Teletec Corporation

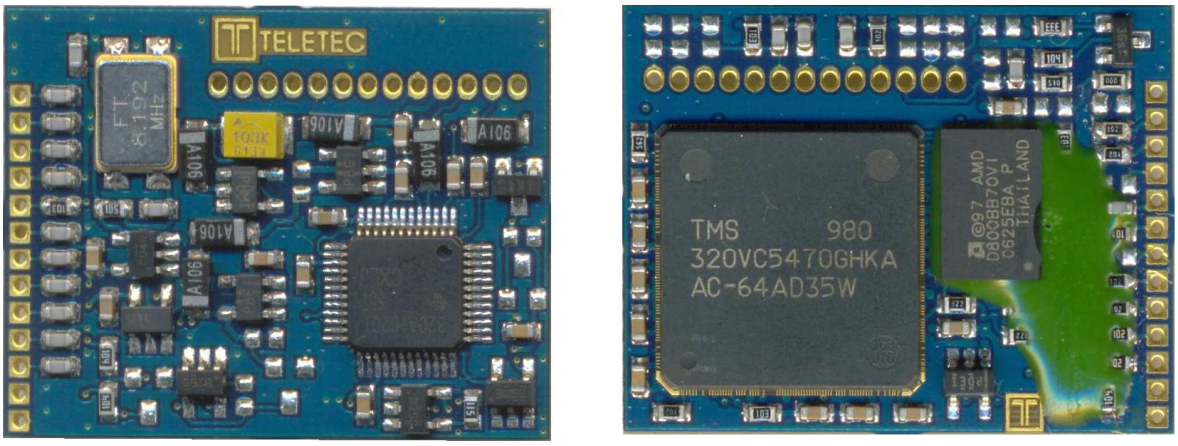
Security Policy
Subscriber Encryption Module

Document Version 13

TABLE OF CONTENTS

1. MODULE OVERVIEW

The Subscriber Encryption Module (SEM) is a multi-chip embedded cryptographic module intended to be installed in conventional FM radio equipment. The primary purpose for this device is to provide encrypted digital communication. Figure 1-1 shows a physical view of the module. The diagram 1-1 illustrates module structure and physically contiguous cryptographic boundary, which is defined as the outer perimeter of the SEM PCB.



front side back side

Figure 1-1: *Physical View of the Cryptographic Module*

FLASH memory contains CSPs and firmware components. Firmware for ARM core realizes cryptographic functions and FSM. All code that is executed on ARM affects the security of the cryptographic module, because this core has direct access to FLASH memory. On power-up, DSP firmware is loaded to internal RAM by ARM. DSP code contains both security relevant components such as data routing and non-security relevant components that do not need to meet requirements of FIPS 140-2. These non-security relevant components are:

- MELP vocoder
- QPSK subcarrier modem
- Automatic Gain Control
- Silicon Serial Number readout

This security policy is applicable to the following versions of hardware and firmware:

- Hardware: R2
- Main firmware: v1.00.02
- Bootloader firmware: v1.00.01

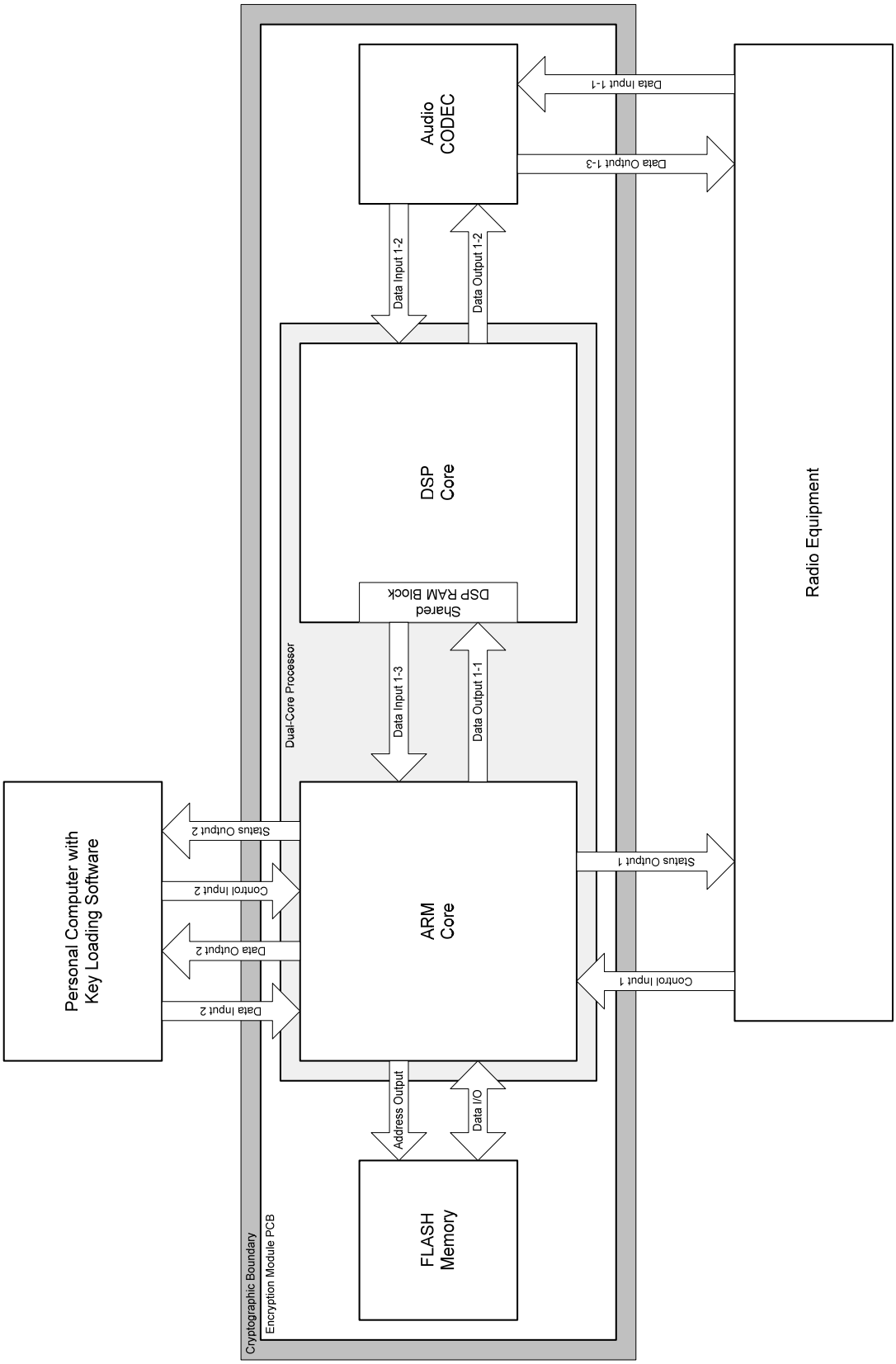


Diagram 1-1: *Encryption module components, ports and cryptographic boundary*

2. INTENDED FIPS 140-2 SECURITY LEVELS

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

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

Table 2-1: *SEM Security Levels*

3. MODES OF OPERATION

3.1. Approved Mode of Operation

SEM cryptographic module only supports a FIPS mode of operation.

SEM supports electronic key entry and output using the key loading software executed on a non-networked PC. Key loading is performed by means of serial programming cable, connecting SEM with COM or USB port. Cryptographic keys and other CSPs are transferred in plaintext form. CSPs entered using “Key Loader” software are verified in CEM with applied EDC (CRC32).

Here is a list of cryptographic algorithms that are supported by SEM (with certificate numbers):

1. AES-256 OFB for voice encryption (AES: #826)
2. AES-256 ECB, on which base AES-256 OFB is implemented (AES: #826)
3. HMAC-SHA-1 used in firmware load test (SHA: #825, HMAC: #460)
4. PRNG to generate initialization vectors (RNG: #476)

The PRNG is implemented using AES-256 as described in "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms", National Institute of Standards and Technology, January 31, 2005. ARM 5ms timer/counter output is taken as date/time vector, required in this document.

4. PORTS AND INTERFACES

The SEM cryptographic module provides the following physical ports and logical interfaces:

4.1. Radio Equipment Connector

Contact #	Name	Purpose	Type
1	CSQ In	Input from carrier detector	not used
2	PTT In	“Transmit Mode” input	not used
3	SCR Out	“Encrypted Channel” output to LED	status output
4	SCR2 In	Bypass selection input	control input
5	Tx In	Input from microphone	data input
6	Rx In	Input from discriminator	data input
7	SCR1 In	Bypass selection input	control input
8	PTT InOut	“Transmit Mode” input/output	control input
9	GND	Ground	-
10	Vcc	External supply voltage from radio equipment	power port
11	Rx Out	Output to speaker amplifier	data output
12	Tx Out	Output to modulator	data output
13	PTT Out	“Transmit Mode” output	not used

4.2. Auxiliary Connector

Contact #	Name	Purpose	Type
1	GND	Ground	-
2	VCC_IN	External supply voltage from Key Loader (while removed from radio)	power port
3	R_AUX0	Reserved	not used
4	R_AUX1	Reserved	not used
5	R_AUX2	Reserved	not used
6	R_AUX3	Reserved	not used
7	R_AUX4	Reserved	not used
8	R_PRG_TX	Maintenance/Key Loader port: serial transmit	data output status output
9	R_PRG_RX	Maintenance/Key Loader port: serial receive	data input control input
10	R_AUX5	Reserved	not used
11	R_AUX6	Test port: serial transmit	not used
12	R_AUX7	Test port: serial receive	not used
13	R_PA_CTRL	“Enable Speaker Amplifier” output	not used

The module supports a maintenance interface through which an authorized maintenance operator can service the module. The interface can be accessed by removing the radio’s outer case; the module must be zeroized upon entry and exit of the maintenance interface.

5. IDENTIFICATION AND AUTHENTICATION POLICY

5.1. Assumption of Roles

The SEM cryptographic module shall support three distinct operator roles (User, Crypto Officer, and Maintenance). As a Level 1 cryptographic module, the SEM does not support authentication. The role is implicitly selected by the service that is initiated.

Before the module will be serviced by maintenance engineer, crypto officer must first perform key zeroization using following instruction.

Using Key Loader software full zeroization of the module is performed by sequentially executing two commands: “Zeroize” and “Zeroize HMAC Key”, that are located in “Module” menu as it is displayed on picture 5-1. The module should be connected to PC using serial programming cable before invoking these commands.

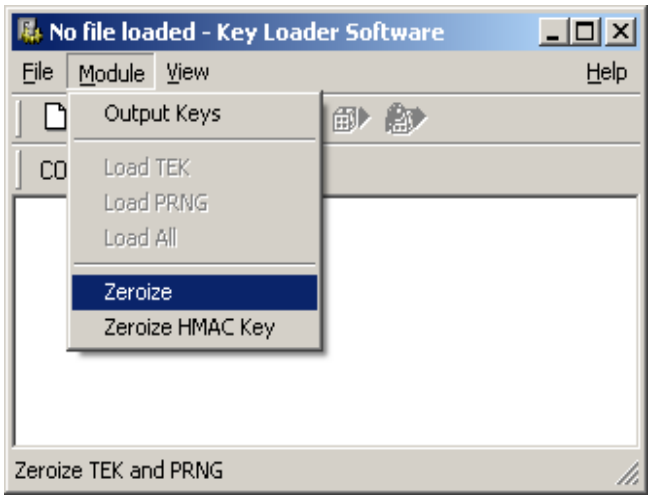


Figure 5-1: *"Zeroize" command in Key Loader software*

Role	Type of Authentication	Authentication Data
User	N/A	N/A
Crypto Officer	N/A	N/A
Maintenance	N/A	N/A

Table 5-1: *Roles and Required Identification and Authentication*

Authentication Mechanism	Strength of Mechanism
N/A	N/A

Table 5-2: *Strengths of Authentication Mechanisms*

6. ACCESS CONTROL POLICY

6.1. Roles and Services

Role	Authorized Services
User: This role shall provide all of the services necessary for secure digital communication.	• **Encrypt digital communication:** uses AES 256 OFB • **Decrypt digital communication:** uses AES 256 OFB • **Bypass selection:** select encrypted or unencrypted transmission and reception. • **Show status:** This service provides the current status of the cryptographic module. • **Power-up Self-tests:** This service, which can be invoked by cycling power to the radio, executes the suite of self-tests required by FIPS 140-2.

Crypto Officer: This role shall provide all of the services necessary for secure administration of the module.	• **Key Entry:** keys are manually established but electronically entered using "Key Loader" software • **Key Output:** keys are manually established but electronically outputted using "Key Loader" software • **Firmware Update:** load firmware with HMAC-SHA-1 verification • **Zeroize:** This service actively destroys all critical security parameters except for HMAC Key • **Zeroize HMAC Key:** This service actively destroys HMAC Key making future firmware update impossible • **Reset:** restarts execution of firmware. This service is invoked when key management tasks are complete. • **Power-up Self-tests:** This service, which can be invoked by cycling power to the radio, executes the suite of self-tests required by FIPS 140-2.
Maintenance: This role shall provide all of the services necessary for secure maintenance of the module.	• **Write Configuration:** load non-security relevant settings into the module • **Read Configuration:** readout non-security relevant settings from the module • **Zeroize:** This service actively destroys all critical security parameters except for HMAC Key • **Zeroize HMAC Key:** This service actively destroys HMAC Key making future firmware update impossible • **Reset:** restarts execution of firmware. This service is invoked when maintenance tasks are complete. • **Power-up Self-tests:** This service, which can be invoked by cycling power to the radio, executes the suite of self-tests required by FIPS 140-2.

Table 6-1: *Services Authorized for Roles*

6.1.1. Encrypt digital communication

This service performs encryption of transmitted voice messages with AES cipher in OFB mode. Voice messages inputted from microphone circuit of the radio are digitized by A/D converter and are compressed with MELP algorithm beforehand. Initialization vector for OFB mode is generated by ANSI X9.31 PRNG and is transmitted over the air before encrypted message data. TEK is used as encryption key and PRNG K and V are used for random IV generation. PRNG V is modified by this service at each PRNG algorithm iteration.

6.1.2. Decrypt digital communication

This service performs decryption of received voice messages with AES cipher in OFB mode using TEK as decryption key. Decrypted voice messages are then decompressed with MELP algorithm and are outputted through D/A converter into speaker circuit of the radio.

6.1.3. Bypass selection

This service selects encrypted or unencrypted transmission and reception by enabling or disabling exclusive bypass capability of the module. When a switch between a bypass and a cryptographic processing takes place, the bypass test is performed. To prevent the inadvertent bypass of plaintext data due to a single error, two independent internal actions are required to activate bypass capability.

Procedure of enabling exclusive bypass capability depends of how input ports of the module are configured. If the module is configured to use both SCR1 In and SCR2 In input ports, then both inputs should be driven to “inactive” state, for example with two switches, to activate this capability. If the module is configured to use only SCR1 In port that is connected to push-button of the radio then two sequential clicks of this button are required to activate exclusive bypass capability. When this capability is active, SCR Out port is driven to “inactive” logic state. Because this port controls dedicated LED or icon on LCD screen of the radio, operator can use this indication device to check if exclusive bypass capability is active in the current moment or not.

6.1.4. Show status

This service outputs the current status of the cryptographic module to SCR Out port. Additionally a number corresponding to the current state of the main FSM is outputted in binary code on four external lines: R_AUX0-R_AUX3, with least significant bit on R_AUX0. When Bootloader firmware is executed, code “0000b” is indicated on these lines.

6.1.5. Power-up Self-tests

This service, which can be invoked by cycling power to the module, executes the suite of self-tests required by FIPS 140-2 that includes:

- SHA-1 Known Answer Test
- HMAC-SHA-1 Known Answer Test
- AES Known Answer Tests
- PRNG Known Answer Test
- Firmware Integrity Test
    - Main Firmware Integrity Test
    - Bootloader Firmware Integrity Test
- Key Storage Integrity Test

Additional information regarding self-tests is provided in the “Self-Tests” document.

6.1.6. Key Entry

This service inputs cryptographic keys and other critical security parameters into the cryptographic module. Keys are manually established and are entered using “Key Loader” software running on personal computer. “Key Loader” software supports independent entry of TEK, PRNG K and PRNG V. Out of the factory the module comes with blank CSP storages intended for these parameters and it is required for Crypto Officer to load the keys before the module can perform User role services.

6.1.7. Key Output

This service outputs cryptographic keys and other critical security parameters out of the cryptographic module. Keys are outputted using “Key Loader” software running on personal computer. “Key Loader” software supports joint readout of TEK, PRNG K and PRNG V. Since PRNG V is modified at each iteration of PRNG algorithm, the value outputted by this service will differ from the entered one if “Encrypt digital communication” service was invoked at least once since last entry of this CSP.

6.1.8. Zeroize

This service actively destroys all critical security parameters stored in the module except for HMAC Key. Zeroization may take up to 5 seconds. During zeroization CSPs are not accessible via external ports and data output interface is disabled. It is required that during execution of this service a stable continuous electrical power will be provided to one of the two power ports: “Vcc” or “VCC_IN”. Zeroization methods are specified in the “Cryptographic Key Management” document.

6.1.9. Zeroize HMAC Key

This service actively destroys HMAC Key stored in the module. After HMAC Key zeroization module will not support “Firmware Update” service because firmware authenticity can not be verified without it. HMAC Key can be reloaded only at the factory, so if it is needed to restore firmware update capability of the module, it should be returned to vendor. During zeroization data output interface is disabled. It is required that during execution of this service a stable continuous electrical power will be provided to one of the two power ports: “Vcc” or “VCC_IN”. Zeroization methods are specified in the “Cryptographic Key Management” document.

6.1.10. Write Configuration

This service inputs non-security relevant settings into the module using “Configuration” software running on personal computer. Configuration parameters include:

- Pre-emphasis and de-emphasis settings for receive and transmit modes
- Gin settings for analog input and output ports
- Microphone AGC settings
- Active level for ports “SCR Out”, “SCR1 In”, “SCR2 In” and “PTT InOut”
- Bypass switch operation: using both “SCR1 In” and “SCR2 In” or only “SCR1 In”
- Modem parameters
- Encrypted/plaintext autodetect option for receive mode

6.1.11. Read Configuration

This service outputs non-security relevant settings stored in the module using “Configuration” software running on personal computer. List of configuration parameters is provided in the description of “Write Configuration” service.

6.1.12. Firmware Update

This service updates Main firmware stored in the Flash memory of the module. Before actual firmware load operation starts, this service erases current firmware, its CRC, firmware length table and zeroizes all critical security parameters stored in the module except for HMAC Key. After successful firmware load and MAC entry, Firmware Load Test is performed to verify authenticity of the new code. This test uses HMAC-SHA-1 algorithm to calculate firmware MAC. If the test fails, the newly loaded firmware will not be executed and module functionality will be restricted to the following services provided by Bootloader firmware:

- Firmware Update
- Zeroize HMAC Key
- Reset

6.1.13. Reset

This service restarts execution of firmware. Reset is accomplished by entering an endless loop that stops “re-initializing” impulses transmitted to external watchdog timer IC. When watchdog discovers loss of transitions on its input, it resets processor by holding RESET input low for a sufficient time. This service is invoked when crypto-officer or maintenance tasks are complete and module has to be restarted to re-enable user services.

6.2. Definition of Critical Security Parameters (CSPs)

The table 6-2 provides a list of all cryptographic keys and other critical security parameters that are contained in the module. Information regarding access to these parameters and zeroization is provided in the next subsection “Definition of CSPs Modes of Access”.

6.2.1. Traffic Encryption Key (TEK)

TEK, the Traffic Encryption Key is a 256-bit key that is used with AES algorithm in OFB mode for encryption/decryption of digital communication. It is entered and outputted by means of "Key Loader" software and programming cable that directly connects cryptographic module to COM or USB port. Out of the factory the module comes without TEK and it is required for Crypto Officer to load the key before the module can perform User role services. “Zeroize” service erases TEK stored in Flash memory and all RAM data derived from it, including AES expanded encryption and decryption keys.

6.2.2. HMAC Key

HMAC Key is a 160-bit key that is used with HMAC-SHA-1 algorithm in firmware load test. It is written in Flash memory on production stage of the cryptographic module together with Bootloader firmware. HMAC Key is not modifiable except for zeroization process. “Zeroize HMAC Key” service erases HMAC Key stored in Flash memory and its working copy in RAM.

6.2.3. PRNG K

PRNG K is a 256-bit key that is used as AES encryption key together with PRNG V in ANSI X9.31 RNG algorithm for the generation of pseudo random initialization vectors. It is entered and outputted by means of "Key Loader" software and programming cable that directly connects

cryptographic module to COM or USB port. Out of the factory the module comes without PRNG K and it is required for Crypto Officer to load the key before the module can perform User role services. “Zeroize” service erases TEK stored in Flash memory and all RAM data derived from it, including AES expanded encryption and decryption keys.

6.2.4. PRNG V

PRNG V is a 128-bit seed value that is used together with PRNG K in ANSI X9.31 RNG algorithm for the generation of pseudo random initialization vectors. It is entered and outputted by means of "Key Loader" software and programming cable that directly connects cryptographic module to COM or USB port. Out of the factory the module comes without PRNG V and it is required for Crypto Officer to load the seed before the module can perform User role services. Seed value is modified at each iteration of PRNG algorithm and if “Encrypt digital communication” service was invoked at least once since last seed entry, the value that will be outputted by the module at request of Crypto Officer will differ from the entered one. “Zeroize” service erases PRNG V stored in Flash memory and its working copy in RAM.

Cryptographic Key / CSP	Size, Bits	Algorithm / Approved	Generation	Entered	Output	Storage Across Power Cycles / Location / Form	Zeroized
TEK	256	AES / Yes	No	Yes / plaintext	Yes / plaintext	Yes / Flash memory and RAM / plaintext	Yes
HMAC Key	160	HMAC-SHA-1 / Yes	No	No	No	Yes / Flash memory and RAM / plaintext	Yes
PRNG K	256	ANSI X9.31 RNG using AES / Yes	No	Yes / plaintext	Yes / plaintext	Yes / Flash memory and RAM / plaintext	Yes
PRNG V	128	ANSI X9.31 RNG using AES / Yes	No	Yes / plaintext	Yes / plaintext	Yes / Flash memory and RAM / plaintext	Yes

Table 6-2: *Cryptographic Keys and CSPs*

6.3. Definition of CSPs Modes of Access

Table 6-2 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Read (R):** This operation reads the parameter from memory.
- **Write (W):** This operation writes the parameter to memory.
- **Input (I):** This operation supports the input of the parameter into the cryptographic module's physical boundary.
- **Output (O):** This operation supports the output of the parameter from the cryptographic module's physical boundary
- **Destroy (D):** This operation actively overwrites the parameter, thus destroying the item.

Role			Service	Cryptographic Keys and CSPs Access Operation			
Maint.	**C.O.**	**User**		**TEK**	**HMAC Key**	**PRNG K**	**PRNG V**
		X	Encrypt digital communication	R		R	R,W
		X	Decrypt digital communication	R			
		X	Bypass selection				
		X	Show status				
X	X	X	Power-up Self-tests				
	X		Key Entry	I, W		I, W	I, W
	X		Key Output	R, O		R, O	R, O
X	X		Zeroize	D		D	D
X	X		Zeroize HMAC Key		D		
X			Write Configuration				
X			Read Configuration				
	X		Firmware Update	D	R	D	D
X	X		Reset				

Table 6-3: *CSP Access Rights within Roles & Services*

7. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the SEM device has a limited operational environment. The module only supports firmware updates

using HMAC-SHA-1 verification; the cryptographic module does not support the loading or execution of untrusted code.

8. SECURE OPERATION AND SECURITY RULES

In order to operate the cryptographic module securely, the operator should be aware of the security rules enforced by the module and should adhere to secure operation rules required.

8.1. Security Rules

The SEM cryptographic module's design corresponds to the SEM cryptographic module's 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, and additional security rules imposed by vendor of this module.

8.1.1. FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2:

1. A cryptographic supports the following authorized roles for operators: User Role, Crypto Officer Role and Maintenance Role.

2. The cryptographic module shall perform the following tests:

    2.1.Power-up self-tests

        2.1.1. Cryptographic algorithm tests:

            2.1.1.1.AES Known Answer Tests

            2.1.1.2.PRNG Known Answer Test

            2.1.1.3.SHA-1 Known Answer Test

            2.1.1.4.HMAC-SHA-1 Known Answer Test

        2.1.2. Firmware Integrity Test

            2.1.2.1.Main Firmware Integrity Test

            2.1.2.2.Bootloader Firmware Integrity Test

        2.1.3. Critical functions tests:

            2.1.3.1.Key Storage Integrity Test

    2.2.Conditional self-tests:

        2.2.1. Firmware Load Test

        2.2.2. Key Entry Test

2.2.3. Continuous PRNG Test

2.2.4. Bypass Tests

2.2.5. PRNG Seed Test

3. Data output shall be inhibited during self-tests, key entry, key zeroization, and in error states.

4. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

5. The module shall not support concurrent operators.

8.1.2. Vendor imposed Security Rules

The following are security rules that result from the security requirements of FIPS 140-2 include the following rules:

1. Cryptographic module shall support only FIPS level 1 mode of operation.

2. Cryptographic module shall support only FIPS-approved security functions.

3. The operator shall assume a role based upon the service that is initiated; the cryptographic module shall not support authentication.

4. When assuming the Maintenance role, the operator shall procedurally invoke zeroization upon entering and exiting the maintenance interface. Invoking the zeroization service will cause all CSPs stored within the module to be destroyed (including the HMAC Key).

5. The cryptographic module shall support both encrypted digital communications and unencrypted communications.

6. Key generation is not supported.

8.2. Physical Security Rules

The SEM consists of production grade components and is manufactured employing standard commercial grade passivation techniques. In its application, the SEM is housed in the standard production grade housing of the portable or mobile radio product, which is considered as outside object of the cryptographic boundary.

8.2.1. Operator Required Actions

Since the cryptographic module does not provide any physical security beyond the use of production grade components, the user is not required to inspect the device.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

Table 8-1: *Inspection/Testing of Physical Security Mechanisms*

8.3. Secure Operation Initialization Rules

The crypto officer should follow the following rules to initialize a new cryptographic module. All operations are performed on a non-networked GPC.

1. Start “Key Loader” software.
2. Enter TEK in the “TEK” dialog of the “Key Loader” software. TEK has to be common between the modules of the communication group.
3. Enter PRNG K in the “PRNG K” dialog of the “Key Loader” software. This key must be unique for each device!
4. Enter PRNG V in the “PRNG V” dialog of the “Key Loader” software. This parameter must be unique for each device!
5. Connect programming cable and power-up the module.
6. Chose “Load All” from the “Module” menu to load all entered CSPs into the module. If all keys are entered correctly, after reset that terminates “Load All” command, the module will be ready to provide user role services.

Additional information regarding security administration and maintenance procedures can be found in the “Crypto Officer Guidance” document.

10. MITIGATION OF OTHER ATTACKS POLICY

The module has not been designed to mitigate specific attacks beyond the scope of FIPS 140-2 requirements.

11. REFERENCES

1. FIPS PUB 140-2: “Security Requirements for Cryptographic Modules”, NIST
2. “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”, NIST
3. FIPS PUB 197: “Advanced Encryption Standard (AES)”, NIST
4. NIST SP 800-38A: “Recommendation for Block Cipher Modes of Operation, Methods and Techniques”, NIST
5. FIPS PUB 180-2: “Secure Hash Standard”, NIST
6. FIPS PUB 198: “The Keyed-Hash Message Authentication Code (HMAC)”, NIST
7. “NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms”, NIST

12. ACRONYMS

AES	Advanced Encryption Standard
AGC	Automatic Gain Control
ANSI	American National Standards Institute
ARM	ARM architecture CPU design or one of its derivatives developed by ARM Ltd (originally called The Acorn RISC Machine)
CODEC	Coder-Decoder
COM	Communication port
CRC	Cyclic Redundancy Code
CRC32	32-bit Cyclic Redundancy Code
CSP	Critical Security Parameter
DSP	Digital Signal Processor
EDC	Error Detection Code
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
LED	Light-Emitting Diode
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PC	Personal Computer
PCB	Printed Circuit Board
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
SEM	Subscriber Encryption Module
SHA-1	Secure Hash Algorithm-1
TEK	Traffic Encryption Key

USB Universal Serial Bus