KVL 3000 Security Policy

LAND MOBILE PRODUCTS SECTOR
Radio Network Solutions Group

Version 01.01.01

Last Revision: November 7, 1999

Repository Information

Location: /vobs/kvl/DOCS/KVL3000_APCO/FIPS
Filename: KVL_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	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.
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 CygnaComÕs Comments.
01.01.01	11/08/99	Larry Murrill	Make Changes according to NIST Comments.

Table of Contents

1Introduction 4
1.1Purpose 4
1.2Definitions, Acronyms, Abbreviations 4
1.3References 4
2Roles and Services 5
3Security Rules 5
4Security Related Data Items 6
5Security Level Objectives 6
6Services to SRDI Relationships 7
7Operator Access 7

1 Introduction

1.1 Purpose

This document describes the FIPS 140-1 security policy requirements for MotorolaÕs Land Mobile Products SectorÕs 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

KMC Key Management Controller

KMF Key Management Facility

UKEK Unique Key Encryption Key - The UKEK is used to encrypt keys transmitted from the KMF to the KVL. During system initialization a Unique KEK is programmed into each KVL and that UKEK is associated with that KVL within the KMFÕs database. Once the system is fully initialized, each UKEK can then be used to communicate with only ONE KVL. No other KVL will receive keys encrypted with this UKEK. The KMF uses the concept of the UKEK to created a secure link between itself and any individual unit (KVL) under its management.

USK Unique Shadow Key - The USK is used to encrypt keys transmitted from the KMC to the KVL. During system initialization a USK is programmed into the KVL and that USK is associated with that KVL within the KMCÕs database. Once the system is fully

initialized, each USK can be used to communicate with only ONE KVL. No other KVL will receive keys encrypted with this Unique Shadow Key. The KMC uses the concept of the USK to created a secure link between itself and any individual unit (KVL) under its management.

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 KVLÕs 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 a means to replace the coin-cell battery.

The KVL supports role based authentication, using password entry, as a means to select a role when the KVL is first powered on. The unitÕs *Supervisor mode* serves as the *Crypto Officer* role while the unitÕs *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. 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 Òkeyloading portÓ.
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 unitÕs 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
   - ¥ DES Known Answer Test
8. After power-up tests are completed, the unit will perform role-based authentication using a password entry mode.
9. The cryptographic module shall erase all plaintext keys, the KPK and critical information, when the maintence role is entered.
10. 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).
- KVLÕs 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 FIPS 140-1 Level 1.

6 Services to SRDI Relationships

The following describes the FIPS approved services provided by the module and those servicesÕ 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 KVLÕs 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 KVLÕs 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

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