

Motorola Solutions Inc.

Motorola P25 KVL 7000 HSM

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

Date: July 16, 2026



Table of Contents

1 General	5
1.1 Overview	5
1.2 Security Levels	5
2 Cryptographic Module Specification	5
2.1 Description	5
2.2 Tested and Vendor Affirmed Module Version and Identification	8
2.3 Excluded Components	9
2.4 Modes of Operation	9
2.5 Algorithms	10
2.6 Security Function Implementations	11
2.7 Algorithm Specific Information	14
2.8 RBG and Entropy	14
2.9 Key Generation	14
2.10 Key Establishment	14
2.11 Industry Protocols	14
3 Cryptographic Module Interfaces	14
3.1 Ports and Interfaces	14
4 Roles, Services, and Authentication	15
4.1 Authentication Methods	15
4.2 Roles	16
4.3 Approved Services	16
4.4 Non-Approved Services	24
4.5 External Software/Firmware Loaded	24
5 Software/Firmware Security	25
5.1 Integrity Techniques	25
5.2 Initiate on Demand	25
6 Operational Environment	25
6.1 Operational Environment Type and Requirements	25
7 Physical Security	25
7.1 Mechanisms and Actions Required	25
7.2 EFP/EFT Information	26
7.3 Hardness Testing Temperature Ranges	26
8 Non-Invasive Security	26
9 Sensitive Security Parameters Management	26
9.1 Storage Areas	26

9.2 SSP Input-Output Methods	27
9.3 SSP Zeroization Methods	27
9.4 SSPs	28
10 Self-Tests	34
10.1 Pre-Operational Self-Tests	34
10.2 Conditional Self-Tests	34
10.3 Periodic Self-Test Information	38
10.4 Error States	40
11 Life-Cycle Assurance	41
11.1 Installation, Initialization, and Startup Procedures	41
11.2 Administrator Guidance	41
11.3 Non-Administrator Guidance	41
11.4 End of Life	41
12 Mitigation of Other Attacks	41
References and Definitions	42

List of Tables

Table 1: Security Levels	5
Table 2: Tested Module Identification – Hardware	8
Table 3: Approved Drop-In Algorithms	8
Table 4: Modes List and Description	9
Table 5: Approved Algorithms	11
Table 6: Vendor-Affirmed Algorithms	11
Table 7: Security Function Implementations.....	13
Table 8: Entropy Certificates	14
Table 9: Entropy Sources.....	14
Table 10: Ports and Interfaces	15
Table 11: Authentication Methods.....	16
Table 12: Roles.....	16
Table 13: Approved Services	24
Table 14: Mechanisms and Actions Required	26
Table 15: EFP/EFT Information.....	26
Table 16: Hardness Testing Temperatures	26
Table 17: Storage Areas	27
Table 18: SSP Input-Output Methods.....	27
Table 19: SSP Zeroization Methods.....	28
Table 20: SSP Table 1	31
Table 21: SSP Table 2	33
Table 22: Pre-Operational Self-Tests	34
Table 23: Conditional Self-Tests	38
Table 24: Pre-Operational Periodic Information.....	38
Table 25: Conditional Periodic Information.....	40
Table 26: Error States	40
Table 27: References.....	42
Table 28: Acronyms and Definitions	44

List of Figures

Figure 1: P25 Key Variable Loader (KVL) 7000.....	6
Figure 2: P25 KVL 7000 HSM (Top).....	7
Figure 3: P25 KVL 7000 HSM (Interfaces)	7
Figure 4: P25 KVL 7000 Cryptographic Boundary.....	8

Version	Date	Author	Description
1.0	03/25/2026	Motorola Solutions	Initial release

1 General

1.1 Overview

This document defines the Security Policy for the Motorola P25 Key Variable Loader (KVL) 7000 HSM, manufactured by Motorola Solutions, Inc. (hereafter referred to as 'the Module').

The Motorola P25 KVL 7000 is a portable key distribution device comprising two primary components: the KVL Host Application and the P25 KVL 7000 HSM. The Module itself is a single-chip cryptographic engine designed to meet FIPS 140-3 Level 3 physical security requirements.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module securely generates, loads, and manages encryption and authentication keys for communication products. Through the P25 KVL 7000, it integrates with the Key Management Facility (KMF) to provision radios and consoles for centralized key management.

The Module is designed for the Motorola P25 Key Variable Loader (KVL) 7000 and is intended for US Federal agencies or other markets requiring FIPS 140-3 Overall Security Level 2 validation.

Module Type: Hardware

Module Embodiment: Single Chip

Cryptographic Boundary:

Figure 2 and Figure 3 depict the physical form of the module. The Module is a single-chip embodiment, with its cryptographic boundary illustrated in Figure 4.



Figure 1: P25 Key Variable Loader (KVL) 7000

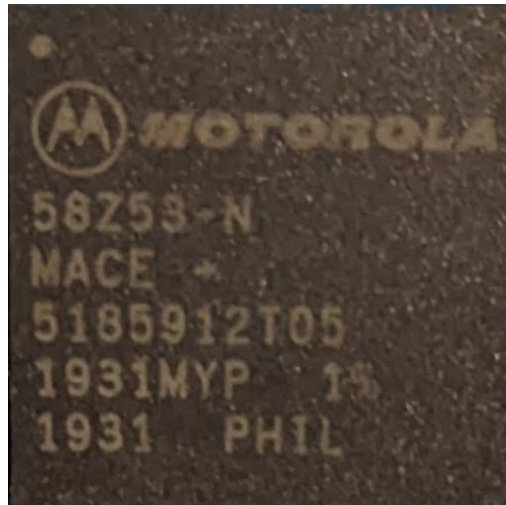


Figure 2: P25 KVL 7000 HSM (Top)

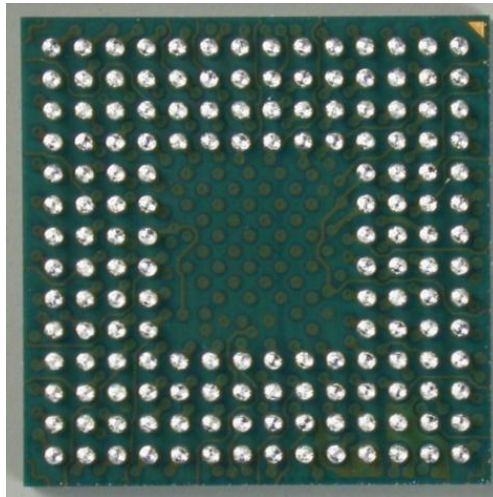


Figure 3: P25 KVL 7000 HSM (Interfaces)

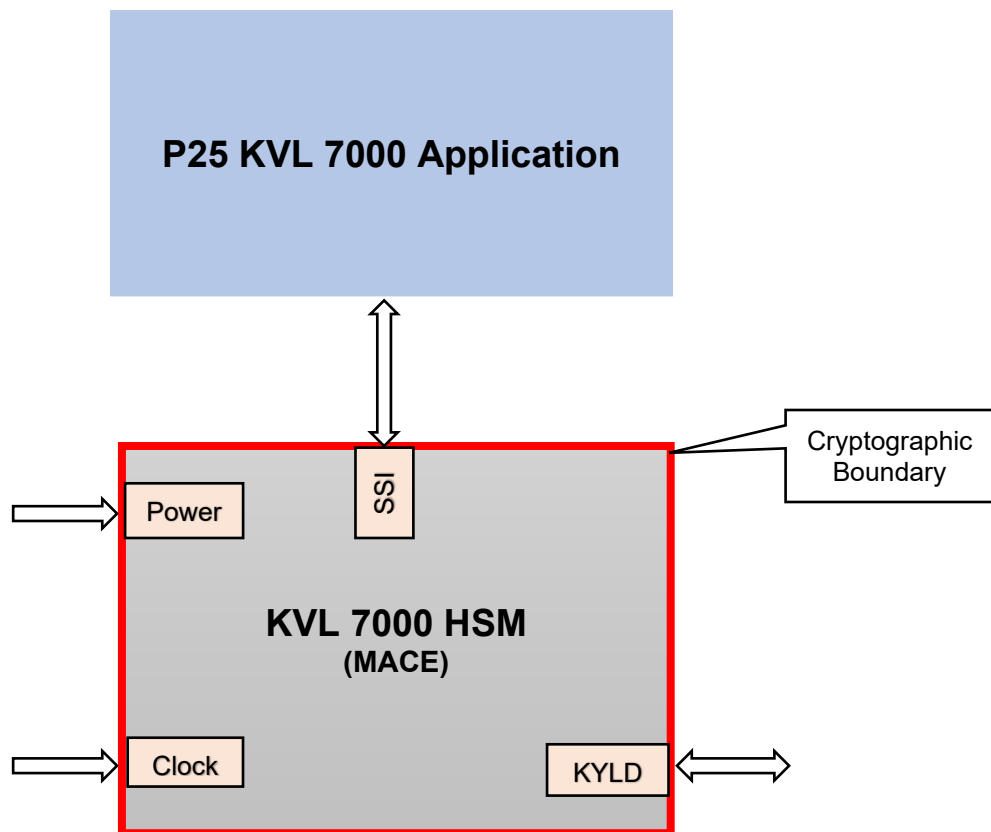


Figure 4: P25 KVL 7000 Cryptographic Boundary

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The Module is tested on the following operational environment:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
5185912T05	5185912	R70.01.01	MACE #5185912 family	

Table 2: Tested Module Identification – Hardware

The Module supports the following approved algorithms that may be installed separately from the Module's base firmware using the Program Update service. While the installation of AES may be done separately, for the purposes of this validation, the Module includes this firmware.

Algorithm	Algorithm FW Version	Base FW Version	Cert. #
AES128	R01.00.06	R70.01.01	A7817
AES256	R01.00.09	R70.01.01	A7818

Table 3: Approved Drop-In Algorithms

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 exclude any components from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode 2	Operating in approved mode	Approved	Approved mode: level 2 (Standard) FIPS Status: Compliant
Approved Mode 3	Operating in approved mode	Approved	Approved mode: legacy level 3 (High) FIPS status: Compliant

Table 4: Modes List and Description

The P25 KVL 7000 HSM Module is initially non-compliant and must be configured by the Crypto Officer (CO) to operate in the approved FIPS 140-3 mode at overall Security Level 2.

To operate in the approved mode, the Crypto Officer must ensure the Module is:

- Properly installed, initialized, and configured. Initialization steps are listed in Section 11.1 of this document.
- Secured by creating passwords for both the Crypto Officer (CO) and User roles.

The operational status of the P25 KVL 7000 is determined via the settings menu of the P25 KVL 7000 Host application graphical user interface. When operating in the approved mode, the display will indicate:

- FIPS mode: Level 2 (Standard) or Legacy level 3 (High)
- FIPS Status: Compliant

When the module is in the approved operating mode, the “Module Info” service can be used to verify that the firmware version matches an approved version listed on NIST’s website:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>

Mode Change Instructions and Status:

In order to configure the Module for an approved mode at overall Security Level 2, the P25 KVL 7000 operator must log in as CO and set the FIPS mode in the settings menu as follows

- FIPS mode: Level 2 (Standard) or Legacy level 3 (High)

Only Approved algorithms may be loaded into the Module. At a minimum, one of the “Drop-In Algorithms” listed in Table 3 must be added from the Module independent of the base firmware via the Program Update service.

The loading of non-validated base firmware or Drop-In-Algorithms within the validated cryptographic module invalidates the module’s validation.

2.5 Algorithms

Approved Algorithms:

The Module implements the FIPS Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CFB128, AES-CFB8, AES-CTR, AES-ECB, AES-OFB	A7818, A7819	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CBC, AES-CTR, AES-ECB, AES-OFB	A7817	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-GCM, AES-GMAC	A7817	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 128	SP 800-38D
AES-GCM, AES-GMAC	A7818, A7819	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 256	SP 800-38D
AES-KW	A8087	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
Counter DRBG	A8088	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 256, 1024 Nonce - Nonce: 128, 512 Personalization String Length - Personalization String Length: 256, 512 Returned Bits - 128	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-5)	A8089	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
RSA SigVer (FIPS186-5)	A5253	Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-256	SHS 817	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-256, SHA2-384	A8090	Message Length - Message Length: 8-2048 Increment 8	FIPS 180-4

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type :AES 128 Symmetric Key Type :AES 256 Symmetric	N/A	SP800-133rev2 Section4, example 1 and IG D.H

Table 6: Vendor-Affirmed Algorithms

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:

N/A for this module.

2.6 Security Function Implementations

The following table shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
A7817 Authenticated	BC-Auth	Authenticated Encrypt, Authenticated Decrypt	IG C.H:Scenario 2	AES-GCM: (A7817) AES-GMAC: (A7817) AES-ECB: (A7817)
A7817 Decryption	BC- UnAuth	Block Cipher		AES-CBC: (A7817)

Name	Type	Description	Properties	Algorithms
				AES-ECB: (A7817) AES-OFB: (A7817) AES-CTR: (A7817)
A7817 Encryption	BC- UnAuth	Block Cipher		AES-CBC: (A7817) AES-ECB: (A7817) AES-OFB: (A7817) AES-CTR: (A7817)
A7818 Authenticated	BC-Auth	Authenticated Encrypt, Authenticated Decrypt	IG C.H:Scenario 2	AES-GCM: (A7818) AES-GMAC: (A7818) AES-ECB: (A7818)
A7818 Decryption	BC- UnAuth	Block Cipher		AES-CBC: (A7818) AES-ECB: (A7818) AES-OFB: (A7818) AES-CTR: (A7818)
A7818 Encryption	BC- UnAuth	Block Cipher		AES-CBC: (A7818) AES-ECB: (A7818) AES-OFB: (A7818) AES-CTR: (A7818) AES-CFB128: (A7818)
A7819 Authenticated	BC-Auth	Authenticated Encrypt, Authenticated Decrypt, Message Authentication	IG C.H:Scenario 2	AES-GCM: (A7819) AES-GMAC: (A7819) AES-ECB: (A7819)
A7819 Decryption	BC- UnAuth	Block Cipher		AES-CBC: (A7819) AES-CFB8: (A7819) AES-ECB:

Name	Type	Description	Properties	Algorithms
				(A7819) AES-OFB: (A7819)
A7819 Encryption	BC- UnAuth	Block Cipher		AES-CBC: (A7819) AES-CFB8: (A7819) AES-ECB: (A7819) AES-OFB: (A7819)
Common- SHA2	SHA	Secure Hash Standard		SHA2-256: (A8090) SHA2-384: (A8090)
Entropy	ENT- ESV	Entropy source		
KeyGen	CKG	Symmetric Key Generation		Counter DRBG: (A8088)
KTS-GCM	KTS- Unwrap KTS- Wrap	Key Transport - Wrapping and Unwrapping	caveat:Key establishment methodology provides 256 bits of security strength	AES-GCM: (A7819) AES-ECB: (A7819)
KTS-KW	KTS- Wrap	Key Transport - Wrapping	caveat:Key establishment methodology provides 256 bits of security strength	AES-KW: (A8087) AES-ECB: (A7819)
RNG	DRBG	AES-256 CTR Deterministic RBG		Counter DRBG: (A8088) AES-ECB: (A7819)
SHA	SHA	Secure Hash Standard		SHA2-256: (SHS 817)
SigVer1	DigSig- SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A5253) SHA2-256: (SHS 817)
SigVer2	DigSig- SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-5): (A8089) SHA2-384: (A8090)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Generation:

Per IG C.H Scenario 2, the Module internally generates a 96-bit GCM IV internally as specified in SP800-38D section 8.2.2 using an approved DRBG (Cert. #A8088).

2.8 RBG and Entropy

Cert Number	Vendor Name
E132	Motorola Solutions

Table 8: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Motorola Solutions Advanced Crypto Engine (MACE) Entropy Source	Physical	Atmel 5186912	1 bit	0.138262	

Table 9: Entropy Sources

2.9 Key Generation

For Key Generation methods, see Section 2.6 Security Function Implementations above.

2.10 Key Establishment

For Key Establishment methods, see Section 2.6 Security Function Implementations above.

2.11 Industry Protocols

N/A, This module does not implement industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
Synchronous Serial Interface (SSI)	Data Input Data Output	This is the interface to the KVL 7000 Host Application. All SSPs exchanged over this interface are always encrypted.

Physical Port	Logical Interface(s)	Data That Passes
	Control Input Status Output	
KYLD (Keyload) Interface	Data Input Data Output Control Input	This is the interface to external devices. All SSPs exchanged over this interface are either encrypted or in plaintext when operating in approved mode.
Clock	Control Input	Clock input.
Power	Power	This interface powers all circuitry.

Table 10: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module supports two authenticated operator roles—Crypto Officer (CO) and User—as well as services that do not require authentication (UA).

The Roles Table below lists all operator roles supported by the Module.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
AM	Identity-based. The password length is a minimum of 15 characters using any combination of ASCII printable characters and is padded to a 30-byte long hexadecimal number. After authenticating, the KVL user may change it any time through the SSI Port.	SHA2-256 (A8090)	Since the password length is a minimum of 15 characters using any combination of ASCII printable characters and is padded to a 30-byte long hexadecimal number; the probability of a successful random attempt is 1 in 95^{15}	The Module limits the number of consecutive failed authentication attempts to a configurable number (Minimum 3, maximum 20). Upon exceeding the maximum number of login attempts, the module can be configured to either lock the device from further login attempts for a specified amount of time (configurable by the CO between 1-30 minutes), or execute the Factory Reset service. The minimum probability of a successful random attempt during a one-

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
				minute period is 20 in 95 ¹⁵

Table 11: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	AM
User	Identity	User	AM

Table 12: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Change CO Password	Change current Crypto-Officer password.	Success or Fail	Password	Successful change the password will allow access to the services allowed for CO role.	Common-SHA2 KTS-GCM	Crypto Officer - AES-GCM IV : E - CO PWD (AM): W,E,Z - IEK: E,Z - KPK: Z - PWD Hash: G,E,Z
Change User Password	Change current User password.	Success or Fail	Password	Successful change the password will allow access to the services allowed for User role.	Common-SHA2 KTS-GCM	Crypto Officer - AES-GCM IV : E - IEK: E,Z - KPK: Z - PWD Hash: G,E,Z - User PWD (AM): W,E,Z
Configure and Query Target Device	Configure target device and retrieve key	Success or Fail	Command In	Target device information or failure	A7819 Encryption A7819 Authenticat	Crypto Officer - AES-GCM IV : G,E - BKK: E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	metadata and versions from the target device.				ed RNG	Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG- EI/Seed: E - DRBG- nonce: E User - AES-GCM IV : G,E - BKK: E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG- EI/Seed: E - DRBG- nonce: E
Configure KVL	Configure the module.	Success or Fail	Configuration parameters	Updated module configuration, or failure.	Common-SHA2 KTS-GCM RNG	Crypto Officer - AES-GCM IV : E - CO PWD (AM): W,E,Z - IEK: W,E,Z - KPK: G,Z - PWD Hash: G,E,Z - User PWD (AM): W,E,Z
Decrypt	Decrypt Ciphertext data	Success or Fail	Ciphertext	Plaintext (success) or failure	A7817 Authenticated A7817 Decryption A7818 Authenticated A7818 Decryption A7819 Authenticated A7819	Crypto Officer - AES-GCM IV : E - KEK: W,E,Z - KPK: E - TEK: W,E,Z User - AES-GCM IV : E - KEK: W,E,Z - KPK: E - TEK: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Decryption KTS-GCM	
Encrypt	Encrypt plaintext data	Success or Fail	Plaintext	Ciphertext (success) or failure	A7817 Encryption A7817 Authenticated A7818 Encryption A7818 Authenticated A7819 Encryption A7819 Authenticated RNG KTS-GCM	Crypto Officer - AES-GCM IV : G,E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-El/Seed: E - DRBG-nonce: E - KEK: W,E,Z - KPK: E - TEK: W,E,Z User - AES-GCM IV : G,E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-El/Seed: E - DRBG-nonce: E - KEK: W,E,Z - KPK: E - TEK: W,E,Z
Factory Reset	Reset the module to factory default	Success or Fail	Command In.	Success or Fail	None	Crypto Officer - BKK: Z - CO PWD (AM): Z - IEK: Z - KPK: Z - PWD Hash: Z - User PWD (AM): Z Unauthenticated - BKK: Z - CO PWD (AM): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IEK: Z - KPK: Z - PWD Hash: Z - User PWD (AM): Z - User - BKK: Z - CO PWD (AM): Z - IEK: Z - KPK: Z - PWD Hash: Z - User PWD (AM): Z
Generate Key	Generate TEK/KEK	Success or Fail	Command In	Encrypted keys (Success) or failure	RNG KeyGen KTS-GCM	Crypto Officer - AES-GCM IV : G,E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E - KEK: G,R - KPK: E - TEK: G,R - User - AES-GCM IV : G,E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E - KEK: G,R - KPK: E - TEK: G,R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Generate Random Number	Generate random number	Success or Fail	Command In	Random number or failure	RNG Entropy	Crypto Officer - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-El/Seed: G,E - DRBG-nonce: G,E Unauthenticated - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-El/Seed: G,E - DRBG-nonce: G,E User - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-El/Seed: G,E - DRBG-nonce: G,E
Key Check	Check the validity of a given key	Success or Fail	Encrypted key	Success or failure	KTS-GCM	Crypto Officer - AES-GCM IV : E - KPK: E - KEK: W - TEK: W User - AES-GCM IV : E - KPK: E - KEK: W - TEK: W
Key Sharing	Combination of receive	Success or Fail	Command In	Success or failure	RNG KTS-GCM	Crypto Officer - AES-GCM IV : G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and transfer TEK/KEK between two KVLs.					- DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E - KEK: R,W - KPK: E - TEK: R,W User - AES-GCM IV : G,E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E - KEK: R,W - KPK: E - TEK: R,W
Login CO	Validate current Crypto-Office passwords .	Success or Fail	Password	Successful authentication will allow access to the services allowed for CO role.	Common-SHA2 KTS-GCM	Crypto Officer - AES-GCM IV : E - CO PWD (AM): W,E,Z - IEK: E,Z - KPK: Z - PWD Hash: G,E,Z
Login User	Validate current User passwords .	Success or Fail	Password	Successful authentication will allow access to the services allowed for User role.	Common-SHA2 KTS-GCM	Crypto Officer - AES-GCM IV : E - IEK: E,Z - KPK: Z - PWD Hash: G,E,Z - User PWD (AM): W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Info	Query module firmware, hardware version.	Success or Fail	Command In.	HSM Firmware version; Hardware information and FIPS status	None	Crypto Officer Unauthenticated User
Power On	Power on the module	Success or Fail	N/A	Module is powered on	SigVer1	Unauthenticated - RSA FW-LD-Pub: E
Program Update	Update the module firmware.	Success or Fail	Firmware image	The module is upgraded to new firmware	SHA SigVer2	Crypto Officer - CO PWD (AM): Z - ECC FW-LD-Pub: E - IEK: Z - KPK: Z - PWD Hash: Z - User PWD (AM): Z
Receive Key	Receive TEK/KEK from KVL or KVL Host	Success or Fail	TEK/KEK	Encrypted keys (Success) or failure	KTS-GCM	Crypto Officer - AES-GCM IV : E - IEK: E - KEK: W - KPK: E - TEK: W User - AES-GCM IV : E - IEK: E - KEK: W - KPK: E - TEK: W
Store and Forward	Receive TEK/KEK from the KMF into the module (store), and then transfer them to the target device (forward).	Success or Fail	TEK/KEK	Encrypted TEK/KEK (Success) or failure	A7819 Encryption RNG KTS-GCM KTS-KW	Crypto Officer - BKK: E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KEK: R,W - KPK: E - TEK: R,W - User - BKK: E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: G,E - DRBG-nonce: G,E - KEK: R,W - KPK: E - TEK: R,W
Transfer Key	Transfer keys to target device.	Success or Fail	TEK/KEK	Success or failure	A7819 Encryption RNG KTS-GCM	Crypto Officer - AES-GCM IV : G,E - BKK: E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E - KEK: R - KPK: E - TEK: R - User - AES-GCM IV : G,E - BKK: E - DRBG Internal State - Key: G,E - DRBG Internal State - V: G,E - DRBG-EI/Seed: E - DRBG-nonce: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KEK: R - KPK: E - TEK: R
Zeroize Key	Zeroize keys in the target device	Success or Fail	Command In	Success or failure	A7819 Authenticated A7819 Encryption RNG	Crypto Officer - AES-GCM IV : G,E - BKK: E - DRBG Internal State - Key: E - DRBG Internal State - V: E - DRBG-EI/Seed: E - DRBG-nonce: E User - AES-GCM IV : G,E - BKK: E - DRBG Internal State - Key: E - DRBG Internal State - V: E - DRBG-EI/Seed: E - DRBG-nonce: E

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

This module supports the loading of external firmware via the Program Update service. The module supports the firmware load test by using ECDSA P-384. In order to load new firmware, the Crypto officer must authenticate to the module before loading the firmware. Execution of the successfully loaded firmware is only effective after the next reset of the security module. The update attempt will be rejected if the verification fails.

Any firmware loaded into the module other than that listed in section 2.2 Tested and Vendor Affirmed Module Version and Identification, is outside the scope of this Security Policy and requires a separate FIPS 140-3 validation.

The module validates the integrity of the components listed in section 5.1 during firmware load.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module has a limited operational environment under the FIPS 140-3 definitions. The Module is composed of the following firmware components:

- Component 1: Executable - binary
- Component 2: Drop-In-Algorithms - binary

The firmware components are protected with the RSA FW-LD-Pub key described in section 9.4 SSPs. The RSA FW-LD-Pub key is loaded into the module at manufacturing.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the Module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

The Module is a production-grade, single-chip cryptographic module as defined by FIPS 140-3, designed to meet Level 3 physical security requirements. The information below applies to Hardware Revision Number 5185912T05.

7.1 Mechanisms and Actions Required

The P25 KVL 7000 HSM (MACE) is covered with a hard, opaque epoxy coating that provides evidence of tampering. The security provided by the hardness of this epoxy encapsulant is claimed for the temperature range of -40°C to 85°C. No assurance of hardness is claimed outside this range.

The Module does not contain any doors, removable covers, ventilation holes, or slits, and no maintenance access interface is available. Therefore, no special procedures are required to maintain physical security during delivery to operators.

Mechanism	Inspection Frequency	Inspection Guidance
Covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the KVL 7000 HSM (MACE)	Periodically	Look for signs of tampering. Remove from service if tampering found.

Table 14: Mechanisms and Actions Required

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-38.1°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
HighTemperature	101.4°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
LowVoltage	1.65V - VDDCORE : 1.350V - VVDBU	EFP	Shutdown - A general reset of the chip is asserted.
HighVoltage	2.04V - VDDCORE : 2.292V - VVDBU	EFP	Shutdown- A tamper flag is raised, a wake-up reset of the product is triggered.

Table 15: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40°C
HighTemperature	85°C

Table 16: Hardness Testing Temperatures

Notes: The module is hardness tested at the lowest and highest temperatures within the module's intended temperature range of operation.

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Flash Memory (S2)	Stored in the flash in plaintext, associated by memory location (pointer).	Static
System Memory (S1)	Stored in the volatile memory (RAM).	Dynamic

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input encrypted on KPK (I2)	Flash Memory (S2)	Host Software (outside)	Encrypted	Manual	Electronic	KTS-GCM
Input encrypted on the IEK (I1)	Host Software (outside)	Flash Memory (S2)	Encrypted	Manual	Electronic	KTS-GCM
Input in plaintext (I3)	Another KVL (outside)	Flash Memory (S2)	Plaintext	Manual	Electronic	
Output encrypted on BKK (O1)	Flash Memory (S2)	Target device (outside)	Encrypted	Manual	Electronic	KTS-GCM
Output encrypted on BKK (O2)	Flash Memory (S2)	Target device (outside)	Encrypted	Manual	Electronic	A7819 Encryption
Output encrypted on KPK (O3)	Flash Memory (S2)	KVL Host (outside)	Encrypted	Manual	Electronic	KTS-GCM
Output in plaintext (O4)	Flash Memory (S2)	Target device (outside)	Plaintext	Manual	Electronic	

Table 18: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized by module power cycle or hard reset.	SSPs in volatile memory zeroized.	Yes
Z2	Zeroized by the "Program Update" service.	SSPs zeroized upon loading of new firmware.	Yes

Zeroization Method	Description	Rationale	Operator Initiation
Z3	Zeroized by the "Configure KVL" service.	CO zeroizes the module when configuring into an Approved mode.	Yes
Z4	Zeroized by the "Login CO Password" service.	CO password zeroized after too many failed login attempts.	Yes
Z5	Zeroized by the "Change CO Password" service.	CO password zeroized after too many failed attempts.	Yes
Z6	Zeroized by the "Login User Password" service.	User password zeroized after too many failed login attempts.	Yes
Z7	Zeroized by the "Change User Password" service.	User password zeroized after too many failed attempts.	Yes
Z8	Zeroized by the "Factory Reset" service.	CO or User performs factory reset of the module.	Yes

Table 19: SSP Zeroization Methods

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in section 4.3 Approved Services.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES-GCM IV	AES-GCM encryption is used for data encryption	96 bits - 96 bits	PSP - PSP	RNG		A7817 Authenticated A7818 Authenticated A7819 Authenticated KTS-GCM
BKK	A 256-bit AES GCM or OFB (A7819) key used for encrypting keys exported over KYLD port.	256 bits - 256 bits	Symmetric Key - CSP	Pre-loaded		A7819 Authenticated A7819 Encryption KTS-GCM KTS-KW
CO PWD (AM)	A 30-byte long hexadecimal number to authenticate the CO role	N/A - N/A	Authentication - CSP	N/A		Common-SHA2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State - Key	AES-256 CTR DRBG state Key used in the generation of a random values	256 bits - 256 bits	DRBG Key - CSP	RNG		RNG KeyGen
DRBG Internal State - V	AES-256 CTR DRBG state V value used in the generation of a random values	128 bit - 128 bits	DRBG V value - CSP	RNG		RNG KeyGen
DRBG-El/Seed	Internally generated by the HWRNG	1856 bit - 256.6 bits	DRBG CSP - CSP	Entropy		RNG KeyGen
DRBG-nonce	Internally generated by the HWRNG	960 bits - 132.7 bits	DRBG CSP - CSP	Entropy		RNG KeyGen
ECC FW-LD-Pub	An ECDSA P-384 public key is used to validate the signature of the upgrade image.	384 bits - 192 bits	Asymmetric Public Key - PSP	Generated outside of the module		SigVer2
IEK	A 256-bit AES GCM (A7819) key used for decrypting keys and passwords entered over SSI port.	256 bits - 256 bits	Symmetric Key - CSP	Generated outside to the module		KTS-GCM
KEK	128, 256-bit AES key used for encryption of keys in the Store and Forward	128 bits or 256 bits - 128 bits or 256 bits	Symmetric Key - CSP	KeyGen		A7817 Authenticated A7817 Decryption A7817 Encryption A7818 Authenticated A7818 Decryption A7818 Encryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						A7819 Authenticated A7819 Decryption A7819 Encryption
KPK	A 256-bit AES GCM key used to encrypt and decrypt keys entered over SSI port.	256 bits - 256 bits	Symmetric Key - CSP	KeyGen		KTS-GCM
PWD Hash	A 256-bit password hash	256 bits - 128 bits	Authentication - CSP	SHA2-256 (A8090)		
RSA FW-LD-Pub	A 2048-bit RSA key is used to validate the firmware image signature during the integrity check and loading process, ensuring only authenticated code is executed.	2048 bits - 112 bits	Asymmetric Public Key - PSP	Generated outside of the module		SigVer1
TEK	128,256 -bit AES key used for enabling secure communication in target devices.	128 bits or 256 bits - 128 bits or 256 bits	Symmetric Key - CSP	KeyGen		A7817 Authenticated A7817 Decryption A7817 Encryption A7818 Authenticated A7818 Decryption A7818 Encryption A7819

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Authenticated A7819 Decryption A7819 Encryption
User PWD (AM)	A 30-byte long hexadecimal number to authenticate the User role	N/A - N/A	Authentication - CSP	N/A		Common-SHA2

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES-GCM IV		System Memory (S1):Plaintext	When module is reset	Z1	
BKK		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1	TEK:Encrypts, Wraps KEK:Encrypts, Wraps
CO PWD (AM)	Input encrypted on the IEK (I1)	System Memory (S1):Plaintext	When module is reset	Z1 Z2 Z3 Z4 Z5 Z8	IEK:Unwraps PWD Hash:Hash of password
DRBG Internal State - Key		System Memory (S1):Plaintext	When module is reset	Z1	DRBG-EI/Seed:Derived From DRBG-nonce:Derived From DRBG Internal State - V:Paired With
DRBG Internal State - V		System Memory (S1):Plaintext	When module is reset	Z1	DRBG-EI/Seed:Derived From DRBG-nonce:Derived From DRBG Internal

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					State - Key:Paired With
DRBG-EI/Seed		System Memory (S1):Plaintext	When module is reset	Z1	DRBG-nonce:Paired With DRBG Internal State - Key:Derives DRBG Internal State - V:Derives
DRBG-nonce		System Memory (S1):Plaintext	When module is reset	Z1	DRBG-EI/Seed:Paired With DRBG Internal State - Key:Derives DRBG Internal State - V:Derives
ECC FW-LD-Pub		System Memory (S1):Plaintext	When module is reset	Z1	
IEK	Input encrypted on the IEK (I1)	System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2 Z8	TEK: Unwraps KEK:Unwraps CO PWD (AM):Unwraps User PWD (AM):Unwraps IEK:Unwraps
KEK	Input encrypted on the IEK (I1) Input encrypted on KPK (I2) Input in plaintext (I3) Output encrypted on BKK (O1) Output encrypted on BKK (O2) Output encrypted on KPK (O3) Output in plaintext (O4)	System Memory (S1):Plaintext	When module is reset	Z1 Z2 Z8	KPK:Wrapped by , Unwrapped by BKK:Wrapped by IEK:Wrapped by, Unwrapped by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KPK		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2 Z8	KEK:Wraps and Unwraps TEK:Wraps and Unwraps
PWD Hash		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8	CO PWD (AM):Hash Of User PWD (AM):Hash Of
RSA FW-LD-Pub		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1	
TEK	Input encrypted on the IEK (I1) Input encrypted on KPK (I2) Input in plaintext (I3) Output encrypted on BKK (O1) Output encrypted on BKK (O2) Output encrypted on KPK (O3) Output in plaintext (O4)	System Memory (S1):Plaintext	When module is reset	Z1 Z2 Z8	KPK:Wrapped by and Unwrapped by BKK:Wrapped by and Unwrapped by IEK:Wrapped and Unwrapped by
User PWD (AM)	Input encrypted on the IEK (I1)	System Memory (S1):Plaintext	When module is reset	Z1 Z2 Z3 Z6 Z7 Z8	IEK:Unwraps PWD Hash:Hash of password

Table 21: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure proper operation. Per FIPS 140-3, these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self-tests can be initiated on demand by power cycling the Module.

The Module performs the pre-operational self-tests listed in the table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	RSA-2048 (Cert. #A5253),SHA2-256 (Cert. #SHS817)	KAT	SW/FW Integrity	Success or ES2 on failure	A digital signature is generated over the Boot Block, Base firmware, and all Drop-In Algorithms when it is built using RSA-2048 (Cert. #A5253) SHA2-256 (Cert. #SHS817), and is stored with the code upon download into the Module.

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-128 AES-CBC Decrypt	AES-128	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-128 AES-CBC Encrypt	AES-128	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-128 AES-CTR Decrypt	AES-128	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-128 AES-	AES-128	KAT	CAST	Success or	Encrypt	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
CTR Encrypt				ES1 on failure		
AES-128 AES-ECB Decrypt	AES-128	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-128 AES-ECB Encrypt	AES-128	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-128 AES-GCM Decrypt	AES-128	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-128 AES-GCM Encrypt	AES-128	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-128 AES-OFB Decrypt	AES-128	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-128 AES-OFB Encrypt	AES-128	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-256 AES-CBC Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-256 AES-CBC Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-256 AES-CTR Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-256 AES-CTR Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-256 AES-ECB Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-256 AES-ECB Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-256 AES-GCM Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-256 AES-GCM Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-256 AES-OFB Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-256 AES-OFB Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES-Key Unwrap	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES-Key Wrap	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES256-Internal AES-CBC Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-CBC Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES256-Internal AES-CFB8 Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
CFB8 Encrypt						
AES256-Internal AES-ECB Decrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-ECB Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
AES256-Internal AES-GCM Decryption	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-GCM Encrypt	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-OFB Decryption	AES-256	KAT	CAST	Success or ES1 on failure	Decrypt	Bootup
AES256-Internal AES-OFB Encryption	AES-256	KAT	CAST	Success or ES1 on failure	Encrypt	Bootup
Counter DRBG (A8088)	AES-256 CTR	KAT	CAST	Success or ES1 on failure	SP 800-90Arev1 Instantiate/Generate/Re seed Known Answer Tests	Bootup
ECDSA SigVer (FIPS186-5)	ECDSA P-384 SigVer	KAT	CAST	Success or ES1 on failure	Verify	Bootup
Entropy E132 - Start-up	Start-up RCT and APT	Fault Detection	Critical Function	Success or ES3 on failure	An RCT and APT as specified in [90B] section 4.4 are executed	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RCT and APT					before generation of the DRBG entropy input	
Firmware Load	ECDSA P-384 SigVer/SHA2-384	KAT	SW/FW Load	Success or ES2 on failure	Verify the image by ECDSA P-384 upon download into the module.	loading a new firmware image
RSA SigVer (FIPS186-5)	RSA-2048 SigVer	KAT	CAST	Success or ES2 on failure	Verify	Bootup
SHA2-256 (A8090)	SHA2-256	KAT	CAST	Success or ES1 on failure	Hash	Bootup
SHA2-256 (SHS 817)	SHA2-256	KAT	CAST	Success or ES2 on failure	Hash	Bootup
SHA2-384 (A8090)	SHA2-384	KAT	CAST	Success or ES1 on failure	Hash	Bootup

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity	KAT	SW/FW Integrity	On demand	Manually

Table 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-128 AES-CBC Decrypt	KAT	CAST	On Demand	Manually
AES-128 AES-CBC Encrypt	KAT	CAST	On Demand	Manually
AES-128 AES-CTR Decrypt	KAT	CAST	On Demand	Manually
AES-128 AES-CTR Encrypt	KAT	CAST	On Demand	Manually
AES-128 AES-ECB Decrypt	KAT	CAST	On Demand	Manually
AES-128 AES-ECB Encrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-128 AES-GCM Decrypt	KAT	CAST	On Demand	Manually
AES-128 AES-GCM Encrypt	KAT	CAST	On Demand	Manually
AES-128 AES-OFB Decrypt	KAT	CAST	On Demand	Manually
AES-128 AES-OFB Encrypt	KAT	CAST	On Demand	Manually
AES-256 AES-CBC Decrypt	KAT	CAST	On Demand	Manually
AES-256 AES-CBC Encrypt	KAT	CAST	On Demand	Manually
AES-256 AES-CTR Decrypt	KAT	CAST	On Demand	Manually
AES-256 AES-CTR Encrypt	KAT	CAST	On Demand	Manually
AES-256 AES-ECB Decrypt	KAT	CAST	On Demand	Manually
AES-256 AES-ECB Encrypt	KAT	CAST	On Demand	Manually
AES-256 AES-GCM Decrypt	KAT	CAST	On Demand	Manually
AES-256 AES-GCM Encrypt	KAT	CAST	On Demand	Manually
AES-256 AES-OFB Decrypt	KAT	CAST	On Demand	Manually
AES-256 AES-OFB Encrypt	KAT	CAST	On Demand	Manually
AES-Key Unwrap	KAT	CAST	On Demand	Manually
AES-Key Wrap	KAT	CAST	On Demand	Manually
AES256-Internal AES-CBC Decrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-CBC Encrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-CFB8 Decrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-CFB8 Encrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-ECB Decrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-ECB Encrypt	KAT	CAST	On Demand	Manually
AES256-Internal AES-GCM Decryption	KAT	CAST	On Demand	Manually
AES256-Internal AES-GCM Encrypt	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES256-Internal AES-OFB Decryption	KAT	CAST	On Demand	Manually
AES256-Internal AES-OFB Encryption	KAT	CAST	On Demand	Manually
Counter DRBG (A8088)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5)	KAT	CAST	On Demand	Manually
Entropy E132 - Start-up RCT and APT	Fault Detection	Critical Function	On Demand	Manually
Firmware Load	KAT	SW/FW Load	N/A	N/A
RSA SigVer (FIPS186-5)	KAT	CAST	On Demand	Manually
SHA2-256 (A8090)	KAT	CAST	On Demand	Manually
SHA2-256 (SHS 817)	KAT	CAST	On Demand	Manually
SHA2-384 (A8090)	KAT	CAST	On Demand	Manually

Table 25: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The Module fails a KAT.	The Module enters the critical error state, stores the status in non-volatile memory, and halts all further operations by entering an infinite loop.	Reboot or power cycle the Module.	The Module will not respond to any requests.
ES2	The Module fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	Following a firmware signature validation failure, the Module ceases normal operations and transitions to flash programming mode.	Reboot or power cycle the module or re-flashing a new image.	The Module will not respond to any requests.
ES3	The Module fails to acquire Entropy.	The Module enters the Fatal Error state.	Automatic	The Module stores the status into the internal flash memory and resets to attempt recovery.

Table 26: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Module is delivered in a non-compliant state and must be initialized to enter the Approved Mode. The Module does not support a non-Approved mode of operation. During initialization the operator shall configure the Module from the instructions below:

1. Load only approved Drop-In-Algorithms listed in Table 3: Approved Drop-In Algorithms
2. Set up the passwords for both the Crypto Officer (CO) and User roles. The Module is not initialized until the passwords for both the CO and User are set.
3. Use Configuration KVL Service, set to FIPS mode to “Level 2 (Standard)” or Legacy Level 3 (High)”.

11.2 Administrator Guidance

Use the P25 KVL 7000 User Guide available on the <https://www.motorolasolutions.com/> website for secure operations.

11.3 Non-Administrator Guidance

Use the P25 KVL 7000 User Guide available on the <https://www.motorolasolutions.com/> website for secure operations.

11.4 End of Life

After the end-of-life, the operator should zeroize all SSPs using “Factory Reset” service followed by shredding the Motorola P25 KVL 7000 HSM.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

Abbreviation	Full Specification Name
[FIPS140-3]	<i>Security Requirements for Cryptographic Modules</i> , March 22, 2019
[ISO19790]	<i>International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017</i>
[ISO24759]	<i>International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015</i>
[IG]	<i>Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program</i> , September 2, 2025.
[131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019</i>
[133]	<i>NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020</i>
[186]	<i>National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 3, 2023.</i>
[197]	<i>National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001</i>
[180]	<i>National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015</i>
[38A]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001</i>
[38D]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007</i>
[38F]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012</i>
[90A]	<i>National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.</i>
[90B]	<i>National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.</i>

Table 27: References

Acronym	Definition
AES	Advanced Encryption Standard
BKK	Black Keyloading Key
CAST	Cryptographic Algorithm Self-Tests
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CO	Crypto-Officer
CO PWD	Crypto-Officer Password
CSP	Critical Security Parameters
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DRBG-EI	DRBG Entropy Input
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature
FIPS	Federal Information Processing Standards
FW	Firmware
FW-LD-Pub	Firmware Load Public Key
GCM	Galois/Counter Mode
HSM	Hardware Security Module
IEK	Interface Encryption Key
IV	Initialization Vector
KAT	Known Answer Test
KEK	Key Encryption Key
KPK	Key Protection Key
KYLD	Keyload
KMF	Key Management Facility
KVL	Key Variable Loader
MACE	Motorola Advanced Crypto Engine
OFB	Output Feedback
PWD Hash	Password Hash
SSI	Synchronous Serial Interface
SSP	Sensitive Security Parameter

Acronym	Definition
TEK	Traffic Encryption Key
UA	Unauthenticated Service
PWD	Password

Table 28: Acronyms and Definitions