Security Policy

Subscriber Encryption Module

5100 Series Portable Radios, 5300 Series Mobile Radios
And Johnson Encryption Machine (JEM)

Author: Angel G. Ortiz

Hardware Version:
023-5000-984, 023-5000-982, 023-5000-980 and 039-575-1200

Firmware Version: 4.0, 4.1 and 4.2

Document Version 4.1
September 21, 2005

Contents

1 Introduction

1.1 Scope

This Security Policy defines the security rules for the E.F. Johnson Co., Subscriber Encryption Module (SEM) that can be used with any radio subscriber equipment, or hardware which requires a FIPS 140-2 module. There are three firmware versions, 4.0, 4.1, and 4.2. Firmware version 4.0 is used in the SEM product 023-5000-980 and 023-5000-984 which contain a 256 KB RAM. Firmware version 4.1 is used in the SEM product 023-5000-982 which contains a 360 KB RAM.

Firmware version 4.2 is used in the SEM product 039-575-1200 and contains a 256 KB RAM. This particular firmware version is used in the E.F. Johnson Co., Johnson Encryption Machine (JEM) hardware. Version 4.2 makes the SEM's DSP operate at the maximum speed of 200 MHz.

All Firmware versions, 4.0, 4.1, and 4.2 are identical in functionality. Firmware version 4.0 and 4.1 use different DSPs, but the DSPs operate at a lower speed in order to conserve power. Version 4.2 uses the same DSP as firmware version 4.0 in SEM product 023-5000-984, except that the DSP operates at the maximum speed of 200 MHz.

Firmware version 4.1 is used on the SEM which contains a DSP with additional memory. The 4.1 firmware checks the additional RAM memory of the DSP in SEM part number 023-5000-982.

The firmware versions 4.0, 4.1, and 4.2 of the SEM contain a new feature that supports multiple encrypted voice channels. This feature is currently only used in the Johnson Encryption Machine (JEM) product of E.F. Johnson.

The E.F. Johnson Co. portable, mobile radio and Johnson Encryption Machine (JEM) are examples of products which contain the SEM.

The security rules specified in this document include rules derived from the FIPS 140-2 standard, as well as requirements imposed by E.F. Johnson Co. This document defines the cryptographic module, crypto officer and user roles, and security related data management.

The SEM module design corresponds to the module's security rules defined in this Security Policy document.

1.2 SEM Implementation

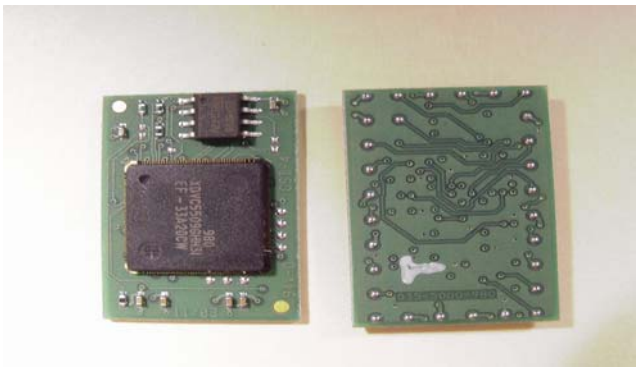
The SEM is implemented as a multi-chip embedded module assembled on a PC board. The two chips include a Digital Signal Processor (DSP) and an associated 2 Mbit Flash memory.

There are four SEM product versions and each product version consists of the two chips. The SEM product versions and firmware versions are shown in Table 1-1 SEM Product Number vs. Firmware Version.

Table 1-1 SEM Product Number vs. Firmware Version

Product Number	Firmware Version	Description	DSP	Memory
023-5000-980	4.0	Operates at 20 MHz to 100 MHz	Texas Instruments C5509	2 Mega-bit Flash, 256 KB RAM
023-5000-984	4.0	Operates at 20 MHz to 100 MHz	Texas Instruments C5509A	2 Mega-bit Flash, 256 KB RAM
023-5000-982	4.1	Operates at 20 MHz to 100 MHz	Texas Instruments C5510	2 Mega-bit Flash, 320 KB RAM
039-575-1200	4.2	Operates at 200 MHz	Texas Instruments C5509A	2 Mega-bit Flash, 256 KB RAM

In all versions of the SEM, the Flash memory stores the program for the DSP in its non-volatile memory. Upon start-up, the Flash memory code is loaded into the Random Access Memory (RAM) embedded in the DSP. Code execution is from this code loaded in the RAM. The following photograph shows the SEM.



The SEM can be incorporated into any hardware device, which requires FIPS 140-2 Level 1 cryptographic security functionality.

1.3 Cryptographic Boundary

The cryptographic boundary consists of the SEM PC board, and includes the Digital Signal Processor (DSP) and associated 2 Mb Flash Read Only Memory (ROM).

2 Intended FIPS 140-2 Security Levels

The SEM is validated to meet FIPS 140-2 security requirements for the levels shown in the Table 2-1 SEM Security Levels. The overall module is validated for Security Level 1.

Table 2-1 SEM Security Levels

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

3 FIPS 140-2 Approved Operational Modes

The SEM can be programmed to operate in a FIPS 140-2 mode or in a non FIPS 140-2 approved mode. In each mode, there are ciphers available to the user for the encryption and decryption of voice.

The SEM supports AES Over-the-Air-Rekeying (OTAR). This is an industry standard implemented in many subscriber equipment radios to rekey radios with new security parameters. The ANSI/TIA Standard for AES OTAR can be found in document **ANSI/TIA-102.AACA-1-2002** titled, *Project 25- Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms*.

Subscriber equipment such as the E.F. Johnson Co. radio in which the SEM is installed, sends a key load message to the SEM via the control Interface. Based on the key load message type, the SEM will operate in either a FIPS 140-2 mode or non FIPS 140-2

mode. Using the E.F. Johnson Co. radio in digital mode will invoke the FIPS 140-2 mode of operation and make available to the user, all FIPS approved cipher algorithms.

The following ciphers are available to the user when the SEM is operating in a FIPS 140-2 approved mode of operation.

1. AES-256 OFB
2. AES-256 ECB
3. AES-256 CBC
4. AES-192 OFB
5. AES-192 ECB
6. AES-192 CBC
7. AES-128 OFB
8. AES-128 ECB
9. AES-128 CBC
10. DES OFB
11. DES ECB
12. DES CBC
13. DES 1 bit CFB
14. DSA Signature Verification
15. HMAC-SHA-1
16. PRNG (both general purpose, and DSA specific; see section 4.2, rule 8)

Note: The PRNG is implemented as described in FIPS 186-2, Appendix 3.1.

When the SEM is operated in a non FIPS 140-2 approved mode, only one cipher is available. This cipher is the following:

1. SecureNet DES 1 bit CFB with differential encoding and decoding

The FIPS Approved mode of operation is selected by choosing one of the approved algorithms, whereas the non-approved mode is selected by choosing the SecureNet mode of operation.

4 Security Rules

4.1 Operating Environment

The SEM does not have an underlying operating system. The SEM's operating environment is implemented in hardware, is static and non-modifiable.

4.2 FIPS 140-2 Related Security Rules

1. The SEM operating environment does not have an underlying operating system. The SEM's operating environment is implemented in hardware, is static, and non-modifiable.

2. The SEM has the following interfaces:

   - Data Input Interface
     The data input consists of the receive half of a duplex synchronous serial port. It transfers plaintext data and ciphertext data.

   - Data Output Interface
     The data output consists of the transmit half of a duplex synchronous serial port. It transfers plaintext data and ciphertext data.

   - Control Input Interface
     The control input interface consists of the receive half of a duplex synchronous serial SPI port. It receives input commands and control data used to control the operation of the SEM.

   - Status Output Interface
     The status output interface consists of the transmit half of a duplex synchronous serial SPI port. The SEM will output status results pertinent to its current state.

   - Power Interface
     The power interface consists of a 3.3 Volt DC input to power the FLASH ROM and DSP, as well as a 1.6 Volt DC input to power the DSP core processor.

3. All data output via the SEM's Data Output Interface is disabled when an error state exists and during Power-up Self Tests.

4. The SEM supports a User role and a Crypto Officer role. The role is selected implicitly by the service that is invoked.

5. The SEM supports the following services requiring a role:
   - Generate Key Storage Key Encryption Key (KSKEK)
   - Generate Keyed-Hashed Message Authentication Code Key (KMACK)
   - Generate Traffic Encryption Key (TEK)
   - Encryption of Keys With a KSKEK
   - Decryption of Cipher Text Keys With a KSKEK
   - Decrypt Encryption Key Using KEK
   - Encrypt Encryption Key Using KEK
   - Zeroize Keys
   - Encrypt Digital Communication
   - Derive Key
   - Decrypt Digital Communication
   - Flash Update
   - Power-up Self Tests

- Show Status

The SEM's Derive Key service is used for AES-OTAR key derivation. It is used for programming radios with new AES keys and is a FIPS 140-2 mode of operation. For further information, see the ANSI/TIA Standard for AES OTAR found in document **ANSI/TIA-102.AACA-1-2002** titled, *Project 25- Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms*.

6. The SEM protects all plaintext keys and critical security parameters from disclosure, modification, or substitution within the SEM cryptographic boundary.

7. The SEM provides the capability to zeroize all plaintext secret keys and critical security parameters within the module.

8. The SEM supports the following FIPS approved algorithms.

   - AES-256 OFB
   - AES-256 ECB
   - AES-256 CBC
   - AES-192 OFB
   - AES-192 ECB
   - AES-192 CBC
   - AES-128 OFB
   - AES-128 ECB
   - AES-128 CBC
   - DES OFB
   - DES ECB
   - DES CBC
   - DES 1 bit CFB
   - SHA-1 hash function algorithm
   - Digital Signature Algorithm (DSA)
   - Keyed-Hash Message Authentication Code (HMAC) Using SHA-1 (HMAC-SHA-1)
   - FIPS 186-2 Appendix 3.1 Pseudo Random Number Generator (PRNG) ~ The SEM contains two PRNGs. One is used for DSA number generation and the other is used for non DSA number generation cases. No generated key will have more than 160 bits of entropy, irrespective of key size.

9. The SEM, when used in conjunction with an E.F. Johnson Co. JEM, series 5100 portable radio or series 5300 mobile radio meets all of the applicable requirements of the FCC rules.

10. The SEM performs the following self-tests:

- Internal Flash Test
  The internal Flash memory is tested by performing a SHA-1 hash on the contents and checking the results against the expected value.

- RAM Test
  The RAM is tested by checking to see that all zeros and all ones can be written into each word. All SEM versions perform these memory tests. However firmware version 4.1 checks the additional RAM which is only available on a 023-5000-982 SEM.

- Software/Firmware Load Test
  All SEM firmware releases are digitally signed using the DSA algorithm at the E.F. Johnson Co. facility. During self-tests, the SEM verifies the integrity of the loaded firmware using the DSA algorithm.

- AES Algorithm Test
  The AES algorithm is tested for encrypt and decrypt using a Known Answer Test in the Electronic Code Book (ECB) mode of operation.

- DES Algorithm Test
  The DES algorithm is tested for encrypt and decrypt using a Known Answer Test in the Electronic Code Book (ECB) mode of operation.

- SHA-1 Algorithm Test
  The SHA-1 hash algorithm is tested using a Known Answer Test.

- HMAC-SHA-1 Algorithm Test
  The HMAC-SHA-1 algorithm is tested using a Known Answer Test.

- DSA Algorithm Test
  The DSA Algorithm test is a DSA signature verification test using a Known Answer Test (KAT).

- Pseudorandom Number Generator Test
  Both SEM Pseudorandom Number Generators (PRNGs) are tested using a Known Answer Test.

- Pseudorandom Number Generator Continuous Test
  Any time the PRNGs are called, a conditional test is performed, comparing the current result with the previously generated number. If they are equal, the SEM enters the error state.

11. The SEM enters an error state upon failure of any of the self-test routines.

12. The SEM outputs a successful status indicator via the Status Indicator interface only when all tests have passed. If an error is encountered, the module inhibits its serial interface. Because of the protocol used, this can be uniquely interpreted as a FIPS error indicator from the Status Indicator interface. This indicates an error has occurred, and the SEM enters the error state. The module does not perform any cryptographic functions while in an error state. An error state is exited by powering the module off and then on.

13. The SEM module supports OTAR as described in APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA.

4.3 E.F. Johnson Co. Imposed Security Rules

1. The SEM does not support multiple concurrent operators.

2. The SEM does not support a bypass mode.

3. All Single DES algorithms are present to allow the module to inter-operate with existing legacy systems. DES is usable in the module's approved mode during the transitional phase only – valid until May 19, 2007.

4. The initial invocation of the Show Status service is accompanied by 44 bytes of data, which contains at least 256 bits of entropy.

5 Identification and Authentication Policy

The SEM does not support authentication for either the User or Crypto Officer Roles.

6 Access Control Policy

6.1 Roles Supported

The SEM cryptographic module supports the User and Crypto-Officer role only. There are no Maintenance User Roles in the SEM. The User and Crypto-Officer roles are mutually exclusive and cannot exist concurrently.

6.1.1 User Role

This role is implicitly assumed when an operator uses one of the User services.

See section 6.2 for a list of User services.

6.1.2 Crypto-Officer Role

This role is implicitly assumed when an operator uses one of the Crypto-Officer services.

A **Crypto-Officer** is responsible for key management functions of the Subscriber Encryption Module. A Crypto-Officer will be able to load, clear, add or delete key management parameters of a radio containing the Subscriber Encryption Module. There are two tools a Crypto-Officer can use for the key management of the Subscriber Encryption Module. These tools are the Motorola 3000 KVL, or the KMF.

A **Crypto-Officer** is also responsible for updating the Subscriber Encryption Module firmware. E.F. Johnson Co. will digitally sign all SEM firmware updates. Any new firmware downloads to the SEM will be digitally verified by the existing firmware for authenticity. Only SEM firmware, which is digitally authenticated, is allowed to be downloaded into the SEM flash memory. Loading non-validated code will invalidate the module's validation to FIPS 140-2.

6.2 Services Provided

The table below lists all the security services and functions that are performed by the SEM. All the security services listed below are available in the FIPS 140-2 modes of operation. The operator using the SEM service is also listed in the table.

The sections that follow, describe the specific services of the SEM.

Table 6-1SEM Services vs. Security Functions

Service	Security Function(s) Used	Key Type and Length	General Mode of Operation	Operator Using Service.
Generate **KSKEK**	PRNG	256 bit AES	Key Generation	Crypto-Officer
Generate **KMACK**	PRNG SHA-1	160 bit Keyed Hashed MAC	Used for data Authentication of new SEM Firmware	Crypto-Officer
Generate **TEK**	PRNG	56 bit DES Key or 256, 192, or 128 bit AES Key	Key Generation	Crypto-Officer
Encryption of Keys With a **KSKEK**	AES	256 bit AES KSKEK	Encryption	Crypto-Officer
Decryption of Cipher text Keys	AES	256 bit AES KSKEK	Decryption	User

Service	Security Function(s) Used	Key Type and Length	General Mode of Operation	Operator Using Service.
With a **KSKEK**				
Decrypt Encryption Key using **KEK**	AES or DES	256, 192, or 128 bit AES Key or 56 bit DES Key	Decryption	Crypto-Officer
Encrypt Encryption Key using **KEK**	AES or DES	256, 192, or 128 bit AES Key or 56 bit DES Key	Encryption	Crypto-Officer
Zeroize Keys	N/A	N/A	Clear Keys	Crypto-Officer
Encrypt Digital Communication	AES or DES	256, 192, or 128 bit AES Key or 56 bit DES Key	Encryption	User
Derive Key	AES	256 bit AES key	Encryption/Decryption	Crypto-Officer
Decrypt Digital Communication	AES or DES	256, 192, or 128 bit AES Key or 56 bit DES Key	Decryption	User
Flash Update	DSA	1024 bit	Signature Verification	Crypto-Officer
Power-up Self Tests	DES AES-256 SHA-1 DSA HMAC PRNG	DES 56 bit, AES 256 SHA-1 160 bit, DSA 1024 bit, HMAC 160 bit, PRNG (both DSA and general purpose) 160 bit	Power up Cryptographic Tests	User

Service	Security Function(s) Used	Key Type and Length	General Mode of Operation	Operator Using Service.
Show Status	SHA-1	SHA-1 160 bit	SEM Services Status	User

6.2.1 Generate Key Storage Key Encryption Key (KSKEK)
This service uses the SEM's Pseudorandom Number Generator to generate the KSKEK, a 256 bit AES key. The KSKEK is used to encrypt other SEM CSPs for storage outside of the SEM boundary.

6.2.2 Generate Keyed-Hashed Message Authentication Code Key (KMACK)
This service uses the SEM's Pseudorandom Number Generator to generate the KMACK, a 160 bit HMAC-SHA-1 key. The KMACK is used to validate the authenticity of SEM CSPs when they are retrieved from outside of the SEM boundary.

6.2.3 Generate Traffic Encryption Key (TEK)
This service uses the SEM's Pseudorandom Number Generator to generate a TEK. The TEK is generated when an OTAR "Reverse Warm Start" block is required. This key is either a 56 bit DES key, 256, 192, or 128 bit AES key. This is a temporary key used for encryption of traffic.

6.2.4 Encryption of Keys With a KSKEK
This service is provided by the SEM's FIPS approved AES algorithm to store secret keys or CSPs outside of the SEM cryptographic boundary in encrypted form. All keys that are used by the SEM are AES encrypted by the 256 bit KSKEK, and stored outside of the SEM cryptographic boundary.

6.2.5 Decryption of Cipher Text Keys with a KSKEK
All keys that are stored outside of the SEM's boundary are stored in encrypted format. This service is provided by the SEM's FIPS approved DES or AES algorithm to retrieve encrypted keys from outside of the SEM boundary into the SEM boundary, decrypt the keys, and use the keys. All keys are decrypted using the AES algorithm and the 256 bit AES KSKEK.

6.2.6 Decrypt Encryption Key Using KEK
This service is provided by the SEM to decrypt a key using the KEK, established through the OTAR protocol. The KEK can be a 256, 192, or 128 bit AES key or 56 bit DES key. The key being decrypted can also be an AES or DES key; in the case where a DES Encryption Key is being decrypted, a DES KEK is used, and in the case where an AES Encryption Key is being decrypted, an AES KEK is used.

6.2.7 Encrypt Encryption Key Using KEK

This service is provided by the SEM's FIPS approved DES or AES algorithm to encrypt a key using the KEK, which is established through OTAR. In the case where a DES Encryption Key is being decrypted, a DES KEK is used, and in the case where an AES Encryption Key is being decrypted, an AES KEK is used.

6.2.8 Zeroize Keys

This service is provided to the operator so that all SEM secret keys and CSPs are zeroized.

6.2.9 Encrypt Digital Communication

This service provides the operator with secure encrypted data communication between another SEM, Motorola Universal Crypto Module (UCM), or other device of similar functionality.

6.2.10 Derive Key

The Derive Key service used for AES-OTAR key derivation is a **FIPS 140-2 state**. It is used to meet the ANSI/TIA Standard for AES OTAR found in document **ANSI/TIA-102.AACA-1-2002** titled, *Project 25- Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms*.

6.2.11 Decrypt Digital Communication

This service provides the operator reception of secure communication from another SEM, Motorola Universal Crypto Module (UCM), or other device of similar functionality.

6.2.12 Flash Update

This service provides the Crypto-Officer the capability of updating the SEM's digitally signed firmware. A reset of the SEM module is performed when new firmware is loaded into the SEM.

6.2.13 Power-up Self Test

This service provides power up and continuous tests to verify the secure state and operation of the SEM. All of the SEM's cryptographic and security functions are tested using known answer tests. The user initiates this service by power cycling or resetting the module.

6.2.14 Show Status

This service provides information on the SEM state such as the Fatal Error State. The initial invocation of the Show Status service is accompanied by 44 bytes of data, which contain at least 256 bits of entropy. The 256 bits are used to establish the PRNG state.

6.3 Critical Security Parameters (CSP) and Public Keys

This section describes the Critical Security Parameters (CSP) and Public Key used by the SEM. The KSKEK and KMACK keys are stored within the SEM boundary, while the TEK and KEK are stored outside of the SEM boundary in encrypted form.

The SEM's Public Key is used during the Flash Update service. This key is used to validate any new code which is loaded into the SEM.

The SEM's PRNG is used in the generation of the KSKEK and KMACK keys. In the case when an OTAR "Reverse Warm Start" block is required, the PRNG is used to generate the TEK.

Table 6-2 Critical Security Parameters and Description

CSP Identifier	Description
Key Storage Key encryption Key (KSKEK)	A 256 bit key used to encrypt and decrypt encryption keys that are stored off-module.
Keyed-Hashed Message Authentication Code Key (KMACK)	A 160 bit key used with SHA-1 to authenticate messages to and from the SEM which contain other encryption keys.
Traffic Encryption Keys (TEK)	A key in plaintext form of length up to 256 bits used to encrypt and decrypt data.
Key Encryption Key (KEK)	A key in plaintext used to encrypt and decrypt an encryption key.
PRNG State	The PRNG state is used by the PRNG security function of the SEM to generate the KSKEK, KMACK, and TEK keys
Derived Key	Used for AES-OTAR key derivation.

6.4 Services Authorized for Roles

Table 6-3 SEM Services vs. Role

Authorized Services	Roles
Generate KSKEK	Crypto-Officer
Generate KMACK	Crypto-Officer
Generate Traffic Encryption Key (TEK)	Crypto-Officer
Encryption of Keys with a KSKEK	Crypto-Officer
Decryption of Cipher text Keys with a KSKEK	User
Decrypt Encryption Key Using KEK	Crypto-Officer
Encrypt Encryption Key Using KEK	Crypto-Officer
Zeroize Keys	Crypto-Officer
Encrypt Digital Communication	User
Decrypt Digital Communication	User
Derive Key	Crypto-Officer
Flash Update	Crypto-Officer
Power-up Self Test	User
Show Status	User

6.5 Access Rights within Services

Table 6-4 SEM Access Rights of CSPs

Service	Cryptographic Keys And CSPs	Type of Access (e.g. Read, Write, Delete, Select)
Generate KSKEK	PRNG State	Write
Generate KSKEK	KSKEK	Write
Generate KMACK	PRNG State	Write
Generate KMACK	KMACK	Write
Generate Traffic Encryption Key (TEK)	PRNG State	Write
Generate Traffic Encryption Key (TEK)	TEK	Write
Encryption of Keys with a KSKEK	KSKEK	Read, Select
Encryption of Keys with a KSKEK	KMACK	Read, Select
Encryption of Keys with a KSKEK	TEK	Write
Encryption of Keys with a KSKEK	KEK	Write
Decryption of Cipher Text Keys With a KSKEK	KSKEK	Read, Select
Decryption of Cipher Text Keys With a KSKEK	KEK	Read, Select
Decryption of Cipher Text Keys With a KSKEK	KMACK	Read, Select
Decryption of Cipher Text Keys With a KSKEK	TEK	Read, Select
Decrypt Encryption Key Using KEK	KSKEK	Read, Select
Decrypt Encryption Key Using KEK	KMACK	Read, Select
Decrypt Encryption Key Using KEK	TEK	Write
Decrypt Encryption Key Using KEK	KEK	Read, Select
Encrypt Encryption Key Using KEK	KSKEK	Read, Select
Encrypt Encryption Key Using KEK	KMACK	Read, Select
Encrypt Encryption Key Using KEK	TEK	Read, Select

Service	Cryptographic Keys And CSPs	Type of Access (e.g. Read, Write, Delete, Select)
Encrypt Encryption Key Using KEK	KEK	Read, Select
Zeroize Keys	KSKEK	Delete
Zeroize Keys	TEK	Delete
Zeroize Keys	KEK	Delete
Zeroize Keys	KMACK	Delete
Zeroize Keys	PRNG State	Delete
Zeroize Keys	Derived Key	Delete
Encrypt Digital Communication	TEK	Select
Decrypt Digital Communication	TEK	Select
Derive Key	TEK	Select
Derive Key	Derived Key	Write
Flash Update	DSA Public Key	Read, Select
Power-up Self Tests	None	N/A
Show Status	PRNG State	Write
Show Status	KSKEK	Read
Show Status	KMACK	Read

7 Physical Security Policy

The SEM consists of production grade components. In its application, the SEM is housed in the standard production grade housing of the portable or mobile radio product.

There are no actions required to ensure that the physical security of the module is maintained.

8 Mitigation of Other Attacks Policy

The SEM is not designed to mitigate against other attacks not specifically mentioned in the FIPS 140-2 document, including but not limited to power analysis, timing analysis, fault indication, or TEMPEST.

9 References

The following standards and documents where used in the development of the SEM module.

1. FIPS 140-2: Security Requirements For Cryptographic Modules
2. FIPS 180-1: Secure Hash Standard
3. FIPS 197: Advanced Encryption Standard (AES)
4. FIPS 198: The Keyed-Hash Message Authentication Code (HMAC)
5. FIPS 46-4: Data Encryption Standard (DES)
6. FIPS 186-2: Digital Signature Standard (DSS)
7. SP 800-38a: Recommendation for Block Cipher Modes of Operation
8. FIPS 81: DES Modes of Operation
9. APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA
10. TIA Standard, Project 25 – Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms.

10 Acronym List

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher-Feedback
CSP	Critical Security Parameter
DC	Direct Current
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
ECB	Electronic Codebook
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
HMAC	Keyed-Hashing for Message Authentication
JEM	Johnson Encryption Machine
KAT	Known Answer Test
KB	Kilo-Byte
KEK	Key Encryption Key
KMACK	Keyed-Hashed Message Authentication Code Key
KMF	Key Management Facility
KSKEK	Key Storage Key Encryption Key
KVL	Key Variable Loader
MHz	Mega Hertz
OFB	Output-Feedback
OTAR	Over-The-Air-Rekeying
PRNG	Pseudo Random Number Generator
ROM	Read Only Memory
RAM	Random Access Memory
SEM	Subscriber Encryption Module
SHA-1	Secure Hash Algorithm-1
SPI	Serial Programming Interface
TIA	Telecommunication Industry Association
TEK	Transmission Encryption Key
UCM	Universal Crypto Module