. The module does not support a maintenance role. Roles and Services are summarized in Table 3. Access to keys and CSPs allowed for each service is shown in Table 4.

The services available to the Crypto Officer are:

- Load and Zeroize the keys.
- Perform Pre-determined algorithm selection.
- Perform crypto operations.
- Obtain Crypto Module status through the external Hand-held Key Fill device.

The User can perform:

- Perform crypto operations.

It is permissible for the User to act as the Crypto Officer if so designated.

Table 3 Roles and Services

ROLE	SERVICES
Crypto Officer	Load and Zeroize Keys Select Algorithm Obtain Crypto Module Status Perform crypto operations
User	Perform crypto operations

Table 4 Access Granted with Each Service

SERVICE	ACCESS
Load and Zeroize Keys	Access to external Key Loader Device. Keys are obfuscated and are loaded electronically using a proprietary method.
Select Algorithm	Access to external Key Loader Device. Algorithm selection is pre-determined and selection is accomplished through electronic means.
Obtain Crypto Module Status	The status of the Crypto Module can be read through the external Key Loader Device. Information available includes the status of BIT and ALARMS.

Perform Crypto Operations	Both Crypto Officer and User can perform crypto operations. Access is not controlled.

3.5 FINITE STATE MODEL

The module has been designed to meet the requirements of the Finite State Model (FSM). A detailed FSM has been submitted as part of the validation process to the lab. The module consists of the following states: Power Off, Power On, Prime Power Detected, Load Boot Code, Perform Initiated BIT, Pass BIT, Load Application Code, Load Previous Algorithm and Keys, Operational Mode, Hand-held Device Detected, Command Message, Execute Command, Load Key Message, Load Keys, Key Fill Pass, Alarm Conditions Detected, Perform Periodic BIT, Pass PBIT, Alarm Check Pass, Fatal Alarms, Zeroize and Set Alarms, Faulted.

3.6 PHYSICAL SECURITY

The crypto module employs physical security. The cryptographic module is covered, prior to shipment, with a tamper-evident coating or potting material to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components. The tamper-evident coating is opaque within the visible spectrum. Use of the tamper-evident potting material satisfies the requirement for Security Level 2 as defined in the FIPS 140-2 publication.

3.7 CRYPTOGRAPHIC KEY MANAGEMENT

No keys are generated within the cryptographic module. The module employs one type of key, the traffic encryption keys.

3.7.1 Traffic Encryption Keys

All traffic encryption keys are loaded from the Hand-held key fill device. These keys are obfuscated at the source using a proprietary method and loaded into the key fill device. The keys are downloaded into the cryptographic module in plaintext. Keys are used based upon the memory locations to which they have been assigned by the Key Fill Device. There are a total of eight Traffic Encryption Keys used by the Module. Traffic Encryption Keys can be zeroized by the ZEROIZE_F signal, a discrete input to the module or by use of the Key Fill Device.

3.7.2 Key Management Summary

The module stores the traffic encryption keys internally in plaintext form and obfuscated with a proprietary method. Keys are used as soon as an algorithm is loaded into the FPGA. Since only a single algorithm is used at any time, all keys loaded are associated with the selected algorithm. The module employs a signal, TAMPDET_F, which when active causes zeroization of all keys within the module.

3.8 EMI/EMC

The Common Crypto Circuit Card Assembly (Cryptographic Module) complies with EMI/EMC requirements as specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A. The module was tested by Intermec Technologies Corporation EMC Test Laboratory in Cedar Rapids, IA, FCC registration number 90691. The compliance certificate has been submitted to the lab as part of the validation process. The test date was April 1, 2004 and the Test Report Number is 040401-1.

3.9 SELF-TEST

The Common Crypto Circuit Card Assembly performs the following self tests:

- Software Power-up Integrity Tests: The module software checks the integrity of its various components using built in test routines in the processor, integrity checks on stored software, integrity checks on stored keys, and checks of the integrity of the algorithm load into the FPGA from memory.

- Software Periodic Tests: The module continuously checks the module status through built in test routines which run in the background. These tests include memory tests and monitoring of alarm conditions.

- Watchdog Timer: The software is protected from aberrant behavior by a watchdog timer which requires a periodic reset. Failure of the software to provide the reset forces the watchdog to initiate a reboot of the crypto module.

- Cryptographic KATs: Known Answer Tests (KATs) are run at power-up on the algorithm which is loaded into the FPGA. This test consists of the AAMP7 processor writing known key and data information to the algorithm block and comparing the algorithm output with stored results.

- No keys are generated by the cryptographic module.

- There are no Random Number Generators implemented in the design.

3.10 DESIGN ASSURANCE

The Common Crypto Circuit Card Assembly satisfies the design assurance requirements as described in the standards by adopting the following methodologies:

1) Configuration Management

    - Rockwell Collins Government System is CMMI level three certified. The Software Engineering Institute's Capability Maturity Model Integrated (CMMI) for System Engineering, Software Engineering and Integrated product and Process Development

has been implemented at Rockwell Collins as the standard to develop, measure and improve the development process.

- The Rockwell Collins Configuration Management (CM) system is a disciplined, integrated, and documented system, which identifies and controls the configuration of software, hardware, and supporting documentation. These disciplines make possible systematic and traceable control of changes to the software and the required documentation from the initial development through the product life cycle.

- It is the policy of Rockwell Collins to implement an effective Configuration Management (CM) system applicable to all hardware and software products designed, built, or sold by the Company. CM is a discipline that is applied over the life cycle of a product to provide visibility and control of its functional and physical characteristics. CM principles provide for the orderly establishment, documentation, and maintenance of a product's functional performance and physical attributes, managing changes to the attributes, and furnishing accurate information essential to the product's use, reproduction, maintenance, and re-procurement.

- The CM process uses a ten digit part numbering scheme to provide component and configuration identification. Additionally, the CM process identifies the criteria and methods for part number re-identification.

- The Computer Software Configuration Item (CSCI) for the Key Manager application software is 091-3186-001.

- The Firmware Configuration Item (FWCI) number of the FIPS-compliant AES Rijndael algorithm, is 091-3192-001.

- The Firmware Configuration Item (FWCI) number of the non-compliant Triple-DES algorithm is 091-3194-001.

- The Firmware Configuration Item (FWCI) number of the Two Fish algorithm is 091-3195-001.

- The Firmware Configuration Item (FWCI) number of the Serpent algorithm is 091-3193-001.

- The Common Crypto Circuit Card Assembly is 944-2541-002.

2) Delivery and Operation

Installation of the Cryptographic Module will be performed in the factory. The units will be assembled and shipped as part of larger assemblies. All configuration items are assigned serial numbers. Items are shipped in accordance with the contract, usually by FedEx using tracking numbers for traceability.

3) Development

- The development of the module conforms to the assurance requirements in the FIPS 140-2 standard in accordance with a Security Level 2 implementation. This is accomplished through adequate design documentation, including assembly drawings, schematic diagrams, documentation of software and firmware source code, functional specifications, and interface descriptions. The development process follows the Rockwell Collins Technical Consistent Process (RC-TCP).

- The RC-TCP is the process framework that defines the technical processes used by engineering, shared services, subcontracting and engineering support to develop and maintain systems which include System, Hardware, Software, Installation, and ASIC technical artifacts. The RC-TCP is invoked by the Rockwell Collins Integrated Project Management (RC-IPM) project planner during development activities to fulfill a work breakdown structure (WBS). A model of the process is shown in Figure 3.

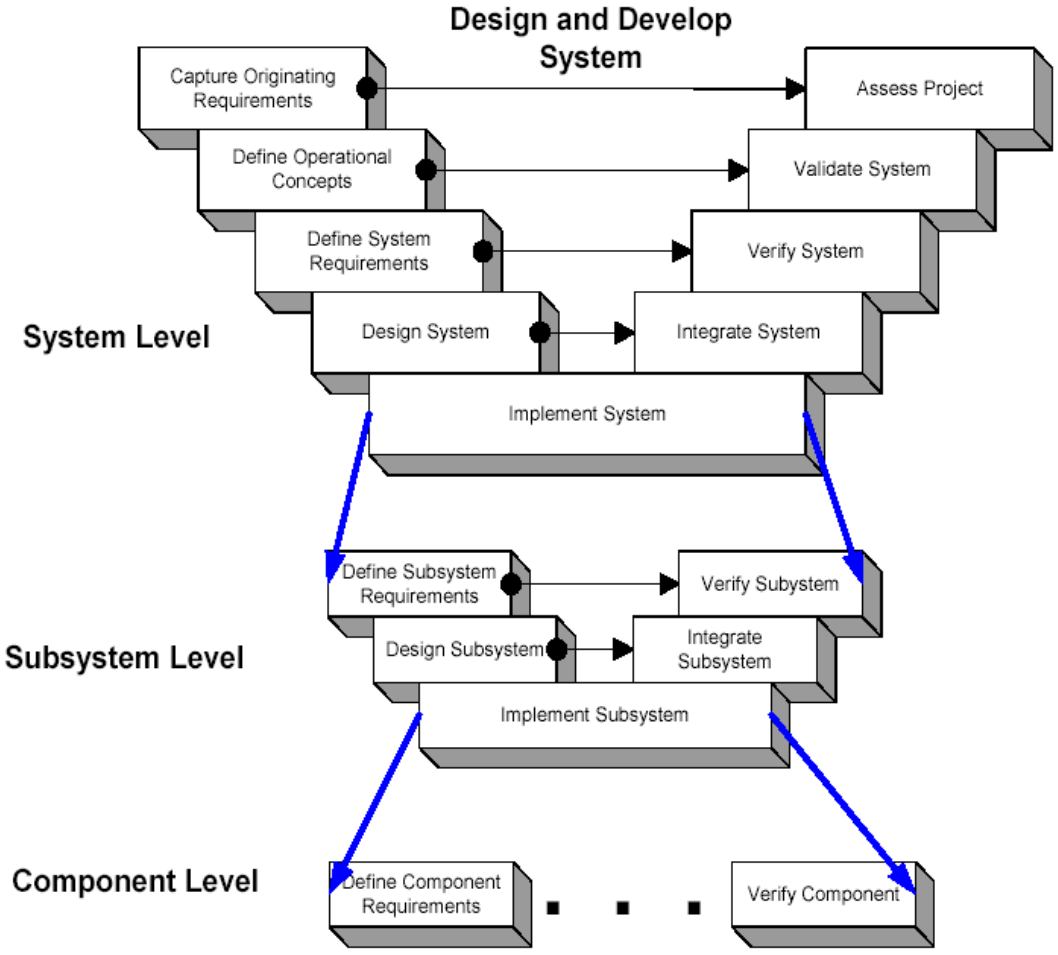

Figure 3 RC-TCP V Model

3.11 MODES OF OPERATION

3.11.1 Approved Modes

One approved mode of operation is supported. The AES Rijndael algorithm operates in an approved mode using a 128 bit key. The AES Rijndael is used to encrypt and decrypt traffic information. All algorithms are implemented in the counter mode of operation. The basic algorithm blocks operation in Electronic Code Book mode using the external key and a counter output as the data input.

To operate the module in the approved mode the Crypto Officer or User must configure the module in the correct manner. The following is the startup and initialization procedure for the Cryptographic Module after the software has been loaded into the device.

- Power Up Module

1. Module loads boot code and runs Initial BIT test
2. Module loads and checks application code.
3. Module loads and checks algorithm and loads keys from memory.
4. Module perform Known Answer tests
5. Module is configured for operational use, which includes encryption and decryption of user data.

- Key Fill

1. Turn on the Key Fill Device.
2. Connect Key Fill Device to the module.
3. Select the "KeyLoader" program from the "Programs" menu.
4. Select the "Keys" tab on the Key Fill Device.
5. Verify that the Key Fill Device recognizes that the crypto module is connected.
6. Load platform configuration.
7. Verify the algorithm in use.

- Zeroize Keys

1. Turn on the Key Fill Device.
2. Connect Key Fill Device to the module.
3. Select the "KeyLoader" program from the "Programs" menu.
4. Select the "Zeroize" tab on the Key Fill Device.
5. Verify that the Key Fill Device recognizes that the crypto module is connected.
6. Zeroize keys as desired.

- Read Status

1. Turn on the Key Fill Device.
2. Connect Key Fill Device to the J1 connector on the unit.
3. Select the "KeyLoader" program from the "Programs" menu.

4. Select the “Status” button from the menu
5. Read Status results from screen.

3.11.2 Unapproved Modes

One non-approved mode of operation is supported. The Triple-DES, Twofish, and Serpent algorithms operate in the non-approved mode using a 128 bit key. These algorithms are used to encrypt and decrypt traffic information.

To operate the module in the non-approved mode the Crypto Officer or User must configure the module in the correct manner. The following is the startup and initialization procedure for the Cryptographic Module after the software has been loaded into the device.

- Power Up Terminal
  1. Module loads boot code and runs Initial BIT test.
  2. Module loads and checks application code.
  3. Module loads and checks algorithm and transfers keys.
  4. Module performs Known Answer tests.
  5. Module is configured for operational use, which includes encryption and decryption of user data.
- Key Fill
  1. Turn on the Key Fill Device.
  2. Connect Key Fill Device to the module.
  3. Select the “KeyLoader” program from the “Programs” menu.
  4. Select the “Keys” tab on the Key Fill Device.
  5. Verify that the Key Fill Device recognizes that the crypto module is connected.
  6. Load platform configuration.
  7. Verify the algorithm in use.
- Zeroize Keys

1. Turn on the Key Fill Device.
2. Connect Key Fill Device to the module.
3. Select the “KeyLoader” program from the “Programs” menu.
4. Select the “Zeroize” tab on the Key Fill Device.
5. Verify that the Key Fill Device recognizes that the crypto module is connected.
6. Zeroize keys as desired.

- Read Status

6. Turn on the Key Fill Device.
7. Connect Key Fill Device to the J1 connector on the unit.
8. Select the “KeyLoader” program from the “Programs” menu.
9. Select the “Status” button from the menu
10. Read Status results from screen.

4.0 ACRONYMS AND ABBREVIATIONS

The purpose of this section is to establish a list of terms, abbreviations, and acronyms that are used in this document.

AES	Advanced Encryption Standard
AAMP7	Advanced Architecture Microprocessor
BIT	Built-In Test
CCA	Circuit Card Assembly
CCC	Commercial Crypto Contract
CM	Configuration Management
CMMI	Capability maturity Model Integrated
COMSEC	Communications Security
DES	Digital Encryption Standard
EMI	Electro-Magnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FSM	Finite State Model
HMC	Hand-held Mobile Computer
KAT	Known Answer Test
KEK	Key Encryption Key
MILS	Multiple Independent Levels of Security
NIST	National Institute of Standards and Technology
PDA	Personal Data Assistant
RC	Rockwell Collins
TCP	Technical Consistent Process