KMF CryptR User Guide

MARCH 2017

MN003313A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003313A01-A	Original release of the *KMF CryptR User Guide*	November 2016
MN003313A01-B	This release contains the following updates: • Added Caution to Login Session and User Authentication on page 34. • Updated Upgrading the KMF CryptR Software Through TFTP on page 40.	March 2017

This page intentionally left blank.

Contents

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About KMF CryptR User Guide

This manual provides instructions on installing, configuring, and using the KMF CryptR hardware and software. Information on troubleshooting and maintenance is also included.

The KMF CryptR is considered a Field Replaceable Unit (FRU), and when determined to be faulty, it may be replaced with a defect-free device to bring the equipment back to normal operation. Contact the Motorola Solutions Support Center (SSC) for replacement or repair directions.

What Is Covered In This Manual?

This manual contains the following chapters:

- KMF CryptR Description on page 21 describes the major components and features of the KMF CryptR.
- KMF CryptR Installation on page 27 provides instructions for installing the KMF CryptR hardware and software.
- KMF CryptR Configuration on page 33 provides instructions for configuring the KMF CryptR.
- KMF CryptR Operation on page 39 provides instructions for operating the KMF CryptR after it is installed and configured.
- KMF CryptR Maintenance on page 45 provides maintenance procedures for the KMF CryptR.
- KMF CryptR Troubleshooting on page 47 provides troubleshooting procedures for the KMF CryptR.
- KMF CryptR FRU/FRE Information on page 49 provides information about Field Replaceable Units (FRUs) and replacement parts for the KMF CryptR.
- KMF CryptR Reference on page 51 provides supplemental reference information for the KMF CryptR.
- KMF CryptR Disaster Recovery on page 53 provides disaster recovery information for KMF CryptR.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).

Table continued…

Related Information	Purpose
ASTRO® 25 *System Overview and Documentation*	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Public Safety LTE *System and Documentation Overview*	Provides an introduction to the overall Public Safety Long Term Evolution (PS LTE) system offering from Motorola Solutions, and describes the associated documentation.
KVL 3000 Plus Key Variable Loader User's Guide (6881132E29)	This manual provides information for the KVL 3000 and KVL 3000 Plus Key Variable Loader.
KVL 4000 Key Variable Loader ASTRO 25 User Guide	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others. This manual describes the ASTRO® 25 operating mode, applicable to ASTRO® 25 systems and PS LTE systems.
KVL 4000 FLASHport Upgrade User Guide	Provides instructions for upgrading the Key Variable Loader (KVL), radios, and other target devices. It also provides instructions for applying security settings on the KVL, installing, and activating VPN software, as well as provides troubleshooting information.
Key Management Facility User Guide	Provides descriptive and procedural information about the Key Management Facility (KMF) including a description of where the KMF can be found, a description of KMF encryption key management, as well as procedures on installation, configuration, operation, upgrade, troubleshooting, and FRU/FRE replacement.
KVL 3000 Plus Key Variable Loader Secure Module Software Upgrade Manual (6881132E26)	This manual provides step-by-step instructions for performing secure modules' upgrades with KVL 3000 Plus.

Chapter 1

KMF CryptR Description

This chapter contains a high-level description of the KMF CryptR and its components and accessories.

1.1 KMF CryptR Overview

The Key Management Facility (KMF) CryptR 2 Unit is a hardware device connected by Ethernet to the KMF Server to provide encryption services for the KMF. It securely stores the KMF master keys and uses them to perform encryption operations for both key storage and OTAK/OTEK message generation. The KMF CryptR is responsible for encrypting and decrypting key material and key management messages.

When keys are defined by a KMF client or when keys are loaded by file, the KMF CryptR encrypts the key material using the master key associated with the key's algorithm. The encrypted key material is then sent to the KMF server for secure storage. When key material is being retrieved from the KMF server, the KMF CryptR decrypts the traffic using the appropriate master key.

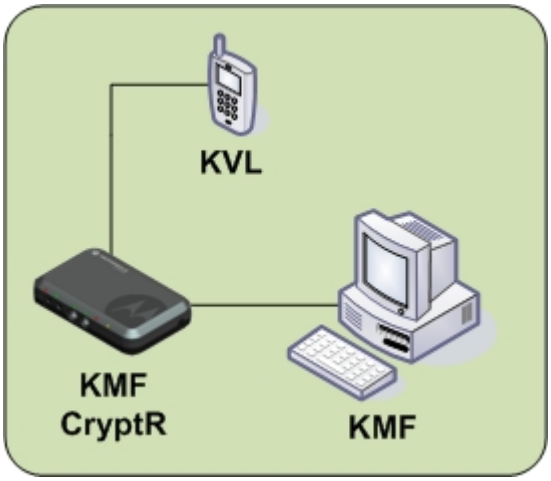
When a target device needs a key update, the KMF CryptR receives encrypted key material from the KMF server. Next, the KMF CryptR decrypts the key material with the KMF master key. The KMF CryptR then encrypts the key material with the target device's key encrypting key (KEK), generates a further encrypted Key Management Message (KMM) with the target device's traffic encryption key (TEK), and sends the encrypted KMM to the KMF server. The KMF server then sends the KMM over the appropriate interface to the target device. For KMMs that do not include key material, the KMF CryptR can still encrypt the KMM, depending on the message.

The KMF CryptR has a connector port for direct connection to a KVL. The KVL can be used to load keys into the KMF CryptR. The KMF CryptR stores master keys in battery-backed memory while other keys are routed to the KMF Server for storage.

The KMF CryptR hardware has a tamper detection mechanism. When the sealed, pressure-sensitive housing of the KMF CryptR is opened or tampered with, the KMF CryptR zeroizes all stored key material. The KMF CryptR also has a button for hard key zeroization. This button can be used, even when the server and/or KMF CryptR is not powered up, to quickly erase all key material stored on the KMF CryptR. When keys have been zeroized, the KMF CryptR resets and enters a nonfatal error state (causing the status LED to turn red). This indicates that the key loading procedure must be performed for each master key. The KMF CryptR is field replaceable and has a replaceable on-board lithium battery.

The following figure shows the KMF CryptR connections. To enable cryptographic services for the KMF Server, the KMF CryptR is connected to the KMF Server using an Ethernet crossover cable. When the KMF CryptR needs to be loaded with a master key or needs to accept keys on behalf of the KMF Server, a KVL is connected to the KMF CryptR using a key loading cable.

Figure 1: KMF CryptR - Connections



1.2
KMF CryptR Components

Table 1: KMF CryptR Components

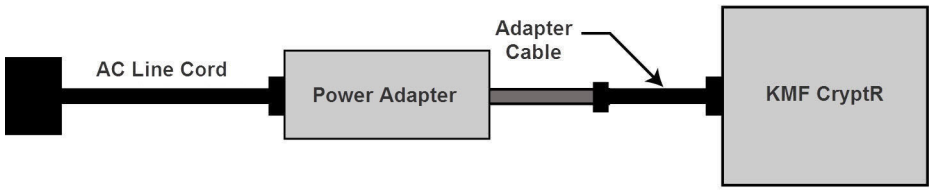
Component	MSI Kit Number	Description
KMF CryptR	SQM01SUM0222A	Provides encryption services for the KMF.
Basic software	CA00143AG	KMF CryptR software
DES-OFB Encryption Kit	CA00143AF	Encryption Algorithm Kit (optional)
DES XL Encryption Kit	CA00144AE	Encryption Algorithm Kit (optional)
DVI XL Encryption Kit	CA00145AM	Encryption Algorithm Kit (optional)
DVP XL Encryption Kit	CA00146AN	Encryption Algorithm Kit (optional)
AES Encryption Kit	CA00182AV	Encryption Algorithm Kit (optional)
CryptR 2 USB Driver CD	KC137C01K00007120	Supports USB driver
AC Line Cord for North America	CA00140AA	Provides 120 V AC to Infrastructure Power Adapter.
AC Line Cord for Europe	CA00140AB	Provides 120 V AC to Infrastructure Power Adapter.
AC Line Cord for UK	CA00140AC	Provides 120 V AC to Infrastructure Power Adapter.
AC Line Cord for Australia	CA00140AF	Provides 120 V AC to Infrastructure Power Adapter.
Power Adapter	0171925M01	Converts 120VAC to 12VDC

Table continued…

Component	MSI Kit Number	Description
Adapter Cable	DLN6739A	Allows Power Adapter to connect to the KMF CryptR Power Connector
Ethernet CrossOver w/ Sealing Boots	DLN6737A	Allows Red-side Communications
Mini USB Cable	DLN6735A SKN6371C	Used for loading configuration parameters
Keyload Cable	0182297T12	Used for key loading
Velcro PS Strap	42009268001	Clamps Power Adapter on Mounting Tray
Rack Mount Kit	TKN9285A	For mounting the unit in a rack

1.3 KMF CryptR Power Connections

Figure 2: Power Connections



1.4 KMF CryptR Physical Description

The front panel of the KMF CryptR consists of the following items (from left to right):

- Erase button
- Reset button
- Key load ports (with protective covers)
- Ready/Link LED
- Tx Clear LED
- Alarm LED
- Status LED
- Power LED

Figure 3: KMF CryptR Front Panel

The port covers are color-coded to indicate network interface usage (red for the red network, black for the black network).

The rear panel of the KMF CryptR consists of the following items (from left to right):

- Power Jack
- Two RJ45 ports (with protective covers)
- Two USB ports (with protective covers)

Figure 4: KMF CryptR Rear Panel

The port covers are color-coded to indicate network interface usage (red for the red network, black for the black network).

1.5 KMF CryptR Hardware Specifications

This section contains specifications for the KMF CryptR hardware.

1.5.1 KMF CryptR Security Specifications

Table 2: KMF CryptR Security Specifications

Characteristic	Value
FIPS	Federal Information Protection Standard 140-2 Level 2 (pending)

1.5.2 KMF CryptR Electrical and Physical Specifications

Table 3: KMF CryptR Electrical and Physical Specifications

Characteristic	Value
Power	12 V DC @ 1.5A

Table continued…

Characteristic	Value
Interfaces	2x 10/100 RJ45 Ethernet, Key Fill, USB Host Port, Device Port with Mini USB Connector
Dimensions ca.	1.5 x 5.7 x 4.7 in (39 x 145 x 120 mm)
Weight ca.	1.75 lbs. (800 g)

1.5.3
KMF CryptR Environmental Specifications

Table 4: KMF CryptR Environmental Specifications

Characteristic	Value
Operating Temperature	-30°C to +60° C
Storage Temperature	-40°C to +85° C
Humidity	Up to 90% RH at Upper Limit Operating Temperature
Environmental Specification	MIL 810F

1.5.4
Compliant Regulatory Standards

Table 5: Compliant Regulatory Standards

Characteristic	Value
CE Standards	EN55022:2006 / EN55024:1998 + A1:2001 + A2:2003
EMC Standards	• EN61000-3-2:2006 / EN61000-3-3:1995 + A1:2001+ A2:2003 • EN61000-4-2:1995 + A1:1998 + A2:2001 • EN61000-4-3:2006 + A1:2008 • EN61000-4-4:2004 • EN61000-4-5:2006 • EN61000-4-6:2007 + Corrigendum August 2007 • EN61000-4-11:2004
FCC Standards	• FCC Part 15.107 Class B • FCC Part 15.109 Class B
Energy Efficiency Standard	EC Regulation 278/2009
UL	60950-1

1.6
KMF CryptR Security Features

The KMF CryptR hardware and software have the following security features.

Tamper Detection

The KMF CryptR instantly destroys the encryption keys stored in it upon detecting tampering. Tamper events require the administrator to log on to the KMF CryptR to acknowledge and clear the tamper event by entering: `errorlog retrieve`

Erase Button

The KMF CryptR features a key erase button that the operator can press to destroy all encryption keys stored in the KMF CryptR.

FIPS mode

The KMF CryptR reports the current FIPS level it is operating in.

Strong Password Validation

The KMF CryptR enforces strong password rules. Too many failed logon attempts result in the KMF CryptR resetting its passwords to their default values and erasing all keys.

For more information, see Security Configuration Commands on page 37.

Chapter 2

KMF CryptR Installation

This chapter provides instructions for installing the KMF CryptR hardware and software.

2.1 Installing and Configuring the KMF CryptR

Process:

1. Unpack the KMF CryptR. See Unpacking the KMF CryptR on page 27.
2. Optional: Install the hardware (the battery is pre-installed). See Mounting the KMF CryptR on page 28.
3. If not already connected, connect the KMF CryptR to the power source and verify that the Power LED is lit.
4. Initiate a connection to the KMF CryptR. See Initiating a Connection to the KMF CryptR on page 33.
5. Log on to the KMF CryptR as `user` and change the default password. Ensure that the password matches the password on the KMF Server.

   For more information, see Login Session and User Authentication on page 34.
6. Log on to the KMF CryptR as `admin` and change the default password. Ensure that the password matches the password on the KMF Server.

   For more information, see Login Session and User Authentication on page 34.
7. Configure KMF CryptR IP addresses. See Configuring KMF CryptR IP Addresses on page 34.
8. Optional: If your organization has a log-on banner that you want to display upon KMF CryptR log-on, change the default log-on banner. See Service Configuration Commands on page 36.
9. Connect the KMF CryptR to the KMF Server. See Connecting the KMF CryptR to the KMF Server on page 32.

   NOTICE: Master Key(s) are loaded into the KMF CryptR as part of the KMF Server installation and configuration process described in the *Key Management Facility User Guide*.

2.2 Unpacking the KMF CryptR

Procedure:

1. Open the box and pull back the top.

   The following items are visible at the top of the box:

   - Power supply (inside the white box)
   - AC line cord (coiled in the visible plastic bag)
   - Power cable (in a smaller plastic bag under the bag containing the AC line cord)

- four (4) self-tapping fasteners (in another small plastic bag under the bag containing the AC line cord)

2 Remove the items described in step 1, then remove the flat foam pad found under them.

The KMF CryptR unit is visible, surrounded by protective padding.

3 Remove the KMF CryptR from the box.

2.3 Mounting the KMF CryptR

When and where to use: Use this procedure if you want to install the KMF CryptR in a rack.

Figure 5: KMF CryptR in Rack Mount

NOTICE: The photos in this procedure show the installation of two KMF CryptR units. The number of units may differ, depending on the configuration.

Procedure:

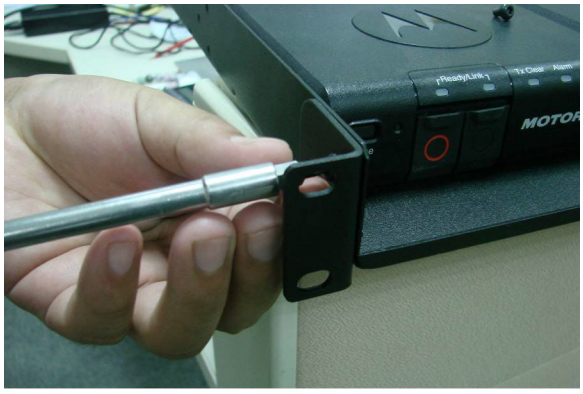
1 Gather the tray and the units to be mounted on the tray in a convenient location of your choice.

2 Insert mounting screws into the tray.

Figure 6: Inserting Mounting Screws Into Tray

3 Attach supporting brackets to the sides of the rack.

Figure 7: Attaching Supporting Brackets



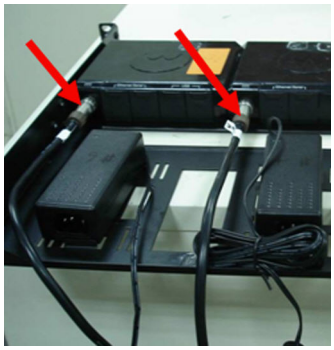
4 Place the KMF CryptR units on the front side of the tray.

Figure 8: KMF CryptR Units Mounted on Tray

5 Turn the tray so that the front side and the mounted units face away from you.

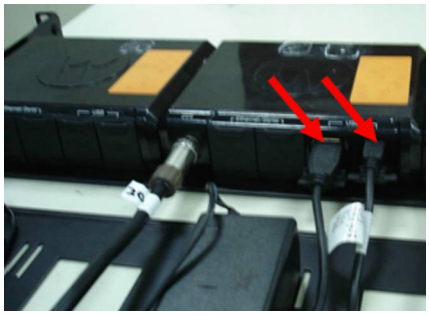
6 Insert an adapter cable into the port on the rear of each KMF CryptR unit and place power supply unit on the tray.

Figure 9: Cables Plugged Into Ports



7 Insert the USB and Mini USB cables into the appropriate ports on each KMF CryptR unit.

Figure 10: USB and Mini USB Cables Inserted



NOTICE: The USB cable is not needed for operation of the unit.

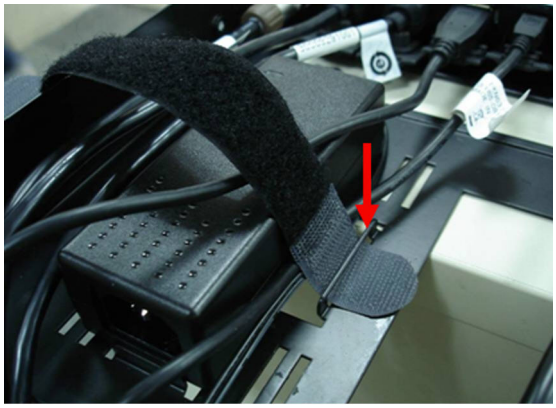
8 Insert the Ethernet cable into the red port on each KMF CryptR unit.

Figure 11: Attaching Ethernet Cable to KMF CryptR

IMPORTANT: Ethernet cables provided by Motorola Solutions for use with the KMF CryptR have a special rubber boot attached to the connector. This is required to provide the proper seal around the connector. When plugging in these cables, make sure that the rubber boot is properly aligned with the KMF CryptR housing.

9 Secure the power supply units with the straps provided and tighten the straps.

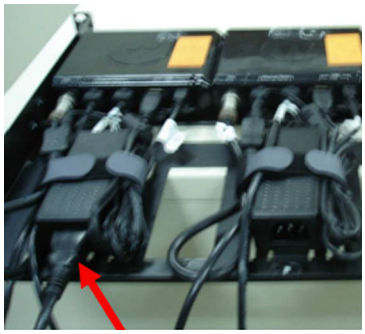
Figure 12: Power Supply Secured



10 Verify that all cables are connected.

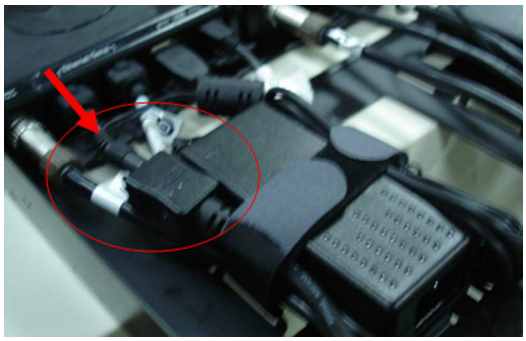
11 Insert the AC line cords.

Figure 13: AC Line Cords Inserted



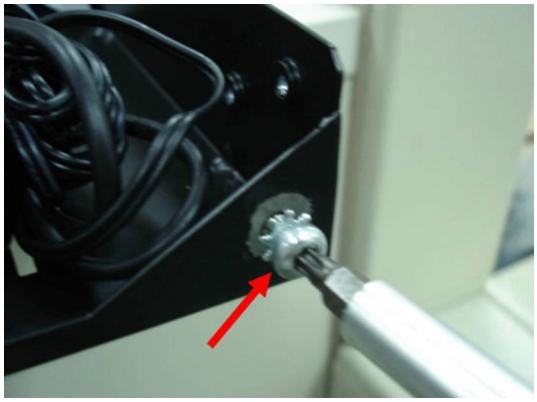
12 Connect the AC line cords to the adapter cables.

Figure 14: AC Line Cords Connected



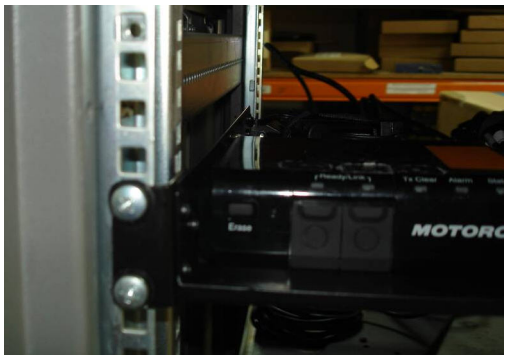
13 Insert the cold lug screw.

Figure 15: Inserting Lug Screw



14 Attach both ends of the tray to the rack.

Figure 16: Tray Attached (Left End Shown)



2.4 Connecting the KMF CryptR to the KMF Server

Procedure:

1. If not already connected, on the KMF CryptR, connect the Ethernet crossover cable to the Red Ethernet port (see Figure 4: KMF CryptR Rear Panel on page 24).
2. Perform one of the following actions:
   - For the High/Mid Tier KMF, connect the cable to the Secondary NIC port on the KMF Server.
   - For the Small Fleet KMF, connect the cable to the Primary Ethernet port on the KMF Server PC.

IMPORTANT: If your KMF Server PC has only one Ethernet port, always use this port to connect the KMF CryptR.

Chapter 3

KMF CryptR Configuration

This chapter contains configuration information for the KMF CryptR.

3.1 Initiating a Connection to the KMF CryptR

To connect to the KMF CryptR, use a computer running Microsoft Windows and a data cable with a mini-USB data connector. The cable is available as an orderable option. For more information, see Table 1: KMF CryptR Components on page 22.

Procedure:

1. Connect the computer's USB port and the KMF CryptR unit's mini-USB port using the data cable with a mini-USB connector.
2. Power on the KMF CryptR if it is not already on.
3. When the KMF CryptR is used with a new Microsoft Windows computer for the first time, a Windows wizard prompts you for the device driver location. Perform the following actions:
   a. Choose the option of installing the driver from a specific location.
   b. Insert the *CryptR 2 Support Software* CD into the CD/DVD drive and point to it as the driver location.

   After the initial installation of the driver, if your Windows computer shows an error message during its initial communication to the KMF CryptR, then reboot your computer.

   The `Motorola_CryptR2.inf` drive file is found and installed.
4. To confirm that the installation was successful, open the Device Manager and verify that `CryptR2` device (probably COM3) appears under **Ports (COM and LPT)**.
5. Start a terminal emulator program and configure it to use the COM port that the KMF CryptR is connected to. Use the following settings:
   - Baud Rate: 9600
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
6. Ensure that the serial terminal program is started **after** the KMF CryptR is powered up. If you need to power-cycle the KMF CryptR while it is being configured, or if you are finished configuring one unit and are about to configure another one, then close the serial terminal program before cycling power of the KMF CryptR or before unplugging one and plugging in another. Most Windows-based serial terminal programs are unable to handle an unplugged USB device, hence they need to be closed and reopened.

   Many serial terminal programs have a *disconnect* feature that can also be used when disconnecting and reconnecting the KMF CryptR. Ensure that the terminal program is in the disconnected state when reconnecting a KMF CryptR.

3.2 Login Session and User Authentication

This section describes the accounts used for log-in session and user authentication.

The administrative log-in names are `user` and `admin`.

- The `user` account is only used to change the `user` password.
- The `admin` account is used to change the `admin` password and to configure the KMF CryptR.

The default password for `user` and `admin` is `CryptrAdmin12345`.

Upon initial log-in, you are prompted to change the default password to a password that conforms to information assurance guidelines. This enables the KMF Server to connect to the KMF CryptR. For more information about the policies that apply to your system, contact your system administrator.

Passwords on the KMF Server and KMF CryptR have to match. Do not connect the KMF CryptR to the KMF Server until the passwords match. To change the passwords on the KMF Server, see "Changing KMF CryptR Embedded Passwords on the KMF Server and KMF Standby Server" in the *Key Management Facility User Guide*.

Since `user` can only change the `user` password, and `admin` can only change the `admin` password, each password must be changed independently.

After verifying the `admin` log-in name and password, the KMF CryptR displays a command prompt of `CRYPTR>`. The KMF CryptR displays the prompt after each successful or unsuccessful command, until you log out.

If you exceed the number of unsuccessful log-in attempts, KMF CryptR erases master keys, erases the `user` and `admin` passwords, restores the default passwords, and must be power-cycled. The number of unsuccessful log-in attempts can be configured through the shell. The default number is 10.

CAUTION: If the limit on failed log-in attempts is set to zero (0) and the owners of the `user` and/or `admin` accounts forget their passwords, there is no method to reset the KMF CryptR passwords. When this occurs, the KMF CryptR must be replaced. Therefore, a value of 0 is not recommended.

If the KMF CryptR detects no user activity for 10 minutes during a log-in session, then the KMF CryptR terminates the log-in session and prompts for log-in and password.

The following commands are used during log-in sessions:

- `exit` causes the KMF CryptR to display the log-in prompt; no other command is allowed until the user authenticates with a user name and password again.
- `passwd` causes the KMF CryptR to prompt `admin` for the existing password and then for a new password.
  - If the old password is entered correctly, the new password is stored within the KMF CryptR and remembered even when the KMF CryptR is powered down and restarted.
  - If the password is not entered correctly, the KMF CryptR displays the error message `password change failed` and returns to the prompt. No changes to the stored password are made in this case.

3.3 Configuring KMF CryptR IP Addresses

The following are the default IP addresses for the KMF CryptR:

- Host IP Address: `192.168.1.1`
- Red PIKE IP Address: `192.168.1.2`

- Red PIKE Subnet mask: `255.255.255.0`
- Red PIKE Default gateway IP address: None
- Host TCP Destination Port: `49166`

It is not recommended to change the default IP addresses for the KMF CryptR.

Procedure:

1. Log on to the KMF CryptR as `admin`.

   The `CRYPTR>` prompt appears.

2. Enter: `cryptrconfig`.

   The following prompt appears: `Enter RED (trusted network) IP address [192.168.1.2]>`

3. Perform one of the following actions:
   - To accept the default IP address, press ENTER.
   - Specify a different IP address. Press ENTER.

   The following prompt appears: `Enter RED subnet mask [255.255.255.0]>`

4. Perform one of the following actions:
   - To accept the default IP address, press ENTER.
   - Specify a different IP address. Press ENTER.

   The following prompt appears: `Enter RED default gateway [none]>`

5. Perform one of the following actions:
   - To accept the default value, press ENTER.
   - Specify an IP address in the same subnet as the CryptR red IP address. Press ENTER.

   The following prompt appears: `Enter Host IP address [192.168.1.1]>`

6. Perform one of the following actions:
   - To accept the default Host IP address, press ENTER.
   - Specify a different Host IP address. Press ENTER.

   The following prompt appears: `Enter Host Port Number [Range:49166-65535] [49166]>`

7. Perform one of the following actions:
   - To accept the default Host Port Number, press ENTER.
   - Specify a different Host Port Number. Press ENTER.

   The following message appears: `CRYPTR configuration successful.`

3.4 Service Configuration Commands

Table 6: Service Configuration Commands

Command	Function of Command
`version`	View the product version.
`Ipversion`	Show the IP stack product versions.
`banner`	Change the text of the log-on banner. The maximum length of banner text is 274 characters, including white space. A maximum of 80 characters is recommended for proper display. • Use `\n\r` (line feed, carriage return) for new lines if needed. You can escape `\n` and `\r` in the serial shell by pressing the ESC key and then sending the appropriate carriage return or line feed character. This may require a SHIFT + ENTER or CTRL + ENTER, depending on your operating system and terminal emulation program. • Customizing the banner overwrites the default banner permanently. The only way to restore the default banner, if necessary, is to manually enter the default banner text: `Use of this device and any related service is your consent to all associated terms, conditions, including consent to monitoring and disclosure provisions.`
`time`	Set the time. This command has the following syntax: `time` ***<hh:mm:ss>***
`date`	Set the date. This command has the following syntax: `date` ***<yyyy-mm-dd>***
`auditlog show`	Display current audit log settings.
`auditlog clear`	Clear the audit log.
`auditlog disable`	Disable logging of audit events.
`auditlog enable`	Enable logging of audit events.
`auditlog`	Configure Audit Log Interface parameters. This command has the following syntax: `auditlog` ***<Audit Log Level><Audit Log Alert>*** Parameters for this command are: • ***<Audit Log Level>***: Enter audit log level [0-7] • ***<Audit Log Alert>***: Enter audit log full alert [0-100]
`errorlog retrieve`	Display the current contents of the error log.
`errorlog clear`	Discard the contents of the error log.
`ethconf`	Retrieve the current configuration of the interface.

Table continued…

Command	Function of Command
	This command has the following syntax: `ethconf` ***<Interface><LINK_CONFIG>***
	Parameters for this command are: • ***<Interface>***: red • ***<LINK_CONFIG>***: Valid values are `10half`, `10full`, `100half`, `100full`, and `auto`.

3.5 Security Configuration Commands

Table 7: Security Configuration Commands

Command	Function of Command
`fips`	Show the Federal Information Protection Standard (FIPS) status. See Table 2: KMF CryptR Security Specifications on page 24 for details about FIPS.

3.6 Miscellaneous Commands

Help on individual command formats is available in the form of usage when a command is typed without its proper parameters. The KMF CryptR displays usage if it cannot correctly parse the command's parameters.

Table 8: Miscellaneous Commands

Command	Description
`help`	The KMF CryptR displays a short list of available commands without their parameters.
`ping`	This command uses Internet Control Message Protocol (ICMP) to elicit an ICMP echo response from a host or gateway.

This page intentionally left blank.

Chapter 4

KMF CryptR Operation

This chapter describes operation of the KMF CryptR after it is installed and configured.

4.1 Resetting the KMF CryptR

Use this procedure to reset the KMF CryptR.

Procedure:

Perform one of the following actions:

- If the alarm LED is not lit, press the **Reset** button located on the front of the KMF CryptR. See Figure 3: KMF CryptR Front Panel on page 24.
- If the alarm LED is lit, then do a power-on-reset (remove and reapply power) to clear the alarm. The alarm LED is set on detection of a failure inside the KMF CryptR. Pressing the **Reset** button only does not work in this situation.

4.2 Zeroizing Keys in the KMF CryptR with the Erase Button

Use this procedure to zeroize, or quickly erase, all stored keys in the KMF CryptR.

Procedure:

Press the **Erase** button on the KMF CryptR. See Figure 3: KMF CryptR Front Panel on page 24.

The **Erase** button works even if you are logged off or the KMF CryptR does not have power.

When keys have been zeroized, the KMF CryptR resets and enters a nonfatal error state (causing the status LED to turn red). This indicates that the key loading procedure must be performed for each master key.

4.3 KMF CryptR Password Management

If you changed KMF CryptR embedded passwords (for `CRYPTR_USER` and `CRYPTR_OFFICER`) on the KMF server, you must also change the `user` and `admin` passwords on the KMF CryptR. These passwords can only be changed separately.

4.3.1 Changing the User Password on the KMF CryptR

Procedure:

1. Initiate a connection to the KMF CryptR. See Initiating a Connection to the KMF CryptR on page 33.
2. Log on as `user`.

   The following prompt appears: `Press any key then press ENTER to change password`.

3 Press any key. Press ENTER.

The following prompt appears: `Do you want to change password? y/n [y]:`

4 Enter: `y`.

5 Enter the current password.

6 Enter the new password.

The password has been changed.

4.3.2
Changing the Admin Password on the KMF CryptR

Procedure:

1 Initiate a connection to the KMF CryptR. See Initiating a Connection to the KMF CryptR on page 33.

2 Log on as `admin`.

3 At the `CRYPTR>` prompt, enter: `passwd`

4 Enter the current password.

5 Enter the new password.

The password has been changed.

4.4
Connecting the KMF CryptR and KVL

Use this procedure to connect the KMF CryptR to the Key Variable Loader (KVL) device.

Procedure:

Connect the red port on the KMF CryptR with the key load port on the KVL (either KVL 3000 Plus or KVL 4000), using an appropriate key load cable.

4.5
KMF CryptR Upgrade

The following are the ways to upgrade software or algorithms on the KMF CryptR:

- Upgrade KMF CryptR software using Trivial File Transfer Protocol (TFTP). See Upgrading the KMF CryptR Software Through TFTP on page 40.
- Upgrade algorithms on the KMF CryptR using the KVL 3000 Plus. See the *KVL 3000 Plus Key Variable Loader Secure Module Software Upgrade Manual* (6881132E26).
- Upgrade algorithms on the KMF CryptR using the KVL 4000. See "Upgrading Algorithms on KMF CryptRs" in the *KVL 4000 FLASHport Upgrade User Guide*.

4.5.1
Upgrading the KMF CryptR Software Through TFTP

Use this procedure to upgrade the KMF CryptR software using Trivial File Transfer Protocol (TFTP).

Prerequisites:

- Place an order with Motorola Solutions Support Center (SSC) to receive the KMF CryptR software upgrade.

- Obtain the previously recorded and maintained key data and configuration information (such as Master Keys, passwords, and IP data) for the KMF CryptR so that it can be reloaded when the upgrade is complete.

CAUTION:
If the version of KMF CryptR software present prior to the upgrade is R01.05.01 or earlier, you must upgrade the boot block software on the **red** side of the KMF CryptR only before upgrading the KMF CryptR software through TFTP. Failure to do so will result in loss of all algorithms after the KMF CryptR is upgraded to version 2.1.6 or later. See Upgrading Boot Block Software on page 42.

CAUTION: When you upgrade from version R01.05.01 or earlier, all key data and configuration information stored in the KMF CryptR will be erased. Failure to recover this information after the upgrade could result in a temporary loss of functionality.

IMPORTANT: If the version of KMF CryptR software present prior to the upgrade is R2.1.6 or later, the boot block upgrade is not required.

Procedure:

1. Connect the KMF CryptR to the TFTP server through an Ethernet switch and Ethernet cables.

   If the TFTP server is installed on the computer that runs on a terminal, and not a standalone computer, you also need to install a network adapter (such as an Ethernet computer card or a USB Ethernet adapter) on your computer.

2. Configure the TFTP server and Ethernet switch with the following information:
   - Ethernet switch IP address: 192.168.0.1
   - TFTP server PC IP address: 192.168.0.187
   - TFTP server PC mask: 255.255.0.0
   - TFTP server PC gateway: 192.168.0.1
3. If a firewall is blocking data transfer, contact your administrator to temporarily disable or remove the firewall.
4. Start the TFTP server if it cannot run as a background task. For example, if the TFTP server is **Tftp32**, double-click the **Tftp32** icon on the desktop.
5. Transfer the `red_cryptr_upgrade.bin` and `blk_cryptr_upgrade.bin` binary images from the KMF CryptR upgrade CDs to the TFTP server. Store the image files in `C:\Programming Files\Tftp32` (if the TFTP server is **Tftp32**).
6. Initiate a connection to the KMF CryptR and log on. See Initiating a Connection to the KMF CryptR on page 33.

   Log on as `admin` to perform the upgrade. To log on, use the previously used password.

   The `CRYPTR>` prompt appears.

7. To upgrade the KMF CryptR, enter: `progconf all`
   - The upgrade is not complete until the Power LED illuminates green. The upgrade can take up to five minutes to complete.
   - If the TFTP server indicates that an upgrade occurred to the Red PIKE only, press the **Erase** button on the KMF CryptR to cause the TFTP server to perform an upgrade to the Red and Black PIKE.
   - If the Power LED does not illuminate green, or if the Tx Clear LED illuminates orange, the upgrade failed. See TFTP Upgrade Failure Troubleshooting on page 48.
8. Close the terminal emulator program.

9 Power cycle the KMF CryptR.

- If the KMF CryptR was upgraded from version R02.01.06 or later, the upgrade is complete. The master keys and configuration settings have been retained. Reconnect the KMF CryptR to the KMF as indicated in the Postrequisites at the end of this procedure.
- If the KMF CryptR was upgraded from version R01.05.01 or earlier, the settings were reset to default. Perform the remaining steps in this procedure to configure the device.

10 If the COM port connection is not restored, perform the following actions:

a Unplug the USB cable.

b Wait about 10 seconds and reconnect the USB cable.

11 Log on to the KMF CryptR as `admin`.

The default password is `CryptrAdmin12345`.

12 Change the default password for `admin`. See Changing the Admin Password on the KMF CryptR on page 40.

13 Enter the maximum number of failed log-in attempts.

CAUTION: If the limit on failed log-in attempts is set to zero (0) and the owners of the `user` and/or `admin` accounts forget their passwords, there is no method to reset the KMF CryptR passwords. When this occurs, the KMF CryptR must be replaced. Therefore, a value of 0 is **not** recommended.

14 Upon an upgrade, an `errorlog` entry may be logged.

To retrieve the entry, enter: `errorlog retrieve`.

15 Configure IP addresses for the KMF CryptR (see Configuring KMF CryptR IP Addresses on page 34).

16 Log out of the KMF CryptR as `admin`.

17 Log on to the KMF CryptR as `user`.

The default password is `CryptrAdmin12345`.

18 Change the default password for `user`. See Changing the User Password on the KMF CryptR on page 39.

19 Power cycle the KMF CryptR.

Postrequisites: Reconnect the KMF CryptR to the KMF and reload the Master Keys. See Reloading Master Keys on page 43.

4.5.1.1
Upgrading Boot Block Software

Use this procedure to upgrade boot block software before upgrading KMF CryptR software. Perform this upgrade on the **red** side of the KMF CryptR only.

Prerequisites: Before upgrading boot block software:

- Obtain an appropriate key load cable. See "Interface Cables" in the *KVL 4000 FLASHport Upgrade User Guide*.
- Copy upgrades onto the Security Adapter of the KVL 4000 Key Variable Loader (KVL). See "Copying Upgrades from the PDA to the Security Adapter" in the *KVL 4000 FLASHport Upgrade User Guide*.
- If the KVL is password protected, log on as an administrator.
- Obtain the previously recorded and maintained key and configuration data for the KMF CryptR so that it can be reloaded once the upgrade is complete.

This upgrade requires the following KVL 4000 software versions:

- PDA: 1.3.x000.174 or later
- Security Adapter: R02.05.03 or later

CAUTION: During the upgrade, all key data and configuration information stored in the KMF CryptR will be erased. Failure to recover this information after the upgrade could result in a temporary loss of functionality.

When and where to use: You must upgrade boot block software before upgrading KMF CryptR software from R01.05.01 or earlier. Failure to do so will result in loss of all algorithms after the KMF CryptR is upgraded to version 2.1.6 or later.
If the pre-upgrade KMF CryptR version is 2.1.6 or later, the boot block upgrade is not required.

Procedure:

1. Insert the *KMF CryptR Application Upgrade Red* CD into the CD/DVD drive.
2. On the CD, navigate to `KVL4000 Upgrade/Security Module/DesktopInstaller`.
3. Download the boot block upgrade software to the Security Adapter of the KVL 4000. See “Running the KVL Software Installation Wizard” and “Copying Upgrades from the PDA to the Security Adapter” in the *KVL 4000 FLASHport Upgrade User Guide*.
4. Put the KMF CryptR into the KVL programming mode. See “Putting the KMF CryptR into the KVL Programming Mode” in the *Key Management Facility User Guide*.
5. Connect the **red** key load port on the KMF CryptR to the key load port on the KVL using an appropriate key load cable.
6. Verify that the KMF CryptR is powered on. Do not switch off the KMF CryptR before completing the upgrade procedure.
7. On the KVL main screen, select **Settings** → **Manage firmware** → **External module firmware** → **Upgrade** → **Upgrade Now**.

   A progress animation appears, indicating that the connected KMF CryptR is being upgraded.

   - If the upgrade process starts but does not progress after 30 seconds, press the **Reset** button on the KMF CryptR.
   - When the process is completed, a **completed** sound is played and a screen appears, indicating that the upgrade was successful.

8. Power cycle the KMF CryptR.
9. Disconnect the KMF CryptR.
10. Tap **Done** on the consecutive screens to return to the KVL main screen.

IMPORTANT: Do not reboot the KMF Server or reload any master keys until **after** completing Upgrading the KMF CryptR Software Through TFTP on page 40.

4.5.1.2
Reloading Master Keys

When and where to use: Perform this procedure if the existing Master Key has been lost due to the reloading of the wrong Master Key, erasure of the existing Master Key, or if the KMF CryptR has been

replaced. If the wrong Master Key is reloaded, the existing keys cannot be used until the KMF is reloaded with the correct Master Key from the Key Variable Loader (KVL).

Procedure:

1. Turn on the KVL and connect it to the KMF CryptR. See Connecting the KMF CryptR and KVL on page 40.
2. Perform one of the following actions:
   - On the active KMF Server, perform the following actions:
     1. Log on to the KMF Client application.
     2. From the main menu, select **Configuration** → **Algorithms**.
     3. In the **Algorithm Management** view, select **Reload** next to the algorithm you want to reload the Master Key for.
     4. To confirm, in the **Reload Master Key Confirmation** window, enter the password and click **Yes**.
   - On the inactive KMF Server, perform the following actions:
     1. Log on to the KMF Server with local Windows Administrator privileges.
     2. On the desktop, right-click the **Configuration Console** icon and select **Run as administrator**. If prompted for administrator credentials or a confirmation, type the administrator credentials or click **Yes**.
     3. Enter: `coco kmf loadmk -a <algorithm name>`

        IMPORTANT: Use capital letters when entering the algorithm name. Spell the algorithm name exactly as it is spelled in the KMF Client application of the active KMF Server.
     4. At the `Provide username` prompt, enter the user name.
     5. At the `Provide password` prompt, enter the password.
3. Load the key from the KVL:
   - If you have KVL 3000 Plus, see “Loading Selected Key” in the *KVL 3000 Plus Key Variable Loader User’s Guide* (6881132E29).
   - If you have KVL 4000, see “Loading a Selected Key” in the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

   You have 60 second to load the key.
4. When the process is complete, disconnect the KVL from the KMF CryptR.

Chapter 5

KMF CryptR Maintenance

This chapter contains maintenance information for the KMF CryptR.

5.1 Replacing Batteries in the KMF CryptR

Use this procedure to replace batteries in the KMF CryptR.

When and where to use: Replacing a battery is considered tampering with the KMF CryptR. If the KMF CryptR detects tampering, it erases master keys.

Procedure:

1. Power down the KMF CryptR and remove the Ethernet cable.
2. Unscrew the four screws of the bottom cover to open the KMF CryptR.
3. Remove the old coin-type battery using a small screwdriver to gently pry the battery out of the holder.
4. Insert a new +3.0 V lithium battery (DL2032) in the battery holder with the positive (+) terminal facing up.
5. Reassemble the KMF CryptR bottom cover.
6. Reconnect the Ethernet cable to the KMF CryptR, and power up the KMF CryptR.
7. Verify that the device powers up normally and that all status LEDs are green.
8. Reload the master keys.

This page intentionally left blank.

Chapter 6

KMF CryptR Troubleshooting

This chapter contains troubleshooting information for the KMF CryptR.

6.1 Status Indicators

The set of Light Emitting Diodes (LEDs) on the front of the KMF CryptR indicates its status.

IMPORTANT: To clear an alarm condition, disconnect and reconnect power.

Table 9: KMF CryptR Front Panel LEDs

Item	LED	Description
1	Alarm	**Solid Red** = unrecoverable error has been encountered. To resume operation, reset the KMF CryptR by removing and reapplying power. **Flashing Red** = A tamper has been detected. Log on to the KMF CryptR and retrieve error logs by entering: `errorlog retrieve`
2	Power	LED flashes when battery is low.
3	Ready / Link Black	This LED is not used and remains off other than at self-test or programming.
4	Ready / Link Red	**Green** = KMF CryptR is ready to communicate with the KMF Server. **Flashing Green** = Activity on the KMF CryptR - KMF Server link. **Red** = KMF CryptR ready for KVL key loading. **Orange** = KMF CryptR is ready to communicate with the KMF Server and ready for KVL key loading. **Flashing Red over Orange** = Activity on the KMF CryptR - KMF Server link while the KMF CryptR is ready for KVL key loading. **Flashing Orange/Red and turning off** = A timeout during master key loading.
5	Tx Clear	**On** during power up and on upgrade error. **Off** during normal operation.
6	Status	**Red** = No master keys loaded in KMF CryptR **Green** = At least one master key loaded **Flashing Orange** = in programming mode

6.2 KMF CryptR Audit and Error Log Collection

The KMF CryptR maintains an internal error log. Use the `errorlog` command to retrieve internal errors. See Service Configuration Commands on page 36.

If configured, the KMF CryptR keeps an internal audit log with significant events and errors. Use the `auditlog` command to configure the log and retrieve its contents. See Service Configuration Commands on page 36.

Alternatively, you can retrieve audit and error logs from the KMF CryptR using the **Get CryptR Logs** button on the KMF Client. See Retrieving Audit and Error Logs from the KMF CryptR on page 48.

6.2.1
Retrieving Audit and Error Logs from the KMF CryptR

If the KMF CryptR was tampered with before connecting to the KMF Server, you need to retrieve logs first. Otherwise, the KMF CryptR will not be initialized successfully.

Prerequisites: Log files are stored in the KMF Server under audit right protection. To retrieve logs you need to belong to the audit group.

Procedure:

1. Log on to the KMF Client application.
2. From the main menu, select **Configuration** → **KMF CryptR**.
3. In the **KMF CryptR Management** view, select **Get CryptR Logs**.

   Two log files are created in `C:\ProgramData\Motorola\KMF Server\log`:

   - `serverAudit_Log_`***`<date_time>`***`.txt`
   - `serverError_Log_`***`<date_time>`***`.txt`

6.3
TFTP Upgrade Failure Troubleshooting

Perform the following actions to troubleshoot a failure of a KMF CryptR software upgrade using Trivial File Transfer Protocol (TFTP) upgrade.

If the problem persists, contact the Motorola Solutions Support Center (SSC).

- Check network connections.
- Check the USB cable and Ethernet cable condition. Verify that the Ethernet cable is a straight cable.
- Check the TFTP server configuration.
- Check the Ethernet switch configuration.
- Check the image file name convention.
- Verify that the TFTP server is started and running.
- Verify that the firewall is disabled.
- Verify that image files are stored in the TFTP server under `C:\Programming Files\Tftp32` (if the TFTP server is Tftp32).
- Use a network monitor tool to monitor the network transfer messages.

Chapter 7

KMF CryptR FRU/FRE Information

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) applicable to the KMF CryptR.

The KMF CryptR is considered a Field Replaceable Unit (FRU), and when determined to be faulty, it may be replaced with a defect-free device to bring the equipment back to normal operation. The faulty KMF CryptR must then be shipped to Motorola Solutions for further troubleshooting and repair.

7.1 KMF CryptR FRU

Table 10: KMF CryptR FRU

Item	MSI Kit Number
KMF CryptR	T7734A

7.2 KMF CryptR Replacement Parts

Table 11: KMF CryptR Replacement Parts

Item	MSI Kit Number
Power Adapter	DLN6732A
Ethernet CrossOver w/Sealing Boot	DLN6736A
Mini USB Cable	DLN6735A
Adapter Cable	DLN6739A
Rack Mount Kit	TKN9285A
Key Load Cable	TKN8531C
Velcro PS Straps	42009268001
AC Line Cord for North America	3082933N08
AC Line Cord for Europe	3082933N28
AC Line Cord for UK	3082933N29
AC Line Cord for Australia	3082933N26

This page intentionally left blank.

Chapter 8

KMF CryptR Reference

This chapter contains supplemental reference information for the KMF CryptR.

8.1 General Safety Guidelines

The following information contains general safety guidelines:

- All equipment must be properly grounded according to Motorola Solutions installation instructions for safe operation.
- All equipment must be serviced only by a qualified technician.
- Wear an ESD (Electrostatic discharge) strap and connect its cable to a tested earthing connection. The strap must be worn throughout this procedure to prevent component damage due to ESD.
- This equipment uses a Lithium battery.
- Failure to install and/or replace this battery correctly may result in explosion. Replace only with the same or equivalent type of battery. Dispose of used batteries at an authorized metal reclamations dealer.

This page intentionally left blank.

Chapter 9

KMF CryptR Disaster Recovery

This chapter provides disaster recovery information for KMF CryptR.

Process:

1. Remove the old KMF CryptR hardware.
2. Unpack the new KMF CryptR. See Unpacking the KMF CryptR on page 27.
3. Optional: Install the new hardware (the battery is pre-installed). See Mounting the KMF CryptR on page 28.
4. Initiate a connection to the KMF CryptR. See Initiating a Connection to the KMF CryptR on page 33.
5. Log on to the KMF CryptR as `user` and change the default password. Verify that the password matches the password on the KMF Server.

   For more information, see Login Session and User Authentication on page 34.
6. Log on to the KMF CryptR as `admin` and change the default password. Verify that the password matches the password on the KMF Server.

   For more information, see Login Session and User Authentication on page 34.
7. Configure KMF CryptR IP addresses. See Configuring KMF CryptR IP Addresses on page 34.
8. Optional: If your organization has a log-on banner that you want to display upon KMF CryptR log-on, change the default log-on banner. See Service Configuration Commands on page 36.
9. Connect the KMF CryptR to the KMF Server. See Connecting the KMF CryptR to the KMF Server on page 32.
10. Reload Master Key(s). See Reloading Master Keys on page 43.

This page intentionally left blank.

Appendix A

Open Source Software Legal Notice

This media, or Motorola Product, may include Motorola Software, Commercial Third Party Software, and Publicly Available Software.

The Motorola Software that may be included on this media, or included in the Motorola Product, is Copyright (c) by Motorola Solutions, Inc., and its use is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Product and Motorola Solutions, Inc.

The Commercial Third Party Software that may be included on this media, or included in the Motorola Product, is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Product and Motorola Solutions, Inc., unless a separate Commercial Third Party Software License is included, in which case, your use of the Commercial Third Party Software will then be governed by the separate Commercial Third Party License.

The Publicly Available Software that may be included on this media, or in the Motorola Product, is listed below. The use of the listed Publicly Available Software is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Product and Motorola Solutions, Inc., as well as the terms and conditions of the license of each Publicly Available Software package. Copies of the licenses for the listed Publicly Available Software, as well as, all attributions, acknowledgments, and software information details, are included below. Motorola is required to reproduce the software licenses, acknowledgments and copyright notices as provided by the Authors and Owners, thus, all such information is provided in its native language form, without modification or translation.

The Publicly Available Software in the list below is limited to the Publicly Available Software included by Motorola. The Publicly Available Software included by Commercial Third Party Software or Products, that is used in the Motorola Product, are disclosed in the Commercial Third Party Licenses, or via the respective Commercial Third Party Publicly Available Software Legal Notices.

For instructions on how to obtain a copy of any source code being made publicly available by Motorola related to software used in this Motorola Product you may send your request in writing to:

Motorola Solutions, Inc.
Open Source Software Management
500 W. Monroe Street
Chicago, IL 60661, USA

In your request, please include the Motorola Product Name and Version, along with the Publicly Available Software specifics, such as the Publicly Available Software Name and Version.

Note, the source code for the Publicly Available Software may be resident on the Motorola Product Installation Media, or on supplemental Motorola Product Media. Please reference and review the entire Motorola Publicly Available Software Legal Notices and End User License Agreement for the details on location and methods of obtaining the source code.

Note, dependent on the license terms of the Publicly Available Software, source code may not be provided. Please reference and review the entire Motorola Publicly Available Software Legal Notices and End User License Agreement for identifying which Publicly Available Software Packages will have source code provided.

To view additional information regarding licenses, acknowledgments and required copyright notices for Publicly Available Software used in this Motorola Product, please select “Legal Notices” display from the Graphical User Interface (if applicable), or review the Legal Notices or End User License Agreement File/README, on the Motorola Product Install Media, or resident in the Motorola Product.

A.1 PUBLICLY AVAILABLE SOFTWARE LIST

Name:	CRC-32
Version:	N/A
Description:	CRC-32 Algorithm by Gary Brown. This CRC-32 Package was included by Commercial Third Party Software, from WindRiver-Interpeak, within the Motorola Product. The Package has been modified by both WindRiver-Interpeak and Motorola. Copyright 2000-2005 Interpeak AB (http://www.interpeak.se). All rights reserved.
Software Site:	N/A
Source Code:	No Source Code Distribution Obligations.
License:	Public Domain
COPYRIGHT (C) 1986 Gary S. Brown. You may use this program, or code or tables extracted from it, as desired without restriction.	
Credits:	See License Above

Name:	Header Files from OpenBSD Operating System
Version:	N/A
Description:	Portions of the Header Files were included by Commercial Third Party Software, from WindRiver-Interpeak, within the Motorola Product. The Files have been modified by both WindRiver Interpeak and Motorola. Copyright 2000-2007 Interpeak AB (http://www.interpeak.se). All rights reserved.
Software Site:	http://www.openbsd.org
Source Code:	No Source Code Distribution Obligations
License:	The utilized Header Files are under BSD License

Copyright (c) 1982, 1986

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2 Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ”AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Credits:	OpenBSD Project, http://www.openbsd.org Additionally, see License Above

---

A.2
PUBLICLY AVAILABLE SOFTWARE - COMMON LICENSES

No Common Licenses included.

This page intentionally left blank.