MOTOROLA

KVL 3000 Security Policy

LAND MOBILE PRODUCTS SECTOR
Radio Network Solutions Group

Version 01.00.05

Last Revision: October 2, 1998

Repository Information

Location: /vobs/kvl/doc/fips
Filename: KVL_Security_Policy

Revision History

Revision	Date	Author	Comments
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	LarryMurrill	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.

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

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 Crypo 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. Lastly, the Maintenance role provides means to perform diagnostics, coin-cell battery replacement.

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, 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 KVL3000 is placed in FIPS 140-1 Level 1 compliant mode by turning the FIPS option, located in the config menu, ON.
2. If a KVL3000 receives keys from a Motorola KMC, 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 HARD RESET, to destroy the NON-FIPS compliant keys, and turn on the FIPS config option again, which was reset to OFF during the HARD RESET.
3. A SUPERVISOR may prevent an OPERATIOR from inadvertently downloading keys from a KMC into a FIPS-compliant KVL by turning off the KMC option in the config menu. With this option turned off, KMC key downloads are prohibited.
4. Upon detection of a low voltage power condition the cryptographic module shall erase all plaintext keys and critical data.
5. The module shall not at any time output any security related data items (SRDIs) from any ports other than the "keyloading port".
6. The cryptographic module shall erase all plaintext keys, the USK and critical information, when a tamper condition is detected. It shall also reset the KG. Please refer the "KVL3000 FIPS 1401-1 Certification" section VE05.01.02 for details.
7. 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.

8. The cryptographic module shall be capable of encrypting, using the USK, 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.
9. 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
10. After power-up tests are completed, the unit will perform role-based authentication using a password entry mode.
11. An operator in the supervisor mode shall do a HARD RESET to zeroize the PASSWORDS before the Maintenance role is entered.

4 Security Related Data Items

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

- Traffic Encryption Keys (TEK)
- The Key Encryption Keys (KEK) (Where a USK is the KVL's master KEK used to encrypt all TEKs & KEKs stored in the cryptographic module's EEPROM).
- KVL's Supervisor and Operator Passwords. (Can only be entered and modified by the Supervisor)

5 Security Level Objectives

The cryptographic module meets the requirements applicable to Level 1 security of FIPS 140-1 and Level 1 physical security.

6 Services to SRDI Relationships

The following describes the 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 USK, packaged/concatenated with that keys associated key tag+logical ID and 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 a key tag+logical ID, encrypted using the KVL's USK, and stored in a pre-specified (by user) location in the EEPROM.
3. **USK Entry :** Once the USK has been fully entered into the cryptographic module, it is stored as plaintext in a 64-bit volatile shift register.
4. TEK/KEK/USK Zeroization : Each Traffic Encryption Key and Key Encryption Key, Including the USK, 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

	Key Load	KMF Key Req	Key Zeroization	Key Entry	SRDI Mods
Crypto Officer	X	X	X	X	X
User	X	X			