Security Policy: Key Variable Loader (KVL) 4000 PIKE2

Cryptographic module used in Motorola's Key Variable Loader (KVL) 4000 keyloader.

Version: R01.03.15

Date: September 16, 2014

Table of Contents

1. Introduction

1.1. Scope

This Security Policy specifies the security rules under which the Key Variable Loader (KVL) 4000 PIKE2 must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and those imposed additionally by Motorola. These rules, in total, define the interrelationship between the:

1. Module Operators,
2. Module Services, and
3. Critical Security Parameters (CSPs).

1.2. Definitions

AES		Advanced Encryption Standard
CBC		Cipher Block Chaining
CFB		Cipher Feedback
CKR		Common Key Reference
CO		Cryptographic Officer or Crypto-Officer
CSP		Critical Security Parameter
DES		Data Encryption Standard
DRBG		Deterministic Random Bit Generator
ECB		Electronic Code Book
FCK		FIPS Cipher Key
IC		Integrated Circuit
IV		Initialization Vector
K		Authentication Key
KEK		Key Encryption Key
KPK		Key Protection Key
KPKEK		KPK Encryption Key
KVL		Key Variable Loader
MAC		Message Authentication Code
USB		Universal Serial Bus
OFB		Output Feedback
OTAR		Over The Air Rekeying
PDA		Personal Digital Assistant
RNG		Random Number Generator
TEK		Traffic Encryption Key

1.3. Overview

The KVL 4000 PIKE2 provides security services for the KVL 4000. The KVL 4000 is a portable key distribution device that consists of a Personal Digital Assistant (PDA) and Security Adapter that connects to the PDA. The PIKE2 IC is embedded in the Security Adapter. Encryption keys can be loaded into the KVL 4000 manually through its keypad interface or transferred from a key management facility through its RS-232 interface. These keys can then be distributed to various secure communications equipment such as mobile and portable radios, base stations, zone controllers, data controllers, and other fixed network devices.

1.4. KVL 4000 PIKE2 Implementation

The KVL 4000 PIKE2 is implemented as a single-chip cryptographic module as defined by FIPS 140-2.

1.5. KVL 4000 PIKE2 Hardware / Firmware Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
51009397004	R02.03.07

The KVL 4000 PIKE2 supports the following FIPS Approved algorithms which may be installed separately from KVL 4000 PIKE2 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.

Approved Algorithm	Certificate Number	Part Number	Firmware Version Number
AES-128 (ECB, CBC, OFB)	1491	51009397004	R01.01.00
AES-256 (ECB, CBC, OFB, CFB-8)	1492	51009397004	R01.01.00

1.6. KVL 4000 PIKE2 Cryptographic Boundary

The KVL 4000 PIKE2 Cryptographic Boundary is drawn around the PIKE2 IC as shown below.

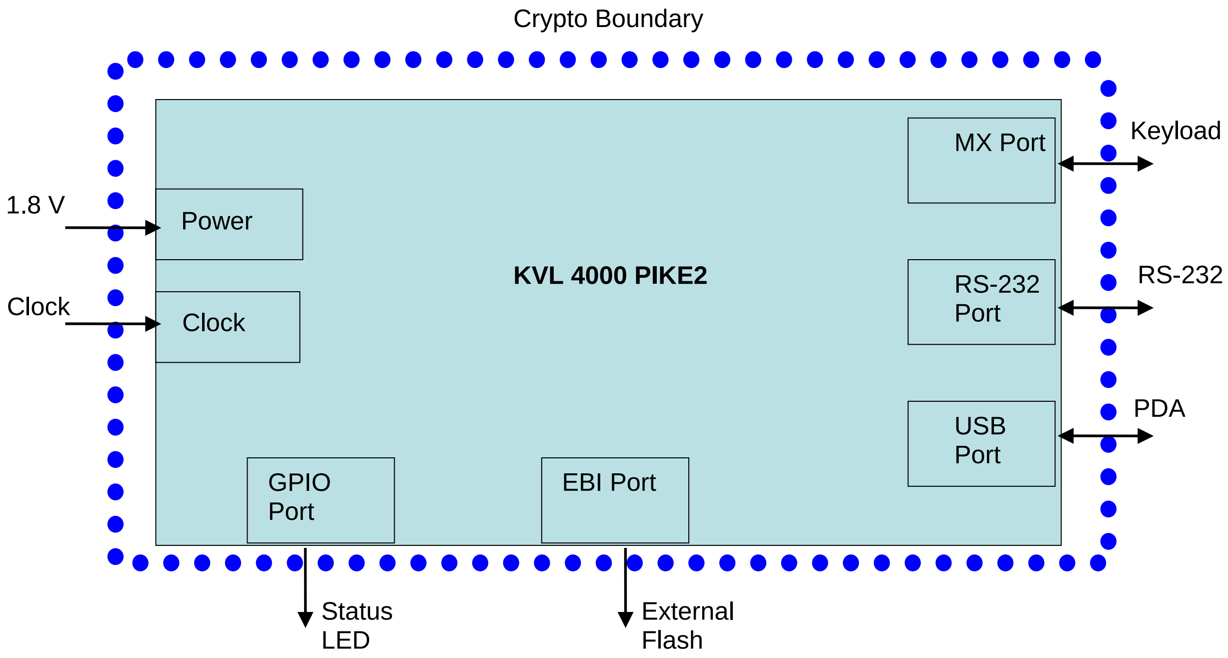

Figure 1: The KVL 4000 PIKE2 in the block diagram above provides data security services required by the KVL 4000 key loader. The module is a single PIKE2 processor with the set of interfaces shown in the diagram above. The Crypto Boundary is drawn around the PIKE2 IC.

1.7. Ports and Interfaces

The KVL 4000 PIKE2 provides the following physical ports and logical interfaces:

Table 1: Ports and Interfaces

Physical Port	Qty	Logical interface definition	Description
Power	1	• Power Input	This interface powers all circuitry.
Universal Serial Bus (USB) Interface	1	• Data Input • Data Output • Control Input • Status Output	This is the interface to the PDA host software. All CSPs exchanged over this interface are always encrypted.

Physical Port	Qty	Logical interface definition	Description
Keyload (MX) Interface	1	• Data Input • Data Output • Control Input • Status Output	This is the interface to external devices. All CSPs exchanged over this interface are in plaintext form when operating at FIPS 140-2 overall Level 2.
RS-232 Interface	1	• Data Input • Data Output • Control Input • Status Output	Provides an interface for factory programming and execution of RS-232 shell commands. All CSPs exchanged over this interface are always encrypted.
LED Output	1	• Status Output	The LED 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 fatal error state.
IRQ/FIQ	3	• Control Input	External interrupts.
Clock	1	• Control Input	Clock Input.
EBI Interface	1	• Data Input • Data Output • Control Input • Status Output	This is the interface to the external flash memory on the KVL 4000 Security Adapter. All CSPs exchanged over this interface are encrypted.

2. FIPS 140-2 Security Levels

The KVL 4000 PIKE2 can be configured to operate at FIPS 140-2 overall Security Level 2. The table below shows the FIPS 140-2 Level of security met for each of the eleven areas specified within the FIPS 140-2 security requirements.

Table 2: KVL 4000 PIKE2 Security Levels

FIPS 140-2 Security Requirements Section	Validated Level at overall Security Level 2
Cryptographic Module Specification	3
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

3. FIPS 140-2 Approved Operational Modes

The KVL 4000 PIKE2 can be configured to operate in a FIPS Approved mode of operation and a Non-FIPS Approved mode of operation. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 2.

At any given time, the FIPS Status service can be used to determine whether the module is operating at overall Security Level 2 or in a non-FIPS Approved mode.

3.1. Configuration Settings for operation at FIPS 140-2 overall Security Level 2

Documented below are the actions and configuration settings required to enable FIPS 140-2 overall Security Level 2.

1. Enable User and Crypto-Officer passwords.
2. Enable FIPS 140-2 overall Security Level 2 by selecting Level 2 in the settings menu of the PDA graphical user interface.
3. Only Approved and Allowed algorithms installed. The module supports the following Approved algorithms:

    - AES-256 (Cert. #1492) –Used for encryption and decryption in the following Approved modes: OFB, ECB, CBC, and 8-bit CFB.
    - AES-128 (Cert. #1491) –Used for encryption and decryption in the following Approved modes: OFB, ECB, and CBC.
    - SHA-256 (Cert. #1345) – used for password hashing for internal password storage.
    - SHA-384 (Cert. #1345) – used for digital signature verification during software/firmware integrity test and software/firmware load test.
    - ECDSA-384 (Cert. #183) – used for digital signature verification during software/firmware integrity test and software/firmware load test
    - SP800-90 CTR DRBG (Cert. #159) – used for IV and KPK generation

    The module supports the following Allowed algorithms:

    - AES MAC (Cert. #1492) – Used to provide message authentication within APCO OTAR and APCO Link Layer Authentication. AES MAC as used within APCO OTAR and APCO Link Layer Authentication has been vendor affirmed and is approved when used for Project 25 APCO OTAR and Project 25 APCO Link Layer Authentication.
    - AES Key Wrap (Cert. #1492) – Used for inner layer encryption within APCO OTAR and APCO Link Layer Authentication. AES Key Wrap as used within APCO OTAR and APCO Link Layer Authentication has been vendor affirmed and is approved when used for Project 25 APCO OTAR and Project 25 APCO Link Layer Authentication. Key establishment methodology provides 256 bits of encryption strength.
    - Non-deterministic Hardware Random Number Generator – used to provide random numbers used as Initialization Vectors (IV) and the seeds for the Approved RNG

3.2. Non Approved Mode of Operation

A non-FIPS Approved mode of operation is transitioned to when any of the following is true:

1. User and Crypto-Officer password have not been enabled.
2. FIPS 140-2 overall Security Level 2 has not been enabled.
3. Non-Approved algorithms are installed. The module supports the following non-Approved algorithms:
    - DES-XL
    - DVP-XL
    - DVI-XL
    - ADP
    - DES (OFB, ECB, and CBC modes)

The module maintains FIPS mode status and will provide this upon operator request.

4. Crypto Officer and User Guidance

4.1. Administration of the KVL 4000 PIKE2 in a secure manner (CO)

The KVL 4000 PIKE2 requires no special administration for secure use after it is set up for use in a FIPS Approved manner. To do this, configure the module as described in section 3 of this document.

Note that all keys will be zeroized after the Program Update service has completed.

4.2. Assumptions regarding User Behavior (CO)

The KVL 4000 PIKE2 has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

4.3. Approved Security Functions, Ports, and Interfaces available to Users

KVL 4000 PIKE2 services available to the User role are listed in section 8.2.

No Physical Ports or Logical Interfaces are directly available to the KVL 4000 PIKE2 User, only indirectly through the KVL 4000 in which the module is installed.

4.4. User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the KVL 4000 PIKE2.

5. Security Rules

The KVL 4000 PIKE2 enforces the following security rules. These rules are separated into those imposed by FIPS 140-2 and those imposed by Motorola.

5.1. FIPS 140-2 Imposed Security Rules

1. The KVL 4000 PIKE2 inhibits all data output via the data output interface whenever an error state exists and during self-tests.
2. The KVL 4000 PIKE2 logically disconnects the output data path from the circuitry and processes when performing key generation, manual key entry, or key zeroization.
3. Authentication data (e.g. passwords) are entered in encrypted form. Authentication data is not output during entry.
4. At FIPS 140-2 overall Security Level 2, secret cryptographic keys are entered in plaintext form over a logically separate port.
5. The KVL 4000 PIKE2 enforces Identity-Based authentication.
6. The KVL 4000 PIKE2 supports a User role and a Crypto-Officer role. Authenticated operators are authorized to assume either supported role.
7. The KVL 4000 PIKE2 re-authenticates an operator when it is powered-up after being powered-off. The module also re-authenticates an operator upon expiration of the inactivity timer. The inactivity timer is user-configurable to 1, 3, or 5 minutes.
8. The KVL 4000 PIKE2 prevents brute-force attacks on its User and Crypto-Officer passwords by using a password that is a minimum of 15 ASCII printable characters in length. The probability of a successful random attempt is one in 463,291,230,159,753,366,058,349,609,375.
   - There are 95 ASCII printable characters; password is a minimum of 15 characters.
   - 95 ^ 15 = 463,291,230,159,753,366,058,349,609,375

   It would require 4,632,912,301,597,533,660,583,496 attempts in one minute to lower the random attempt success rate to less than 1 in 100,000. Each attempt takes at least 500 milliseconds. Therefore, a maximum of 120 attempts are possible during any one minute period.
9. The KVL 4000 PIKE2 uses ECDSA-384 to prevent brute-force attacks on the digital signature used to verify software/firmware integrity during a Program Update. As the Program Update service requires more than one minute to complete, the random attempt success rate during a one minute period cannot be lowered to less than 1 in 100,000.
10. Authentication data is not output during entry.
11. The KVL 4000 PIKE2 provides the following services requiring a role:
    - Program Update
    - Change Crypto-Officer password
    - Change User password
    - Configure KVL
    - Extract Action Log
    - Version & Algorithm List Query
    - Logout

- Transfer Key Variable
- Receive Key Variable
- Generate Key Variable
- Delete Key Variable
- Edit Key Variable
- Key Check
- Zeroize Keys
- Encrypt
- Decrypt
- Validate Crypto-Officer Password
- Validate User Password
- Store & Forward
- Reset Crypto Module

12. The KVL 4000 PIKE2 provides the following services not requiring a role:
    - FIPS Status
    - Perform Self Tests
13. The KVL 4000 PIKE2 implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
14. The KVL 4000 PIKE2 protects secret keys and private keys from unauthorized disclosure, modification, and substitution.
15. The KVL 4000 PIKE2 provides a means to ensure that a key entered into or stored within the module is associated with the correct entities to which the key is assigned. Each TEK, KEK in the KVL 4000 PIKE2 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.

    Each K key in the KVL 4000 PIKE2 is entered and stored with the following information:
    - Subscriber ID – 56 bit identifier

16. The KVL 4000 PIKE2 denies access to plaintext secret and private keys contained within the module.
17. The KVL 4000 PIKE2 provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
18. The KVL 4000 PIKE2 provides the following non-FIPS Approved Random Number Generators to provide random numbers used as Initialization Vectors (IV) and the seeds for the Approved RNG.

    - Non-deterministic Hardware Random Number Generator
19. The KVL 4000 PIKE2 conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

20. The KVL 4000 PIKE2 performs the following self-tests:

- Power up and on-demand tests
  - Cryptographic algorithm test: Each algorithm (SHA-256, SHA-384, AES-256 in the OFB, CBC, ECB, 8-bit CFB, and Key Wrap modes) is tested by using a known key, known data, and if required a known IV. The data is then encrypted and compared with known encrypted data; the test passes if the final data matches the known data, otherwise it fails. The encrypted data is then decrypted and compared with the original plaintext; the test passes if the decrypted data matches the original plaintext, otherwise it fails.
  - DRBG KAT test: the DRBG is initialized with a known answer seed and V generated by the hardware RNG. The DRBG is run and a random bit block is generated. The DRBG is then reseeded and another random bit block is generated. The two random bit blocks are compared. The test passes if the generated data does not match. DRBG KAT test also performs a monobit test to test if the data is within the required range..
  - Software/firmware Integrity test: A digital signature is generated over the code when it is built using SHA-384 and ECDSA-384 and is stored with the code upon download into the module. When the module is powered up the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
  - External Indicators test: Upon every power up, the module will assert and de-assert each signal connected to an external indicator, so that the User may verify that the indicators are functioning and controlled properly.

Powering the module off then on will initiate the power-up and on-demand self-tests.

- Conditional tests
  - Software/firmware Load test: A digital signature is generated over the code when it is built using SHA-384 and ECDSA-384. Upon download into the module, the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
  - Continuous Random Number Generator test: The continuous random number generator test is performed on all DRBGs supported by the module. For each DRBG, 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 any one of the DRBGs 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.

21. The KVL 4000 PIKE2 enters an error state if the Cryptographic Algorithm Test, Continuous Random Number Generator Test, or DRBG KAT fails. This error state may be exited by powering the module off then on.

22. The KVL 4000 PIKE2 enters an error state if the Software/Firmware Integrity test fails. As soon as an error indicator is output via the status interface, the module transitions from the error state to a state that only allows new software to be loaded.

23. The KVL 4000 PIKE2 enters an error state if the Software/Firmware Load test fails. This error state may be exited by powering the module off then on which will start the download and validation process over.

24. The KVL 4000 PIKE2 outputs a status indicator via the LED Output interface to indicate all self-tests passed or when an error state is entered due to a failed self-test.
25. The KVL 4000 PIKE2 does not perform any cryptographic functions while in an error state.

5.2. Motorola Imposed Security Rules

1. The KVL 4000 PIKE2 does not support multiple concurrent operators.
2. All cryptographic module services are suspended during key loading.

6. Identification and Authentication Policy

The KVL 4000 PIKE2 supports a User and a Crypto-Officer role.

The Crypto-Officer role is authenticated by a digital signature during the Program Update service and a password which is a minimum of 15 and maximum of 30 ASCII printable characters in length for the remaining Crypto-Officer services.

The User role is authenticated by a password that is a minimum of 15 and a maximum of 30 ASCII printable characters in length.

Both Crypto-Officer and User ID's and passwords are initialized to a default value during manufacturing and are sent in encrypted form to the module for authentication.

Role	Authentication Type	Authentication Data Required
User	Identity-Based	User ID and 15-30 character ASCII Password
Crypto-Officer	Identity-Based	ECDSA-384 digital signature for Program Update service; Crypto-Officer ID and 15-30 character ASCII Password for all other services

7. Physical Security Policy

The KVL 4000 PIKE2 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 4000 PIKE2 is covered with a hard opaque epoxy coating that provides evidence of attempts to tamper with the module. The KVL 4000 PIKE2 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. Physical Security Testing was performed at ambient temperature.

8. Access Control Policy

8.1. KVL 4000 PIKE2 Supported Roles

The KVL 4000 PIKE2 supports two (2) roles. These roles are defined to be the:

- User role and,
- Cryptographic Officer (Crypto-Officer or CO) role.

8.2. KVL 4000 PIKE2 Services

All services listed are available in both FIPS mode and non-FIPS mode.

- Program Update: Update the module 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. All keys and CSPs are zeroized during a Program Update. To maintain validation, only validated software should be loaded. Loading non-validated software will invalidate the modules validation. Available to CO role.
- Validate Crypto-Officer Password: Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the USB interface. Available to the CO role.
- Change Crypto-Officer Password: Modify the current password used to identify and authenticate the CO Role via USB interface. Available to CO role.
- Validate User Password: Validate the current User password used to identify and authenticate the User role via the USB interface. Available to the User role.
- Change User Password: Modify the current password used to identify and authenticate the User Role via USB interface. Available to User role.
- Configure KVL: Set configuration parameters used in Store and Forward protocols and other module-specific parameters over the USB interface. Available to User and CO roles.
- Extract Action Log: Exports a history of actions over the RS-232 interface. Available to User and CO roles.
- Version and Algorithm List Query: Provides module firmware version number and list of algorithms over the USB interface. Available to User and CO roles.
- Logout: Logs out the operator. Available to User and CO roles.
- Transfer Key Variable: Transfer key variables (Ks, KEKs, TEKs) to the target devices over the Keyload (MX) and RS-232 interfaces. Available to User and CO roles.
- Receive Key Variable: Receive key variables (KEKs, TEKs) from the USB, Keyload (MX), and RS-232 interfaces and key variables (Ks) from the USB Interface. Available to CO role.
- Generate Key Variable: Auto-generate Keys (Ks, KEKs, TEKs) and KPK within the module. Available to CO role.
- Delete Key Variable: Delete Keys (Ks, KEKs, TEKs) managed by the module. Available to CO role.
- Edit Key Variable: Edit Keys (Ks, KEKs, TEKs) managed by the module. Available to CO role.
- Key Check: Validate the correctness of a Key based on algorithm properties. Available to User and CO roles.

- Zeroize Keys: Zeroize Keys (KEKs, TEKs) in the KVL and target devices over the Keyload (MX) and RS-232 interfaces. Available to User and CO roles.
- Encrypt: Encrypt plaintext data to be transferred over the USB, Keyload (MX), RS-232, and EBI interfaces. Available to User and CO roles.
- Decrypt: Decrypt ciphertext data received over the USB, Keyload (MX), RS-232, EBI interfaces. Available to User and CO roles.
- Store and Forward (SAF): Modify and query the Key, SAF, and TTU Databases via SAF Key Management Messages. Available to User and CO roles.
- Reset: Reset the databases and module parameters to system defaults via a command over the USB interface. Available to User and CO roles.
- Perform Self-Tests: Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by module reset or transition from power off state to power on state. Available without a role.
- FIPS Status: Provides current FIPS status about whether the module is operating at overall Security Level 2, or in a non-Approved mode of operation. Available without a role.

8.3. Key Management

CSPs: The following table provides a list and description of all CSPs managed by the module.

Table 3: CSP Definition

CSP Identifier	Description
SP800-90 CTR DRBG V	A 64-bit seed value used within the SP800-90 CTR DRBG. The V is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed is not entered into or output from the module.
SP800-90 CTR DRBG key	Key used to seed the SP800-90 CTR DRBG during initialization. The seed key is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed key is not entered into or output from the module.
Black Keyloading Key (BKK)	A 256-bit AES key used for encrypting keys output over the MX and RS-232 ports. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The BKK is entered using the Program Update service and is not output from the module.
FIPS Cipher Key (FCK)	A 256-bit AES key used for decrypting keys and passwords entered into the module over the USB 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 module.

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 module.
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The IDK is entered using the Program Update service and is not output from the module.
Key Encryption Keys (KEKs)	256-bit AES key used for encryption of keys in the Store and Forward, and Transfer Key Variable services. KEKs are entered in encrypted form via the USB interface (encrypted with the FCK) and the Store and Forward service (encrypted with other TEKs and KEKs), and can also be generated internally. Stored in plaintext in RAM and zeroized via power cycle. At FIPS 140-2 overall Security Level 2 KEKs are output over the MX and RS-232 ports in plaintext form. KEKs output over the EBI and USB ports are encrypted on the KPK.
Key Protection Key (KPK)	256-bit AES key used to encrypt TEKs and KEKs output over the EBI and USB ports. The KPK is generated internally by the SP800-90 CTR DRBG and is not output from the module. Store in plaintext in volatile memory and encrypted with the KPKEK in non-volatile memory. Zeroized by power cycle for volatile memory.
Crypto-Officer Password	A 15-character ASCII password entered encrypted on the FCK and used to authenticate the Crypto-Officer role. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the module. Zeroized by power cycle.
User Password	A 15-character ASCII password entered encrypted on the FCK and used to authenticate the User role. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the module. Zeroized by power cycle.
Traffic Encryption Keys (TEKs)	256 bit AES key used for enabling secure communication in target devices. TEKs are entered in encrypted form via the USB interface (encrypted with the FCK) and the Store

	and Forward service (encrypted with other TEKs and KEKs), and can also be generated internally. TEKs are stored in plaintext in RAM. At FIPS 140-2 overall Security Level 2 TEKs are output over the MX and RS-232 ports in plaintext form. TEKs output over the EBI and USB ports are encrypted on the KPK. Zeroized by power cycle.
External Authentication Key (K)	128-bit AES key used for enabling authentication in target devices. Ks are entered in encrypted form via the USB interface (encrypted with the FCK using AES256-OFB), and can also be generated internally (the K can only be entered or generated in overall FIPS Security Level 2). Ks are stored in plaintext in RAM. Ks are output over the RS-232 ports in plaintext form. Ks are output over the EBI and USB ports are encrypted on the KPK using AES256-CFB8 or KEKs using AES128 Key Wrap. In the context of key management, this key is managed the same as a TEK. Zeroized by power cycle or Program Update service.

Public Keys: The following table lists and describes all Public Keys managed by the module.

Table 4: Public Key Definition

Public Key Name	Description
Public Signature Validation Key	384-bit ECDSA key used to validate the signature of the firmware image being programmed before it is allowed to be executed and is also used for authentication of the Crypto-Officer role. Loaded during manufacturing. The Public Signature Validation Key is not output from the module.

8.4. CSP Access Types

Table 5: CSP Access Types

CSP Access Type	Description
c - Check CSP	Checks status of the CSP.
d - Decrypt CSP	Decrypts KEKs and TEKs retrieved over the EBI port using the KPK. Decrypts KEKs and TEKs retrieved over RS-232 using other KEKs and TEKs. Decrypts entered password & KEKs and TEKs using the FCK during CSP entry over the USB interface.
e - Encrypt CSP	Encrypts KEKs and TEKs prior to output over the EBI interface using the KPK.

	Encrypts KEKs, TEKs, and SEKs prior to output over the RS-232 interface using another KEK and SEK.
g - Generate CSP	Generates KPK, SP800-90 CTR DRBG V, or SP800-90 CTR DRBG key.
i - Invalidate CSP	Marks encrypted TEKs or KEKs stored in non-volatile memory as invalid. TEKs or KEKs marked invalid can then be over-written when new TEKs or KEKs are stored.
s - Store CSP	Stores KPK in volatile and non-volatile memory. Stores plaintext BKK, FCK, or IDK in volatile and non-volatile memory.
u - Use CSP	Uses CSP internally for encryption / decryption services.
z - Zeroize CSP	Zeroizes CSP.

Table 6: CSP versus CSP Access

Service	CSP												Role		
	SP800-90 CTR DRBG V	SP800-90 CTR DRBG key	FCK (FIPS Cipher Key)	KPKEK (Key Protection Key Encryption Key)	TEK (Traffic Encryption Key)	K (Authentication Key)	KEK (Key Encryption Key)	KPK (Key Protection Key)	BKK (Black Keyloading Key)	IDK (Image Decryption Key)	User Password	Crypto-Officer Password	User Role	Crypto-Officer Role	No Role Required
1. Program Update			z, s	z,s	z	z	z	z,s	z, s	u, z, s	z	z		√	
2. Validate Crypto-Officer Password								d,g, s				d, u, z		√	
3. Change Crypto-Officer Password												d, u, z, s		√	
4. Validate User Password								d,g, s			d,u,z		√	√	
5. Change User Password												d,u,z, s	√		
6. Configure KVL					c,d,e, s,u,z	c,d,e, s,z	c,d,e, s,u,z				c,d,e , s,u,z	c,d,e, s,u,z	√	√	
7. Extract Action Log													√	√	
8. Version & Algorithm List Query													√	√	
9. Logout													√	√	
10. Transfer Key Variable					d,e,u	d,e,	d,e,u	u	u				√	√	
11. Receive Key Variable					d,e,s, u	d,e,s,	d,e,s, u	u						√	
12. Generate Key Variable					e,g,s	e,g,s	e,g,s	u						√	

13. Delete Key Variable					z	z	z							√	
14. Edit Key Variable					d,s	d,s	d,s	u						√	
15. Key Check					c	c	c						√	√	
16. Zeroize Keys (in target devices)													√	√	
17. Encrypt			u	u	u		u	u	u	u			√	√	
18. Decrypt			u	u	u		u	u	u				√	√	
19. Store & Forward					d,e,s, u,z	d,e,s, z	d,u	u					√	√	
20. Reset Crypto Module software	g, u, z	g, u, z			z	z	z	z,g, s					√	√	
21. Perform Self-Tests															√
22. FIPS Status													√	√	√

9. Mitigation of Other Attacks Policy

The KVL 4000 PIKE2 is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.