Key Variable Loader (KVL) 5000 PIKE

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.2

Date: November 14, 2024

Table of Contents

List of Tables

List of Figures

1 General

This document defines the Security Policy for the Key Variable Loader (KVL) 5000 PIKE module by Motorola Solutions, Inc., hereafter denoted the Module. The KVL 5000 is a portable key distribution device that consists of the KVL Host Application processor and KVL 5000 PIKE Hardware Security Module (HSM). The PIKE IC is integrated into the HSM. The Module is a single-chip cryptographic module to meet FIPS 140-3 Level 2 physical security requirements as defined by FIPS 140-3. The Module allows the user to generate, transport, and load encryption keys, securely and efficiently into secure communication products thereby enabling secure encrypted communications

The FIPS 140-3 security levels for the Module are as follows:

Table 1 – Security Levels

ISO/IEC 24759 Section 6 [Number below]	FIPS 140-3 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	2
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		**2**

2 Cryptographic Module Specification

The PIKE cryptographic module is a single chip hardware cryptographic module. The Motorola Solutions Inc. module is used in the KVL 5000 Key Variable Loader product. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall Security Level 2.

2.1 Operational Environment

The Module is tested on the following operational environment.

Table 2 – Cryptographic Module Tested Configuration

Model	HW P/N, Version	Base Firmware version	Distinguishing Features
Key Variable Loader (KVL) 5000 PIKE	51009397004 (Model Number: T8476B).	R50.07.10	Single chip embodiment

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.

Table 3 – Approved Mode Drop-in Algorithms

Algorithm	Algorithm Firmware Version	Base Firmware Version	Cert. #
AES128	R01.00.01	R50.07.10	C909
AES256	R01.00.01	R50.07.10	C908

2.2 Cryptographic Boundary

The KVL 5000 Key Variable Loader (KVL) production diagram is shown in Figure 1. The Motorola PIKE chip is shown in Figure 2 provides the data security services required by the KVL 5000 Key Variable Loader.

Figure 1: KVL 5000 Key Variable Loader (KVL)

Figure 2: Motorola PIKE Chip

The FIPS Boundary is drawn around Motorola PIKE chip, as shown in Figure 3.

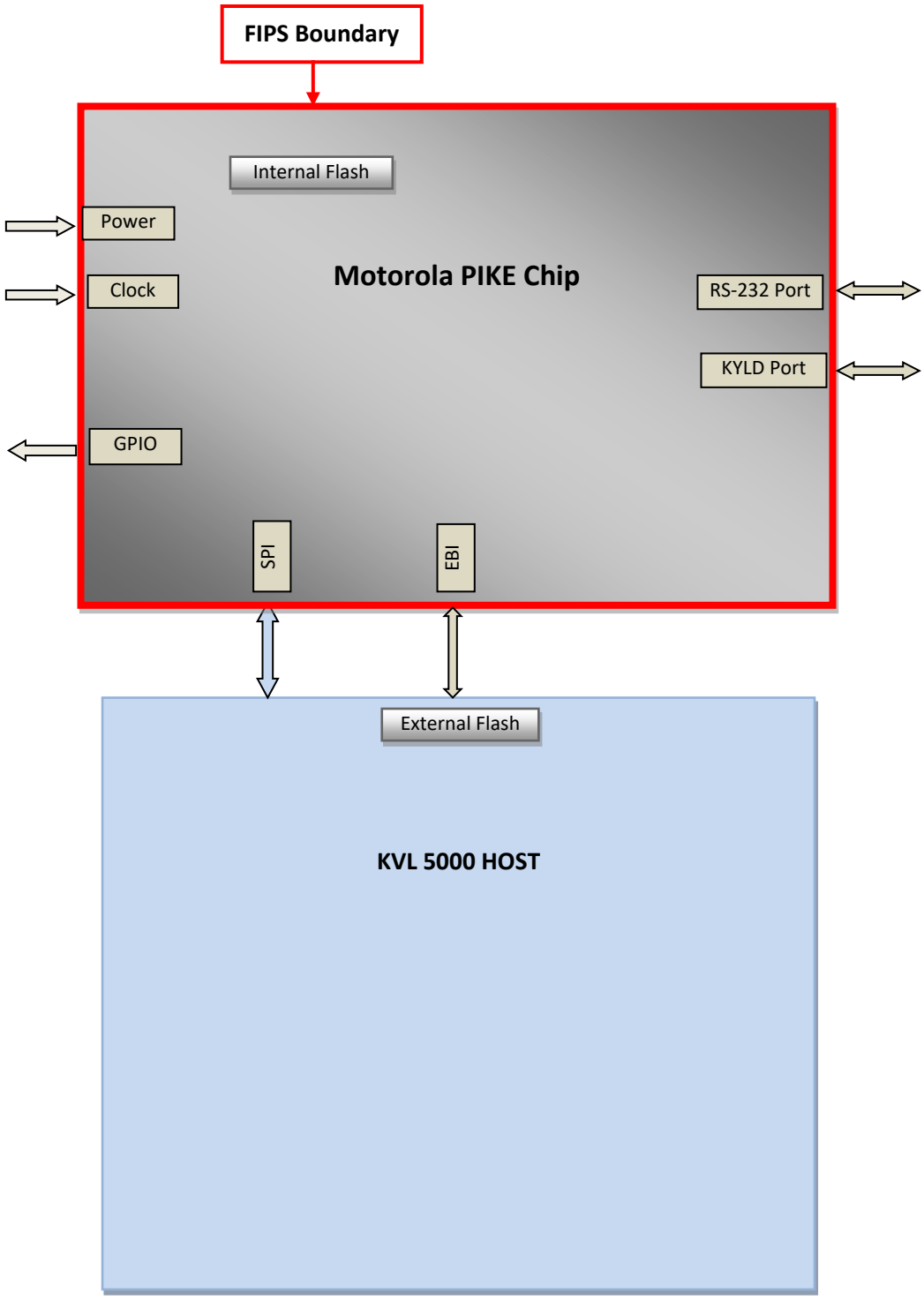

Figure 3: Cryptographic Boundary

2.3 Modes of Operation

The KVL 5000 Key Variable Loader (KVL) module is originally non-compliant and must be configured to operate in an approved mode of operation. The Crypto Officer shall configure the Module to operate in an approved mode of operation. In order for the Module to operate in the approved mode, the Module must be properly installed, initialized and configured, which includes the creation of the passwords for the Crypto Officer (CO) and User role. Documented below in Section 2.3.1 are the additional configuration settings that are required for the Module to be used in a FIPS 140-3 approved mode of operation at overall Security Level 2.

The settings menu of the KVL Host application graphical user interface in the settings menu will be used to determine whether the KVL 5000 is operating in an approved mode. When operating in an approved mode the display will indicate.

- "FIPS mode: Level 2 (Standard)"
- "FIPS Status: Compliant"

Use *Version and Algorithm List Query* service to verify that the firmware version matches an approved version listed on NIST's website: http://csrc.nist.gov/groups/STM/cmvp/validation.html

2.3.1 Configuration of the Approved Mode of Operation

In order to configure the Module for an Approved mode at overall Security Level 2, the operator shall use the Configure KVL service to set the following configuration parameters as shown below.

1. Either Clear Key Export or Encrypted Key Export: Enabled
2. For an incorrect login attempt, the CO must configure the module 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 default setting is to lockout the CO/User for 15 minutes after three (3) unsuccessful login attempts.

Only Approved algorithms may be loaded into the Module; in particular AES-128 Cert. #C908) and/or AES-256 (Cert. #C909). At a minimum, one of these "drop-in algorithms" must be added from the Module independent of the base firmware via the *Program Update* service. In addition to the approved algorithms, external entropy must also be supplied to the Module from the host application upon successful authentication of the operator of the Module.

The loading of non-validated firmware within the validated cryptographic module invalidates the module's validation.

2.4 Security Functions

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C908	AES [197]	ECB [38A]	Key Size: 256	Encrypt, Decrypt
		CBC [38A]	Key Size: 256	Encrypt, Decrypt
		OFB [38A]	Key Size: 256	Encrypt, Decrypt
C909	AES [197]	ECB [38A]	Key Size: 128	Encrypt, Decrypt
		CBC [38A]	Key Size: 128	Encrypt, Decrypt
		OFB [38A]	Key Size: 128	Encrypt, Decrypt
C930	AES [197]	KW [38F]	Forward Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt
C931	AES [197]	CFB8 [38A]	Key Size: 256	Encrypt, Decrypt
		OFB [38A]	Key Size: 256	Encrypt, Decrypt
		ECB [38A]	Key Size: 256	Encrypt, Decrypt
		CBC [38A]	Key Size: 256	Encrypt, Decrypt
		GCM [38D][1]	Key Size: 256	Encrypt, Decrypt
VA	CKG [IG D.H]	[133rev2] Section 4 and Section 6.1 (example 1) - Direct symmetric key generation using unmodified DRBG output		Key Generation
		[133rev2] Section 6.3 (#2) Symmetric Keys Produced by Combining (Multiple) Keys and Other Data		
C949	DRBG [90A]	CTR	AES-256	Deterministic Random Bit Generation[2]
ECDSA 183	ECDSA [186]		P-384 SHA (384)	SigVer
C930	KTS [38F]	KW	Key Sizes: 128, 256	Key establishment methodology provides 128 or 256 bits of encryption strength Restricted to only wrap keys with an equal strength to the wrapping

[1] 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. #C949).

[2] The entropy for seeding the SP 800-90A DRBG is determined by the host application using the Module and is outside of the module's physical boundary. The operator shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by using *Load Entropy* service listed in section 4.3. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

Cert	Algorithm	Mode	Description	Functions/Caveats
				mechanism (i.e., 128-bit keys cannot wrap 256-bit keys)
C931	KTS [IG D.G]	GCM	Key Size: 256	Key establishment methodology provides 256 bits of encryption strength
SHS 1345	SHS [180]	SHA2-256 SHA2-384		Message Digest Generation, Password Obfuscation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
KTS (AES Key Unwrap)	[IG D.G] AES (Cert. #C931) key unwrapping for use in key transport; Key establishment methodology provides 256 bits of encryption strength.

Table 6 – Non-Approved but Allowed Cryptographic Functions with No Security Claimed

Algorithm	Description
AES MAC	[IG 2.4.A] P25 AES OTAR. No Security Claimed. AES MAC is used as part of OTAR but is considered obfuscation. KTS encryption is performed on the OTAR key components using AES KW Cert. #C930.

The module does not implement any Non-Approved Algorithms not allowed in the Approved Mode of Operation.

2.5 Overall Security Design

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle or logout
4. The Module does not provide any cryptographic services while in critical error state.
5. An operator does not have access to any cryptographic services prior to assuming an authorized role.
6. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
7. Power up self-tests do not require any operator action.
8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. The Module does not support a maintenance interface or role.
11. The Module does not support manual SSP establishment method.

12. The Module does not have any proprietary external input/output devices used for entry/output of data.
13. The Module does not output intermediate key values.
14. The Module does not provide bypass services or ports/interfaces.
15. The Module does not support a bypass capability.
16. The Module does not support concurrent operators.

2.6 Rules of Operation

The Module shall be installed in the Motorola KVL 5000 Key Variable Loader product. Prior to the initial use of the Module, the operator is required to set the passwords for the Crypto Officer (CO) and User roles. The Module is not usable until the passwords for both the CO and User are set.

The Module shall be operated such that only approved Drop-in algorithms listed in Table 3 are installed and configured as per Section 2.3.1.

3 Cryptographic Module Interfaces

The Module's ports and associated logical interface categories are listed in Table 7.

Table 7 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
Power	Power Input	This interface powers all circuitries. This interface does not support input/output of SSP.
EBI	Data Input Data Output	This is the interface to the external flash memory. Password hash and system parameters are stored in the external flash.
KYLD (Keyload) Interface	Data Input Data Output Control Input	This is the interface to external devices. All SSP exchanged over this interface are either encrypted or plaintext when operating in approved mode.
RS-232 Interface	Data Input Data Output Status Output	Provides an interface for factory programming, execution of RS-232 shell commands, and error logs.
SPI	Data Input Data Output Control Input Status Output	This is the interface to the KVL 5000 Host Application. All SSP exchanged over this interface are always encrypted.
GPIO	Status Output Control Input	This is the interface to control the LED of the KVL 5000. The output turns flashing amber during self-tests and momentary solid green after self-tests are completed successfully. The LED output turns solid red upon entering a critical error state. This interface is also used to configure SPI interface.

Physical Port	Logical Interface	Data that passes over port/interface
Clock	Control Input	Clock input.

NOTE: The module does not have Control Output.

4 Roles, Services and Authentication

4.1 Assumption of Roles and Related Services

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). Table 8 lists all operator roles supported by the Module and their related services. In addition, the Module supports services which do not require to be authenticated, listed as UA in Table 8.

Table 8 – Roles, Service Commands, Input and Output

Role			Service	Input	Output
CO	User	UA			
X	–	–	Program Update	Firmware image	The Module is upgraded to new firmware.
X	–	–	Configure KVL	Configuration parameters	The Module is configured as requested. Success/Failure status.
X	–	–	Change CO Password	Password	Updated the CO password. Success/failure status.
X	–	–	Logout CO	Command In	Logout CO role.
X	X	–	Load Entropy	DRBG seed	The DRBG is seeded and initialized. The Module is ready to provide services. Success/failure status.
X	X	–	Change User Password	Password	Updated the user password. Success/failure status.
–	X	–	Logout User	Command In	Logout the User role.
X	X	–	Version and Algorithm List Query	Command In	Provides module firmware version and list of algorithms.
X	X	–	Transfer Key Variable	Command In	Transfer keys to the target devices. Success/failure status.
X	X	–	Receive Key Variable	TEKs and KEKs	Receive keys. Success/failure status.
X	X	–	Generate Key Variable	Command In	Auto-generate keys using DRBG. Success/failure status.
X	X	–	Key Check	Command In	Validate the correctness of a key based on algorithm properties. Success/failure status.
X	X	–	Zeroize Keys	Command In	Zeroize keys in the Module and target devices over the KYLD interface. Success/failure status.
X	X	–	Encrypt	Plaintext	Ciphertext. Success/failure status.
X	X	–	Decrypt	Ciphertext	Plaintext. Success/failure status.
X	X	–	Store and Forward (SAF)	TEKs and KEKs	Receive (store) keys from the KMF into the module, then transfer (forward) to the target. Success/failure status.

Role			Service	Input	Output
CO	User	UA			
X	X	–	Key Sharing	TEKs and KEKs	Combination of receive and transfer key variable services. Transport keys between two KVLs. Success/failure status.
X	X	X	Factory Reset	Command In	Reset the databases and module parameters to system defaults. Success/failure status.
X	X	–	Module Info	Command In	Provides current Module Id, FW version, and FIPS status.
–	–	X	Validate CO Password	Password	Successful authentication will allow access to the services allowed for CO role.
–	–	X	Validate User Password	Password	Successful authentication will allow access to the services allowed for User role.
–	–	X	Diagnostics	Command In	Success/failure status.
–	–	X	Perform Self-Tests	Command In	Success/Reset.

4.2 Authentication Methods

The Module supports two distinct operator roles (User and Crypto-Officer). The Module uses 30-byte long hexadecimal number to authenticate the User and CO roles. The Module enforces the separation of roles using login credentials and re-authentication is enforced when changing roles.

The module ensures that there is no visible display of the authentication data.

Table 9 – Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	Identity-based. 30-byte long hexadecimal number.	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}.
User		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-minute period is 20 in 95^{15}

4.3 Services

All services implemented by the Module are listed in Table 10. The Module does not allow any non-approved service while operating in FIPS 140-3 level 2 mode.

The SSPs modes of access shown in Table 10 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.
- **E** = Execute: The Module uses the SSP in performing a cryptographic operation.
- **Z** = Zeroize: The Module zeroizes the SSP.

Table 10 – Approved Services

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Program Update	Update the Module firmware.	ECDSA Cert. #ECDSA 183, SHS Cert. #SHS 1345	IDK	CO	Z	Approved Mode
			IDK-ROM		E	
			IDK-Block		EZ	
			FCK		Z	
			BKK		Z	
			KPK		Z	
			KEK		Z	
			TEK		Z	
			KPKEK		Z	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
			FW-LD-Pub		Z	
Configure KVL	Set configuration parameters used in Store and Forward protocols and other module-specific parameters over the SPI or RS-232 interfaces.	N/A	KPK	CO	Z	Approved Mode
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
Change CO Password	Change the current password for CO role.	AES Key Unwrap, AES Cert. #C931,	FCK	CO	E	Approved Mode
			KPK		Z	
			CO PWD		Z	

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		SHS Cert. #SHS 1345	User PWD		Z	
			PWD Hash		Z	
Logout CO	Logs out CO role.	N/A	N/A	CO	N/A	Approved Mode
Load Entropy	Load entropy into the Module.	AES Key Unwrap, AES Cert. #C931, DRBG Cert. #C949	DRBG-EI/Seed	CO, User	WE	Approved Mode
			DRBG-State		G	
			FCK		E	
			KPK		G	
Change User Password	Change the current password for User role.	AES Key Unwrap, AES Cert. #C931, SHS Cert. #SHS 1345	FCK	CO, User	E	Approved Mode
			KPK		Z	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
Logout User	Logout User role.	N/A	N/A	User	N/A	Approved Mode
Version and Algorithm List Query	Query module firmware version number and list of algorithms over the SPI interface.	N/A	N/A	CO, User	N/A	Approved Mode
Transfer Key Variable	Transfer KEKs and TEKs to the target devices over the KYLD and SPI interfaces.	AES Key Unwrap, AES Cert. #C931, AES GCM Cert. #C931	FCK	CO, User	E	Approved Mode
			BKK		E	
			KPK		E	
			KEK		R	
			TEK		R	
Receive Key Variable	Receive KEKs, TEKs over the KYLD and SPI interfaces.	AES Key Unwrap, AES Cert. #C931, AES GCM Cert. #C931	FCK	CO, User	E	Approved Mode
			KPK		E	
			KEK		W	
			TEK		W	
Generate Key Variable	Auto-generate	DRBG Cert. #C949	KEK	CO, User	G	Approved Mode
			TEK		G	

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
	KEKs and TEKs.		DRBG-State		EG	
Key Check	Validate the correctness of a key based on algorithm properties.	N/A	N/A	CO, User	N/A	Approved Mode
Zeroize Keys	Zeroize KEKs and TEKs in the KVL and target devices over the KYLD interface.	N/A	KEK	CO, User	Z	Approved Mode
			TEK		Z	
Encrypt	Encrypt plaintext data to be transferred over the SPI, KYLD, and EBI interfaces.	AES Cert. #C908, AES Cert. #C909, AES Cert. #C931, CKG (VA)	FCK	CO, User	E	Approved Mode
			BKK		E	
			KPKEK		E	
			KPK		E	
			KEK		E	
			TEK		E	
			DRBG-State		E	
Decrypt	Decrypt ciphertext received over the SPI, KYLD, and EBI interfaces.	AES Cert. #C908, AES Cert. #C909, AES Cert. #C931, CKG (VA)	IDK	CO, User	E	Approved Mode
			FCK		E	
			BKK		E	
			KPKEK		E	
			KPK		E	
			KEK		E	
			TEK		E	
			DRBG-State		E	
Store and Forward (SAF)	Receive KEKs and TEKs from the KMF into the module, and	AES Key Unwrap, AES Certs. #C930, #C931,	FCK	CO, User	E	Approved Mode
			BKK		E	
			KPK		E	
			KEK		E	

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
	then transfer those keys (forward) to the target device attached to the KVL.	AES GCM Cert. #C931	TEK		E	
Key Sharing	Combination of receive and transfer KEKs and TEKs between two KVLs.	N/A	KEK	CO, User	RW	Approved Mode
			TEK		RW	
Factory Reset	Reset the databases and module parameters to system defaults via a command over the SPI interface or a manual reset button.	N/A	KPK	CO, User, UA	Z	Approved Mode
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
Module Info	Show Module ID, FW version, and FIPS status.	N/A	N/A	CO, User	N/A	Approved Mode
Validate CO Password	Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the SPI interface.	AES Key Unwrap, AES Cert. #C931, SHS Cert. #SHS 1345	FCK	UA	E	Approved Mode
			KPK		GEZ	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
Validate User Password	Validate the current User password used to identify and	AES Key Unwrap, AES Cert. #C931, SHS Cert. #SHS 1345	FCK	UA	E	Approved Mode
			KPK		GEZ	
			CO PWD		Z	
			User PWD		Z	

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
	authenticate the User role via the SPI interface.		PWD Hash		Z	
Diagnostics	Read logs, run LED test, test external flash erase and write, and other non-security relevant status information over the RS-232 interface.	N/A	N/A	UA	N/A	Approved Mode
Perform Self-Tests	Perform module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by a transition from power off state to power on state.	N/A	N/A	UA	N/A	Approved Mode

5 Firmware Security

The Module is composed of a base firmware version identified in Table 2, and at least one of the drop-in algorithms listed in Table 3.

The firmware components are protected with the authentication technique(s) Firmware Load Public Programmed Signature Key described in Table 16

The Module includes a firmware verification and load service to support necessary updates using ECDSA SigVer (ECDSA Cert. #ECDSA 183).

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

6 Operational Environment

The Module has a limited operational environment under the FIPS 140-3 definitions. The tested operational environment is listed in Table 2. The Module includes a Program Update service to support necessary updates. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Physical Security

The Module is a production grade, single-chip cryptographic module as defined by FIPS 140-3 and is designed to meet level 2 physical security requirements.

The Module is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the Module. The security provided from the hardness of the Module's epoxy encapsulate is claimed at ambient temperature (25 degrees Celsius) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The Module does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the Module while delivering to operators.

Table 11 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the chip.	Periodically	Look for signs of tampering. Remove from service if tampering found.

8 Non-Invasive Security

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

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in Table 12 below:

Table 12 – SSP Management Methods

Method	Description
G1	Generated external to the Module and installed during manufacturing.
G2	Derived from the DRBG input per SP800-90Ar1.
G3	Symmetric key generated by internal CAVP validated DRBG.
G4	Hash data generated by internal CAVP validated hash function
G5	Generated per SP800-133r2 (Section 6.3 #2) via XOR of 2 other keys (IDK ROM and IDK Block)
S1	Stored in the volatile memory (RAM) in plaintext while in use.
S2	Stored in the internal flash in plaintext, associated by memory location (pointer).
S3	Stored in the internal flash encrypted, associated by memory location (pointer).
E1	Electronically input AES-256 CBC encrypted by the IDK-Block and ROM using AES KTS (Cert. #C931).
E2	Electronically input/output AES-256 OFB encrypted by the FCK using AES KTS (Cert. #C931).
E3	Electronically output AES-256 OFB encrypted by the BKK using AES KTS (Cert. #C931).
E4	Electronically input/output using AES-KW key transport by the KPK using AES KTS (Cert. #C930).
E5	Electronically input or output in plaintext.
E6	Electronically input/output using AES-GCM key transport by the KPK using AES (Cert. #C931).
Z1	Zeroized by the “Program Update” service by overwriting with a fixed pattern of “1s” in internal flash.
Z2	Zeroized by module power cycle or hard reset by overwriting RAM with a fixed pattern of “0s” in RAM.
Z3	Zeroized by the “Configure KVL” service by overwriting with a fixed pattern of “0s” in RAM.
Z4	Zeroized by the “Change CO Password” service by overwriting with a fixed pattern of “0s” in RAM.
Z5	Zeroized by the “Validate CO Password” service by overwriting with a fixed pattern of “0s” in RAM.
Z6	Zeroized by the “Change User Password” service by overwriting with a fixed pattern of “0s” in RAM.
Z7	Zeroized by the “Validate User Password” service by overwriting with a fixed pattern of “0s” in RAM.
Z8	Zeroized by the “Factory Reset” service by overwriting with a fixed pattern of “1s” in in internal flash.

NOTE: Zeroization is implicit and is considered complete either after boot sequence is complete or when User/CO initiates zeroization via Zeroize Key service and the module provides success/fail status.

9.1 Sensitive Security Parameters (SSPs)

All SSPs (CSPs and PSPs) used by the Module are described in this section. All usage of the CSPs by the Module is described in the services detailed in 4.3.

Table 13 – CSPs Management

Key/SSP Name/Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
CSPs								
DRBG-EI/Seed	N/A	N/A	N/A	E2 (Input only)		S1	Z2	Externally generated, a minimum of 48 bytes are passively entered into the Module.
DRBG-State	256	DRBG #C949 AES ECB Cert. # C931	G2	N/A	N/A	S1	Z2	CTR_DRBG internal state: V (128 bits) and Key (AES 256) per IG D.L
BKK	256	AES OFB Cert. #C931, ECDSA Cert. #ECDSA 183	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES OFB key used for encrypting keys exported over KYLD port.
FCK	256	AES OFB Cert. #C931, ECDSA Cert. #ECDSA 183	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES OFB key used for decrypting CSP entered into the module over the SPI port.
IDK ROM	256	AES CBC Cert. # C931	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK Block.
IDK Block	256	AES CBC Cert. #C931, ECDSA Cert. #ECDSA 183	G1	E1	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK ROM.
IDK	256	AES CBC Cert. #C931	G5	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used to decrypt downloaded images.

Key/SSP Name/Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
KPKEK	256	AES GCM Cert. #C931, ECDSA Cert. #ECDSA 183	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES GCM key used to encrypt the KPK.
KPK	256	AES GCM Cert. #C931, DRBG #C949	G3	N/A	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8	A 256-bit AES GCM key used to encrypt all TEK and KEK stored in the external flash.
KEK	128/256	AES-KW Cert. #C930, AES OFB, CFB8 Cert. #C931, DRBG #C949	G3	E2, E3, E4, E6	N/A	S1	Z2	A 128/256-bit AES key used for encryption of keys in the Store and Forward, and Transfer Key Variable services.
TEK	128/256	AES ECB, CBC, OFB, GCM Cert. #C931, AES ECB, CBC, CFB8, OFB Certs. #C908, C909, DRBG Cert. #C949	G3	E2, E3, E4, E6	N/A	S1	Z2	A 128/256-bit AES Key used for enabling secure communication in target devices.
CO PWD	N/A	AES OFB Cert. #C931	N/A	E2 (Input only)	N/A	S1	Z2, Z3, Z4, Z5, Z6, Z7, Z8	A 30-byte long hexadecimal number to authenticate the CO role
User PWD	N/A	AES OFB Cert. #C931	N/A	E2 (Input only)	N/A	S1	Z2, Z3, Z4, Z5, Z6, Z7, Z8	A 30-byte long hexadecimal number to authenticate the User role
PWD Hash	192	SHS Cert. #SHS 1345 SHA2-384	G4	E5	N/A	S1	Z2, Z3, Z4, Z5, Z6, Z7, Z8	384-bit password hash.
PSPs								
FW-LD-Pub	192	AES CBC Cert. #C931,	G1	N/A	N/A	S1, S2	Z1, Z2	FW Load: 384-bit ECDSA signature

Key/SSP Name/Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
		ECDSA Cert. #ECDSA 183						key to validate the signature of the firmware image upon download into the Module.

Table 14 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
External	384 bits of entropy	The entropy for seeding the SP 800-90A DRBG is determined by the host application using the Module and is outside of the module's physical boundary. The operator shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by using Load Entropy service listed in section 4.3. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

10 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3, these are categorized as either pre-operational self-tests or conditional self-tests. Power-up self–tests are available on demand by power cycling the Module.

All Cryptographic Algorithm Self-Tests (CAST) must be completed successfully prior to any other use of cryptographic functionality by the Module. The Module outputs a status indicator via the LED output interface to indicate all self-tests passed or when a critical error state is entered due to a failed self-test. LED status solid green means power-up self-tests passed, flashing amber means self-tests is in progress, solid red means the Module is in critical error state due to power-up self-tests failure or critical error condition.

The self-tests error states and status indicator are described in Table 15 below:

Table 15 – Error States and Indicators

Error state	Description	Indicator
ES1	The Module fails a KAT.	The Module enters the Critical Error state. In this state, the Module stores the status into the internal flash memory and then halts all further operation by entering an infinite loop. The operator may correct this state by power cycling the Module.
ES2	The Module fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	The Module enters the Firmware Signature Validation Failure state. In this state, the Module halts all further operations and erase entire flash. The operator may correct the issue by re-flashing a new image.

The Module performs the following pre-operational self-tests:

Table 16 – Pre-Operational Self-Test

Security Function	Method	Description	Error state
Firmware integrity	ECDSA (Cert. #ECDSA 183), SHA2-384 (Cert. #SHS 1345)	A digital signature is generated over the Boot Block, Base firmware, and all Drop-in algorithms code when it is built using SHA2-384 and ECDSA P-384 (Cert. #ECDSA 183) and is stored with the code upon download into the PIKE chip. When the Module is powered up, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.	ES2

The Module performs the following conditional self-tests:

Table 17 – Conditional Self-Tests[3]

Security Function	Method	Description	Error state
Firmware Load	ECDSA P-384 SigVer	A digital signature is generated over the code when it is built using SHA2-384 and ECDSA P-384. The digital signature is verified upon download into the Module.	ES2
ECDSA P-384 (Cert. #ECDSA 183)	KAT	ECDSA P-384 SigVer KAT.	ES2
SHS (Cert. #SHS 1345)	KAT	SHA2-384 KAT.	ES2
AES128 – ECB, CBC, and OFB (Cert. #C909)	KAT	AES-128 encryption KAT.	ES1
AES128 – ECB, CBC, and OFB (Cert. #C909)	KAT	AES-128 decryption KAT.	ES1
AES256 – ECB, CBC, and OFB (Cert. #C908)	KAT	AES-256 encryption KAT.	ES1
AES256 – ECB, CBC, and OFB (Cert. #C908)	KAT	AES-256 decryption KAT.	ES1
AES256 – CFB8, OFB, ECB, CBC, and GCM (Cert. #C931)	KAT	AES-256 encryption KAT.	ES1
AES256 – CFB8, OFB, ECB, CBC, and GCM (Cert. #C931)	KAT	AES-256 decryption KAT.	ES1
AES KW (Cert. #C930)	KAT	AES-128 and 256 key wrap KAT.	ES1
AES KW (Cert. #C930)	KAT	AES-128 and 256 key unwrap KAT.	ES1
DRBG (Cert. #C949)	KAT	AES-256 CTR_DRBG instantiation, generate, and reseed KATs performed before the first random data generation.	ES1

[3] All Conditional Self-Test KATs are executed during the module power-up sequence except the DRBG KAT which is performed during CO/User login.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation and Initialization

The Module is originally a non-compliant and must be initialized to be in approved mode. There is no non-approved mode. During initialization the operator shall configure the Key Variable Loader (KVL) 5000 PIKE from the instructions below:

1. Upon first access, the operator will use the default passwords (Crypto Officer and User) provided by Motorola in a separate communication.
2. The operator will then change the default passwords (Crypto Officer and User) based on the requirements in Section 2.3 - Modes of Operation
3. The operator will then configure the Module using the Configure KVL service as specified in the section 2.3.1.

11.1.2 Delivery

The Key Variable Loader (KVL) 5000 PIKE is embedded in Key Variable Loader (KVL). Motorola uses commercially available courier systems such as UPS, FedEx, and DHL with a tracking number and requires a signature at the end by an authorized client.

11.2 Administrator Guidance

Use the Key Variable Loader (KVL) 5000 user guide available on the www.motorolasolutions.com website for secure operations.

11.3 Non-Administrator Guidance

Use the Key Variable Loader (KVL) 5000 user guide available on the www.motorolasolutions.com website for secure operations.

11.4 Maintenance Requirements

The Key Variable Loader (KVL) 5000 PIKE does not require any special maintenance.

11.5 End of Life

After the end-of-life, the operator should zeroize all SSPs using the “Zeroize all keys and password“ service listed in the Section 4.3 followed by shredding the Key Variable Loader (KVL) 5000 PIKE chip.

12 Mitigation of Other Attacks

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

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, May 16, 2022.*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*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*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 19 – Acronyms and Definitions

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
DRBG	Deterministic Random Bit Generator
DRBG-EI	DRNG Entropy Input
EBI	External Bus Interface
ECB	Electronic Code Book
FCK	FIPS Cipher Key
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
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KEK	Key Encryption Key
KPK	Key Protection Key
KPKEK	KPK Encryption Key
KYLD	Keyload
KVL	Key Variable Loader
OFB	Output Feedback
OTAR	Over The Air Rekeying

Acronym	Definition
PWD Hash	Password Hash
SSI	Synchronous Serial Interface
SSP	Sensitive Security Parameter
TEK	Traffic Encryption Key
UA	Unauthenticated Service
User PWD	User Password