System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Secure Communications Feature Guide

NOVEMBER 2016

MN003351A01-A

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.

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 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
MN003351A01-A	Original release of the *Secure Communications Feature Guide* manual	November 2016

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.

About Secure Communications - System Perspective

This manual provides descriptive information about the Secure Communications features of the ASTRO® 25 Trunking Integrated Voice and Data (IV&D), ASTRO® 3.1 Conventional IV&D, and ASTRO® 25 Conventional IV&D systems.

This manual is intended to be used by technicians and system operators as a resource for understanding secure communications in ASTRO® systems. This manual should be used in conjunction with the ASTRO® 25 system documentation and the *Key Management Facility* manual.

What Is Covered In This Manual?

This manual contains the following chapters:

- Secure Communications Overview on page 23, describes secure communications concepts in your ASTRO® 25 Trunking Integrated Voice and Data (IV&D), ASTRO® 3.1 Conventional IV&D, or ASTRO® 25 Conventional IV&D system.
- Key Management Overview on page 35, covers the use of keys in secure communications.
- Secure Communications Equipment on page 59, provides descriptions of the secure communications hardware.
- Secure Communications Configuration on page 79, provides information and procedures to help you configure secure communications components.
- Secure Communications Performance and Troubleshooting on page 89, describes the tools and methods used to manage performance and troubleshooting for secure communications services.
- Secure Communications Field Replaceable Units and Entities on page 95, lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to secure communications.
- Supported Algorithms on page 99, covers the algorithms supported in ASTRO® 25 systems.
- Federal Information Processing Standards (FIPS) on page 103, covers the Federal Information Processing Standards (FIPS) supported in ASTRO® 25 systems.
- Secure Call Processing for ASTRO 25 Trunking IVD Systems on page 105, describes the processes that the ASTRO® 25 Trunking IV&D system performs when secure voice calls are initiated.
- Acronyms on page 111, contains acronyms related to secure communications.

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).
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.
Key Management Facility	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, troubleshooting, and FRU/FRE replacement.
Encrypted Integrated Data	Provides information necessary to understand, install, configure, operate, maintain, and troubleshoot the Encrypted Integrated Data feature. This feature enables encryption of data calls between ASTRO® 25 subscriber units and data applications such as ASTRO Advanced Messaging Solution (AAMS) that reside in the Customer Enterprise Network (CEN).
PDEG Encryption Unit	Provides information on the PDEG Encryption Unit hardware, which is a component of the Encrypted Integrated Data (EID) feature and is located within the Customer Enterprise Network (CEN). The EID feature provides data encryption services for dedicated ASTRO® 25 Trunked Integrated Voice and Data applications between the CEN and subscriber radios.
Conventional Data Services	Provides descriptive and procedural content relating to the ASTRO® 25 conventional data feature which includes a description of the feature, a description of the role of the components supporting this feature, a description of how conventional data call processing is implemented and how data messages are processed. Additional information provided includes procedures for installation, configuration, operation, and troubleshooting.

Table continued…

Related Information	Purpose
CAI Data Encryption Module	Provides information about the CDEM, the component that provides secure data encryption and decryption services for the ASTRO® 25 Conventional with Integrated Data feature.
KVL 3000 Plus Key Variable Loader User's Guide	Provides information for the KVL 3000 and KVL 3000 Plus.
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 secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others. This manual describes the ASTRO® 25 mode of operation.
KMF CryptR User Guide	Provides instructions on installing, configuring, and using the KMF CryptR hardware and software. Information on troubleshooting and maintenance is also included.

This page intentionally left blank.

Chapter 1

Secure Communications Overview

This chapter describes secure communications concepts in your ASTRO® 25 Trunking Integrated Voice and Data (IV&D), ASTRO® 3.1 Conventional IV&D, or ASTRO® 25 Conventional IV&D system.

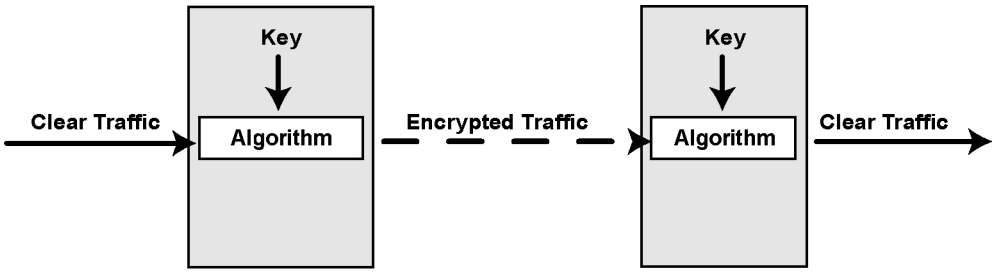
NOTICE: In general, throughout the manual, when referring to Over-The-Air Rekeying (OTAR), the same information applies for Over-The-Ethernet Keying (OTEK). OTAR and OTEK provide the same basic remote centralized key management capability. OTAR refers to managing devices such as radios over the air, while OTEK refers to managing devices such as an MCC 7500 Dispatch Console, MCC 7500 Archiving Interface Server (AIS), PDEG Encryption Unit, or CAI Data Encryption Module (CDEM) over a wired network.

1.1 What Is Secure Communication?

The Motorola Solutions ASTRO® 25 secure communication solution allows two-way voice and data transmissions to be encrypted and secure. When encryption is used to protect digital traffic, the transmitting device uses an encryption key to transform clear digital messaging into encrypted code. Modern algorithms do not scramble messages, but convert messages bit-by-bit into an entirely different encrypted form. Figure 1: Basic Encryption/Decryption of Traffic on page 23 shows the basic process used for secure communication. The sender uses a particular key and algorithm to encrypt clear traffic. The traffic is passed across the medium in an encrypted form. The recipient uses the same key and algorithm to decrypt the traffic. See Supported Algorithms on page 99 for details about algorithms used in the ASTRO® 25 secure communication solution.

An encryption key is a sequence of characters known to both or all parties to a communication and it enables the encryption process. Encryption is based on subjecting digitized signals to numerical variables so that the signals cannot be interpreted by anyone but the intended parties. Subscriber units (for example, radios) without encryption keys cannot communicate in secure mode.

Figure 1: Basic Encryption/Decryption of Traffic



The Motorola Solutions secure voice and data solution uses sophisticated algorithms to protect voice and data traffic. Depending on the algorithm used, a radio can be provisioned with keys from a total selection of 1.1×10^{77} unique keys. By rotating keys on a regular basis, it is nearly impossible for an interceptor to find the correct key and decrypt the traffic.

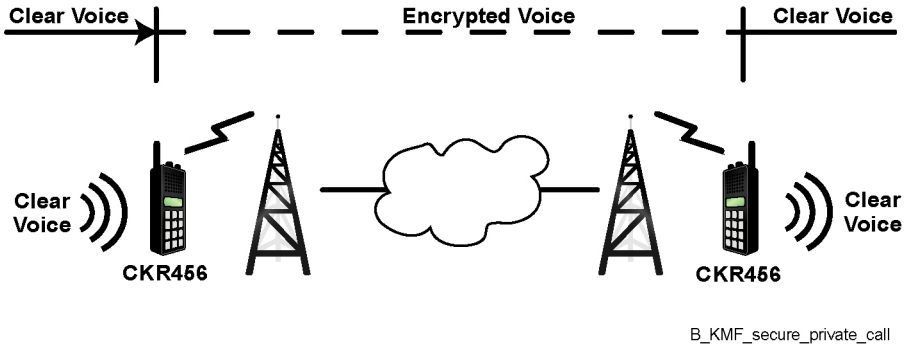
For radio systems, encryption does not prevent hobbyists or hostile groups with Internal Multi-Band Excitation (IMBE) or Advanced Multi-Band Excitation (AMBE)-capable radio equipment from intercepting traffic. Encryption also does not prevent anyone from noticing the amount of activity on a particular channel. However, encryption does protect the information from being deciphered and understood by anyone outside your organization. Without the proper algorithm and the encryption key,

any intercepted traffic is received as a bunch of garbled digital bits wrapped in common air interface packets.

1.1.1
What Is Secure Voice?

Figure 2: Basic Secure Voice Operation on page 24 shows basic secure voice operation between two radios. The transmitting radio encrypts clear voice using a particular key (CKR456) and transmits the encrypted voice to the transport network. The secure voice traffic is routed over the network while remaining in an encrypted form, and is transmitted to the intended recipient. The receiving radio then uses the same key (CKR456) to decrypt the traffic and provide clear voice to the user.

Figure 2: Basic Secure Voice Operation



In the ASTRO® 25 system, secure voice is supported in the following ways:

- Using a secure-capable Voice Processor Module (VPM) device with the VPM-based MCC 7500 Dispatch Console. The VPM replaces the voice card, secure card, and General Purpose Input/ Output Module (GPIOM) hardware used in earlier versions of the MCC 7500 consoles.
- Installing encryption cartridges in each DIU (for ASTRO® 3.1 Conventional IV&D systems only). The DIU encryption cartridge provides the encryption/decryption of all the secure call activity between the radios and consoles.
- Using a secure-capable radio equipped with an encryption module – a Motorola Advanced Crypto Engine (MACE), a Universal Crypto Module (UCM), or an Encryption Module Card (EMC).

The secure-capable VPM provides secure voice capability for console calls. When a secure call is taking place, the VPM provides the encryption/decryption of all the secure call activity between the system and the consoles.

1.1.1.1
Secure Voice in an ASTRO 25 Trunking IVD System

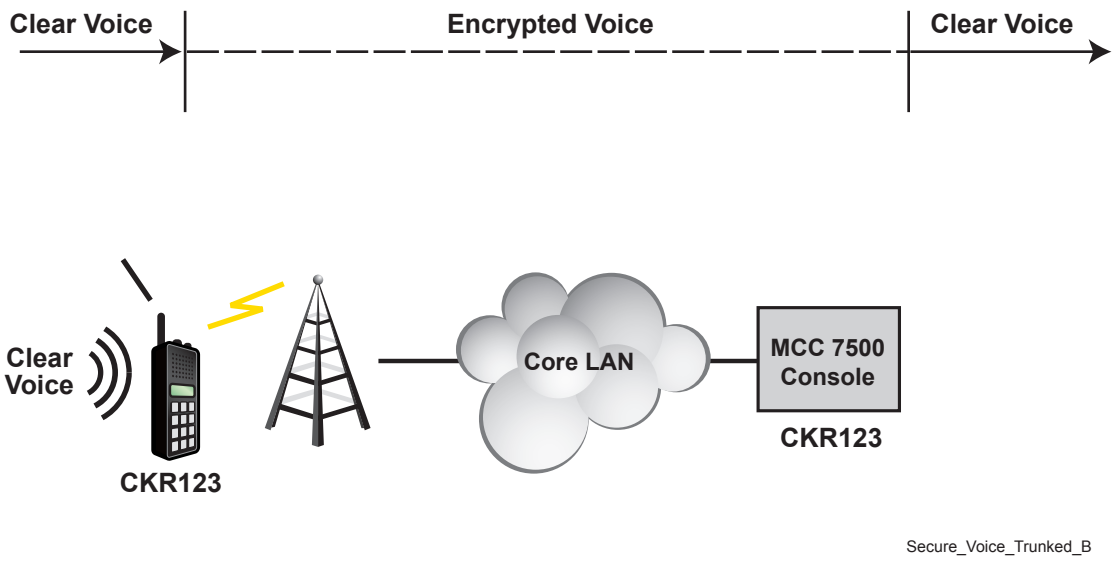
The following figure shows an illustration of an inbound secure call. The radio uses a particular key to encrypt the voice traffic, then transmits the encrypted traffic to the radio system. The system then routes the traffic, which is still in an encrypted form, to the MCC 7500 Dispatch Console, where the secure card or circuitry decrypts the traffic. The MCC 7500 processes the audio for the MCC 7500 consoles.

The MCC 7500 Dispatch Consoles support multiple encryption algorithms and secure keys which provide access and control of talkgroups from different agencies, if necessary. Sending encryption keys from the Key Management Facility (KMF) to the MCC 7500 consoles can be accomplished by using the Key Variable Loader (KVL) device or by sending keys using Over-the-Ethernet Keying (OTEK).

For more information, see the following manuals:

- *Key Management Facility*
- *KMF CryptR User Guide*
- *MCC 7500 Dispatch Console with Voice Processor Module*

Figure 3: Secure Voice in an ASTRO 25 Trunking IVD System



1.1.1.2

Secure Voice in an ASTRO 3.1 Conventional IVD System

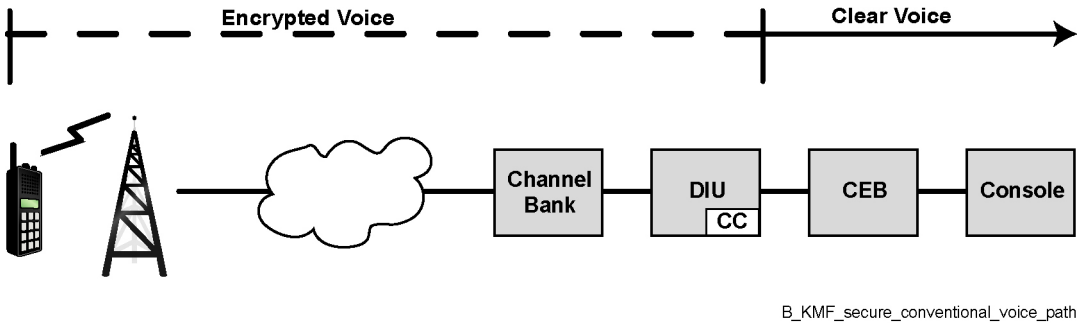
In an ASTRO® 3.1 Conventional IV&D system, secure voice is supported by installing encryption cartridges in each DIU, and installing either a Universal Crypto Module or Advanced Digital Privacy software into the radios. The Universal Crypto Module or Advanced Digital Privacy software allows the radio to be loaded with keys and operate in secure mode (encrypting and decrypting secure traffic).

The DIU encryption cartridge provides secure voice capability for console calls. When a secure call is taking place, the DIU encryption cartridge provides the encryption/decryption of all the secure call activity between the radios and consoles.

The following figure shows an illustration of an inbound secure call. The radio uses a particular key to encrypt the voice traffic, then transmits the encrypted traffic to the radio system. The system then routes the traffic, which is still in an encrypted form, to the DIU. The DIU selects the appropriate key, decrypts the traffic, and delivers the clear audio to the intended console. This same basic process is used in reverse for outbound secure calls from the consoles.

For more information, see the *ASTRO 25 Conventional Systems – System Overview* (68P81000Y13) manual.

Figure 4: Secure Voice in an ASTRO 3.1 Conventional IVD System



1.1.1.3

Secure Voice in an ASTRO 25 Conventional IVD System

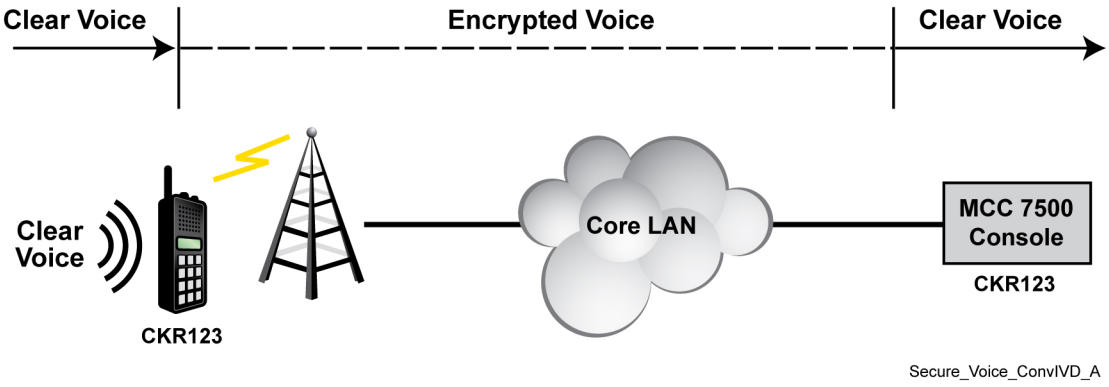
Secure voice is available for ASTRO® 25 Conventional IV&D channels using the MCC 7500 Dispatch Console and MCC 7500 Archiving Interface Server (AIS). VPM-based MCC 7500 Dispatch Console and MCC 7500 AIS always include one VPM. The MCC 7500 consoles can send and receive encrypted calls and control various sub-features of the encrypted calls and channels. Secure voice for digital conventional channels provides encrypted voice directly from subscriber radio to MCC 7500 console, and MCC 7500 console to subscriber radio. Several conventional secure console features are added for the control of secure use per channel.

The MCC 7500 Dispatch Consoles support multiple encryption algorithms and secure keys which provide access and control of talkgroups from different agencies, if necessary. Sending encryption keys from the Key Management Facility (KMF) to the MCC 7500 consoles can be accomplished by using the Key Variable Loader (KVL) device or by sending keys using Over-the-Ethernet Keying (OTEK).

For more information, see the following manuals:

- *Key Management Facility*
- *KMF CryptR*
- *MCC 7500 Dispatch Console with Voice Processor Module*

Figure 5: Secure Voice in an ASTRO 25 Conventional IVD System



1.1.1.4

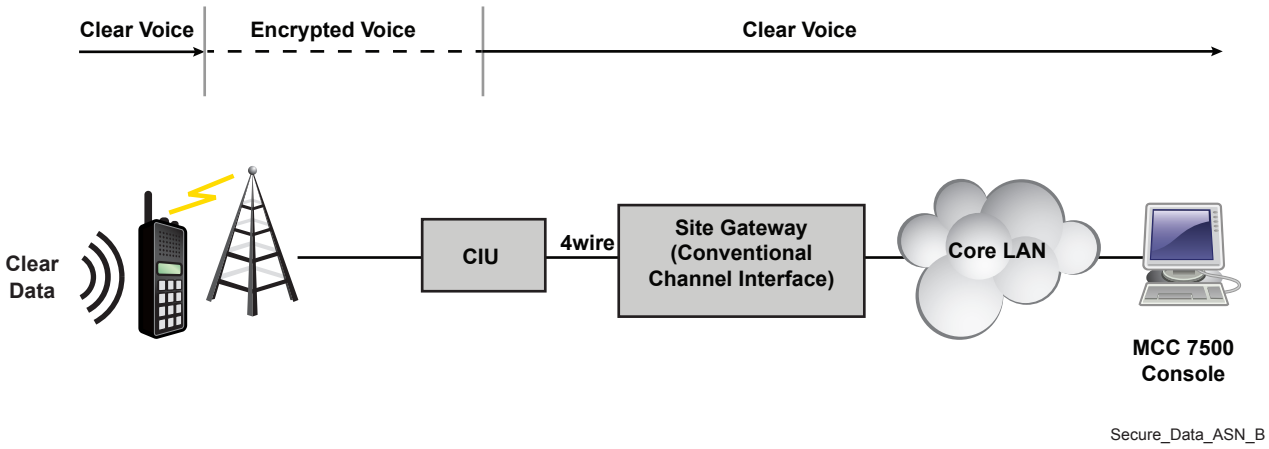
Secure Voice Using Advanced SECURENET for Analog and MDC 1200 Channels

Advanced SECURENET® (ASN) Conventional Operation allows for secure communication on Analog (both with and without MDC 1200) channels with VPM-based MCC 7500 Dispatch Consoles in an M3 core ASTRO® 25 system.

NOTICE: Secure communication using Advanced SECURENET® (ASN) encryption is also supported on Digital Conventional channels using MCC 7500 Dispatch Consoles in K, L, or M core ASTRO® 25 systems.

Advanced SECURENET® (ASN) Conventional Operation on Analog Channel Types requires an existing ASN Console Interface Unit (CIU) that is connected to an existing secure-capable base radio, to be connected to a GGM 8000 Conventional Channel Interface, in order to be utilized by VPM-based MCC 7500 Dispatch Consoles.

Figure 6: Secure Voice Using Advanced SECURENET for Analog and MDC 1200 Channels



NOTICE: Important limitations:

- Advanced SECURENET® Conventional Operation on Analog Channel Types only works with QUANTARs that are version 10 or earlier.
- Advanced SECURENET® Conventional Operation on Analog Channel Types is not supported by GTR 8000s.
- Advanced SECURENET® Conventional Operation on Analog Channel Types connections to MCC 7500s are only supported in ASTRO® 25 systems with an M3 core.

Advanced SECURENET® CIUs are infrastructure encryption devices which use PID-based storage. For more information, see Physical Identifier Key Storage (for Prior System Releases) on page 48.

ASN channels are limited to a set of 8 secure keys (DES-OFB, DES, or DES-XL algorithms) loaded in the CIUs and radios. The ASN secure keys are referred to as “Key Numbers” rather than CKRs.

Key Numbers are configured for each ASN channel from the set of 8 secure keys. For information about mapping ASN Key Numbers to ASTRO® CKRs, see Secure Interoperability With Channels Having Different Encryption Key Types on page 53.

If a site using the Key Management Controller (KMC) for Advanced SECURENET® is added to a system with the current ASTRO® 25 system Key Management Facility (KMF), the KMC can still be used at its site, but it is recommended that your organization maps the relationship between keys in the KMC and keys in the KMF to avoid confusion. For more information about KMC, see the *KMC System Installation and User Guide* (6881091E95).

For more information about Advanced SECURENET, see Appendix C “Advanced SECURENET” in the *Conventional Operations* manual.

1.1.1.5
Conventional Talkgroups

A Conventional Talkgroup provides group separation of voice communications on digital-only conventional channels. Subscribers and console operators using the same talkgroup can communicate

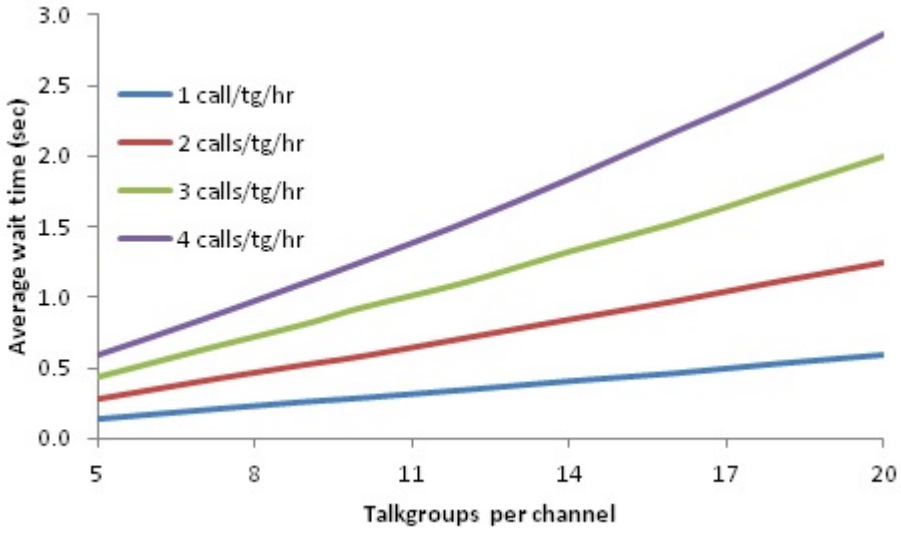
with each other and users of other talkgroups do not hear them. When a transmission is made to a certain talkgroup, only users monitoring that talkgroup hear the transmission. Also, talkgroups provide for separation of emergency alarms. After a talkgroup is assigned to a conventional channel, it cannot be used on a different channel or be used for trunked operation.

An MCC 7500/7100 Dispatch Console operator or subscriber user can initiate a conventional talkgroup call. The subscriber LED is illuminated if activity from a different talkgroup is on the channel. The console shows a talkgroup Cross Busy indication due to a subscriber radio Push-to-Talk (PTT), subscriber radio emergency PTT, or a console PTT on a different talkgroup on the Conventional Talkgroup channel.

The maximum number of conventional talkgroups that can be configured per channel is 20. However, to prevent over-use of the channel, use a lower limit depending on the call rates of the talkgroups. Configuring a channel to capacity with talkgroups that have high call rates results in a busy channel which might provide few opportunities for PTTs. Furthermore, the dispatcher also sees the resource busy most of the time, and radio users might key up on top of each other causing unintelligible audio. And finally, a busy channel leaves little, if any, bandwidth for data transactions.

Figure 7: Expected Wait Time for Users

This figure shows the expected “wait time” for users. Wait time is meant to indicate the expected time a talkgroup user would be delayed on average before being able to initiate a call. Since Conventional Talkgroup calls are not busied, this time is an indication only of how active the channel is.



All Conventional Talkgroup IDs must be home IDs, and cannot be used as Trunked Talkgroup IDs. Radio IDs used on a Conventional Talkgroup channel use the same Radio ID range as trunked Radio IDs. Conventional Unit IDs programmed into a subscriber or dispatch console are less than 10,000,000.

When a Conventional Talkgroup is disabled using Network Manager (NM), radio transmission does not stop, but console transmission does stop.

For inbound calls, the console indicates cross busy for the activity of other conventional talkgroups on that conventional talkgroup channel. The indications are cross busy due to subscriber and subscriber emergency. The console operator is not shown the Unit ID of these transmitting subscribers. A console transmit results in taking over the outbound audio path from the subscriber.

For outbound calls, the console indicates with cross busy the activity of other conventional talkgroups on that conventional talkgroup channel. The indication is cross busy due to console. The console operator is not shown the Unit ID of these transmitting consoles. An attempted console transmit results in busy/queuing.

The console operator is unaware subscribers are in voice-selective calls on the conventional talkgroup channel because cross busy indications are not shown for them. A console talkgroup transmit takes the outbound path from a subscriber in a voice-selective call.

When a subscriber transmits a talkgroup not configured for that conventional talkgroup channel, fault management is notified of an invalid talkgroup. The console operator is unaware subscribers are using invalid talkgroups because cross busy indications are not shown for them. A console talkgroup transmit takes the outbound path from a subscriber using an invalid talkgroup.

Before ending a call, the call controller must wait 500 ms for a new start and for audio in transit to be received at consoles.

Comparator voting status/control at the console is not talkgroup-based; it remains channel-based. If the site is disabled, the site is disabled for all talkgroups.

With Tactical Normal with Conventional Site Controller (CSC), the last state is retained and the next time consoles connect, the state of tactical could cause confusion. If switching between the zone controller and CSC, the console operator may need to reinstate tactical.

The following conventional features are compatible with Conventional Talkgroups:

- Talkgroup Call
- Emergency Alarm
- Emergency Call
- Patch
- Multiselect (MSEL)
- Repeat Disable (per talkgroup)
- Channel Marker
- Paging - Internal
- Paging - External
- Alert Tones
- Keyset Display and Keyset Selection
- Auto Key within the Keysets used by a Common Key Reference (CKR)
- Tactical Priority
- Cross Busy

A Conventional Talkgroup does not support the following conventional features:

- RF Cross Mute
- Customized Paging Formats
- Encryption Key Selection
- Main/Alternate
- Radio Message
- Radio Status
- Status Request
- Voice Selective Call
- Call Alert
- Remote Monitor
- Radio Check
- Radio Disable

- Station Channel Selection
- Second Receiver Control (Mute R2)
- Station WildCard Control Functions at Console
- Multi-Network Access Codes (NAC)

Conventional talkgroups do not support STR3000 Base Radios.

Because it does not operate on mixed mode channels, Conventional Talkgroup is not compatible with Dual Comparator Mixed Mode Simulcast operation.

Cross mute between a Conventional Talkgroup channel and a classic conventional channel is not supported. Cross mute between Conventional Talkgroup channels is also not supported. Other channel receivers may receive other transmitters. When both channels are Conventional Talkgroup channels using channel-wide talkgroups, these calls may be heard on the other channel. If the receiving channel is a conventional talkgroup channel, other talkgroups are detected as invalid talkgroups. To mitigate these effects, use different NACs for each channel, or if that is not possible, use a headset for audio issues.

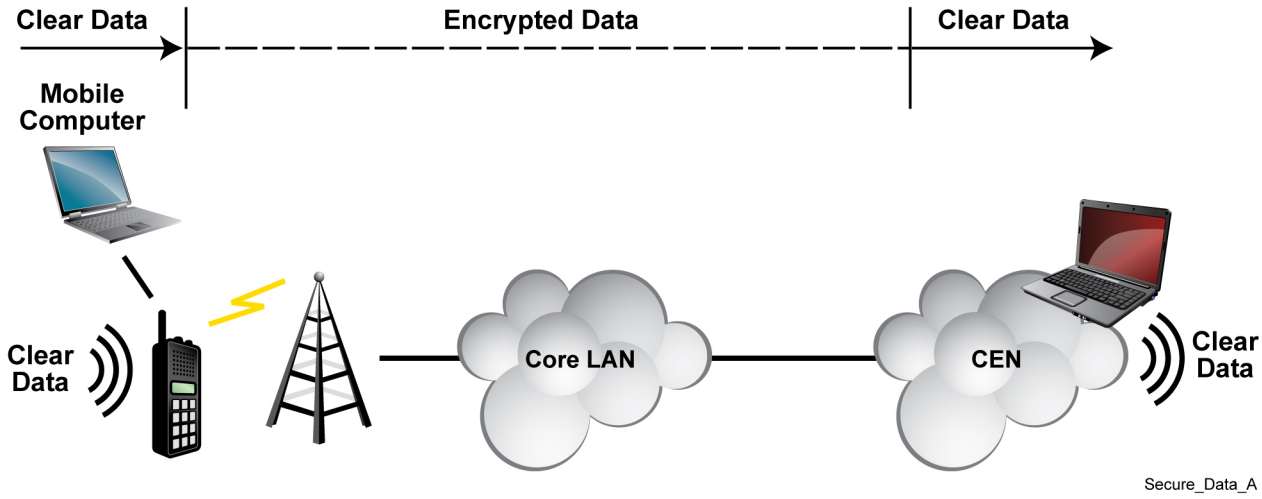
Conventional talkgroup-related Air Traffic Information Activity (ATIA) messages are trunked format ATIA messages.

1.1.2
What Is Secure Data?

Secure data enables the transmission of data between fixed wireline networks that are part of the Customer Enterprise Network (CEN) and the wireless data clients connected through radio subscriber units to the Motorola ASTRO® 25 communication network. This feature places office-centric capabilities in the hands of the mobile work force. Subscriber client applications can connect to server applications that reside in networks outside the trunked radio system's boundary. Client applications can be hosted in the subscriber itself, or in an attached mobile computer.

The following figure shows basic secure data operation between a radio and the CEN. The transmitting radio encrypts clear data using a particular key and transmits the encrypted data inbound to the transport network. The secure data traffic is routed over the network while remaining in an encrypted form, and is then transmitted to the CEN. The receiving data application then uses the same key to decrypt the traffic and provide clear data to the application.

Figure 8: Basic Secure Data Operation



In the ASTRO® 25 system, secure data is supported in the following ways:

- Installing a PDEG Encryption Unit (for ASTRO® 25 Trunking IV&D systems)

- Installing a Radio Network Controller (RNC) and a Wireless Network Gateway (WNG), to manage and route data (for ASTRO® 3.1 Conventional IV&D systems)
- Installing a CAI Data Encryption Module (CDEM) to encrypt/decrypt data and a Conventional IV&D Packet Data Gateway (PDG) unit to manage and route data (for ASTRO® 25 Conventional IV&D systems)

1.1.2.1

Secure Data in an ASTRO 25 Trunking IVD System

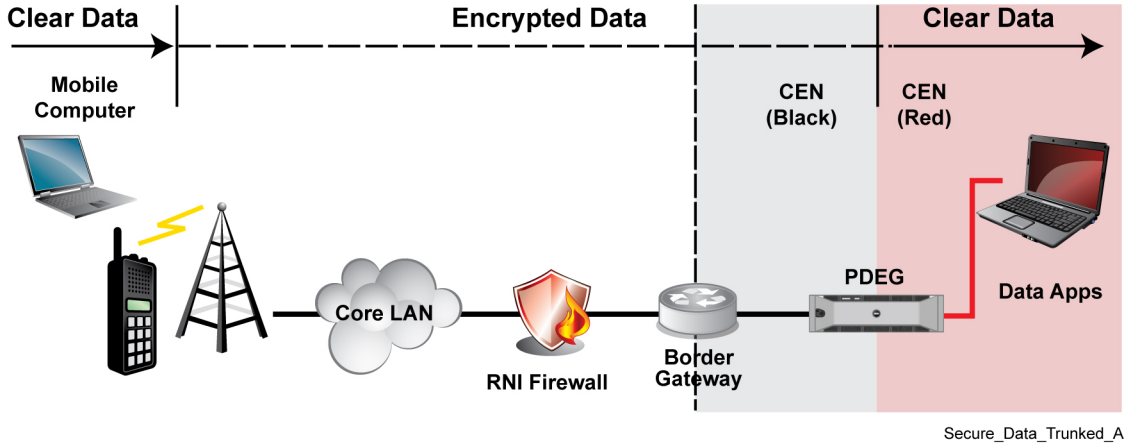
ASTRO® 25 Trunking IV&D systems use the Encrypted Integrated Data (EID) feature to provide data encryption services between the Customer Enterprise Network (CEN) and subscriber radios. EID provides data encryption, decryption, and authentication between each EID-enabled subscriber radio and a device in the CEN called a PDEG Encryption Unit by using a customized implementation of Internet Protocol Security (IPsec) suitable for narrowband radio networks. The IPsec defines encryption, authentication, and key management routines for ensuring the privacy, integrity, and authenticity of data in the system. The encryption algorithm used is Advanced Encryption Standard (AES) for Project 25 standard to enable voice encryption. The subscriber radio and PDEG Encryption Unit data encryption keys can be centrally managed using a KMF server and client in the CEN.

NOTICE: Only the AES algorithm is supported for ASTRO® 25 Trunking IV&D system data encryption.

IMPORTANT: Encrypted Integrated Data service is not compatible with ASTRO® 25 systems using the Transit 25 feature and cannot be used to encrypt the Broadcast Data or High Performance Data (HPD) features.

For more information, see the *Encrypted Integrated Data* manual.

Figure 9: Secure Data in an ASTRO 25 Trunking IVD System



1.1.2.2

Secure Data in an ASTRO 3.1 Conventional IVD System

Secure data in the ASTRO® 3.1 Conventional IV&D system enables the wireless exchange of data messages between subscriber data terminals and a central computer. The data messages share channel time with voice messages and are carried on the same channel. Data service is transparent to the voice user and voice is given priority over data transmission.

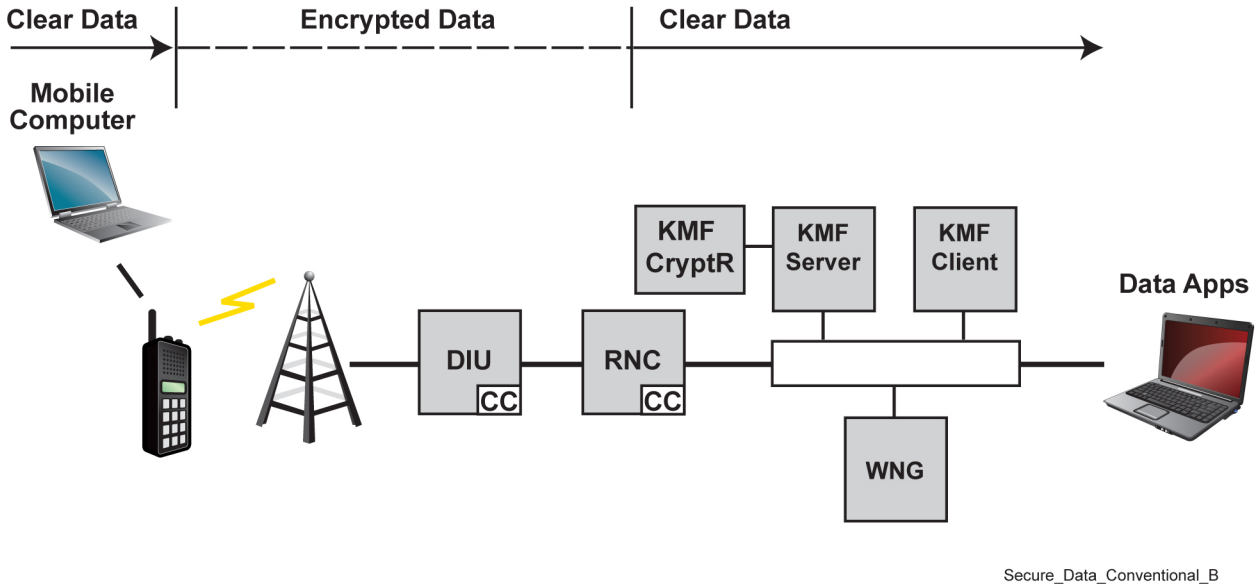
In an ASTRO® 3.1 Conventional IV&D system, secure data is supported by connecting an RNC Encryption Unit to the RNC. Up to five encryption units can be connected to the RNC. The encryption unit allows the RNC to encrypt or decrypt secure data traffic (not including key management messages) as the traffic is being passed between the conventional radios and the customer host network.

The RNC provides the interface, and is the central management point, for monitoring data traffic between the ASTRO® 25 RF system and the WNG. The RNC tracks currently active users and site registration information. It formats data for transmission and provides tables for data site steering. It also provides basic statistics and information about the system at the RNC console or host computer.

The Wireless Network Gateway (WNG) provides a standard IP router interface between hosts on the wireline network and the subscriber data terminals and manages message routing to and from the RF network. It uses Project 25 compliant Layer 3 IP addresses to route messages to the appropriate subscriber terminals or wireline host computers.

For more information, see the *ASTRO 25 Conventional Systems – System Overview* (68P81000Y13) manual.

Figure 10: Secure Data in an ASTRO 3.1 Conventional IVD System



1.1.2.3
Secure Data in an ASTRO 25 Conventional IVD System

The CAI Data Encryption Module (CDEM) is a component that provides data encryption and decryption services for inbound and outbound datagrams in ASTRO® 25 Conventional IV&D systems. The CDEM implements secure processing according to the APCO standards, and supports centralized key management via store and forward (KVL) as well as Over-the-Ethernet Keying (OTEK). As in the ASTRO® 3.1 Conventional IV&D system, the ASTRO® 25 Conventional with Integrated Data feature provides secure communication only between the endpoints of the CAI (over-the-air) interface. Full end-to-end secure capability (to and from a CEN host) is not provided. The CAI interface endpoints are the subscriber unit and the RNG within the ASTRO® infrastructure.

Only a single CDEM per zone is supported in the context of this feature, and it is considered to be part of the Data Subsystem. All network communication to and from the CDEM is through the RNG. The CDEM is not visible as a separate ASTRO® network element. The CDEM connects to the RNG via an Ethernet port. The RNG is a component of the PDG virtual machine which resides on a host virtual management server.

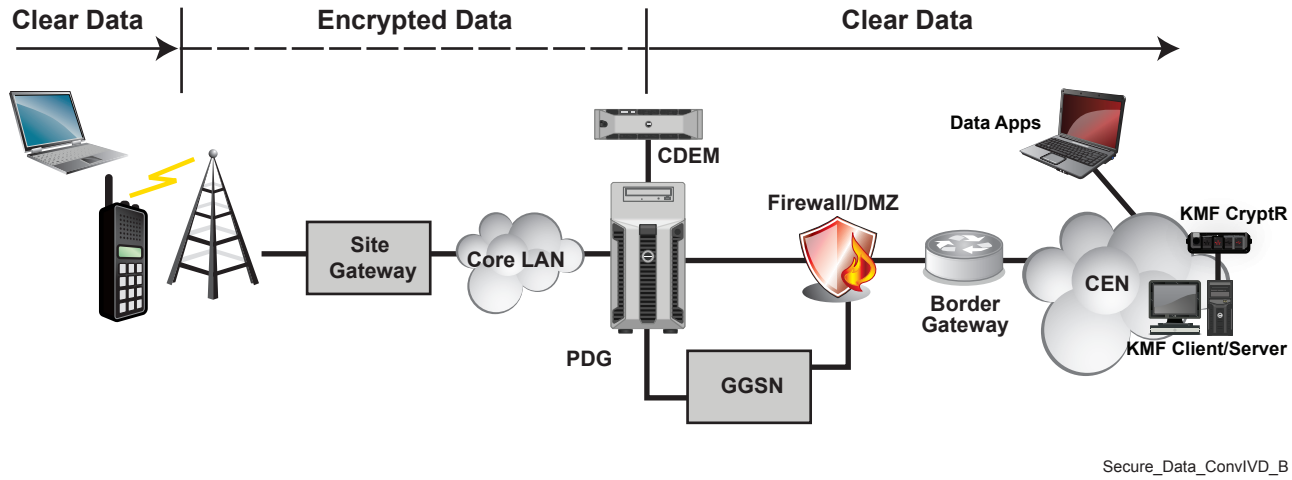
Upon receipt of an outbound datagram, the RNG determines whether the destination subscriber (or broadcast data agency) has been provisioned for secure outbound service and, if so, sends the datagram to the CDEM for encryption. When the response message is received from the CDEM, the RNG creates a header and includes it after the CAI header but before the user data in the outbound encrypted datagram. Outbound processing then proceeds depending on whether the datagram is addressed to a Unicast subscriber or a Broadcast data agency.

Upon receipt of an encrypted inbound datagram, the RNG determines whether the originating subscriber has been provisioned for secure inbound service and, if so, sends the datagram to the CDEM for decryption. The header information received in the inbound datagram is provided to the CDEM as part of this message. When the response message is received from the CDEM, the RNG forwards the datagram to the PDR for delivery to the destination CEN host.

NOTICE: Only the AES and DES-OFB algorithms are supported for ASTRO® 25 Conventional IV&D system data encryption.

For more information, see the *Conventional Data Services* manual.

Figure 11: Secure Data in an ASTRO 25 Conventional IVD System



This page intentionally left blank.

Chapter 2

Key Management Overview

This chapter covers the use of keys in secure communications.

2.1 What Is Key Management?

There are two ways to manage keys in an ASTRO® 25 system:

- Non-centralized, using a key loading device
- Centralized, using the Key Management Facility (KMF)

2.1.1 Initial Key Loading

Initial encryption key distribution is performed manually using a key loader. A key loader is a handheld portable device that connects through a cable to a secure device. The following key loaders are supported in an ASTRO® 25 system: the KVL 3000, the KVL 3000 Plus, and the KVL 4000.

There are two ways to handle initial key loading for a device:

- Store and Forward
- Manual key loading

NOTICE: When manually loading keys to a device, the device must be marked as “Provisioned” before key loading. See the “KMF Configuration” chapter in the *Key Management Facility* manual for more information about marking devices as provisioned.

2.1.2 Key Management

Once keys are initially loaded into the correct radios and other system entities, you must manage key material to ensure that your encryption scheme remains effective. Effective management of keys requires changing them regularly.

2.1.2.1 Rekeying in ASTRO 25 Systems

One way of changing keys is by loading new keys into existing units, known as rekeying. Before the existence of the KMF, changing the encryption keys meant bringing radios into the shop or carrying a hand-held device into the field to load the new keys. With the help of the KMF, new keys can be loaded into radios using Over-the-Air Rekeying (OTAR) or other devices using Over-The-Ethernet Keying (OTEK). The Full Update command sends all OTAR information, including keys, for the selected unit, regardless of currency status. The CKR Update command uses OTAR to assign new encryption keys to a CKR group. All radios that use the CKR are updated by the KMF and acknowledgments are tracked and reflected in the CKR currency display.

A Rekey Request is a message sent from a radio to the KMF requesting an update to the key management information. This request can be encrypted or clear. The KMF automatically sends a response to the radio and begins an update, full or optimized, without any actions required by the

operator. The **Operations Status** view in the KMF Client application displays the status of Rekey Requests and Full Updates.

2.1.2.2
Keyset Changeover

A Crypto Period represents the maximum time a secure system's administrator wants a set of voice and data TEKs to be in service.

When a Crypto Period expires, all the TEKs that are currently in service must be retired, and another set of TEKs must be brought into service.

To help realize this needed behavior, the Key Management Facility (KMF) and the managed devices support two keysets, an active and an inactive keyset.

In anticipation for the expiration of the TEKs in the active keyset, the system administrator can update the inactive keyset with a fresh set of keys for the next Crypto Period. When the active keyset expires, a Keyset Changeover can be used to instruct every device in the managed fleet to switch to the inactive keyset.

2.1.2.3
Key Management Tasks

A wise key management practice is to periodically change key material to stay ahead of any intruders trying to break keys and decipher communications. See Crypto Period Planning on page 51 for more information.

Encryption key management encompasses every stage in the life of a cryptographic key, including:

- Generating new keys
- Distributing keys to secure devices
- Distributing keys to data encryption devices
- Storing keys and key variables in a KVL or in a key kettle
- Deleting keys or objects (such as devices, groups, or KVLs)
- Archiving keys

The Motorola Solutions centralized key management solution allows you to manage all your encryption keys for each secure device using the KMF.

2.2
Non-Centralized Key Management Using KVL

The Motorola Solutions non-centralized key management solution allows you to manage encryption keys for your entire system using one or more key loading devices, such as the KVL 3000, KVL 3000 Plus, or KVL 4000. The KVL is a handheld portable device that connects to a secure device through a cable.

The KVL supplies the encryption keys the secure device needs to perform encryption and decryption operations. The KVL uses Traffic Encryption Keys (TEKs) to encrypt voice or data. To load keys manually, do one of the following:

- Take the KVL to the secure device (such as a radio).
- Bring the secure devices to the KVL.

If you have many portable or mobile radios in your system, this process can take a considerable amount of time, especially if the radios are widely dispersed.

NOTICE: Additionally, the KVL initializes secure devices for OTAR, OTEK, and Store and Forward operations.

2.2.1 Tactical OTAR

Tactical OTAR is a Motorola Solutions feature that allows a KVL to wirelessly manage a key (TEK only) for a small group of radios, with one radio serving as an RF modem.

NOTICE:
The radio serving as an RF modem must be equipped with the Tactical Rekey/OTAR feature.

The radio serving as an RF modem may also be a member of any one of the managed Tactical OTAR groups.

For details about configuring tactical OTAR, see the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*, depending on your KVL model.

2.3 Centralized Key Management Using the KMF

Centralized key management uses the KMF to associate groups of devices with specific keys. When these associations have been created, the keys must be loaded into the correct devices for the encryption scheme to function. There are four methods of transporting keys using the KMF:

- Over-The-Air Rekeying (OTAR)
- Store and Forward rekeying
- Over-The-Ethernet Keying (OTEK)
- Exported Encrypted Key File

The key transport method you use depends on the types of secure devices you have and the capabilities of your system.

2.3.1 Over-The-Air Rekeying (OTAR) in ASTRO 25 Systems

OTAR provides the ability to rekey portable and mobile radios remotely over an RF channel.

The KMF formulates and originates the OTAR messages and acts as the key manager for the system. OTAR provides several benefits, including:

- Reducing the manpower and time in the field to rekey radio users manually, leading to improved productivity.
- Offering an advanced key management solution that allows you to plan, generate, store, track, and maintain all encryption keys for the entire system using one central device instead of tracking everything on paper. This solution reduces key management resources.
- Providing the ability to change your encryption keys frequently, which enhances the security of your system by eliminating security leaks.

IMPORTANT: In IP systems does not support OTAR. Use the KVL or Store and Forward Rekeying to change keys.

2.3.1.1
OTAR Registration/Context Activation

The OTAR client process uses a registration procedure to inform the KMF Server of its presence. The registration procedure:

- Creates a communication path between the radio's OTAR client application and the server.
- Provides an opportunity to the server to update the radio's OTAR client. When the server receives a registration KMM, the server can send the required KMMs that the radio's OTAR client has missed.

For ASTRO® 25 Conventional IV&D systems, ASTRO® 25 Conventional IV&D registration for manually registered subscribers occurs automatically when the Conventional PDG starts up. To avoid sending OTAR Registration messages to the KMF at too high a rate if many subscribers are configured, the PDG introduces a random delay in their OTAR registration time, based on the setting of the Maximum OTAR Registration Delay parameter provisioned via the Network Manager. The delay also takes into account the number of OTAR registration transactions outstanding between the Conventional PDG and the KMF so that the delay is longer when many transactions are outstanding.

2.3.1.2
IP Allocation for Radios

NOTICE: This section applies to ASTRO® 25 Trunking IV&D systems only.

In ASTRO® 25 Trunking IV&D systems, the radio communicates with the KMF using Data Bearer Transport (through the Packet Data Gateway). The KMF uses a configurable User Datagram Protocol (UDP) port value as a UDP port address of the radio's OTAR client applications. The OTAR client application uses UDP to send KMMs. The radio requests a dynamic IP address as part of IV&D context activation. The PDG then supplies the IP address to the radio. Depending on your organization, the PDG either uses an IP address that was assigned to the unit through Network Management, or gets a dynamic IP address from a DHCP server.

An alternative approach to obtaining the IP address is for the radio to have a CPS-programmed IP address to use. In this case, the radio does not request an IP address during the IV&D context activation.

The KMF uses the UDP/IP protocol when transporting (that is, sending/receiving) KMMs to a radio. The KMF obtains the IP address of a radio from the IP header of the KMM (that is, OTAR Registration) that the radio sends. On receipt of the registration KMM, the KMF creates or updates a binding between the source Radio Set Identifier (RSI) and the source network/transport layer address. The KMF uses the binding between the RSI for the radio's OTAR client and the network/transport layer address to send the KMMs.

2.3.1.3
Retry Opportunities

If a Key Management Message (KMM) delivery fails, the KMF marks the radio for a Retry Opportunity (ROP). Reasons for failure include:

- The radio is not on the air. Its power is either switched off, or it is outside the coverage area.
- The radio is not context-activated.
- The radio is busy in voice-related activity. The voice-related activity has higher priority than data.
- The KMM is lost during transportation.
- The radio is not tuned to a data-capable Conventional channel when the attempt is made (ASTRO® 25 Conventional IVD only).

NOTICE: The Retry Opportunity feature can be enabled or disabled in the KMF.

In response to a Retry Opportunity, the KMF can be configured to respond with either a Full Update or an Optimized Update.

2.3.1.3.1
Retry Opportunities for ASTRO 25 Trunking IVD Systems

In ASTRO® 25 Trunking IVD systems, the KMF Server receives information about the delivery failure of a Key Management Message (KMM) by the absence of an application layer acknowledgment. After the initial failure, the KMF Server keeps the state information (for example, keys, RSI, keyset attributes, and so on) for the radio. The KMF Server delivers all the information (Update) to the radio when it hears from the radio. The Registration KMM or a Rekey request from the radio can trigger the Update. After successfully sending an Update, the KMF Server clears the Retry Opportunity (ROP) flag to indicate that the radio does not have a pending update.

The KMF retries the unit update. If the unit update is unsuccessful, the system can follow the retry procedure an unlimited number of times.

A registration KMM is sent on every context activation or change of the associated KMF Server.

2.3.1.3.2
Retry Opportunities for ASTRO 3.1 Conventional IVD Systems

In ASTRO® 3.1 Conventional IVD systems, after a KMF initiates a Unit Update, and the KMF does not receive an acknowledgment from the targeted unit (the KMF receives a message from the Wireless Network Gateway (WNG) or Radio Network Controller (RNC), indicating that the KMM could not be delivered). The WNG may deliver a `not-registered` message after checking the targeted unit's address against its registration log. The RNC may deliver a `no service` message after checking the status of the targeted unit through the Confirmed Data Service feature.

The KMF places the unit on the Retry Opportunity (ROP) list, which identifies units still in need of an Update. Placing a unit on the ROP list sets a trap for the unit in the RNC, which waits to hear from the unit. When the targeted unit becomes active, the RNC hears either packet data or Digital Interface Unit (DIU) sourced voice logging datagrams from it. The RNC sends a message through the WNG to the KMF, informing the KMF that the unit is registered and in service. The KMF retries the unit update. If the unit update is unsuccessful, the system can follow the retry procedure an unlimited number of times.

A registration KMM is sent on every context activation or change of the associated KMF Server.

2.3.1.3.3
Retry Opportunities for ASTRO 25 Conventional IVD Systems

The ASTRO® 25 Conventional IVD KMF Server receives information about the delivery failure of a Key Management Message (KMM) by the absence of an application layer acknowledgment. After the initial failure, the KMF Server keeps the state information (for example, keys, RSI, keyset attributes, and so on) for the radio. The KMF Server delivers all the information (Update) to the radio when it next hears from the radio.

When a Conventional subscriber sends packet data or finishes an inbound audio call on a data-capable channel, the Site Gateway (Conventional Channel Interface) sends a message to the Conventional IVD Packet Data Gateway (PDG) indicating the subscriber is on the channel. If the subscriber is OTAR-capable, the Conventional PDG sends a message to the serving KMF, indicating an attempt may be made to rekey the subscriber. These notifications are only sent to the KMF if such a message has not already been sent for the same subscriber within the previous 10-minute period.

The KMF retries the unit update. If the unit update is unsuccessful, the system can follow the retry procedure an unlimited number of times.

A registration KMM is sent on every context activation or change of the associated KMF Server.

2.3.1.4
Support for Rekey Request

A subscriber unit can request a rekey from the KMF. If the subscriber has lost or manually removed their TEKs, or has possibly missed an update or keyset changeover, they may need to manually initiate a rekey. If a radio is manually zeroized, the UKEKs are lost and a rekey request is not processed. All models of Motorola OTAR radios support rekey request through button selection. Model 2 and Model 3 portables also support rekey request via a menu selection.

2.3.2
Store and Forward Rekeying

With Store and Forward Rekeying, the KMF delivers the encryption keys and related information to secure units using a KVL.

Use Store and Forward Rekeying in the following situations:

- When you are initially provisioning secure units in an OTAR system.
- When the secure units (radios) are not within broadcast range for OTAR, but do have a phone line or modem available. In this situation, the KVL uses the modem to dial into the KMF for key material.

The KMF can download KMMs to a connected KVL by using Clear Store and Forward, Encrypted Store and Forward, or Auto Store and Forward. In Clear Store and Forward, the KMF only sends KMMs that are encrypted using the UKEK and the Warm Start key for the KVL. In Encrypted Store and Forward, the KMF only sends KMMs that are encrypted using the UKEK and the TEK for the target radio. The keys remain encrypted until the target device decrypts the KMMs with their own UKEK. In Auto Store and Forward, the KMF decides the best method to use for the appropriate device, either Clear or Encrypted.

2.3.3
Over-The-Ethernet Keying (OTEK)

OTEK provides the ability to rekey consoles, AISs, CDEMs (ASTRO® 25 Conventional IV&D systems only), PDEGs (ASTRO® 25 Trunking IV&D systems only), and TMGs remotely over the Ethernet. OTEK works the same as OTAR except that the KMMs are delivered over an Ethernet connection rather than over the air.

2.3.4
Key Management in an ASTRO 25 Trunking IVD System

Table 1: Key Management Devices in an ASTRO 25 Trunking IVD System

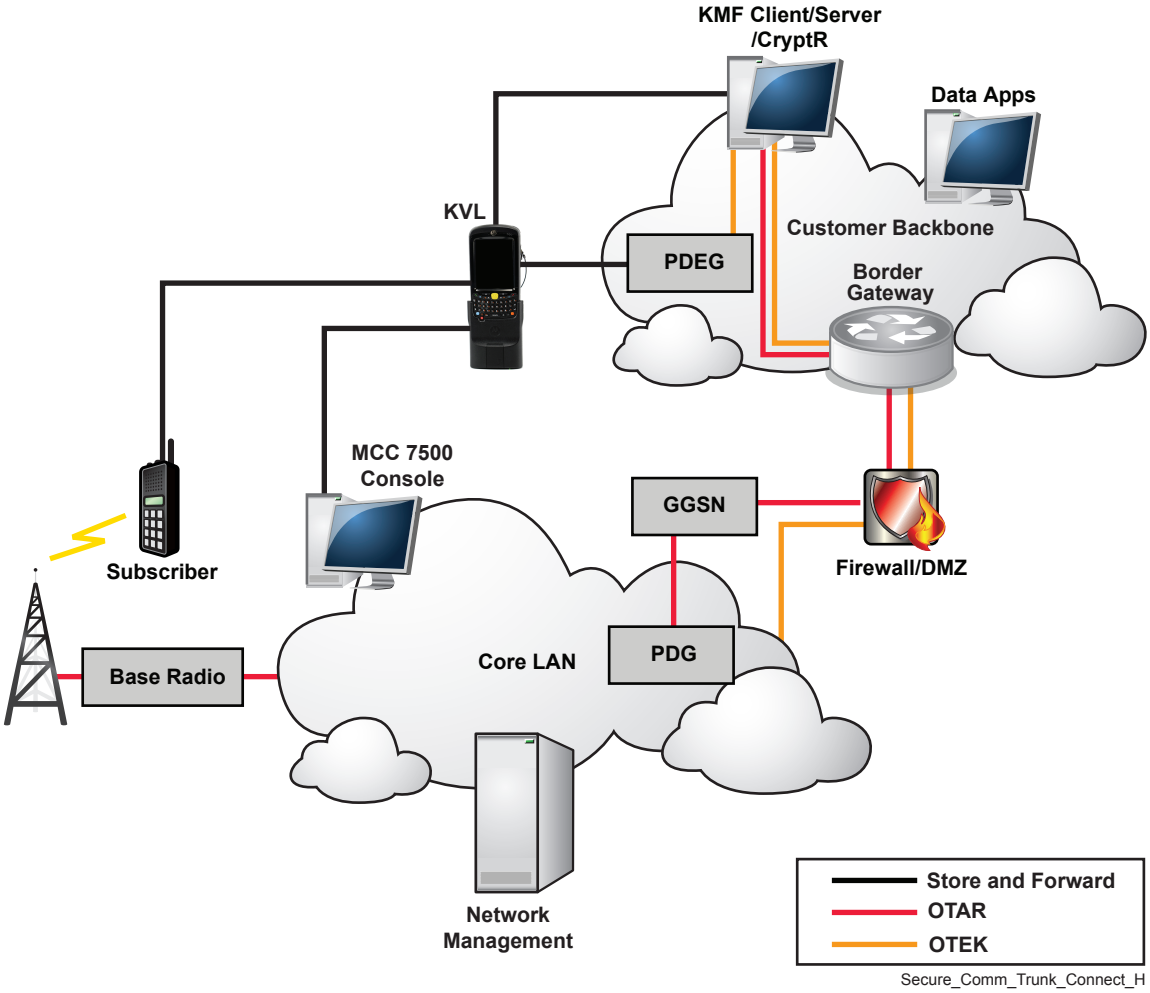
Device	Function
Packet Data Gateway (PDG)	Provides the interface between the Customer Enterprise Network (CEN) and packet data users in the system. The PDG performs registration services for packet data users, maintains user permissions and mobility information, as well as provides routing of traffic to the radio network or the GPRS Gateway Support Node (GGSN) router.

Table continued…

Device	Function
Packet Data Router (PDR)	The PDR is a software component of the PDG which provides tunneling of packet data traffic to the GGSN router, which then routes the traffic to the Customer Enterprise Network (CEN).
Radio Network Gateway (RNG)	The RNG is a software component of the PDG that interfaces with the remote sites to handle inbound/outbound packet data traffic between the remote sites and the PDR. The RNG provides a logical connection to the sites, and facilitates delivery of traffic between the PDR and the remote sites.
Gateway GPRS Support Node (GGSN)	Special purpose device that provides a network interface between the CEN and the radio network.
PDEG Encryption Unit	Encrypts, decrypts, and authenticates data transmissions entering and leaving the CEN.
Key Variable Loader (KVL)	Enables Store and Forward operations
MCC 7500 Console	Motorola Solutions IP-based Dispatch Console system
MCC 7100 IP Dispatch Console	Motorola Solutions software-based console
Subscriber	User of telecommunications services attached to the network (that is, a radio)

The following figure shows the key management architecture for ASTRO® 25 Trunking IV&D systems:

Figure 12: Key Management in an ASTRO 25 Trunking IVD System



2.3.5

Key Management in an ASTRO 3.1 Conventional IVD System

Table 2: Key Management Devices in an ASTRO 3.1 Conventional IVD System

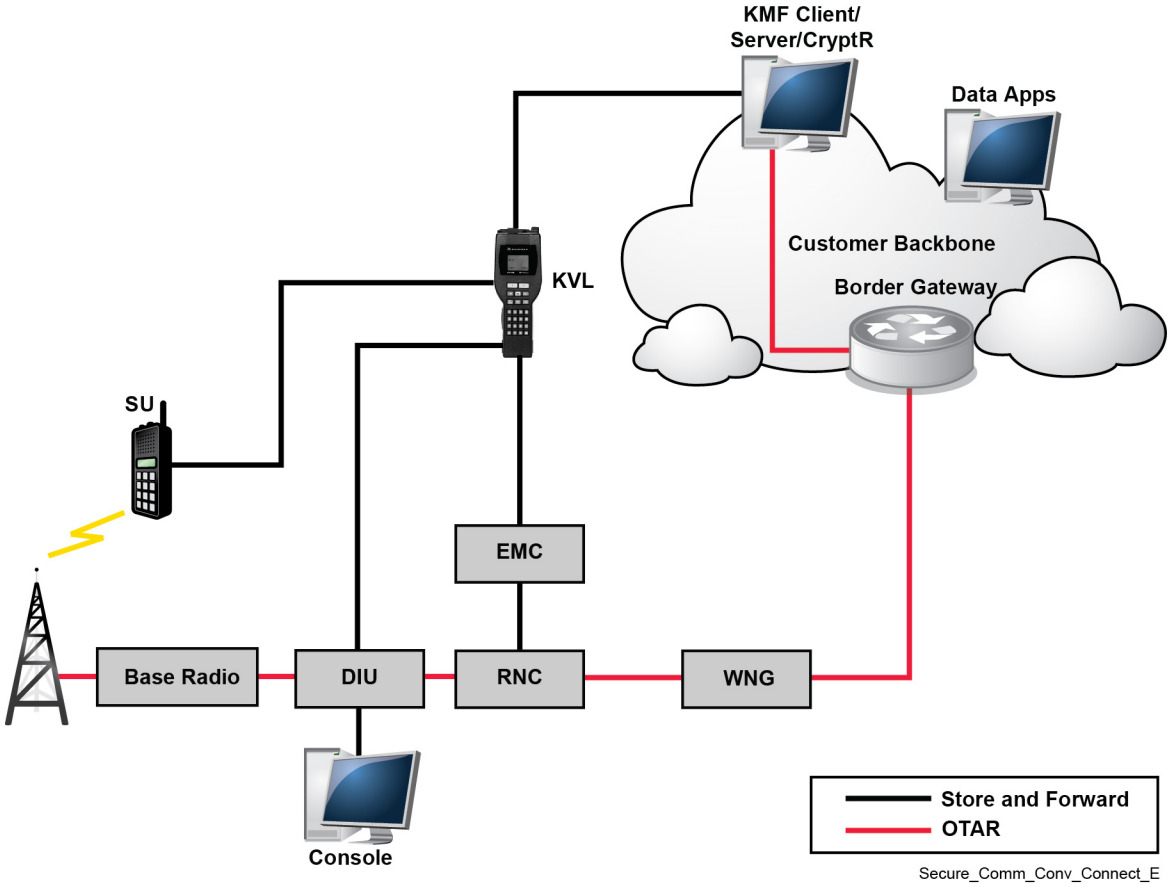
Device	Function
Wireless Network Gateway (WNG)	Manages data connections with CEN; registers radios to enable OTAR.
Radio Network Controller (RNC)	Routes data packets over the infrastructure links to the sites in the zone.
Encryption Module Controller (EMC)	Connects to the RNC and allows the RNC to encrypt or decrypt secure data traffic (not including KMMs) as the traffic passes between the conventional radios and the customer host network.
Digital Interface Unit (DIU)	A transcoding device used to convert digital signals to analog signals (and the other way around) between console positions and other components of

Table continued…

Device	Function
	the system. The encryption cartridge in the DIU provides encryption and decryption services between the console or telephone interconnect devices and radios.
Key Variable Loader (KVL)	Enables Store and Forward operations.
Subscriber	User of telecommunications services attached to the network (that is, a radio)

The following figure shows the key management architecture for ASTRO® 3.1 Conventional IV&D systems:

Figure 13: Key Management in an ASTRO 3.1 Conventional IVD System



2.3.6
Key Management in an ASTRO 25 Conventional IVD System

Table 3: Key Management Devices in an ASTRO 25 Conventional IVD System

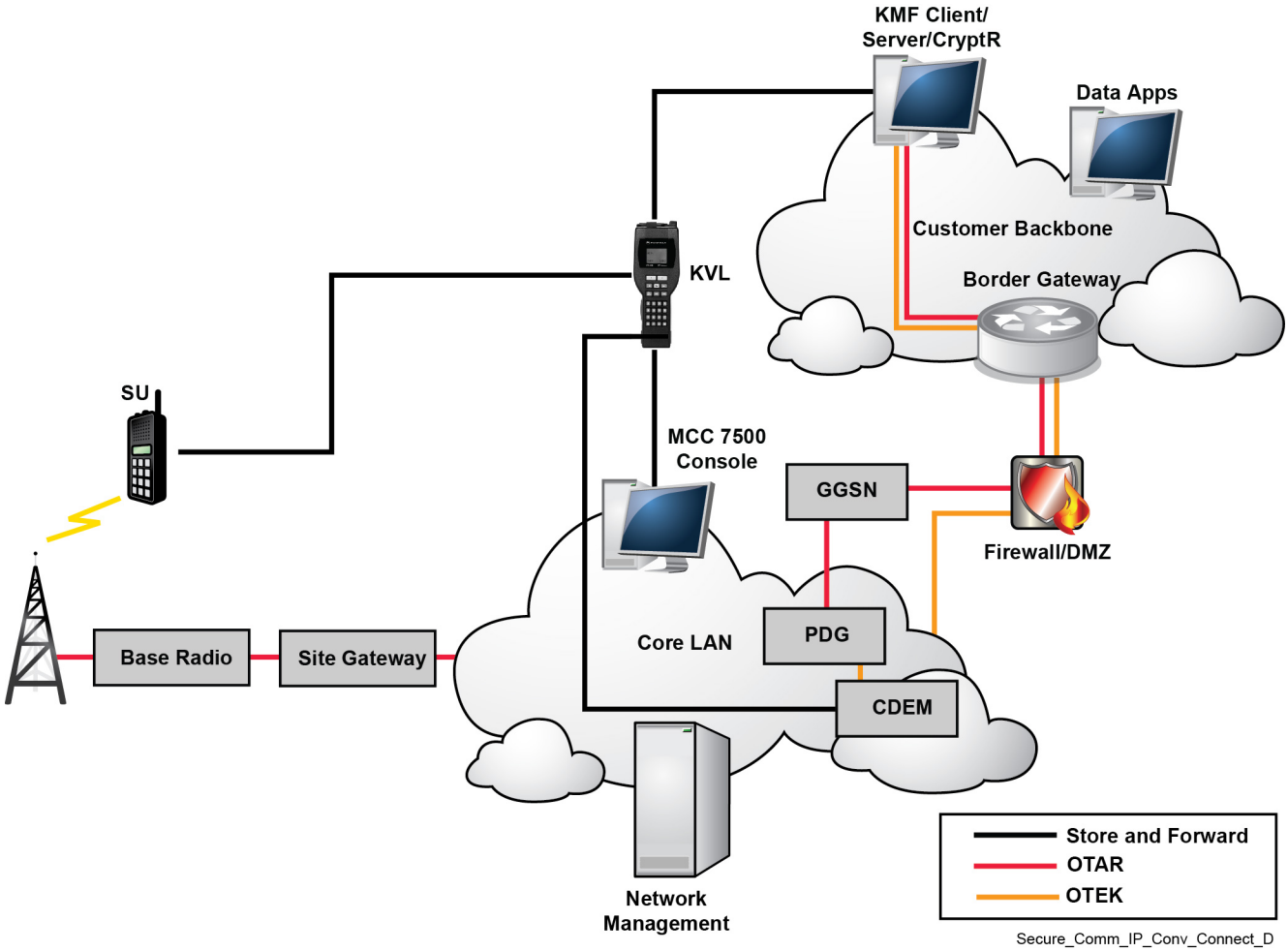
Device	Function
Packet Data Gateway (PDG)	Receives data from either the Customer Enterprise Network (CEN) or from a subscriber via Conventional RF equipment. If secure data services are required, PDG

Table continued…

Device	Function
	passes data to the CDEM, communicating with KMF on behalf of CDEM.
Packet Data Router (PDR)	Manages packet data registrations, authorizing registration requests based on packet data registration information provisioned through the Network Manager. Also manages subscriber deregistrations.
Radio Network Gateway (RNG)	Routes data packets over the infrastructure links to the sites in the zone.
CAI Data Encryption Module (CDEM)	If secure data services are required, receives data from the PDG, performs data encryption or decryption operations, and sends the data back to the PDG for transmission to its final destination.
Site Gateway (Conventional Channel Interface)	Interfaces with the RNG component of the PDG to manage access to the conventional channel resource for conventional data.
Key Variable Loader (KVL)	Enables Store and Forward operations.
Gateway GPRS Support Node (GGSN)	Special purpose device that provides a network interface between the CEN and the radio network.
MCC 7500 Console	Motorola Solutions IP-based Dispatch Console system
MCC 7500 Archiving Interface Server (AIS)	Provides an interface between the Motorola Solutions radio system and the MCC 7500 IP Logging Recorder.
MCC 7100 IP Dispatch Console	Motorola Solutions software-based console
Subscriber	User of telecommunications services attached to the network (a radio)

The following figure shows the key management architecture for ASTRO® 25 Conventional IV&D systems:

Figure 14: Key Management in an ASTRO 25 Conventional IVD System



2.4 Encryption Key Overview

An encryption key is a variable used in combination with an encryption algorithm to encrypt and decrypt voice, data, or key messages. Encryption is based on subjecting digitized signals to numerical variables so the signals cannot be interpreted by anyone but the intended parties. Subscriber units (for example, radios) without encryption keys cannot communicate in secure mode.

NOTICE: Throughout this manual, the term “secure key” is used to describe either a CKR index number (used for ASTRO® Trunking, Digital Conventional, ACIM, and Mixed Mode Channels) or a Key Number (used for Advanced SECURENET® Analog Conventional and MDC 1200 Channels).

2.4.1
Key Types

The types of keys used in an ASTRO® 25 system are described in the following table:

Table 4: Key Types

Key Type	Description
Master Key	A key used to encrypt and decrypt all key material stored in the KMF database.
Traffic Encryption Key (TEK)	Encrypts voice, data, or Over-The-Air Rekeying (OTAR) and is assigned to Common Key References (CKRs). For OTAR, the TEK is used to outer layer encrypt the KMMs.
Unique Key Encryption Key (UKEK)	A key assigned to a subscriber for encrypting keys within an individually delivered OTAR command. For OTAR, the UKEK is used to inner layer encrypt the KMMs.
Common Key Encryption Key (CKEK)	A key assigned to a group of units for encrypting keys within an OTAR command delivered using the group OTAR method. It is provisioned on the trunking system but only used for conventional OTAR channels.
Key Loss Key (KLK)	Enables a KMF to restore a unit's UKEK after it has been erased by using the unit's Key Loss Key to receive OTAR commands.

2.4.2
Key Management Messages

The KMF uses Key Management Messages (KMMs) to communicate encrypted information to radios, infrastructure, and data devices. This encrypted information may include the following information for the SUs:

- load initial keys
- load new keys (rekey)
- keyset changeover
- change radio set identifier (RSI)
- change UKEK

These KMMs are transferred to a unit manually using the Key Variable Loader (KVL) or using the RF interface. KMMs are composed and encrypted at the KMF Server using two layers of encryption: inner and outer. The inner layer is encrypted using a UKEK, while the outer layer is encrypted using a TEK. This scheme protects the integrity of any key data in the KMM and it requires two types of keys to be designated and managed by the KMF.

2.4.3
Where Keys Are Used

Keys are used in the ASTRO® 25 components listed in this section.

ASTRO® 25 systems support both Common Key Reference (CKR) and Physical Identifier (PID) key storage, which are described in the next section.

Table 5: Where Keys Are Used

Secure Data Type	ASTRO® 25 Trunking IV&D System	ASTRO® 3.1 Conventional IV&D System	ASTRO® 25 Conventional IV&D System
Traffic Encryption Key (TEK)	KMF, Radio, KVL, MCC 7500, AIS, PDEG	KMF, Radio, KVL, DIU, RNC	KMF, Radio, KVL, MCC 7500, CDEM
Unique Key Encryption Key (UKEK)	KMF, Radio, KVL, MCC 7500, AIS, PDEG	KMF, Radio, KVL, DIU, RNC	KMF, Radio, KVL, MCC 7500, CDEM
Common Key Encryption Key (CKEK)	Not used	KMF, Radio	KMF, Radio
Key Loss Key (KLK)	KMF, Radio	KMF, Radio	KMF, Radio

2.4.4 Where Keys Are Stored

Keys are stored in the Common Key Reference (CKR) or the Physical Identifier (PID) (for prior system releases).

2.4.4.1 Common Key Reference Storage

The Common Key Reference (CKR) is a storage location for keys used in encrypted calls by the subscriber. Each CKR contains two TEKs (one active and one inactive) used by radios and infrastructure for secure voice and OTAR operations. ASTRO® 25 systems support the use of CKR key management to reference and identify encryption keys in:

- MCC 7500 Dispatch Console (ASTRO® 25 Trunking IV&D or ASTRO® 25 Conventional IV&D systems)
- DIU 3000 (ASTRO® 3.1 Conventional IV&D systems only)
- RNC 3000 (ASTRO® 3.1 Conventional IV&D systems only)
- ASTRO® digital radios
- Key Management Facility (KMF)
- KVL: 3000, 3000 Plus, and 4000
- PDEG Encryption Unit (ASTRO® 25 Trunking IV&D systems only)
- CDEM (ASTRO® 25 Conventional IV&D systems only)
- AIS
- MCC 7100 IP Dispatch Console
- Provisioning Manager (PM): although no actual keys are stored in PM, it is used to assign a CKR to a talkgroup.

Each encryption key is associated with a system-wide key reference, commonly referred to as a CKR; the same key is referenced by the same CKR in every secure component. The CKRs are assigned to

talkgroups, multigroups, and other voice functions (that is, private calls, emergency calls, interconnect calls) in the radio. CKRs are also assigned to subscribers for data encryption.

In ASTRO® 25 Trunking IV&D and ASTRO® 25 Conventional IV&D systems: The MCC 7500 Dispatch Console receives the CKR mapping for talkgroup calls, private calls, and supergroup calls from the Provisioning Manager (PM) records through the Zone Database Server (ZDS). The MCC 7500 Dispatch Console stores this information internally and is able to retrieve the appropriate CKR when an encrypted call request is received.

NOTICE: The console sets up a supergroup when it regroups several talkgroups into a single group. This supergroup lets the regrouped talkgroups talk to each other.

CKR key management is compatible with the APCO Project 25 definition of Storage Location Number (SLN) key variables.

In ASTRO® 3.1 Conventional IV&D systems: Each encryption key is associated with a system-wide key reference, commonly referred to as a CKR; the same key is referenced by the same CKR in every secure component. The DIU 3000 and RNC 3000 store this information in their encryption modules and are able to retrieve the appropriate CKR when an encrypted call request is received.

CKR key management supports mapping of encryption keys in a device-independent manner. All devices that support CKRs access the same encryption keys, independent of the physical storage capabilities of the device. Radios that support CKR Key Storage have the capability of mapping PIDs to CKRs for backward compatibility. The Customer Programming Software (CPS) feature allows you to load CKR radios with a PID-based key loader (such as the KVL 3000 Plus), and still operate using CKRs. The user does not need to know that Key 3 in one radio is the same as Key 6 in a second radio, and Key 400 in the infrastructure encryption card. This feature allows you to assign CKR 1 to all secure devices in your system using a logical, system-wide reference, instead of a local physical, reference.

- The KMF loads the same key under 1 to each device.
- If, for example, Talkgroup X uses 1, whenever someone makes a call on Talkgroup X, all devices that belong to that talkgroup use the same key.

2.4.4.2
Physical Identifier Key Storage (for Prior System Releases)

Physical Identifier (PID) key storage identifies a physical memory slot that can store a key variable in a secure device. All products that support PIDs access the same encryption keys depending on the physical storage capability of the product.

PID key storage can be complex for system installers and radio programmers. The system installers or radio programmers have to determine which slots to put the keys into to make secure operation transparent to the radio and console operators. For example, the radio programmer must know that Radio 1 has a particular key in slot 1, Radio 2 has the same key in slot 3, and the infrastructure encryption card has the same key in slot 4. The following table shows an example with slots containing different keys. When using PID key storage, manage key-to-slot assignments on paper to determine whether different devices match up.

Table 6: Physical ID Key Storage Example

Radio 1 Encryption Module	Radio 2 Encryption Module	Radio Infrastructure Encryption Module
Slot 1 - Key A	Slot 1 - Key D	Slot 1 - Key A
Slot 2 - Key B	Slot 2 - Key B	Slot 2 - Key B
Slot 3 - Key C	Slot 3 - Key C	Slot 3 - Key C
Slot 4	Slot 4	Slot 4 - Key D

Table continued...

Radio 1 Encryption Module	Radio 2 Encryption Module	Radio Infrastructure Encryption Module
Slot 5	Slot 5	Slot 5

NOTICE:
Some devices begin numbering at Slot 0, in which case the slot numbers would be 0, 1, 2, 3, and 4.

For Advanced SECURNET® Conventional Operation, the PID-based secure keys are loaded into the infrastructure encryption device (CIU) for each ASN channel. Then the corresponding key numbers are assigned to channel resources by the Provisioning Manager to allow them to be selected at the console. Therefore, ASN secure keys are referred to as *Key Numbers* to differentiate them from CKRs used for other channel types.

2.5 Planning for Key Management

This section covers a planning strategy for determining keys used for secure communications.

2.5.1 Key Mapping

The key map is the basic plan your organization creates so that the relationships between groups, encryption keys, keysets, and Common Key References (CKRs) can be planned out and understood.

Before setting up the system, your organization needs to consider such questions as:

- What groups must talk to each other on a regular basis?
- Are there groups within groups that must be able to communicate securely?
- Are there groups that must communicate securely, but not as often?
- What group or groups is the console communicating with?

For example, the start of such a plan may include the following three groups that need secure communications. Within each group, subgroups that must maintain secure communications separate from the larger group are identified.

- Fire Department
  - Fire Company #1
  - Fire Company #2
- Police Department
  - Precinct 1
  - Precinct 2
- Search and Rescue
  - Harbor Area
  - Mountain Villas

Once the various groups are determined, keys and CKRs can be set up.

2.5.1.1 Common Key Reference (CKR) Planning in ASTRO 25 Systems

In an ASTRO® 25 system, radios communicate using clear talkgroups that are managed using Customer Programming Software (CPS) at the radio. Centralized key management imposes a layer of

encryption over these clear talkgroups. This encryption layer is created by distributing certain keys to certain users, forming secured groups because only users with keys in common are able to communicate in secured mode. These groups of users share encryption keys called CKRs that are created and managed using the KMF. All devices in the system use Common Key References (CKRs) to select a key to use for initiating outgoing secure communications.

Determine CKRs in coordination with the overall communications plan. In a KMF-managed system, all devices assigned to the same CKR are provisioned with the same key data for securely communicating with one another.

Table 7: Groups Needing Secure Communications - Example

In this example, the organization assigned a unique Key ID to each encryption key during the key map design. The Key ID is an identification number that identifies a key without revealing an actual key variable. Radios, MCC 7500 Dispatch Consoles, MCC 7100 IP Dispatch Consoles, and Dynamic Transcoders use the Key ID to identify the correct key for each encrypted voice call in the ASTRO® 25 system. Encryption key and CKR aliases are optional. The alias aides the radio users or console operators to identify the purpose for the key or CKR.

NOTICE: A CKR number can point to any encryption key in the system. The match between Key IDs and CKR number IDs is used only as an example of initial key map planning.

Group	Encryption Key ID	Encryption Key Alias	CKR Number	CKR Alias
Fire Department	01	FireKey1	99	Fire_01
• Company 1	02	FireKey2	98	Fire_02
• Company 2	03	FireKey3	97	Fire_03
Police Department	11	PoliceKey1	89	Police_01
• Precinct 1	12	PoliceKey2	88	Police_02
• Precinct 2	13	PoliceKey3	87	Police_03
Search and Rescue	21	RescueKey1	79	Rescue_01
• Harbor	22	RescueKey2	78	Rescue_02
• Mountain	23	RescueKey3	77	Rescue_03

Users are grouped according to their need to communicate in secure mode once the groups, keys, and CKRs have been identified.

Table 8: Mapping CKRs - Example

In this example, keys are mapped to CKRs, CKRs are mapped to talkgroups, and radio users with access to the talkgroups are identified. With the mapping shown in this example, members of the Fire Department can communicate with each other in secure mode. Members of the police department can also communicate with each other, but not with the fire department.

Talkgroup	Radio ID	Device User	CKRs	Key
Fire Department	123456	Fire A	Fire_01	FireKey_1
	123457	Fire B	Fire_01	FireKey_1
	123458	Fire C	Fire_01	FireKey_1

Table continued…

Talkgroup	Radio ID	Device User	CKRs	Key
Police Department	223456	Police Q	Police_02	PoliceKey_1
	223457	Police R	Police_02	PoliceKey_1
	223458	Police S	Police_02	PoliceKey_1

Typically, console operators must be able to talk to all the different groups. Since the consoles have a graphical user interface (GUI), they can click icons to connect to communication resources. Each of these resources has an individual ID. Consequently, a talkgroup resource has two identifiers: the resources individual ID and the talkgroup ID.

Table 9: Mapping CKRs to Console Operator Positions - Example (ASTRO 25 Systems)

This table shows an example of how consoles are mapped. In this example, Operator 1 can talk to the various fire department groups, while Operator 2 can talk to the police groups. However, Operator 1 cannot talk to the police groups, and Operator 2 cannot talk to the fire department groups.

Console Operator	Talkgroup	Radio ID	Talkgroup Alias	CKRs	Key
Operator 1	Fire Department	123466	Fire A	Fire_01	FireKey_1
		123467	Fire B	Fire_01	FireKey_1
		123468	Fire C	Fire_01	FireKey_1
Operator 2	Police Department	223466	Police Q	Police_02	PoliceKey_1
		223467	Police R	Police_02	PoliceKey_1
		223468	Police S	Police_02	PoliceKey_1

2.5.1.2

Crypto Period Planning

The crypto period is the time span during which an encryption key remains valid for use. You determine a crypto period according to the security policies defined by your organization, such as how often keys are changed and who initiates the changes. Typical crypto periods can be bi-weekly, monthly, or quarterly.

In the KMF, two keysets are assigned to each Common Key Reference (CKR), one active and one inactive. Using the Keyset Changeover OTAR command, the keysets can be toggled according to the established crypto period. After all units are current, the formerly active (used) keyset is made inactive, and can be renamed and replaced without any interruption of secured communications. Using the CKR Update OTAR command, the new key material in the inactive keyset is loaded onto all radios in the CKR for the next instance of the keyset changeover cycle.

Table 10: Sequence of Events in an Example Bi-Weekly Crypto Period

Day of Week	Crypto Period Activity
Week 1: Monday	6:00 AM Night shift is on the air
	6:00 AM Execute Keyset Changeover
	6:00 AM Unit Retry Opportunities (ROPs) occur as units appear on the air
	7:00 AM Day shift starts going on the air
	7:00 AM Night shift goes off the air

Table continued…

Day of Week	Crypto Period Activity
	6:00 PM DB Backup 7:00 PM Day shift goes off the air 7:00 PM Night shift goes on the air Unit ROPs continue throughout the night (Typically 70% of the units on the air may be rekeyed by the end of Change-over day, though currency may reflect less than this)
Week 1: Tuesday through Sunday	Unit ROPs continue 7:00 AM Day shift starts going on the air 7:00 AM Night shift goes off the air 6:00 PM DB Backup 7:00 PM Day shift goes off the air 7:00 PM Night shift goes on the air
For week 1, typically: 80% of the units on the air may be rekeyed by the end of day 2. 90% of the units on the air may be rekeyed by the end of day 3. 95% of the units on the air may be rekeyed by the end of day 4. 99% of the units on the air may be rekeyed by the end of days 5-7. Currency may reflect less than these amounts.	
Week 2: Monday	6:00 AM Night shift is on the air 6:00 AM Rename Inactive Keyset 6:00 AM Create new TEKs 6:30 AM Associate new TEKs to the inactive keyset of each CKR 6:30 AM Execute CKR Update 6:30 AM Unit ROPs occur as units appear on the air 7:00 AM Day shift starts going on the air 7:00 AM Night shift goes off the air 6:00 PM DB Backup 7:00 PM Day shift goes off the air 7:00 PM Night shift goes on the air Unit ROPs continue throughout the night (Typically 70% of the units on the air may be rekeyed by the end of key change day)
Week 2: Tuesday through Sunday	Unit ROPs continue 7:00 AM Day shift starts going on the air 7:00 AM Night shift goes off the air 6:00 PM DB Backup 7:00 PM Day shift goes off the air

Table continued…

Day of Week	Crypto Period Activity
	7:00 PM Night shift goes on the air
For week 2, typically: 80% of the units on the air may be rekeyed by the end of day 2. 90% of the units on the air may be rekeyed by the end of day 3. 95% of the units on the air may be rekeyed by the end of day 4. 99% of the units on the air may be rekeyed by the end of days 5–7. Currency may reflect less than these amounts.	

2.5.1.3
Cryptographic Separation in a Multi-Agency System

To achieve cryptographic separation in a multi-agency system with MCC 7500 consoles, each agency has its own MCC 7500 consoles with each agency controlling the consoles' encryption keys. For the MCC 7500 consoles, there is no need to rely on shared resources and shared key management. The MCC 7500 consoles offer true end-to-end encryption.

2.5.1.4
Secure Interoperability With Channels Having Different Encryption Key Types

CKRs for Digital channels can be mapped to ASN Key Numbers to achieve secure interoperability at the Console using both types of encrypted channels to communicate with radios using either type of channel.

Although the configuration of secure keys (Key Numbers) for the Advanced SECURENET® Conventional Operation is different from the configuration of keys (CKRs) for digital conventional channels, there is a way to set up the key configuration to achieve secure interoperability between them if required. For example, limitations or differences in radio equipment between groups or users may drive the need for setting up key interoperability between CKRs and ASN Key Numbers.

2.5.1.4.1
MultiSelect (MSEL) and MO (Momentary Override) Features

The console operator can make a secure call on a mix of the following channel types with a single secure key selection. Such a secure key is referred to as an “interoperable key”.

- Digital conventional channels (Digital, Mixed Mode, and ACIM)
- Advanced SECURENET® channels

This is done using a MultiSelect (MSEL) group containing the above types of secure channel resources. The group transmit is performed on the MSEL group using a selected secure key reference from the Momentary Override (MO) console capability. The following sections provide information about configuring the MO key to enable these communications.

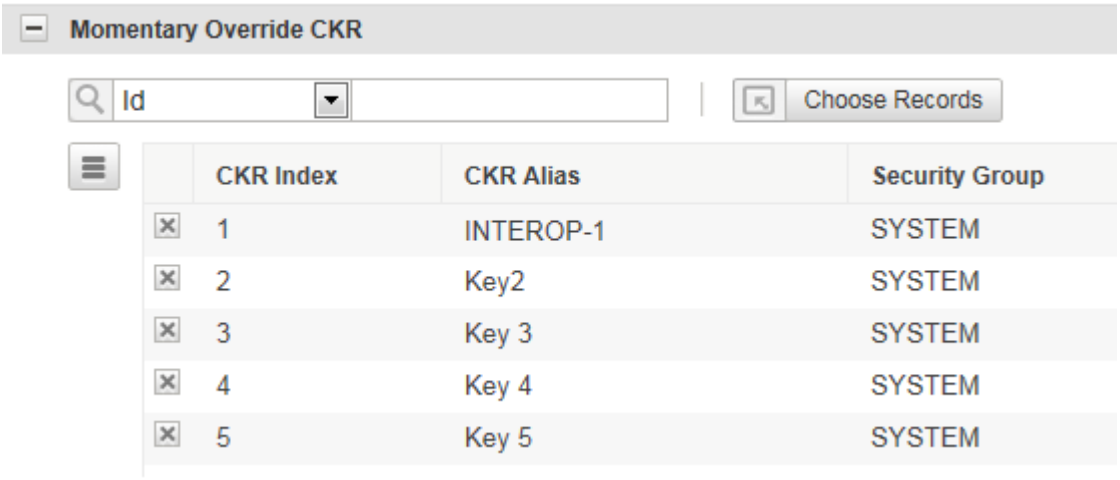
2.5.1.4.2
Interoperable Key Reference Configuration

In the MO key selection configuration tab of the Provisioning Manager (PM), only CKR Indexes can be selected. See Figure 15: Momentary Override and Channel Configuration in the PM – Console User Capabilities Profile on page 54.

For ASN channels, only Momentary Override references 1 through 8 can be used to key the ASN channels. Therefore, to make the CKR references interoperable with the ASN channels, CKR indexes in the range of 1 through 8 must be used for the CKRs for the Digital, Mixed Mode, and ACIM channels that are interoperable with the ASN channels.

Figure 15: Momentary Override and Channel Configuration in the PM – Console User Capabilities Profile on page 54 through Figure 17: Momentary Override and Channel Configuration in the PM – Digital, Mixed Mode, or ACIM Channel Configuration on page 55 show an example of how MO on the Console User Capability Profile can be configured to work with interoperable keys that have been properly mapped on the channels. In this example, only MO Index 1 is designated to be interoperable.

Figure 15: Momentary Override and Channel Configuration in the PM – Console User Capabilities Profile



NOTICE: The MO keys will show the CKR Alias as it is configured in the CKR database.

Figure 16: Momentary Override and Channel Configuration in the PM – ASN Channel Configuration

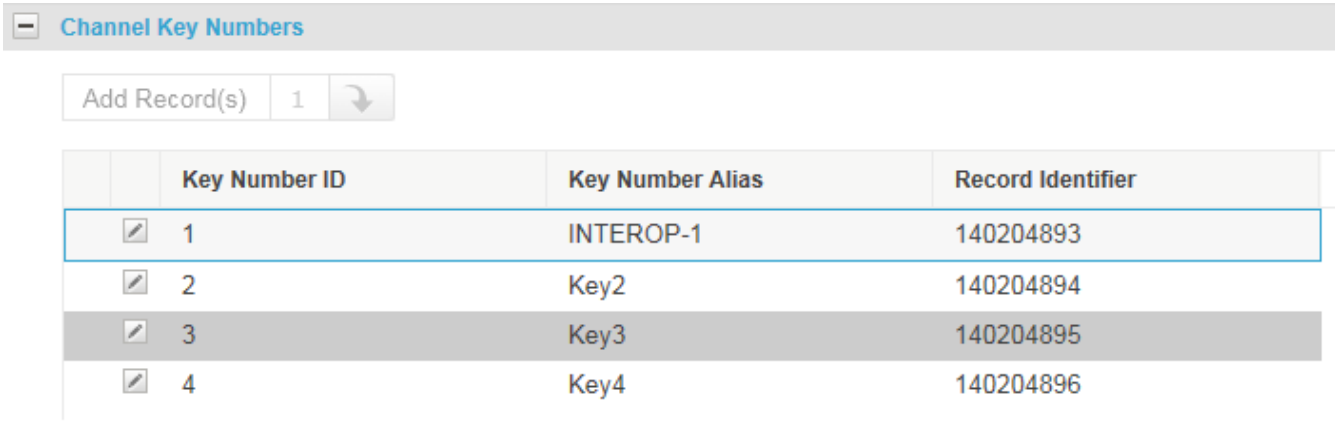
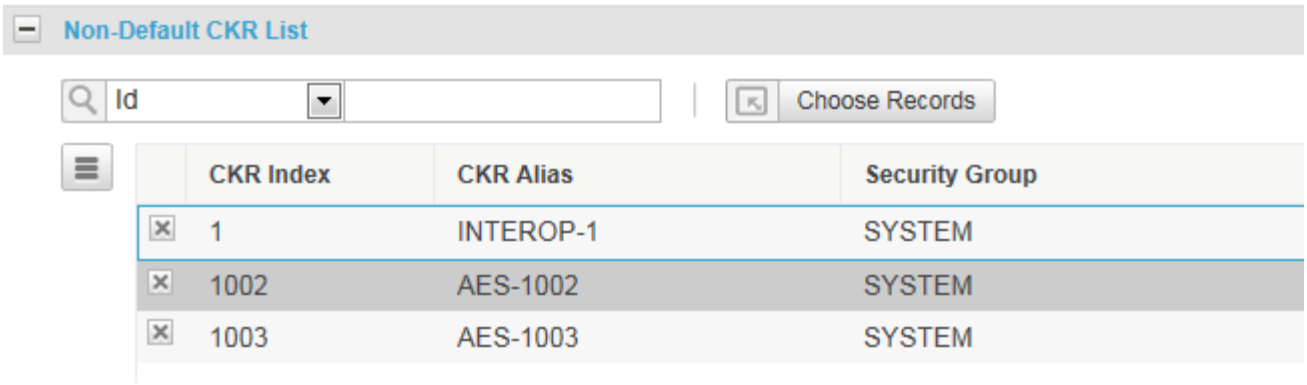


Figure 17: Momentary Override and Channel Configuration in the PM – Digital, Mixed Mode, or ACIM Channel Configuration



2.5.1.4.3

How Secure Interoperability Works on the Consoles

The MO secure keys that are configured and the secure keys the console displays in the MO selection box, represent either CKR Indexes or Key Numbers, depending on which channel type the console keys the MO call on.

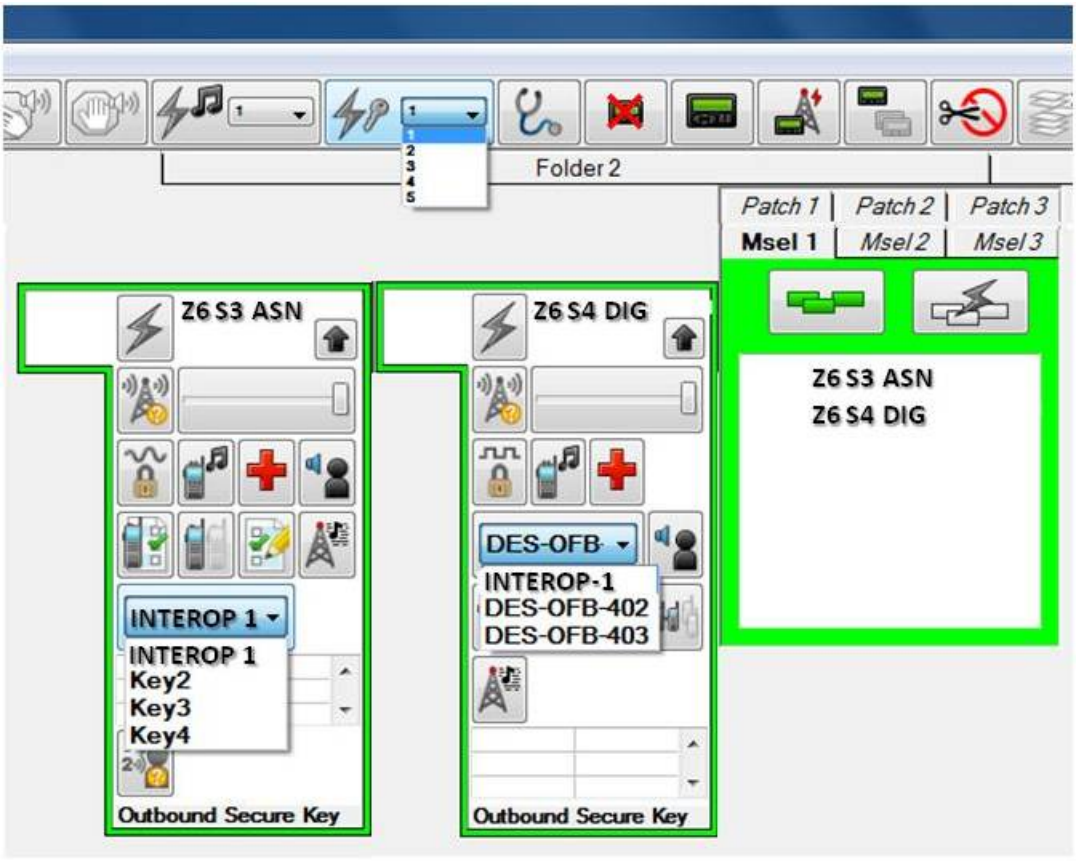
When you select a CKR in the range of 1 through 8 and an ASN channel is in the MSEL, it will be part of the call and will work with digital channels using the CKR in the range of 1 through 8. See Figure 18: Momentary Override with Both Resource Types in the MSEL Group on page 56 for an example.

- On Digital, ACIM, or Mixed Mode Channels, the secure key that is displayed on the resource key selection box and used to key the secure call, is the CKR index associated with the MO selection (as configured in the PM) that also needs to be configured in the radio.
- For ASN channels, the secure key that is displayed on the resource key selection box and used to key the secure call, is the Key Number that matches the MO selection that also needs to be configured in the CIU and the radio (in the PID slot that matches the Key Number).

In either case, if a secure key corresponding to the MO key is not selectable on a resource, then the resource will not be keyed up, and the `Momentary Override secure key is invalid` error warning will be displayed on the console status bar.

Figure 18: Momentary Override with Both Resource Types in the MSEL Group on page 56 shows an example Console OP User Interface, showing Interoperable Secure key setup on an Advanced SECURENET® Conventional resource (Z6 S3 ASN) and a Digital Conventional resource (Z6 S4 DIG).

Figure 18: Momentary Override with Both Resource Types in the MSEL Group



2.5.1.4.4

How Secure Interoperability Works in the Radios

All radios (both digital and ASN type) that are authorized to use the interoperable keys, have the interoperable keys loaded so that they are all able to decrypt secure calls.

The dispatcher can be informed which keys are cross-group capable by the alias provided on the key selection list of each console resource. Even if aliases are not configured, when the MO call is keyed up, each resource displays the key in use corresponding to the selected index on the MO button, so operators can easily identify if a key that is common between ASN and Digital has been selected. It is assumed the operators are well informed of what each secure key is designated for.

2.5.1.4.5

Advanced Digital Privacy (ADP) Keys

If you choose to use ADP encryption which is limited to a set of 8 unique key references, it is possible to plan the key mapping to enable ADP-secured radio users to also interoperate with users that have ASN-based encryption. Since ADP keys are defined as CKRs using the same indexing, both non-ADP

CKR interoperability with ASN and ADP key interoperability with ASN cannot be configured at the same time.

Table 11: Mapping Interoperable Keys for Momentary Override Keying – Example

MO Index	CKR Index assigned to MO Index	Key Numbers available on ASN channels*	Key Alias	Interoperability enabled (assuming Fire and Service have all CKR keyed radios and Police has only ASN keyed radios)
1	CKR-1	Key 1	INTEROP-1	All agencies
2	CKR-2	Key 2	IntFandP-2	Fire and Police
3	CKR-3	Key 3	IntSvcPol-3	Service and Police
4	CKR-4	Key 4	IntPol-4	All Police agencies
5	CKR-401		Fire-401	Fire only*
6	CKR-402		Svc-402	Service only*
7	CKR-777		IntFandS-1	Fire and Service group 1
8	CKR-888		IntFandS-2	Fire and Service group 2
9	CKR-999			None
...	...			None
250	CKR-4096			None

*If more keys are configured on an ASN channel (up to 8), the console can take advantage of MO indexes 5 through 8 to key them up. However, in this example there are no “interoperable keys” mapped for Keys 5 through 8, so the ASN radios are assumed to have different keys than the Fire and Service digital radios, and therefore would not be included in secure calls with the other agencies.

This page intentionally left blank.

Chapter 3

Secure Communications Equipment

This chapter provides functional descriptions of hardware in the secure communications system.

3.1 Key Management Facility in ASTRO 25 Systems

NOTICE: This section is applicable to the High/Mid Tier KMF. For information on the Small Fleet KMF, see Small Fleet Key Management Facility (KMF) on page 61.

The KMF is the central repository of encryption keys and provides a strategic method for managing all of the secure resources in an ASTRO® 25 system. The KMF allows you to manage the keys and secure data used by all of the devices in the system. The KMF system consists of:

- KMF Server and Client running on Windows Server 2012 with a KMF CryptR connected
- KMF Client running on Windows 7 or Windows 10

3.1.1 KMF Server

NOTICE: This section is applicable to the High/Mid Tier KMF. For information on the Small Fleet KMF, see Small Fleet Key Management Facility (KMF) on page 61.

The KMF Server hosts the KMF Server application, handles key management messages (KMMs), manages Over-The-Air Rekeying (OTAR) operations, and stores all key material and configuration settings.

The KMF Clients access key management information by logging on to the server. From the client, you can configure key management information and load keys on the KMF Server. The KMF Server handles all Over-The-Air Rekeying (OTAR) operations, including rekey requests, full and optimized update, CKR update, clear and encrypted hello, zeroize, inhibit, enable, and keyset changeover commands. The KMF Server maintains currency information for all commands and performs retry opportunities for target devices that have not yet acknowledged commands.

NOTICE: In general, throughout this manual, when referring to OTAR, the same information applies to Over-The-Ethernet Keying (OTEK).

The KMF Server provides encapsulation and encryption services for all key management messages (KMMs) through the KMF CryptR. The KMF CryptR supports a serial connection for key loading to a locally connected KVL. The UDP/IP Ethernet port connects to the Customer Enterprise Network (CEN) to support all inbound and outbound KMMs. The Ethernet port also supports traffic between the KMF Server and the KMF Clients. The DVD-RW drive is available for software installation, loading keys from file, and storing data to DVD.

The Hewlett Packard DL380 Gen8 and Gen9 server is supported by and certified for the KMF Server.

3.1.2 KMF CryptR

NOTICE: This section is applicable to the High/Mid Tier KMF. For information on the Small Fleet KMF, see Small Fleet Key Management Facility (KMF) on page 61.

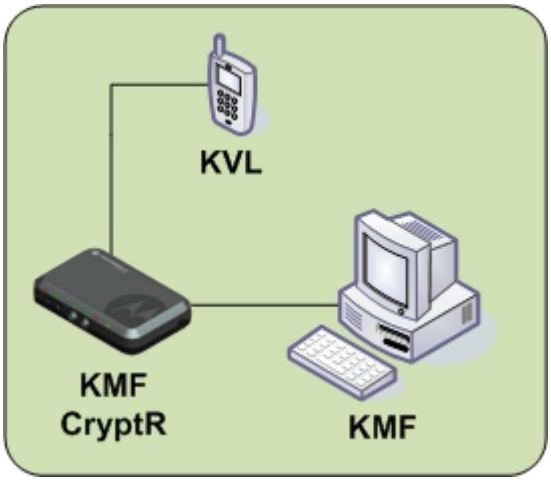
The KMF CryptR provides encryption services for the Key Management Facility. It securely stores the KMF master keys and uses them to perform encryption operations for both key storage and OTAR/ OTEK message generation.

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's master key. The KMF CryptR then encrypts the key material with the target devices key encrypting key (KEK), generates a further encrypted Key Management Message (KMM) with the target devices 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 Hewlett Packard DL380 Gen8 and Gen9 server is supported by and certified for the KMF CryptR.

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 19: KMF CryptR Connections



3.1.3
KMF Client

The KMF Client provides the main user interface in the KMF subsystem. The clients allow up to 65 simultaneous users at different physical locations to log on to the KMF Server and perform any necessary key management, secure device configuration, and OTAR commands. These commands include full and optimized update, CKR update, clear and encrypted hello, zeroize, inhibit, enable, and keyset changeover commands. The KMF Client application allows complicated relationships between devices, groups, and encryption keys for management by users. The KMF Client has an integrated interface to support ASTRO® 25 Trunking IVD, ASTRO® 3.1 Conventional IVD, ASTRO® 25 Conventional IVD, and PS LTE systems attached to the KMF subsystem. The KMF Client application is a Web-based application, accessed by using a web browser.

The Hewlett Packard Z420 and Z440 workstations and Gen8 and Gen9 servers are supported by and certified for the KMF Client. The supported Operating Systems are Windows 7, Windows 10, and Windows Server 2012. You can also access the KMF Client application from any computer by using a web browser. For the KMF Client application access, Motorola Solutions supports Internet Explorer 11. You can also access the KMF Client application by using Microsoft Edge or Google Chrome web browsers.

3.2

Small Fleet Key Management Facility (KMF)

The KMF is the central repository of encryption keys and provides a strategic method for managing all of the secure resources in an ASTRO® 25 or PS LTE system. The KMF allows you to manage the keys and secure data used by all of the devices in the system.

Small Fleet KMF is a smaller version KMF that is installed on a PC running Windows 7 or Windows 10. Small Fleet KMF can support up to 500 Radios and/or Secure Phones, three Agencies, and three simultaneous user connections. Small Fleet KMF does **not** support Redundancy. Small Fleet KMF consists of:

- KMF Server and Client running on Windows 7 or Windows 10 with a KMF CryptR connected
- KMF Client running on Windows 7 or Windows 10

KMF Server

The KMF Server hosts the KMF Server application, handles key management messages (KMMs), manages Over-The-Air Rekeying (OTAR) operations, and stores all key material and configuration settings. The KMF Server handles such operations as rekey requests, full and optimized update, CKR update, clear and encrypted hello, zeroize, inhibit, enable, and keyset changeover commands. The KMF Server maintains currency information for all commands and performs retry opportunities for target devices that have not yet acknowledged commands. The KMF Server provides encapsulation and encryption services for all key management messages (KMMs) through the KMF CryptR.

NOTICE: In general, throughout this manual, when referring to OTAR, the same information applies to Over-The-Ethernet Keying (OTEK).

Table 12: Small Fleet KMF Server Minimum Hardware Requirements

Requirement	Description
Processor	4 cores, 2 GHz
Memory	4 GB
Hard Drive	100 GB
Cache	3 MB
Storage Device	DVD-ROM
Ethernet Port	KMF CryptR Connection
Secondary Ethernet Port (recommended) or USB Port (with USB to Ethernet Adapter) or Wi-Fi	Network Connection
Operating System	Windows 7 64 bit or Windows 10 64 bit

KMF CryptR

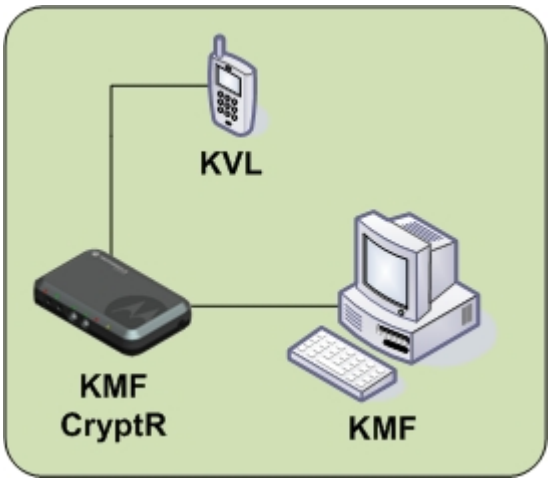
The KMF CryptR provides encryption services for the Key Management Facility. It securely stores the KMF master keys and uses them to perform encryption operations for both key storage and OTAR/OTEK message generation.

When a target device needs a key update, the KMF CryptR receives encrypted key material from the KMF Server and decrypts the key material with the KMF master key. The KMF CryptR then encrypts the key material with the target device's key encryption key (KEK), generates a further encrypted Key Management Message (KMM) with the target devices 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.

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 20: KMF CryptR Connections



KMF Client

The KMF Client provides the main user interface in the KMF system. KMF Clients allow up to three simultaneous users at different physical locations to log on to the KMF Server and perform any necessary key management, secure device configuration, and OTAR commands. These commands include full and optimized update, CKR update, clear and encrypted hello, zeroize, inhibit, enable, and keyset changeover commands. The KMF Client application allows relationships between radios, groups, and encryption keys for management by users. The KMF Client has an integrated interface to support ASTRO® 25 Trunking IVD, ASTRO® 3.1 Conventional IVD, ASTRO® 25 Conventional IVD, and PS LTE systems attached to the KMF system. The traffic between the KMF Server and the KMF Clients can be supported through an Ethernet port, a USB port with a USB to Ethernet adapter, or a Wi-Fi connection, depending on the KMF Server hardware specification.

The KMF Client application is a Web-based application, accessed by using a web browser. For the KMF Client application access, Motorola Solutions supports Internet Explorer 11. You can also access the KMF Client application by using Microsoft Edge or Google Chrome web browsers.

Table 13: Small Fleet KMF Client Minimum Hardware Requirements

Requirement	Description
Hard Drive	60 GB
Storage Device	CD-ROM
Ethernet Port	Network Connection
Operating System	Windows 7 64 bit or Windows 10 64 bit

3.3 PDEG Encryption Unit

The Motorola Solutions PDEG Encryption Unit unit is a high-quality, high security IPSec Virtual Private Network (VPN) gateway solution that enables end-to-end secure communications between

applications in the CEN and mobile applications over a Motorola Solutions ASTRO® 25 network. The PDEG installs easily with standard RJ–45 Ethernet ports for red-side (clear) and black-side (encrypted) network interfaces. The PDEG Encryption Unit is certified to National Institute of Standards and Technology FIPS Level 3. The PDEG Encryption Unit data encryption keys can be centrally managed using a Key Management Facility server (KMF) in the Customer Enterprise Network (CEN).

The PDEG Encryption Unit is a component of the Encrypted Integrated Data (EID) feature located within the CEN. The EID feature provides data encryption services for ASTRO® 25 system applications between the CEN and subscriber radios. The EID feature uses IPsec to provide AES encryption, decryption, and authentication of packet data between each EID enabled subscriber radio and a PDEG Encryption Unit. Using the EID feature, your organization can secure data sent between CEN applications and subscriber radio internal or external applications.

Key features of the PDEG Encryption Unit are:

- ASTRO® 25 IV&D data transmissions are protected over-the-air and in the Radio Network Infrastructure.
- Encrypts, decrypts, and authenticates data traffic entering and leaving the Customer Enterprise Network (CEN) using AES.
- FIPS certified

Distinctive characteristics of the PDEG Encryption Unit are:

- Integrated physical security
- Highly tamper resistant
- FIPS Level 3 security

NOTICE: EID does not support encryption of data for the following features or services:

- ASTRO® 25 High Performance Data (HPD) services
- ASTRO® 25 IV&D Broadcast Data traffic
- Transit 25 Data

These features may exist on a system where EID also exists, but EID cannot be used to encrypt data for these features.

3.4 Border Gateway

The Border Gateway serves as the demarcation between a peripheral network and the Motorola Solutions Radio Network Infrastructure (RNI). One side of the Border Gateway provides an interface with the CEN. The other side of the Border Gateway attaches to a peripheral network to interface with devices included as part of the RNI.

See the *System Gateways - GGM 8000* manual for more information.

3.5 Firewall

A firewall is a network security device providing network boundary enforcement and attack detection features. The firewall restricts traffic to known sources, destinations, and protocols, based on the hosts and services specified in the firewall configuration. All other traffic that is not defined is discarded.

The firewall can be managed by the Network and Security Manager software residing on the Firewall Management Server, if present in the system, with a graphical user interface located on the Core Security Management Server (CSMS) or another Windows server at the Master Site in the radio network infrastructure.

For more information, see the *Fortinet Firewall* or *Juniper Firewall* manual, depending on your firewall brand.

3.6 Radio Network Controller (RNC) Encryption Unit

The RNC encryption unit is an external device which connects to the Radio Network Controller (RNC) to support secure data services for ASTRO® 3.1 Conventional IV&D systems. Up to five encryption units can be connected to the RNC. The encryption unit allows the RNC to encrypt or decrypt secure data traffic (not including key management messages) as the traffic is being passed between the conventional radios and the customer host network. The encryption unit encrypts outbound data from the host computers on the network for over-the-air delivery to conventional radios. The encryption unit also decrypts inbound secure data, allowing clear data to be delivered to the fixed host computers on the customer network.

NOTICE: The RNC is only used in ASTRO® 3.1 Conventional IV&D systems. The RNC encryption unit is only required for secure data in ASTRO® 3.1 Conventional IV&D systems, and is not used to encrypt or decrypt OTAR traffic between the KMF and radios. Key management messages in a conventional system are routed through the RNC 3000 chassis. The RNC 3000 chassis can deliver all forms of KMMs between the KMF and radios.

Eight different models of the encryption unit are available, including four different single algorithm units which provide either AES, DVP-XL, DES-XL, DES-OFB, or DVI-XL capability. Four dual algorithm encryption units are also available.

See the *ASTRO 25 RNC/KMF Encryption Unit Service Manual* (6880800B70) and *ASTRO 25 RNC/KMF Encryption Unit Functional Manual* (6880800A30) for additional information about the RNC encryption unit.

3.7 Wireless Network Gateway (WNG)

The WNG is the network routing component of a Motorola Solutions mobile data communications network. The WNG connects wireline networks and radio frequency (RF) data networks. This interconnection allows applications to pass data between hosts and mobile devices on the different networks as if they were on one network.

NOTICE: The WNG is used only in ASTRO® 3.1 Conventional IV&D systems.

In systems configured for end-to-end Internet Protocol (IP) communications, the WNG functions as an IP router. The WNG is positioned at the junction of the wireline networks and RF data networks and provides the routing, translation, fragmentation, and error notification services needed to transfer messages from one network to another.

See the *Wireless Network Gateway Installation and Operations Reference* (6871015P29) manual for more information.

3.8 DIU 3000 Encryption Cartridge

The DIU 3000 encryption cartridge is installed in a DIU to provide encryption/decryption of voice traffic between the consoles and radios on the ASTRO® 3.1 Conventional IV&D network. The cartridge decrypts inbound secure voice and delivers the clear voice to the console. The cartridge encrypts outbound secure voice for over-the-air propagation to the radios.

NOTICE: The DIU is used only in ASTRO® 3.1 Conventional IV&D systems.

In ASTRO® 25 mode, the DIU encryption cartridge stores keys according to the Common Key Reference (CKR). For decryption of received messages, the DIU encryption cartridge determines the received key information and selects the appropriate key from storage to decrypt the voice traffic and deliver the traffic to the console. When a console intends to transmit secure voice traffic, the DIU receives the clear voice traffic and a key selection from the console. The encryption module uses the selected CKR to encrypt the traffic and deliver it to the base station for delivery to the radio.

The DIU can receive keys from the KMF over the network. The key material is stored securely in non-volatile battery-backed memory, using a 3 V internal battery. The encryption cartridge has a tamper detection mechanism which zeroizes keys when the sensitive portion of the internal card is tampered with. Keys can be also erased from the DIU encryption module by pressing the ERSE button on the panel, then pressing the ENTR button.

The DIU encryption cartridge supports up to 1024 traffic encryption keys, four key encryption keys (KEKs). The cartridge is offered with up to two algorithms (single or dual algorithm). Available algorithms include DES-OFB, DES-XL, DVI-XL, DVP-XL, AES, and ADP software-based encryption.

The DIU can be configured for FIPS mode through DIU CSS. When FIPS mode is enabled through DIU CSS, three classes of user access are enforced, and passwords are required for access to the DIU configuration environment. These classes of users include the User, Crypto Officer, and Crypto Maintenance Officer. The User can receive and transmit secure voice at the DIU, but cannot access or change encryption-related settings. The Crypto Officer can perform rekeying operations with a KVL and can locally receive and transmit secure voice using the DIU handset. The Crypto Maintenance Officer has full access to all DIU CSS and encryption-related settings in the DIU.

The encryption cartridge can also use indexed keying (ASN mode). This method allows either one key or a pair of keys to be mapped to each of the physical key ID numbers. This method also permits configuration of the DIU with an active and inactive key at each index number. However, the DIU cannot receive keys over the network from the KMF while in ASN mode.

For additional information for the DIU 3000 and encryption cartridge, see the *ASTRO DIU 3000 Digital Interface Unit Owner's Manual* (6802949C65) and *ASTRO Digital Interface Unit Encryption Cartridge Instruction Manual* (68P80801G85). For additional information about DIU CSS and configuration settings for the DIU, see the *ASTRO Digital Interface Unit (DIU) 3000 Configuration Service Software (CSS) User's Guide* (6802972C90).

3.9 GPRS Gateway Support Node (GGSN)

The GGSN provides a network interface between the CEN and the radio network, allowing mobile subscribers to access the CENs to which they belong. A mobile subscriber typically consists of a mobile computer attached to a mobile radio through a serial or USB connection. The mobile radio performs all mobility tasks on behalf of the mobile computer.

One side of the GGSN connects to the RNI while the other connects to a peripheral network to interface with the border gateways of the CEN.

The GGSN is designed to handle IP routing services for end-to-end data messaging on the ASTRO® 25 High Performance Data (HPD) and Integrated Voice and Data (IV&D) Trunking and Conventional communication network.

A redundant GGSN can be employed to support High Availability (HA) Data. In the event of a failure, the HA Data feature provides an automatic switchover to the redundant GGSN device, but the user also has the option to initiate a switchover manually. A manual GGSN switchover is executed from the Unified Network Configurator (UNC) by performing a reboot of the primary GGSN router. The reboot causes the redundant GGSN to take over. For more information on the HA Data feature, see the *Trunked Data Services* manual.

For more information on the GGSN, see the *System Routers - S6000/S2500* manual.

3.10 Packet Data Gateway

The Motorola Solutions Packet Data Gateway (PDG) is designed to link a customer data network to their radio network. It is placed at the junction of the wire line network and the Radio Frequency (RF) data network. It provides the interconnection between the two networks through its routing, translation, fragmentation, and error reporting services. The PDG employs Internet Protocol Version 4 (IPv4) routing. A multizone system requires one PDG per zone for seamless system-wide packet data service operation.

The Packet Data Service is a bearer service that connects two parties in a communication system with the IP protocol. One party is either a subscriber or a mobile terminal connected to the subscriber, and the other is an application in the CEN.

The PDG platform supports the following system types:

- **Conventional Integrated Voice and Data (IV&D) PDG**
  - within M core zones
  - within K core zones

  NOTICE: The Conventional IV&D K core PDG is functionally equivalent to the Conventional IV&D M core PDG, but is configured to operate in the K core without core services such as Authentication Services, Domain Name Server, Network Time Protocol Server, and the full centralized Network Management.
- **Trunked Integrated Voice and Data (IV&D) PDG**
  - within L core zones
  - within M core zones
- **High Performance Data (HPD) PDG**
  - within M core zones

IMPORTANT: Each type of data service requires a separate PDG.

For Trunked IV&D and HPD, the Packet Data Service is an implementation of the APCO 25 Common Air Interface (CAI) and the Standard Subnetwork Dependence Convergence Protocol (SNDCP) to provide IP datagram exchange between applications on mobile subscriber units and Fixed Network Equipment (FNE). To support High Availability for Trunked IV&D and HPD (HA Data), redundant PDGs, GGSNs, and CNI path equipment (data network transport devices) can be implemented in the L2, M2 and M3 zone cores. For a detailed description of the HA Data feature, see the *Trunked Data Services* manual.

For Conventional IV&D, the Packet Data Service is an implementation of the APCO standard SCEP (Simple CAI Encapsulation Protocol) air interface to provide IP datagram exchange between applications or attached to mobile subscriber units and Fixed Network Equipment (FNE).

The PDG is installed as a virtual machine on an HP DL380 server. For the description of the server, see the *Virtual Management Server Hardware* manual. To support High Availability for Conventional IV&D, redundant PDGs, GGSNs, and CNI path equipment (data network transport devices) can be implemented in the M2 and M3 zone cores. For a detailed description of the HA Data feature, see the *Conventional Data Services* manual.

The virtual appliance of the PDG includes the following components:

- **Linux Operating System**

- **Packet Data Router (PDR) application**: The PDR provides a logical interface between the GPRS Gateway Support Node (GGSN) router and the Radio Network Gateway (RNG). The PDR forwards outbound data traffic to the RNG.
- **Radio Network Gateway (RNG) application**: The RNG provides a logical interface between the local Radio Frequency (RF) resources and the PDR to support data calls to subscriber radios.

3.10.1
Trunked IVD and HPD PDG Components and Architecture

The Packet Data Gateway (PDG) provides the interface between the Customer Enterprise Network (CEN) and packet data users in the system. The PDG performs registration services for packet data users, maintains user permissions and mobility information, as well as provides routing of traffic to the radio network or the GPRS Gateway Support Node (GGSN) router.

The main software components of the PDG are the Packet Data Router (PDR) and the Radio Network Gateway (RNG).

The PDG is installed on the virtual server, which interfaces directly with the Ethernet LAN switch. For the description of the hardware components, see the *Virtual Management Server Hardware* manual.

Figure 21: Data Subsystem – Trunked IV&D and HPD PDG – M3 Zone Core

The following diagram shows the Trunked IV&D and HPD PDG in an M3 zone core employing the VMS host server architecture.

NOTICE: The virtual machine (VM) for the PDG can be incorporated with other VMs on a VMS host.

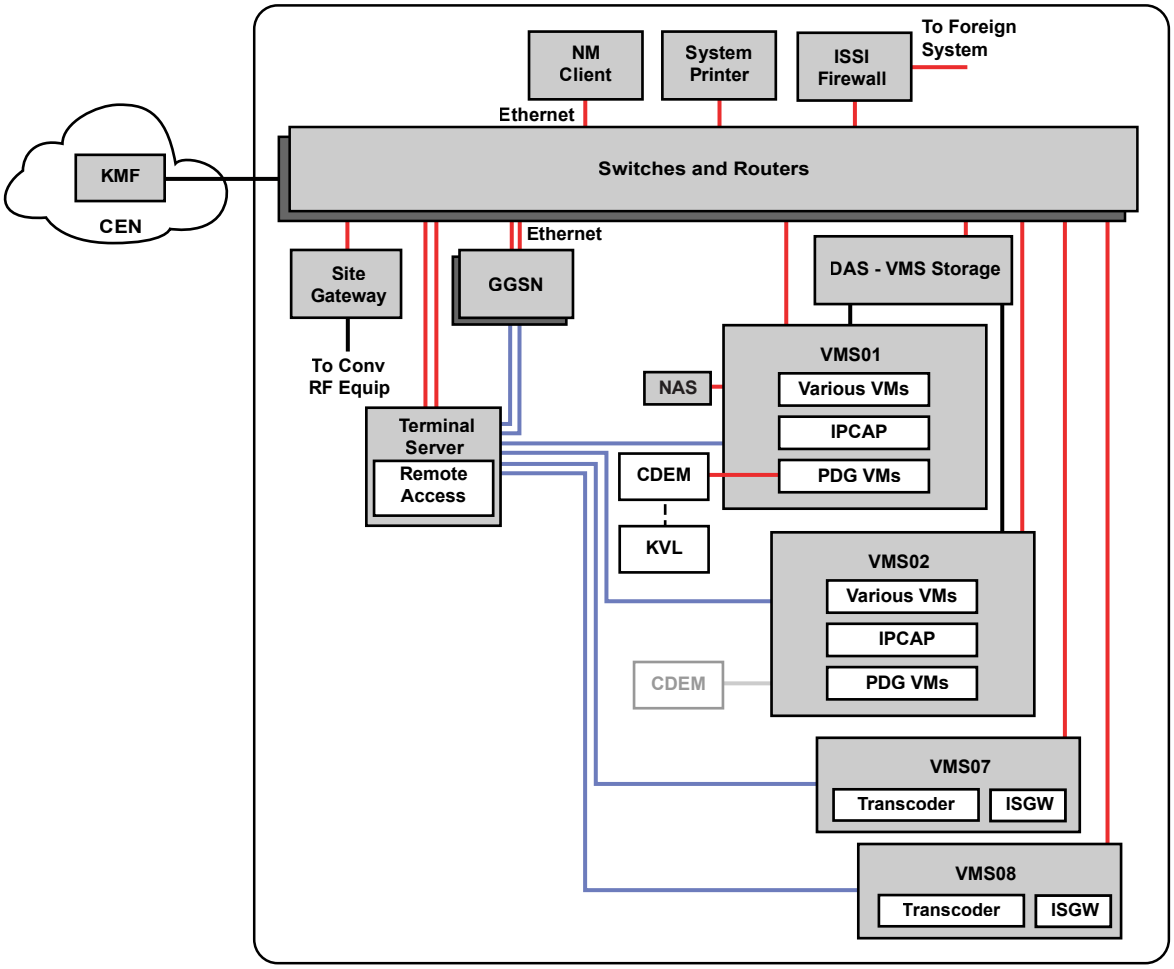


Table 14: Trunked IV&D and HPD PDG Components

Component	Description
RNG	The RNG is a software component which interfaces with the remote sites to handle inbound/outbound packet data traffic between the remote sites and the PDR. The RNG provides a logical connection to the sites, and facilitates delivery of traffic between the PDR and the remote sites. In Outbound direction, RNG supports fragmentation of IP datagrams received from PDR and formats them to Logical Link Control (LLC) packets. Then, it forwards the packets to the subscriber in the zone through the local site of the subscriber. In inbound direction, LLC assembles LLC packets and converts them to IP Packets before forwarding them to PDR. The RNG also communicates with the zone controller and maintains a packet data visitor location register (PD-VLR).
PDR	The PDR is a software component which provides tunneling of packet data traffic to the GGSN router, which then routes the traffic to the Customer Enterprise

Component	Description
	Network (CEN). The PDR hosts the Packet Data Home Location Register (PD-HLR), tracks mobility of mobile subscribers on the network, and controls access to the GGSN and CEN.

3.10.2

Conventional IVD PDG Components and Architecture

The Packet Data Gateway (PDG) provides the interface between the Customer Enterprise Network (CEN) and packet data users in the system. The PDG performs registration services for packet data users, maintains user permissions and mobility information, as well as provides routing of traffic to the radio network or the GPRS Gateway Support Node (GGSN) router.

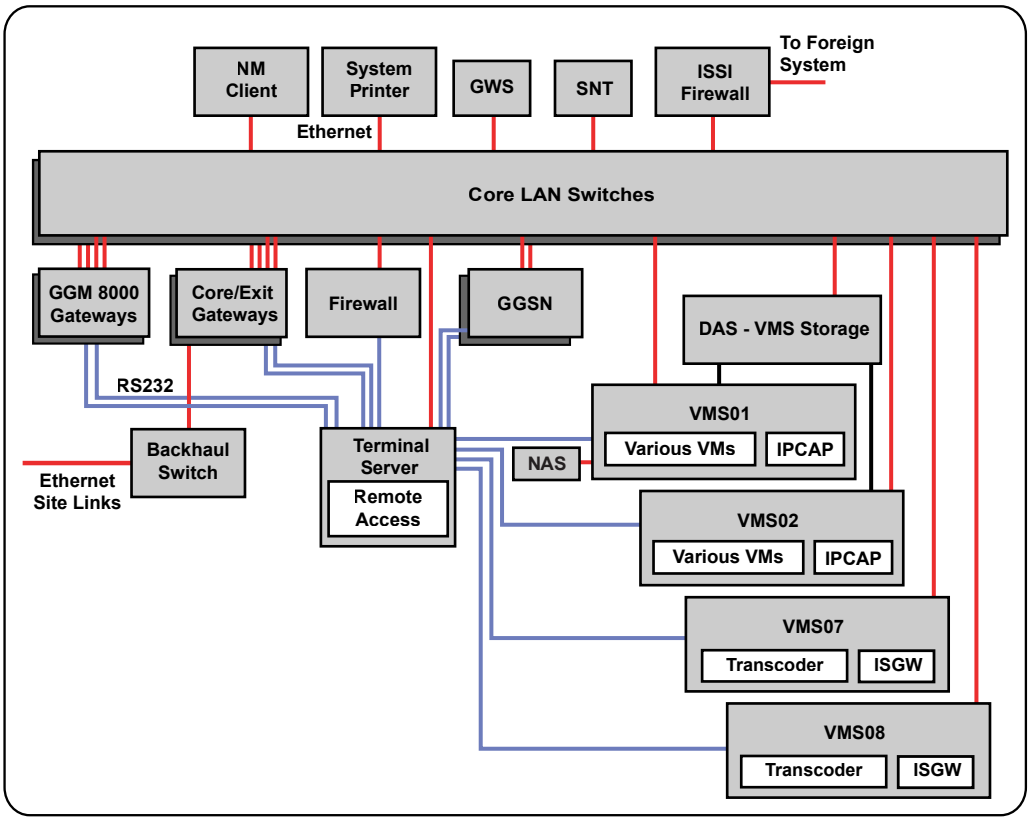
The main software components of the PDG are the Packet Data Router (PDR) and the Radio Network Gateway (RNG).

The PDG is installed on the virtual server, which interfaces directly with the Ethernet LAN switch. For the description of the hardware components, see the *Virtual Management Server Hardware* manual.

Figure 22: Data Subsystem – Conventional IV&D PDG – M3 Zone Core

The following diagram shows the Conventional IV&D PDG in an M3 zone core employing the VMS host server architecture.

NOTICE: The virtual machine (VM) for the PDG can be incorporated with other VMs on a VMS host or it can be placed on a dedicated VMS host platform.



S_A717_M3_Primary_System_Zone_Core_Config_A

Figure 23: Data Subsystem – Conventional IV&D PDG – K1 Core

The following diagram shows the Conventional IV&D PDG in a K1 Conventional System.

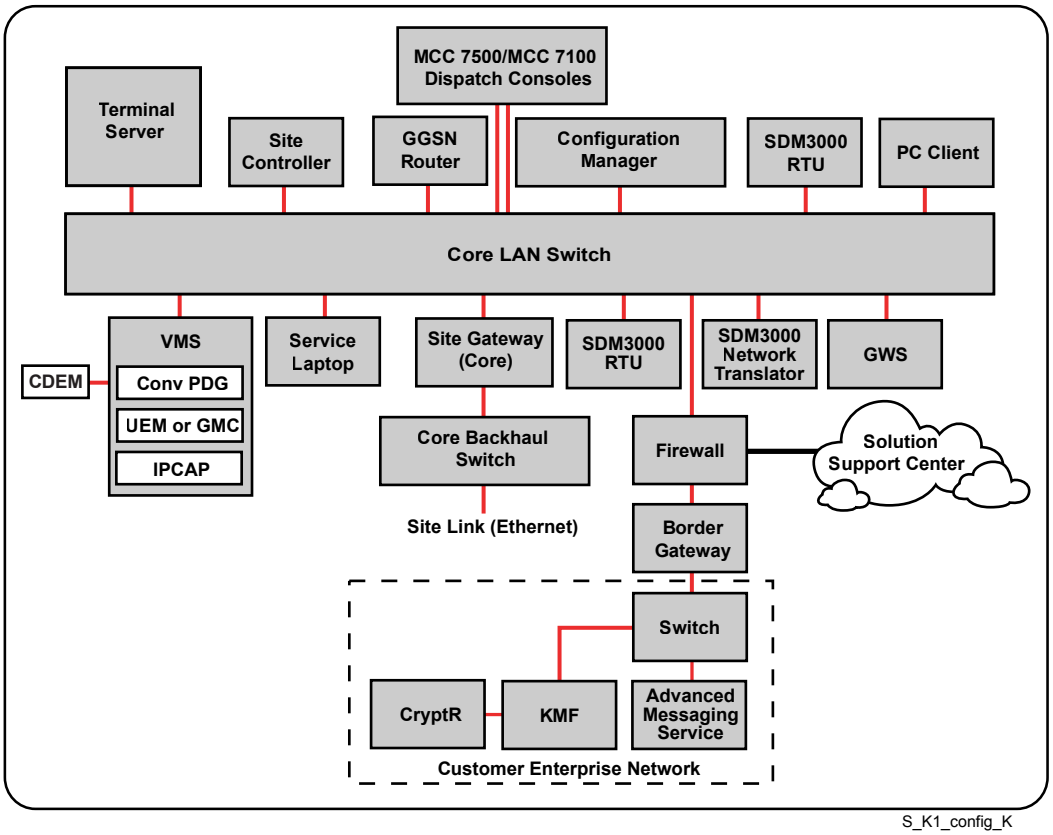


Figure 24: Data Subsystem – Conventional IV&D PDG – K2 Core

The following diagram shows the Conventional IV&D PDG in a K2 Conventional System.

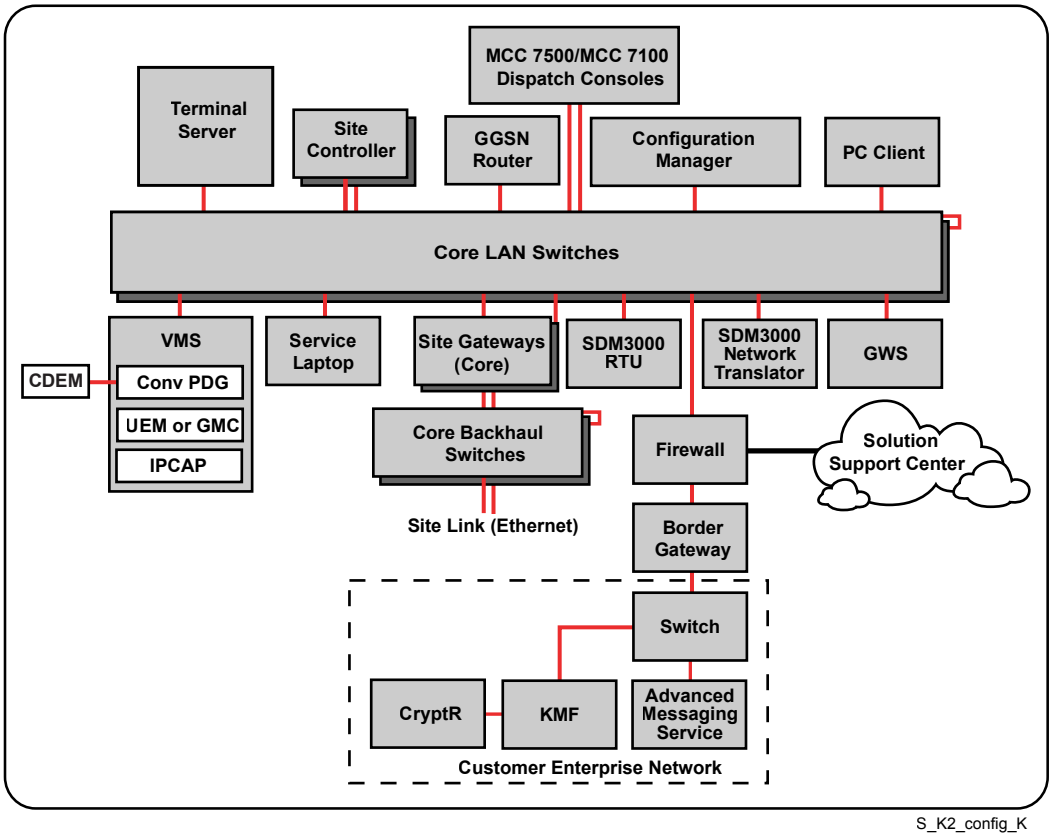


Table 15: Conventional IV&D PDG Components

Component	Description
RNG	The RNG is a software component which provides a link (CAI) layer termination point for all the Conventional Sites in that same zone. The RNG routes data packets over the infrastructure links to the Conventional Sites in the zone. The RNG receives packets from, and sends packets to, the PDR in the same zone. The RNG sends datagrams to the CDEM for encryption/decryption as needed before routing them to their ultimate destination. When key management of the CDEM is performed through OTEK, the RNG proxies the OTEK connection to the KMF on behalf of the CDEM.
PDR	The PDR is a software component which serves as the termination point for the GTP tunnel (the GGSN being the other termination point). The PDR also interacts with the local Radio Network Gateway (RNG). The PDR is responsible for managing Packet Data registrations and de-registrations, tracking subscriber location, interfacing with the Network Manager for configuration and fault management, proxying configuration and fault management messaging for the RNG and CDEM, and ensuring maintenance of persistent contexts. The PDR is also responsible for maintaining registrations for configured Broadcast Data Agencies.

3.11 CAI Data Encryption Module (CDEM)

The CDEM is a component that provides secure data encryption and decryption services for the ASTRO® 25 Conventional with Integrated Data feature. The CDEM is located in the Radio Network Infrastructure (RNI) and connects to the Radio Network Gateway (RNG) component of the Packet Data Gateway (PDG) virtual machine through an Ethernet crossover cable. When the PDG receives data from either the Customer Enterprise Network (CEN) or from a subscriber through the Conventional RF equipment, it passes that data to the CDEM if secure services are required. The CDEM performs the desired encryption or decryption operation and sends the data back to the PDG for transmission to its final destination.

Key features of the CDEM are:

- Installs easily with standard RJ-45 Ethernet ports for network interfaces
- Easy to configure
- Low power consumption
- Small size/light weight
- Supports DES-OFB and AES 256 encryption algorithms
- Certified to National Institute of Standards and Technology FIPS 140–2 Level 3
- Data encryption keys can be centrally managed using a Key Management Facility (KMF)

3.12 MCC 7500 Dispatch Console with VPM/AIS with Voice Processor Module

The MCC 7500 Dispatch Console with Voice Processor Module (VPM) console equipment consists of the:

- MCC 7500 Dispatch Console
- Voice Processor Module (VPM)
- Associated peripheral hardware such as microphone and speakers.

The VPM connects to the console site LAN switch and communicates with the dispatch console PC or Archiving Interface Server (AIS) through the Ethernet.

The Archiving Interface Server (AIS) provides an interface between the Motorola Solutions radio system and the Logging Recorder.

NOTICE: The MCC 7500 Dispatch Console with VPM is only available on ASTRO® 25 Trunking IV&D or ASTRO® 25 Conventional IV&D systems. VPM-based consoles support OTEK.

For more information, see the *MCC 7500 Dispatch Console with Voice Processor Module* manual.

3.13 MCC 7100 IP Dispatch Console

The MCC 7100 IP Dispatch Console is a software-based dispatch console that requires no external hardware connections to perform dispatch operations. Audio Vocoding is performed within the Windows 7 operating system. The MCC 7100 IP Dispatch Console can work with the computer's built-in speakers and microphone, if equipped. External peripherals such as a microphone, headset and foot-switch are also supported.

The MCC 7100 IP Dispatch Console can be located inside the ASTRO RNI at a console site or conventional subsystem. It can also be deployed outside the ASTRO RNI and connect through a

firewall to a console proxy located inside the RNI. A minimum audio quality of DAQ 3.4 is required when using certified commercially available peripherals inside the ASTRO RNI. The MCC 7100 IP Dispatch Console can be configured to dispatch trunking and/or conventional resources.

The MCC 7100 IP Dispatch Console supports secure end-to-end audio via hardware (Micro SD Card) or software-based encryption. The MCC 7100 IP Dispatch Console supports the AES, ADP, and DES-OFB encryption algorithms.

For the MCC 7100 IP Dispatch Console configured with hardware-based (CRYPTR micro device) key storage, the KMF can deliver keys securely to the MCC 7100 IP Dispatch Console using OTEK (Over-the-Air-Keying). For the MCC 7100 IP Dispatch Console configured with software-based key storage, the KMF can export an xml file you can use to import keys into the console. For details and procedures, see the *Key Management Facility* manual.

The KVL 4000 can also be used to load encryption keys into the CRYPTR micro device and to configure the following parameters: the Individual RSI, KMF RSI, and MNP. For details, see the *MCC 7100 IP Dispatch Console Setup and User Guide* and the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

The following are the system components for the MCC 7100 IP Dispatch Console:

- MCC 7100 IP Dispatch Console Software
- PRX 7000 Console Proxy
- Console Site Control Room Firewall
- License Server
- Key Management Facility (KMF)
- Key Variable Loader (KVL)
- Customer Supported Components:
  - DNS Server
  - DHCP Server
  - Customer Enterprise Network (CEN)
  - Virtual Private Network (VPN)

For more information on the MCC 7100 IP Dispatch Console, see the *MCC 7100 IP Dispatch Console Setup and User Guide*.

3.14 Site Gateway (Conventional Channel Interface)

For voice, the Site Gateway (Conventional Channel Interface) provides an interface between the console and the base station. For data, the Site Gateway (Conventional Channel Interface) interfaces between the PDG and the station equipment.

For ASTRO® 3.1 Conventional IV&D, the Site Gateway (Conventional Channel Interface) provides call detection, vocoding and devocoding of audio, station keying and dekeying through Tone Remote Control (TRC) or E & M relay, and tone Line Operated Busy Light (LOBL) detection for parallel console interoperation.

For ASTRO® 25 Conventional IV&D, the Site Gateway (Conventional Channel Interface) interfaces to a base station through the ASTRO Infrastructure Signaling (AIS) protocol. The AIS protocol supports digital conventional calls in secure coded, clear, or analog modes at the base station.

The GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels in your system. For more information, see the *System Gateways - GGM 8000* manual.

3.15 Telephone Media Gateway (TMG)

The Telephone Media Gateway (TMG) is a device that translates audio between the ASTRO® 25 AMBE audio and IP PBX G.711 audio. The TMG supports both encrypted and clear audio to and from the ASTRO® 25 network. All audio exchanged with the IP PBX is clear.

If encryption is required, sending encryption keys from the Key Management Facility (KMF) to the TMG consoles can be accomplished either by using the Key Variable Loader (KVL) or by sending it through the network with the Over-the-Ethernet Keying (OTEK).

A single TMG supports up to 15 calls. For more information, see the *Enhanced Telephone Interconnect* manual.

The TMG is based on the Voice Processor Module (VPM) hardware platform. Specialized software allows the VPM to perform the tasks required for TMG operation. For details on the hardware, see the *Voice Processor Module* manual.

3.16 ASTRO 25 Digital Secure Radios

Motorola Solutions offers secure-capable radios that are compatible for use with the ASTRO® 25 system. Secure-capable radios include the APX two-way radios, XTS 5000 portable radio, XTL 5000 mobile radio, and ASTRO® Spectra Plus mobile radio. Several previously installed radios can also use secure voice features on the ASTRO® 25 system.

3.16.1 Radio Encryption Modules

Secure-capable radios are equipped with an optional encryption module which handles all encryption, decryption, and key loading for the radio (the ADP algorithm can be run with or without an encryption module installed in the radio). A radio may have a Motorola Advanced Crypto Engine (MACE), a Universal Crypto Module (UCM), or an Encryption Module Card (EMC) installed to perform the encryption operations. This module connects directly to the main PCB inside the radio, and interfaces with the vocoder circuitry in the radio to encrypt and decrypt voice traffic. When these radios are properly provisioned, they can participate in secure private calls, group calls, and telephone interconnect calls on the system.

NOTICE: EMC encryption hardware is only supported in 800 MHz previously installed radios, not in VHF/UHF previously installed radios.

The encryption module stores algorithms and key material in an encrypted form using a randomly generated key protection key (KPK). The key material is stored in secure form in tamper protected battery-backed flash memory. The tamper protection mode for the radio can be enabled or disabled through the infinite key retention parameter in radio programming software. When tamper protection is enabled, the radio erases all key material when the pressure-sensitive mechanism on the encryption module is disturbed or the encryption module is removed from the radio.

3.16.2 Secure Radio Settings

For proper operation, settings must match the parameters defined in the Provisioning Manager, and keys/algorithms must match the parameters defined in the KMF. For OTAR operation, program the radio for packet data capability and provide the complete address of the KMF configured (including the KMF UDP/IP address and RSI).

On the radio, the **Ø** symbol denotes secure voice, and the **O** symbol denotes clear voice. Secure voice is selected on the radio by turning the selector to **Ø** (or pressing the **Ø** button). Clear voice is selected by turning the selector to **O** (or pressing the **O** button). Using Customer Programming Software (CPS), other buttons on a portable radio can be programmed to select secure voice. When secure voice is selected, the **Ø** symbol is displayed on the screen. The **Ø** symbol flashes on the screen when the radio is receiving a secure call. When selecting secure voice capability, the radio's screen displays the alias for the key if an alias has been defined in the CPS. A KEY FAIL message appears if any key failures occur. If a selected talkgroup is not configured for secure service, a CLR TX ONLY message appears.

The radio can initiate rekey requests (REKY), key erase (ERAS), and keyset changeovers (KSET) through its on-screen menu. For a rekey request, the radio sends the request to the KMF, and the KMF responds with a rekey update. When a key erase is selected from the radio's menu, the radio user can select a single key to erase or choose to erase all keys. When erasing all keys, the radio erases all stored key material, including its key loss key (KLK). When a keyset changeover is selected from the menu, the radio user can select the keyset to become active (KSET1 or KSET2).

NOTICE: User interfaces and secure capabilities vary for the different radios. Refer to your radio documentation for specific details that apply to your radios.

When the radio registers with the system during power up, the radio tries to establish a data connection with the KMF. The radio supplies the KMF with the radio's IP address and RSI. When the KMF receives the radio's message, the KMF sends any pending rekeying commands or other key management messages. As necessary, the KMF can try to send rekeying commands or other key management messages to the radio at any time, as long as the radio is still registered with the network.

Radios must be properly programmed for secure operation and provisioned with the correct algorithms and key material. For systems supporting the Advanced Digital Privacy (ADP) algorithm, key loading and secure settings are provisioned through the radio Customer Programming Software. ADP does not support Over-The-Air Rekeying (OTAR). Any previously installed radios operating in PID key management mode do not support trunked OTAR.

3.17 Key Variable Loader (KVL)

The Key Variable Loader (KVL) is used to create, store, and transfer encryption keys into secure devices. The KVL can also be used to add or remove algorithms into secure devices. Encryption keys can be entered manually by the KVL user, auto-generated by the KVL, obtained from or shared with another KVL, or downloaded from a KMF. Keys can be transferred to secure mobile and portable radios, infrastructure devices, and system test equipment. The KVL also provides internal processing and memory for secure key storage, as well as interfaces for data communication.

When the KMF manages encryption keys, the KVL is used for Store and Forward operation. The KVL downloads key material and key management messages for target devices from the KMF, either by a direct, modem, or network connection. The KVL user then loads the keys and key management messages to each assigned target device. The KVL maintains acknowledgments for all the key loading operations to the target devices. When the KVL is reconnected with the KMF, the KMF updates the current provisioning status for all the target devices. Note that if Store and Forward is used only, currency may not reflect the actual radio state.

The KVL supports Red Store and Forward and Black Store and Forward. During Red Store and Forward, the KMF encrypts all key material using the UKEK and TEK for the KVL. When the KVL provisions a target device, the KVL decrypts the key material and loads the clear key material into the device. During Black Store and Forward, the KMF encrypts outbound key material with the UKEK and TEK of the target device, and then sends the key material to the KVL for key transfer. When the KVL provisions the target device, it loads the encrypted key material into the device, and the device decrypts the key material with its own UKEK and appropriate TEK. Red Store and Forward is typically used for the first time loading of keys into a radio or secure infrastructure device.

The following key loaders are supported in an ASTRO® 25 system: KVL 3000, KVL 3000 Plus, and KVL 4000. The KVL 3000 Plus and KVL 4000 offer two modes of operation: the Advanced SECURENET (ASN) Mode and the ASTRO® 25 Mode. The KVL 4000 also offers the Radio Authentication mode.

Advanced SECURENET (ASN) Mode: ASN mode provides Physical Identifier (PID) key management. PID key management identifies a physical memory slot where a key variable is stored in a unit. All products that support PID key management access the same encryption keys dependent on the physical storage capability of the product.

ASTRO® 25 Mode: ASTRO® 25 mode provides Common Key Reference (CKR) key management. CKR key management eliminates the need to place a key in a specific memory location. All secure products that support CKRs access the same encryption keys independent of physical storage capabilities of the product. CKR key management is used with ASTRO® digital radios equipped with the Universal Crypto Module (UCM). This mode is required for ASTRO® 25 conventional OTAR, which is performed with the KMF.

NOTICE: The ASTRO® 25 mode is required for OTAR operations.

Radio Authentication Mode: This mode provides a user interface for entering authentication keys and transferring them to target radios. It also provides internal processing and memory for secure key storage, as well as an interface for data communication with the Authentication Center (AuC). This mode is not used for end-to-end encryption key management.

Tactical OTAR is a Motorola feature that allows a KVL to wirelessly manage a key (TEK only) for a small group of radios, with one radio serving as an RF modem. The radio serving as an RF modem must be equipped with the Tactical Rekey/OTAR feature. The radio serving as an RF modem may also be a member of any one of the managed Tactical OTAR groups. For details about configuring tactical OTAR, see the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*, depending on your KVL model.

For more information, see the *KVL User Guide* for your KVL model and mode of operation.

3.18 Secure Communications Security Policies

This section describes the security policies for secure communications components.

3.18.1 Radio Security Policies

Unauthorized individuals can use lost or stolen radios with previously loaded valid encryption keys. Take the following actions to prevent this use:

- Never leave radios unattended and store them in a secure location when not in use, whenever practical in the business logistics of your organization.
- Plan to execute the quick removal and/or change of valid encryption keys in a situation when security may be compromised.
- OTAR-inhibit or zeroize compromised units, or inhibit the unit using the Radio Control Manager (RCM).
- Use the lock feature to password protect the radio.
- Disable Rekey request and use the Erase all keys feature when temporarily leaving service. Request a rekey by voice (authenticating the end user) when returning to service.
- If a radio is lost, stolen or missing, rekey all the radios that use the same keys.

3.18.1.1

KMF Profiles for the Radio

A KMF Profile is a list of configuration parameters that a radio requires to talk with the desired KMF. The CPS provides the radio with the following parameters, based on the KMF Profile:

- Rekey request status alert tone (Enabled/Disabled)
- Receive security levels for KMF-initiated Key Management Messages (KMMs)
- Transmit security level parameter for radio-initiated KMMs (Basic/Enhanced)
- User selectable rekey request (Enabled/Disabled)
- Preserve keyset on OTAR changeover (Y/N)
- Confirmed OTAR messaging (Y/N)
- Individual RSI
- Number of Attempts/Retries
- Time between Attempts/Retries
- OTAR Inactivity Timer (72 hours default value)
- KMF Server IP and UDP address

These parameters allow the radio to communicate with the identified KMF and obtain OTAR service. The KMF Server IP and UDP address allow the key management messages to be delivered to the KMF over the trunked system. These fields are not used for delivery of KMMs over an ASTRO® 3.1 Conventional IV&D system.

IMPORTANT: The number of CKRs a radio can hold varies by model. If a radio works in multiple systems, cross-system coordination must be in place to ensure that the appropriate number of CKRs is in the radio. When a radio roams to a new system, it is rekeyed with the key variables from the KMF's CKR set. Only CKRs from the selected KMF system profile are used (as opposed to having access to the entire CKR list).

The radio uses the information in the selected KMF profile for all OTAR-capable modes within that associated conventional personality or trunked system for connecting and communicating with the KMF. The radio also uses the parameters within the KMF profile for formatting KMMs to the KMF.

If a mode is chosen that is associated with a trunked or conventional personality different from the current one, the radio uses the parameters of the KMF profile associated with the new chosen mode, if OTAR-capable.

The CPS provides the radio with up to five KMF Profiles to allow the radio to communicate with up to five different KMFs without the need to reconfigure. The radio CPS tells the radio what KMF profile is associated with each conventional personality and each ASTRO® 25 Trunking IV&D system, if OTAR-capable.

3.18.2

KMF Security Policy

The KMF is the central repository of key material in a system. Control access to the KMF to prevent unauthorized access to the key material resident in the KMF, or improper manipulation of key material or addition of spoof key material in the KMF. If security is compromised, erase the master keys using the Erase button on the KMF CryptR. For details, see the *KMF CryptR User Guide* manual.

3.18.3
Key Variable Loader Security Policy

After you enter a key into the KVL, the KVL stores the encryption keys and transfers the keys to the supported devices, so keep the KVL in a secure location. Supported devices include:

- MCC 7500 Dispatch Console (ASTRO® 25 Trunking IV&D or ASTRO® 25 Conventional IV&D systems)
- DIU encryption cartridges (ASTRO® 3.1 Conventional IV&D systems)
- RNC encryption units (ASTRO® 3.1 Conventional IV&D systems)
- ASTRO® digital radios
- PDEG Encryption Unit (ASTRO® 25 Trunking IV&D systems)
- CDEM (ASTRO® 25 Conventional IV&D systems)
- MCC 7500 Archiving Interface Server (AIS)
- MCC 7100 IP Dispatch Console

The KVL stores the keys in nonvolatile memory. Never leave the KVL unattended. When not using it, store it in a secure location where only authorized personnel have access to it.

If a KVL is lost, change the Traffic Encryption Key (TEK) it contained in the rest of the system. The KVL can be deleted from any KMF to prevent unauthorized key distribution to compromised KVLs.

3.18.4
Security Policy for Consoles, AIS, CDEM, PDEG, and TMG

Control access to the Consoles, AIS, CDEM, PDEG, and TMG to prevent unauthorized access to the key material resident in these devices. If security is compromised, erase the master keys by pressing the appropriate key reset button.

Chapter 4

Secure Communications Configuration

This chapter describes configuration instructions for secure communications components.

To correctly configure a secure system, configure the Key Management Facility (KMF) subsystem and related components of the radio system with the same parameters. See the *Key Management Facility* manual for details about configuring the KMF.

4.1 Configuring Secure Entities for ASTRO 25 Trunking IVD Systems

The following table lists the items to configure for secure voice, data, and OTAR operations in an ASTRO® 25 Trunking IV&D system.

Table 16: Configuring Secure Entities for ASTRO 25 Trunking IVD Systems

Entity	Reference
Configure the components for the ASTRO® 25 Trunking IV&D system.	See Configuring ASTRO 25 Trunking IVD System Components on page 80.
Configure the KVL for OTAR.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*, depending on your KVL model.
Configure the KMF.	See the “KMF Configuration” chapter in the *Key Management Facility* manual.
Configure the radios.	See Configuring Radios for Secure Communications on page 85.
Configure the Firewall for OTEK.	Open a case with the Motorola Solution Support Center (SSC) to modify the RNI-DMZ firewall configuration for OTEK.
Configure the Console to work with KMF/OTEK.	See the following manuals, depending on your console model: • *MCC 7500 Console Sites with VPM* • *MCC 7100 IP Dispatch Console Setup and User Guide*
Configure the MCC 7500 Archiving Interface Server (AIS).	See the *MCC 7500 Dispatch Console with Voice Processor Module* manual.
Configure the PDEG (for secure data only).	See the *PDEG Encryption Unit* manual.
Set up the KVL 3000 Plus or KVL 4000 and load keys into all the secure devices.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

4.1.1
Configuring ASTRO 25 Trunking IVD System Components

In an ASTRO® 25 Trunking IV&D system, radios are not assigned to a fixed channel. Channels are common resources that are accessible to all users on an as-needed and as-available basis. When a radio user initiates a call, the system assigns an available channel to that call, eliminating the condition in which one channel is busy while another channel is inactive. When the call is finished, the channel is released and made available for other users.

All participants of a talkgroup must have the same encryption key so that they can communicate within their talkgroup. Types of secure calls in a trunked system:

- Group (Talkgroup, Multigroup, Agencygroup, Supergroup)
- Private
- Telephone Interconnect

For more information about how secure trunking calls are processed, see Secure Call Processing for ASTRO 25 Trunking IVD Systems on page 105.

This section describes configuring the trunked system for secure operation:

- Configuration for Secure Talkgroup/Multigroup/Agencygroup Calls on page 80
- Configuration for Secure Supergroup Calls on page 81
- Configuration for Secure Private Calls on page 81
- Configuration for Secure Interconnect Calls on page 82
- Creating Secure Encryption Card Records on page 83

4.1.2
Configuration for Secure Talkgroup/Multigroup/Agencygroup Calls

Each secure-capable talkgroup, multigroup, or agencygroup must have certain secure settings defined in the Provisioning Manager. The talkgroup is associated with a TG/MG Capabilities Profile record. This record defines the secure communication mode (clear, secure, or both) and the Common Key Reference (CKR) number that radios must use when making a secure call to the talkgroup. The following table lists the secure settings for each secure-capable talkgroup, multigroup, or agencygroup:

Table 17: Configuring Talkgroups/Multigroups/Agencygroups for Secure Voice Capability

Record	Field	Setting
TG	Talkgroup Enabled	Yes
MG	Multigroup Enabled	Yes
TG/MG Capabilities Profile	Secure Communication Mode	Secure or Both
	Secure Common Key Reference Number	Common Key Reference (CKR) number to use for secure talkgroup calls. This setting should correspond with CKR settings made in the KMF. Radios must also be provisioned with this CKR.
AG	Agencygroup Enabled	Yes

The **Secure Communication Mode** field has three choices: clear, secure, or both. The following takes place based on the selection:

- Talkgroups and announcement groups programmed for clear only are not allowed to initiate a call in secure mode or upgrade to secure while the call is in progress. The zone controller sends a deny OSP to the requesting radio.
- Talkgroups and announcement groups programmed for secure only are not allowed to initiate a call in clear mode or downgrade to clear while the call is in progress. The zone controller sends a deny OSP to the requestor.
- Talkgroups and announcement groups programmed for “Both” are allowed to upgrade and downgrade.

The system processes dynamic regrouping as a talkgroup call. Dynamic regrouping, which is initiated from the RCM, takes individual radios that normally do not communicate with each other, and groups them into a talkgroup reserved for specific events. The operation is transparent to the radio user. The radio responds to the regrouping command, joins the dynamic talkgroup specified in the OSP, and notifies the user, through a tone and its display, that communication from that point forward is with the dynamic talkgroup and not the talkgroup indicated by the selector position.

Talkgroups designated for dynamic regrouping in the system fleetmap must also be assigned a CKR if it is intended that they have secure capability. The talkgroups and their corresponding CKRs are programmed in the Provisioning Manager (PM). Radios do not know the talkgroup ID or CKR assignment until the regrouping OSP is received through their Control Channel.

Once active, dynamic regrouping talkgroups follow the same rules for channel grants busies, and denials as all other talkgroups in the system.

4.1.3
Configuration for Secure Supergroup Calls

To allow secure supergroup calls, a Common Key Reference (CKR) number must be defined for supergroup calls in the Provisioning Manager. This setting is made in the System record, as shown in the following table:

Table 18: Configuring Supergroup Calls for Secure Voice Capability

Record	Field	Setting
System	Supergroup Call Secure Key Reference	Common Key Reference (CKR) number to use for secure supergroup calls. This setting should correspond to CKR settings made in the KMF.

The zone controller designates a call as a Supergroup call when a console operator initiates a patch or multiselect function.

When a patch or multiselect call is active, changes in transmission mode are not allowed for any of the participants. The controlling console's transmits mode secure selector is latched throughout the duration of the active call. Participating consoles and radios must respond in the mode assigned by the controlling console. The zone controller rejects any attempts to transmit in a mode different from the controlling console assignment.

4.1.4
Configuration for Secure Private Calls

To enable secure private calls, both the System record and each IVD Radio record must be configured appropriately in the Provisioning Manager. In the System record, the Common Key Reference (CKR)

number is defined for all private calls made in the system. In the IVD Radio record, set the secure communication mode to either Secure or Both. The following table lists the settings required for secure private call capability:

Table 19: Configuring Private Call for Secure Voice Capability

Record	Field	Setting
IVD Radio	Interconnect Enabled	Yes
Radio User Capabilities Profile	Private Call (PC) Enabled	Yes
IVD Radio	Secure Communication Mode	Secure or Both
System	Private Call Secure Key Reference	Common Key Reference (CKR) number to use for all secure private calls in the system. This setting should correspond with CKR settings made in the KMF. Radios must also be provisioned with this CKR.

The zone controller examines the requestor's individual record to determine whether the individual record is strapped secure or selectable. The zone controller either grants or denies an encrypted private call request based upon the requestor's individual record. The zone controller denies the following requests:

- Secure mode PTT to a clear only target. The zone controller indicates to the requestor that the call can be **Clear Only**.
- A private call request between a clear only unit and a secure only unit.

4.1.5
Configuration for Secure Interconnect Calls

For secure-capable telephone interconnect services, each IVD Radio record must be properly configured in the Provisioning Manager. Each radio must be defined with the appropriate secure communication mode (Secure or Both), the Common Key Reference (CKR) for telephone interconnect calls must be defined, and the default mode for all land-initiated interconnect calls must be set.

The following table lists the settings for secure interconnect capability:

Table 20: Configuring Telephone Interconnect for Secure Voice Capability

Record	Field	Setting
IVD Radio	Interconnect Enabled	Yes
	Interconnect Enabled	Yes
	Secure Communication Mode	Secure or Both
	Interconnect Secure Key Reference	Common Key Reference (CKR) number to use for secure interconnect calls. This setting should correspond to CKR settings made in the KMF. Radios must be provisioned with this CKR.
	Secure Land to Mobile Start Mode	Set to Secure if all land initiated calls should default to secure mode when started.

The Secure Land to Mobile Start Mode field has two values: **Secure** and **Clear**.

ASTRO® 25 supports secure upgrades for telephone interconnect calls but only from the radio side. Whether the call is initiated by the radio or the land line, if the call starts in clear mode, the radio is able to request a change to secure mode. Once secure resources are assigned, the call remains secure until either the radio or the land line terminates it.

4.1.6
Creating Secure Encryption Card Records

A Secure Card record must be defined in the Provisioning Manager (PM) for each secure card installed in the zone. Each record identifies the secure console, card ID, and slot number for the secure card.

CAUTION: Disable the secure console before you set the provision flag. If you do not disable the console before provisioning, you might terminate call processing by the console.

4.2
Configuring Secure Entities for ASTRO 3.1 Conventional IVD Systems

This section lists the items to configure for secure voice, data, and OTAR operations in an ASTRO® 3.1 Conventional IV&D system.

Table 21: Configuring Secure Entities for ASTRO 3.1 Conventional IVD Systems

Entity	Reference
Configure the KMF.	See the “KMF Configuration” chapter in the *Key Management Facility* manual.
Configure the KVL for OTAR.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*, depending on your KVL model.
Configure the WNG.	See Wireless Network Gateway Configuration on page 84.
Configure the RNC encryption unit.	See the *ASTRO 25 RNC/KMF Encryption Unit Service Manual* (6880800B70) and *ASTRO 25 RNC/KMF Encryption Unit Functional Manual*.
Configure the DIU 3000 encryption cartridge.	See the *ASTRO DIU 3000 Digital Interface Unit Owner's Manual* (6802949C65) and *ASTRO Digital Interface Unit Encryption Cartridge Instruction Manual* (68P80801G85).
Configure the radios.	See Configuring Radios for Secure Communications on page 85.
Set up the KVL 3000 Plus or KVL 4000 and load keys into all the secure devices.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

4.2.1
Wireless Network Gateway Configuration

The Wireless Network Gateway (WNG) must be properly configured to communicate with the KMF. This configuration allows Over-The-Air Rekeying (OTAR) messages to be properly routed between the KMF host network and the analog conventional radio system. In the WNG, the SNMP protocol must be enabled, CAI numbers for each radio unit must be entered, CAI_Group CAI ID numbers must be added, and Connection ID (CID) Idle Time must be set to zero.

When and where to use: After the Wireless Network Gateway (WNG) has been installed in the ASTRO® 3.1 Conventional IV&D system, use the following process to configure the WNG to communicate with the KMF.

NOTICE:
For current part numbers for any Motorola Solutions manuals, contact your Motorola Solutions representative.

For additional information on WNG configuration, see the *Wireless Network Gateway Installation and Operations Reference* (6871015P29).

Process:

1. Enable SNMP in the Wireless Network Gateway (WNG). See the “SNMP Configuration” section in the *Wireless Network Gateway Installation and Operations Reference* (6871015P29).

   NOTICE: The KMF and WNG communicate using both FLM (an IP-based protocol) and SNMP. Normal installation of the WNG does not require that SNMP be enabled, therefore it must be enabled for OTAR to work.

2. Enter CAI numbers for each unit into the WNG. See the *Wireless Network Gateway Installation and Operations Reference* (6871015P29) for adding or modifying a device in the configuration section.

   NOTICE: Each CAI number must have the CID from the WNG procedure entered in the **FLM Host CID(s)___KMM___** field in the WNG mobile device management database. A radio unit's CAI ID is programmed into the radio unit using the Customer Programming Software. This number must be entered in the WNG and must contain the prefix **7F00**_ _ _ _. The last four digits of the unit CAI ID are stored in the WNG in hexadecimal, as compared to the decimal representation in the KMF user interface.

3. Add the All Call group CAI ID, which enables CKR updates to be broadcast through OTAR:
   1. In the WNG application, select **Adding a Device**.
   2. Set the device LLI number to **7fffffff**.
   3. Set the device type to **CAI_Group**. Press ENTER.
   4. At the next screen, set Reg State to **Deregistered**.
   5. Set the ICMP to **N** (No). Press ENTER.
4. Change the connection ID idle time. The default value for this parameter (**FLM Host CID Session IDLE Time**) is 10 seconds. Set this value to zero. Perform this configuration change as described in the section on using FLM host services in the *Wireless Network Gateway Installation and Operations Reference* (6871015P29).

4.3

Configuring Secure Entities for ASTRO 25 Conventional IVD Systems

This section lists items to configure for secure voice, data, and OTAR operations in an ASTRO® 25 Conventional IV&D system.

Table 22: Configuring Secure Entities for ASTRO 25 Conventional IVD Systems

Entity	Reference
Configure the KMF.	See the “KMF Configuration” chapter in the *Key Management Facility* manual.
Configure the KVL for OTAR.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or the *KVL 4000 Key Variable Loader ASTRO 25 User Guide*, depending on your KVL model.
Configure the radios.	See Configuring Radios for Secure Communications on page 85.
Configure Firewall for OTEK.	Open a case with the Motorola Solution Support Center (SSC) to modify the RNI-DMZ firewall configuration for OTEK.
Configure the Console to work with KMF/ OTEK.	See the following manuals, depending on your console model: • *MCC 7500 Console Sites with VPM* • *MCC 7100 IP Dispatch Console Setup and User Guide*
Configure the MCC 7500 Archiving Interface Server (AIS).	See the *Audio Logging* manual.
Configure the CDEM (for secure data only).	See the *CAI Data Encryption Module* manual.
Set up the KVL 3000 Plus or KVL 4000 and load keys into all the secure devices.	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

4.4

Configuring Radios for Secure Communications

Radio configuration is achieved through Customer Programming Software (CPS). A PC running CPS is directly connected to the radio's universal connection port and the codeplug is loaded. After the codeplug is loaded, the radio can be initially provisioned with keys from a KVL. Subsequent key loads can be accomplished through KVL or through OTAR (if available).

The configuration settings in CPS are categorized into different types, such as Radio Wide settings, Controls, Display and Menu settings, Phone settings, and Secure settings. By navigating to the Secure settings, you can open the Secure Configuration window or view Secure Hardware Encryption Multikey records.

The Secure Configuration window contains all the fields and settings specific to secure voice and OTAR operation. These fields must be properly configured for the radio to have secure voice and OTAR capability. In addition to the Secure Configuration window, the radio must also be configured with the appropriate parameters for packet data capability (for OTAR connection to the KMF). Other

parameters must be set according to the services used by the radio (such as telephone interconnect). Key assignment slots are assigned for the radio by the Secure Hardware Encryption Multikey records in CPS. Keys can be defined with two slots per CKR (to support two TEKs per CKR).

After radios have been configured through CPS, you can manually load keys into the radio with a KVL, or load keys from the KMF to the radio through a KVL using the store and forward feature.

NOTICE: Fields and settings for radios vary slightly. Refer to your CPS online help to determine the appropriate secure settings for your radios.

4.4.1
Configuring Subscriber Radios for Encrypted Integrated Data (EID)

To enable EID for subscriber radio internal applications, you enable the EID feature in the subscriber radio. However, data association rules must be added to the PDEG Encryption Unit the subscriber uses to process data flows between the subscriber radios and the red subnet servers used by the subscriber radio internal applications.

The procedures for configuring subscriber radios for EID depend on the model of subscriber radio used in your system. For detailed configuration procedures, refer to the following documentation and help:

- ASTRO® 25 subscriber radio user guide for your specific model
- *ASTRO 25 Customer Programming Software* online help
- *Encrypted Integrated Data* manual
- *PDEG Encryption Unit* manual

4.5
Secure Communications Interoperability

The Key Management Facility can manage Over-The-Air Rekeying (OTAR) operations over multiple radio systems, including ASTRO® 25 Trunking IV&D, ASTRO® 3.1 Conventional IV&D, and ASTRO® 25 Conventional IV&D systems. The KMF equipment resides on an external Customer Enterprise Network which is connected to all the supported ASTRO® 25 Trunking IV&D, ASTRO® 3.1 Conventional IV&D, and ASTRO® 25 Conventional IV&D systems. The KMF can communicate with radios using any of the available transport networks.

The KMF provides a centralized interface which transparently sends OTAR messages to target radios over the appropriate transport network. Key material and OTAR operations can be managed centrally through the KMF as if all radios operated on the same infrastructure. If the radio is context-activated and registered over the trunked network, the KMF delivers OTAR traffic as packet data through the trunked network. If the radio is active on the ASTRO® 3.1 Conventional IV&D or ASTRO® 25 Conventional IV&D network, the KMF tries to deliver OTAR messages to radios as data messages over the ASTRO® 3.1 Conventional IV&D or ASTRO® 25 Conventional IV&D network.

In the ASTRO® 25 Trunking IV&D and ASTRO® 25 Conventional IV&D network, OTAR traffic is routed over the DMZ to the firewall, GGSN, and Packet Data Gateway (PDG) for delivery to the appropriate radios on the trunked network. The KMF must be provisioned with a trunking system record with the appropriate transmit and receive ports. The KMF must also be provisioned with records for each MCC 7500 Dispatch Console in the trunked system.

In the ASTRO® 3.1 Conventional IV&D network, OTAR traffic is routed through the Wireless Network Gateway (WNG), then distributed through the RNC 3000, and sent to the appropriate DIU 3000 for delivery over the conventional channel. The KMF must be provisioned with a conventional system record which includes the IP address of the WNG. The KMF must also be provisioned with records for each RNC encryption unit and each DIU encryption cartridge.

4.5.1

Configuring Secure Communications Entities for Interoperability

When and where to use: Follow this procedure to configure secure communications entities for interoperable OTAR over ASTRO® 25 Trunking IV&D, ASTRO® 3.1 Conventional IV&D, and ASTRO® 25 Conventional IV&D systems.

Process:

1. Install and configure all non-secure equipment according to your system documentation.
2. Install the appropriate secure hardware for each RNC 3000 and DIU 3000 in the ASTRO® 3.1 Conventional IV&D system.
3. In the ASTRO® 3.1 Conventional IV&D system, configure the Wireless Network Gateway.
4. Configure the ASTRO® 25 Trunking IV&D system for secure operation, as described in Configuring Secure Entities for ASTRO 25 Trunking IVD Systems on page 79.
5. Install and configure the KMF hardware, as described in the “KMF Installation” chapter in the *Key Management Facility* manual. A KMF supporting interoperability uses the ASTRO® 25 Trunking IV&D KMF configuration.
6. Configure the KMF parameters and records, as described in the “KMF Configuration” chapter in the *Key Management Facility* manual.
7. Configure the radios for secure operation using the information in CPS online help or Configuring Radios for Secure Communications on page 85.
8. Configure the consoles for secure operation, as described in the *MCC 7500 Console Sites with Voice Processor Module* manual, or the *MCC 7100 IP Dispatch Console Setup and User Guide*.
9. Set up the KVL 3000 Plus or KVL 4000 and load keys into all the secure devices, as described in the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*.

This page intentionally left blank.

Chapter 5

Secure Communications Performance and Troubleshooting

This chapter describes the tools and methods used to manage performance and troubleshooting for secure communications services.

5.1 Performance Management and Troubleshooting Tools

Various tools are available to monitor the secure communications system and capture information for users, talkgroups, radios, and infrastructure devices. Using this information, you can analyze how your system is operating, whether resources are being allocated properly, and whether users can communicate without delays or bottlenecks. The following tools are covered in this section:

5.1.1 Key Management Facility

The KMF manages all keys for the secure system and provides the following tools to help diagnose secure communications problems:

- Event Viewer, to view the status and progress of OTAR and other commands initiated by the KMF Client
- Event Logs, to view KMF events, such as OTAR operations and server processes
- Summarized reports for Radio, Console, CDEM, or TMG records, which display the device name, assigned and actual RSI, and device state
- Detailed reports for Radio, Console, CDEM, TMG, CKR, RNC, AIS, PDEG, MDEG, and DIU records, which display the assigned device group, current device status, and pending actions for the device. The report also displays all algorithms and keys (KEKs, TEKs, CKRs) associated with the device, and its keyset status.
- The Export Unit Report, which provides currency, device state, transport system, and air address data in comma–separated value (CSV) format for each device managed by the KMF
- Current real-time currency status, displays at the bottom of the KMF main window.
- Currency update status, an indicator immediately to the right of the System Currency status bar.

- Group currency state, listed on the Details page for the following groups: radio, MDEG, AIS, Console, DIU, RNC, PDEG, CDEM, and TMG.

For more information about system performance measurement using the KMF, see the “KMF Operation” chapter in the *Key Management Facility* manual.

5.1.2
InfoVista

InfoVista is a performance monitoring tool that provides reports for usage statistics applicable to voice only, data only, or for both voice and data. Reports are available at the channel, site, and zone level. See the *InfoVista User Guide* manual for a description of the reports and how to access them via the InfoVista console. Specific information in the reports includes the following:

- Amount of time channel allocated for data
- Percent of time channel allocated for data
- Number of data channel requests
- Total busies for data channel requests
- Total busy duration
- Max busy duration
- Average busy duration
- Total number of data allocations
- Total time duration for data
- Total time in use for voice and data

The following reports are available for broadcast data usage analysis:

- Number of broadcast messages sent to the sites
- Number of broadcast messages sent to each broadcast agency/ID
- Number of dropped broadcast messages per site
- Number of dropped broadcast messages overall

5.1.3
Event Reporting for Subscriber Radios

The subscriber radio provides the ability to report exception events (failure to encrypt/decrypt) to the user display and to a connected mobile computer through SNMP trap messages (per Project 25 Radio Management Protocol, also known as Radio Control Protocol – RCP, ANSI/TIA-102.BAEE-B). Consult the specific subscriber radio user manual used in your ASTRO® 25 system for details about these event reporting capabilities.

5.1.4
ATIA Logs (ASTRO 25 Trunking IVD Systems Only)

The Air Traffic Information Access (ATIA) Log Viewer application allows you to view log files. These log files contain records of all recent zone activity, such as site registrations and calls processed. For example, you can view the logs to determine if a console has registered. For more information, see the *ATIA Log Viewer* manual.

5.1.5
PDEG Encryption Unit Event Logging (ASTRO 25 Trunking IVD Systems Only)

A CEN-based syslog server is required to monitor events from the PDEG Encryption Unit. Alternatively, a freeware syslog server application can be installed on a CEN host connected to the PDEG Encryption Unit for event and fault logging. Syslog reporting must be enabled in a PDEG Encryption Unit to use its event logging reporting capability and then configuration changes in the device can be monitored. Extensive event logging capabilities are available by placing the PDEG Encryption Unit in debug mode. For details, see the *PDEG Encryption Unit* manual.

5.1.6
Radio Network Controller (ASTRO 3.1 Conventional IVD Systems Only)

The RNC 3000 provides monitoring functions for all connected RF network devices and the repeaters that provide the wireless connectivity. In the ASTRO® 25 system, many of the radios and other infrastructure devices get their secure key information using OTAR commands. The RNC performs the following monitoring functions:

- User device status
- Base radios status
- Host interface status
- Encryption device status
- RNC log messages
- RNC statistics

See the *Radio Network Controller 3000 Operations Manual* (68P81098E70) for complete details of the information provided by the RNC 3000 monitoring functions.

5.1.7
Wireless Network Gateway (ASTRO 3.1 Conventional IVD Systems Only)

The WNG provides information about network devices in the system and network activities. See the *Wireless Network Gateway Installation and Operations Reference* (6871015P29) for complete details of the information provided by the WNG monitoring functions.

5.1.8
Repair and Configuration Records

The following information should be considered a minimum for repair reports:

- The dates of all troubleshooting and repair activity.
- Records of conversations with users or technicians regarding the fault and its repair.
- Records of conversations with the Motorola Solution Support Center (SSC) before and after performing system repairs.
- Detailed descriptions of the fault isolation procedure you used to determine the faulty device.
- Any data you backed up before performing the repair.
- The items you replaced, including serial numbers and model numbers.

- Any items you returned to Motorola Solutions for repair, including serial numbers and model numbers.
- Software titles and versions that you had to reinstall.
- Data you had to restore and the date on which you restored it.
- The reset and optimization procedures you performed.
- Changes or restorations to user configurations you made.
- Whether the repair resolved the problem.
- Other devices involved in the failure that require repair, calibration, or optimization.

Repair records are valuable. How a problem was corrected in the past can help you troubleshoot new problems.

5.2 Secure Communications Troubleshooting – General Process

Many of the Motorola devices installed in your system provide their own diagnostics through their CPS, status through LEDs, and troubleshooting processes in their manuals. This guide is not intended to replace these diagnostics but to provide a system-level troubleshooting process. Troubleshooting should start from the least invasive and easiest-to-do and progress to the more difficult.

When and where to use: Use this process to identify, isolate, and analyze problems in the secure communications system. For detailed troubleshooting procedures, see the following application manuals or online helps, as appropriate:

- *Key Management Facility* manual
- *Encrypted Integrated Data* manual
- *PDEG Encryption Unit* manual
- *Conventional Data Services* manual
- *CAI Data Encryption Module* manual
- *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*
- *Provisioning Manager* manual
- *Unified Network Configurator* manual
- *Packet Data Gateways* manual
- *MCC 7100 IP Dispatch Console Setup and User Guide*
- *Configuration/Service Software (CSS)* online help
- *ASTRO 25 Customer Programming Software (CPS)* online help

Process:

1. Categorize the problem.
   - Does rekeying through the Key Variable Loader (KVL) work?
   - Can radios communicate in secure mode and in clear mode, or in just one mode? Which mode is not working?
   - Can the console operator position communicate in secure mode and in clear mode, or in just one mode? Which mode is not working?
   - Is Over-the-Air Rekeying (OTAR)/Over-the-Ethernet Keying (OTEK) working?
   - Can wireless network elements communicate?

- Have both voice communication and data communication failed?
- Is the failure intermittent or absolute?
- Is voice communication of poor quality?

2 Isolate the potential source of the fault.

- Run specific tests (such as attempting to use a feature) to isolate the device or software at fault.
- Use statistics (such as replacing a module that has a high probability of being the cause).
- Verify CKR numbering and Key IDs. Connect the KVL to the radio to verify which keys are loaded, to determine the currently active keyset, and to confirm that the Radio Set Identifier (RSI) of the radio is consistent with the RSI as listed in the KMF.

If…	Then…
The problem appears to be hardware-related...	Repair the failure by replacing the faulty Field Replaceable Unit (FRU).
The problem appears to be software-related...	Reload or reconfigure the application software, utility software, or database.
The problem appears to be user-related...	Educate the user as to proper operation.

3 Correct the problem. You may need to perform one or more of the following steps:

- Replace a failed component.
- Educate a user about proper operation.
- Reconfigure the KMF.
- Update the KMF database.
- Reconfigure the radio.
- Reinstall keys in a secure device.
- Reconfigure the MCC 7500/7100 Dispatch Console.
- Reconfigure the DIU 3000 (ASTRO® 3.1 Conventional IV&D systems only).
- Reconfigure the Provisioning Manager (PM) and Zone Configuration Manager (ZCM) (for M Core Systems only)
- Reconfigure the Configuration Manager (for K core systems only).

4 Verify if the problem has been solved. If the problem has not been solved, repeat the process. You may have made an error in categorizing the problem or in isolating the source. If you cannot correct the problem, contact the Motorola Solution Support Center (SSC).

5.2.1
Troubleshooting Communications Problems

There are several situations that prevent radio units from communicating with each other and with the Console Operators. These situations include:

- Radio unit to unit secure communications does not work. Possible causes are:
  - Missing keys in a radio unit
  - CPS configuration of the radio units does not match.
  - Radio units do not contain the same encryption algorithms.

  - Different keys in the radio units under the same CKR
- Radio unit to radio unit works but radio unit to console and console to radio unit does not. Possible causes are:
  - Manager and CPS configure a different CKR for the call.
  - No keys in the MCC 7500 Dispatch Console
  - Radio unit and MCC 7500 Dispatch Console contain different keys under the same CKR.
  - Radio unit and MCC 7500 Dispatch Console do not contain the same algorithms.
- Radio unit to radio unit and console to radio unit work but radio unit to console does not. A possible cause is:
  - Incorrect “DES-XL Tx default” setting in radio CPS (radio is transmitting with DES-XL or DES-OFB, but the MCC 7500 Dispatch Console expects the opposite algorithm)

This list is not meant to be complete. However, it demonstrates some of the situations that can cause secure voice communication to fail.

If you need further help, contact the Motorola SSC for assistance.

Chapter 6

Secure Communications Field Replaceable Units and Entities

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to secure communications.

6.1 Secure Communications Equipment - Service Overview

Due to the high percentage of surface-mount components and multi-layer circuit boards, the ASTRO® 25 system hardware follows the Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) maintenance philosophy.

The ASTRO® 25 FRU hardware is composed of self-contained modules that, when determined to be faulty, are quickly and easily replaced with a known good module to return the equipment to normal operation. The faulty module must be shipped to the Motorola Infrastructure Depot Operations (IDO) for further troubleshooting and repair.

The ASTRO® 25 FRE hardware does not contain any replaceable modules. When FRE hardware is determined to be faulty, the entire unit is replaced. The faulty hardware must also be shipped to the Motorola IDO for further troubleshooting and repair.

Table 23: Secure Voice Equipment FRU/FRE Replacement Information

Secure Communications Equipment	FRU/FRE Replacement Information and Procedures
Key Management Facility (KMF)	See the *Key Management Facility* manual.
KMF CryptR	See the *KMF CryptR User Guide* manual.
PDEG (ASTRO® 25 Trunking IV&D systems only)	See the *PDEG Encryption Unit* manual.
Border Gateway	See the *System Gateways – GGM 8000* manual.
Firewall server	See the *Fortinet Firewall* or *Juniper Firewall* manual.
Radio Network Controller (RNC) (ASTRO® 3.1 Conventional IV&D systems only)	See the *ASTRO 25 RNC/KMF Encryption Unit Functional Manual*.
Wireless Network Gateway (WNG) (ASTRO® 3.1 Conventional IV&D systems only)	See the *Wireless Network Gateway Installation and Operations Reference* (6871015P29) manual.
Digital Interface Unit (DIU) (ASTRO® 3.1 Conventional IV&D systems only)	See the *ASTRO DIU 3000 Digital Interface Unit Owner's Manual* (6802949C65).
Gateway GPRS Support Node (GGSN)	See the *System Routers - S6000/S2500* manual.

Table continued…

Secure Communications Equipment	FRU/FRE Replacement Information and Procedures
Packet Data Gateway (PDG)	See the *Packet Data Gateways* manual.
CDEM (ASTRO® 25 Conventional IV&D systems only)	See the *CAI Data Encryption Module* manual.
Site Gateway (Conventional Channel Interface)	See the *System Routers – S2500 and S6000* manual.
ASTRO® 25 Digital Secure Radios	See the service manual for your specific radio model.
KVL 3000 Plus or KVL 4000	See the *KVL 3000 Plus Key Variable Loader User's Guide* (6881132E29) or *KVL 4000 Key Variable Loader ASTRO 25 User Guide* and *MC55 Enterprise Digital Assistant User Guide*.

6.2 General Tools and Equipment

Where appropriate, this chapter lists the tools and equipment needed for replacing parts in the system. In addition to the specific tools and equipment listed, consider taking the following equipment to the repair site, as applicable:

- This manual
- ASTRO® 25 documentation set CD
- Product-specific documentation
- Customer system documentation
- List of equipment logins and passwords
- Wooden or fiberglass ladder
- Flashlight pens, markers, and wire labels

6.3 General Safety Information

Follow all applicable safety procedures, such as Occupational, Safety, and Health Administration (OSHA) requirements, National Electrical Code (NEC) requirements, local code requirements, and safe working practices. Read and follow all warning notices and instructions marked on the product and included in this booklet before installing, servicing, or operating equipment. Always exercise good judgment when servicing equipment.

Important safety information is listed here and throughout this manual to point out situations that may result in injury, interruption in services, or damage to equipment. Always observe all safety information when servicing equipment and take appropriate action.

WARNING:
Dangerous voltages are present in system equipment which can cause electrical shock or damage to equipment. Carefully follow the replacement procedures and avoid contact with any sources of high voltage when servicing equipment. Unless the equipment is designed for hot swapping components, always turn off the equipment and remove all power cabling and battery backup sources before servicing the equipment. Avoid touching any live voltage sources when hot swapping equipment or when working near disconnected wires.

Avoid sources of high voltage when wearing an electrostatic discharge (ESD) strap. The path to ground can increase the risk of electrical shock.

Do not operate any RF-based equipment near electrical blasting caps or in an explosive atmosphere. Do not operate radio transmitters unless all RF connectors are secure and all connectors are properly terminated.

Invisible laser radiation may be emitted from disconnected fibers and cables in certain devices in the system. Avoid eye contact with beams to prevent damage to eyes when working with this equipment.

CAUTION:
Some equipment in the system is extremely heavy. Have another person help support and lift any heavy equipment when replacing to avoid personal injury and to avoid dropping or damaging the equipment.

Ground all equipment properly according to Motorola Solutions installation instructions for safe operations. See *Standards and Guidelines for Communication Sites* (6881089E50). Reattach grounding cables to equipment after replacement.

Do not install substitute parts or perform any unauthorized modifications to equipment. Unauthorized modifications or substitute parts may introduce additional hazards.

IMPORTANT:
Items identified as FRUs or FREs do not include any field serviceable parts. Replace any damaged or impaired FRU or FRE equipment and send the damaged equipment to Motorola Solutions for repair.

Several replacement procedures in this booklet affect system operation and may affect radio services. Take note of any potential affects on the system and consider the consequences of powering down or removing a device. Alert the affected individuals who might experience a loss of service before powering down or replacing equipment.

All equipment should be serviced only by a qualified technician in accordance with all national and local codes. See the appropriate manuals for additional pertinent safety information.

6.3.1
Electrostatic Discharge and Safety

This section describes how to protect secure equipment and components from electrostatic discharge (ESD).

CAUTION: CMOS devices are susceptible to damage. ESD damage can be latent, with units failing weeks or months later. The handling precautions provided in this section are required when you are replacing FRUs in units, especially in low-humidity conditions.

Before replacing FRUs in any secure equipment, take the following precautions:

- Eliminate static generators in the work area.
- Remove nylon or double-knit polyester jackets, roll up long sleeves, and remove or tie back loose hanging neckties.
- Store and transport all static-sensitive devices in ESD-protective containers.
- Disconnect all power from the unit before static-sensitive components are removed or inserted.

- Use a static-safeguarded workstation, which uses an anti-static kit *(Motorola Solutions PN 01-80386A82)*:
  - Wrist strap
  - Two ground cords
  - Static-control table mat
  - Static-control floor mat

  CAUTION: If a static-safeguarded workstation is not available, use a conductive surface for placement of static-sensitive devices. Touch and maintain contact with the conductive work surface when you set down the device or pick up the device.
- Read the *Service and Repair Note SRN-F1052, Static Control Equipment for Servicing ESD Sensitive Products*.

6.4 Verifying Serviced Equipment

After equipment has been serviced and restored to normal operation, verify that the original problem has been resolved and that all other components are still working properly. This section lists several verification methods that can be applied to serviced equipment. If a device cannot be restored to normal operation, contact the Motorola Solution Support Center.

NOTICE: When verifying equipment, note that some devices that have been serviced may take some time before they are operational and back in service.

Check the physical condition of the unit:

1. Verify that all affected components are fully and appropriately installed.
2. Verify that all cabling is securely connected to the correct ports and that there are no stray wires near the unit.
3. Verify that there are no tools or hardware (including nuts, bolts, or screws) located in or around the unit.
4. Listen to verify that all mechanical equipment such as hard drives, fans, and other equipment are operating properly in the unit.

Check LED indicators:

1. Verify that the LEDs are indicating that each component is in good condition and operating properly. Indicators typically show that the device is powered, enabled, and performing operations.
2. For equipment such as processor cards, networking cards, and hard drives, verify that the activity LEDs are neither fully on or fully off. The activity LEDs should appear to fluctuate as traffic is being handled or as processes are taking place.

Verify that the device is operating properly:

1. Verify that the device is supporting its intended function in the system. Use a radio, client PC, or other applicable device to determine that the call services or network services supported by the device are working.
2. For fixed-radio equipment, use the appropriate test equipment and tools such as Configuration/ Service Software (CSS) to run transmission tests and determine signal integrity.
3. Verify that other related equipment at the site, which may have been affected by the serviced device, are now operating properly.

NOTICE: Descriptions for all devices and their components are provided in the individual chapters of this booklet.

Appendix A

Supported Algorithms

An encryption algorithm is a mathematical formula that uses a set of bit shifts, permutations, and logic operations to transform clear data into encrypted code. Only the intended recipient can decrypt the code. The algorithm uses a key to uniquely encrypt traffic. This encryption requires the recipient to have the same key and use the same algorithm to decrypt the traffic. Anyone trying to decrypt traffic without the same key and the same algorithm cannot recover the original unencrypted voice traffic.

A device supporting encryption can implement an algorithm as a function of software, hardware, or a combination of both hardware and software. Secure devices in the ASTRO® 25 system support the addition and removal of algorithms that can be loaded into the secure devices.

This appendix describes the following ASTRO® 25 system-supported algorithms:

- AES
- DES-OFB
- DES-XL
- DVP-XL
- DVI-XL
- ADP

NOTICE:

- Not all secure devices in the system support all algorithms.
- Proprietary encryption algorithms (DVP-XL, DVI-XL, and DES-XL) are not supported in TDMA mode.
- Only the AES and DES-OFB algorithms are supported for ASTRO® 25 Conventional IV&D system data encryption.
- AES and DES-OFB are standard encryption algorithms. All other algorithms are proprietary Motorola Solutions encryption algorithms.

A.1 Data Encryption Standard (DES/DES-XL/DES-OFB)

The Data Encryption Standard (DES) was developed by IBM for the federal government, and is approved to provide security for sensitive, unclassified radio communication. This standard uses 56-bit keys, with each byte of the key having odd parity (odd number of binary 1s). 7.2 x 10E16 unique keys can be used with this algorithm.

While several varieties of DES exist, the ASTRO® 25 system supports DES-XL and DES-OFB. The DES-OFB algorithm has been selected as the APCO 25 digital encryption standard. DES-OFB utilizes the output feedback (OFB) method of encryption synchronization and is only compatible with systems using the APCO 25 specified Advanced Multi-Band Excitation (AMBE) vocoder. DES-OFB is not compatible with Vector Sum Excited Linear Prediction (VSELP). For DES-OFB, data is divided into blocks of bits, and encrypted output from one block of data is used as an additional input for encrypting the next block of data. DES-OFB is not self-synchronizing.

DES-XL is an enhanced version of the DES algorithm that uses the counter addressing method of encryption synchronization. Counter addressing is a Motorola Solutions proprietary method of encryption synchronization that attaches a synchronization preamble bit string to the front of an encrypted voice signal. Counter addressing also periodically inserts a synchronization update during

the message. This continual re-synchronization corrects errors that may corrupt the signal and keeps the communicating radios synchronized. One bit of error introduced to a radio signal causes only one bit of encrypted audio to be destroyed (rather than several bits that would be destroyed with the original DES algorithm). Error correction allows a radio operating in noisy or fringe coverage areas to experience the same performance and quality of call services in both clear and secure modes.

The Data Encryption Standard is defined in FIPS publications 46-2, 46-3, and 81.

A.2 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an improvement over DES algorithms, using keys of 128, 192 bits, or 256 bits to encrypt blocks of 128-bit traffic. The Motorola Solutions secure voice solution uses a 256-bit key. AES uses the Rijndael algorithm with symmetric block cipher. Between 3.4 x 10E38 and 1.1 x 10E77 possible unique keys can be used with this algorithm, depending on the size of the key used. This enhances communication security by providing a range of at least 10E21 more unique keys than DES. AES is not compatible with VSELP. The Advanced Encryption Standard is defined in FIPS publication 197. AES allows interoperability, like DES-OFB.

A.3 Digital Voice Privacy - Extended Range (DVP-XL)

Digital Voice Privacy is a proprietary algorithm developed by Motorola Solutions. It features a sophisticated encryption technique using a 32-bit key to provide high-level digital voice security for two-way radio communication. The algorithm supports a total of 2.36 x 10E21 unique keys. This algorithm is primarily used by non-federal government agencies, commercial firms, national organizations, and state and local governments. The DVP-XL algorithm is an enhanced version of the DVP algorithm, using a counter addressing method of synchronization. This enhancement promotes a low bit error rate over larger ranges, allowing radios to experience equal performance for both clear and secure voice calls, even in fringe coverage areas.

NOTICE: Proprietary encryption algorithms (DVP-XL, DVI-XL, and DES-XL) are not supported in TDMA mode.

A.4 Digital Voice International - Extended Range (DVI-XL)

DVI-XL is a proprietary algorithm developed by Motorola Solutions to meet the requirements of secure communications for international markets. While other algorithms have certain export restrictions, DVI-XL is designed for international export and can be readily sold to customers outside of the United States. DVI-XL uses the counter addressing method of synchronization.

NOTICE: Proprietary encryption algorithms (DVP-XL, DVI-XL, and DES-XL) are not supported in TDMA mode.

A.5 Advanced Digital Privacy (ADP)

ADP is an encryption option, which can be used for secure communication, but where extensive encryption capabilities are not required. The algorithm and keys for ADP can be installed on radios (with or without a Universal Crypto Module). The keys are loaded into a radio either through Customer Programming Software (CPS) or KVL.

ADP uses a 40-bit key and the RC4 cipher algorithm to encrypt and decrypt voice traffic. Up to 8 ADP keys can be loaded into a radio or secure infrastructure. ADP does not support Over-The-Air Rekeying

(OTAR) and does not support keyset changeover. ADP also does not support centralized key management from a Key Management Facility.

A.6 Single Algorithm

ASTRO® 25 radios support a single algorithm encryption capability. This capability is an optional feature.

Single algorithm capability means that one encryption algorithm is used system wide. The algorithm can be either a standard or a proprietary algorithm.

A single encryption key or multiple encryption keys can be used with a single algorithm.

NOTICE: The multi-key option is required to use multiple encryption keys.

A.7 Multiple Algorithm

ASTRO® 25 radios support multiple algorithm encryption capability. This capability is an optional feature.

Multiple algorithm capability means that you can use more than one encryption algorithm system wide. Multiple algorithms provide flexibility for large organizations. The algorithms can either be standard or proprietary or a combination of both. Multiple algorithm capability allows organizations to create separate operational groups by using a different encryption algorithm for each operational group.

Multiple algorithm capability also allows for interoperability between organizations and operational groups. Organizations or groups that must communicate with each other can do so by using a common encryption algorithm. Radios with multiple algorithms can operate on different system infrastructures where each system uses a different encryption algorithm.

Multiple algorithm capability also provides backward compatibility during a migration to a new encryption algorithm by allowing a radio to use the old and new encryption algorithms.

A.8 Single Key

Single key encryption systems offer the ability to encrypt voice transmissions using a single encryption key. This capability is an optional feature.

Radios can communicate to other radios possessing that key. This capability enhances the transmission of highly sensitive information. Users can speak freely without concern that their conversations can be picked up by unauthorized listeners.

Radios can communicate in secure mode with other radios programmed with the same key. Radios that do not have the appropriate encryption key cannot decode encrypted transmission.

You can use single key encryption when the radios operating in the system only support one key at a time. Single key encryption also only uses one encryption algorithm. When single key encryption is used, OTAR and keysets are not used.

A.9 Multi-Key

The ASTRO® 25 system can support multi-key encryption. This capability is an optional feature.

Multi-key is the capability to use different ASTRO® 25 secure keys for the various talkgroups and individuals throughout the system. In an ASTRO® 25 system equipped with multiple keys, each user radio can maintain up to 48 different traffic Common Key References (CKRs). The infrastructure encryption cards can maintain up to 500 different traffic keys for encrypting and decrypting voice traffic. In trunking, “talkgroups” separate different groups of users. One key is used for a given talkgroup, and all talkgroup members must possess that key to communicate securely. It is possible to program a radio for many talkgroups, although the radio can only operate one talkgroup at a time. The radio must possess all the keys that the talkgroups use so that the radio user can carry on secure voice communication. The same key may be used for more than one talkgroup.

The following demonstrates how keys can be assigned to talkgroups and how the key assignments affect communication capability:

Table 24: Example of Using Encryption Keys with Talkgroups

Radio 1	Radio 2	Radio 3
Talkgroup 1 - Key A	Talkgroup 1 - Key A	Talkgroup 1 - Key A
Talkgroup 2 - Key A	Talkgroup 2 - Key A	Not programmed for Talkgroup 2
Talkgroup 3 - Key B	Not programmed for Talkgroup 3	Talkgroup 3 - Key B
Not programmed for Talk-group 4	Talkgroup 4 - Key C	Talkgroup 4 - Key C

- Radios 1, 2, and 3 can communicate on Talkgroup 1 using key A
- Radios 1 and 2 can communicate on Talkgroup 2 using key A
- Radios 1 and 3 can communicate on Talkgroup 3 using key B
- Radios 2 and 3 can communicate on Talkgroup 4 using key C

In ASTRO® 25 systems, multiple key encryption is standard for the MCC 7500 Dispatch Console and is an option for radios. The secure cards can store up to 500 different keys. A Key Variable Loader (KVL) is used to load the encryption keys in the console and radios. The console requires that the Key Variable Loader operate in the ASTRO® 25 mode. OTAR is optional for the multi-key solution.

Appendix B

Federal Information Processing Standards (FIPS)

An ASTRO® 25 system supports several Federal Information Processing Standards (FIPS).

B.1 FIPS 140-2

This standard specifies the security requirements of a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include:

- Specification
- Ports and interfaces
- Roles, services, and authentication
- Finite state model
- Physical security
- Operational environment
- Cryptographic key management
- Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
- Self-tests
- Design assurance
- Mitigation of other attacks

B.2 FIPS 197

This standard covers the Advanced Encryption Standard (AES) algorithm, which specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

This page intentionally left blank.

Appendix C

Secure Call Processing for ASTRO 25 Trunking IVD Systems

The following sections describe the processes that the ASTRO® 25 Trunking IV&D system performs when users initiate secure voice calls. The types of calls are:

- Console operator-initiated secure calls
- Radio user-initiated secure calls
- Telephone Interconnect calls

C.1 Console Operator-Initiated Secure Calls

This section discusses the various types of calls that a console operator can initiate. These types include:

- Secure calls to a talkgroup
- Secure calls to an individual radio user

C.1.1 Making a Secure Call From the Console Operator to a Talkgroup

This section describes the events that take place when a console operator makes a secure call to a talkgroup.

Prerequisites: To make a secure call to a talkgroup, the console must be capable of making secure calls.

Process:

1. The console operator selects a talkgroup.
2. The console equipment generates a request for service.
3. The request is routed to the zone controller.
4. The zone controller locates the appropriate resources and identifies the encryption mode capability for the requested talkgroup.
5. The zone controller sends the multicast address and secure voice capability for this call to all required RF resources and the MCC 7500 Dispatch Console.
6. Voice processing and encryption take place:

If…	Then…
If you have an MCC 7500 Dispatch Console with VPM,	the following events take place: **a** Voice from the operator is digitized at the VPM and sourced to the multicast address allocated to the call. **b** The VPM encodes the audio with the encryption key configured for that specific talkgroup.

C.1.2
Making a Secure Call From a Console Operator to a Radio User

This section describes the events that take place when a console operator makes a secure call to an individual radio user.

Prerequisites: For a console operator to make a secure call to a radio user, the radio user's radio must be capable of making secure calls.

Process:

1. The console operator selects a radio user Radio ID and presses the transmit switch.

   NOTICE: Consoles have several buttons or switches that the operator can use to initiate a call. These are generically called “transmit switches” in Motorola documents.

2. The console equipment generates a request for service.
3. The request is routed to the zone controller.
4. The zone controller locates the appropriate resources and identifies the encryption mode capability for the requested secure radio user.
5. The zone controller sends the secure radio user address and secure voice capability for this call to all required RF resources and the MCC 7500 Dispatch Console.
6. Voice processing and encryption take place:

If…	Then…
If you have an MCC 7500 Dispatch Console with VPM,	the following events take place: **a** Voice from the operator is digitized at the VPM and sourced to the multicast address allocated to the call. **b** The VPM encodes the audio with the encryption key configured for that specific talkgroup.

C.2
Radio User-Initiated Secure Calls

This section describes various types of radio user-initiated secure calls. These types include:

- Secure calls to a console operator
- Secure calls to a talkgroup
- Secure calls to another radio user

C.2.1
Making a Secure Call From a Radio User to a Console Operator

This section describes the events that take place when a radio user initiates a secure call and the call includes a console. Console operators can participate in secure communications through the decoding and encoding services provided by the MCC 7500 Dispatch Console. When a radio transmits in secure mode, and the audio must be routed to the console, the MCC 7500 dispatch console selects the appropriate encryption key, based on the talkgroup ID, decrypts the audio, and routes the decrypted audio to the console.

Prerequisites: To make a secure private call to the console operator, the radio user's radio must be capable of making secure calls.

Process:

1. The radio user selects the console's Radio ID.
2. The radio user presses the push-to-talk (PTT) button, which sends the request for a secure call to the zone controller.
3. The zone controller locates the appropriate resources and identifies the encryption mode capability for the requested secure radio user.
4. The zone controller sends the multicast address and secure voice capability for this call to all required RF resources and the MCC 7500 Dispatch Console.
5. The user's radio:
   1. Receives the voice channel assignments over the Control Channel.
   2. Moves to the voice channel.
   3. Encrypts the radio user's audio with the appropriate key.
   4. Transmits the encrypted audio to the voice channel.
6. The RF station converts the encrypted ASTRO® 25 audio to IP packets and forwards the packets to the master site through the master site's site router and transport network. No decoding takes place at the RF station or the transport network.
7. The following events take place:

If…	Then…
If you have an MCC 7500 Dispatch Console with VPM,	the VPM retrieves the audio (IP packets) from the Ethernet switch and decodes the audio with the encryption key configured for that specific talkgroup.

8. The following events take place:

If…	Then…
If you have an MCC 7500 Dispatch Console with VPM,	the following events take place: **a** The VPM converts the digital audio to analog. **b** The clear analog audio is routed to one of the console speakers.

C.2.2
Making a Secure Call From a Radio User to a Talkgroup

This section describes the events which take place when a radio user initiates a secure call to a talkgroup.

Prerequisites: For a radio user to make a secure call to a talkgroup, the radio user's radio and the radios in the talkgroup must be capable of making secure calls.

Process:

1. The radio user selects a talkgroup.
2. The radio user presses the PTT button:
   1. The radio sends a call request on the Control Channel to the local RF site base station.
   2. The site base station site Control Channel:
      a Receives the call request.

b Encapsulates the Call Request message in a UDP/IP datagram with the destination IP address of the zone controller.

c Forwards it to the Ethernet LAN.

3 IP packet network routes the call request packet to the zone controller.

4 The zone controller checks an internal database to determine the location of all members in the requested talkgroup (such as RF sites and remote dispatch sites locations).

5 The zone controller assigns a multicast group address to the call and sends the assigned multicast group address in a call grant message. The address is sent to all the participating RF sites, remote dispatch resources, and the MCC 7500 Dispatch Console at the master site (if the console operator is a member of the talkgroup). If the Console Operator is **not** a member of the talkgroup, the secure console does not receive the Call Grant message.

6 Upon receiving the IP group Join message, the RF and dispatch site routers communicate with Rendezvous Point (RP) routers in the system to set up an IP multicast distribution tree.

7 The radio receives the voice channel assignments over the Control Channel, and moves to the voice channel.

3 The original radio user who began the call starts speaking:

1 The radio encrypts the radio user's audio with the appropriate key, and transmits the encrypted audio to the RF station.

2 The audio is received by the RF station and is placed in an IP datagram destined to the assigned IP multicast address (as assigned in the Call Grant). The IP multicast packet is placed on the Ethernet LAN.

3 The IP multicast audio stream is distributed to all the RF and dispatch sites through the Rendezvous Point router and IP multicast tree.

4 The other user radios in the talkgroup receive the encrypted audio, and use the key associated with the talkgroup ID to decrypt the audio.

C.2.3
Making a Secure Call Between Radio Users

This section describes the events which take place when a radio user initiates a secure call to another radio user.

Prerequisites: For a radio user to make a secure call to another user, both users must have radios capable of making secure calls.

Process:

1 The radio user selects the Radio ID for the other user.

2 The radio user presses the PTT button:

1 The radio sends a call request on the Control Channel to the local RF site base station.

2 The site base station site Control Channel:

a Receives the call request.

b Encapsulates the Call Request message in a UDP/IP datagram with the destination IP address of the zone controller.

c Forwards it to the Ethernet LAN.

3 The IP Packet network routes the call request packet to the zone controller.

4 The zone controller checks an internal database to determine the location of the other user (such as the RF site and remote dispatch site locations).

5. The zone controller assigns a multicast group address to the call and sends the assigned multicast group address in a Call Grant message to the participating RF sites and the remote dispatch resources.
6. Upon receiving the IP group Join message, the RF and dispatch site routers communicate with RP routers in the system to set up an IP multicast distribution tree.
7. The radio receives the voice channel assignments over the Control Channel, and moves to the voice channel.

3. The original radio user who began the call starts speaking:
   1. The radio encrypts the radio user's audio with the appropriate key and transmits the encrypted audio to the RF station.
   2. The audio is received by the RF station and is placed in an IP datagram destined to the assigned IP multicast address as assigned in the call grant. The IP multicast packet is placed on the Ethernet LAN.
   3. The IP multicast audio stream is distributed to the RF and dispatch sites through the Rendezvous Point (RP) router and IP multicast tree.
4. The other user's radio receives the encrypted audio, and uses the key associated with the ID to decrypt the audio.

C.3 Telephone Interconnect Calls

The Telephone Media Gateway (TMG) is a device that translates audio between the ASTRO® 25 AMBE audio and IP PBX G.711 audio. The TMG supports both encrypted and clear audio to and from the ASTRO® 25 network. All audio exchanged with the IP PBX is clear. If encryption is required, sending encryption keys from the Key Management Facility (KMF) to the TMG consoles can be accomplished either by using the Key Variable Loader (KVL) or by sending keys through the network with Over-the-Ethernet Keying (OTEK). A single TMG supports up to 15 calls. For more information, see the *Enhanced Telephone Interconnect* manual.

C.3.1 Making an Interconnect Call

This section describes the events that take place when a radio user initiates an interconnect (telephone) call on a secure-voice-enabled radio.

Process:

1. The radio user selects telephone interconnect mode on the radio, enters the number to be called, and presses the PTT button on the radio.
2. The radio sends a telephone interconnect call request over the Control Channel with the dialed digits information.
3. The system:
   1. Verifies that the radio is authorized for telephone interconnect service.
   2. Determines the zone PBX for the call to use. The location of the PBX determines:
      - The controlling zone for the call
      - The point where the multicast addresses originate
      - The location of the Rendezvous Point (RP) for the call
4. The system assigns radio system resources to the call. The resources include:
   - The site where the radio is located

- A TMG router for distribution to the network

5 The zone controller sends two multicast addresses, one for the receive side of the call and one for the transmit side. Transmission of the multicast addresses sets up the audio RP.

6 The TMG and sites send a join message to the RP for the assigned multicast addresses.

7 The system checks the telephone number dialed to verify that the number represents a valid telephone number. The system also verifies that dialing restrictions allow the radio to initiate calls to the dialed telephone number.

8 A PBX-to-public switched telephone network (PSTN) resource is selected for the call.

9 The PBX initiates the call to the PSTN.

10 Radio system resources are granted for the call.

11 The radio switches to the voice channel.

12 The caller hears a ringing tone to indicate that the call is being placed.

IMPORTANT: Traffic between the radio user and the TMG is encrypted. However, once the voice signal from the radio user reaches the TMG, it is decrypted and sent to the PBX. Traffic between the PBX and the telephone user is **not** encrypted.

Appendix D

Acronyms

Table 25: Secure Communications-Related Acronyms

Item	Description
ACIM	ASTRO Console Interface Module
ADP	Advanced Digital Privacy
AES	Advanced Encryption Standard
AG	Agencygroup
AIS	Archiving Interface Server
ASN	Advanced SECURENET
CAD	Computer-Aided Dispatch
CAI	Common Air Interface
CDEM	CAI Data Encryption Module
CEN	Customer Enterprise Network
CID	Connection ID
CKEK	Common Key Encryption Key
CKR	Common Key Reference
CPS	Customer Programming Software
DES-OFB	Data Encryption Standard - Output Feedback Mode
DES-XL	Data Encryption Standard - synchronous mode
DIU	Digital Interface Unit
DVI-XL	Digital Voice International - synchronous mode
DVP-XL	Digital Voice Protection - synchronous mode
EID	Encrypted Integrated Data
EMC	Encryption Module Controller
FIPS	Federal Information Processing Standard
FRE	Field Replaceable Entity
FRU	Field Replaceable Unit
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPS	Global Positioning System
IP	Internet Protocol
IV&D	Integrated Voice and Data
JVM	Java Virtual Machine

Table continued…

Item	Description
KEK	Key Encryption Key
KID	Key ID
KLK	Key Loss Key
KMF	Key Management Facility
KMM	Key Management Message
KPK	Key Protection Key
KVL	Key Variable Loader
LED	Light Emitting Diode
MACE	Motorola Advanced Crypto Engine
MG	Multigroup
MO	Momentary Override
MOSCAD	Motorola Supervisory Control And Data Acquisition
MSEL	MultiSelect
NIB	Network Interface Barrier
NM	Network Manager
OTAR	Over The Air Rekeying
OTEK	Over The Ethernet Keying
PDEG	A packet data encryption device in the CEN.
PDG	Packet Data Gateway
PDR	Packet Data Router
PID	Physical Identifier
PM	Provisioning Manager
POP25	Programming over P25
RNC	Radio Network Controller
RNG	Radio Network Gateway
RNI	Radio Network Infrastructure
ROP	Retry Opportunities
RSI	Radio Set Identifier
SU	Subscriber
TEK	Traffic Encryption Key
TG	Talkgroup
TMG	Telephone Media Gateway
UCM	Universal Crypto Module
UKEK	Unique Key Encryption Key
VPM	Voice Processing Module
WNG	Wireless Network Gateway