MOTOROLA

R3.0 ASTRO Digital Subscriber Cryptographic Module Security Policy

version 1.2

last revision January 6, 1998

A. *Scope of Document*

This document describes the FIPS 140-1 security policy requirements for Motorola's Land Mobile Products Sector's cryptographic module used in the ASTRO Digital SABER™ and SPECTRA™ radios. The encryption module has been revised to support system release R3.0. This release required hardware and software changes to an existing module to support a new encryption algorithm called DES-OFB.

B. *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 radios. The cryptographic module will authenticate a valid user and will allow that user access to certain services. Other services will be provided without user authentication. Those services which do require authentication will be identified in the rules below. This approach is consistent with the requirements of FIPS 140-1 Level 2 security.

C. *FIPS Approved Operational Modes*

The cryptographic module includes modes of operation which are not FIPS approved. This section documents the conditions that must be met for the module to be used in a FIPS 140-1 approved mode of operation.

1. *The cryptographic module shall have OTAR disabled.*

2. *The cryptographic module shall have KLK generation disabled.*

3. *The cryptographic module shall use DES for encryption and decryption in the following approved modes: CFB or OFB.*

4. *Use of the following proprietary algorithms and modes is not FIPS approved: DES-XL, DVI-XL, DVI-SPFL, DVP-XL, and DVP.*

D. *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[1].

1. *The cryptographic module shall not provide User Role services until the operator has entered the PIN code stored in the cryptographic module.*

   Services provided within the User Role or Crypto Officer Role are not available until the operator has entered the PIN code currently stored in the cryptographic module. Crypto Officer Role services are available through use of a Key Variable Loader.

---

[1] Rules are contained in the number paragraphs and are shown in italics. Other information is included for background purposes only.

Services requiring prior operator authentication include:

a) Change PIN Code
b) Enter ASTRO Mode
c) Enter Securenet Mode
d) Enter Encrypt Mode
e) Enter Decrypt Mode
f) Perform Internal Key Load
g) Perform Key Variable Loader 'External' Key Load
h) Receive RSS parameters

2. *The cryptographic module will continue to provide User Role and Crypto Officer Role services after the PIN code has been entered until the module has been powered down.*

3. *User Role services are not available during a KVL load sequence.*

4. *An operator who has not entered a valid PIN code is permitted to command the module to erase all keys and reset the PIN code to the manufacturers default value.*

This rule permits a module in which the stored PIN code is no longer known to be reset so that the module can be returned to service. If this is done the keys must be reloaded into the radio before it can be returned to service.

5. *After a sufficient number of consecutive unsuccessful PIN code validation attempts have occurred, the cryptographic module shall erase all keys.*

6. *Upon detection of a low voltage power condition the cryptographic module shall erase all plaintext keys.*

This rule ensures that all plaintext keys will be erased if the module is turned off without receiving a power down command. This rule does not apply to the Key Loss Key, which is stored red in EEPROM. KLK generation can be disabled via programmable parameters.

7. *Upon detection of a critically low voltage power condition the cryptographic module shall erase all plaintext keys and the KPK.*

This rule ensures that the KPK will be actively erased if the battery is removed long enough such that the tamper responding circuitry will not function. This rule does not apply to the KLK.

8. *The module shall not at any time output any security related data items (SRDIs).*

9. *At power down, the cryptographic module shall erase all unencrypted SRDIs except the Key Protection Key (KPK) and KLK. Note that a trickle of power is needed to retain the KPK when the module's processor is powered down.*

10. *The cryptographic module shall erase all keys (both encrypted and unencrypted), the KPK, and the PIN code when a "All Key Erase Including Password" command is received.*

11. *Keys loaded into the cryptographic module shall be accompanied by a valid key tag. Also, CRCs stored over blocks of EEPROM shall be designed such that all loaded keys are protected.*

Keys in which the key tag identifies the target algorithm as other than one supported by the module will not be used. Blocks in which the stored CRC does not match the computed CRC will be erased.

Keys may be loaded into the module directly through the Key Variable Loader (KVL) port. Regarding KVL keyloading, the EMC will accept keys only when one of its available algorithms matches the KVL's algorithm type.

12. *Only traffic encryption keys shall be used in the encryption of message traffic.*

The only exception to this rule is the allowance of the use of field test keys for message traffic. These field test keys are used only for special development purposes.

13. *The cryptographic module shall optionally be capable of encrypting and decrypting message traffic using DES operated in the single bit Cipher Feedback Mode (CFB) as described in FIPS 81. The cryptographic module shall optionally 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, the module will contain one or both of the DES devices.

14. *Upon the application of power or the receipt of a Reset command the Cryptographic module shall perform the following tests:*

    a) *ROM Test*
    b) *RAM Test*
    c) *Cryptographic Algorithm Known Answer Test*

15. *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.*

16. *KPK generation in the cryptographic module shall be done at a random event like during an external keyload.*

17. *The cryptographic module shall test the random number generator.*

E. Security Related Data Items

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

a) Traffic/OTAR Encryption Keys (TEKs/KEKs)
b) The Key Protection Key (KPK)
c) The User's PIN code

F. Security Level Objectives

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

G. Services to SRDI Relationships

The following table depicts the relationship between the services provided by the module and that services access to SRDIs.

The access modes shown in this table are defined as follows:

a) Load Key: A traffic key is received directly from a Key Variable Loader (KVL). The keytag and CRC are verified to ensure that the key is valid and has been received error free, and the valid key is then loaded into RAM.

b) Erase Key: Traffic or shadow keys are erased from either RAM or E^2PROM or both, depending on the cause of the action. All plaintext Keys are erased from RAM on Shutdown or Reset. All keys are erased from both RAM and E^2PROM on command, and during certain error conditions. Specific traffic keys or shadow keys are erased from RAM and E^2PROM on command. When tamper response is enabled, 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 E^2PROM.

e) Unwrap Key: As a result of a successful validation of the entered PIN code, all ciphertext keys stored in E^2PROM are decrypted using the KPK and stored in RAM.

f) Wrap PIN: The PIN code is encrypted using an expanded version of the PIN, and is then stored in E^2PROM.

g) Unwrap PIN: The cipher text stored in E^2PROM is decrypted using an expanded version of the PIN so that it can be compared to the PIN code entered.

Table 1 Services Versus SRDI Modes of Access

User Service[2]	Load Key	Erase Key	Select Key	Wrap Key	Unwrap Key	Wrap PIN	Unwrap PIN
1. Reset ($F9)		X					
2. Enter Shutdown State ($F8)		X					
3. Validate PIN Code ($AF)		X			X		X
4. Change PIN Code ($AE)		X				X	X
5. Perform Internal Key Load ($AB)			X				
6. Perform Key Erase ($AC)		X					
7. External Key Load (Valid KVL Handshake)	X	X		X			
8. Receive RSS Parameters ($B0)		X					

[2] A brief description of each User Service can be found in "Host_EMC_SPI_Message_Formats".