MOTOROLA

# Security Policy: Radio Network Controller Encryption Module Controller (RNC EMC)

Cryptographic module used in Motorola's Radio Network Controller

Version: R01.00.08

Date: September 17, 2007

## Table of Contents

# 1. Introduction

## 1.1. Scope

This Security Policy specifies the security rules under which the Radio Network Controller Encryption Module Controller, herein identified as the RNC EMC, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators
2. module services
3. Critical Security Parameters (CSPs).

## 1.2. Overview

The RNC EMC provides secure key management, Over-the-Air-Rekeying (OTAR), and voice and data encryption for Motorola's Radio Network Controller (RNC).

## 1.3. RNC EMC Implementation

The RNC EMC is implemented as a multi-chip standalone cryptographic module as defined by FIPS 140-2.

## 1.4. RNC EMC Hardware / Firmware Version Numbers

| Kit Name | FIPS Validated Cryptographic Module Hardware Kit Numbers | FIPS Validated Cryptographic Module Firmware Version Numbers |
|---|---|---|
| RNC EMC (AES-256) | T7289A | R03.04.00 |

## 1.5. RNC EMC Cryptographic Boundary

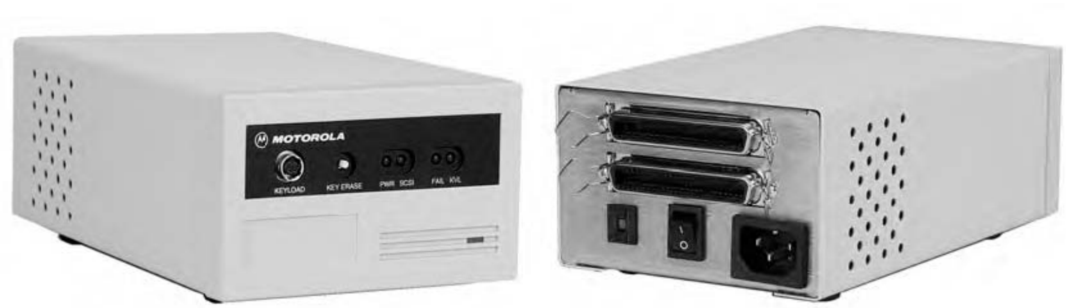

**Figure 1**: HW kit T7289A. The Crypto Boundary includes the entire encryption module and housing. The module contains 3 connectors: SCSI (Data, Control, Status, and OTAR Key data) connector, KVL (Key Data, Control, and Status) connector, and Power Connecter. The module also contains a Key Erase button (equivalent to tamper) and 4 status LEDs.

## 2. FIPS 140-2 Security Level

The RNC EMC is validated to meet the FIPS 140-2 security requirements for the levels shown below. The overall module is validated to FIPS 140-2 Security Level 1.

**Table 1: RNC EMCSecurity Levels**

| FIPS 140-2 Security Requirements Section | Level |
|---|---|
| Overall Security Level | 1 |
| Cryptographic Module Specification | 1 |
| Module Ports and Interfaces | 1 |
| Roles, Services, and Authentication | 1 |
| Finite State Model | 1 |
| Physical Security | 1 |
| Operational Environment | N/A |
| Cryptographic Key Management | 1 |
| EMI / EMC | 1 |
| Self Tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

# 3. FIPS 140-2 Approved Operational Modes

The RNC EMC supports both a FIPS approved mode of operation and a non-approved mode of operation. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 approved mode of operation:

1. Key Loss Key (KLK) generation disabled

AND

2. AES-256 encryption, decryption, and authentication (authentication, AES MAC, is approved when used for Project 25 OTAR) shall be used in the following approved modes: OFB, ECB, and CBC.

The module employs two Deterministic Random Number Generators as described below:

- ANSI X9.17: The ANSI X9.17 DRNG is used in FIPS mode to generate IVs and obfuscation keys. None of the random values produced by this RNG are used to provide any FIPS approved Security.

- 64 bit Linear Feedback Shift Register LFSR: The 64 bit Linear Feedback Shift Register is used to provide IVs.

# 4. Non FIPS Mode

The module will transition into a non-FIPS approved mode if any of the following algorithms are invoked:

- DES (ECB, OFB, CFB, and CBC modes)
- DES-XL
- DVI-XL
- DVI-SPFL
- DVP-XL

# 5. Security Rules

The RNC EMC enforces the following security rules. These rules are separated into two categories

1. those imposed by FIPS 140-2 and,
2. those imposed by Motorola.

## 5.1. FIPS 140-2 Related Security Rules

1. The RNC EMC supports the following interfaces:
   - Data input interface
     a. Synchronous Serial Interface (SCSI) - Plaintext Data, Ciphertext Data, Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR), Authentication Data
     b. Key Variable Loader (KVL) - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys
   - Data output interface
     a. Synchronous Serial Interface (SCSI) - Plaintext Data, Ciphertext Data, Key Management Data (OTAR)
   - Control input interface
     a. Synchronous Serial Interface (SCSI) - Input Commands
     b. Key Variable Loader (KVL) - Input Commands
   - Status output interface
     a. Synchronous Serial Interface (SCSI) - Status Codes
     b. Key Variable Loader (KVL) - Status Codes
     c. LEDs – Status Codes
        - Power LED – Power applied
        - SCSI LED – SCSI Activity
        - Fail LED – Indicates fatal or non-fatal error
        - KVL LED – Indicates KVL keyloading mode
   - Power interface
     1. Switched - Powers all circuitry except Battery Backed Register
     2. Unswitched - Powers Battery Backed Register
2. The RNC EMC inhibits all data output via the data output interface whenever an error state exists and during self-tests.
3. The RNC EMC logically disconnects the output data path from the circuitry and processes when performing key generation or key zeroization.
4. Critical security parameters are entered in plaintext form.
   ***AND***
   Secret cryptographic keys are entered over a physically separate port.
5. The RNC EMC supports a User role, a Cryptographic Officer role, and the Maintenance role. The first two roles allow the same set of services while the third role allows a different set of services. A role is implicitly selected based on the service being used.
6. The RNC EMC provides the following services requiring a role:
   - Transfer Key Variable

   - Privileged APCO OTAR
   - Change Active Keyset
   - Encrypt Digital
   - Decrypt Digital
   - Zeroize Selected Keys
   - Show Status
   - Battery Replacement
   - Firmware Upgrade
   - SCSI ID Change
7. The RNC EMC provides the following services not requiring a role:
   - Initiate Self Tests
   - Zeroize all keys
   - Non-Privileged APCO OTAR
   - Reset
   - Download configuration parameters via SCSI messages
   - Key/Keyset Check
8. The RNC EMC implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
9. The RNC EMC protects private keys from unauthorized disclosure, modification and substitution.
10. The RNC EMC provides a means to ensure that a key entered into, stored within, or output from the RNC EMC is associated with the correct entities to which the key is assigned. Each key in the RNC EMC is entered and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID, Common Key Reference (CKR) number, or CKR/Keyset number – Identifiers indicting storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption. When used or deleted the keys are referenced by Key ID/Algid, Physical ID, or CKR/Keyset.
11. The RNC EMC denies access to plaintext private keys contained within the RNC EMC.
12. The RNC EMC provides the capability to zeroize all plaintext cryptographic keys within the RNC EMC.
13. The RNC EMC supports the following FIPS approved algorithms:
    - AES-256
      - OFB for symmetric encryption / decryption of digital voice and data
      - CBC for MACing of Project 25 OTAR
      - ECB for symmetric decryption of Project 25 OTAR
14. The RNC EMC conforms to all FCC requirements for this product.
15. The RNC EMC performs the following self-tests:
    - Power-up and on-demand tests
      - Cryptographic algorithm test: Each algorithm is tested by using a known key, known data, and if required a known IV. The data is then encrypted and compared with known encrypted data; the test passes if the final data matches

the known data, otherwise it fails. The encrypted data is then decrypted and compared with the original plaintext; the test passes if the decrypted data matches the original plaintext, otherwise it fails. The Encryption HW is inherently checked here as well.

  - Software/firmware test: The software firmware test calculates a checksum over the code. The checksum is calculated by summing over the code in 32 bit words. The code is appended with a value that makes the checksum value 0. The test passes if the calculated value is 0, otherwise it fails.

- Critical Functions tests:
  - General Purpose RAM Test: The general purpose RAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the RAM. The test passes if all values read from the RAM are correct, otherwise it fails.
  - Battery Test: The battery is checked for a failure condition. If it is under a critically low voltage, it fails, otherwise it passes.
  - Int EEPROM Test: All bytes in the Internal EEPROM are tested, akin to the General Purpose RAM Test. The test passes if all values read from the EEPROM are correct, otherwise it fails.
  - Ext EEPROM Test: All bytes in the External EEPROM are tested, akin to the General Purpose RAM Test. The test passes if all values read from the EEPROM are correct, otherwise it fails.
  - SCSI Test: The SCSI HW is tested for functionality. This is accomplished by write a series of values to the SCSI register and reading back. If all the values match the written ones, the test passes, otherwise it fails.
  - Key Database Test: The key database is tested to see if any keys exist. The test passes if any Traffic Keys exist, otherwise it fails.

  Powering the module off then on or resetting the module using the Reset service will initiate the power-up and on-demand self tests.
- Conditional tests
  - ANSI X9.17 Continuous Random Number Generator test: The continuous random number generator test is performed on the RNG within the module. For this RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to this RNG generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller.
  - LFSR Test: The LFSRs are tested by setting the feedback taps to a known value, loading them with known data, shifting the LFSR 64 times, and then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails.

16. The RNC EMC enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, or General Purpose RAM Test fails. This error state may be exited by powering the module off then on.
17. The RNC EMC enters an error state if the Software/Firmware test fails.
18. The RNC EMC outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.

19. The RNC EMC does not perform any cryptographic functions while in an error state.

## 5.2. Motorola Imposed Security Rules

1. The RNC EMC does not support multiple concurrent operators.
2. All cryptographic module services are suspended during key loading.
3. Upon detection of a critically low voltage condition on the switched power supply, the cryptographic module shall erase all plaintext keys.
4. Upon detection of a critically low voltage condition on the unswitched power supply, the cryptographic module shall erase all CSPs.
5. Upon detection of tamper, the cryptographic module shall erase all CSPs.
6. The module shall at no time output any Critical Security Parameters (CSPs)

# 6. Crypto Officer Guidance

## 6.1. Administration of the RNC EMC in a secure manner

The RNC EMC requires no special administration for secure use after it is set up for use in a FIPS approved manner. To do this, set the module's parameters to the settings listed in section 3 of this document via the Configuration service by using SCSI messages.

## 6.2. Assumptions regarding User Behavior

The RNC EMC has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

# 7. User Guidance

## 7.1. Approved Security Functions, Ports, and Interfaces available to Users

All RNC EMC services are available to the RNC EMC User. These are listed in section 9.2 of this document.

The only directly accessible interfaces to the module by the user are the Key Erase button and KVL port.  No other Physical Ports or Logical Interfaces are directly available to the RNC EMC User, only indirectly through the RNC in which the RNC EMC is installed. The User need not concern himself with them.

## 7.2. User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the RNC EMC.

## 8. Identification and Authentication Policy

The RNC EMC does not employ an authentication mechanism to control access to the module. It supports three roles: the user role, the cryptographic officer role, and the maintenance role.

# 9. Physical Security Policy

The RNC EMC is production grade and does not use any FIPS approved physical security mechanisms.

# 10. Access Control Policy

## 10.1. RNC EMC Supported roles

The RNC EMC supports both a User role and a Crypto Officer role, however these may both be accessed by one operator. This is done to allow the customer maximum flexibility in configuring his system for rekeying the EMC. This approach is consistent with the requirements of FIPS 140-2 Level 1 security. Both the user and the cryptographic officer have access to all the user services of the module and both of them can perform key entry via the KVL. During normal operation the RNC EMC implicitly selects the user/cryptographic officer role.

The maintenance role is defined as performing physical maintenance on the module after erasing the keys with the KVL.  The maintenance role is for firmware upgrades, replacing of the battery, and changing the SCSI ID only. The maintenance role is implicitly selected when the module is powered and the lid (maintenance interface) is open. Critical security parameters are automatically zeroized upon entering this state, and the module does not allow critical security parameters to be entered while in this state.

## 10.2. RNC EMC Services

- Show Status: Available through SCSI Commands to User and CO roles.
- Transfer Key Variable: Transfer key variables and/or zeroize key variables to/from the Key Database via a Key Variable Loader (KVL).  Available to User and CO Roles.
- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages. Available to User and CO Roles.
- Change Active Keyset: Modify the currently active keyset used for selecting keys by PID or CKR. Available to User and CO Roles.
- Encrypt Data: Encrypt data. Available to User and CO Roles.
- Decrypt Data: Decrypt data. Available to User and CO Roles.
- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, software firmware test, and critical functions test. Initiated by module reset or transition from power off state to power on state. Available without a Role.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR). Available to User and CO Roles.
- Zeroize all keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL)
- Non-Privileged APCO OTAR: Hello and Capabilities Key Management Messages may be performed without a Role.
- Reset Crypto Module: Soft reset of module to remove module from error states. Available without a Role.
- Configure: Download configuration parameters used to specify module behavior. Examples include enable/disable APCO OTAR rekey request, enable/disable KLK mode, etc. Available without a Role.

- Key/Keyset Check: Obtain status information about a specific key/keyset. Status information may include whether a key with a given key identifier exists, a list of key identifiers for all valid keys currently in the module, a list of valid keyset names, or a list of valid keyset identifiers.  Available without a Role.
- Battery Replacement: Physical replacement of the coin-cell batteries under the EMC lid.
- Firmware Upgrade: Physical replacement of the firmware chip where the running software is stored.
- SCSI ID Change: Physical change of the SCSI ID on the DIP switches under the EMC lid.

### 9.3 Critical Security Parameters (CSPs)

**Table 2: CSP Definition**

| CSP Identifier | Description |
|---|---|
| Plaintext Traffic Encryption Keys ( TEKs) | Keys used for voice and data encryption |
| Plaintext Key Encryption Keys ( KEKs ) | Keys used for encryption of keys in OTAR |

### 9.4 CSP Access Types

**Table 3: CSP Access Types**

| CSP Access Type | Description |
|---|---|
| Retrieve key | Retrieves plaintext TEKs or KEKs from the database |
| Store key | Stores plaintext TEKs or KEKs in  the database |
| Erase Key | Marks encrypted TEK or KEK data in key database as invalid |

**Table 4: CSP versus CSP Access**
**(Shaded Services are available to User or CO role only)**

| | CSP Access Operation | | | Applicable Role | | | |
|---|---|---|---|---|---|---|---|
| User Service | Retrieve Key | Store Key | Erase Key | User Role | Crypto Officer Role | Maintenance Role | No Role Required |
| 1. Transfer Key Variable | | X | X | X | X | | |
| 2. Privileged APCO OTAR | X | X | X | X | X | | |
| 3. Change Active Keyset | | | | X | X | | |
| 4. Encrypt Data | X | | | X | X | | |
| 5. Decrypt Data | X | | | X | X | | |
| 6. Zeroize Selected Keys | | | X | X | X | | |
| 7. Show Status | | | | X | X | | |
| 8. Initiate Self Tests | | | | | | | X |
| 9. Zeroize All Keys | | | X | | | | X |
| 10. Non-Privileged APCO OTAR (not for key entry) | | | | | | | X |
| 11. Reset | | | | | | | X |
| 12. Configure Parameters | | | X | | | | X |
| 13. Key/Keyset Check | | | | | | | X |
| 14. Battery Replacement | | | | | | X | |
| 15. Firmware Upgrade | | | | | | X | |
| 16. SCSI ID Change | | | | | | X | |

## 11. Mitigation of Other Attacks Policy

The RNC EMC is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.

## 12. Definitions, Acronyms, Abbreviations

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CKR | Common Key Reference |
| CSP | Critical Security Parameters |
| DES | Data Encryption Standard |
| EEPROM | Electrically Erasable Programmable Read Only Memory |
| EMC | Encryption Module Controller |
| IV | Initialization Vector |
| KG | Key Generator |
| KMM | Key Management Message |
| KVL | Key Variable Loader |
| OFB | Output Feedback |
| OTAR | Over The Air Rekeying |
| PIC | PIC16C57 RISC Microcontroller by Microchip Corp |
| PID | Physical ID |
| RAM | Random Access Memory |
| RNC | Radio Network Controller |
| SCSI | Small Computer System Interface |
| SLN | Storage Location Number |