Security Policy for FIPS 140-2

KVL 3000 *Plus*

Version 01.01.16

Repository Information:

Location: /vobs/kvl/DOCS/KVL3000_Plus/FIPS_140_2

Filename: KVL 3000 Plus Security Policy.doc

1 Introduction

KVL 3000 Plus

1.1 Scope

This Security Policy specifies the security rules under which the KVL 3000 *Plus*, herein identified as the KVL, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Motorola. These rules, in total, define the interrelationship between the:

1) module operators,
2) module services,
3) Critical Security Parameters (CSPs).

1.2 Overview

The Key Variable Loader (KVL) is a portable key distribution device. Encryption keys can be loaded into the KVL manually through its keypad interface or transferred from a key management facility through its serial 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. The KVL also includes a PCMCIA interface for firmware upgrades.

1.3 KVL Implementation

The KVL is implemented as a multi-chip standalone cryptographic module as defined by FIPS 140-2.

1.4 KVL Cryptographic Boundary

The KVL is defined as the handheld portable keyloading device with a built-in crypto engine. This includes the KVL motherboard containing various ICs, EEPROMS, RAM, and I/O ports.

1.5 KVL Hardware and Firmware Version Numbers

Certificate Number	HW Version Number	SW Version Number
229	8482867Y02 rev. B	R3.51.01
230	8482867Y02 rev. B	R3.51.06
480	P/N CLN7493D. Version 8	P/N U239AC, X795AH. Version R3.52.17, R3.52.22, R3.52.31

1.6 KVL Acronym List

CBC	Cipher Block Chain
CFB	Cipher Feedback
CKR	Common Key Reference
CO	Crypto Officer
CSP	Critical Security Parameter
ECB	Electronic Code Book
IV	Initial Vector
KPK	Key Protection Key
KVL	Key Variable Loader
LFSR	Linear Feedback Shift Register
MAC	Media Access Control
MNP	Message Number Period
OFB	Output Feedback
OTAR	Over The Air Rekeying
RNG	Random Number Generator
RSI	Radio Set Indicator
SAF	Store and Forward
UCM	Universal Crypto Module

2 FIPS 140-2 Security Levels

The KVL is validated to meet the FIPS 140-2 security requirements for the levels shown in Table 2.1. The overall module is validated FIPS 140-2 Security Level 1.

FIPS 140-2 Security Requirements Section	Level
1. Cryptographic Module Specification	1
2. Module Ports and Interfaces	1
3. Roles, Services, and Authentication	2
4. Finite State Model	1
5. Physical Security	1
6. Operational Environment	N/A
7. Cryptographic Key Management	1
8. EMI / EMC	1
9. Self Tests	1
10. Design Assurance	1
11. Mitigation of Other Attacks	N/A

Table 2.1 KVL Security Levels

3 FIPS 140-2 Approved Operational Modes

The KVL includes modes of operation that are not FIPS 140-2 approved. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 approved mode of operation:

1. Tamper Enabled
2. Passwords enabled
3. DES for encryption, decryption, and authentication shall be used in the following approved modes, for legacy systems only: ECB, OFB, CFB, and CBC **OR**
4. AES-256 encryption, decryption, and authentication may be used in the following approved modes: OFB, ECB, and CBC.
5. Use of 3DES 8-bit CFB mode for symmetric encryption / decryption of keys and parameters stored in the internal database, and 3DES CBC mode for symmetric decryption of UCM firmware upgrades are approved modes

Use of the following algorithms and modes are not FIPS 140-2 approved: DES-XL, DVI-XL, DVI-SPFL, DVP-XL, SHA-1, AES MAC, HCA (Home Country Algorithm).

4 Security Rules

4.1 FIPS140-2 imposed Security Rules

This section documents the security rules used by the cryptographic module to implement the security requirements of a FIPS 140-2 Level 1 module.

1. The KVL 3000 Plus is placed in FIPS 140-2 Level 1 compliant mode by turning the FIPS option, located in the CONFIG menu, ON. Note that when toggling between FIPS modes (ON & OFF), the KVL shall erase all its keys in the database.

2. Upon detection of a low voltage power condition the cryptographic module shall erase the KPK, and consequently, all the TEKs and the KEKs would be unusable.

3. The module shall not at any time output any CSPs from any ports other than the "keyloading port".

4. The cryptographic module shall erase all plaintext keys, the KPK and critical information, when a tamper condition is detected.

5. Keys entered into the cryptographic module shall be accompanied by a valid key tag and unique logical ID. Also, Checksums will be calculated over each encrypted key to ensure the key's integrity throughout its lifetime. Each key in the KVL 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, or CKR/Keyset number – Identifiers indicating storage locations.

   Along with the encrypted key data, this information is stored in a key record that includes a Checksum over all of the fields to detect data corruption. When used or deleted the keys are referenced by Key ID/Algid, Physical ID, or CKR/Keyset.

6. The cryptographic module shall be capable of encrypting, using the KPK, all keys before they are stored in the unit's EEPROM. The cryptographic module shall also be capable of decrypting all keys stored in the EEPROM.

7. Upon the application of power or the receipt of a Reset command the Cryptographic module shall perform the following cryptographic related tests:
   - EEPROM Test where we validate the checksum over the entire EEPROM.
   - KPK Integrity Check, where KPK encrypts known value in the

EEPROM and compares to a known value, using the TDES algorithm.

- Flash Memory Test (32-bit Checksum test)

The self-tests and algorithm implementations are performed within the crypto engine (Universal Crypto Module). The UCM-performed self-tests are as follows:

- Power-up and on-demand tests
  - Cryptographic algorithm test: Each algorithm 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.
  - Firmware test: The firmware test calculates a checksum over the code. The checksum is calculated by summing over the code in 32 bit words. The code is appended with a value that makes the checksum value 0. The test passes if the calculated value is 0, otherwise it fails.
  - Critical Functions test.
  - LFSR Test: The LFSRs are tested by setting the feedback taps to a known value, loading them with known data, shifting the LFSR 64 times, then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails.
  - General Purpose RAM Test: The general purpose RAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the RAM. The test passes if all values read from the RAM are correct, otherwise it fails.

Powering the module off then on or resetting the module using the Reset service will initiate the power-up and on-demand self tests.

- Conditional tests
  - Firmware load test: A 24-bit MAC is generated over the UCM code when it is built using DES-CBC. Upon download into the module, the MAC is verified. If the MAC matches the test passes, otherwise it fails.
  - Continuous Random Number Generator test: The continuous random number generator test is performed on 3 RNGs within the module. The first is a hardware RNG which is used to seed the ANSI X9.31 DRNG and the maximal length 64-bit LFSR. The second is an implementation of Appendix C ANSI X9.31 which is used for key generation, and the third is a maximal length 64-bit LFSR which is used for IV generation. For each RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. Successive calls to any one of the RNGs 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.

8. After power-up tests are completed, the unit will perform role-based authentication using a password entry mode.

9. Firmware Integrity Test: The KVL supports loading its main firmware using a PCCard Flash Card. To authenticate the data, the KVL uses a DAC (Data Authentication Code) modeled after the FIPS approved method described in FIPS PUB 113 documentation (Computer Data Authentication). A 24-bit MAC is generated over the KVL firmware upgrade code when it is built using DES-CBC. The KVL host processor tests the firmware by calculating the checksum and comparing it against a known value programmed into the upgrade card.

10. If a KVL undergoes a firmware upgrade, it is no longer considered to be operating in a FIPS approved mode. To return to this mode of operation the Crypto Officer must turn on the FIPS config option again.

11. The cryptographic module shall support the Key Management Security Requirements for Type 3 Block Encryption Algorithms as described in Addendum A of the APCO Project 25 OTAR Protocol (TIA/EIA 102.AACA-A). The requirements dictate the security standards to be followed when transmitting Type 3 Key Management Messages and also the standards for encrypting Type 3 keys when sent as part of a KMM.

12. The KVL supports the following interfaces:
    - Data input interface
        a) RS 232 - Plaintext Data, Ciphertext Data, Key Management Data (target RSI and MNP), Encrypted Cryptographic Keys, Configuration Data
        b) PCMCIA - Plaintext Data, Ciphertext Data, Key Management Data (target RSI and MNP), Encrypted Cryptographic Keys, Configuration Data, firmware upgrades
        c) Keypad – Plaintext data and CSPs.
    - Data output interface
        a) Keyloading (MX) port - Plaintext Keys and Data, Key Management Data (target RSI and MNP), Encrypted Cryptographic Keys, Configuration Data
        b) RS 232 - Plaintext Data, Ciphertext Data, Key Management Data (target RSI and MNP), Encrypted Cryptographic Keys, Authentication Data(s) KVLRSI, KMFRSI and TargetRSI.
        c) PCMCIA - Plaintext Data, Ciphertext Data, Key Management Data (target RSI and MNP), Encrypted Cryptographic Keys, Authentication Data(s) KVLRSI, KMFRSI and TargetRSI.
        d) Display – Configuration and Key Management data, Plaintext Keys
    - Control input interface
        a) Keypad - Input Commands
    - Status output interface
        a) Display – status messages (text)

b) RS 232 – status codes
c) PCMCIA – status codes
d) MX Port – status codes

- Power interface
  a) 7.5V Main Battery – Powers entire KVL
  b) 3.0V Coin Cell Battery – Powers the Real Time Clock

The function of the various interfaces are as follows:
1. RS-232: This interface is used for downloads from the KMF.
2. MX: This interface is used to communicate with the targets. The target could be either a radio, or an infrastructure device or another KVL.
3. PCMCIA: This interface is used to upgrade the KVL code using a PCMCIA card, as well as communicate with external devices using a modem.
4. Keypad: This interface is used to enter keys as well as select the GUI options.
5. Power: This interface is used to provide power to the KVL.

13. The KVL inhibits all data output via the data output interface whenever an error state exists and during self-tests.

14. The KVL logically disconnects the output data path from the circuitry and processes when performing manual key entry, or key zeroization.

15. Authentication data and Secret cryptographic keys are entered through the Keypad.

16. The KVL supports a User role and a Cryptographic Officer role. The Cryptographic Officer role has a higher number of services.

17. The KVL re-authenticates a role when it is powered-up after being powered-off by using a 6 byte alpha-numeric (0-9 and A-F) password.

18. The KVL provides the following services not requiring a role:
    - Enter password
    - Initiate Self Tests.

19. In addition to services that do not require a role, the KVL provides the following services that do require one:

    - Manual Key Data Entry

- Manual Key Zeroization
- Transfer Key Variable
- APCO OTAR Store and Forward
- Privileged Store and Forward
- Change Active Keyset
- Change Password
- Zeroize selected keys
- Zeroize all keys
- Zeroize passwords
- Shutdown Crypto Module
- Extract Error and Action Log
- Clear Logs
- Program Update

20. The KVL implements all firmware using a high-level language, except the limited use of low-level languages to bootstrap module and enhance performance.

21. The KVL protects secret keys from unauthorized disclosure, modification and substitution.

22. The KVL denies access to the module's only plaintext secret key, the Key Protection Key, or KPK, which is used to encrypt the database.

23. The KVL provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within it. This is done by holding down 'Shift' while pressing the 'Enter' key.

24. The KVL supports the following FIPS approved algorithms:
    - DES
        a) OFB for symmetric encryption / decryption of digital voice, data, and Project 25 OTAR
        b) 1-Bit CFB for symmetric encryption / decryption of analog voice
        c) CBC for authentication of Project 25 OTAR
        d) ECB for symmetric decryption of Project 25 OTAR
        e) CBC for authentication of the KVL main code and the UCM code.

    - 3DES
        a) 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
        b) CBC for symmetric decryption of UCM firmware upgrades

    - AES-256

a) OFB for symmetric encryption / decryption of digital voice and data
b) CBC for authentication when used for Project 25 OTAR
c) ECB for symmetric decryption of Project 25 OTAR

25. The KVL conforms to all FCC requirements.

26. The KVL enters an error state if the Firmware 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 firmware to be loaded.

27. The KVL outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.

28. The KVL does not perform any cryptographic functions while in an error state.

4.2 Motorola Imposed Security Rules

1. The KVL does not support multiple concurrent operators.

2. The cryptographic module will continue to provide User Role and Crypto Officer Role services until the module has been powered down.

3. All cryptographic module services are suspended during key loading.

4. Upon detection of tamper, the cryptographic module shall erase all CSPs.

5 Crypto Officer Guidance

5.1 Administration of the KVL in a secure manner

In order to ensure that the KVL is operating in FIPS approved manner, the Operator is expected to turn ‘On’ FIPS mode *and* enable passwords for the ‘User’ and ‘Crypto Officer’ roles. Please refer to the KVL 3000 Plus User Guide for detailed information on Crypto Officer guidance.

6 User Guidance

6.1 Approved Security Functions, Ports, and Interfaces available to Users

Some KVL services are available to the KVL User. These services are listed in section 9 of this document. Please refer to the KVL 3000 Plus User Guide for detailed information on User Guidance.

6.2 User Responsibilities necessary for Secure Operation

The user is expected to enable passwords when operating in FIPS-approved mode. Passwords are enabled through the KVL user interface.

7 Identification and Authentication Policy

The KVL uses unique passwords to authenticate the User and the Crypto Officer. The password is made up of 6 alpha-numeric (0-9 and A-F) characters which is the equivalent of a 24-bit password with 16,777,216 possible values. The passwords are cleared (i.e. disabled) during manufacturing. They may be initialized/changed at the discretion of the user.

Role	Authentication Type	Authentication Data Required
User	Role-Based	6 BYTE Password
Crypto Officer	Role-Based	

8 Physical Security Policy

The KVL uses a tamper-detect circuit that triggers a tamper detection mechanism whenever module's housing is removed while operating under FIPS approved mode. Any detection of a physical intrusion will cause all CSPs to be deleted immediately if the module is still powered up, or at next powerup if it is not powered up. No Operator maintenance is needed for the physical security mechanisms.

Physical Security Mechanism	**Maintenance Needed**
Tamper Detect Circuit	None

9 Access Control Policy

9.1 KVL Supported Roles

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

- the User Role,
- the Cryptographic Officer (CO) Role

9.2 KVL Services

- Enter Password: Enter an alpha-numeric password through the keypad. Done on powerup.
- Manual Key Data entry: Plaintext key data may be manually entered through the keypad. Available in CO mode only.
- Manual Key Zeroization: Keys may be deleted from the database. Available in CO mode only.
- Transfer Key Variable: Transfer Plaintext key variables and/or zeroize key variables from the Key Database to a target device through the MX port. The target could be either a radio, or an infrastructure device or another KVL. Available in both, User as well as CO roles.
- APCO OTAR Store and Forward: Download SAF data from a KMF and transfer SAF KMMs to target units. The target could be either a radio, or an infrastructure device or another KVL. Available in both, User as well as CO roles. Data could be clear (in Red SAF) or encrypted (Black SAF). Red SAF is only used to transfer keys through the MX port to a connected target.
- Privileged Store and Forward: Delete SAF data downloaded from KMF. Available only in CO role.
- Change Active Keyset: Modify the currently active keyset used for selecting keys by PID or CKR. Available in User and CO Roles.
- Change Password: Modify the current password used to identify and authenticate the User and CO Roles. Available to User and CO Roles. Note: User can only modify ‘User’ password.
- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, firmware test, and critical functions test. Initiated by module reset or transition from power off state to power on state. Available without a Role.
- Zeroize Selected Keys: Zeroize selected key variables in a target by Physical ID (PID) or Common Key Reference (CKR). Available to User and CO Roles.
- Zeroize all keys: Zeroize all keys in a target. The target could be either a radio, or an infrastructure device or another KVL. Available in User and CO Roles.

- Zeroize All Keys and Password: Zeroizes all keys and CSPs in the key database. Disables the passwords. Allows Operator to gain controlled access to the module if the password is forgotten. Available in User and CO roles.
- Shutdown Crypto Module: Prepares module for removal of power. Available in User and CO roles.
- Extract Action and Error Logs: Provides detailed history of success and failure events. Available in User and CO roles.
- Clear Log: Clears history of error events. Available to User and CO Roles.
- Program Update: Update the module firmware.

9.3 Critical Security Parameters (CSPs)

CSP Identifier	Description
Key Protection Key (KPK)	TDES Key used to encrypt the database and other non-volatile parameters. Randomly generated. Generated on Initial firmware programming, or on every firmware upgrade, or successful powerup after erasure. Erased when any of the following occurs: physically tampering with the KVL, no power for more than a minute, resetting the KVL.
Plaintext Traffic Encryption Keys (TEKs)	Keys used for data encryption. Algorithms, as purchased and specified by the user. Entered by the Operator through the keypad, or received through the MX port during Store and Forward. Erased on KPK loss or active Operator deletion.
Plaintext Key Encryption Keys (KEKs)	Keys used for encryption of keys in during Store and Forward (SAF)). Algorithms, as purchased and specified by the user. Entered by the Operator through the keypad, or received through the MX port during Store and Forward. Erased on KPK loss or active Operator deletion.
Passwords	User and CO passwords entered during Operator authentication. Created by the Operator. Hash of the password (and not the password itself) is stored in the EEPROM. Erased on resetting the KVL or Operator deletion.
KVL Main Plaintext MAC Key	DES algorithm key used for authentication of KVL Main firmware upgrade. Stored in non-volatile memory
UCM Plaintext MAC Key	DES algorithm key used for authentication of UCM firmware upgrade. Stored in non-volatile memory

9.4 CSP Access Types

CSP Access Type	Description
Retrieve key	Decrypts encrypted TEKs or KEKs in the database using the KPK and returns plaintext version
Store key	Encypts plaintext TEKs or KEKs using the KPK and stores the encrypted version in the database
Invalidate Key	Marks encrypted TEK or KEK data in key database as invalid
Create KPK	Generates and stores new KPK
Store Password	Hashes Operator password and stores it in the database

9.5 Critical Security Parameter (CSP) Services and Access

	CSP Access Operation					Applicable Role		
Operator Service	Retrieve TEK/KEK	Store KEK/TEK	Erase TEK/KEK	Create/Modify KPK	Store Password(hash	User Role	Crypto Officer Role	No Role Required
1. Enter Password								X
2. Manual Key Data Entry		X					X	
3. Manual Key Zeroization	X		X				X	
4. Transfer Key Variable	X					X	X	
5. APCO OTAR Store and Forward	X	X	X			X	X	
6. Privileged Store and Forward			X				X	
7. Change Active Keyset	X					X	X	
8. Change Password					X	X	X	
9. Initiate Self-Tests								X

	CSP Access Operation					Applicable Role		
10. Zeroize Selected Keys	X		X			X	X	
11. Zeroize All Keys			X			X	X	
12. Zeroize All Keys and Passwords			X	X	X	X	X	
13. Shut Down Crypto Module						X	X	
14. Extract Action and Error Logs						X	X	
15. Clear Log						X	X	
16. Program Update			X	X	X	X	X	

10 Mitigation of Other Attacks Policy

The KVL 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.