Security Policy: MCC7500 Secure Card Crypto Engine Cryptographic Module

Version R01.01.22

Date: June 3, 2009

Table of Contents

1. INTRODUCTION 3

1.1. PURPOSE 3
1.2. SCOPE 3
1.3. DEFINITIONS 3
1.4. OVERVIEW 4
1.5. MCC7500 SCCE HARDWARE / SOFTWARE VERSION NUMBERS 4
1.6. MCC7500 SCCE IMPLEMENTATION 4
1.7. MCC7500 SCCE CRYPTOGRAPHIC BOUNDARY 5

2. FIPS 140-2 SECURITY LEVEL 7

3. APPROVED OPERATIONAL MODES 8

4. GUIDANCE DOCUMENTATION 9

4.1. ADMINISTRATION OF THE MCC7500 SCCE IN A SECURE MANNER (CO) 9
4.2. ASSUMPTIONS REGARDING USER BEHAVIOR (CO) 9
4.3. APPROVED SECURITY FUNCTIONS, PORTS, AND INTERFACES AVAILABLE TO USERS 9
4.4. USER RESPONSIBILITIES NECESSARY FOR SECURE OPERATION 9

5. SECURITY RULES 11

5.1. FIPS PUB 140-2 IMPOSED SECURITY RULES 11
5.2. MOTOROLA IMPOSED SECURITY RULES 15

6. PHYSICAL SECURITY 16

6.1. MECHANISMS 16
6.2. MAINTENANCE 16

7. ROLES AND SERVICES 17

7.1. MCC7500 SCCE SUPPORTED ROLES 17
7.2. MCC7500 SCCE SERVICES 17

8. MODULE INTERFACES 19

9. AUTHENTICATION 20

10. ACCESS CONTROL 21

10.1. SECURITY RELATED DATA ITEMS (CSPS) 21
10.2. CSP ACCESS TYPES 21
10.3. ACCESS MATRIX 22

11. MITIGATION OF ATTACKS 23

1. Introduction

1.1. Purpose

This Security Policy is the precise specification of the security rules under which the MCC7500 Secure Card Crypto Engine Cryptographic Module must operate.

1.2. Scope

This Security Policy specifies the security rules under which the MCC7500 Secure Card Crypto Engine Cryptographic Module, herein identified as the MCC7500 SCCE, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 as well as those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators
2. module services
3. security related data items (critical security parameters, CSPs).

1.3. Definitions

AIS		Archiving Interface Server
ALGID		Algorithm Identifier
CBC		Cipher Block Chaining
CFB		Cipher Feedback
CKR		Common Key Reference
CO		Crypto Officer
CSP		Critical Security Parameter (security related data items)
DES		Data Encryption Standard
DPRAM		Dual Port RAM
ECB		Electronic Code Book
IV		Initialization Vector
KEK		Key Encryption Key
KID		Key Identifier
KLK		Key Loss Key
KMM		Key Management Message
KPK		Key Protection Key
KVL		Key Variable Loader
LFSR		Linear Feedback Shift Register
MAC		Message Authentication Code
OFB		Output Feedback
OTAR		Over The Air Rekeying

PCI		Peripheral Component Interconnect
PRNG		Pseudo Random Number Generator
RNG		Random Number Generator
SCCE		Secure Card Crypto Engine
TEK		Traffic Encryption Key
QUICC		Quad Universal Integrated Communications Controller

1.4. Overview

As Motorola radio systems migrate from traditional circuit switched infrastructure to packet based infrastructure, new cryptographic modules are needed to replace those in the current system. Astro 6.7 represents the first Astro release to support end-to-end encryption to the console in the packet-based infrastructure. This has been made possible only with the development of the packet based MCC7500 console. It is within this console that the MCC7500 Secure Card resides. Also with the release of Astro 6.7 an audio archiving device called the secure Archiving Interface Server (AIS) is being released which also contains the MCC7500 Secure Card providing end-to-end encryption services.

The MCC7500 Secure Card Crypto Engine Cryptographic Module is a sub portion of a PCI express card which provides encryption services for up to 60 audio streams for the Secure Operator Position (B1908) and Secure Archiving Interface Server (B1918). Each Secure Operator Position will contain one Secure Card providing encryption services for 60 simultaneous audio streams. Each Secure AIS will contain 1 or 2 Secure Cards providing encryption services for 60 or 120 audio streams, respectively. The Spare Crypto Card (B1924) may be used to upgrade an Operator Position or AIS.

1.5. MCC7500 SCCE Hardware / Software version numbers

FIPS Validated Hardware Version Numbers	FIPS Validated Software Version Numbers
R01.00.00	R02.00.00 R02.01.10 R02.01.11 R01.11.00

1.6. MCC7500 SCCE Implementation

The MCC7500 SCCE is implemented as a multi-chip embedded module as defined by FIPS PUB 140-2.

1.7. MCC7500 SCCE Cryptographic Boundary

The MCC7500 SCCE's crypto boundary is defined as the portion of the MCC7500 Secure Card's PCI printed circuit board containing the processors, memory, keyloader interface, associated power and physical security circuitry.

Figure 1: MCC7500 Secure Card front. The crypto boundary is defined by the metallic shield.

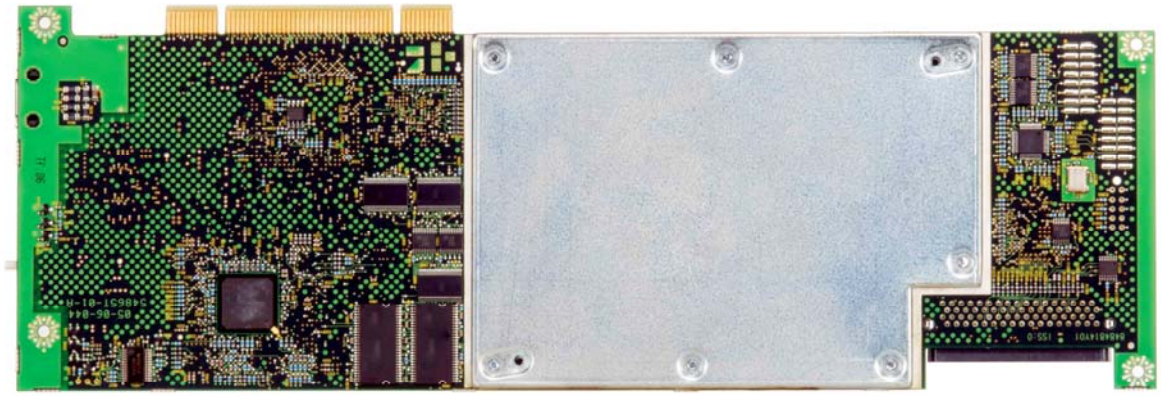

Figure 2: MCC7500 Secure Card back. The crypto boundary is defined by the metallic shield.

2. FIPS 140-2 Security Level

The MCC7500 SCCE is designed to meet FIPS 140-2 security at the levels indicated in the table below.

Table 2-1

FIPS 140-2 Security Requirements Section	Level
Overall Security Level	1
Cryptographic Module Specification	1
Ports and Interfaces	1
Roles Services and Authentication	2
Finite State Machine 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	1

3. Approved Operational Modes

The MCC7500 SCCE provides modes of operation that are not Approved. Below is a list of configuration settings that are required to provide FIPS 140-2 approved operation. To run the MCC7500 SCCE in Approved mode the following steps must be taken (note: 1 and 2 default to FIPS approved settings at initial power up):

1. Key Loss Key (KLK) generation disabled

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

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

- ADP

4. Guidance Documentation

4.1. Administration of the MCC7500 SCCE in a secure manner (CO)

The MCC7500 Secure Card can be shipped already installed in the PCI slot of the console or AIS. In this case, the MCC7500 SCCE requires no special administration for secure use assuming the settings in section 3 of this document have not been modified from the default (FIPS approved state) and only FIPS approved encryption algorithms are being used. If the settings have been modified, they must be returned to the FIPS approved state to place the module in FIPS approved mode of operation.

If the Secure Card (ordered as a B1824 Spare Crypto Card) is not installed in the PCI slot upon shipment (i.e. Operator Position or AIS upgrade to secure) the user must install the cards in a secure manner. With the console or AIS powered off, the cards must be placed in the PCI slot without removing the tamper shield. At initial power up the cards will be in FIPS approved mode of operation (assuming FIPS approved algorithms are purchased). If the configuration settings in section 3 of this document are modified, the card is no longer in FIPS approved mode. To return to FIPS approved mode, follow the guidelines in section 3 of this document.

4.2. Assumptions regarding User Behavior (CO)

The MCC7500 SCCE has been designed in such a way that very few assumptions regarding User Behavior have been made that are relevant to the secure operation of the module. It has been assumed that the user will keep all CSPs private. It has also been assumed that the user will deny use of the module to unapproved personnel while the user is logged in as the User or CO.

4.3. Approved Security Functions, Ports, and Interfaces available to Users

All MCC7500 SCCE services are available to the user assuming the appropriate role. These are listed in section 7 of this document.

Only the KVL port (used for electronic key entry and OTAR store and forward) is directly available to the MCC7500 SCCE user. This interface is logically disconnected when the user is not logged in with the appropriate role.

4.4. User Responsibilities necessary for Secure Operation

The User and CO must keep all CSPs private. The User and CO must not allow unapproved operation of the module while logged in. The user must ensure the module is operating in the FIPS approved mode as discussed in section 3 of this document.

5. Security Rules

This section lists the security rules enforced by the MCC7500 SCCE. The rules are separated into two categories, 5.1) those imposed by FIPS PUB 140-2 and, 5.2) those imposed by Motorola.

5.1. FIPS PUB 140-2 Imposed Security Rules

See section 8 for a description of the module's interfaces.

1. The MCC7500 SCCE inhibits all data output via the data output interface whenever an error state exists and during self-tests.

2. The MCC7500 SCCE logically disconnects the output data path from the circuitry and processes when performing key generation, electronic key entry, or key zeroization.

3. Authentication data (e.g. PINs) and other critical security parameters are entered / output in plaintext form.

   AND

   Secret cryptographic keys are entered / output over a physically separate port.

4. The MCC7500 SCCE supports a User role and a Cryptographic Officer role. These two roles have the same set of services.

5. The MCC7500 SCCE re-authenticates a role when it is powered-up after being powered-off.

6. The MCC7500 SCCE provides the following services requiring a role:

   - Transfer Key Variable
   - Privileged APCO OTAR
   - Change Password
   - Encrypt
   - Decrypt
   - Zeroize Selected Keys
   - Zeroize All Keys
   - Programming Upgrade

7. The MCC7500 SCCE provides the following services not requiring a role:

   - Validate Password
   - Tamper[1] Response
   - Non-Privileged APCO OTAR
   - Reset Crypto Module
   - Shutdown Crypto Module
   - Download Config Parameters
   - Query Config Parameters
   - Traffic Algorithm Query

8. The MCC7500 SCCE enforces Role-Based identification.

9. The MCC7500 SCCE implements all software using high-level language except the limited use of low-level language to enhance performance.

10. The MCC7500 SCCE protects secret keys and private keys from unauthorized disclosure, modification and substitution.

11. The MCC7500 SCCE provides a means to ensure that a key entered into, stored within, or output from the MCC7500 SCCE is associated with the correct entities to which the key is assigned. Each key in the MCC7500 SCCE is entered and stored with the following information:

    - Key Identifier (KID) – 16 bit identifier
    - Algorithm Identifier (ALGID) – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Common Key Reference (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 KID/ALGID, CKR/Keyset or KID/ALGID/CKR.

12. The MCC7500 SCCE denies access to plaintext secret and private keys.

[1] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

13. The MCC7500 SCCE provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters.

14. The MCC7500 SCCE supports the following FIPS approved algorithms:

    - AES
      - OFB for symmetric encryption / decryption of digital voice and data
      - CBC for authentication of Project 25 OTAR
      - ECB for symmetric decryption of Project 25 OTAR
    - 3DES
      - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
      - CBC for symmetric decryption software upgrades
      - TDES MAC (vendor affirmed) for authentication of software upgrades
    - SHA-1
      2 Password hashing for internal storage
    - ANSI x9.31 PRNG
      3 IV and KPK generation

15. The MCC7500 SCCE performs the following self-tests:

    - Power-up and on-demand tests
      - Cryptographic Algorithm Test: Each algorithm is tested using a known key, known data and, if required, known IV. The known clear data is encrypted with the known key and tested against the known encrypted data. The encrypted data is then decrypted and tested against the original known clear data. The test passes if both the encrypted and the decrypted known data match their corresponding counterparts, otherwise the test fails and the module will require a hard reset.
      - 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 and the module will need to be reprogrammed.
      - Critical Functions Test:

- 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, then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails and the module will require a hard reset.

- 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 and the module will require a hard reset.

- DPRAM Test: The DPRAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the DPRAM. The test passes if all values read from the DPRAM are correct, otherwise it fails and the module will require a hard reset.

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

- Software/Firmware Load Test: A MAC is generated over the code when it is built using 3DES-CBC. Upon download into the module, the MAC is verified. If the MAC matches the test passes, otherwise it fails and the module will need to be reprogrammed.

- Continuous Random Number Generator Test: The continuous random number generator test is performed on 3 RNGs within the module. The first is a hardware RNG which is used to seed the ANSI X9.31 PRNG and the maximal length 64-bit LFSR. The second is an implementation of Appendix C ANSI X9.31 which is used for key generation, and the third is a maximal length 64-bit LFSR which is used for IV generation. For each RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. Successive calls to any one of the RNGs generate 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 and the module will require a hard reset.

16. The MCC7500 SCCE enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, or the General Purpose RAM Test fails. This error state may be exited by powering the module off then on.

17. The MCC7500 SCCE enters a non-fatal error state if the Software/Firmware test fails. This state is exited as soon as an error indicator is output via the status interface and the module enters programming mode.

18. The MCC7500 SCCE enters an error state if the Software/Firmware Load test fails. This state is exited as soon as an error indicator is output via the status interface.

19. The MCC7500 SCCE outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.

20. The MCC7500 SCCE does not perform any cryptographic functions while in an error state.

5.2. Motorola Imposed Security Rules

The MCC7500 SCCE:

1. Does not support a bypass mode.

2. Does not support multiple concurrent operators.

3. Will continue to provide User Role and Crypto Officer Role services until the module has been powered down.

4. Will suspend all services during key loading.

5. Will zeroize all keys from the Key Database after a sufficient number (15) of consecutive, unsuccessful user login attempts.

6. Shall erase all plaintext keys upon detection of a critically low voltage on the switched (SW_3.3) power supply.

7. Shall erase all security related data items (CSPs, see section 10.1) upon detection of a critically low voltage condition on both the switched (SW_3.3) and continuous (CONT_3.3) power supply.

8. Shall erase all CSPs upon detection of tamper[2].

9. Shall at no time output any CSPs.

[2] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

6. Physical Security

6.1. Mechanisms

The MCC7500 SCCE is production grade and does not use any FIPS approved physical security mechanisms.

6.2. Maintenance

No maintenance is required to ensure physical security.

7. Roles and Services

7.1. MCC7500 SCCE Supported Roles

The MCC7500 SCCE supports two (2) roles:

- User Role
- Crypto Officer (CO) Role

7.2. MCC7500 SCCE Services

- Transfer Key Variable: Transfer Key variables to the Key Data Base (KDB) of the MCC7500 SCCE via a Key Variable Loader (KVL). Available to User and CO roles Service input: KMM. Service output: KMM.
- Change Password: Modify the current password used to identify and authenticate the User and CO Roles. Available to User and CO Roles. Service input: DPRAM message (opcode; old password; new password). Service output: DPRAM message (opcode; status).
- Validate Password: Provides a method of controlling use of CSPs. Available to all roles. Service Input: DPRAM message.
- Encrypt: Encrypt digital voice or data. Available to User and CO Roles. Service input: DPRAM message (opcode, red data). Service output: DPRAM message (opcode, black data, status).
- Decrypt: Decrypt digital voice or data. Available to User and CO Roles. Service input: DPRAM message (opcode, black data). Service output: DPRAM message (opcode, red data, status).
- Traffic Algorithm Query: provides a list of encryption algorithm identifiers.
- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages (KMMs). Available to User and CO Roles. Service input: KMM. Service output: KMM.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Common Key Reference (CKR). Available to User and CO Roles. Service input: KMM. Service output: KMM.
- Zeroize all keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL). Service input: KMM. Service output: KMM.

- Tamper[3] Response: Erases all CSP's with the exception of the password upon detection of tamper. Service Input: Hardware Tamper switch.

- Non-Privileged APCO OTAR: Hello and Capabilities KMMs may be performed without a Role. Service input: KMM. Service output: KMM.

- Reset Crypto Module: Soft reset of module to remove module from error states. Available without a Role. Service input: DPRAM message (opcode). Service output: DPRAM message (opcode).

- Shutdown Crypto Module: Prepares module for removal of power. Available without a Role. Service input: DPRAM message (opcode). Service output: DPRAM message (opcode).

- Download Configuration Parameters: Download configuration parameters used to specify module behavior. For example enable/disable APCO OTAR etc. Modification of some security related parameters (single key mode, tamper[4] mode) causes key erasure. Available without a Role. Service input: DPRAM message (opcode, parameter ID, parameter value). Service output: DPRAM message (opcode, parameter ID, parameter status).

- Query Configuration Parameters: module supplies a list of the current configuration parameter settings.

- Programming Upgrade: Allows users to upgrade CE software. Service Input: Programming messages via the KVL or DPRAM.

[3] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

[4] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

8. Module Interfaces

The MCC7500 SCCE supports the following interfaces.

- Data input interface

  a. DPRAM – Plaintext Data, Ciphertext Data, OTAR KMMs, password

  b. KVL – Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys, OTAR (Store & Forward)

  c. SCI – used to flash program the master crypto engine in the factory

- Data output interface

  4 DPRAM- - Plaintext Data, Ciphertext Data, OTAR KMMs

- Control input interface

  a. DPRAM – Input Commands, Programming Upgrade

  b. KVL – Input Commands, Programming Upgrade

  c. Tamper[5] – in addition to the tamper switch beneath the tamper shield, a tamper switch is physically available to the user to cause a tamper response on demand.

  d. Hardware reset line available to host processor

  e. CPLD used for external interrupts

- Status output interface

  a. DPRAM – Status Codes

  b. KVL – Status Codes

  c. KVL LED – KVL interface state

- Power interface

  b. SW_3.3 – Switched power supply powers all circuitry except Battery Backed Register

  c. CONT_3.3 – Continuous power supply powers Battery Backed Register

[5] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

9. Authentication

The MCC7500 SCCE uses a 40-bit password to implicitly authenticate the User and CO roles. The password is initialized to a default value during manufacturing. After authenticating, the password may be changed at any time. Fifteen consecutive invalid authentication attempts cause the KPK to be zeroized and all keys in the Key Database to be marked invalid.

10. Access Control

10.1. Security Related Data Items (CSPs)

Table 10-1

CSP Identifier	Description
Key Protection Key (KPK); TDES	Key used to encrypt the database and other non-volatile parameters
Plaintext Traffic Encryption Keys (TEKs); AES256	Keys used for voice and data encryption
Plaintext Key Encryption Keys; AES256	Keys used for encryption of keys in OTAR
Plaintext MAC Key; 3DES	Key used for authentication of software upgrade. Stored in non-volatile memory
Plaintext Password; 40-bits	Operator password entered during user authentication

10.2. CSP Access Types

Table 10-2

CSP Access Type	Description
Retrieve key	Decrypts encrypted TEKs or KEKs in the database using the KPK and returns plaintext version
Store key	Encypts plaintext TEKs or KEKs using the KPK and stores the encrypted version in the database
Erase Key	Marks encrypted TEK or KEK data in key database as invalid
Create KPK	Generates and stores new KPK
Store Password	Hashes user password and stores it in the database

10.3. Access Matrix

	CSP Access Operation					Applicable Role		
User Service	Retrieve Key	Store Key	Erase Key	Create KPK	Store Password	User Role	Crypto Officer Role	No Role Required
1. Transfer Key Variable		X				X	X	
2. Privileged APCO OTAR	X	X	X			X	X	
3. Validate Password				X[1]		X	X	X
4. Change Password			X	X[1]	X	X	X	
5. Encrypt	X					X	X	
6. Decrypt	X					X	X	
7. Zeroize Selected Keys			X			X	X	
8. Zeroize All Keys			X			X	X	
9. Tamper[6] Response			X			X	X	X
10. Non-Privileged APCO OTAR						X	X	X
11. Reset Crypto Module						X	X	X
12. Shutdown Crypto Module						X	X	X
13. Download Config Parameters			X	X[2]		X	X	X
14. Programming Upgrade						X	X	
15. Query Config Parameters						X	X	X
16. Traffic Algorithm Query						X	X	X

1 – initial power-up out of factory or after tamper condition

2 – after modification of a security related config parameter

[6] The tamper mechanisms are not tested as part of the FIPS 140-2 validation.

11. Mitigation of Attacks

The MCC7500 SCCE provides tamper detection and response circuitry to prevent unauthorized physical access to the crypto module within the tamper shield. The tamper detection and response circuitry remains active even while the Secure Card is powered off. In addition to the tamper switch beneath the tamper shield, a tamper switch is physically available to the user to cause a tamper response on demand. Tamper mode must be enabled through the Download Configuration Parameters service in order to enable tamper response functionality. The MCC7500 SCCE erases all CSP's with the exception of the password upon detection of tamper. The tamper detection and response circuitry has been tested and proven to function as specified.