JVCKENWOOD Corporation

Secure Cryptographic Module (SCM)

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0
Last Modified: 22/10/2025

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 9
2.7 Algorithm Specific Information 10
2.8 RBG and Entropy 10
2.9 Key Generation 10
2.10 Key Establishment 11
2.11 Industry Protocols 11
3 Cryptographic Module Interfaces 11
3.1 Ports and Interfaces 11
3.2 Trusted Channel Specification 12
3.3 Control Interface Not Inhibited 12
3.4 Additional Information 12
4 Roles, Services, and Authentication 12
4.1 Authentication Methods 12
4.2 Roles 12
4.3 Approved Services 13
4.4 Non-Approved Services 25
4.5 External Software/Firmware Loaded 26
4.6 Bypass Actions and Status 26
4.7 Cryptographic Output Actions and Status 27
5 Software/Firmware Security 27
5.1 Integrity Techniques 27
5.2 Initiate on Demand 27
5.3 Open-Source Parameters 27
5.4 Additional Information 27
6 Operational Environment 27
6.1 Operational Environment Type and Requirements 27

6.2 Configuration Settings and Restrictions 27
7 Physical Security 28
7.1 Mechanisms and Actions Required 28
8 Non-Invasive Security 28
9 Sensitive Security Parameters Management 28
9.1 Storage Areas 28
9.2 SSP Input-Output Methods 28
9.3 SSP Zeroization Methods 29
9.4 SSPs 29
9.5 Transitions 31
9.6 Additional Information 31
10 Self-Tests 31
10.1 Pre-Operational Self-Tests 31
10.2 Conditional Self-Tests 32
10.3 Periodic Self-Test Information 33
10.4 Error States 34
11 Life-Cycle Assurance 34
11.1 Installation, Initialization, and Startup Procedures 34
11.2 Administrator Guidance 35
11.3 Non-Administrator Guidance 35
11.4 Design and Rules 35
11.5 Maintenance Requirements 36
11.6 End of Life 36
12 Mitigation of Other Attacks 36
12.1 Attack List 36
12.2 Mitigation Effectiveness 36
13 Acronyms 37

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 7
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 9
Table 5: Non-Approved, Not Allowed Algorithms 9
Table 6: Security Function Implementations 10
Table 7: Ports and Interfaces 12
Table 8: Roles 12
Table 9: Approved Services 25
Table 10: Non-Approved Services 26
Table 11: Mechanisms and Actions Required 28
Table 12: Storage Areas 28
Table 13: SSP Input-Output Methods 29
Table 14: SSP Zeroization Methods 29
Table 15: SSP Table 1 30
Table 16: SSP Table 2 30
Table 17: Pre-Operational Self-Tests 31
Table 18: Conditional Self-Tests 33
Table 19: Pre-Operational Periodic Information 33
Table 20: Conditional Periodic Information 33
Table 21: Error States 34

List of Figures

Figure 1– Physical Form of the SCM 6
Figure 2 – SCM Block Diagram 7

1 General

1.1 Overview

This document defines the FIPS 140-3 Security Policy for the Secure Cryptographic Module (SCM).
The SCM is a hardware cryptographic module developed by JVCKENWOOD Corporation to provide FIPS 140-3 validated cryptographic security functionality for the following radio device series:

TK-5XX0 Series FM/P25 digital two-way radios
NX-/NXR- Series FM/P25/NEXEDGE digital radios
VPxxx0 Series FM/P25 digital two-way radios
VMxxx0 Series FM/P25 digital two-way radios

The SCM is a multi-chip embedded cryptographic module that meets the overall Level 1 requirements of FIPS 140-3.
It connects to the above radio devices and provides cryptographic services compliant with FIPS 140-3, supporting digital communication standards such as P25, DMR, and NEXEDGE.

・P25 (Project 25) is a digital radio standard developed for public safety communications. It enables interoperability across agencies and jurisdictions. P25 is defined by the TIA-102 series of standards.
・DMR (Digital Mobile Radio) is an ETSI standard for professional mobile radio systems, widely used in commercial and industrial sectors. It supports tiered functionality (Tier I–III) and efficient spectrum use.
・NEXEDGE is a proprietary digital radio protocol developed by Kenwood. It is designed for conventional and trunked radio systems. It is often used in private and commercial radio networks.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	1
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The cryptographic module is intended to be embedded in JVCKENWOOD radio devices and to perform cryptographic functions.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Module Characteristics:

Cryptographic Boundary:

The physical form of the cryptographic module is shown in Figure 1.
The cryptographic boundary is defined as the external surface of the SCM printed circuit board with the shield cover attached.
The shield cover provides physical protection and is considered part of the cryptographic boundary.

A block diagram showing the connection between the cryptographic module and external hardware (radio device) is provided in Figure 2.
The red frame indicates the cryptographic boundary.
The SCM consists of a processor (DSP), non-volatile memory (NVM), clock, tamper detection circuitry, and a board-to-board connector.

Figure 1– Physical Form of the SCM

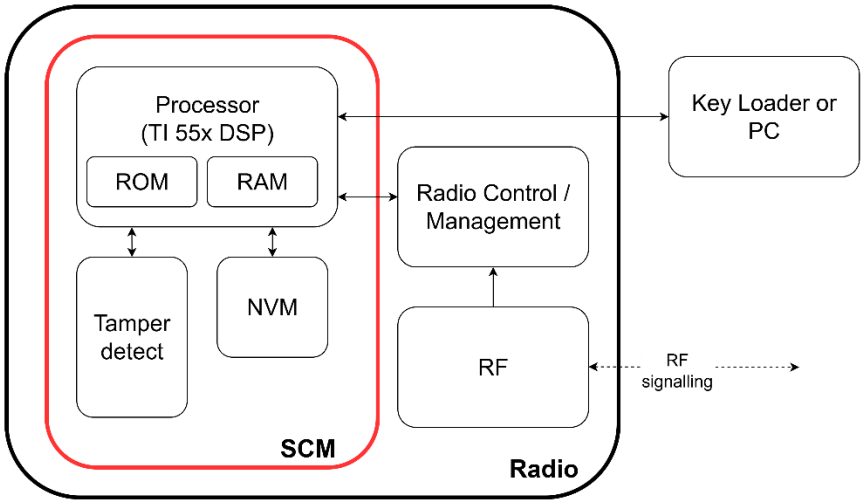

Figure 2 – SCM Block Diagram

When loading cryptographic keys, an external key loader device is used in conjunction with the radio device.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
KWD-AE30-0	2.0.0	A3.2.0	TI DSP TMS320C5517	NVM: EN39SL801-70 / 8 Mbit/ EON
KWD-AE30-1	2.1.0	A3.2.0	TI DSP TMS320C5517	NVM: EN39SL800-70 / 8 Mbit / EON
KWD-AE30-2	2.2.0	A3.2.0	TI DSP TMS320C5517	NVM: SST39WF800B / 8 Mbit / Microchip

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The module does not claim any excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode		Approved	Show Status
Non-Approved Mode		Non-Approved	Show Status

Table 3: Modes List and Description

As shown in Table “Modes List and Description”, the cryptographic module includes both Approved Mode and Non-Approved Mode.
Immediately after power-on, the module starts in Approved Mode.

Mode Change Instructions and Status

The cryptographic module transitions to Non-Approved Mode when any of the following services are requested by the Crypto Officer:

- A request is received to initialize (key expansion) for DES.
- A request is received for the OTAR Calc MAC DES service.
- A request is received to input a DES key.
- A request is received to delete a DES key.

Conversely, the module transitions to Approved Mode when any of the following services are requested by the Crypto Officer:

- A request is received to initialize (key expansion) for AES Encryption or Decryption.
- A request is received for the OTAR Calc-MAC service that verifies the integrity of KMM using CMAC.
- A request is received to input an AES key.
- A request is received to delete an AES key.
- A request is received for the AM Calculation service.
- A request is received for the Firmware Update service.

The operator can confirm the current mode by invoking the Show Status service to check the value of the cryptographic status flag.
If the flag is set to “1”, the module is in Approved Mode; if set to “0”, it is in Non-Approved Mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	AES 2696	Direction - Generation, Verification Key Length - 256	SP 800-38B
AES-ECB	AES 2696	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-OFB	AES 2696	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
SHA2-256	SHS 2285	Message Length - Message Length: 0-51200 Increment 1	FIPS 180-4

Table 4: Approved Algorithms

The CAVP certificates for the cryptographic module include algorithms and options that are not used in the Approved mode of the module.
Only the algorithms and options listed in the above table are used in the module's Approved mode.

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
DES-MAC	MAC generation
DES	encryption, decryption

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Block Cipher	BC-UnAuth	Encryption and Decryption	Key Length:128, 256 bits	AES-OFB: (AES 2696)
Key Expansion	BC-UnAuth	Expanding the key to generate expanded keys	Key Length:128, 256 bits	AES-OFB: (AES 2696)
Key Decryption	BC-AuthDecrypt	Decrypts an encrypted key that has been encrypted using a KEK	Key Length:256 bits	AES-ECB: (AES 2696)

Name	Type	Description	Properties	Algorithms
Secure Hash	SHA	Secure Hash Function		SHA2-256: (SHS 2285)
Firmware Authentication	MAC	Verifies the authenticity of received firmware during update	Key Length:256 bits	AES-CMAC: (AES 2696)
Firmware Integrity Verification	MAC	Verifies the integrity of firmware, including boot firmware, during pre-operational self-tests.	Key Length:256 bits	AES-CMAC: (AES 2696)
OTAR MAC Generation	MAC	Message Authentication Code Generation using AES-CMAC	Key Length:256 bits	AES-CMAC: (AES 2696)
Link Layer Authentication	BC-AuthEncrypt	Generates the Response for link layer authentication by encrypting input RS and RAND using AMK with AES-ECB.	Key Length:128 bits	AES-ECB: (AES 2696)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

Note:
AES Encryption and Decryption services require prior execution of the corresponding initialization process. Without initialization, the module will return an INVALID_RSP, and the cryptographic operation will not proceed.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

N/A for this module.

2.10 Key Establishment

The module does not support key establishment.

2.11 Industry Protocols

The cryptographic module, when integrated with the radio device, supports industry-standard protocols defined under the Project 25 (P25) suite for secure land mobile radio communications. Specifically, the module complies with the following protocols:

Over-The-Air Rekeying (OTAR):
Defined in TIA-102.AACA-A, this protocol enables secure remote distribution and updating of encryption keys over radio networks.
The module, in conjunction with the radio device, facilitates OTAR functionality to ensure secure and efficient key management.

Key Fill Device (KFD) Interface Protocol:
Defined in TIA-102.AACD-A, this protocol specifies the interface and procedures for manually provisioning encryption and authentication keys from external key loaders to mobile radios.
The module operates in coordination with the radio device to support secure key loading via KFD.

These protocols ensure interoperability and secure key management within P25-compliant systems.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Vcc	Power	+3.3V
BUSY	Status Output	Busy Indicator
TXD	Data Output Status Output	UART data for firmware updating and key loading
RXD	Data Input Control Input	UART data for firmware updating and key loading
TAMPER	Data Input	Tamper detection information
TAMPER2	Data Input	Tamper detection Information
SCK	Control Input	SPI shift clock
/BFS	Status Output	Frame sync
MOSI	Data Input Control Input	SPI data
MISO	Data Output Control Input	SPI data
/SS	Control Input	SPI slave enable

Physical Port	Logical Interface(s)	Data That Passes
/WAKEUP	Control Input	Wakeup from sleep mode
/Reset	Control Input	Reset
/REQ	Status Output	Interrupt request
GND	Power	Ground

Table 7: Ports and Interfaces

None of the available ports implement the Control Output function.

3.2 Trusted Channel Specification

N/A

3.3 Control Interface Not Inhibited

N/A

3.4 Additional Information

The cryptographic module does not allow any other services to operate while a service is in progress.
When the cryptographic module is performing self-tests or executing a zeroization process, all data output through the data output interface is prohibited.
If the cryptographic module enters an error state, data output is also prohibited; however, status output remains enabled.
During the firmware load process, all data output through the data output interface is prohibited.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

N/A for this module.

This module does not support operator authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto-Officer	None
User	Role	User	None

Table 8: Roles

The cryptographic module supports two roles: the Cryptographic Officer (CO) and the User. These roles are implicitly selected by the operator based on the services being accessed. The module does not support a maintenance role.

- **CO Role**: Responsible for managing the module. This includes installing the module into the radio and managing of cryptographic keys.
- **User Role**: Has access to general cryptographic operations supported by the module. This includes using cryptographic functions such as encryption and decryption.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Power-up Self-test	The module performs a series of self-tests upon power-up to verify the integrity of its firmware and the correct operation of its cryptographic algorithms .	SPI Command Response (ACK_SELF_TEST), Success: "0xAA0100000", Failure: Any response not matching the defined Success response	Power Up, Port:/Reset	SPI ACK: Self-tests Result	Firmware Integrity Verification	CO
Radio Pairing	The module performs Kenwood ESN authentication of the radio device. The module verifies whether the	SPI Command Response (ACK_AUTH1 or ACK_AUTH2), Success: "0x81010000" or "0x92010000", Failure: "0x8101FFFF" or "0x9201FFFF" or" 0x86010000"	SPI Command (AUTH_CMD1 or AUTH_CMD2) : ESN (Electronic Serial Number)	SPI ACK: Response (Success / Failure)	Secure Hash	CO - TEK: Z - KEK: Z - AMK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	connected radio device is same as the previously connected one or not. If not, required processes (e.g., key zeroization) are performed.					
AES Encryption Initialization	The module performs the encryption initialization process, including AES key expansion and IV generation.	SPI Command Response (ACK_ENC_INIT), Success: "0x82060084" + Any or "0x8205" + Any, Failure (INVALID_RSP): "0xFF01" + Any	SPI Command (ENC_INIT_CMD): [CKR] or [Algorithm, Key ID]	SPI ACK: [Algorithm ID, Key ID, IV] or [CKR, IV]	Key Expansion	CO - TEK: E
AES Decryption Initialization	The module performs the decryption initialization process, including AES	SPI Command Response (ACK_DEC_INIT), Success: "0x8301" + Any, Failure (INVALID_RSP): "0xFF01" + Any	SPI Command (DEC_INIT_CMD): Algorithm, Key ID, IV	SPI ACK:CKR (Common Key Reference)	Key Expansion	CO - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	key expansion.					
AES Encryption	The module encrypts the given plaintext and outputs the resulting ciphertext. It is needed that AES Encryption Initialization has been executed.	SPI Command Response (ACK_ENC), Success: "0x8408" + Any, Failure (INVALID_RSP): "0xFF01" + Any	SPI Command (ENC_CMD): Plaintext	SPI ACK: Ciphertext	Block Cipher	User - TEK: E
AES Decryption	The module decrypts the given ciphertext and outputs the resulting plaintext. It is needed that AES Decryption Initialization has been executed.	SPI Command Response (ACK_DEC_INIT), Success: "0x8508" + Any, Failure (INVALID_RSP): "0xFF01" + Any	SPI Command (DEC_CMD): Ciphertext	SPI ACK: Plaintext	Block Cipher	User - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AM Calculation	The module generates the Response for Link Layer Authentication.	SPI Command Response (ACK_AM_CALC), Success: RES (Response), Failure (INVALID_RSP): "0xFF01" + Any	SPI Command (AM_CALC_CMD): SUID RS (Random Seed) RAND (Random Challenge) Mode (AM1-AM4)	SPI ACK: RES (Response)	Link Layer Authentication	CO - AMK: E
Zeroize	The module zeroizes designated keys.	SPI Command Response (ACK_ZERO), Success: "0x8601" + Any	SPI Command(ZERO_CMD): All key Request or Keyset's CKR	SPI ACK: Response (Success / Failure)	None	CO - TEK: Z - KEK: Z - AMK: Z
KVL mode	The module enables communication with a Key Variable Loader to input or delete AES cryptographic keys.	SPI Command Response (KVL_MOD_CMD), Success: "0x88020000", Failure: Any response not matching the defined Success response	SPI Command (KVL_MOD_CMD): Enter or exit KVL Mode, UART Input: KMM messages containing key data	SPI ACK: Response (Success), UART ACK: Response, Key-related information	None	CO - TEK: W,Z - KEK: W,Z - AMK: W,Z
Show Status	The module returns its current status in response to a status request.	SPI Command Response (STS_RSP), Success: "0x8902" + Any	SPI Command (STS_REQ): Request	SPI ACK: Self-tests Status, Cipher Status	None	Unauthenticated
Firmware Update	The module loads a	SPI Command Response (ACK_FIRM_UPD	SPI Command (FIRM_UPDT_CMD): Request, UART	SPI ACK:	Firmware	CO - FWI: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	new firmware image and verifies authenticity through a Firmware Load Test. If the test passes, the module reboots and activates the newly loaded firmware, resulting in a version change.	T), Success: "0x8A01" + Any, Failure: "0x8A00" or "0xFF01" + Any (INVALID_RSP)	Input: Firmware Data	Checksum	Authentication	- TEK: Z - KEK: Z - AMK: Z
Sleep	The module enters sleep mode to suspend cryptographic operations and reduce power consumption.	SPI Command Response (ACK_SLEEP), Success: "0x8D00"	SPI Command (SLEEP_CMD): Request	SPI ACK: Response (Success)	None	User
Wake-up	The module exits sleep mode	SPI Command Response (ACK_IDLE), Success: "0xAB00"	Interrupt request for /WAKEUP port	SPI ACK: Response	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and resumes normal operations.			(Success)		
Modify clock rate	The module modifies the DSP's clock rate.	SPI Command Response (ACK_CHG_CLK), Success: "0x8E00"	SPI Command (CHG_CLK_CMD): Clock Rate	SPI ACK: Response (Success)	None	User
Beat Shift	The module shifts the frequency of its clock generator.	SPI Command Response (ACK_BSHIFT), Success: "0x8F00"	SPI Command (BSHIFT_CMD): ON or OFF	SPI ACK: Response (Success)	None	User
Show Version	The module returns its module's firmware version number in response to a version request.	SPI Command Response (VER_SUM_RSP), "0x9005"+Any	SPI Command (VER_SUM_REQ): Request	SPI ACK: Version	None	Unauthenticated
OTAR Calc-MAC	The module calculates a Message Authentication Code (MAC) for a	SPI Command Response (OTAR_ACK_CALC_MAC), :Success: "0xE00A81000241" + Any, Failure: "0xE0018101" or "0xE0018104"	SPI KMM Command (OTAR_CALC_MAC_CMD): Algorithm(AES) Format(CMAC) Message	SPI ACK: MAC	OTAR MAC Generation	CO - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	given message upon request.					
OTAR Set-Key	The module receives a key encrypted with the KEK, decrypts it internally, and stores it in the designated location. This operation is part of the P25 AES OTAR key management process.	SPI Command Response (OTAR_ACK_SET_KEY), Success: "0xE0018200", Failure: Any response from"0xE0018201 "through "0xE0018204"	SPI Command (OTAR_SET_KEY_CMD): KEK information (Algorithm ID, Key ID) , Encrypted Key information (Keyset ID, SLN, Algorithm ID, Key ID, Key Name, Key Data)	SPI ACK: Response (Success / Failure)	Key Decryption	CO - TEK: W - KEK: W,E
OTAR Set-KeysetInfo	The module stores Keyset information upon receiving a request.	SPI Command Response (OTAR_ACK_SET_KSI), Success: "0xE0018300", Failure:"0xE0018301" or "0xE0018304"	SPI Command (OTAR_SET_KSI_CMD): Keyset Information(Keyset ID, Algorithm ID, Format, Key Name)	SPI ACK: Response (Success / Failure)	None	CO
OTAR Set-RSI	The module stores RSI informati	SPI Command Response (OTAR_ACK_SET_RSI), Success: "0xE0018400",	SPI Command (OTAR_SET_RSI_CMD): RSI information (Update Type,	SPI ACK: Respo nse (Succ	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	on upon receiving a request.	Failure: Any response from "0xE0018401" through "0xE0018404"	Message Number, Affected RSI, New RSI)	ess / Failure)		
OTAR Delete-Key	The module deletes the specified key upon receiving a request.	SPI Command Response (OTAR_ACK_DEL_KEY), Success: "0xE0038500" + Any, Failure: "0xE0018501"	SPI Command (OTAR_DEL_KEY_CMD): Key ID, Algorithm ID	SPI ACK: SLN, Keyset ID	None	CO - TEK: Z - KEK: Z
OTAR Delete-Keyset	The module deletes the specified Keyset information upon receiving a request.	SPI Command Response (OTAR_ACK_DEL_KSET), Success: "0xE0018600", Failure: "0xE0018601"	SPI Command (OTAR_DEL_KSET_CMD): Keyset ID	SPI ACK: Response (Success / Failure)	None	CO - TEK: Z - KEK: Z
OTAR Chageover-Keyset	The module deletes the specified Keyset information upon receiving a request	SPI Command Response (OTAR_ACK_CO_KSET), Success: "0xE0028700" + Any, Failure:"0xE0028701" + Any or "0xE0028704" + Any	SPI Command (OTAR_CO_KSET_CMD): Keyset ID SPI Command: superseded Keyset ID, Activated Keyset ID, Erase mode	SPI KMM ACK: superseded Keyset ID, Activated Keyset ID	None	CO - TEK: Z - KEK: Z
OTAR Zeroize	The module deletes all stored keys (excluding FWI) upon	SPI Command Response (OTAR_ACK_ZERO), Success: "0xE0018800"	SPI Command (OTAR_ZERO_CMD): Request	SPI KMM ACK: None	None	CO - TEK: Z - KEK: Z - AMK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	receiving a request.					
OTAR Get-KeyIDs	The module outputs all stored key information upon receiving a request.	SPI Command Response (OTAR_ACK_GETKEY), Success: "0xE" + Any(12bit) + "0x8900" + Any, Failure:"0xE0018901"	SPI Command (OTAR_GET_KEY_CMD): Request	SPI ACK: Key Information (Key ID, Algorithm ID, SLN), Key count	None	CO
OTAR Get-KeysetIDs	The module outputs all stored Keyset information upon receiving a request.	SPI Command Response (OTAR_ACK_GETKSET), Success: "0xE" + Any(12bit) + "0x8A00" + Any, Failure:"0xE0018A01"	SPI Command (OTAR_GET_KSET_CMD): Request	SPI ACK: Keyset information (Keyset ID, status), Keyset count	None	CO
OTAR Get-Keyset KeyIDs	The module outputs the key information within the specified Keyset upon receiving a request.	SPI Command Response (OTAR_ACK_GETKSET_KEY), Success: "0xE" + Any(12bit) + "0x8B00" + Any, Failure:	SPI Command (OTAR_GET_KSET_KEY_CMD): Keyset ID	SPI ACK: Keyset ID, Key information (Key ID, Algorithm	None	CO
OTAR Get-KeysetInfo	The module outputs the specified Keyset	SPI Command Response (OTAR_ACK_GETKSI), Success: "0xE" + Any(12bit) + "0x8C00" + Any,	SPI Command (OTAR_GET_KSI_CMD): Keyset ID	SPI Command: Keyset ID	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	information upon receiving a request.	Failure:"0xE0018C01"				
OTAR Get-RSI	The module outputs the RSI information upon receiving a request.	SPI Command Response (OTAR_ACK_GETRSI), Success: "0xE" + Any(12bit) + "0x8D00" + Any, Failure:"0xE0018D01"	SPI Command (OTAR_GET_RSI_CMD): RSI	SPI ACK: RSI Information	None	CO
OTAR Get-Capabilities	The module outputs the supported Option Service IDs and Message IDs upon receiving a request.	SPI Command Response (OTAR_ACK_GETCAPS), Success: "0xE0138E00" + Any	SPI Command (OTAR_GET_CAPS_CMD): Request	SPI ACK: Capability	None	CO
Static Tamper Detect	The module detects tamper events (such as removal from the radio) that may have occurred while power was not supplied. Upon detectio	SPI Command Response (ACK_ZERO), Success: "0x86010000" (ALL), or "0x87010000" (RAM only)	Static Tamper Flag	SPI Command: Response (Zeroize Success)	None	CO - TEK: Z - KEK: Z - AMK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	n, the module initiates zeroization of stored keys.					
Active Tamper Detect	The module detects tamper events (such as removal from the radio) while power is being supplied. Upon detection, the module immediately initiates zeroization of stored keys.	SPI Command Response (ACK_ZERO), Success: "0x86010000” (ALL), or "0x87010000” (RAM only)	Active Tamper Flag	SPI Command :Response (Zeroize Success)	None	CO - TEK: Z - KEK: Z - AMK: Z
Show Module ESN	The module outputs its ESN and its Hardware version upon receiving a request.	SPI Command Response (KEN_ESN_RSP), "0x8B10"+Any	SPI Command (KEN_ESN_REQ): Request	SPI ACK: Module ESN	None	Unauthenticated
Show NVM ESN	The module outputs	SPI Command Response	SPI Command (FLSH_ESN_REQ) : Request	SPI ACK:	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the ESN stored in the NVM upon receiving a request.	(FLSH_ESN_RSP), "0x8C08"+Any		NVM ESN		
Show Module Model	The module outputs its model name upon receiving a request.	SPI Command Response (MODEL_RSP), "0x9406"+Any	SPI Command (MODEL_REQ): Request	SPI ACK: Module Model Name	None	Unauthenticated
SUID Report	The module receives the radio's SUIDs (WACN ID, System ID, Subscriber ID) and their active status. It supports up to 64 SUIDs per device.	SPI Command Response (ACK_SUID_RPT), "0x9600"	SPI Command (SUID_RPT_CMD): SUID	SPI ACK: Response (Success)	None	User
Factory Reset	The module restores itself to the factory default state. It deletes	SPI Command Response (ACK_FIPS_CMP_CMD), "0x9D010100"	SPI Command (FIPS_CMP_CMD): Request	SPI ACK: Response (Success)	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	all keys (except FWI) and resets configuration settings to their initial state.					

Table 9: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Zeroize	The module zeroizes designated keys.		CO
DES Encryption	The module encrypts the given plaintext and outputs the resulting ciphertext.	DES	User
DES Decryption	The module decrypts the given ciphertext and outputs the resulting plaintext.	DES	User
DES Encryption Initialization	The module performs the encryption initialization process, including DES key expansion and IV generation. Encryption operations must be executed after this initialization session.	DES	CO
DES Decryption Initialization	The module performs the decryption initialization process, including DES key expansion. Decryption operations must be executed after this initialization session.	DES	CO
Sleep	The module enters sleep mode to suspend cryptographic operations and reduce power consumption.		User
Wake-up	The module exits sleep mode and resumes normal operations		User
SUID Report	The module receives the radio's SUIDs (WACN ID, System ID, Subscriber ID) and their active status. It supports up to 64 SUIDs per device.		CO
KVL mode N	The module enables communication with a Key Variable Loader to input or delete DES cryptographic keys.		CO
Modify clock rate	The module modifies the DSP's clock rate.		User
Beat Shift	The module shifts the frequency of its clock generator.		User
OTAR Calc MAC DES	The Module calculates a MAC for a given message using DES in CBC-MAC mode.	DES-MAC	CO

Name	Description	Algorithms	Role
OTAR Calc Checksum	The Module calculates Checksum for a given message.		CO
OTAR Set-Key N	The module receives an encrypted key wrapped with the KEK, decrypts it internally, and stores it in the designated location. This operation is part of the P25 DES OTAR key management process.	DES	CO
OTAR Set-KeysetInfo	The module stores Keyset information upon receiving a request.		CO
OTAR Set-RSI	The module stores RSI information upon receiving a request.		CO
OTAR Delete-Key N	The module deletes the specified DES key upon receiving a request.		CO
OTAR Delete-Keyset	The module deletes the specified Keyset information upon receiving a request.		CO
OTAR Changeover-Keyset	The module changes the active Keyset upon receiving a request.		CO
OTAR Zeroize	The module deletes all stored keys (excluding FWI) upon receiving a request.		CO
OTAR Get-KeyIDs	The module outputs all stored key information upon receiving a request.		CO
OTAR Get-KeysetIDs	The module outputs all stored Keyset information upon receiving a request.		CO
OTAR Get-KeysetKeyIDs	The module outputs the key information within the specified Keyset upon receiving a request.		CO
OTAR Get-KeysetInfo	Request the Keyset Information.		CO
OTAR Get-RSI	The module outputs the specified Keyset information upon receiving a request.		CO
OTAR Get-Capabilities	The module outputs the supported Option Service IDs and Message IDs upon receiving a request.		CO
Factory Reset	The module restores itself to the factory default state. It deletes all keys (except FWI) and resets configuration settings to their initial state.		CO

Table 10: Non-Approved Services

4.5 External Software/Firmware Loaded

The cryptographic module supports a Firmware Update service.
The authenticity and integrity of the firmware image are verified using AES-CMAC before it is accepted by the module.

4.6 Bypass Actions and Status

The module does not support bypass capability.

4.7 Cryptographic Output Actions and Status

The module does not support a self-initiated cryptographic output capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The cryptographic module performs a firmware integrity test using AES-CMAC (CAVP #A2696) to verify the integrity of the firmware.

5.2 Initiate on Demand

Firmware integrity tests can be initiated by power-on or reboot.

5.3 Open-Source Parameters

The module is not open source.

5.4 Additional Information

- Firmware image format: Intel HEX (.hex).

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

This cryptographic module is designated as operating in a limited operational environment, as defined by FIPS 140-3.
The operational environment consists of firmware that manages the SSP within the cryptographic module.
No operating system is present in the module.

6.2 Configuration Settings and Restrictions

The cryptographic module is a hardware module operating in a limited environment.

Firmware components and storage (inside the cryptographic boundary)
- ROM Boot Firmware: stored in DSP internal ROM.
- Boot Firmware: stored in NVM; coordinates loading of the Crypto Firmware.
- Crypto Firmware: stored in NVM; loaded to and executed from RAM.

Boot flow

1) Power ON → ROM Boot Firmware starts.
2) ROM Boot Firmware loads Boot Firmware from NVM.
3) Boot Firmware loads Crypto Firmware from NVM into RAM and transfer's control.

Note
In case of a Crypto Firmware Update failure, the previously active firmware remains available to support recovery.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
N/A	N/A	N/A

Table 11: Mechanisms and Actions Required

This cryptographic module is a standalone unit incorporating multiple integrated circuits and meets the physical security requirements for FIPS 140-3 Level 1.
It uses commercially available IC chips and is constructed with production-grade materials.
During operation, the module is embedded inside a radio device.

The component side of the module, where the IC chips are mounted, is physically protected by a shield cover. This shielding ensures that there are no visible gaps that would allow observation or tampering.
As a result, operators are not required to take any special actions to maintain physical security.

8 Non-Invasive Security

N/A

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary SSPs	Dynamic
NVM	TEK, KEK, FWI, AMK	Static

Table 12: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SPI_in	EXT: Radio Module	NVM	Encrypted	Manual	Electronic	AES-OFB (AES 2696)
KVL_in	EXT: Key Loader Module	NVM	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

The methods for inputting SSPs into the cryptographic module are strictly limited.
SSPs can be entered in plaintext using a key loader or in encrypted form via the radio's OTAR (Over-the-Air Rekeying) functionality.

When using a Key Variable Loader (KVL), the KFD-P25 Interface Protocol is used.
When using a radio, the P25 OTAR Protocol is used.
No other methods are permitted for inputting or modifying SSPs.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroizes SSPs (TEK, KEK, AMK) stored in both NVM and RAM via SPI command.	Overwrites the SSPs in NVM and RAM with zeros (0x00) to render them unrecoverable. Used to provide zeroisation as a service	Initiated by operator via Zeroize service or OTAR Zeroize service.
Z2	Power cycling the module to zeroise temporary SSPs	Power cycling the module to zeroize temporary SSPs	Initiated by operator by powering off the module.
Z3	If the conditions to Zeroize are met, the module will Zeroize the SSPs SSPs (TEK, KEK, AMK).	Overwrites the SSPs in NVM and RAM with zeros (0x00) to render them unrecoverable.	Module initiated when the module is removed from the radio device (tamper event).
Z4	FWI is embedded in the firmware and is zeroized by replacing the firmware during the Firmware Update process.	FWI is overwritten when the firmware image is replaced, effectively zeroizing the embedded key.	Initiated by the operator via Firmware Update service.

Table 14: SSP Zeroization Methods

The zeroization process overwrites data with zeros.
Once zeroized, the SSPs cannot be reused.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TEK	Traffic Encryption Key	128, 256 bit -	Symmetric Key - CSP			Block Cipher Key Expansion
KEK	Key Encryption Key	256 bit -	Symmetric Key - CSP			Key Decryption
FWI	CMAC key used to verify the integrity of Crypto Firmware and Boot Firmware and authenticity during update	256 bit - 256	Symmetric Key - CSP			Firmware Integrity Verification
AMK	Authentication Mechanism for P25 Link Layer Authentication	128 bit -	Symmetric Key - CSP			Block Cipher

Table 15: SSP Table 1

Note: SSP Table 1 describes only the SSPs used in Approved Mode. SSPs used exclusively in Non-Approved Mode (e.g., DES-based TEK/KEK) are excluded from this table.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TEK	KVL_in SPI_in	NVM:Plaintext RAM:Plaintext	Until Zeroize service or other similar services are performed, or tamper is detected	Z1 Z2 Z3	
KEK	SPI_in KVL_in	NVM:Plaintext RAM:Plaintext	Until Zeroize service or other similar services are performed, or tamper is detected	Z1 Z2 Z3	TEK:Encrypts
FWI		RAM:Plaintext NVM:Plaintext	until firmware is upgraded.	Z2 Z4	
AMK	KVL_in	NVM:Plaintext RAM:Plaintext	Until Zeroize service or other similar services are performed, or tamper is detected	Z1 Z2 Z3	

Table 16: SSP Table 2

This section describes all SSPs used by the module.
The module does not use public key cryptography.

More than two TEKs or KEKs can be stored in the module. They are managed by CKR, which associates each key with its KeyID and algorithm (i.e., AES or DES).
TEK or KEK associated with AES can be used only in Approved Mode, and TEK or KEK associated with DES can be used only in Non-Approved Mode.

Note:
The FWI is implemented as a key embedded within the Crypto firmware.

No Assurance:
TEK, KEK, and AMK are externally loaded. There is no assurance of their strength.

9.5 Transitions

The cryptographic module uses AES-ECB, AES-OFB, AES-CMAC and SHA2-256 as Approved algorithms.
According to NIST SP 800-131A Rev.2, there are currently no plans for these algorithms to be removed from the list of Approved algorithms.
Non-Approved algorithms (DES, DES-MAC) are not permitted in Approved mode and are already considered non-compliant per SP 800-131A Rev.2.

9.6 Additional Information

The cryptographic module does not provide any mechanism for outputting SSPs, in order to protect this sensitive information.
As a hardware module, it is not possible to externally interfere with the SSP processes.
Therefore, all SSPs are securely protected.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Crypto Firmware	key size: 256 bits	CMAC	SW/FW Integrity	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Performed on Firmware binary data
Boot Firmware	key size: 256 bits	CMAC	SW/FW Integrity	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Performed on Boot Firmware binary data

Table 17: Pre-Operational Self-Tests

Each time the cryptographic module is powered on, it performs pre-operational self-tests listed in the table.
Before performing the firmware integrity test using CMAC, the module first executes a Known Answer Test (KAT) on the CMAC algorithm to verify its correct operation.

The self-tests can also be initiated on demand by cycling the module’s power.

The firmware consists of Crypto Firmware, Boot Firmware, and ROM Boot Firmware.
The firmware integrity test covers both the Crypto Firmware and the Boot Firmware.
ROM Boot Firmware resides in mask ROM, and its integrity test is not required according to Section 7.10.2.2 of ISO/IEC 19790:2012.
If the integrity test fails, the SCM enters an error state in which only the Show Status service remains functional.
Operators can use the Show Status service to confirm that the self-tests have failed.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Firmware Load	AES CMAC	MAC verification	SW/FW Load	"Firmware Update Ack" SPI command: "0x8A01" + Checksum (Pass), "0x8A00" or "0xFF01" (Fail)	Verification of loaded firmware image	when firmware is loaded
AES-ECB (AES 2696)	key size: 256 bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Encrypt	Upon power-up
AES-ECB (AES 2696)	key size: 256 bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Decrypt	Upon power-up
AES-CMAC (AES 2696)	key size: 256 bits, MAC Length:128bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	MAC	Upon power-up
AES-OFB (AES 2696)	key size: 256 bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Encrypt	Upon power-up
AES-OFB (AES 2696)	key size: 256 bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status	Decrypt	Upon power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				Request" SPI command: 0 (Pass), 1 (Fail)		
SHA2-256 (SHS 2285)	message size: 256 bits	KAT	CAST	Corresponding bit of "Self Test Status" for "Status Request" SPI command: 0 (Pass), 1 (Fail)	Hash	Upon power-up

Table 18: Conditional Self-Tests

Each time the cryptographic module is powered on, it performs cryptographic algorithm tests. Firmware load test is initiated by requiring Firmware Update service.

If any of the Known Answer Tests (KATs) or the firmware load test fail, the SCM enters an error state in which only the Show Status service remains functional.
Operators can use the Show Status service to confirm that the self-tests have failed.

The cryptographic module does not implement any critical functions as defined by FIPS 140-3. Therefore, no critical function tests are required or performed.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Crypto Firmware	CMAC	SW/FW Integrity	On Demand	manually
Boot Firmware	CMAC	SW/FW Integrity	On Demand	manually

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Load	MAC verification	SW/FW Load	N/A	Provided service
AES-ECB (AES 2696)	KAT	CAST	On Demand	manually
AES-ECB (AES 2696)	KAT	CAST	On Demand	manually
AES-CMAC (AES 2696)	KAT	CAST	On Demand	manually
AES-OFB (AES 2696)	KAT	CAST	On Demand	manually
AES-OFB (AES 2696)	KAT	CAST	On Demand	manually
SHA2-256 (SHS 2285)	KAT	CAST	On Demand	manually

Table 20: Conditional Periodic Information

Firmware integrity tests and cryptographic algorithm tests can be executed on demand by cycling the module's power.
The firmware load test is not executed by power cycling; it is performed only during the firmware loading process.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module transitions to the Error state when any of the defined transition conditions are met. In this state, only the "Show Status" service is operational; all other services are disabled.	Failure of a Self-tests (e.g., KAT, Firmware Integrity Test, Firmware Load Test) CRNG test failure during encryption/decryption initialization Detection of active tamper ESN authentication timeout during boot	the module shall be re-booted to perform normal operation	Any bit of "Self Test Status" for "Status Request" SPI command is "1"

Table 21: Error States

The module automatically transitions to an error state when a self-test or firmware load test fails, without requiring any explicit command.
When the module is in an error state, it only accepts the *Show Status* service. This service allows the operator to confirm that the module is in an error state. There is no error state in which the module does not accept the *Show Status* service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation
The cryptographic module is intended to be embedded within a radio device.

Just after shipping, the module is not validated one. To cause the module to become validated one, the following procedures are needed.
The procedure is as follows:

1. The Crypto Officer powers on the cryptographic module and verifies that both the self-tests and radio authentication have completed successfully.
2. The Crypto Officer sends the SPI FIPS Validated Mode Set command to initiate the transition to FIPS140-3 Validated mode. (Refer to the **SPI Interface Specification** for command details.)
3. Reboot the module to complete the transition.
4. After rebooting, the module becomes the validated one.
5. The validated state can be confirmed by checking the firmware version (A3.2.0),. Approved Mode can be confirmed by using the Show Status service to check that the Approved Mode flag within the 16-bit Cipher Status value is set to "1".

For details on how to install the module into the radio, refer to the **Administrator User Guidance** document.

Initialization

After the module has entered FIPS 140-3 Validated mode, the Crypto Officer must perform certain operations at each power-on to ensure secure operation.

Specifically, after verifying the completion of self-tests, the Crypto Officer must execute the Authentication command via the SPI interface to identify the radio device and enable cryptographic services.

If required, cryptographic keys may also be loaded into the module using the KVL mode service or the OTAR Set-Key service. However, key loading is not mandatory at every power-on and should be performed only when necessary.

11.2 Administrator Guidance

For administrative guidance, refer to the Administrator User Guidance document.

11.3 Non-Administrator Guidance

For non-administrative user guidance, also refer to the Administrator User Guidance document.

11.4 Design and Rules

The design of the cryptographic module complies with the security rules defined for FIPS 140-3 Level 1.
This section describes the security rules enforced by the module to meet the applicable requirements.

1. **Physical Security**:
   All components within the module are production-grade and utilize standard protective technologies.
2. **Restrictions in Error State**:
   When the module enters an error state, all operations except status checking are prohibited.
   Self-tests, zeroization, and data output are not permitted during this state.
3. **Protection of Status Information**:
   Status information does not include any Critical Security Parameters (CSPs) or other sensitive data that could compromise the security of the module if misused.
4. **Key Input Methods**:
   Keys are input either in plaintext using a compatible key loader by the Crypto Officer, or in encrypted form via the OTAR (Over-the-Air Rekeying) function.
5. **CSP Output Prohibition**:
   The Secure Cryptographic Module (SCM) does not output any CSPs.
6. **Approved Mode Operation**:
   Secure communication in approved mode must use AES.
   DES are not permitted in approved mode.

7. **Radio Pairing**:
   The cryptographic module is paired with a specific radio device.
   If an invalid radio identifier is detected, the SCM zeroizes the SSPs, including TEK, KEK, and AMK.
8. **Tamper Response Behavior**:
   The module's response to tamper detection depends on the Key Retention flag.
   - If the flag is set, all SSPs are zeroized upon a tamper event.
   - If the flag is not set, only SSPs stored in RAM are zeroized.
9. **Secure Development Environment:**
   The firmware development environment uses Code Composer Studio IDE Version 9.01 and Code Generation Tool Version 4.4.1.
   Program code is managed using Git for version control.
   To ensure secure code development, a static analysis tool is employed to detect and remediate potential vulnerabilities during the development process.

11.5 Maintenance Requirements

The cryptographic module does not require maintenance or inspection.

11.6 End of Life

When the cryptographic module reaches the end of its operational life, the Crypto Officer executes the Factory Reset service to return the module to its factory default state.
This service deletes all Security Sensitive Parameters (SSPs) and resets configuration settings to their initial state.

12 Mitigation of Other Attacks

12.1 Attack List

- Key misuse due to module relocation:

The cryptographic module may be removed from its originally paired radio device and connected to another device. Stored keys (e.g., TEK, KEK, AMK) may be misused on another radio device.

- Key misuse via powered interface substitution:

While the module is powered on, an attacker may redirect the interface connection to another device, enabling unauthorized use of the keys.

12.2 Mitigation Effectiveness

- Active Tamper Detection:

If the module is removed from the radio while powered on, immediate zeroization is triggered.

- Static Tamper Detection:

If removal is detected while the module is powered off, zeroization is performed during the next power-up.

13 Acronyms

Acronyms	Definition
ACK	Acknowledgment
AM	Authentication Mechanism
AMK	Authentication Management Key
CKR	Common Key Reference
DSP	Digital Signal Processor
ESN	Electronic Serial Number
FWI	Firmware Integrity
IV	Initialization Vector
KEK	Key Encryption Key
KFD	Key Fill Device
KMM	Key Management Message
KVL	Key Variable Loader
NVM	Non-Volatile Memory
OTAR	Over the Air Rekeying
P25	Project 25
RSI	Radio Set ID
SCM	Secure Cryptographic Module
SLN	Storage Location Number
SPI	Serial Peripheral Interface
SUID	Subscriber Unit ID
TEK	Traffic Encryption Key
UART	Universal Asynchronous Receiver/Transmitter