Subscriber Encryption Module

Viking Series Portable and Mobile Radios

FIPS 140-2 Cryptographic Module Security Policy

Hardware Version: R023-5000-980

Firmware Version: 5.28

September 4, 2014

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the EFJohnson Technologies Subscriber Encryption Module (SEM), hereafter denoted the Module. The Module, validated to FIPS 140-2 overall Security Level 1, is used for encryption/decryption of voice and data adhering to the TIA Project 25 (P25) standards on any radio subscriber equipment. The EFJohnson portable and mobile radio products are examples of subscriber equipment that contain the Module.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Land Mobile Radios. The Module is a multi-chip embedded embodiment; the cryptographic boundary is a printed circuit board (PCB) with a Digital Signal Processor (DSP) and an associated 2 Mbit Flash Read Only Memory (ROM).

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	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
Self-Tests	Level 1
Design Assurance	Level 1
Mitigation of Other Attacks	N/A

Table 1 – Security Level of Security Requirements

The Module implementation is compliant with:

- Telecommunications Industry Association (TIA) standards <http://www.tiaonline.org/>

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1; the red outline depicts the physical cryptographic boundary. Figure 1 is a circuit board that can be placed in any radio device that requires FIPS 140-2 validation. This board includes the DSP and associated ROM. The Module relies on a radio embedded processor and a radio DSP as input/output devices.

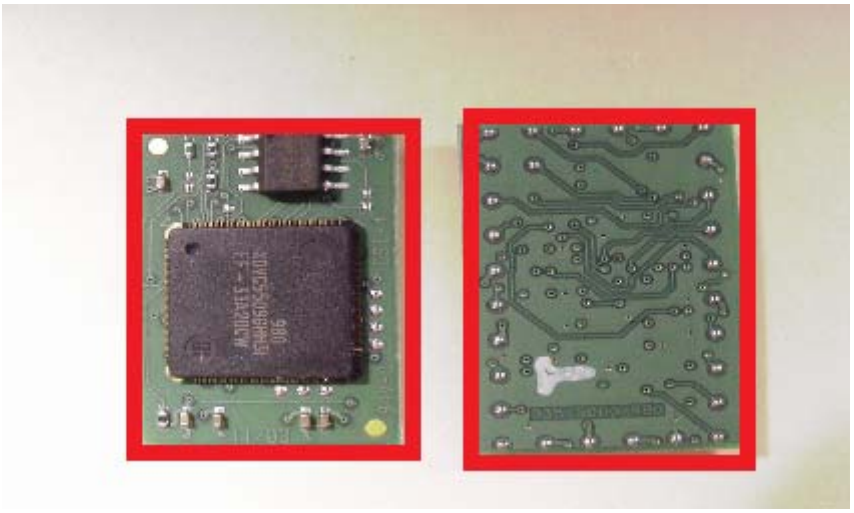

Figure 1 – Module, Top and Bottom

Port	Description	Logical Interface Type
SPI	Full-duplex communication to radio ARM	Data in/Data out
McBSP	Full-duplex communication to radio DSP	Data in/Data out
3.3V DC	Power in	Power
1.6V DC	Power in	Power

Table 2 – Ports and Interfaces

1.2 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

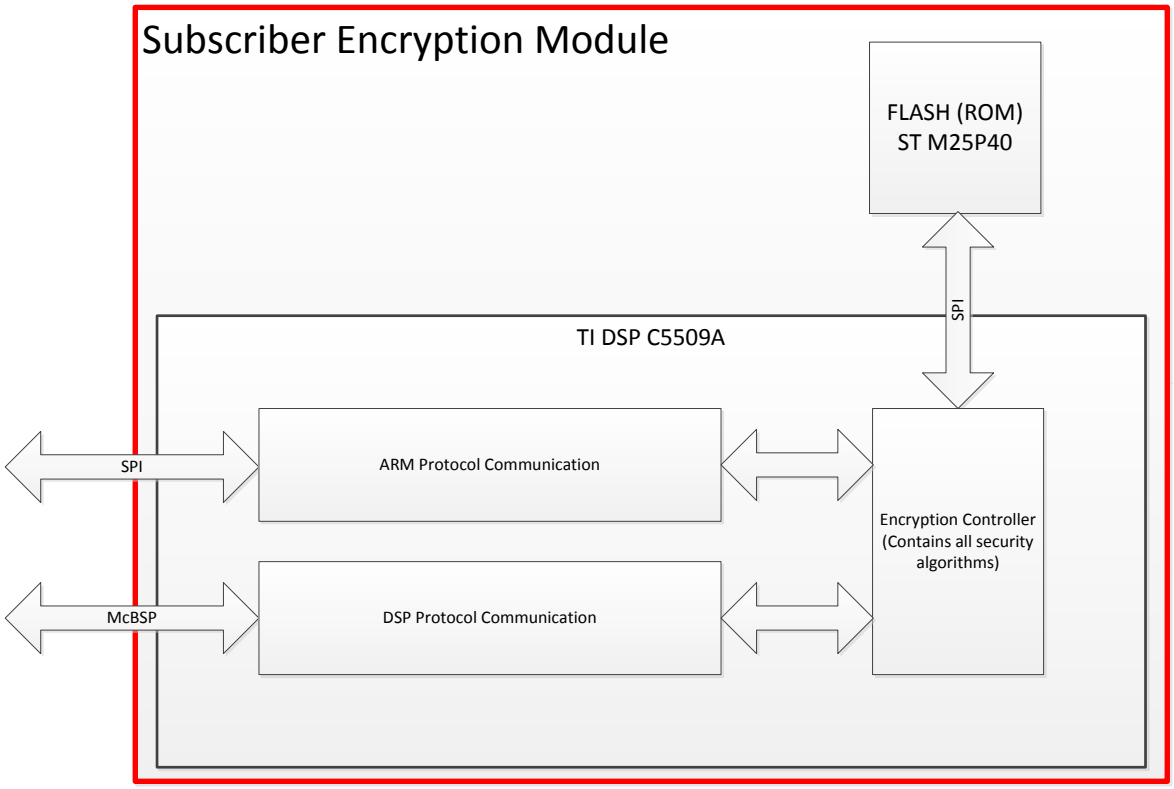

Figure 2 – Module Block Diagram

The Module has two (2) chips on board. The DSP chip handles the external interfaces to the radio. The ROM flash communicates only with the DSP. The DSP has three (3) software functional blocks. The Encryption Controller block contains all security algorithms while the other two blocks handle external communications.

1.3 Versions and Mode of Operation

This SEM version consists of the two (2) chips. The board contains a 2 Mega-bit ROM with the Texas Instruments C5509A DSP.

The ROM stores the program for the DSP in its non-volatile memory. Upon start-up, the ROM code is loaded into the Random Access Memory (RAM) embedded in the DSP. Code execution is from this code loaded in the RAM.

	Module	HW P/N and Version	FW Version	OE (if applicable)
1	SEM	R023-5000-980	V5.28	

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.

Subscriber equipment such as the EFJohnson Technologies radio in which the SEM is installed, sends a key load message to the SEM via one of the external interfaces. 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 EFJohnson Technologies 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-128 OFB
2. AES-128 ECB
3. AES-128 CBC
4. AES-192 OFB
5. AES-192 ECB
6. AES-192 CBC
7. AES-256 OFB
8. AES-256 ECB
9. AES-256 CBC

When the SEM is operated in a non FIPS 140-2 approved mode the following ciphers are also available:

1. DES OFB
2. DES ECB
3. DES CBC
4. DES 1 bit CFB
5. SecureNet DES 1 bit CFB with differential encoding and decoding
6. SecureNet DES-XL

In order to switch from a non-approved mode to an approved mode of operation, the operator must perform a zeroize keys command and then use only approved algorithms.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Table 3 and Table 4 below.

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, OFB Key sizes: 128, 192, 256 bits	#2640
DRBG	[SP 800-90] Functions: HASH DRBG Security Strengths: 128 bits	#411
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: SHA-256	#1632

Algorithm	Description	Cert #
RSA	[FIPS 186-3, ANSI X9.31-1998] Functions: Signature Verification Key sizes: 3072 bits	#1351
SHA	[FIPS 180-3] Functions: Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-256	#2213

Table 3 –Approved Cryptographic Functions

Algorithm	Description
AES Key Wrap/Unwrap	[IG D.2] and [AES Key Wrap Specification, Nov 2001] AES (Cert. #2640, key wrapping; key establishment methodology provides 128 bits of encryption strength)
AES OTAR	AES MAC (AES Cert. 2640, vendor affirmed; P25 AES OTAR)
NDRNG	Used to seed the FIPS Approved DRBG

Table 4 – Non-Approved But Allowed Cryptographic Functions

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- DES

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

CSP	Description / Usage
Key Storage Key encryption Key (KSKEK)	An AES-256 key used to encrypt and decrypt encryption keys that are stored off-module.
Keyed-Hashed Message Authentication Code Key (KMACK)	A 256 bit key used with SHA-256 to authenticate messages to and from the SEM which contain other encryption keys.
Traffic Encryption Keys (TEK)	An AES-256 key in plaintext form used to encrypt and decrypt data.
Key Encryption Key (KEK)	An AES-256 key in plaintext form used to encrypt and decrypt an encryption key.
DRBG Working State	The DRBG working state is used by the DRBG security function of the SEM to generate the KSKEK, KMACK, and TEK keys
Derived Key	Used for AES-OTAR key derivation.
System Validation Key	A 128 bit AES key in plaintext form used for TIA P25 Phase 2 System Validation.

Table 5 – Critical Security Parameters

2.2 Public Keys

Key	Description / Usage
RSA Public Key	Public component of an RSA key pair (3072-bit), used by the Module for signature verification.

Table 6 – Public Keys

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two (2) distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles because one authentication is allowed per module reset. The User and CO roles are mutually exclusive and cannot exist concurrently.

Table 7 lists all operator roles supported by the module. The Module does not support a maintenance role. The Module does not support concurrent operators. The Module does not support authentication for either the User or CO roles.

Role ID	Role Description
CO	Cryptographic Officer – This role is implicitly assumed when an operator uses one of the CO services. See Table 9 below.
User	User – This role is implicitly assumed when an operator uses one of the User services. See Table 8 below.

Table 7 – Roles Description

A CO is responsible for key management functions of the Module. A CO will be able to load, clear, add or delete key management parameters of a radio containing the Module. There are four (4) tools a CO can use for the key management of the Module. These tools are the Motorola 3000 KVL, Motorola 4000 KVL, Key Management Facility (KMF), or the EFJ Subscriber Management Assistant (SMA).

A CO is also responsible for updating the Module's firmware. EFJohnson Technologies 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.

3.2 User Services

All services implemented by the Module are listed in Table 8 and Table 9 below.

Service	Security Function(s) Used	Key Type and Length	General Mode of Operation
Decryption of Cipher text Keys With a **KSKEK**	AES	256 bit AES KSKEK	Decryption
Encrypt Digital Communication	AES or DES*	256 bit AES Key or 56 bit DES Key*	Encryption
Decrypt Digital Communication	AES or DES*	256 bit AES Key or 56 bit DES Key*	Decryption
Power-up Self-Tests	DES* AES-256 SHA-256 RSA HMAC DRBG	DES 56 bit*, AES 256 bit, SHA 256 bit, RSA 3072 bit, HMAC 256 bit, DRBG 512 bit	Power up Cryptographic Tests
Show Status	SHA-256	SHA 256 bit	SEM Services Status

*When these services are used with DES keys the module is operating in a non FIPS 140-2 approved mode.

Table 8 – User Services

3.2.1 Decryption of Cipher Text Keys with a KSKEK

All keys that are stored outside of the Module's boundary are stored in encrypted format. This service is provided by the Module's FIPS approved AES algorithm to retrieve encrypted keys from outside of the Module's boundary into the Module's boundary, decrypt the keys, and use the keys. All keys are decrypted using the AES algorithm and the 256 bit AES KSKEK.

3.2.2 Encrypt Digital Communication

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

3.2.3 Decrypt Digital Communication

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

3.2.4 Power-up Self-Test

This service provides power up and continuous tests to verify the secure state and operation of the Module. All of the module's algorithms are tested using KATs. The user initiates this service by power cycling or resetting the module.

3.2.5 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 384 entropy bits from an external source. These bits are used to seed the working state of the DRBG.

3.3 CO Services

Service	Security Function(s) Used	Key Type and Length	General Mode of Operation
TIA P25 Phase 2 System Validation	AES DRBG	128 bit AES Key, DRBG 40 bit	Encryption
Generate KSKEK	DRBG	256 bit AES	Key Generation
Generate **KMACK**	DRBG SHA-256	256 bit Keyed Hashed MAC	Used for data authentication of new SEM Firmware
Generate **TEK**	DRBG	56 bit DES Key* or 256 bit AES Key	Key Generation
Encryption of Keys With a **KSKEK**	AES	256 bit AES KSKEK	Encryption
Decrypt Encryption Key using **KEK**	AES or DES	256 bit AES Key or 56 bit DES Key*	Decryption
Encrypt Encryption Key using **KEK**	AES or DES*	256 bit AES Key or 56 bit DES Key*	Encryption
Zeroize Keys	N/A	N/A	Clear Keys
Derive Key	AES	256 bit AES key	Encryption/Decryption
Flash Update	RSA	3072 bit	Signature Verification

*When these services are used with DES keys the module is operating in a non FIPS 140-2 approved mode.

Table 9 – CO Services

3.3.1 TIA P25 Phase 2 System Validation

This service uses the module's DRBG to generate an AES-128 system validation key. This is a temporary key used for validating the radio to the system.

3.3.2 Generate Key Storage Key Encryption Key (KSKEK)

This service uses the Module's Deterministic Random Bit Generator to generate the KSKEK, a 256 bit AES key. The KSKEK is used to encrypt other Module CSPs for storage outside of the Module boundary.

3.3.3 Generate Keyed-Hashed Message Authentication Code Key (KMACK)

This service uses the Module's Deterministic Random Bit Generator to generate the KMACK, a 256 bit HMAC-SHA-256 key. The KMACK is used to validate the authenticity of Module CSPs when they are retrieved from outside of the Module boundary.

3.3.4 Generate Traffic Encryption Key (TEK)

This service uses the Module's Deterministic Random Bit 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, or a 256 bit AES key. This is a temporary key used for encryption of traffic. When a DES key is used, the module is operating in a non FIPS 140-2 approved mode.

3.3.5 Encryption of Keys With a KSKEK

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

3.3.6 Decrypt Encryption Key Using KEK

This service is provided by the Module to decrypt a key using the KEK. The KEK can be either a 256 bit AES key or 56 bit DES key. The key being decrypted can also be an AES or DES key. When a DES key is used for either the KEK or the key to be decrypted, the module is operating in a non FIPS 140-2 approved mode.

3.3.7 Encrypt Encryption Key Using KEK

This service is provided by the Module's DES or AES algorithm to encrypt a key using the KEK. If either the KEK or algorithm used to encrypt the key is DES, the module is operating in a non FIPS 140-2 approved mode.

3.3.8 Zeroize Keys

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

3.3.9 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*.

3.3.10 Flash Update

This service provides the CO the capability of updating the Module's digitally signed firmware. A reset of the Module is performed when new firmware is loaded into the Module.

3.4 Services and CSP relationships

Table 10 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Service	CSPs						
	Key Storage Key Encryption Key (KSKEK)	Keyed-Hashed Message Authentication Code Key (KMACK)	Traffic Encryption Key (TEK)	Key Encryption Key (KEK)	DRBG Working State	Derived Key	System Validation Key
Decryption of Cipher text Keys With a **KSKEK**	R / E	R / E	R / E	R / E	-	-	-
Encrypt Digital Communication	-	-	E	-	-	-	-
Decrypt Digital Communication	-	-	E	-	-	-	-
Power-up Self-Tests	-	-	-	-	-	-	-
Show Status	R	R	-	-	G	-	-
TIA P25 Phase 2 System Validation	R / E	R / E	-	-	E / W	-	E
Generate **KSKEK**	G	-	-	-	E / W	-	-
Generate **KMACK**	-	G	-	-	E / W	-	-
Generate **TEK**	-	-	G	-	E / W	-	-

Service	CSPs						
	Key Storage Key Encryption Key (KSKEK)	Keyed-Hashed Message Authentication Code Key (KMACK)	Traffic Encryption Key (TEK)	Key Encryption Key (KEK)	DRBG Working State	Derived Key	System Validation Key
Encryption of Keys With a **KSKEK**	R / E	R / E	W	G	-	-	G
Decrypt Encryption Key using **KEK**	R / E	R / E	W	R / E	-	-	-
Encrypt Encryption Key using **KEK**	R / E	R / E	R / E	R / E	-	-	-
Zeroize Keys	Z	Z	Z	Z	Z	-	Z
Derive Key	-	-	E	-	-	G	-
Flash Update	Z	Z	Z	Z	Z	Z	Z

Table 10 – CSP Access Rights within Services

4 Self-Test

4.1 Power Up Self-Tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 11 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the Fatal Error Alarm state.

The operator is notified of a self-test failure when there is no response to any messages. The module becomes unresponsive in the Fatal Error Alarm State. For example, the first message sent to the module is always a “Powerup Request” message (which contains the entropy for seeding the DRBG); the operator will fail to receive the “Powerup Status” message in response if a self-test failure has occurred.

Test Target	Description
Firmware Integrity	SHA1 performed over all code in flash.
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 256 bits
DRBG	KATs: HASH DRBG
HMAC	KATs: Generation, Verification SHA sizes: SHA-256
RSA	KATs: Signature Verification Key sizes: 3072 bits
SHA	KATs: SHA-256

Table 11 – Power Up Self-tests

4.2 Conditional Self-tests

Two conditional self-tests are performed on the module. They are shown in Table 12 below.

A RSA 3072-bit signature is used to verify firmware load on the module. During the firmware upgrade process a message "Download Code Signature" is sent to the module which contains the RSA signature. The operator will receive a "Download Code Signature Response" message which will inform the operator of either a success or failure in signature verification.

Each time the DRBG is used to generate a random number a continuous block test is run on the generated output. The DRBG must not produce an identical random number in succession. If this failure does occur the module immediately enters the Fatal Error Alarm state and becomes unresponsive. The operator is notified of this condition when there are no responses to any messages.

Test Target	Description
Firmware Load	RSA 3072 signature verification performed when firmware is loaded.
DRBG	Continuous block test on output of DRBG

Table 12 – Conditional Self-tests

5 Physical Security Policy

The Module consists of production grade components. In its application, the Module 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.

6 Operational Environment

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

7 Mitigation of Other Attacks Policy

The Module 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.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

8.1 FIPS 140-2 Related Security Rules

1. The module shall provide two distinct operator roles: User and Cryptographic Officer. The role is selected implicitly by the service that is invoked.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support concurrent operators.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.
14. The module does not output intermediate key values.

8.2 EFJohnson Technologies Imposed Security Rules

1. The SEM does not support a bypass mode.
2. All Single DES algorithms are present only to allow the module to inter-operate with existing legacy systems. When the operator uses any DES algorithm the module is operating in a non FIPS 140-2 approved mode.

3. The initial invocation of the Show Status service is accompanied by 66 bytes of data, which contain at least 384 bits of entropy.
4. The Module, when used in conjunction with an EFJohnson Technologies series VP600 portable radio or series VM600 mobile radio meets all of the applicable requirements of the FCC rules.
5. The Module protects all plaintext keys and critical security parameters from disclosure, modification, or substitution within the Module cryptographic boundary.
6. The Module provides the capability to zeroize all plaintext secret keys and critical security parameters within the module.
7. The Module operating environment does not have an underlying operating system. The Module's operating environment is implemented in hardware, is static, and non-modifiable.
8. The Module outputs a successful status indicator via the ARM SPI 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 SPI interface. This indicates an error has occurred, and the Module 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.
9. 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.

9 References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-57]	*Recommendation for Key Management*, Part 1 July 2012, Part 2 August 2005, Part 3 December 2009
[SP800-90A]	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012
[SP800-107]	*Recommendation for Applications Using Approved Hash Algorithms,* August 2012
[FIPS186-3]	*Digital Signature Standard*, June 2009
[FIPS198-1]	*The Keyed-Hash Message Authentication Code*, July 2008
TIA-AACA	*APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards*, TSB102.AACA
TIA-AACE-A	*Digital Land Mobile Radio Link Layer Authentication,* April 2011.
TIA P25 Standard	*Digital Radio Over-the-Air-Rekeying (OTAR) Protocol Addendum 1 – Key Management Security Requirements for Type 3 Block Encryption Algorithms*.

Table 13 – References

10 Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher-Feedback
CSP	Critical Security Parameter
DC	Direct Current
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSP	Digital Signal Processor
ECB	Electronic Codebook
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards

Acronym	Definition
HMAC	Keyed-Hashing for Message Authentication
KAT	Known Answer Test
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
LMR	Land Mobile Radio
OFB	Output-Feedback
OTAR	Over-The-Air-Rekeying
P25	Project 25
ROM	Read Only Memory
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman Public-Key cryptography algorithm
SEM	Subscriber Encryption Module
SHA-256	Secure Hash Algorithm-256 bits
SMA	EFJ Subscriber Management Assistant
SPI	Serial Programming Interface
TIA	Telecommunication Industry Association
TEK	Transmission Encryption Key
UCM	Universal Crypto Module

Table 14 – Acronyms and Definitions