THALES

Liberty™ Cryptographic Module
Non-Proprietary Security Policy
Revision No - 12

Prepared by:

Thales Communications Inc.

22605 Gateway Center Drive

Clarksburg, MD 20871

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

This document describes the Security Policy that governs the FIPS-approved usage of the Liberty™ Cryptographic Module. It also provides the associated User Guidance and Crypto Officer Guidance for this module.

1.2 Liberty™ Cryptographic Module Definition

The Liberty™ Cryptographic Module, hereafter referred to as LCM, is defined as a firmware cryptographic module executable code. This document contains information required for a FIPS 140-2 Level 1 certification.

The LCM is a stand-alone firmware module. It executes in a single operator mode, and it can operate in an Approved or Non – Approved Modes. It is intended to be used in radio communications equipment that utilizes the APCO Project 25 standard.

The LCM has no bypass capabilities.

Figure 1 LibertyTM Cryptographic Module Block Diagram, highlights the main blocks that make the LCM, and its interfaces.

As a non-hardware cryptographic module, the FIPS 140-2 physical security requirements are not applicable to the LCM.

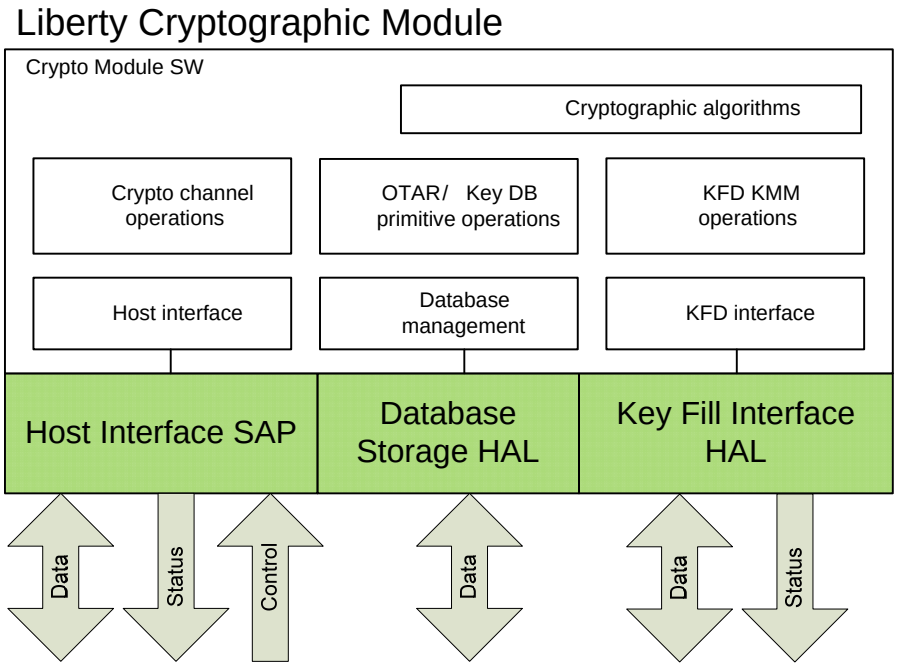

Figure 1 Liberty™ Cryptographic Module Block Diagram

1.3 Acronyms and Abbreviations

Term	Elaboration
AES	Advanced Encryption Standard
APCO	Association of Public-Safety Communications Officials
CSP	Critical Security Parameter
DES	Data Encryption Standard
FIPS	Federal Information Processing Standards
HAL	Hardware Abstraction Layer
HMAC	Hash-based Message Authentication Code
KEK	Key Encryption Key
KFD	Key Fill Device
KMF	Key Management Facility
KMM	Key Management Message
KSK	Key Storage Key
MAC	Message Authentication Code
MNP	Message Number Period
OTAR	Over-the-Air Rekeying
PRNG	Pseudo Random Number Generator
P25	Project 25
RNG	Random Number Generator
RSI	Radio Set Identifier
RSK	RNG Seed Key
SAP	Service Access Point
SHA-1	Secure Hash Algorithm-1
LCM	Liberty™ Crypto Module
TEK	Traffic Encryption Key
UKEK	Unique KEK

1.4 Design Assurance

1.4.1 Configuration Management

The Liberty™ Cyptographic Module is contained in a single firmware configuration item:

- FipsCryptoModule: Version 01.00.05.0018

This is a binary GHS integrity loadable address space. It can be loaded on a device separately or embedded in the device main operational firmware (application). In the latter case the device application must load "FipsCryptoModule". The FIPS Crypto module maintains its own version number and can report it to the application.

All source code and build files are maintained in a separate configuration database and are baselined to allow recreation of the exact binary FipsCryptoModule CI:

- Baseline: Liberty_Crypto_01.00.05.0018

1.5 References

[1] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules,* FIPS PUB 140-2, May 25, 2001 (Change Notices 12-03-2002).

[2] National Institute of Standards and Technology, *Data Encryption Standard (DES),* FIPS PUB 46-3, October 25, 1999.

[3] National Institute of Standards and Technology, *Advanced Encryption Standard (AES),* FIPS PUB 197, November 26, 2001.

[4] National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)* FIPS PUB 198-1, July 2008

[5] National Institute of Standards and Technology, *Digital Signature Standard,* FIPS PUB 186-2, January 27, 2000.

[6] Telecommunications Industry Association, *Digital Land Mobile Radio, Security Services Overview,* ANSI/TIA-102.AAAB-2002, July 2002.

[7] Telecommunications Industry Association, *TIA/EIA STANDARD, Project 25 Digital Radio Over-the-Air Rekeying (OTAR) Protocol,* TIA/EIA-102.AACA, April 2001.

[8] Telecommunications Industry Association, *TIA STANDARD, Project 25 Digital Radio Over-the-Air-Rekeying (OTAR) Protocol, Addendum 2 – Data Link Independent OTAR* TIA-102.AACA-2, March 2003.

[9] Telecommunications Industry Association, *TIA STANDARD, Project 25 – Over-the-Air-Rekeying (OTAR) Operational Description,* TIA-102.AACB, November 2002.

[10] Telecommunications Industry Association, *TIA STANDARD, Project 25 Key Fill Device (KFD) Interface Protocol,* TIA-102.AACD, February 2005.

2 Ports and Interfaces

The LCM has the following Service Access Point (SAP) and Hardware Abstraction Layer (HAL) interfaces.

2.1 Host Interface SAP

The LCM implements a messaging interface via which it receives commands from the Host and returns the results of handling those requests.

The Data Input Interface for this SAP consists of the data input parameters of the SAP's input request messages. Likewise, the Data Output Interface consists of the data output parameters of the SAP's output confirmation messages.

The Control Input Interface for this SAP consists of the control input parameters of the SAP's input request messages.

The Status Output Interface for this SAP consists of the result parameter of the SAP's output confirmation messages.

2.2 Database Storage HAL

The LCM implements management for storing and retrieving key material. The platform-dependent storage hardware is abstracted by the database storage HAL.

The Data Input Interface for this HAL consists of the data input parameters of the HAL's input request messages. Likewise, the Data Output Interface consists of the data output parameters of the HAL's output confirmation messages.

2.3 Key Fill Interface HAL

Provides the logical interface required for key fill. The platform-dependent external device interface is abstracted by the key fill interface HAL.

The Data Input Interface for this HAL consists of the data input parameters of the HAL's sole input indication message. Likewise, the Data Output Interface consists of the data output parameters of the HAL's sole output response message.

The Status Output Interface for this HAL consists of the HAL's output response message itself.

2.4 Logical to Physical Interface Mapping

The LCM interfaces physically to the PXA-320 processor RAM, through the PXA-320 MMU memory controller. In the tested physical deployment the host platform has several physical devices that are the ultimate destination or source of the information on the logical interfaces.

Logical Interface	Physical Interface	Host Interface	Comment
Host Interface SAP	RAM	RAM	GHS Integrity inter-address space communication OS services
Database Storage HAL	RAM	Flash ROM	GHS Integrity inter-address space communication OS services. GHS file system read/write on host, which uses FLASH ROM (NAND) for storage.
Key Fill Interface HAL	RAM	Shared RAM	GHS Integrity shared RAM address space. GHS Integrity inter-address space synchronization services (semaphore). Host P25 compliant P25 key fill device (KFD) serial port and driver to transfer device data to/from shared RAM

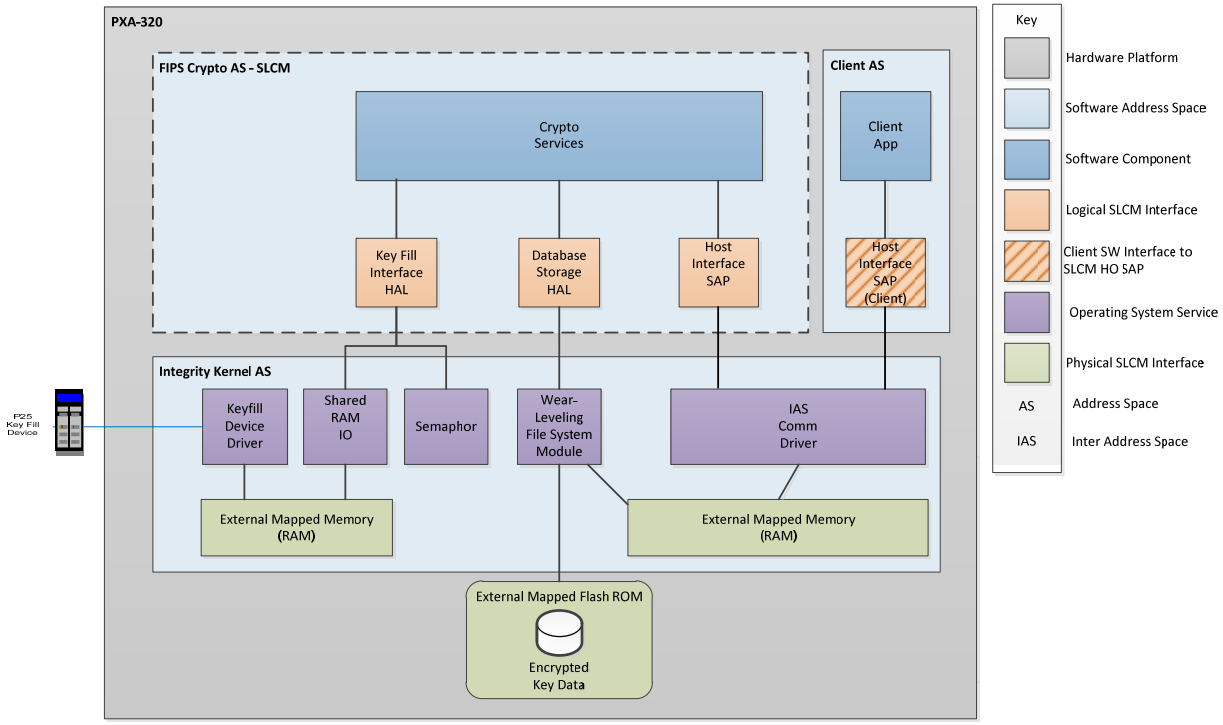

Figure 2 Logical and Physical LCM Interfaces

3 Operational Environment

The LCM executes in RAM on a general purpose processor (GPP) which is categorized as a modifiable operational environment. The LCM relies on operating system (OS) address space separation to ensure non FIPS approved software or firmware does not have access to this environment. The operating system (OS) used to support the execution of the LCM is Green Hills Integrity 5.0.10.

For the LCM, the Green Hills Integrity 5.0.10 OS is restricted to a single operator mode of operation.

The LCM testing and algorithm validation was performed on a Marvel PXA-320 general purpose processor (GPP).

The processor interfaces to RAM (DDR SDRAM) and ROM (NAND FLASH). GHS Integrity utilizes the hardware MMU capability in the PXA-320 processor to isolate the RAM used by the LCM address space (other address spaces cannot access). The FLASH ROM is only accessed through the LCM Database Storage HAL, and all data output to the Database Storage HAL is encrypted.

3.1 Test Environment

The Thales LCM was tested while running on a Thales Liberty Radio PRC7332.

3.2 Cryptographic Boundary

The cryptographic boundary, for the LCM, is made up by the compiled application executable file.

4 Roles, Services and Authentication

4.1 Roles

The LCM supports a single operator mode. The single operator can assume the roles of a 'User' or a 'Crypto Officer', only one role at a time. Operator authentication is not supported. Also, no maintenance role is supported.

Roles are implicitly selected when service calls are made to the LCM via its service access points.

Table 1 Single Operator Mode Roles

Role	Authentication
User	None
Crypto Officer	None

The services provided by the LCM are grouped in two main categories, Host Services and Key Fill Device Services. Despite the presence of the Database Storage HAL, there are no database services exported by the LCM. All database interaction is internally controlled by the LCM. The LCM only permits for one service to be invoked at a time.

4.2 Self-Tests

The LCM provides power-up and conditional self-tests.

The LCM will enter an error state and issue a failure status indication via the Host Interface status output should any self-test fail. Once in this error state, the LCM can only be recovered by powering it off and on again. In addition, the LCM will inhibit any data output and will not perform any cryptographic operations while in this state.

4.2.1 Power-Up Self-Tests

The LCM automatically runs a set of self-tests during its self-initialization sequence at power-up. These power-up self-tests include the following:

- Firmware integrity test using HMAC-SHA-1
- Known-answer-tests for all approved cryptographic algorithms: AES, PRNG, both implementations of SHA-1, and HMAC.
- Initial iteration of the approved RNG continuous random number generator test (4.2.3 Continuous Random Number Generator Test).

While performing these tests, the LCM will inhibit all data output. It will issue a success or failure indication via the Host Interface status output upon completing the tests. If a power up self test fails the LCM will enter the error state, and data output will remain inhibited.

These power-up self-tests will also run on-demand, when an appropriate request is issued via the Host Interface control input.

4.2.2 Conditional Self-Tests

4.2.3 Continuous Random Number Generator Test

When the approved random number generation function is invoked via the Host Interface, the LCM will perform a continuous random number generator test. If the continuous random number generator test fails the LCM will enter the error state, and data output will remain inhibited.

4.2.4 Firmware Integrity Load Test

The LCM provides the following host services to allow the LCM host to allow the host software to test the integrity of a new LCM image:

Firmware Integrity Test Algorithm Initialization
Firmware Integrity Test Algorithm Process
Firmware Integrity Test Algorithm Complete

The host software may use these services to calculate the HMAC of a new image before overwriting the old image. The LCM is loaded on host restart and cannot be (re)loaded while the current LCM image is operational. Section 9.3 Module Installation and Startup contains crypto officer guidance for using this service.

4.3 Host Services

Host Services are those services provided via the Host Interface SAP. Each service is implicitly associated with only one of the single operator roles, user or crypto officer, and is assumed when the service is invoked.

Table 2 shows the Host Services, the role approved for using these services, and a brief description of the service.

Each Host Service takes an input handle parameter, which the LCM returns unmodified as an output handle parameter in the associated confirmation message, allowing the client to track different requests. Note that this is an unlisted input parameter for every Host Service listed in the table below. It is not explicitly listed, since every service requires it.

Table 2 Host Services

Host Service	Approved Role	Non-Approved Role	Host Service Description
Boot Start	User	None	Configure LCM features and startup module. **Inputs:** Enabled Features Flags. **Outputs:** Result, scRetrieveSensitiveConfigReq
scRetrieveSensitiveConfigCnf	User	None	Provide KSK and RNG Seed keys. (KSKSK, RSK) **Inputs:** Sensitive configurarion data: KSK Seed Data, Entropy Data **Outputs:** None
Channel Open	User	User	Open cryptographic channel for data processing. **Inputs:** Channel Type, Channel Number, Mode, Message Length,

Host Service	Approved Role	Non-Approved Role	Host Service Description
			Derived Key Flag, Algorithm ID, Key Address, Message Indicator (Optional). **Outputs:** Result, Current Message Indicator, Clocked Message Indicator.
Channel Data	User	User	Encryption/ Decryption of data in a voice or data channel, or Message Authentication Code (MAC) generation from message in a MAC channel. **Inputs:** Channel Type, Channel Number, Channel Data. **Outputs:** Result, Channel Data.
Channel Close	User	User	Close cryptographic channel. **Inputs:** Channel Type, Channel Number. **Outputs:** Result, Channel Data.
Channel Short Data	User	User	Encryption/ Decryption of data in a voice or data channel, or Message Authentication Code (MAC) generation from message in a MAC channel. Cryptographic channel state is not saved for subsequent processing. **Inputs:** Channel Type, Channel Number, Mode, Message Length, Derived Key Flag, Algorithm ID, Key ID, Key Address, Message Indicator (Optional), Channel Data. **Outputs:** Result, Channel Data, Current Message Indicator.
Set Key	Crypto	Crypto	Store a key.

Host Service	Approved Role	Non-Approved Role	Host Service Description
	Officer	Officer	**Inputs:** Keyset ID, Key algorithm ID, Key ID, Key Type, Key Name, SLN, KEK Algorithm ID, KEK Key ID, Temporary Key Flag, Key Name, Key Material. **Outputs:** Result.
Delete Key	Crypto Officer	Crypto Officer	Delete a stored key. **Inputs:** Key Type (Optional), Algorithm ID, Key ID, Key Address (Optional). **Outputs:** Result.
Delete Keyset	Crypto Officer	Crypto Officer	Delete a stored Keyset. **Inputs:** Keyset ID. **Outputs:** Result.
Changeover Keyset	Crypto Officer	Crypto Officer	Change to a new active Keyset. **Inputs:** Superseded Keyset ID, Activated Keyset ID. **Outputs:** Result, Superseded Keyset ID, Activated Keyset ID.
Set Keyset Info	Crypto Officer	Crypto Officer	Stores Keyset information. **Inputs:** Keyset ID, Algorithm ID, Key Type, Keyset Name. **Outputs:** Result.
Get Key Info	Crypto Officer	Crypto Officer	Reports information on stored keys. **Inputs:** Iteration Marker, Filter Type, Keyset ID (Optional), Storage Location Number (Optional). **Outputs:** Result, Iteration Marker, Key IDs, Key Keyset IDs, Key Storage Location Numbers, Key Statuses.

Host Service	Approved Role	Non-Approved Role	Host Service Description
Set Key Assignment	Crypto Officer	None	Stores Key assignment mapping information. **Inputs:** Key Assignment Type, Key Assignment ID, Storage Location Number. **Outputs:** Result.
Get Key Assignment	Crypto Officer	None	Retrieve stored key assignment mapping information. **Inputs:** Key Assignment Type, Iteration Marker. **Outputs:** Result, Iteration Marker, Key Assignments.
Set RSI	Crypto Officer	None	Store Over The Air Rekey RSI information. **Inputs:** Affected RSI, New RSI, Message Number. **Outputs:** Result.
Get RSI	Crypto Officer	None	Retrieve Over The Air Rekey RSI information. **Inputs:** RSI or RSI Type. **Outputs:** Result, KMF RSI, Incoming Message Number, Outgoing Message Number, Message Number Period, RSIs.
SetKmfRsi	Crypto Officer	None	Store Key Management Facility RSI information. **Inputs:** RSI. **Outputs:** Result.
SetMnp	Crypto Officer	None	Store Message Number Period. **Inputs:** MNP.

Host Service	Approved Role	Non-Approved Role	Host Service Description
			Outputs: Result.
Set Reverse Warm Start Policy	Crypto Officer	Crypto Officer	Store policy for Over The Air Rekey reverse warm start procedure **Inputs:** TEK Algorithm ID. **Outputs:** TEK Key ID.
Zeroize	User	None	Zeroize a select portion or all critical security parameters. **Inputs:** Level of zeroization. **Outputs:** Result.
Get Keyset IDs	Crypto Officer	None	Reports IDs of stored Keysets. **Inputs:** None. **Outputs:** Result, Keyset IDs, Keyset Statuses.
Get Keyset Info	Crypto Officer	Crypto Officer	Retrieves stored Keyset information. **Inputs:** Keyset ID. **Outputs:** Result, Keyset ID, Algorithm ID, Key Type, Keyset Name.
Generate Warm Start Key	Crypto Officer	Crypto Officer	Generate a key for use in the Over The Air Rekey reverse warm state segment. **Inputs:** TEK algorithm ID, TEK Key ID, TEK address, KEK algorithm ID, KEK Key ID, KEK address (All optional inputs) **Outputs:** Result algorithm ID, Key ID, Key adresss, KEK algorithm ID, KEK address, Wrapped Key material.
Validate Algorithm	User	None	Run a validation test for an algorithm.

Host Service	Approved Role	Non-Approved Role	Host Service Description
			Inputs: Validation mode, SHA reset, SHA complete, key, initialization vector, plain text, cipher text **Outputs:** Result, key, initialization vector, plain text, cipher text.
Validate Key	Crypto Officer	None	Validates the existence of a key. **Inputs:** Key Type, Algorithm ID, Key ID. **Outputs:** Result.
Firmware Integrity Test Algorithm Initialization	Crypto Officer	None	Configures the algorithm used for firmware integrity checks. **Inputs:** Algorithm ID*, Data, Data Length. **Outputs:** Result.
Firmware Integrity Test Algorithm Process	User	None	Processes one of a series of data blocks to be integrity checked. Called serially until all data blocks have been provided. **Inputs:** Algorithm ID*, Data, Data Length. **Outputs:** Result.
Firmware Integrity Test Algorithm Complete	User	None	Called after all data blocks have been provided via Firmware Integrity Test Algorithm Process in order to compute and compare the integrity check value to the expected value. **Inputs:** Algorithm ID*, Result Expected, Result Expected Length. **Outputs:** Result, Result Calculated, Result Calculated Length.

Host Service	Approved Role	Non-Approved Role	Host Service Description
Show Status	User	User	The LCM supports the "Show Status" service by issuing confirmation messages for each requested Host Service. Each confirmation message contains a result parameter, which indicates the status of the associated request.
Perform Self-Tests	User	None	The self tests are performed by initializing the LCM by invoking the "Boot Start" service. The self test service cannot be run independently of the power up/self test service.

*NOTE: Only HMAC-SHA-1 is supported for the Firmware Integrity Test services.

4.4 Key Fill Services

Key Fill Services are those logical services provided to an attached Key Fill Device via the Key Fill Interface HAL. The HAL consists of a single input message, the indication message, which contains the raw Key Management Message (KMM) data from the Key Fill Device. Likewise, the HAL has a single output message, the response message, which also uses KMM formatting. The incoming KMMs are decoded, in order to establish which service is being requested.

Table 3 shows these logical Key Fill Device Services, the role approved for using these services, and a brief description of the service.

The LCM supports the "Show Status" service by issuing the output response message for each input indication message it receives.

Table 3 Key Fill Device Services

Key Fill Device Service	Approved Role	Non Approved Role	Key Fill Device Service Description
KFD Inventory – List Active Keyset IDs	Crypto Officer	None	Retrieve the active Keyset IDs. **Inputs:** None. **Outputs:** Active keyset IDs.
KFD Inventory – List Active Keys	Crypto Officer	Crypto Officer	Retrieve the stored Keyset IDs, SLNs, Algorithm IDs and Key IDs of the active keys. **Inputs:** Inventory marker, maximum key count. **Outputs:** Inventory marker, key keyset IDs, key storage location numbers, key algorithm IDs, key IDs.
KFD Inventory – List RSI Items	Crypto Officer	None	Retrieve the stored individual RSI and group RSIs. **Inputs:** None. **Outputs:** RSIs, message numbers.
KFD Inventory – List KMF RSI	Crypto Officer	None	Retrieve the stored KMF RSI. **Inputs:** None. **Outputs:** KMF RSI.
KFD Inventory – List Message Number Period	Crypto	None	Retrieve the stored MNP parameter.

Key Fill Device Service	Approved Role	Non Approved Role	Key Fill Device Service Description
(MNP)	Officer		**Inputs:** None. **Outputs:** Message number period.
KFD Inventory – List Keyset Tagging Info	Crypto Officer	Crypto Officer	Retrieve stored Keyset information. **Inputs:** None. **Outputs:** Keyset IDs, keyset algorithm IDs, update instruction blocks (optional), date times (optional), keyset names (optional)
KFD Modify Key	Crypto Officer	Crypto Officer	Modify, set or erase a stored key. **Inputs:** KEK Algorithm ID, KEK Key ID, Update Count (Optional), Message Indicator (Optional), Keyset ID, Keyset Algorithm ID, Storage Location Numbers, Key IDs, Key Materials, Key Checksums (Optional), Key Names (Optional). **Outputs:** Algorithm IDs, Key IDs, Modify Key Statuses.
KFD Change RSI	Crypto Officer	None	Change or set the individual RSI or a group RSI. **Inputs:** Changed RSIs, Added RSIs, Message Numbers. **Outputs:** Changed RSIs, Added RSIs, Change RSI Statuses.
KFD Load Config	Crypto Officer	None	Load KMF configuration parameters (KMF RSI, MNP) into the module. **Inputs:** KMF RSI, Message Number Period. **Outputs:** KMF RSI, Message Number Period, Result.
KFD Zeroize	Crypto Officer	None	Zeroize all critical security parameters.

Key Fill Device Service	Approved Role	Non Approved Role	Key Fill Device Service Description
			Inputs: None. **Outputs:** None.
KFD Changeover	Crypto Officer	Crypto Officer	Perform a keyset changeover from one stored keyset to another stored keyset. **Inputs:** Superseded Keyset IDs, Activated Keyset IDs. **Outputs:** Superseded Keyset IDs, Activated Keyset IDs.

4.5 Database HAL Services

The client software/platform provides non volatile storage for the crypto module. The crypto module will read/write encrypted data for non volatile storage using this HAL. The client software has no means of determining or understanding this "black" data.

Table 4 Database HAL Services

Database HAL Service	Approved Role	Non Approved Role	Database HAL Service Description
dsReadPhysicalPageReq	Crypto Officer	None	Issued by the Crypto Module to read a physical page of data from database storage. **Inputs:** Physical Page Address **Outputs:** None
dsReadPhysicalPageCnf	Crypto Officer	None	Issued to the Crypto Module to return the result of a database page read. **Inputs:** Result - Success/Fail(reason) Page Data - The page data if success **Outputs:** None
dsWritePhysicalPageReq	Crypto Officer	None	Issued by the Crypto Module to write a physical page of data to database storage. **Inputs:** Physical Page Address Page Data **Outputs:** None
dsWritePhysicalPageCnf	Crypto Officer	None	Issued to the Crypto Module to return the result of a database page write. **Inputs:** Physical Page Address Result - Success/Fail(reason) **Outputs:** None
dsErasePhysicalPageReq	Crypto Officer	None	Issued by the Crypto Module to erase a physical page of database storage. **Inputs:** Physical Page Address **Outputs:** None

Database HAL Service	Approved Role	Non Approved Role	Database HAL Service Description
dsErasePhysicalPageCnf	Crypto Officer	None	Issued to the Crypto Module to return the result of a database page erase. **Inputs:** Result - Success/Fail(Reason) Physical Page Address **Outputs:** None

4.6 Approved Modes of Operation

Table 5 lists the approved mode of operation security functions and the purpose for their use.

Invoking an approved mode of operation requires the host to request the creation of a cryptographic channel. The cryptographic channel is closed when the host no longer requires it.

A cryptographic channel is initialized with a channel type, a mode (encrypt/decrypt), algorithm identification, key identification, and an initialization vector.

The AES MAC PRNG, SHA-1 and HMAC functions only operate in approved mode. The LCM is always in approved mode for these functions as long as the power on self tests pass. If a power on self test fails the LCM will enter the error state. The user is informed of the LCM error state, and the LCM cannot be in an approved mode if in this state.

For the AES-256 algorithm the user (client software) must query the LCM for the mode of the current cryptographic channel. An initialized cryptographic channel using AES algorithm indicates approved mode operation. Typically the client software will provide an indication to the device HMI of approved operation – for example a "AES" ICON. If the algorithm type is DES the LCM is operating in a non-approved mode. If no cryptographic channel is initialized the LCM is not operating so it is of course not operating in an approved mode. Table 7 below contains details on specific services which may change the LCM to/from approved mode operation.

Table 5 Approved Mode Security Functions

Algorithm (approved security function)	Purpose	Validation Certificate
AES – 256	Key Wrapping and transport, P25 Data Confidentiality	**#2185**
AES MAC, Vendor Affirmed	P25 AES OTAR	**#2185**
PRNG	Key generation	**#1106**
SHA – 1	PRNG	**#1893**
SHA – 1	Firmware Load and Integrity Tests	**#1894**
HMAC	Firmware Load and Integrity Tests	**#1338**

4.7 Non - Approved Mode of Operation

Table 6 lists the non - approved mode of operation security functions and the purpose for their use. These non – approved modes of operation are for backward interoperability purposes or to satisfy import/export restrictions.

Table 6 Non - Approved Mode Security Functions

Algorithm (non approved security function)	Purpose
DES	Key wrapping, P25 data confidentiality, P25 OTAR / KFD MAC calculation.

4.8 Non Approved Mode Services

Services that can be used in a non approved mode are identified in the previous service definition paragraphs. The services have the same inputs and outputs and are identified as being used in a non approved mode by the algorithm type (DES) or channel type (MAC). This section provides a brief description of possible non approved mode operation for each of these services.

If a service supports a non approved mode of operation, it will provide the algorithm type of the key used for that service (i.e. "DES"), or the channel type for MAC operations. Each service operates only on the key/algorithm type indicated for that service invocation. The user of the LCM can always determine the approved/non approved mode of each service.

Table 7 Host Services Non Approved Modes

Host Service	Non-Approved Role	Host Service Description
Channel Open	User	A channel may be open with a DES key. The DES algorithm type of the channel key indicates non approved mode of operation.
Channel Data	User	The algorithm type of the key passed to the channel open is used for the channel operations. DES algorithm type indicates a non approved mode of operation, as does a MAC channel type.
Channel Close	User	A DES channel may also be closed.
Channel Short Data	User	The algorithm type of the key passed to the channel open is used for the channel operations. DES algorithm type indicates a non approved mode of operation, as does a MAC channel type.
Set Key	Crypto Officer	This service may be used to set a DES key. The DES algorithm type of the key indicates non approved mode of operation.
Delete Key	Crypto Officer	This service may be used to delete a DES key. The DES algorithm type of the key indicates non approved mode of operation.
Delete Keyset	Crypto Officer	This service may be used to delete a keyset which includes DES keys. The DES algorithm type of the keys indicates non approved mode of operation.
Changeover Keyset	Crypto	This service may be used to change to a keyset

Host Service	Non-Approved Role	Host Service Description
	Officer	which includes DES keys. The DES algorithm type of the keys indicates non approved mode of operation.
Set Keyset Info	Crypto Officer	This service may be used to change a keyset algorithm type to DES. The DES algorithm type of the keyset indicates non approved mode of operation.
Get Key Info	Crypto Officer	This service may be used to retreive key info for a DES key. The DES algorithm type of the key indicates non approved mode of operation.
Set Reverse Warm Start Policy	Crypto Officer	This service may be used to set a DES key for use by the Over The Air Rekey reverse warm start procedure. The DES algorithm type of the key indicates non approved mode of operation.
Get Keyset Info	Crypto Officer	This service may be used to retreive keyset info for a DES keyset. The DES algorithm type of the keyset indicates non approved mode of operation.
Generate Warm Start Key	Crypto Officer	This service may be used to generate a DES warmstart key for use by the Over The Air Rekey reverse warm start procedure. The DES algorithm type of the key indicates non approved mode of operation.
Show Status	User	The key or keyset algorithm type, and channel type (MAC channel) are available in all affected services.

Table 8 Key Fill Device Non Approved Mode Services

Key Fill Device Service	Non Approved Role	Key Fill Device Service Description
KFD Inventory – List Active Keys	Crypto Officer	This service will retrieve key information for DES keys. The DES key algorithm type indicates a non approved mode of operation.
KFD Inventory – List Keyset Tagging Info	Crypto Officer	This service will retrieve keyset information for DES keysets. The DES keyset algorithm type indicates a non approved mode of operation.
KFD Modify Key	Crypto Officer	This service may be used to modify, set or erase a stored DES key. The DES key algorithm type indicates a non approved mode of operation.
KFD Changeover	Crypto Officer	This service may be used to perform a keyset changeover from one stored keyset to another stored keyset. Either or both of the keysets may be DES keysets. The DES keyset algorithm type indicates a non approved mode of operation.

Table 9 Database HAL Non Approved Mode Services

Database HAL Service	Approved Role	Key Fill Device Service Description
None	None	The database HAL uses only approved mode algorithms for raw data storage and retrieval. The included raw data may be used for non approved modes of operations as defined in the Host and KFD Non approved service tables.

4.8.1 **MAC Channel Operations**

A channel used for MAC operations will use the algorithm type of the key used to open the channel. The MAC is calculated using the key, algorithm, and either fixed initialization data, or a portion of the message data as defined in [7].

Either a DES key or AES key may be used for MAC calculations. A DES key indicates a unapproved mode of operation.

5 Critical Security Parameters, Cryptographic Keys

Table 10 lists all critical security parameters. Entropy data to initialize the RNG seed key is provided to the LCM at boot up, as is the KSK seed key.

Table 10 Critical Security Parameters, Cryptographic Keys

Critical Security Parameter	Purpose	Key Stored	Key Generated	Key Zeroizable
Key Storage Key (KSK)	An AES 256 key. The KSK is used to encrypt keys prior to storage.	No	Yes	Yes
Traffic Encryption Key (TEK)	An AES 256 key. The TEK provides confidentiality to data traffic. It is also used to perform OTAR MAC calculations.	Yes	No	Yes
Key Encryption Key (KEK)	An AES 256 key. The KEK provides confidentiality to TEKs or other KEKs.	Yes	No	Yes
Unique Key Encryption Key (UKEK)	This is a KEK. The first KEK loaded in the LCM is treated as the OTAR "UKEK". This KEK will be selected for OTAR warm start procedures. It is otherwise identical to other KEK's.	Yes	No	Yes
Working Key (WK)	An AES 256 key. The WK is a working copy of key types, KSKs, TEKs or KEKs.	No	Reverse Warm Start Key Only	Yes
HMAC Key (HK)	A 256 bit secret key. The HK is used by the firmware boot integrity test.	Yes	No	No
KSK Seed Key (KSKSK)	Seeds the PRNG used to generate the KSK.	No	No	Yes
RNG Seed Key (RSK)	Seeds the PRNG used to generate the OTAR Reverse Warm Start Key*.	No	No	Yes

5.1 Reverse Warm Start Key

The Reverse Warm Start Key is a Working Key and a temporary TEK used for OTAR radio initiated message authentication when the radio has no TEKs available.

The Reverse Warm Start Key is generated using the approved PRNG in response to the "Generate Warm Start Key" host service call. The algorithm of the resulting key will be the same as the algorithm if the passed in TEK. Use of a DES algorithm TEK will result in a DES Reverse Warm Start Key, for unapproved (DES) mode of operation.

5.2 KSK Seed (KSKSK) and RNG Seed Key (RSK)

The KSK and RSK seed data keys are stored in internal LCM RAM in plain text form. They are protected from access by software or firmware outside of the LCM address space. The KSK and RSK seed data are cleared on zeroize. The LCM will request a new KSK and RSK seed on zeroize as a new KSK must be generated to allow loading of new KEK or TEK keys post zeroization.

5.3 Access Rights to CSP by Service

5.3.1 User Role

W: Write, the module modifies the Key/CSP.

Table 11 Host Services Access Rights to CSPs

Host Service	KSK	KSKSK	RSK	KEK	TEK	WK
Set Key	-	-	-	-	-	-
Delete Key	-	-	-	-	-	-
Delete Keyset	-	-	-	-	-	-
Generate Warm Start Key	-	-	-	-	-	-
Partial Zeroize	-	-	-	W	W	W
Zeroize	W	W	W	W	W	W

Table 12 Key Fill Device Services Access Rights to CSPs

Key Fill Device Service	KSK	KSKSK	RSK	KEK	TEK	WK
KFD Modify Key	-	-	-	-	-	-
KFD Zeroize	-	-	-	-	-	-

5.3.2 Crypto Officer Role

W: Write, the module modifies the Key/CSP.

Table 13 Host Services Access Rights to CSPs

Host Service	KSK	KSKSK	RSK	KEK	TEK	WK
Set Key	-	-	-	W	W	-
Delete Key	-	-	-	W	W	-
Delete Keyset	-	-	-	W	W	-
Generate Warm Start Key	-	-	-	-	-	W
Partial Zeroize	-	-	-	W	W	W
Zeroize	W	W	W	W	W	W

Table 14 Key Fill Device Services Access Rights to CSPs

Key Fill Device Service	KSK	KSKSK	RSK	KEK	TEK	WK
KFD Modify Key	-	-	-	W	W	-
KFD Zeroize	W	W	W	W	W	W

6 Cryptographic Key Management

6.1 Key Generation

The Reverse Warm Start Key is generated using the approved PRNG in response to the Generate Warm Start Key host service request. It is generated rather than being read from the Database.

6.2 Key Input/Output

Key material is input/output via the key fill interface service access point. Any Key Fill Device that complies with the APCO Project 25 standard KFD interface specification is authorized to invoke the KFD Services exported by the LCM. Such a device will use the KMM formatting expected by the KFD Interface.

6.3 Key Storage

Key material is encrypted using the KSK prior to being stored. The data storage area itself lies outside the boundary of the LCM. The LCM will only store encrypted key data in this database.

6.4 Key & Cryptographic Security Parameters (CSP) Zeroize

The LCM provides three different levels of zeroization via the Host Interface:

- 0 – Zeroizes all CSP data including the RSK, UKEK, KSK and the KSKSK. The individual RSI and MN, the KMF RSI and the MNP non-CSP OTAR configuration data are reset. The RSK and KSK are regenerated.
- 1 – Zeroizes all CSP data including the RSK, UKEK and the KSK. The individual RSI and MN, the KMF RSI and the MNP non-CSP OTAR configuration data are preserved. The RSK and KSK are regenerated.

Note that Level 0 is the only level that is equivalent to zeroization as defined by FIPS PUB 140-2.

KFD Zeroize, which may be invoked via the KFD Interface, is the same as Level 1 zeroization above.

6.5 APCO P25 Over The Air Rekeying (OTAR)

The LCM module does not directly support the APCO Project 25 Over The Air Rekeying (OTAR) protocol – it does however provide the cryptographic services required to implement that protocol.

The user (client software) must implement the P25 OTAR protocol while using the LCM services for any and all required cryptographic processing of the OTAR messages.

- OTAR cryptographic keys.
    - The LCM provides storage for OTAR keys as defined in 5 Critical Security Parameters, Cryptographic Keys:
        - UKEK
        - Reverse Warm Start Key
- Key privacy
    - The LCM stores the KEK and provides AES encryption/decryption services for TEK's transported in the OTAR messages.
- Message Authentication
    - The LCM provides the vendor affirmed AES-MAC service to support MAC authentication on OTAR messages
- Message Privacy
    - The LCM provides the AES-256 service for encryption/decryption of OTAR message contents.
- Key Input/Storage/Management
    - The user invokes Host Services (4.3) to add, delete or modify keys or keysets as directed by OTAR messages. Refer to the Host Services section for details on these services.
        - Set Key
        - Delete Key
        - Delete Keyset
        - Changeover Keyset
        - Set Keyset Info
        - Get Key Info
        - Get Keyset IDs
        - Get Keyset Info

- Generate Warm Start Key
- Zeroize
- These services affect OTAR operational parameters, not keys but are similarly managed using OTAR
    - Set RSI
    - Get RSI
    - Set KmfRsi
    - SetMnp
    - SetReverseWarmStartPolicy

7 Security Policy for Mitigation of other Attacks

The LCM is not designed to mitigate specific attacks.

8 User Guidance

8.1 Interfaces and Services

The LCM offers the following to the User:

- Host Logical Interfaces as described in Section 2.
- Host Services for the User as described in Section 4.3.

8.2 User Responsibilities

The LCM provides both FIPS-approved and non-FIPS-approved modes of operation. It is the responsibility of the User to only invoke Host Services using the approved algorithms listed in Section 4.5 Approved Modes of Operation, in order to ensure that the module operates in a FIPS-approved mode of operation.

Requesting the use of the DES or AES MAC algorithms for any purpose will cause the module to operate in a non-FIPS-approved mode of operation, although only for the duration of the request. Any subsequent requests to use FIPS-approved algorithms will cause the LCM to operate in a FIPS-approved mode.

9 Crypto Officer Guidance

9.1 Interfaces and Services

The LCM offers the following to the Crypto Officer:

- Host and KFD Logical Interfaces as described in Section 2.
- Host Services for the Crypto Officer
  - A high-level overview can be found in Section 4.3.
  - Keys and CSPs are accessed via these services as described in Section 5.
- KFD Services
  - A high-level overview can be found in Section 4.4.
  - Keys and CSPs are accessed via these services as described in Section 5.

9.2 Module Administration

After manufacture or full zeroization, the LCM will contain no key data. The Crypto Officer must load key data via the Host or KFD interfaces. The radio level key management procedures are described in the Liberty™ Land Mobile Radio User's Manual. At a software interface level, the client software must clear the buffer used to transfer the key data, when using the Host interface to perform the Set Key service.

It is assumed that any key fill device that conforms to the APCO Project 25 standard KFD interface specification is authorized to invoke KFD services on the module. It is the responsibility of the Crypto Officer to only employ such key fill devices.

9.3 Module Installation and Startup

The LCM is distributed as part of a suite of radio software or firmware that automatically handles its secure installation and ensures that only an authenticated LCM firmware image is loaded by using the FIPS-approved HMAC supplied by the currently operating LCM to check it. The firmware download procedure is described in the Liberty™ PC Programmer User's Manual.

As with installation, the accompanying radio firmware or software must also initialize the LCM, when the radio is turned on.