KVL 3000 Plus Security Policy

COMMERCIAL, GOVERNMENT, AND INDUSTRIAL SOLUTIONS SECTOR

Secure Design Center

Version 01.01.04

Last Revision: February 1, 2002

Repository Information

Location: /vobs/kvl/DOCS/KVL3000 Plus/FIPS
Filename: KVL3000 Plus_Security_Policy

Revision History

01.00.00	11/20/97	Larry Murrill	Initial Creation
01.00.03	09/21/98	Larry Murrill	Add Hard Reset Procedure
01.00.04	10/01/98	Larry Murrill	Add Rule stating how to put the KVL into FIPS mode.
01.00.05	10/02/98	Larry Murrill	Remove the reference to the USK in rule 11.
01.00.06	10/13/98	Larry Murrill	Add Passwords to list of SRDI in section 4.
01.00.07	11/19/98	Larry Murrill	Make Wording Changes And Additions for Roles and Services and Security Rules.
01.01.00	09/23/99	Raed Hafez	Make Changes according to CygnaCom's Comments.
01.01.01	06/04/01	Larry Murrill	Make Minor Change to support re-validation effort for KVL3000 Plus
01.01.02	10/12/01	Arun Victor	Mentioned Users' ability to modify Operator Password
01.01.03	02/01/02	Mohamad Bouji	Included NIST Review Changes
01.01.04	04/02/02	Mohamad Bouji	Added AES Crypto Information where Needed

Table of Contents

1 Introduction

1.1 Purpose

This document describes the FIPS 140-1 security policy requirements for Motorola's Land Mobile Products Sector's Key Variable Loader.

1.2 Definitions, Acronyms, Abbreviations

AES	Advanced Encryption Standard
DES	Data Encryption Standard
EEPROM	Electrically Erasable Programmable Read Only Memo
IV	Initialization Vector
KVL	Key Variable Loader
RAM	Random Access Memory
SRDI	Security Related Data Items

1.3 References

2 Roles and Services

The KVL supports a Crypto Officer, User, or Maintenance role during operation.

While in the Crypto Officer role, all of the KVL's configuration parameters can be edited and all of its services can be accessed. While in the User role, only key loading services can be accessed, no editing of SRDI is allowed with the exception of the Operator Password. Lastly, the Maintenance role provides a means to replace the coin-cell battery and perform firmware upgrades.

The KVL supports role based authentication, using password entry, as a means to select a role when the KVL is first powered on. The unit's *Supervisor mode* serves as the *Crypto Officer* role while the unit's *Operator mode* serves as the *User role*.

Both the Supervisor and the Operator can perform the following cryptographic services: Key load, Request for keys from a central KMF.

The Supervisor can perform the following additional cryptographic services: Key zeroization, Key entry, and Modification of SRDI parameters.

3 Security Rules

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

1. The KVL 3000 Plus is placed in FIPS 140-1 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 all plaintext keys and critical data.
3. The module shall not at any time output any security related data items (SRDIs) 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. It shall also reset the KG.
5. Keys entered into the cryptographic module shall be accompanied by a valid key tag and unique logical ID. Also, CRCs will be calculated over each encrypted key to ensure the keys integrity throughout its lifetime.
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 (includes Key Database test)
   - Flash Memory Test
   - Crypto Engine Self Test (AES, DES and TDES Implementations)

   The self-tests and algorithm implementations are performed within the ASTRO Subscriber Encryption Module (Universal Crypto Module).
8. After power-up tests are completed, the unit will perform role-based authentication using a password entry mode.
9. If a KVL3000 performs a software upgrade, the KVL is no longer considered to be operating in a FIPS approved mode. To return to this mode of operation the Supervisor must perform a RESET, to destroy the NON-FIPS compliant keys, and turn on the FIPS config option again, which was reset to OFF during the RESET.

4 Security Related Data Items

There are four types of security related data items (SRDIs). These are:

- Traffic Encryption Keys (TEK)
- The Key Encryption Keys (KEK).
- The Key Protection Key (KPK).
- KVL’s Supervisor and Operator Passwords.

5 Security Level Objectives

The cryptographic module meets the requirements applicable to Level 1 security of FIPS 140-1 and Level 1 physical security. If passwords are enabled, the KVL operates at Level 2 for roles and services. If passwords are not enabled, the KVL operates at Level 1 for roles and services.

6 Services to SRDI Relationships

The following describes the FIPS approved services provided by the module and those services' use of the existing SRDIs:

1. **Load Key :** When the cryptographic module is instructed to load a selected key, that key is decrypted using the KVL's KPK, packaged/concatenated with that keys associated algorithm ID and Key ID, and it is transmitted to the intended cryptographic target.
2. **TEK/KEK Entry :** Once a key has been fully entered into the cryptographic module, it is associated with an algorithm ID and a Key ID, encrypted using the KVL's KPK, and stored in the EEPROM.
3. **TEK/KEK Zeroization :** Each Traffic Encryption Key and Key Encryption Key can be actively zeroized by the crypto officer.

7 Operator Access

The following is a table of what access an operator has to the critical security parameters while performing one of the cryptographic functions: Keyload, KMF Key Request, Key Zeroization, Key Entry, SRDI Modifications. Note that the only operators authorized are the persons in the User or Crypto Service Roles. Also, the User is allowed to modify his/ her own password. This is the only SRDI modification allowed by the User.

	Key Load	KMF/KMC Key Req	Key Zeroization	Key Entry	SRDI Mods
Crypto Officer	X	X	X	X	X
User	X	X			X (Opera tor pass word only)