3.0A RNC EMC Security Policy

LAND MOBILE PRODUCTS SECTOR
Radio Network Solutions Group

Version 01.02.00

Last Revision: December 29, 1999

Repository Information

Location: /vobs/emc_kmc_dcc/docs/fips
Filename: RNC EMC Security Policy

Revision History

Revision	Date	Author	Comments
01.00.00	10/11/96	Bhavesh Shah	Initial Creation
01.00.01	1/7/97	Brett Szudy	Changed for Domus requests
01.00.02	11/05/97	Brett Szudy	Added erasing of EEPROM keys req. for maintenance role
01.01.00	6/25/99	Brett Szudy	Updates for APCO OTAR release
01.02.00	12/29/99	Brett Szudy	Minor deletion for FIPS

Table of Contents

1 Introduction

1.1 Purpose

This document describes the FIPS 140-1 security policy requirements for Motorola's Land Mobile Products Sector's Encryption Module Controller (EMC) which will be used for the Radio Network Controller (RNC).

1.2 Definitions, Acronyms, Abbreviations

CKR	Common Key Reference
DES	Data Encryption Standard
EEPROM	Electrically Erasable Programmable Read Only Memory
EMC	Encryption Module Controller
IV	Initialization Vector
KG	Key Generator
KMM	Key Managagement Message
KPK	Key Protection Key
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
SRDI	Security Related Data Items

1.3 References

- "EMC SCSI Interface" Version 02.04.00 /vobs/emc_kmc_dcc/docs

2 Roles and Services

The cryptographic module does not distinguish between the user role and the crypto officer role. 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 140-1 Level 1 security. The maintenance role is for flash upgrades, replacing of the battery, and changing the SCSI ID only. All services in the module are provided without user authentication. Both user and the crypto officer can perform the following services - encryption, decryption, indexing, key erase, and key entry.

3 Security Rules

This section documents the security rules used by the cryptographic module to implement the security requirements of a FIPS 140-1 Level 1 module.

Note: Rules are contained in the number paragraphs and are shown in italics. Other information is included for background purposes only.

1. *Upon detection of a low voltage power condition the cryptographic module shall erase all plaintext keys and critical data.*

   This rule ensures that all plaintext keys will be erased if the module is turned off without powering down.

2. *Upon detection of a low battery when module is powered down, the cryptographic module shall erase the KPK.*

   The plaintext keys should have already been erased earlier due to power down.

3. *The module shall not at any time output any security related data items (SRDIs) in plaintext.*
4. *At power down, the cryptographic module shall erase all plaintext SRDIs except the Key Protection Key (KPK). Note that a 6V battery will power the shift register to retain the KPK when the module's processor is powered down.*
5. *The cryptographic module shall erase all the plaintext keys, the KPK and critical information when the Emergency Erase Switch is activated or a tamper condition is detected. It shall also reset the KGs and the PIC.*
6. *KPK generation in the cryptographic module shall be done at a random event like entering KVL mode.*

   This rule ensures that the KPK is random because entering a KVL mode is a random event and the KPK generation is based on the 68HC11K4's free running counter.

7. *The cryptographic module shall test the random number generator. The first IV generated at powerup is not used for encryption but saved for comparison with the next IV generated.*

   This ensures that the random number generator is working correctly.

8. *Keys loaded into the cryptographic module shall be accompanied by a valid key tag. Also, CRCs over each key will be stored encrypted with the encrypted key data in the EEPROM so that all loaded keys are protected.*

   Keys may be loaded into the module directly through the Key Variable Loader (KVL) port (in PID mode). Regarding KVL keyloading, the EMC will accept keys only when one of its available algorithms matches the KVL's algorithm type. Keys for which the stored CRC does not match the computed CRC will be erased.

   Keys may also be loaded into the module via OTAR KMM messages coming from the KMF via the host or KVL (in SLN/CKR mode). The EMC shall accept KMM rekey messages from host only if they are encrypted and authenticated. KVL can send clear and non-authenticated KMMs to the EMC.

9. *Only traffic encryption keys shall be used in the encryption of message traffic.*
10. *The cryptographic module shall be capable of encrypting and decrypting message traffic using DES operated in the Output Feedback Mode (OFB).*

    The module is capable of supporting two separate algorithms simultaneously. However only one will be used at a time, and within the modules that are being certified, one of them will be DES.

11. *Upon the application of power or the receipt of a Reset command the Cryptographic module shall perform the following tests:*
    - *Battery Test*
    - *RAM Test*
    - *Program Memory Test*
    - *Int EEPROM Test*
    - *Ext EEPROM Test*
    - *KG/PIC Security Tests (includes Cryptographic Algorithm Known Answer Test)*
    - *SCSI Test*
    - *Key Database Test*
12. *The operator shall be capable of repeating the above tests by cycling the power. The cryptographic module shall also provide support of a "Reset" command, which when received, will invoke the above tests.*

4 Security Related Data Items

There are two types of security related data items (SRDIs). These are:

- Traffic Encryption Keys (TEK)
- Key Encryption Keys (KEK)
- Warm Start Key
- Temporary Keys
- The Key Protection Key (KPK)

5 Security Level Objectives

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

6 Services to SRDI Relationships

The following depicts the access modes provided by the module and that services access to SRDIs:

a)Load Key: A traffic key is received directly from a KVL (in PID mode) or OTAR KMMs (in SLN/CKR mode). The keytag and CRC are verified to ensure that the key is valid and has been received error free. A traffic key may also be received via encrypted and authenticated OTAR KMM messages that come from the host. The valid plaintext key is then loaded into RAM, encrypted using the KPK and stored in the EEPROM.

b)Erase Key: Traffic or shadow keys are erased from either RAM or EEPROM or both, depending on the cause of the action. All plaintext keys are erased from RAM on Shutdown. Specific traffic keys are erased from RAM and EEPROM by KVL (in PID mode or SLN/CKR mode) or via OTAR KMMs from host (NOTE: The keys must be erased using the KVL before accessing the maintenance interface, in order to be FIPS compliant. This is to erase the keys backed up in EEPROM, which a maintenance operator should not have access to). When tamper condition is detected (or the Emergency Erase Switch is activated), all plaintext keys are erased from RAM and the KPK is erased upon detection of tamper.

c)Select Key: The specified key is loaded into the Key Generator specified in the keytag for the key.

d)Wrap Key: The specified key is encrypted using the KPK and the cipher text key is stored in EEPROM.

e)Unwrap Key: As a result of detecting a valid KPK at powerup, all ciphertext keys stored in EEPROM are decrypted using the KPK and stored in RAM.

For detail descriptions on user services and data formats please refer to following documents -

- EMC SCSI Interface

7 Operator Access

The following is a table of what access an operator has to the critical security parameters while performing one of the cryptographic functions: Encryption, Decryption, Indexing, Key Entry, or Key Erase. Note that the only operators authorized are the persons in the User or Crypto Service Roles

TABLE 1 Access of User/Crypto Officer

		Critical Security Parameter			
		Traffic Keys	**KPK**	**System Keys**	**WarmStart/ KEK/ Temp**
Cryptographic Service	**Enc/Dec**	Use	-	Use	-
	Indexing	-	-	-	-
	Key Entry	Write, Delete	Use	Write	Write,Use,Delete
	Key Erase	Delete	Delete	Delete	Delete