System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Encrypted Integrated Data Feature Guide

NOVEMBER 2016

MN003266A01-A

Copyrights

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

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

Furthermore, the purchase of Motorola 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, 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 contact for further information.

Trademarks

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

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

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

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

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

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

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

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

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

North America Parts Organization

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

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

This page intentionally left blank.

Document History

Version	Description	Date
MN003266A01-A	Original release of the *Encrypted Integrated Data Feature Guide* manual	November 2016

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Encrypted Integrated Data Feature Guide

The Encrypted Integrated Data (EID) feature provides data encryption services to ASTRO® 25 Trunked Integrated Voice and Data (IV&D) IP bearer services (including Classic Data and Enhanced Data) between the Customer Enterprise Network (CEN) and subscriber radios. The data transmitted in the system is encrypted, whether the data is sourced by a mobile application within the subscriber radio or an application external to the subscriber radio. For more information on Classic Data and Enhanced Data, see the *Trunked Data Services* manual.

The PDEG Encryption Unit for trunked systems should not be confused with the CAI Data Encryption Module (CDEM), which is used for ASTRO® 25 Conventional IV&D systems. If you do not have a trunked system, for more information, see the *CAI Data Encryption Module* and *Conventional Data Services* manuals.

What Is Covered In This Manual?

This manual is organized into the following chapters:

- Encrypted Integrated Data Description on page 25 provides a high-level description of the Encrypted Integrated Data feature and the function it serves on your system.
- Encrypted Integrated Data Theory of Operation on page 37 explains how the Encrypted Integrated Data feature works in the context of your system.
- Encrypted Integrated Data Installation and Configuration on page 45 details hardware and software installation process, as well as the initial configuration required for connectivity to the network for the Encrypted Integrated Data feature. See the related PDEG Encryption Unit, KVL, or KMF hardware manuals for installation and configuration procedures.
- Encrypted Integrated Data Optimization on page 57 is for optimization procedures and recommended settings relating to the Encrypted Integrated Data feature. Currently, there are no optimization procedures necessary for the EID feature.
- Encrypted Integrated Data Operation on page 59 is for tasks that are performed once the Encrypted Integrated Data feature is operational on your system.
- Encrypted Integrated Data Maintenance on page 61 describes maintenance instruction for the Encrypted Integrated Data feature.
- Encrypted Integrated Data Troubleshooting on page 63 provides fault management and troubleshooting information relating to the Encrypted Integrated Data feature.
- Encrypted Integrated Data FRU/FRE on page 67 describes Field Replaceable Units (FRU) and Field Replaceable Entities (FRE) relating to the Encrypted Integrated Data feature.
- Encrypted Integrated Data Feature Expansion/Upgrades on page 69 describes how to add the EID feature to an existing system and the impacts to the system during the expansion.
- Encrypted Integrated Data Disaster Recovery on page 77 describes the recovery process for EID functionality, which consists of the same installation and configuration steps as an expansion.

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

See the following documents for associated information about the radio system.

Related Information	Purpose
System Overview and Documentation	Describes the manuals that comprise the ASTRO® 25 IV&D system documentation set, a list of new features for this release, system diagrams, and system-level disaster recovery information.
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.
Trunked Data Services	Describes the implementation and use of data services on ASTRO® 25 systems, specific to the Classic Data (IV&D) and Enhanced Data functionalities, and the High Availability for Trunked IV&D and HPD feature.
Conventional Data Services	Provides descriptive and procedural content relating to the ASTRO® 25 conventional data feature. The manual describes the feature and the role of the components supporting the feature, and explains how conventional data call processing is implemented and how data messages are processed. Additional information provided includes procedures for installation, configuration, operation, and troubleshooting.
CAI Data Encryption Module	Provides descriptive and procedural information about the CAI Data Encryption Module (CDEM). Included in this manual is the description of the CDEM and its location in the ASTRO® 25 Conventional with Integrated Data feature architecture. In addition, procedures are provided for installation, configuration, operation, maintenance, troubleshooting, FRU/FRE replacement, and disaster recovery.
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.
KMF CryptR	Provides information required to install, configure, and operate the CryptR 2 unit connected to the host computer for the Key Management Facility (KMF) application.
KVL 3000 Plus Key Variable Loader User's Guide (6881132E29)	Provides information about the KVL 3000 Plus Key Variable Loader equipment.

Table continued…

Related Information	Purpose
KVL 4000 Key Variable Loader ASTRO 25 User Guide	This manual 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.
System Routers – S6000/ S2500	Provides information relating to the installation, configuration, and management of the S6000 and S2500 routers as used in various network locations.
System Gateways – GGM 8000	Provides information relating to the installation, configuration, and management of the GGM 8000 gateway as used in various network locations.
Motorola GGM 8000 Hardware User Guide *Motorola Network Router (MNR) S2500 Hardware User Guide* *Motorola Network Router (MNR) S6000 Hardware User Guide*	These manuals are available on Motorola Online: https://businessonline.motorolasolutions.com To access the manuals, select **Resource Center** → **Product Information** → **Manuals** → **Network Infrastructure** → **Routers and Gateways**.

This page intentionally left blank.

Chapter 1

Encrypted Integrated Data Description

This chapter provides a high-level description of the Encrypted Integrated Data feature and the function it serves on your system.

1.1 What is Encrypted Integrated Data?

The Encrypted Integrated Data (EID) feature provides encryption from wireless data modems, which are the ASTRO® 25 Trunked Integrated Voice and Data subscriber, to a point inside the customer's network for data applications, such as the following:

- Global Positioning System (GPS) receivers
- ASTRO® 25 Advanced Messaging Solution
- POP25
- Outdoor Location/Unified Network Services (UNS)
- Computer-Aided Dispatch (CAD)

The EID feature provides data encryption services to ASTRO® 25 Trunked Integrated Voice and Data (IV&D) IP bearer services (including Classic Data and Enhanced Data) between the Customer Enterprise Network (CEN) and subscriber radios. This encryption service provides data encryption, decryption, and authentication between each EID-enabled subscriber radio and a new device in the CEN called a PDEG Encryption Unit by using a customized implementation of Internet Protocol Security (IPsec) suitable for narrowband radio networks. IPsec defines encryption, authentication, and key management routines for ensuring the privacy, integrity, and authenticity of data in the system. The EID implementation of IPsec is tunnel mode, but does not utilize Internet Key Exchange (IKE) for establishing the IPsec parameters. The encryption algorithm used is Advanced Encryption Standard (AES), which is also used for Project 25 voice encryption. The subscriber radio and PDEG Encryption Unit data encryption keys can be centrally managed using a Key Management Facility (KMF) server and client in the CEN.

Using the EID feature, you can secure data sent using ASTRO® 25 IP bearer service between the CEN and subscriber radio, including data sent between CEN applications and subscriber radio internal or external applications. Data remains encrypted between the IPsec tunnel endpoint within the subscriber radio and the IPsec tunnel endpoint within the PDEG Encryption Unit located in the CEN.

The PDEG Encryption Unit for trunked systems should not be confused with the CAI Data Encryption Module (CDEM), which is used for ASTRO® 25 Conventional IV&D systems. The CDEM 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. See the *CAI Data Encryption Module* and *Conventional Data Services* manuals for information if you do not have a trunked system.

1.1.1 EID Benefits

ASTRO® 25 Trunked Integrated Voice and Data systems with the Encrypted Integrated Data feature have the following benefits:

- Capability to encrypt the data that is sent or received by devices that are not capable of supporting a Virtual Private Network (VPN).

- Compliance with laws, and requirements that rely on over-the-air confidentiality of data, such as Health Insurance Privacy and Portability Act (HIPPA) laws, Criminal Justice Information Sharing (CJIS) requirements, and National Crime Information Center (NCIC) requirements.
- Minimal changes to a subscriber already equipped for voice encryption.
- Ability to designate which system traffic is encrypted and which traffic is not.

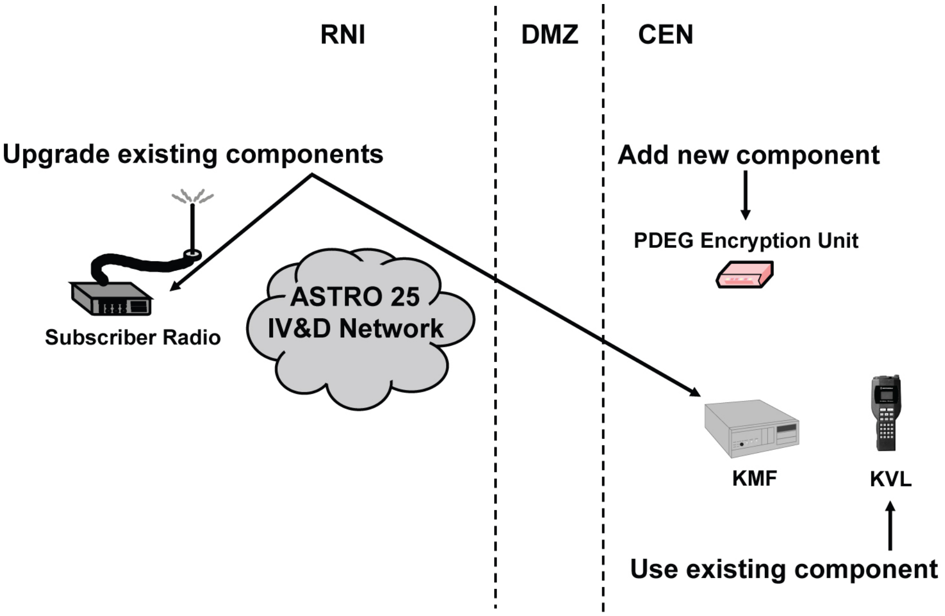
1.2 Physical Description

Encrypted Integrated Data (EID) relies on the following system components:

- PDEG Encryption Unit
- Subscriber radio
- Key Management Facility (for centralized key management)
- Key Variable Loader (for manual key management)

Figure 1: Encrypted Integrated Data System Components

The following figure shows where these components reside in the ASTRO® 25 radio system and the CEN.



EID_system_impact_A

IMPORTANT: The EID service cannot be used to encrypt Broadcast Data or High Performance Data (HPD).

1.2.1 PDEG Encryption Unit Description

The PDEG Encryption Unit is a standalone hardware platform with an embedded operating system. The PDEG Encryption Unit provides an IPsec tunnel endpoint for EID communications with subscriber radios. The PDEG Encryption Unit provides security, encryption/decryption, and authentication.

The EID feature involves adding one or more PDEG Encryption Units in the Customer Enterprise Network (CEN). The PDEG Encryption Unit provides two network interfaces and when deployed effectively splits the CEN into two subnets.

Redundancy is optional. A pair of PDEG Encryption Units can be configured for automatic switchover using Virtual Redundant Router Protocol (VRRP), described in the *PDEG Encryption Unit* manual. The two devices are independently manageable by KMF and KVL. However, they appear to be the same PDEG Encryption Unit to mobile endpoints and to the red CEN application servers.

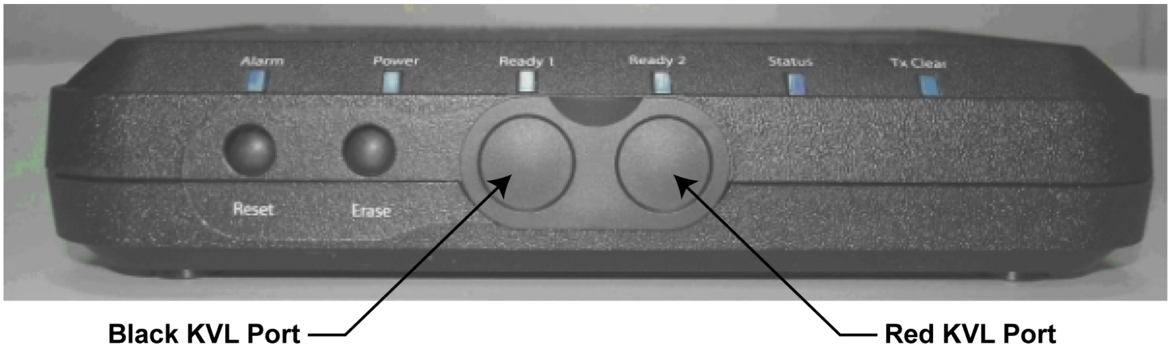
Figure 2: PDEG Encryption Unit Front View

The following figure shows the front panel of the PDEG Encryption Unit. The front panel is equipped with the following elements:

- Reset button
- Erase button
- Two Key Variable Loader (KVL) ports (with protective covers)
- Alarm LED
- Power LED
- Ready1 LED
- Ready2 LED
- Tx Clear LED
- Status LED

IMPORTANT: Keep the protective covers in place when the KVL ports are not in use.

For more information on the LED status, see Table 3: PDEG Encryption Unit LED Status on page 63.

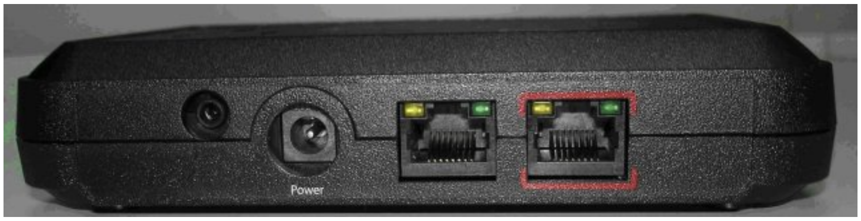


ph_CryptR_FrontView1

Figure 3: PDEG Encryption Unit Rear View

The following figure shows the rear panel of the PDEG Encryption Unit. The rear panel is equipped with the following:

- Mini jack
- Power jack
- Two RJ-45 ports (red and black)



The PDEG Encryption Unit configuration is performed with Microsoft Windows HyperTerminal or equivalent terminal emulation program. The encryption key provisioning and key loading is performed with a Motorola Key Variable Loader.

This hardware is used for multiple Motorola platforms and is also branded as CryptR. When used within the ASTRO® 25 system, the device is referred to as a PDEG Encryption Unit. The hardware can be mounted on a desktop or a rack based on the customer's preference.

Each PDEG Encryption Unit can provide EID services for up to 64,000 subscriber radios. However, each subscriber radio can provide EID services with only one PDEG Encryption Unit at a time.

If your system has more than 64,000 encrypted data capable subscriber units, the system must use two KMFs and two PDEGs.

1.2.2 Subscriber Radio Description

An ASTRO® 25 subscriber radio provides an IPsec tunnel endpoint for EID communications with a PDEG Encryption Unit. Subscriber radios that support the EID feature include all models of ASTRO® 25 APX (with a MACE) and XTL and XTS (with a UCM) radios and a compatible software version.

Each subscriber radio can provide EID services with only one PDEG Encryption Unit at a time. However, each subscriber radio can be configured with up to six PDEG Encryption Unit IP addresses that can be used with different trunking system personalities.

Subscriber radios must have the Q947/W947 Packet Data option and be operating in a trunking mode to use the EID feature.

1.2.3 Key Management Facility

The encryption keys within the PDEG Encryption Unit can be centrally managed using the Key Management Facility (KMF) client and server. The following figure shows the KMF client that may reside in the CEN. The KMF hardware is not required for EID functionality. However, if existing KMF hardware is used, the software must be upgraded.

Figure 4: Example of a KMF Client

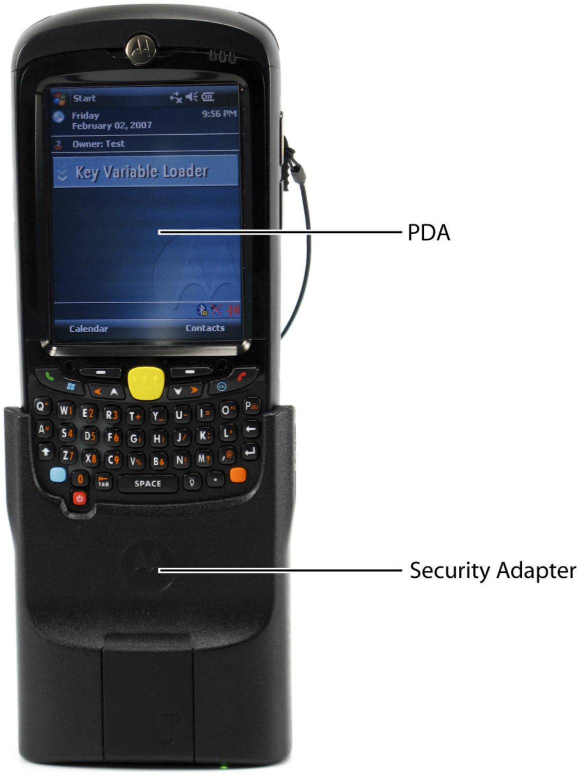
KMF_client_front

1.2.4 Key Variable Loader Description

The Motorola Key Variable Loader (KVL) is a handheld device that allows encryption key management and configuration for the PDEG Encryption Unit and subscriber radios, and can install software updates into the PDEG Encryption Unit (the device ships with necessary hardware installed). There are several models of Motorola KVL hardware available. The following figure shows one example.

For software updates, the KVL requires a PDEG Encryption Unit software installation flash card and PDEG Encryption Unit connection cable to support the EID feature. See the *PDEG Encryption Unit* manual for the necessary cables to use with the KVL device.

Figure 5: Example of a Key Variable Loader



1.2.5 Customer Programming Software and Software Flashing

Motorola Customer Programming Software (CPS) is a proprietary application used to configure subscriber radios to operate on an ASTRO® 25 system. CPS is a Windows-based application.

PDEG Encryption Unit software installation requires a Motorola Key Variable Loader (KVL) with the PDEG Encryption Unit software installation flash card and PDEG Encryption Unit connection cable. Each PDEG Encryption Unit has two MACEs that require two independent updates, so you must use two PCMCIA cards. With one KVL, you must update all of the red subnets before switching cards and then update all of the black subnets to load the software. Alternatively, you can use two KVLs to load the necessary software to both subnets on a device. Whereas, subscriber radio software installation requires a PC with the Motorola FLASHport software tool and subscriber radio connection cable.

1.2.6 FLASHport Upgrade

Model DeFinition (MDF) bits in the codeplug are used by the CPS to determine the features that are available to customers. The features are made available to users through various constraints set in the CPS Graphical User Interface (GUI). The MDF file is used by the CPS FLASHport upgrade feature to know how to update the software in a radio. A FLASHport upgrade is a CPS mechanism that uses a PCMCIA card to deliver radio software features, such as EID, when the radio is in the field. Basically, when performing a FLASHport upgrade, you are updating the fielded radio's codeplug capability and adding data blocks needed with the resulting capability level.

To perform a FLASHport update, the following hardware is needed:

- A FLASHkey: A small piece of hardware equipment, which looks like an RS232 gender changer, connected between the radio and the PC during FLASHport operation. This device houses information regarding various specifics of the upgrade.

- Radio programming cable.
- Smart RIB (Radio Interface Box): Storage for radio bootcode and host firmware.
- Personal Computer: To install CPS and load files for the software update.
- Software: CVN (software reference that is not an acronym), Universal Crypto Module (UCM), and MDF files.

For the actual authentication and update procedures using FLASHport with the KVL, see the FLASHport User's Guide for your subscriber radio model.

1.2.7
PCMCIA Card Authentication

Before using the PCMCIA card for the first time, you must have the card authenticated by the Motorola Solution Support Center (SSC). After a card has been authenticated, you may use the card to perform the upgrade procedure for as many upgrades as the card has been programmed to perform (determined at time of purchase).

Some important things to know about PCMCIA authentication are:

- Each PCMCIA card requires authentication only one time.
- Once a PCMCIA card has been authenticated for use with a particular KVL, the card may be used only with that particular KVL.
- Once a PCMCIA card has been authenticated for use with a particular KVL, the card must be used to completion (that is, all updates performed) before inserting and authenticating another card. For example, suppose that you insert and authenticate Card A (contains upgrades for ten APX radios). You perform six updates, and then remove the card and insert Card B. As soon as you authenticate Card B, Card A may not be reinserted to perform the remaining four updates. Card A is effectively “dead” and may not be used again.
- A particular KVL can accept one (and only one) authenticated PCMCIA card for each supported product (fox example, DIU, ASTRO® 25 system radio, APX radio, and KMF). For example, a KVL can support one authenticated DIU PCMCIA card, one authenticated ASTRO® 25 system radio PCMCIA card, one authenticated APX radio PCMCIA card, and one authenticated KMF PCMCIA card, but it cannot support two different authenticated APX radio PCMCIA cards.

1.3
EID Terminology

The Encrypted Integrated Data (EID) feature references the terms listed in the following table.

Table 1: EID Terminology

Term	Description
AES	Advanced Encryption Standard. A United States government encryption/decryption standard. Defined in Federal Information Processing Standard 197 (FIPS-197).
Black subnet	The untrusted network interface where data is encrypted when passing through. The trusted interface is the red subnet. PDEG Encryption Units and subscriber radios share this concept of red and black subnets. In the CEN, the black subnet is on the border gateway side of the PDEG Encryption Unit.
CEN	Customer Enterprise Network. The telecommunication network belonging to a customer that is connected to an ASTRO® 25 system.

Table continued…

Term	Description
	For the EID feature, the PDEG Encryption Unit must be installed with the customer's network equipment where data is encrypted/decrypted.
CPS	Customer Programming Software. The application used to update software in the subscriber radios.
CKR	Common Key Reference. A number used for all secure calls in the radio system. This setting should correspond with CKR settings in the Key Management Facility (KMF). Subscribers must also be provisioned with this CKR.
DMZ	DeMilitarized Zone. A neutral area between the CEN and the radio network infrastructure.
EID	Encrypted Integrated Data. Provides encryption from wireless data modems (ASTRO® 25 IV&D subscriber radios) to a point inside the customer's network for data applications.
ESP	Encapsulating Security Payload protocol.
FIPS 140	Federal Information Processing Standard. This Federal processing standard assures that cryptographic modules are effectively designed to meet specific security objectives.
HPD	High Performance Data. A system that provides an efficient and reliable wireless transport medium for standard IP packet transfer, with raw data rates up to 96 Kbps. This data rate allows service for medium bandwidth applications, such as still image transfers, vehicle location services, and constrained web browsing services. An HPD system may be colocated with an existing IV&D system or as a standalone system.
IPsec	Internet Protocol security. A combination of key and algorithm combinations through SPI. IPsec tunnel mode, but does not utilize Internet Key Exchange (IKE) for establishing the IPsec parameters.
KEK	Key Encryption Key. A Unique Key Encryption Key (UKEK) assigned to a subscriber for encrypting keys within an OTAR or OTEK command sent only to the specific subscriber. Each radio has its own UKEK.
KMF	Key Management Facility. A server and workstation used to manage the encryption keys in an ASTRO® 25 system. KMF provides a central point at which keys may be managed. It can use OTAR and OTEK to transfer key management information to the secure equipment, including subscriber radios and PDEG Encryption Units. Up to 50 PDEG Encryption Units (redundant pairs count as 2) can be centrally managed by KMF.
KMM	Key Management Messages. A series of commands and responses between a Key Management Facility (KMF) and secure devices, such as subscribers. The commands and responses carry out the key management and secure configuration of the devices.
KVL	Key Variable Loader. A hand-held device used to load or erase keys, view, or modify secure configuration parameters of secure devices, and substitute for over-the-air transport of OTAR and OTEK transfer methods between the Key Management Facility (KMF) and devices.

Table continued…

Term	Description
NAT	Network Address Translation. A functional process used to coordinate the radio network infrastructure IP plan with IP plans used outside the Radio Network Infrastructure (RNI).
OTAR	Over the Air Rekeying. Rekeys subscribers at their current physical location by using over-the-air commands without connecting the subscriber radio directly to the Key Variable Loader (KVL) for rekeying.
OTEK	Over the Ethernet Keying. Provides key management for devices such as consoles and PDEG Encryption Units using the Key Management Facility (KMF), which is installed on a Customer Enterprise Network (CEN).
PDEG Encryption Unit	A packet data encryption device used in the CEN for encryption in Trunked IV&D ASTRO® 25 radio systems.
Red subnet	The trusted network interface where sensitive data is unencrypted. The untrusted network interface is the *black subnet*. PDEG Encryption Units and subscriber radios share this concept of red and black subnets. In the CEN, the red subnet is on the side of the PDEG Encryption Unit where application hosts reside that use the EID feature.
RNI	Radio Network Infrastructure. The ASTRO® 25 radio system equipment that processes voice and data. For the purposes of EID, the system is divided into the RNI, DMZ, and CEN.
RSI	Radio Set Identifier. Each radio needs a unique RSI assigned to it in order for KMF key management messages to be directed to the proper secure endpoint (for example, console or subscriber radio).
SPI	Security Parameter Index. Used within IPSec for EID encryption services.
TCP/IP	Transmission Control Protocol/Internet Protocol. A complex suite of protocols that includes IP, TCP, and the associated application protocols for exchanging data over a network.
TEK	Traffic Encryption Key.
Trusted network	In the context of the EID feature, the CEN red subnet (the subnet where application hosts will reside that uses the EID feature).
UDP	User Datagram Protocol. Part of the Internet Protocol suite.
UKEK	Unique Key Encryption Key. Also, see KEK.
Untrusted network	In the context of the EID feature, the black subnet which is the existing ASTRO® 25 radio system.
VRRP	Virtual Router Redundancy Protocol. Used between PDEG Encryption Units in the CEN if there is a redundant pair (optional configuration).

1.4

EID Features

This section provides the specifications, limitations, and Dynamic System Resilience (DSR) impact associated with the Encrypted Integrated Data (EID) feature.

1.4.1 EID Specifications

This table provides details on the system specifications that support the Encrypted Integrated Data (EID) feature.

Table 2: Encrypted Integrated Data Specifications

Specification	Description
Supported configurations	Any ASTRO® 25 IV&D trunking system that supports EID-compatible subscriber radios, that is ASTRO® 25 APX (with a MACE) and XTL and XTS (with a UCM) radios with a compatible software version.
Connectivity	IPv4
Data encryption	Advanced Encryption Standard (AES) 256–bit. FIPS 197.
Authentication	IPsec – provides AES encryption, decryption, and authentication of packet data between each EID-enabled subscriber radio and a PDEG Encryption Unit in the CEN.
Protocol	Encapsulating Security (ESP) – Used between PDEG Encryption Unit and subscriber radio.
Protocol	Virtual Router Redundancy (VRRP) – Used between a redundant pair of PDEG Encryption Units within the CEN.
Redundancy	Optional configuration of the PDEG Encryption Unit in the CEN. The two devices are independently manageable by KMF and KVL. Automatic switchover between devices is accomplished through VRRP. The two devices appear to be the same PDEG Encryption Unit to mobile endpoints and CEN hosts.
Data key changeover	Auto-Key Receive on data keys is seamless using the Auto CKR receive feature.
Endpoint capacity	• 64,000 subscribers supported • 50 fixed endpoints (PDEG Encryption Units) supported
Application capacity	16 CEN application interfaces supported per PDEG Encryption Unit.
Data capacity	520 Kbps fixed endpoint (PDEG Encryption Unit) capacity.
Data association rules	PDEG Encryption Unit - 32 data associations (16 inbound and 16 outbound rules) Subscriber radios - 40 bypass data associations
Key management capacity	• KMF can manage the data encryption key material for 50 PDEG Encryption Units (redundant pair of PDEG Encryption Units count as 2) and 64,000 subscriber radios (a subscriber radio that is centrally key managed for both voice and data keys counts as 1 managed device). • A KVL can provide centralized key management support of up to 10 PDEG Encryption Units with a profile of 100 data keys. • A KVL can provide centralized store and forward key management support of up to 75 subscriber radios at a time with a profile of 8 voice keys and 2 data keys.

Table continued…

Specification	Description
	• A PDEG Encryption Unit can store 50 CKRs with 2 keysets per CKR (active and inactive). • A subscriber radio can store up to 48 CKRs with 2 keysets per CKR (active and inactive). Subscriber radio CKRs can be used for voice or data encryption.
PDEG Encryption Units required	The number of PDEG Encryption Units required is determined by customer needs. Your Motorola Field Services representative can provide a recommendation based on data traffic. However, only one PDEG Encryption Unit is necessary to implement EID on a single ASTRO® 25 IV&D system and a subscriber radio can only communicate with one PDEG Encryption Unit per user-selected trunking system personality.

1.4.2

EID Feature Limitations

Since the Encrypted Integrated Data services are not applicable to ASTRO® 25 systems using the Broadcast Data or High Performance Data (HPD) features, bypass rules must be in place to allow delivery service.

With the Broadcast Data feature, if broadcast messaging is used from a CEN red subnet application to subscriber radios, you need to set up bypass rules in the PDEG Encryption Unit for these messages. Subscriber radios must either have bypass rules configured for these messages or enable the “allow all clear data” option. If broadcast messaging is used from a CEN black subnet application to subscriber radios, only subscriber radios must be configured to allow these messages to bypass EID since they do not need to pass through a PDEG Encryption Unit.

EID services cannot be applied to messages addressed to a Network Address Translation (NAT) address of a subscriber radio. The EID feature encapsulates customer application messages sent to a subscriber radio within an IPsec message. If the destination IP address of the encapsulated message is a NAT address, the decrypted application message contains the NATed IP address and is discarded by the subscriber radio.

Lastly, Internet Control Message Protocol (ICMP) responses generated by the ASTRO® 25 infrastructure to outbound (CEN to subscriber radio) encrypted datagrams are not passed back to the sending application in the CEN red subnet. Rules can be added to a PDEG Encryption Unit to allow ICMP message responses to clear outbound datagrams from the ASTRO® 25 infrastructure, if desired.

1.4.3

EID and Dynamic System Resilience

If the Dynamic System Resiliency (DSR) feature is present with the EID feature, the PDEG Encryption Unit data association rules must account for fleets of subscriber radios that change IP addresses following a failover. See your Motorola System Planner for other implications.

This page intentionally left blank.

Chapter 2

Encrypted Integrated Data Theory of Operation

This chapter explains how the Encrypted Integrated Data feature works in the context of your system.

2.1

Encrypted Integrated Data in an ASTRO 25 Trunked IV&D System

The EID feature involves adding one or more PDEG Encryption Units (redundancy is optional) in the Customer Enterprise Network (CEN). Generally, only one PDEG Encryption Unit (or redundant pair) is required per ASTRO® 25 system. The PDEG Encryption Unit provides two network interfaces and when deployed, effectively splits the CEN into two subnets: the red subnet and the black subnet. The red subnet is considered the trusted subnet and the black is the untrusted subnet of the CEN. Thus, data is encrypted when passing through the black subnet. The red and black network interfaces must be on different subnets. The PDEG Encryption Unit is therefore a multi-homed device in that it supports a unique IP address on its red subnet interface and another unique IP address on its black subnet interface for EID services. A separate unique IP address for each redundant PDEG Encryption Unit is also supported on either the black or red subnet interface (as configured) for key management services with a KMF.

Data encryption/decryption/authentication takes place within the PDEG Encryption Unit between the red and black subnets within the CEN. CEN application hosts that require EID services are located in the CEN red subnet. CEN application hosts that do not require EID services may be located in the CEN black or red subnet.

See EID Specifications on page 34 for the number of IPsec data association rules for processing specific data flows, including broadcast messages.

NOTICE: Creating separate red and black subnets for this feature may require changing the IP address of existing application hosts and other CEN facing network devices.

The subscriber radio shares a similar concept of red and black subnets since it is also the point where data encryption/decryption/authentication takes place, but the subscriber radio red subnet can include internal applications, as well as external applications. The subscriber radio serves as one IPsec endpoint and the PDEG Encryption Unit serves as the other endpoint.

Typically, only data that is not considered sensitive (because it is inherently not sensitive) or that is secure (because it is encrypted) should be allowed on the black subnet. This way, sensitive data is only in its unencrypted form when it is on the red subnet, but this is up to the customer's discretion.

2.2

Components of the EID Architecture

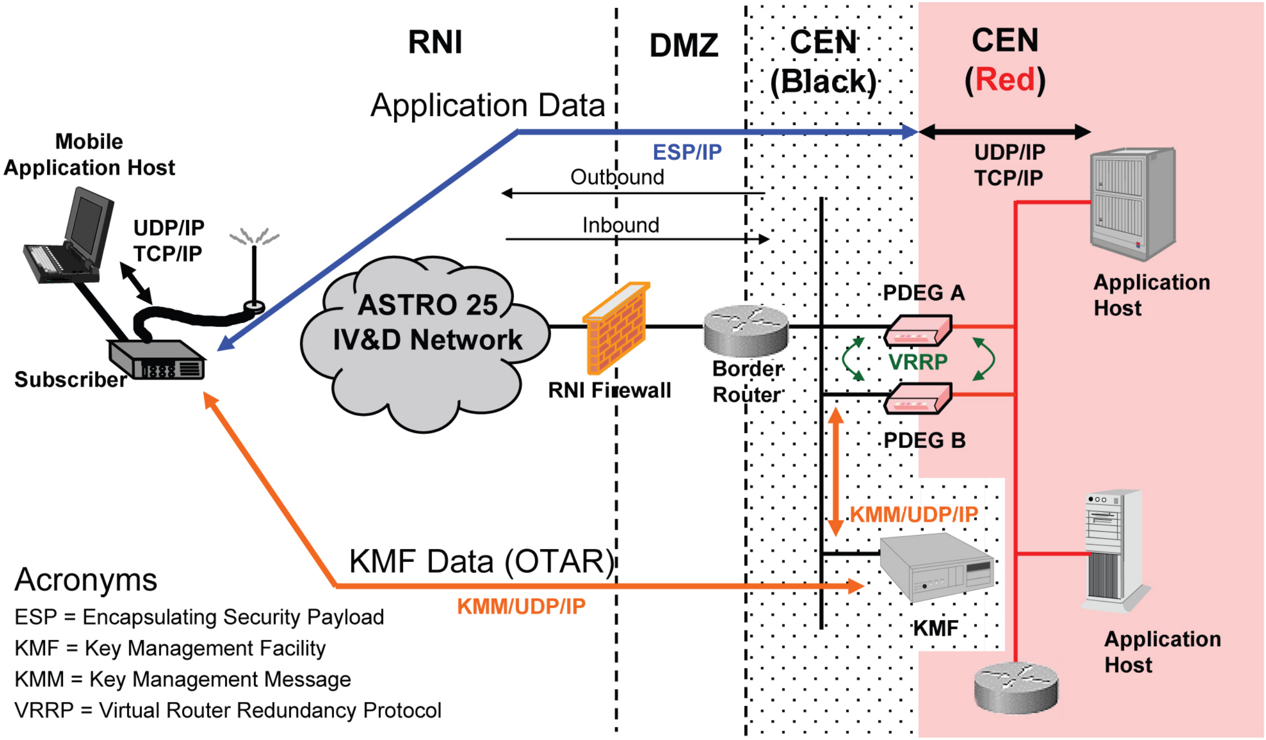
The following components comprise the Encrypted Integrated Data feature architecture:

- PDEG Encryption Unit
- KMF server and application (optional)
- Key Variable Loader (KVL)
- Subscriber radios

Figure 6: Encrypted Integrated Data System Architecture

The following figure illustrates the EID system architecture with these components between the Radio Network Infastructure (RNI) and the Customer Enterprise Network (CEN).

NOTICE: The border gateway provides a preferred alternative solution for the border router depicted in this illustration. See the *System Gateways – GGM 8000* manual.



EID_system_architecture

2.2.1 PDEG Encryption Unit

This encryption unit hardware is used in a CEN attached to an ASTRO® 25 radio system. This hardware:

- Provides an IPsec endpoint for EID communications with subscriber radios.
- Stores 50 Common Key references (CKRs) with two keysets per CKR (active and inactive).
- Supports EID services for up to 64,000 subscriber radios.

The throughput capacity of a single PDEG makes it possible to process the total data service capacity of a single IV&D zone (300,000 messages per hour of 512 bytes or less). Each PDEG can encrypt/decrypt data using encryption keys provided by the customer. When centrally managing PDEGs with KMF, the number of PDEGs that can be supported by a single KMF is 50. A redundant PDEG pair counts as two PDEGs for key management. The number of PDEGs required by a specific system implementation is determined by customer needs. However, only one PDEG is necessary to implement EID on a single ASTRO® 25 IV&D system and a subscriber radio can only communicate with one PDEG per user-selected trunking system personality. More than one PDEG may be used in the same CEN to provide EID services to different fleets of subscriber radios. Different fleets of radios must be provided with IP addresses from distinguishable IP subnets in order to effectively separate EID services between separate PDEGs in the same CEN.

Provisioning for the PDEG Encryption Unit relies on:

- Microsoft Windows HyperTerminal or equivalent for programming and configuration.
- Motorola Key Variable Loader for encryption key provisioning and key loading.

2.2.2 Key Management Facility Server and Application (Optional)

The KMF is comprised of a Windows-based server and a workstation used to manage the encryption keys in an ASTRO® 25 system. KMF provides a central point at which keys may be managed. It can use OTAR or OTEK to transfer key management information to the secure equipment.

A single KMF can manage the data encryption key material for 50 PDEG Encryption Units and 64,000 subscriber radios. If centralized key management is deployed, endpoint EID keys can be centrally managed using a KMF, using either a KVL and/or using Over-The-Air-Rekeying (OTAR) or Over-The-Ethernet-Keying (OTEK) as the transport mechanism. OTEK is used by the KMF for key management of the PDEG Encryption Unit over a CEN Ethernet connection, while key management of subscriber radios uses OTAR over a system radio channel.

For subscriber radios, KMF needs to know which Unique Key Encryption Key (UKEK) and Radio Set Identifier (RSI) a particular target unit has before communicating with the unit over the air. Manual provisioning is one method of ensuring that the KMF knows the correct information to reach the target unit. Using a defined set of OTAR or OTEK attributes, the KMF can determine if a target unit has been correctly configured for OTAR or OTEK messages. The OTAR or OTEK attributes used to determine this configuration are:

- UKEKs
- CKEKs
- Group RSI
- Individual RSI
- keyset alias or name
- TEKs for all CKRs
- Zeroize state

Since the KMF, subscriber radio, and PDEG provide separate encryption of OTAR messages, the EID feature is not required for OTAR data flows. Therefore, locating the KMF in the black subnet is recommended to avoid the need to bypass key management traffic through a PDEG and consuming a portion of its capacity. However, locating the KMF in the red subnet is also supported, but requires you to configure EID bypass rules in the PDEG for KMF traffic with subscriber radios and consoles.

2.2.3 Key Variable Loader

The KVL is a hand-held device used to load or erase keys, view or modify secure configuration parameters of secure devices, and can be used as a transport of key management messages (KMMs) between the Key Management Facility (KMF) and secure devices. A KVL can be used in lieu of a KMF to manage EID key material in an ASTRO® 25 system.

A KVL can provide centralized key management support of up to 10 PDEG Encryption Units with a profile of 100 data keys. KVL can provide centralized store and forward key management support of up to 75 subscriber radios at a time with a profile of eight voice keys and two data keys.

2.2.4 Subscriber Radios

In order to work with EID, subscriber radios must have an encryption module (option Q159) and IV&D Data capability (option Q947 or W947). The following subscriber radios models support the EID feature: ASTRO® 25 APX, XLT, and XTS radios with a compatible software version. Existing subscriber radios require a software update to support EID. The existing radios can be upgraded independently, which means upgraded and existing subscriber radios can co-exist in the same system.

An ASTRO® 25 system subscriber radio provides an IPsec endpoint for EID communications with a PDEG Encryption Unit. Each trunking system personality may communicate with the same or different PDEG Encryption Unit. The subscriber radio shares a similar concept of red and black subnets since it is also the point where data encryption/decryption/authentication takes place, but the subscriber radio red subnet can include internal applications, as well as external applications.

Within the subscriber radio is an encryption module. For the XTL/XTS model radios, the encryption module is called a Universal Crypto Module (UCM) and the APX model radios have a Motorola Advanced Crypto Engine (MACE). The encryption module provides secure key management, Over-the-Air-Rekeying (OTAR), and voice and data encryption for operation within the ASTRO® 25 system. The modules operate using security rules derived from the security requirements of FIPS 140-2 using the AES-256 algorithm for encryption, decryption, and authentication. The FIPS 140–2 level 3 allows for black keyloading, and is enabled by default.

If the existing subscriber radios have the Advanced Encryption Standard (AES) algorithm, you need to update the software version to support the EID feature. If the radios do not already have AES, you must purchase the AES algorithm and the Galois Counter Mode (GCM) options.

2.3 Planning Considerations for EID

Before implementing the EID feature, there are bandwidth planning considerations with both the radio channel and the PDEG Encryption Unit.

If there is an existing Key Management Facility (KMF) installed, you need to decide if you want the KMF to reside on the red or black subnet. Since KMF communications is already encrypted, it is recommended to locate the KMF in the black subnet in order to preserve PDEG Encryption Unit throughput capacity. If you use the red subnet, add bypass rules to the PDEG Encryption Unit to allow KMF traffic to pass through unencrypted.

If there are other mobile data applications already on the system, this impacts whether you retain the existing CEN subnet as the red subnet and change the black subnet address through the border gateway.

Plan to add bypass rules to the PDEG Encryption Unit to allow any red subnet non-subscriber traffic and any already encrypted traffic to pass through to/from the black subnet without processing.

Contact your Motorola Field Services representative for assistance with additional considerations specific to your system.

2.3.1 Bandwidth Planning

There are two types of bandwidth to consider when planning for the Encrypted Integrated Data feature.

- Radio channel bandwidth
- PDEG bandwidth

2.3.1.1 Radio Channel Bandwidth

The EID feature adds overhead to each IP datagram that it encrypts. This overhead is the result of encapsulating the IP datagram within Encapsulating Security Payload (ESP) protocol according to IPsec standards. ESP adds header and trailer information to each datagram following encryption. The current EID implementation adds approximately 60 bytes of ESP overhead. Unfragmented IP datagrams only have this much additional overhead. However, fragmented IP datagrams have additional overhead.

When a customer application sends an IP datagram that is more than 1442 bytes (including IP header), the overhead added by ESP results in the need to fragment the IP datagram in order to comply with the ASTRO® 25 IV&D system maximum transmission unit (MTU) size of 1500 bytes. This results in a 1500 byte IP datagram and the additional overhead of a second IP datagram consisting of approximately 60 bytes of ESP overhead plus the balance of the datagram that is above 1442 bytes. Fragmentation also results in two messages being sent over the air interface.

The subscriber radio also fragments inbound bypassed IP datagrams that are more than 1442 bytes when EID is enabled. The additional overhead is a second IP datagram consisting of only a 20 byte IP header and the balance of the user data that is more than 1442 bytes. The PDEG Encryption Unit does not fragment bypassed IP datagrams unless they are more than 1500 bytes.

As a result of EID encryption, adjust the customer data message profile to account for EID and fragmentation overhead when determining channel capacity and the number of channels required for the profile.

2.3.1.2 PDEG Encryption Unit Bandwidth

A single PDEG Encryption Unit supports 520 Kbps (combined inbound and outbound) encrypted data throughput with 500 byte IP datagrams from applications (including IP header). This is sufficient to support encryption of the maximum specified IP bearer service throughput of an ASTRO® 25 IV&D zone (300,000 messages per hour of 512 bytes or less, combined inbound and outbound). However, care should be taken to minimize the amount of data allowed to bypass EID through the PDEG Encryption Unit. Bypassed data through the PDEG Encryption Unit reduces the available throughput capacity of the PDEG Encryption Unit for encrypted data by an equivalent amount. Design clear data flows so that they originate from the black subnet and avoid passing through the PDEG Encryption Unit if possible. If PDEG Encryption Unit throughput capacity consumption by bypassed data is a concern, the ability to route this traffic around the PDEG Encryption Unit is recommended. If additional PDEG Encryption Unit capacity is required, deploy multiple PDEG Encryption Units to divide the load between different subscriber radio IP address subnets or different application data flows.

2.3.2 Preplanning Examples

This section provides recommendations based on the presence of mobile data applications within an existing ASTRO® 25 system.

2.3.2.1 Mobile Data Applications Already Online (excluding KMF)

If the customer has existing mobile data applications online, you should create a new black subnet address and keep the applications online with the same red subnet IP addresses of hosts in the red subnet during expansion. A temporary rule needs to be added to the PDEG Encryption Unit to pass all data from hosts through unencrypted to allow non-expanded subscribers to continue to function. At the same time, another temporary rule allows the PDEG Encryption Unit to process encrypted data from expanded subscribers and to pass through unprocessed unencrypted data from non-expanded subscribers. If you also want to keep the KMF online during EID configuration, the KMF must go in the red subnet to keep its IP address unchanged. A rule must be added to the PDEG Encryption Unit to pass this traffic through unprocessed. If not, the KMF IP address can be changed and the KMF can go in the black subnet and when a subscriber is expanded, the provisioned KMF address is changed to a new black subnet address.

2.3.2.2 No Mobile Data Applications Already Online (excluding KMF)

If there are no applications online for mobile data, you can create a new red subnet and set the application IP addresses to a red subnet address and the black subnet can remain unchanged from the current CEN pre-expansion subnet. In this case, if there is a KMF, it will reside in the black subnet with the same IP address and remain operational during EID configuration. However, your system may have existing application servers (such as a Computer Aided Dispatch system) that are online, but not for mobile data. In this case, you may not want to change the IP addresses of the application servers. Then, the black subnet is the new subnet and the red subnet is the current pre-expansion CEN subnet. In this case, if there is a KMF already online doing OTAR, you must decide if the KMF will reside in the black subnet and lose OTAR capability until a subscriber is expanded, or in the red subnet and keep OTAR functioning during EID configuration.

2.4 Call Processing with EID

This section describes messages sent through the PDEG Encryption Unit passing to and from the red subnet and the subscriber radio.

2.4.1 Routing from the Red Subnet to a Subscriber Radio

When a message is sent by an application host in the CEN red subnet to a subscriber radio, the CEN red subnet routes the message through the PDEG Encryption Unit. The PDEG Encryption Unit inspects the message “selectors”, including its destination and/or source address and protocol, and compares these against the configured data associations/policy rules to determine what to do with the message. Then, the message is either processed (encrypted, authenticated, encapsulated, and forwarded to the subscriber radio), bypassed unprocessed, or discarded. “Discard” is the default data association policy rule for the PDEG Encryption Unit.

When a subscriber radio receives a message from the air interface, it inspects the message selectors, including its source address, and compares these against the configured and default data association/policy rules to determine what to do with the message. The radio either processes (decrypts, authenticates, and forwards to the destination), bypasses unprocessed, or discards. A subscriber radio always discards an IPsec ESP/IP message if it is not sourced from the PDEG Encryption Unit with which the subscriber radio is configured to communicate. There is also an optional configuration that allows all clear outbound data (CEN to subscriber) to bypass EID processing.

2.4.2 Routing from the Subscriber Radio to the Red Subnet

When a subscriber radio receives a message destined for the CEN from a mobile application, it inspects the message selectors, including its source address, and compares these against the configured and default data association/policy rules to determine what to do with the message. The radio either processes (decrypts, authenticates, and forwards to the PDEG Encryption Unit), bypasses unprocessed, or discards.

When the PDEG Encryption Unit receives a message from the black subnet, it inspects the message selectors, including its destination and/or source address and protocol, and compares these against the configured and default data association/policy rules to determine what to do with the message. Then, the message is either processed (decrypted, authenticated, and forwarded to the destination), bypassed unprocessed, or discarded.

Incoming calls (subscriber radio to host) can be routed using the Process Bypass action, which allows clear or encrypted messaging from the same radio. If the message is sent as encrypted, it is decrypted.

If the message is sent as clear, it passes through without decryption. Process is the default data association policy rule for the subscriber radio.

This page intentionally left blank.

Chapter 3

Encrypted Integrated Data Installation and Configuration

This chapter details installation and configuration processes relating to the Encrypted Integrated Data feature.

3.1 Installing EID Components

The installation of the EID feature assumes that the ASTRO® 25 IV&D system is installed and operational. For detailed procedures on installing and configuring the PDEG Encryption Unit, see the *PDEG Encryption Unit* manual. This process provides a list of items you need to have access to before you can complete the installation and configuration described in this chapter.

Process:

1. Make sure that the ASTRO® 25 system media are available to you. Specifically, you need:
   - KVL software version must be R03.52.45 or later to be FIPS Level 3 compliant (for black keyloading only) on a PDEG Encryption Unit. Obtain software update media and install, if your system does not comply.
   - KMF requires a software version R03.09.20 or later. Obtain software update media if using this optional equipment.
   - Subscriber radios require software version R14.00.00 or later for XTL/XTS models and version R4.00.00 for APX radios. Also, the subscriber radios must have Q947/W947 Packet Data option and be operating in a trunking mode.
   - XTL/XTS model radios must have UCM (Universal Crypto Module) version R05.07.00 or later and APX radios must have Motorola Advanced Crypto Engine (MACE) version R01.02.00 or later.

     NOTICE: Consult your subscriber radio user guide to determine how to retrieve the encryption engine version information from the radio.
   - Subscriber radios in the field require an Advanced Encryption Standard (AES) refresh if they already had a previous version of the AES algorithm, or you must purchase Galois Counter Mode (GCM) and AES options for new or existing subscriber radios without AES.

     NOTICE: To verify the AES-GCM algorithm is loaded on the subscriber radio, place the radios into service mode to view the loaded algorithms.
   - PDEG Encryption Units ship with the OS pre-installed. Encryption material is distributed by a PCMCIA card with the KVL. You need to load software to the black subnet and to the red subnet.

     IMPORTANT: When loading software to multiple PDEG Encryption Units with the KVL, load all black subnets that you plan to configure and then all red subnets. You cannot load the black and the red on one device and then go to the next one.

2 Make sure that you have the user names, passwords, and procedures you need to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.

3 Acquire a service laptop/PC with a terminal emulator program, such as HyperTerminal or PuTTY, to connect to the PDEG Encryption Unit using an RS232 cable. See the *PDEG Encryption Unit* manual for cable part numbers and ordering information. You also need Motorola Customer Programming Software (CPS) to configure the subscriber radios.

4 Ensure that you have the default credentials (local account usernames and passwords) for the devices being installed, as well as updated passwords for those types of accounts (so that you can change the password once you install the device). Contact your system administrator, if you do not have this information.

5 If the black subnet is a new subnet, you can use the existing CEN subnet as the red subnet and change the black subnet address through the border gateway. Call the Motorola Solution Support Center (SSC) to open a case to provide updated configurations for the routers/gateways to account for EID. See the *System Routers – S6000/S2500* or *System Gateways – GGM 8000* manuals for more information on the border router/gateway hardware.

6 If you need to update the KMF client and server to support the EID feature, backup the KMF server.

CAUTION: Save the database backup `.dmp` file to the KMF server's desktop or drive. Using a flash drive could cause problems when importing the data.

7 Obtain the following values for the PDEG Encryption Unit configuration from the system administrator:

- IP address and subnet mask for the red subnet
- IP address and subnet mask for the black subnet
- KMF port assignment
- KMF IP address
- Secure/clear policy for all data

  NOTICE: Up to 16 exceptions/policies are allowed.

- Local and remote host addresses and parameters for associations including:
  - source IP address (local)
  - destination IP address (remote)
  - protocol (ID or name)
  - direction (inbound or outbound)
  - CKRs

8 Obtain the following values for the subscriber radio configuration from the system administrator:

- Encryption/decryption key material
- PDEG Encryption Unit endpoint IP address
- CEN IP address (or addresses) for EID bypass rules
- KMF IP address
- KMF port assignment
- Clear policy for all data

  NOTICE: Up to 20 exceptions/policies are allowed.

9 Obtain the following values for the Key Variable Loader configuration from the system administrator:

- If KMF is used for centralized key management, you need the KMF RSI
- Target RSI
- CKRs (key material)

NOTICE: You also need to set up the KMF CryptR.

10 Optional: Obtain the following values for the Key Management Facility configuration from the system administrator:

- CEN IP address
- PDEG Encryption Unit IP address

NOTICE: The PDEG Encryption Unit is provisioned in the KMF by selecting **Security**, **Infrastructure**, then **PDEGs**.

- Algorithm
- Common Key Reference (CKR) assignment
- Transport system

IMPORTANT: Radio information in the KMF must match the parameters programmed into the radio using the Customer Programming Software (CPS). See the CPS for your radio model.

11 Connect a data PC (on the red subnet) to the PDEG Encryption Unit.

12 Add a route to use the PDEG Encryption Unit IP address as a default gateway to reach subscriber radios. See Adding Routes for the Red CEN PC and Subscriber Radios on page 52.

13 If applicable, obtain the following values for the Centralized Event Logging server (syslog server) in the CEN from the system administrator:

- red subnet IP address
- syslog network IP address
- syslog port (the default is 514)
- syslog level (0 through 7)

NOTICE: If the customer does not provide a Centralized Event Logging server (syslog server) in the CEN that you can use for troubleshooting EID, you need a PC with appropriate Centralized Event Logging server software to use this feature. Motorola can assist you in identifying a standard Centralized Event Logging server application that can provide this capability.

14 Various tools are needed to install and service the equipment. If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solution Support Center (see Contacting Motorola for Technical Support on page 65 for the contact number). The following is a list of general recommended tools for installing and servicing the hardware:

- 1 service laptop with CPS, FLASHport, and HyperTerminal or equivalent are required.
- 1 Rack Units (RUs) of space or desk space for the PDEG Encryption Unit hardware.
- 1 PDEG Encryption Unit software installation flash card for the KVL.

NOTICE: Although the PDEG Encryption Unit is one device, it requires two pieces of software for the distinct subnets.

- 1 PDEG Encryption Unit connection cable for the KVL to connect to the PDEG Encryption Unit. See the *PDEG Encryption Unit* manual for the necessary cables to use with the KVL device.
- 1 screwdriver.
- RS232 serial port with a DB-9 connector cable to connect the PDEG Encryption Unit to the service laptop.
- 1 Ethernet cable.
- FLASHport to install updates on the subscriber radios.
- 1 PCMIA card to install software updates on the subscriber radios.
- Charged battery and a backup battery for the KVL.
- Phone to call Motorola and activate the card on site

Postrequisites:
See the following manuals for installation procedures for the EID components:

- *PDEG Encryption Unit* manual, which provides hardware installation procedures.
- *Key Management Facility* manual, which provides hardware installation and configuration procedures. The KMF client also has online help.
- *KVL 3000 and KVL 3000 Plus Key Variable Loader User's Guide* (6881131E16) for manual software updates to subscriber radios.
- *KVL 4000 Key Variable Loader ASTRO 25 User Guide* for manual software updates to subscriber radios.
- *Customer Programming Software* Online Help, which provides field descriptions for this software.
- ASTRO® 25 subscriber radio User's Guide for your specific model, which provides information on software updates for the subscriber radios you have deployed.

3.2 Configuring the Customer Enterprise Network for EID

The driving force of the Encrypted Integrated Data feature is the PDEG Encryption Unit, which must be installed and configured in the Customer Enterprise Network (CEN) using two IP addresses: one for the red subnet interface and one for the black subnet interface.

See the *PDEG Encryption Unit* manual for the actual procedures needed to commission this device.

Process:

1. If you have MAC Port Lockdown installed on the system, disable the feature. If you are using the Motorola CEN Ethernet switch solution, see the *MAC Port Lockdown* manual.
2. Configure the Key Management Facility (KMF), if desired.

   This includes:

   - Installing the KMF server and client hardware, if necessary.
   - Installing the KMF software.
     - For centralized key management, install KMF software version R03.09.20 or later.
     - For non-centralized key management where KMF is not used, verify that KVL software version R03.52.45 or later is installed (for black keyloading) to key manage a PDEG Encryption Unit.
   - See the *Key Management Facility* manual and *KMF Online Help* on the KMF client for the complete configuration process.

See the “PDEG Encryption Unit Configuration” chapter in the *PDEG Encryption Unit* manual for procedures related to each subsequent step in this process.

3. Set up a serial connection for the PDEG Encryption Unit using the red port on the front of the device to connect to the service laptop.

   NOTICE:
   If the PDEG Encryption Unit is already initialized when the terminal emulation session is started, then press Enter to notify the PDEG Encryption Unit of the connection. If the PDEG Encryption Unit is powered up after the terminal emulation session has started, then the PDEG Encryption Unit displays a greeting and prompts for a login name and password.

   The PDEG Encryption Unit validates the login name against a pre-configured user name and password before the command prompt appears. Motorola recommends changing the password after this initial login to a unique password 14–16 characters in length.

4. Assign IP addresses for the PDEG Encryption Unit using the service laptop with terminal emulation software, such as HyperTerminal or PuTTY. See “Configuring Associations and Rules” in the *PDEG Encryption Unit* manual for details.

5. Optionally, you can customize the login banner for the interface to the PDEG Encryption Unit. See the *PDEG Encryption Unit* manual for details.

6. Load encryption keys to the PDEG Encryption Unit using the red port on the front of the device to connect to the Key Variable Loader (KVL).

   NOTICE: Keys must be loaded before the associations are made or an error message appears.

7. Set up the PDEG Encryption Unit Over the Ethernet Keying (OTEK) configuration.

   IMPORTANT: Consult with your system administrator on the IP plan for your system. Port values may be fixed. Do not change the port values without consulting with your system administrator first.

8. Configure the PDEG Encryption Unit for event logging.

9. Configure the PDEG Encryption Unit associations between the local and remote hosts in the PDEG Encryption Unit.

   IMPORTANT: When setting up data associations, ensure that the rules do not overlap in any way to have predictable PDEG Encryption Unit behavior. Overlap means that one data association is an exception to or policy selectors could also apply to another data association. For example, two data associations that apply to the same source IP subnet, but one applies to a destination subnet and the other applies to a specific IP address within that same destination subnet. For more information, see “Configuring Associations and Rules” in the *PDEG Encryption Unit* manual.

10. Connect the PDEG Encryption Unit to the ASTRO® 25 system.

11. Verify PDEG Encryption Unit connection with the KMF, Centralized Event Logging server (syslog server), and that the device is reachable on the red subnet by all intended hosts.

    CAUTION: Be careful when handling the PDEG Encryption Unit. Pressing the Erase button deletes the key material. If this happens, you must re-configure the device.

12. Enable MAC Port Lockdown on the system, if you disabled the feature at the beginning of this process. If you are using Motorola CEN Ethernet switch solution, see the *MAC Port Lockdown* manual.

3.2.1 Keyloading Configuration with KVL

In some cases, when an older model KVL (KVL 3000 Plus at version R03.52.45 or later works without this additional configuration) that only does red keyloading is used, additional PDEG Encryption Unit configuration is required. If you are required to be FIPS level 3 compliant, set the PDEG Encryption Unit as:

- `fips enabled`: allows only black keyloading
- `fips disabled`: allows red or black keyloading

The default setting is `fips enabled`. You must have software version R03.52.45 or later to do this.

3.3 Configuring the PDEG Encryption Unit Associations

When setting up data associations, ensure that the rules do not overlap in any way to have predictable PDEG Encryption Unit behavior. Overlap means that one data association is an exception to or policy selectors could also apply to another data association. For example, two data associations that apply to the same source IP subnet, but one applies to a destination subnet and the other applies to a specific IP address within that same destination subnet.

To prevent overlapping data associations, use selectors that make the data associations not overlap. For example, to send data to the same subnet (for example, subscriber subnet) but with a different data association policy (process versus bypass), make the source IP address specific and different between the two data associations (for example, two different CEN host server IP addresses). Another example would be to send from the same IP address using different policies. In this case, make the destination address selector different. For example, use the subscriber destination subnet for the secure policy and use a different destination subnet for the bypass policy for broadcast messages by placing broadcast destination addresses in a different subnet than the subscriber destination subnet.

CAUTION: If you are using the ANY rule for processing in the PDEG Encryption Unit, you must also create a specific rule to allow UDP traffic in addition to the ANY rule.

See “Configuring Associations and Rules” in the *PDEG Encryption Unit* manual for more information.

3.4 Adding Routes to the KMF

If you are using a Key Management Facility (KMF) in your system and the KMF is located in the red subnet, you must configure the KMF routing tables to direct centralized key management traffic to the PDEG Encryption Unit for proper EID routing. If you do not configure the KMF routing tables, the KMMs may not get routed to the PDEG Encryption Unit and then forwarded to the targeted secure device (for example, a subscriber radio or console). All servers in the red subnet need to have similar routes added for reaching the black network. This procedure describes how to configure the network to ensure KMF-to-secure device connectivity. The “`-p`” in the command indicates that this is set as a persistent route.

Prerequisites:
Before you begin this procedure, obtain the following values for the secure endpoints that will be key managed by the KMF in the red subnet that is connected to the PDEG Encryption Unit:

- destination: Secure endpoint destination IP address (OTEK console clients) or destination subnet and subnet mask (subscriber radios)
- source: KMF source IP address
- gateway: PDEG Encryption Unit red subnet IP addresses

All servers in the CEN's red subnet need to have similar routes for the black network added.

Procedure:

1. On the KMF client, access the command window. For example, pressWindows icon +R keys.

   The Run dialog box appears.

2. Type `cmd` and press Enter.

   The command prompt window appears.

3. Type
   `route add` ***`<destination IP address>`*** `mask` ***`<subnet mask><outbound red PDEG Encryption Unit gateway IP address>`***`-p`
   and press Enter to direct all the traffic with destination of the subscriber radios to go through the red side of the PDEG Encryption Unit. Perform this step for each different subscriber subnet and for OTEK console clients.

   Step example: `route add 192.6.89.0 mask 255.255.255.0 50.6.1.10 –p`
   This command creates a persistent route. When the KMF sends a data packet to a subscriber radio or OTEK console client in the specific IP address subnet or address, the KMF routes the packet to the PDEG Encryption Unit address on the network.

4. On the KMF, type `route print` and press Enter to verify the additional route.

The routing between the KMF and the secure device is complete.

3.4.1 Configuring OTAR Clients with New KMF IP Address

When Encrypted Integrated Data is introduced in an ASTRO® 25 system, the KMF may be in the new subnet, which means a new IP address. It is important to remember to reconfigure all OTAR clients (remote devices) in the system with the new KMF IP address.

3.5 Adding Routes for Subscriber Radios

When and where to use:
The data PC in the red subnet is set as the destination and the inbound gateway is the subscriber radio. When defining these associations, each PDEG Encryption Unit requires two commands to set up the outgoing (red subnet) and the incoming (black subnet). The “ `-p`” in the command indicates that this is set as a persistent route. The interface between the red subnet PC and the subscriber radio is configured as a “modem”. In most cases, you see the model of Motorola radio on COM3 for the device once you perform this procedure.

Procedure:

1. Establish a physical connection with a PC in the red subnet and the subscriber radio using the radio data interface cable for the specific model of radio you are using.
2. Power on the subscriber radio.

   The radio initializes and the drivers automatically install.

3. From the **Start** menu on the PC, choose **Settings**, **Network Connections**, then **New Connection Wizard**.
4. Click **Next**.

   The Network Connection Type screen appears.

5. Choose **Connect to the network at my workplace**. Click **Next**.

   The Network Connection screen appears.

6. Choose **Dial-up connection**. Click **Next**.
7. Type the name of the connection. Click **Next**.

   The **Phone Number to Dial** screen appears.

8. Type the connection phone number you want to use to make the connection. Click **Next**.

   The Smart Cards screen appears.

9. Specify whether you are using a smart card. Click **Next**.

   The Connection Availability screen appears.

10. Choose **Anyone's use**, click **Next**, then **Finish**.

    The subscriber radio connection now appears in the list of Network Connections. Typically, the radio appears as a COM port.

The association between the PC in the red subnet and the subscriber radio is complete.

3.6 Adding Routes for the Red CEN PC and Subscriber Radios

When and where to use:
This procedure describes how to configure the routes from the PC in the red subnet to the subscriber radios being deployed.

⚠ **CAUTION:** Ensure that the IP address used for Secure data does not conflict with the IP address set in the CPS for Bypass (clear). If there is a conflict, the Secure data is sent as clear.

Procedure:

1. On the PC in the red subnet, access the command window. For example, pressWINDOWS ICON + R keys.
2. In the **Run** dialog box, enter: `cmd`
3. In the command prompt window, enter:

   ```
   route add <red CEN PC IP address> mask <subnet mask><IP address of the PC's physical interface>-p
   ```

   to direct all the traffic with destination of the subscriber radios to go through the red side of the PDEG Encryption Unit.

   Step example: `route add 192.6.89.0 mask 255.255.255.0 50.6.1.10 –p`
   This command creates a persistent route for the packet to the PDEG Encryption Unit address on the network.

4. Add similar routes using this same command for each of the subscriber radios.
5. On the PC in the red subnet, enter: `route print` to verify the new routes.

The routes from the PC in the red subnet to the subscriber radios are set.

3.7 Setting Networking Properties

Once the subscriber radio network connection is added on the PC, follow this procedure to set the networking properties for this connection.

Procedure:

1. From the list of network connections on the PC, highlight the radio you want to configure, right-click that device, then select **Properties**.

   The radio device **Properties** dialog box appears.

2. On the **General** tab, set the **maximum speed** to `115200` and select all of the **Hardware features** check boxes, as well as **Enable modem speakers**. Click the **Options** tab.
3. On the **Options** tab, clear any **Dialing options** check boxes, set the **redial attempts** to **3**, **time between redial attempts** to **1 minute**, and **Idle time before hanging up** to **Never**. Click the **Security** tab.
4. On the **Security** tab, select **Typical**. Click the **Networking** tab.
5. On the **Networking** tab, select **PPP** for the **Type of dial-up server I am calling**. Click **Settings**.

   IMPORTANT: This step may change if you are using APX subscriber radios that support an RNDIS connection through USB.

   The **PPP Settings** dialog box appears.

6. Select **Enable LCP extensions** and **Enable software compression**. Click **OK**.

   The **PPP Settings** dialog box closes.

7. Back on the **Networking** tab, highlight **Network Monitor Driver**. Click **Properties**.

   The **Internet Protocol (TCP/IP) Properties** dialog box appears.

8. Click **Advanced**.

   The **Advanced TCP/IP Settings** dialog box appears.

9. On the **General** tab, clear the **Use default gateway on remote network** and **Use IP header compression** check boxes. Click **OK**.

   The **Advanced TCP/IP Settings** dialog box settings are saved and you return to the **Network** tab of the device's **Properties** dialog box.

10. On the **Advanced** tab, click **Settings** in the **Windows Firewall** section.

    The **Windows Firewall** dialog box opens.

11. On the **General** tab, click **Off (not recommended)**. Click the **Exceptions** tab.
12. Select the **AQT Remote Agent**, **BPT Test**, **DCOM**, **File and Printer Sharing**, **Remote Assistance**, **Remote Desktop**, **rserver3.exe**, **Display a notification when Windows Firewall blocks a program** check boxes. Click the **Advanced** tab.
13. On the **Advanced** tab in the **Windows Firewall** dialog box, click **Settings** in the **Network Connection Setting** section.

    An **Advanced Settings** dialog box appears.

14 Clear all check boxes on the **Services** and **ICMP** tabs. Click **OK**.

The **Advanced Settings** dialog box closes and you return to the **Advanced** tab on the **Windows Firewall** dialog box.

15 On the **Advanced** tab in the **Windows Firewall** dialog box, click **Settings** in the **Security Logging** section.

A **Log Settings** dialog box appears.

16 Clear the **Logging Options** check box, set the **Log File Options** name to `C:\Windows\pfirewall.log` with a size limit of `4096`. Click **OK**.

The **Log Settings** dialog box closes and you return to the **Advanced** tab on the **Windows Firewall** dialog box.

17 On the **Advanced** tab in the **Windows Firewall** dialog box, click **Settings** in the **ICMP** section.

An **ICMP Settings** dialog box appears.

18 Select **Allow incoming echo request** and leave all other check boxes cleared. Click **OK**.

The **ICMP Settings** dialog box closes and you return to the **Advanced** tab on the **Windows Firewall** dialog box.

19 Click **OK**. Click **OK** again to save the settings.

The **Windows Firewall** dialog box settings are saved and you return to the device's **Properties** dialog box, which also closes.

Postrequisites:
Set up PDEG Encryption Unit Secure, Bypass, or Both data associations for the subscriber radios to communicate with hosts in the CEN red subnet. Motorola recommends using a 32–bit subnet mask for specifying all red subnet host destination and source addresses.

Example: 50.6.1.12/32 = 32–bit subnet mask, where “/32” indicates an exact value for all 32 bits or exactly address 50.6.1.12.

Once you perform Adding Routes for Subscriber Radios on page 51 and this procedure, you can establish the routes using the physical connection between the PC and the radio. Keep in mind that the radio has an IP address, then generates a second IP address for the PC it is connected to automatically. There is also an ASTRO® 25 IP address that the network generates. To add routes for the PC and the subscriber radios, obtain the following values:

- Red CEN IP address – Secure (for example, 50.6.1.119)
- Red CEN IP address – Bypass (for example, 50.6.1.120)
- ASTRO® 25 network subnet (for example, 192.6.89.1)

3.8 Configuring Subscriber Radios for EID

To enable the Encrypted Integrated Data (EID) feature for subscriber radio internal applications, enable the EID option in the subscriber radio and add association rules to the PDEG Encryption Unit that the subscriber uses to process data flows between the subscriber radios and the red subnet servers used by subscriber radio internal applications.

For more information on how to configure EID, see the documentation for your specific radio model, the *Customer Programming Software* online help, and FLASHport User's Guide.

Procedure:

1 Start the **CPS** application.

2 From the navigation pane on the left, select **Secure Configuration** → **Secure Wide**.

3 In the **General** tab, enable the **Secure Operation** option.

4 From the navigation pane on the left, select **Data Configuration** → **Data Profiles** and select the **Data Profile** that you want to set up for EID.

5 In the **Network Layer Security** tab, set the **Secure/Clear Strapping** field to **Secure**.

6 In the **Key Selection** field, select the encryption key that you want to use on this radio.

7 In the **Encrypted Gateway Address** field, enter the appropriate IP address.

8 Perform one of the following actions:

- If you want to receive clear (unencrypted) text data on a secure radio, select the **Allow Rx Clear Packet Data** check box.

  This option does not apply to KMF OTAR, which is handled as a special case by subscribers and needs no rules.
- If you do **not** want to receive clear text data on a secure radio, clear the **Allow Rx Clear Packet Data** check box.

9 To configure subscriber radios for bypassing EID, select the **EID Bypass List** tab.

10 In the **Bypass List** tab, perform one of the following actions:

- If you want to set a bypass rule for communications with a single IP address in the red subnet, enter an **IP Address** and set its **Address Type** to **Both**.
- If you want to set a bypass rule for sending data to and receiving data from two different IP addresses in the red subnet, specify the **Source** and **Destination** IP addresses in separate bypass rules.

NOTICE: Typically, the PDEG Encryption Unit is used in secure mode to benefit the encryption feature. When in secure mode, ensure that the bypass IP addresses that are set in the CPS do not conflict with the end-to-end IP addresses that are used in secure mode. If there is any conflict, the subscriber radio sends clear data instead of encrypted data.

11 From the top menu, select **Device** → **Write Device** to save the changes.

3.9 Existing System with EID Configuration

For information on how to add the EID feature to an existing ASTRO® 25 radio system, see Encrypted Integrated Data Feature Expansion/Upgrades on page 69.

This page intentionally left blank.

Chapter 4

Encrypted Integrated Data Optimization

This chapter contains optimization procedures and recommended settings relating to the Encrypted Integrated Data feature.

4.1

Optimizing for EID

There are no optimization procedures necessary for the EID feature. If encrypted data traffic capacity is likely to increase, contact your Motorola Field Services representative for assistance.

This page intentionally left blank.

Chapter 5

Encrypted Integrated Data Operation

This chapter details tasks to perform once the Encrypted Integrated Data feature is installed and operational on your system.

5.1 Operating EID Components

The EID feature relies on several pieces of hardware, which have general operating procedures covered in their own manuals. See the following ASTRO® 25 system documentation for more information:

- *PDEG Encryption Unit* manual
- *Key Management Facility* manual
- *KVL 3000 and KVL 3000 Plus Key Variable Loader User's Guide*
- *KVL 4000 Key Variable Loader ASTRO 25 User Guide*

5.2 Managing Keys

Encryption keys are stored on both the PDEG Encryption Unit in the CEN and in the subscriber radio within the ASTRO® 25 system.

The act of installing encryption keys to the PDEG Encryption Unit or subscriber radios is called *loading*. The act of erasing the keys is called *zeroizing*.

5.2.1 Managing Keys on the PDEG Encryption Unit

You can load, view, or zeroize the encryption key material in the PDEG Encryption Unit. Zeroizing permanently erases the encryption key from the CKR memory.

5.2.1.1 Loading Keys on the PDEG Encryption Unit

You can load new keys on PDEG Encryption Unit by using one of the following solutions:

- Key Variable Loader (KVL)
- Key Management Facility (KMF)

You can load keys from the KVL to the PDEG Encryption Unit by using the TARGET selection in the Main menu on the KVL. When in this menu, you have the option of performing the following tasks:

- LOAD – Allows you to load encryption key material into the PDEG Encryption Unit.
- ZERO – Allows you to zeroize encryption key material in the PDEG Encryption Unit.
- VIEW – Allows you to query the target device and display information for each encryption key material stored in the PDEG Encryption Unit (use the arrow keys to scroll through the keys in the display).

You can load keys from the KMF to the PDEG Encryption Unit. For more information, see the *Key Management Facility* manual or *KMF Online Help*.

5.2.1.2
Zeroizing Keys on the PDEG Encryption Unit

The simplest way to zeroize all keys, press the Erase button on the front of the PDEG Encryption Unit. The backup battery normally retains the keys while no main power is supplied, but also allows you to press the Erase button and remove the keys while there is no main power.

You can also use the KVL or KMF to erase the keys from the PDEG Encryption Unit.

5.2.1.3
Rotating Keys on the PDEG Encryption Unit

When using the KMF to manage keys, the PDEG Encryption Unit can have two distinct keysets. When the device is transmitting data, it encrypts using the keys in the active keyset. The KMF can send new keys to the inactive keyset, which does not interfere with data communication while the new keys are being established.

When all of the new keys have been delivered to all of the devices, the KMF sends a message to the devices to switch the active keyset to the new keys. At this point, the devices begin using the new keyset for communication. Since switching can take time, the devices decrypt data that comes from devices that have already switched and from devices that have not and know how to determine which key to use. This is similar to how the subscriber radios rotate keys. However, the subscriber radios have the option to erase keys on changeover and the PDEG Encryption Units cannot.

5.2.2
Managing Keys on the Subscriber Radio

You can load, rotate, or zeroize the encryption keys on an ASTRO® 25 system subscriber radio through the KVL device or centralized through the optional KMF equipment.

Subscriber radio EID configuration parameters other than encryption keys are statically configured using the appropriate configuration tool. EID does not support Internet Key Exchange (IKE) for establishing the IPsec parameters. Encryption keys may be dynamically managed using centralized key management only. Since CPS is used to configure subscriber radio EID parameters, it is possible to remotely manage these parameters using the POP25 feature.

Chapter 6

Encrypted Integrated Data Maintenance

This chapter describes periodic maintenance procedures relating to the Encrypted Integrated Data feature.

6.1 Maintaining the Encrypted Integrated Data

The Encrypted Integrated Data feature relies on periodic hardware, software, and encryption key maintenance.

6.1.1 Maintaining Hardware

All physical components associated with the EID feature must be maintained in proper operating condition. Depending on the hardware, this may include routine inspection, cleaning of exterior surfaces, and proper ventilation.

The EID feature relies on several components, which have general maintenance procedures covered in their own manuals. See the following ASTRO® 25 system documentation for more information:

- *PDEG Encryption Unit* manual
- *Key Management Facility* manual
- *KVL 3000 and KVL 3000 Plus Key Variable Loader User’s Guide* or *KVL 4000 Key Variable Loader ASTRO 25 User Guide*
- ASTRO® 25 subscriber radio User's Guide for your specific model

6.1.2 Maintaining Software

Software and firmware updates to the EID components must be installed as and when they become available for optimal operation.

Although the PDEG Encryption Unit is one device, it requires two pieces of software for the distinct subnets, which are installed with a KVL.

The subscriber radios receive their software updates through Customer Programming Software (CPS) or FLASHport. See the user guide for your specific radio model for more information.

6.1.3 Rotating Keys

Periodically, depending on the customer policy, full rekeying should be done, which means that new Key Encryption Keys (KEKs) should be loaded by using a KVL on both the subscriber radio and the PDEG Encryption Unit.

A radio, after it has been initially setup, supports the following additional operations:

- Rekeying: A radio requests a rekey update from KMF Then, the KMF provides new keys through OTAR.

- Zeroizing/erasing: All the keys stored in the subscriber radio can be erased by the administrator.
- Zeroizing/erasing select keys: Individual keys in the subscriber radio can be erased by the administrator.
- Changing the active keyset: Once a new keyset is added, the previous material is erased.

Chapter 7

Encrypted Integrated Data Troubleshooting

This chapter provides fault management and troubleshooting information relating to the Encrypted Integrated Data feature.

7.1 Troubleshooting Tools

The following tools and applications can be used to monitor the Encrypted Integrated Data components:

- PDEG Encryption Unit event logging
- PDEG Encryption Unit LED status monitoring
- KMF status monitoring for PDEG Encryption Unit
- subscriber radio event reporting capability

7.1.1 Logging PDEG Encryption Unit Events

A CEN-based Centralized Event Logging server (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 (Centralized Event Logging) 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 that shipped with the hardware.

7.1.2 Monitoring PDEG Encryption Unit LED Status

A PDEG Encryption Unit has a series of LED indicators that provide status as described in Encrypted Integrated Data Description on page 25. This table describes the LED status on the PDEG Encryption Unit.

Table 3: PDEG Encryption Unit LED Status

LED Color	Status Description
Red	Indicates no encryption key loaded and no/low battery.
Orange	Indicates no encryption key loaded and a good battery.
Green	Indicates that the encryption key loaded and good battery.

7.1.3 Monitoring the PDEG Encryption Unit with KMF

A KMF application, if used to manage keys on the PDEG Encryption Unit, can provide basic status monitoring of PDEG Encryption Units. The KMF provides a periodic status check of each PDEG Encryption Unit, and reports this status to the KMF user interface and log files.

The KMF monitors and logs the in-service/out-of-service status of PDEG Encryption Units in the CEN. It also manages and logs key distribution status for PDEG Encryption Units.

Consult the *Key Management Facility* manual or *KMF Online Help* for details on this monitoring capability.

7.1.4 Event Reporting for Subscriber Radios

The subscriber radio provides the ability to report EID-related exception events (failure to encrypt/ decrypt) to the user display and to a connected mobile computer through SNMP trap messages. Consult the specific subscriber radio user manual used in your ASTRO® 25 system for details about these event reporting capabilities.

7.2 Failure Scenarios and Possible Resolutions

Table 4: Encrypted Integrated Data Failure Scenarios

Problem	Recovery Action
Unable to log on to PDEG Encryption Unit Admin Account	After 10 failed login attempts, security provisions are in place to lock the device, erase all sensitive material (keys), and reset the password to the default. If you are not sure what the default password is, contact your system administrator or the Motorola Solution Support Center (SSC) for assistance. Re-configure the PDEG Encryption Unit. See the *PDEG Encryption Unit* manual for the configuration procedures.
Red Encryption Status icon on the KMF for the PDEG Encryption Unit	• Hover over the Encryption Status icon with the mouse to determine which PDEG Encryption Unit failed. • Send hello message and see if there is a response. • Unplug the network cable and plug it back in to see if the PDEG Encryption Unit registers. • Verify that the PDEG Encryption Unit has the right keys.
Unable to load key material on the PDEG Encryption Unit	This may be caused by the `fips` setting and compatibility with the KVL software (must have version R03.52.45 or later). Log on, type `fips` and verify that it says `enabled`. If you do not want to use FIPS level 3, then disable it. If you do want FIPS enabled, the software in the KVL might not be supporting the feature and you need to update to version R03.52.45). If this does not resolve the issue, call Motorola Solution Support Center (SSC).
Network services, such as Centralized Event	• Make sure your PDEG Encryption Unit is configured correctly. • Verify that there is a UKEK.

Table continued…

Problem	Recovery Action
Logging (syslog), OTAR, or OTEK unavailable	• Log on and check the key management configuration.
Update of the end-to-end encryption algorithms does not complete successfully	Possible causes: • Poorly connected transfer cable: Ensure that each end of the transfer cable is securely connected to the KVL and the secure component. After ensuring secure connections, repeat the update procedure. • Power failure during the update procedure: Ensure that the KVL battery is charged and repeat the update procedure.
Only able to load red and black subnets on one PDEG Encryption Unit using KVL	Each PDEG Encryption Unit has two MACEs that require two independent updates. Update all red subnets on multiple PDEG Encryption Units, then go back and complete loading of all black subnets to multiple devices using the KVL. This requires two PCMCIA cards.
Previously working PDEG Encryption Unit no longer works.	Possible cause: Erase button was accidentally pushed while handling the device. You must reload all key material.

7.3 Contacting Motorola for Technical Support

The Motorola Solution Support Center (SSC) provides technical support, Return Material Authorization (RMA) numbers, and confirmations for troubleshooting results. Call the SSC for information about returning faulty equipment or ordering replacement parts. North America: 800-221-7144 / International: 302-444-9800.

This page intentionally left blank.

Chapter 8

Encrypted Integrated Data FRU/FRE

This chapter provides replacement information on the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) applicable to the Encrypted Integrated Data feature.

8.1 Replacing EID Hardware

The PDEG Encryption Unit is considered a Field Replaceable Entity (FRE), and when determined to be faulty, may be quickly and easily replaced with a defect-free device to bring the equipment back to normal operation. See the *PDEG Encryption Unit* manual for the part numbers. After removing a failed PDEG Encryption Unit, it must be shipped to the Motorola Infrastructure Depot Operations (IDO) for further troubleshooting and repair. You must return any failed units to the Motorola IDO at 2214 Galvin Dr, Elgin, IL 60123. The field shop contacts the Solution Support Center to request a replacement or repair, and the Depot ships out a replacement FRE. Included in the packaging is paperwork with instructions on how to return the failed unit.

Likewise, see the appropriate ASTRO® 25 system subscriber radio, Key Variable Loader (KVL), and KMF manuals for the specific repair and replacement procedures.

This page intentionally left blank.

Chapter 9

Encrypted Integrated Data Feature Expansion/Upgrades

This chapter includes information pertaining to expansions and upgrades of the Encrypted Integrated Data (EID) feature.

9.1

Adding New EID-Enabled Subscriber Radios or PDEG Encryption Units to an Existing System with EID

Minimal downtime can be achieved for existing online applications when expanding the Encrypted Integrated Data (EID) feature by applying temporary rules in the PDEG Encryption Unit and subscriber radio, such that subscriber radios can be expanded independently following deployment of the PDEG Encryption Unit in the CEN. Non-expanded subscriber radios can continue to function on the system along with expanded subscriber radios until all radios are expanded. The temporary rules can be removed from the PDEG Encryption Unit first and then optionally from each subscriber radio at the earliest convenience.

The EID feature expansion allows endpoints to receive clear or encrypted data during subscriber expansion. The subscriber radios can be upgraded independently allowing upgraded and non-upgraded subscribers to coexist.

Reconfiguration of a fixed PDEG Encryption Unit after a subscriber upgrade is complete prevents clear data from passing into CEN.

Reconfiguration of subscriber radios after the subscriber upgrade is complete can be done at earliest convenience to prevent clear data from passing to the mobile subnet.

9.2

Expanding a System with EID

This process describes the steps you need to take when planning to add the EID feature into an existing system.

Process:

1. Obtain the prerequisite information listed in Installing EID Components on page 45.
2. Evaluate the red and black subnet strategy for the CEN and the application host network location and decide. See Planning Considerations for EID on page 40.

If…	Then…
If there are other mobile data applications on the system,	plan to retain the existing CEN subnet as the red subnet and change the black subnet address through the border gateway.
If there are no active mobile data applications on the system,	plan to make the existing CEN IP address the red or black subnet based on customer preference.

3. Decide if the Key Management Facility (KMF) is going to reside in the CEN black subnet (recommended) or red subnet.

NOTICE: Since KMF OTAR communications is already encrypted, it is recommended to locate the KMF in the black subnet in order to preserve PDEG Encryption Unit throughput capacity.

If…	Then…
If the black subnet is the new subnet,	plan to set the IP address of the KMF to a black subnet address and set all subscriber radios provisioned KMF IP address to this address.
If the red subnet is the new subnet,	**a** Plan to set the IP address of the KMF to a red subnet address and set all subscriber radios provisioned KMF IP address to this address. **b** Plan to add bypass rules to the Packet Data Encryption Gateway to allow KMF traffic to pass through unencrypted by this feature. **NOTICE:** An alternate configuration is to add a gateway and route already-encrypted KMF traffic around the PDEG Encryption Unit. There should be no issues with PDEG Encryption Unit handling this additional traffic, however.

4 Plan to add clear text rules to the PDEG Encryption Unit to allow any clear text or already encrypted traffic to/from the red subnet to bypass the PDEG Encryption Unit without processing.

5 Plan to set the IP address of all hosts, clients, and network devices of the new subnet (red or black to matching subnet addresses.

6 Open a case with the Motorola Solution Support Center (SSC) to modify the border gateway configuration.

9.3 Adding the Encrypted Integrated Data Functionality to an Existing ASTRO 25 System

This process describes the addition of the EID feature to an existing ASTRO® 25 radio system.

Process:

1 If MAC Port Lockdown is being used, enable unused CEN Ethernet switch ports for the new KMF and PDEG Encryption Unit connections. If you are using Motorola CEN Ethernet switch solution, see the *MAC Port Lockdown* manual.

2 Install and configure the KMF to manage the PDEG Encryption Unit.

CAUTION: Update an existing KMF to software version R03.09.20 or later. See the *Key Management Facility* manual for more information.

If…	Then…
If the PDEG Encryption Unit is	**a** Ensure there is a Trunking System record created for communication with the PDEG Encryption Unit(s).

If…	Then…
being centrally managed,	**NOTICE:** The Trunking System record ensures that the KMF has port number configuration for OTEK communication with the PDEG Encryption Unit. **b** Using KMF Client, create a record for the PDEG Group. **c** Create a PDEG record for each PDEG Encryption Unit. **d** Modify the default route in the KMF to point to the PDEG Encryption Unit for OTAR of the radios.
If the KMF is not used,	Skip this step.

3 Install the PDEG Encryption Unit hardware. See the *PDEG Encryption Unit* manual for details.

> **NOTICE:** The PDEG Encryption Unit ships with the necessary software and algorithm installed.

4 Configure the PDEG Encryption Unit's IP addresses, subnet masks, default gateway address for red and black subnets, any OTEK-related (whether the KMF network is in the red or black subnet, as well as the KMF IP address), and Centralized Event Logging server (syslog server) address (including whether the Centralized Event Logging server is on the red or black subnet) parameters, and security policies for the PDEG Encryption Unit by using the serial connection on a field service laptop, RS232 serial port with a DB-9 connector cable, and terminal emulation program like HyperTerminal or PuTTY. See the *PDEG Encryption Unit* manual. Also, add the temporary rules to allow data communications with non-expanded subscribers during the process if mobile data applications are already online using Motorola CPS.

> **NOTICE:** The PDEG Encryption Unit's IP addresses configured here are the actual unique IP addresses (as compared to the virtual addresses configured in the VRRP configuration for redundant units).

5 If there is a redundant pair of PDEG Encryption Units, configure the Virtual PDEG Encryption Unit IP address and Virtual Router Redundancy Protocol (VRRP) ID. See the *PDEG Encryption Unit* manual.

> **NOTICE:** Both PDEG Encryption Units share a Virtual PDEG IP address for the red network and also a Virtual PDEG IP Address for the black network. The PDEG Encryption Units share a VRRP ID and are configured with a priority that determines which device is the preferred active unit.

6 Configure data associations for outgoing (host to subscriber radio) and incoming (subscriber radio to host) data messages. This includes:

- Host IP or subnet
- Radio IP or subnet
- Protocol (or “Any” to not specify a particular protocol)
- Action (Bypass, Discard, Process, Process Bypass for Incoming only)
- CKR

1. If the KMF resides in the red subnet and is routing traffic through the PDEG Encryption Unit, configure PDEG Encryption Unit with outbound data association rules with a setting of **Bypass**.
2. If any red subnet non-subscriber traffic or any already encrypted traffic is passing through the PDEG Encryption Unit, configure the outbound data association rules with a setting of **Bypass**.

3 If there are any clear data transmissions (including subscriber radio to host), either during or after the EID expansion is complete, configure the PDEG Encryption Unit(s) with inbound data association rules with a setting of **Process Bypass** and configure the outbound data association rules with a setting of **Bypass**.

IMPORTANT: When setting up data associations, ensure that the rules do not overlap in any way to have predictable PDEG Encryption Unit behavior. Overlap means that one data association is an exception to or policy selectors could also apply to another data association. For example, two data associations that apply to the same source IP subnet, but one applies to a destination subnet and the other applies to a specific IP address within that same destination subnet. For more information, see “Configuring Associations and Rules” in the *PDEG Encryption Unit* manual.

CAUTION: If you are using the ANY rule for processing in the PDEG Encryption Unit, you must also create a specific rule to allow UDP traffic in addition to the ANY rule.

7 Using the KVL to configure the PDEG Encryption Unit:

1 Set the KMF RSI and PDEG RSI through the **Load KMF RSI** and **Load Target RSI** menus.

NOTICE: RSI configured in KMF through the KVL RSI IDs must match.

2 Provision PDEG Encryption Unit(s) with the key material. Even when a KMF is part of the configuration, the initial keyload of a device must be through the KVL. If there is a KMF, this step should be accomplished using the Store and Forward key distribution function available, with the KVL connected to the KMF.

8 Apply the updated router/gateway configuration files from Motorola SSC case opened during planning.

If…	Then…
If a customer gateway/router is installed between the black and red subnets,	**a** Configure the border gateway routing rule through the Motorola SSC case opened during planning such that the customer router's black subnet interface IP address is the gateway to reach the red subnet. **b** Connect the PDEG Encryption Unit to the CEN red and black subnets. This step requires Ethernet switches with sufficient unused and unlocked ports are available on both the red and black CEN subnets. **c** Verify CEN red and black subnet communications. **NOTICE:** Data communications between the red and black subnets is unavailable at this point of the installation. **d** Verify KMF communications with PDEG Encryption Unit(s) by issuing a status check from the KMF to ensure that the PDEG Encryption Unit is registered with the KMF. **e** Configure routing rules in the CEN border gateway to reach hosts and servers in the CEN red subnet.
If the PDEG Encryption Unit is the only device between the red and black subnets,	**a** Configure the border gateway routing rule through the Motorola SSC case opened during planning such that the PDEG Encryption Unit black subnet interface IP address is the gateway to reach the red subnet. **b** Connect the PDEG Encryption Unit to the CEN red and black subnets. This step requires Ethernet switches with sufficient unused and unlocked ports are available on both the red and black CEN subnets.

If…	Then…
	c Verify CEN red and black subnet communications. **NOTICE:** Data communications between the red and black subnets is unavailable at this point of the installation. **d** Verify KMF communications with PDEG Encryption Unit(s) by issuing a status check from the KMF to ensure that the PDEG Encryption Unit is registered with the KMF. **e** Configure routing rules in the CEN border gateway to reach hosts and servers in the CEN red subnet.

9 Reconfigure the CEN and the clients with new IP addresses and routing tables. This is included in the Motorola SSC support case.

If…	Then…
If the black subnet is the new subnet,	**a** Reconfigure all black subnet or black subnet facing hosts and network appliances with new black subnet IP addresses on black subnet interfaces, including the border gateway. **b** If there is a black host (or hosts) that communicates through the border gateway with clients or hosts in the RNI (excluding subscriber radios), modify the border gateway NAT address configuration to match the new black host IP address. For example, is using OTEK where the IP address of the KMF in the black subnet changes and the KMF has OTEK clients in the RNI, such as MCC 7500 consoles.
If the red subnet is the new subnet,	**a** Reconfigure all red subnet and red subnet facing hosts and network appliances with new red subnet IP addresses on red subnet interfaces. **CAUTION:** Mobile data and RNI-CEN communications are unavailable until this step is completed for affected hosts, devices, and clients. **b** If there is a red host (or hosts) that communicates through the border gateway with clients or hosts in the RNI (excluding subscriber radios), through the SSC case opened during planning modify the border gateway NAT address configuration to match the new red host IP address. For example, with AAMS service where the IP address of the AAMS server in the red subnet changes and the AAMS server has messaging clients on dispatch consoles in the RNI. **c** If the red host(s) is connected to the PDEG Encryption Unit through the CEN router, modify the CEN router routing tables to include a route for red hosts to reach subscribers in the RNI (through the red side of the PDEG Encryption Unit). If not, modify the red host routing tables to include a route to reach subscribers in the RNI (through the red side of the PDEG Encryption Unit).

10 Verify mobile data communications capability from non-expanded subscriber radios to the CEN red or black subnet for all affected hosts, clients, and network devices. See the appropriate subscriber radio manual for more information on initiating mobile data applications.

11 Verify mobile data communications capability from the CEN red subnet to the CEN black subnet and RNI (if applicable) for all affected hosts and clients. For example, with KMF-to-KMF client communications, you could ping the device.

12 If the system has AAMS, send a test message from the Dispatcher Smart Client to the host on the CEN red subnet. See the *ASTRO® 25 Smart Client Messaging User Guide*.

13 If the KMF received a new IP address during this installation, reconfigure all OTAR clients with the new KMF IP address. See the *Key Management Facility* manual.

14 Configure subscriber radios that function as secure data devices using Motorola Customer Programming Software (CPS). This includes:

- Configuring temporary rules to allow subscribers to receive secure or clear data messages. This is done in the subscriber radio. Check **Allow Rx Clear Packet Data** configuration in CPS.

  IMPORTANT: Until all subscribers are updated and loaded with keys, the PDEG Encryption Unit(s) are configured to send clear data transmissions.

- Configuring security policies.
- Changing the CEN host IP addresses (including KMF), if necessary.

15 Provision subscriber radios that will function as secure data devices with key material using the KVL or KMF. Then, verify that subscriber radios are now capable of encrypted voice and data communications. See the *Key Management Facility* manual.

NOTICE: If there is a KMF, use the Store and Forward key distribution function available, with the KMF connected to the KVL.

16 If the system is being used for secure data communications only, reconfigure the following:

- On the PDEG Encryption Unit(s): Reconfigure data association rules to always **Process** (not bypass) data messages.
- On the subscriber radios: Reconfigure data associations rules to only allow secure data. This rule means once again reprogramming all subscriber radios that function as secure data devices, so you do not need to perform this step right away. Secure data communications works with the subscriber radios configured to receive secure or clear data.

17 If MAC Port Lockdown is used on the CEN Ethernet switch, configure the CEN Ethernet switch with information about valid MAC addresses for each port used for new KMF and PDEG Encryption Unit connections. If you are using Motorola CEN Ethernet switch solution, see the *MAC Port Lockdown* manual.

18 If there are redundant PDEG Encryption Units and MAC Port Lockdown in the system and the Ethernet switch is configured with MAC address info by operating in a learning mode:

1 Unplug the active PDEG Encryption Unit from the network to affect a PDEG Encryption Unit switchover.

NOTICE: You need to know which PDEG Encryption Unit is preferred (which would be the active PDEG Encryption Unit if it is up), or perform two switchovers.

2 Once the Ethernet switch has learned the virtual MAC address on the port(s) used by the secondary (now active) PDEG Encryption Unit, reconnect the previously active PDEG Encryption Unit to the network.

19 Lock the CEN Ethernet switch ports used for new KMF and PDEG Encryption Unit connections to allow only those configured or learned MAC addresses. If you are using Motorola CEN Ethernet switch solution, see the *MAC Port Lockdown* manual.

20 Verify the Encrypted Integrated Data feature within the ASTRO® 25 system as follows:

- If you are using the KMF to centrally manage keys:
  - Verify that the KMF can key manage each PDEG Encryption Unit.
  - Verify that the KMF can key manage subscriber radios using OTAR.

- Send an encrypted data message and confirm its receipt.
- Test redundant PDEG Encryption Unit functionality, if applicable:
  1. Unplug the network cable from one of the redundant PDEG Encryption Units.
  2. After 3 seconds, send encrypted data message and confirm its receipt.
  3. Reconnect the network cable to the PDEG Encryption Unit.
  4. Unplug the network cable from the other redundant PDEG Encryption Unit.
  5. After 3 seconds, send encrypted data message and confirm its receipt.
  6. Reconnect the network cable to the PDEG Encryption Unit.

This page intentionally left blank.

Chapter 10

Encrypted Integrated Data Disaster Recovery

This chapter provides references and information that enables you to recover the Encrypted Integrated Data (EID) functionality in the event of a failure.

10.1 Recovering EID Functionality

In the event that the system needs to be reinstalled with EID functionality, refer to the same processes described in Expanding a System with EID on page 69 and Adding the Encrypted Integrated Data Functionality to an Existing ASTRO 25 System on page 70.

This page intentionally left blank.