Non-Proprietary FIPS 140-2 Security Policy: Key Variable Loader (KVL) 5000 PIKE2

Document Version: 1.2

Date: November 30, 2020

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Motorola Solutions Key Variable Loader (KVL) 5000 PIKE2 module, also known as the KVL 5000 PIKE2 Hardware Security Module (HSM). The KVL 5000 is a portable key distribution device that consists of KVL Host Application processor and KVL 5000 PIKE2 Hardware Security Module (HSM). The Motorola KVL 5000 PIKE2 Hardware Security Module (HSM) is a single-chip cryptographic module to meet FIPS 140-2 Level 3 Physical Security requirements as defined by FIPS 140-2. The KVL 5000 allows programmers to generate, transport, and load encryption keys, securely and efficiently into secure communication products thereby enabling secure encrypted communications.

Table 1 – Cryptographic Module Configuration

Module	HW P/N and Version	Base FW Version
Key Variable Loader (KVL) 5000 PIKE2	51009397004	R50.05.01, R50.07.01

The KVL 5000 supports the following FIPS Approved algorithms which may be installed separately from The KVL 5000 firmware using the Program Update service. While the installation of AES may be done separately, for the purposes of this validation the KVL 5000 includes this firmware.

Table 2 – Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Base FW Version	Cert. #
AES128	R01.00.01	R50.05.01, R50.07.01	C909
AES256	R01.00.01	R50.05.01, R50.07.01	C908

Table 3 - Non-Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Base FW Version
ADP	R01.00.00 (0x52010000)	R50.05.01, R50.07.01
DES	R01.00.00 (0x52010000)	R50.05.01, R50.07.01
DES-OFB	R01.00.00 (0x52010000)	R50.05.01, R50.07.01
DES-XL	R01.00.00 (0x52010000)	R50.05.01, R50.07.01
DVI-XL	R01.00.00 (0x52010000)	R50.05.01, R50.07.01
DVP-XL	R01.00.00 (0x52010000)	R50.05.01, R50.07.01

The KVL 5000 is intended for use by the markets that require FIPS 140-2 validated overall security level 2.

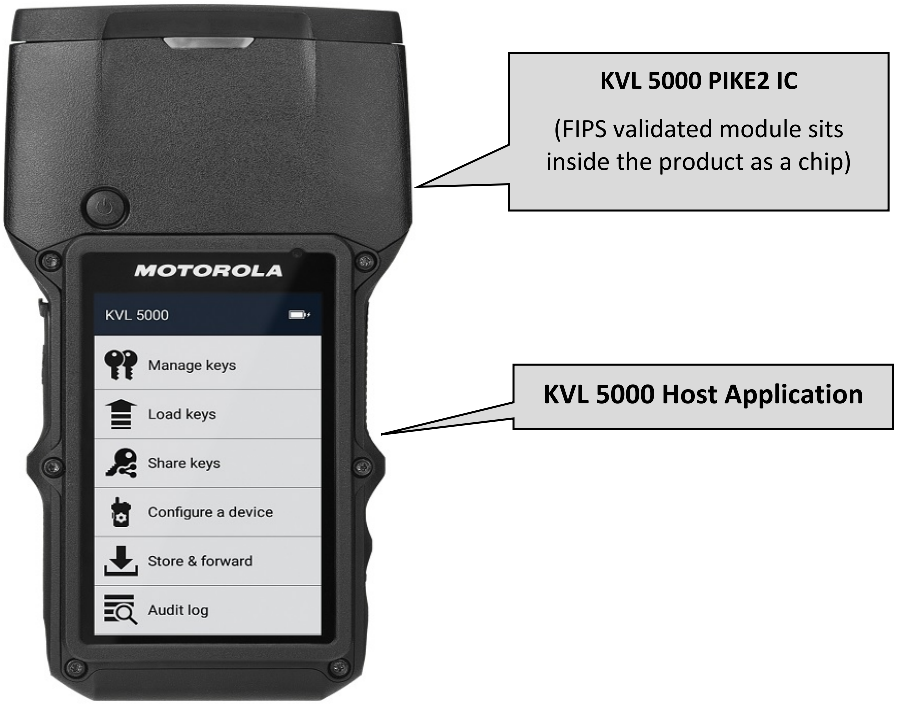
The FIPS 140-2 security levels for the KVL 5000 are as follows:

Table 4 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The KVL 5000 Key Variable Loader (KVL) production diagram is shown in the Figure 1 below. The KVL 5000 PIKE2 Hardware Security Module (HSM), shown in Figure 2, provides data security services required by the KVL 5000 Key Variable Loader.



KVL 5000 PIKE2 IC

(FIPS validated module sits inside the product as a chip)

KVL 5000 Host Application

Figure 1: KVL 5000 Key Variable Loader (KVL)

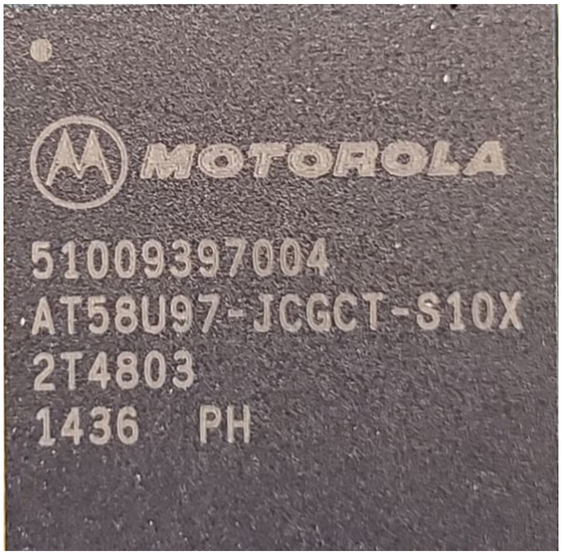


Figure 2: The KVL 5000 PIKE2 Hardware Security Module (HSM)

The Crypto Boundary is drawn around the KVL 5000 PIKE2 Hardware Security Module (HSM), as shown in Figure 3 below.

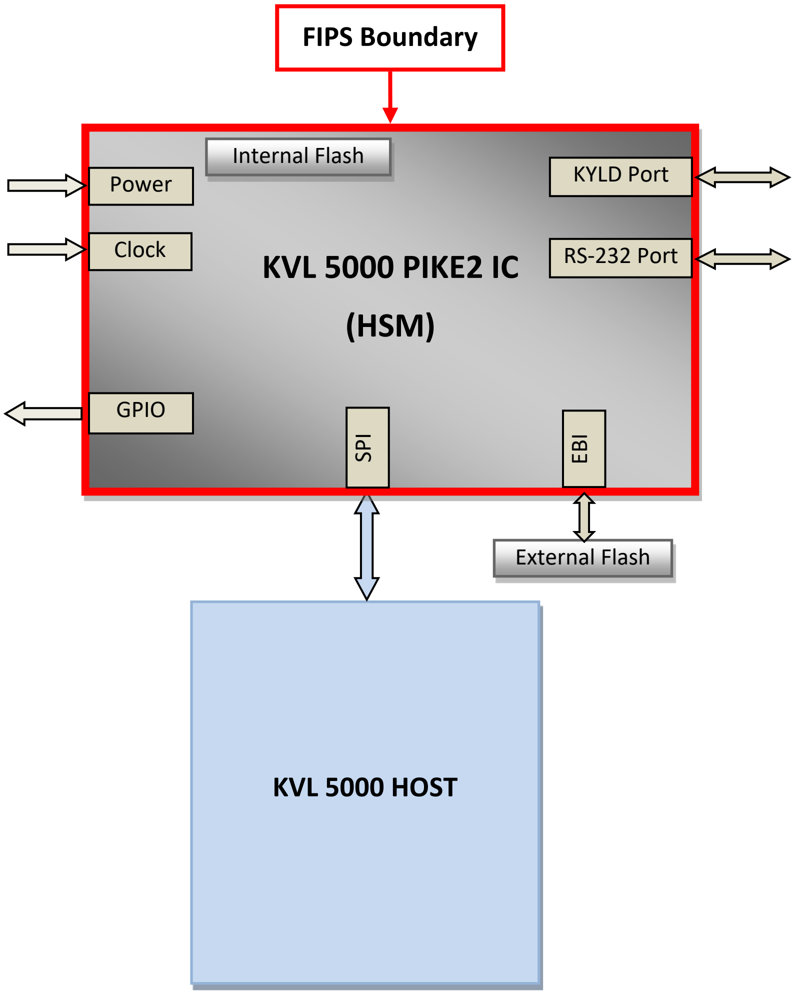


Figure 3: KVL 5000 PIKE2 HSM Cryptographic Boundary

The KVL 5000's ports and associated FIPS defined logical interface categories are listed in Table 5.

Table 5 – Ports and Interfaces

Port	Description	Logical Interface Type
Power	This interface powers all circuitry. This interface does not support input/output of CSP's.	Power Input
EBI	This is the interface to the external flash memory on the KVL 5000. Password hash and system parameters are stored in the external flash memory.	Data Input Data Output

Port	Description	Logical Interface Type
KYLD (Keyload) Interface	This is the interface to external devices. All CSPs exchanged over this interface are either encrypted or plaintext when operating in FIPS approved mode.	Data Input Data Output Control Input
RS-232 Interface	Provides an interface for factory programming, execution of RS-232 shell commands, and error logs.	Data Input Data Output Status Output
SPI	This is the interface to the KVL 5000 Host Application. All CSPs exchanged over this interface are always encrypted.	Data Input Data Output Control Input Status Output
GPIO	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 port is also used to control SPI interface.	Status Output Control Output
Clock	Clock Input.	Control Input

2 Modes of Operation

The Module can be configured to operate in a FIPS 140-2 Approved mode of operation at overall Security Level 2 and a non-Approved mode of operation. The KVL 5000 will be configured to operate in a FIPS 140-2 Approved mode of operation by following the steps in Section 2.1. Disabling FIPS-140-2 in the settings menu of the KVL Host application graphical user interface will transition between FIPS 140-2 Approved and non-Approved modes and set the KVL 5000 into a non-Approved mode of operation. This will force a reset and zeroize all the keys/CSPs. The FIPS Status service can be used to determine whether the KVL 5000 is operating in a FIPS approved mode or in a non-FIPS Approved mode.

The Version Query service can also be used to verify the firmware version matches an approved version listed on NIST's website: https://csrc.nist.gov/groups/STM/cmvp/validation.html

2.1 Approved Mode Configuration

Documented below are the actions and configuration settings required to enable FIPS 140-2 approved mode.

- Enable User and Crypto-Officer passwords.
- Enable FIPS 140-2 in the settings menu of the KVL Host application graphical user interface.
- Additionally, the KVL 5000 supports "drop-in algorithms" via the Program Update service. Drop-in algorithms may be added or removed from the KVL 5000 independent of the base FW. In order to remain in the Approved mode, only Approved algorithms may be loaded into the KVL 5000; in particular AES-128 (Cert. #C908) and/or AES-256 (Cert. #C909).

3 Cryptographic Functionality

The KVL 5000 implements the FIPS Approved and Non-Approved-but-Allowed cryptographic functions listed in the tables below.

Table 6 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C909	AES [197]	ECB [38A]	Key Sizes: 128	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 128	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128	Encrypt, Decrypt
C908	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
C931	AES [197]	CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM [38D]*	Key Sizes: 256	Encrypt, Decrypt
C930	AES [197]	KW [38F]	Forward Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt
N/A	KTS [38F]	KW	AES Cert. #C930	Restricted to only wrap keys with an equal strength to the wrapping mechanism (i.e., 128 bit keys cannot wrap 256 bit keys)
N/A	KTS [38F]	GCM, OFB	AES Cert. #C931	Key establishment methodology provides 256 bits of encryption strength
VA	CKG [IG D.12]	[133rev1] Section 6.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
C949	DRBG [90A]	CTR	AES-256	Deterministic Random Bit Generation
183	ECDSA [186]		P-384 SHA(384)	SigVer
1345	SHS [180]	SHA-256 SHA-384		Message Digest Generation, Password Obfuscation

* Per IG A.5 scenario 2, the KVL 5000 generates a 96-bit GCM IV internally at its entirety randomly as specified in SP800-38D section 8.2.2 using an approved DRBG (Cert. #C949). The DRBG is generated inside the module's physical boundary using the existing NDRNG.

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES Key Unwrap	[IG D.9] AES-OFB (Certs. #C908 and #C909) key unwrapping for use in key transport; provides 128 or 256 bits of encryption strength.
AES MAC	[IG G.13] AES Cert. #C931, vendor affirmed; P25 AES OTAR
NDRNG	[IG G.13] Non-Deterministic RNG used for seeding the DRBG with 2048-bits. Each 128-bit block output from the entropy source is assessed to contain 42.957 bits of min entropy providing at least 256 bits of entropy strength.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- ADP
- AES-OFB Key Wrap
- DES
- DES-OFB
- DES-XL
- DVI-XL
- DVP-XL

Note that all of the above are “drop-in” algorithms, except AES-OFB Key Wrap.

3.1 Critical Security Parameters

All CSPs used by the KVL 5000 are described in this section. Usage of these CSPs by the KVL 5000 (including all CSP lifecycle states) is described in the services detailed in Section 4. It should be noted that keys/CSPs stored in non-volatile memory/storage are normally preserved during a Program Update. However, all keys/CSPs are zeroized during a Program Update if the KVL 5000’s FIPS status changes, post-upgrade (this indicates that a non-FIPS compliant Drop-in algorithm has been loaded onto the KVL 5000)

Table 8 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG Entropy Input	A 2048-bit of entropy used in seeding of the CTR_DRBG during DRBG instantiation at power-up. Stored plaintext in the volatile memory, and zeroized by power cycling. It is not entered into or output from the KVL 5000. Internally generated using NDRNG.
DRBG Internal State (V and Key)	Internal state of SP800-90A CTR_DRBG (V and Key). Stored plaintext in the volatile memory, and zeroized by power cycling. It is not entered into or output from the KVL 5000, generated through SP800-90A CTR_DRBG state modification.
Black Keyloading Key (BKK)	A 256-bit AES key used for encrypting keys output over the KYLD interface. Stored in plaintext in non-volatile memory and zeroized through the Program Update service.

CSP	Description / Usage
	The BKK is entered using the Program Update service and is not output from the KVL 5000.
FIPS Cipher Key (FCK)	A 256-bit AES key used for encrypting and decrypting keys and passwords entered into the KVL 5000 over the SPI port. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The FCK is entered using the Program Update service and is not output from the KVL 5000.
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. Stored in plaintext in the internal flash memory and zeroized through the Program Update service. The IDK is entered using the Program Update service and is not output from the KVL 5000.
KPK Encryption Key (KPKEK)	A 256-bit AES key used to encrypt the KPK. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The KPKEK is entered using the Program Update service and is not output from the KVL 5000.
Key Protection Key (KPK)	A 256-bit AES key used to encrypt TEKs and KEKs output over the EBI interface. The KPK is generated internally by the SP800-90A CTR DRBG and is not output from the KVL 5000. Stored in plaintext in volatile memory and encrypted with the KPKEK in the internal flash memory. Zeroized by power cycle for volatile memory. Zeroize by program update service or changing FIPS mode.
Key Encryption Keys (KEKs)	A 256-bit AES key used for encryption of TEKs and KEKs in the Store and Forward, and Transfer Key Variable services. Stored plaintext in the volatile memory and zeroize by power cycle. Entry: SPI interface - AES256 OFB encrypted by the FCK and AES256 GCM (SP 800-38F) encrypted by the KPK, or AES256 MAC (OTAR) encrypted by the other KEK. KYLD port - plaintext. Output: SPI interface - AES256 OFB encrypted by the FCK and AES256 GCM (SP 800-38F) encrypted by the KPK, or AES256 MAC (OTAR) encrypted by the other KEKs. Could be also internally generated using SP 800-90A CTR DRBG.
Traffic Encryption Keys (TEKs)	128/256-bit AES Key used for enabling secure communication in the target devices. Stored plaintext in the volatile memory and zeroized by power cycle. Entry: SPI interface - AES256 OFB encrypted by the FCK and AES256 GCM (SP 800-38F) encrypted by the KPK, or AES256 MAC (OTAR) encrypted by the KEK. KYLD port - plaintext. Output: SPI interface - AES256 OFB encrypted by the FCK and AES256 GCM (SP 800-38F) encrypted by the KPK, or AES256 MAC (OTAR) encrypted by the KEK. Could be also internally generated using SP 800-90A CTR DRBG.
User Password	A 30-character ASCII password entered encrypted by the FCK and used to authenticate the User role. After decryption the plaintext password is not stored but temporarily exists in the volatile memory. The SHA-256 hash of the decrypted password is compared against the hash value stored in the non-volatile memory during password validation. The password is not output from the KVL 5000, and zeroized by power cycle.

CSP	Description / Usage
Crypto-Officer Password	A 30-character ASCII password entered encrypted by the FCK and used to authenticate the Crypto-Officer role. After decryption the plaintext password is not stored but temporarily exists in the volatile memory. The SHA-256 hash of the decrypted password is compared against the hash value stored in the non-volatile memory during password validation. The password is not output from the KVL 5000 and zeroized by power cycle.

3.2 Public Keys

Table 9 – Public Keys

Key	Description / Usage
ECDSA Public Programmed Signature Key	A 384-bit signature key used to validate the signature of the firmware image being loaded before it is allowed to be executed. Stored in plaintext in non-volatile memory while in use and plaintext in the non-volatile memory. Loaded during manufacturing, and not output from the KVL 5000.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The KVL 5000 PIKE2 HSM supports a User and a Crypto-Officer role. One identity is allowed for each role and each identity is authenticated by 30 ASCII printable characters in length.

Table 10 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer Role SPI interface	Identity-based	30 character ASCII Password
User	User Role over SPI interface	Identity-based	30 character ASCII password

4.2 Authentication Methods

Password Authentication

Since the password length is 30 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95^{30} which is less than 1 in 1,000,000.

The KVL 5000 limits the number of consecutive failed authentication attempts to a configurable number (Minimum 3, maximum 255). The module will zeroize all CSPs and transitions into factory default when the configurable number is met.

The KVL 5000 takes approximately 84ms to authenticate CO/User logging message over SPI interface which translates to 714 attempts per minute. As 255 is the maximum attempts allowed, the worst-case probability of a successful random attempt within a one-minute period is $255/95^{30}$, which is less than 1 in 100,000.

Table 11 – Authentication Description

Authentication Method	Probability	Probability over a One-Minute Period
Password	$1/95^{30}$	$255/95^{30}$ or $714/95^{30}$, depending on configuration

4.3 Services

All services implemented by the KVL 5000 are listed in the tables below. Note that all services listed in Table 12 and Table 13 below are available in both the FIPS Approved and non-Approved mode. The only distinguishing factor between Approved and non-Approved services is whether non-Approved algorithms/ key establishment schemes are available.

Table 12 – Authenticated Services

Service	Description	CO	User
Program Update	Update the KVL 5000 software. Software upgrades are authenticated using a digital signature. The Public Signature Validation Key (a 384-bit public ECDSA key) is used to validate the signature of the firmware image being loaded before it is allowed to be executed. To maintain validation, only validated software should be loaded. Loading non-validated software will invalidate the KVL 5000's validation.	X	
Validate Crypto-Officer Password	Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the SPI interface.	X	
Change Crypto-Officer Password	Modify the current password used to identify and authenticate the CO Role via SPI interface.	X	
Validate User Password	Validate the current User password used to identify and authenticate the User role via the SPI interface.		X
Change User Password	Modify the current password used to identify and authenticate the User Role via SPI interface.	X	X
Configure KVL	Set configuration parameters used in Store and Forward protocols and other module-specific parameters over the SPI or RS-232 interfaces.	X	
Version and Algorithm List Query	Provides module firmware version number and list of algorithms over the SPI interface.	X	X

Service	Description	CO	User
Logout	Logs out the operator.	X	X
Transfer Key Variable	Transfer key variables (KEKs, TEKs) to the target devices over the KYLD and SPI interfaces.	X	X
Receive Key Variable	Receive key variables (KEKs, TEKs) from the KYLD and SPI interfaces.	X	X
Generate Key Variable	Auto-generate Keys (KEKs, TEKs) by the KVL 5000.	X	X
Key Check	Validate the correctness of a key based on algorithm properties.	X	X
Zeroize Keys	Zeroize keys (KEKs, TEKs) in the KVL and target devices over the KYLD interface.	X	X
Encrypt	Encrypt plaintext data to be transferred over the SPI, KYLD, and EBI interfaces.	X	X
Decrypt	Decrypt ciphertext data received over the SPI, KYLD, and EBI interfaces.	X	X
Store and Forward (SAF)	Receive Key Variable keys from KMF into the module, Transfer Key Variable keys to be stored externally (host application), then Transfer Key Variable (forward) to target device attached to the KVL.	X	X
Key Sharing	Combination of receive and Transfer Key Variable service. Transport keys (TEKs/KEKs) between two KVLs.	X	X
Reset	Reset the databases and module parameters to system defaults via a command over the SPI interface.	X	X

Table 13 – Unauthenticated Services

Service	Description
Diagnostics	Read logs, run LED test, test external flash erase and write, and other non-security relevant status information over the RS-232 interface.
Perform Self-Tests	Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by a transition from power off state to power on state.
FIPS Status	Provides current FIPS status about whether the KVL 5000 is operating at overall Security Level 2, or in a non-Approved mode of operation. Available without a role.

Table 14 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- C = Check CSP: Check status of the CSP (i.e. existence, size, format, etc.).

- D = Decrypt: Decrypts entered key using other KEK during CSP entry over the SPI interface or using the KVL-BKK during CSP entry over the KVL interface. In the case of the Program Update service, decryption will occur using the IDK.
- E = Encrypt: Encrypts key prior to output over the SPI interface using a KEK.
- G = Generate CSP: Generates keys.
- S = Store CSP: Stores CSP in volatile or non-volatile memory.
- U = Use CSP: Uses key internally for encryption/decryption services.
- Z = Zeroize: The service zeroizes the CSP.
- - = No access: the service does not access the CSP.

Table 14 – Security Parameters Access by Service

Service	CSPs and Public Keys											
	DRBG Entropy Input	DRBG Internal state (V and Key)	BKK	FCK	KPKEK	IDK	KEKs	KPK	TEKs	Crypto-Officer Password	User Password	ECDSA Public Programmed Signature Key
Program Update	–	–	D,Z,S	D,Z,S	D,Z,S	U,Z,S	Z	Z	Z	Z	Z	U
Validate Crypto-Officer Password	–	–	–	–	–	–	–	D,G,S	–	D,U,Z	–	–
Change Crypto-Officer Password	–	–	–	–	–	–	–	–	–	D,U,Z,S	–	–
Validate User Password	–	–	–	–	–	–	–	D,G,S	–	–	D,U,Z	–
Change User Password	–	–	–	–	–	–	–	–	–	D,U,Z,S	–	–
Configure KVL	–	–	–	–	–	–	–	–	C,D,E,S,U,Z	C,D,E,S,U,Z	C,D,E,S,U,Z	–
Version and Algorithm List Query	–	–	–	–	–	–	–	–	–	–	–	–
Logout	–	–	–	–	–	–	–	–	–	–	–	–
Transfer Key Variable	–	–	U	–	–	–	U	–	D,E,U	–	–	–
Receive Key Variable	–	–	–	–	–	–	U	–	D,E,S,U	–	–	–
Generate Key Variable	–	U	–	–	–	–	–	–	E,G,S	–	–	–
Key Check	–	–	–	–	–	–	C	–	C	–	–	–
Zeroize Keys (in target devices)	–	–	–	–	–	–	–	–	–	–	–	–

Service	CSPs and Public Keys											
	DRBG Entropy Input	DRBG Internal state (V and Key)	BKK	FCK	KPKEK	IDK	KEKs	KPK	TEKs	Crypto-Officer Password	User Password	ECDSA Public Programmed Signature Key
Encrypt	–	U	U	U	U	–	U	U	U	–	–	–
Decrypt	–	–	U	U	U	U	U	U	U	–	–	–
Store and Forward (SAF)	–	–	–	–	–	–	U	–	D,E,S,U,Z	–	–	–
Key Sharing	–	–	–	–	–	–	C,S	–	C,S	–	–	–
Reset	G,U,Z	G,U,Z	–	–	–	–	Z	–	Z	Z	Z	–
Diagnostics	–	–	–	–	–	–	–	–	–	–	–	–
Perform Self-Tests	–	–	–	–	–	–	–	–	–	–	–	–
FIPS Status	–	–	–	–	–	–	–	–	–	–	–	–

5 Self-tests

The KVL 5000 performs self-tests to ensure the proper operation of the KVL 5000. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power-up self–tests are available on demand by power cycling the KVL 5000.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptographic functionality by the KVL 5000. The KVL 5000 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 KVL 5000 is in critical error state due to power-up self-tests failure or critical error condition. The critical error state may be exited by powering the KVL 5000 off then on.

The KVL 5000 performs the following algorithm KATs on power-up. The AES KATS are inclusive of the drop-in algorithms.

- Firmware Integrity: A digital signature is generated over the base firmware and all Drop-in algorithms code when it is built using SHA-384 and ECDSA P-384, and is stored with the code upon download into the KVL 5000. When the KVL 5000 is powered up, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.
- AES-128 encrypt and decrypt KATs for ECB, OFB, and CBC modes.
- AES-256 encrypt and decrypt KATs for ECB, OFB, and CBC modes.
- AES-256 (Internal) encrypt and decrypt KATs for ECB, CBC, OFB, CFB8, and GCM modes.

- SHA-256 KAT.
- CTR DRBG KAT.
- AES KW (SP 800-38F) KAT.

The KVL 5000 performs the following critical functions tests as indicated.

- Random Number Generator entropy test. This test runs two RNG statistical tests: a FIPS monobit test, and a FIPS “runs” test as defined in SP 800-22r1a.
- The Module performs a read/write test of the internal RAM at each power up.

The KVL 5000 performs the following conditional self-tests as indicated.

- Continuous Random Number Generator test: The continuous random number generator test is performed on the NDRNG and DRBG supported by the KVL 5000. An initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to NDRNG/DRBG generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller. This testing is done for each 4 byte NDRNG/16 byte DRBG data block, generated by the DRBG. The KVL 5000 enters the critical error state if this test fails.
- SP800-90A DRBG health tests.
- Firmware load test: a digital signature is generated over the code when it is built using SHA-384 and ECDSA P-384. Upon download into the KVL 5000, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.

6 Physical Security Policy

The KVL 5000 PIKE2 HSM is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 physical security requirements. The KVL 5000 PIKE2 is covered with a hard, opaque epoxy coating that provides evidence of attempts to tamper with the KVL 5000. The KVL 5000 PIKE2 HSM 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 KVL 5000 while delivering to operators. Physical Security Testing was performed at ambient temperature.

7 Operational Environment

The KVL 5000 has a non-modifiable operational environment under the FIPS 140-2 definitions. The KVL 5000 includes Program Update service to support necessary updates. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. If firmware that is not identified in this Security Policy is loaded into the KVL 5000, the KVL 5000 will be in a non-Approved mode. Loading any Non-Approved Drop-in algorithms listed in the Table 3 will also place the KVL 5000 in a non-Approved mode

8 Mitigation of Other Attacks Policy

The KVL 5000 is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

9 Security Rules and Guidance

This section documents the security rules for the secure operation of the KVL 5000 to implement the security requirements of FIPS 140-2.

9.1 Invariant Rules

1. An operator does not have access to any cryptographic services prior to assuming an authorized role.
2. Power up self-tests do not require any operator action.
3. Data output is inhibited during key generation, self-tests, zeroization, and while in critical error states.
4. The KVL 5000 does not perform any cryptographic functions while in a critical error state.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the KVL 5000.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The KVL 5000 provides a means to ensure that a key entered into or stored within the KVL 5000 is associated with the correct entities to which the key is assigned. Each TEK, KEK in the KVL 5000 is entered and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID, Common Key Reference (CKR) number, and Keyset number – Identifiers indicating storage locations.

   Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption.
8. The KVL 5000 denies access to plaintext secret and private keys contained within the KVL 5000.
9. The KVL 5000 provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the KVL 5000.
10. The KVL 5000 implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
11. The KVL 5000 conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[133r1]	*NIST Special Publication 800-133 Revision 1, Recommendation for Cryptographic Key Generation, July 2019*
[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*
[22r1a]	*National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[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*

Abbreviation	Full Specification Name
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 16 – Acronyms and Definitions

Acronym	Definition
ADP	Advanced Digital Privacy
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
EBI	External Bus Interface
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FW	Firmware
GCM	Galois/Counter Mode
GPIO	General-Purpose Input/Output
HSM	Hardware Security Module
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KMF	Key Management Facility
KPK	Key Protection Key
KEK	Key Encryption Key
KYLD	Keyload
KVL	Key Variable Loader
OFB	Output Feedback

Acronym	Definition
OTAR	Over The Air Rekeying
NDRNG	Non-Deterministic Random Number Generator
SAF	Store and Forward
SPI	Serial Peripheral Interface
TEK	Traffic Encryption Key