MOTOROLA

3.0A DIU EMC Security Policy

LAND MOBILE PRODUCTS SECTOR
Radio Network Solutions Group

Version 01.00.00

Last Revision: June 28, 1999

Repository Information

Location: /vobs/diu/emc/docs/APCO_OTAR/FIPS/
Filename: DIU EMC OTAR Security Policy

Revision History

Revision	Date	Author	Comments
01.00.00	6/28/99	Bhavesh Shah	Initial Creation - Adapted from 3.0 Security Policy

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 Digital Interface Unit (DIU).

1.2 Definitions, Acronyms, Abbreviations

CKR	Common Key Reference
DES	Data Encryption Standard
DIU	Digital Interface Unit
EEPROM	Electrically Erasable Programmable Read Only Memory
EMC	Encryption Module Controller
IV	Initialization Vector
KG	Key Generator
KMM	Key Management 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
RSS	Radio Service Software
SLN	Storage Location Number
SRDI	Security Related Data Items

1.3 References

- Astro-Tac Digital Interface Unit Encryption Cartridge Instruction Manual part number 68P81090E45-B.

2 Roles and Services

In order to meet FIPS Level 2 secure roles & services, the DIU encryption module supports two forms of the crypto officer role & one form of the user role. The roles are implemented & configured via Radio Service Software (RSS). For information on implementation & configuration see the *Astro-Tac Digital Interface Unit Encryption Cartridge Instruction Manual* pages 3-8 through 3-13. Once secure roles & services have been installed via RSS, the user must login via the front panel of the DIU as one or more of the following to gain access to the encryption module: CRYPTO MAINTENANCE, CRYPTO OFFICER or USER. When the user is completed with their desired encryption function, they must log out from their role via the front panel of the DIU. Once the passwords have been initialized via RSS, users can change their given passwords at the DIU front panel. For information on the procedures of logging in and out of the roles as well as changing passwords see the *Astro-Tac Digital Interface Unit Encryption Cartridge Instruction Manual* pages 3-21 & 3-22. The encryption module can accept up to 10 USER roles, 2 CRYPTO OFFICER roles and 1 CRYPTO MAINTENANCE role. A brief description of each follows.

2.1 CRYPTO MAINTENANCE officer role

The DIU EMC supports only one CRYPTO MAINTENANCE officer role.

The only service allowed when logged in as this role is RSS maintenance.

The user must login as the CRYPTO MAINTENANCE officer via the DIU front panel whenever they wish to use RSS. If the user has not logged in as the CRYPTO MAINTENANCE officer and attempts to read the RSS from the DIU, the encryption parameters will be denied by the EMC, and the user will not have access to those screens in the RSS. Once the user logs in as the CRYPTO MAINTENANCE officer, all of the keys in the module are ZEROIZED. Basically the user can setup the encryption parameters in the Encryption Configuration screen, and change passwords in the FIPS Roles Users screen. They CANNOT however, view the passwords. These are considered critical security parameters and are not uploaded out of the encryption module at any time.

The main purpose here is for either initial installation of the encryption module, or to reconfigure encryption parameters and secure role passwords after a loss of ram. For example, if the module was just tampered with, the passwords and other encryption information has been erased. As a result, the user must login as the CRYPTO MAINTENANCE officer with the default maintenance password (hard coded in the module) and read up the information in RSS (see the *Astro-Tac Digital Interface Unit Encryption Cartridge Instruction Manual* page 3-40 for this default password). They must then setup all of the passwords that are necessary, and program the module. Once this is done they must log out of the CRYPTO MAINTENANCE officer role and inform all of the users & other crypto officers of their new passwords. All of the users should then individually change their passwords via the front panel of the DIU. The encryption cartridge is now ready for operation. Note that logging out from the CRYPTO MAINTENANCE officer role also ZEROIZES all of the keys. This same procedure is also followed at initial installation of the encryption module.

2.2 CRYPTO OFFICER role

The DIU EMC supports up to two CRYPTO OFFICER roles.

The services allowed when logged in as this role are the transmitting and receiving of secure voice, and the rekeying of the key database.

The user must login as a CRYPTO OFFICER via the DIU front panel if they wish to allow the module to transmit or receive secure voice. The user must also login as the CRYPTO OFFICER in order to rekey the module via KVL. For OTAR, the user physically does NOT have to be logged in. The messages coming from KMF are authenticated and encrypted, so a session from KMF can be essentially considered as a Crypto Officer session. Refer to the *Astro-Tac Digital Interface Unit Encryption Cartridge Instruction Manual* pages 3-16 & 3-17 for more information on the rekeying procedure. Once the user is finished rekeying or the voice session is over, they must log out of the CRYPTO OFFICER role.

Logging in and out of the CRYPTO OFFICER role does not zeroize keys.

2.3 USER role

The DIU EMC supports up to ten USER roles.

The services allowed when logged in as this role are the transmitting and receiving of secure voice.

The user must login as a USER via the DIU front panel if they wish to allow the module to transmit or receive secure voice. Once the voice session is over, the user must log out of the USER role.

Logging in and out of the USER role does not zeroize keys.

2.4 MAINTENANCE role

The maintenance role is for physical maintenance only and is used for flash upgrades and replacing of the battery only. 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. In addition, the CRYPTO MAINTENANCE Officer should also use RSS to reset the login passwords to a default value before the maintenance interface is accessed. This is to erase the login passwords backed up in EEPROM, which a maintenance officer should not have access to.

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. It should be noted that the cryptographic module is only operating in a FIPS approved mode when the DES-OFB algorithm is used for encryption and decryption.

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).*
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 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.*

   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. Within the modules that are being certified, one of them will be DES.

11. *Upon the application of power or a hardware reset, 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)*
    - *Key Database Test*
    - *Clear Bypass Test*
12. *The operator shall be capable of repeating the above tests by cycling the power.*

4 Security Related Data Items

There are three 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)
- The secure operator role passwords.

5 Security Level Objectives

The cryptographic module meets the requirements applicable to overall Level 1 security of FIPS 140-1, Level 2 secure roles & services, and Level 1 physical security.

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)Initialize Password: A password is initialized via RSS by the CRYPTO MAINTENANCE officer.

e) Change Password: Passwords can be changed by users from the front panel of the DIU.

f) Login/Logout from password: Users can login and logout of roles by entering their passwords for verification via the DIU front panel.

g)Wrap Key/Password: The specified key/password is encrypted using the KPK and the cipher text key is stored in EEPROM.

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