ASTRO® 25

INTEGRATED VOICE AND DATA

PDEG Encryption Unit Feature Guide

System Release AN2024.HS, AN2024.1, 2022.HS, 2022.1, 2021.1, 2020.HS, 2020.1, 2019.x 7.18

NOVEMBER 2024

MN004403A01-H

Intellectual Property and Regulatory Notices

Copyrights

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

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

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.

License Rights

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

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

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

Disclaimer

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

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

Service agreement customers should be sure to call the CMSO in all situations listed under Customer Responsibilities in their agreement, such as:

- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

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

Document History

Version	Description	Date
MN004403A01-A	Original release of the *PDEG Encryption Unit Feature Guide*	November 2017
MN004403A01-B	Updated sections: ● Assigning IP Addresses for the PDEG Encryption Unit on page 31 ● Configuring PDEG Encryption Units for Redundancy on page 35 ● Associations and Rules on page 36 ● Alternate Configuration Command Mode on page 39 ● Verifying Redundancy Configuration on page 47	June 2018
MN004403A01-C	Updated section: ● Configuring the PDEG Encryption Unit for OTEK on page 32	April 2020
MN004403A01-D	Revised for the 2022.HS and 2022.1 system releases.	September 2022
MN004403A01-E	Updated sections: ● PDEG Encryption Unit on page 13 ● Replacing Batteries in the PDEG Encryption Unit on page 42 ● Key Features on page 13 ● Standards Compliance on page 17 ● Initiating a Serial Shell Connection on page 28 ● Resetting Internal Settings After Downgrade on page 43 ● Cryptographic Algorithm Self-Test on page 44 ● Interpreting Status Indicators on page 45 ● Upgrading PDEG Software or Algorithms on page 43	February 2023
MN004403A01-F	Updated section: ● Associations and Rules on page 36	August 2023
MN004403A01-G	Revised for the AN2024.HS and AN2024.1 system releases.	September 2024
MN004403A01-H	Updated section: ● Upgrading PDEG Software or Algorithms on page 43	November 2024

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About PDEG Encryption Unit Feature Guide

This manual provides descriptive and procedural information about the PDEG Encryption Unit. Included is the description of the PDEG and its role in the Encrypted Integrated Data feature. In addition, procedures are provided for installation, configuration, operation, maintenance, troubleshooting, FRU/FRE replacement, and disaster recovery.

Related Information

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual.
System Overview and Documentation Reference Guide	Provides an overview of the new features, technical illustrations, and system-level disaster recovery for the ASTRO® 25 radio communication system.
Encrypted Integrated Data Feature Guide	Provides information necessary to understand, install, configure, operate, maintain, and troubleshoot the Encrypted Integrated Data feature which enables encryption of data calls between ASTRO® 25 subscriber units and data applications, such as ASTRO® Advanced Messaging Solution (AMS), that reside in the Customer Enterprise Network (CEN).
Key Management Facility User Guide	Provides descriptive and procedural information about the Key Management Facility (KMF) including a description of where the KMF can be found, a description of KMF encryption key management, as well as procedures on installation, configuration, operation, upgrade, troubleshooting, and FRU/FRE replacement.
KVL 4000 Key Variable Loader ASTRO 25 User Guide	Provides instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment, such as radios, fixed encryption units and others, in ASTRO® 25 operating mode. Starting from the AN2024.HS and AN2024.1 system releases KVL 4000 is not supported.
KVL 5000 User Guide	Provides instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment
Secure Communications Feature Guide	Describes the secure communications features found in ASTRO® 25 systems, intended for technicians and system operators. The manual should be used in conjunction with the ASTRO® 25 system documentation and the "Key Management Facility User Guide".

Chapter 1

PDEG Encryption Unit Description

This chapter contains a high-level description of the PDEG Encryption Unit and its components and accessories.

1.1 PDEG Encryption Unit

The Motorola Solutions PDEG Encryption Unit unit is a high-quality, high security IPSec Virtual Private Network (VPN) gateway solution that enables end-to-end secure communications between applications in the CEN and mobile applications over a Motorola Solutions ASTRO® 25 network. The PDEG installs easily with standard RJ–45 Ethernet ports for red-side (clear) and black-side (encrypted) network interfaces.The PDEG Encryption Unit is certified to National Institute of Standards and Technology (NIST) FIPS 140-3 Level 3. The PDEG Encryption Unit data encryption keys can be centrally managed using a Key Management Facility server (KMF) in the Customer Enterprise Network (CEN).

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

Key features of the PDEG Encryption Unit are:

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

Distinctive characteristics of the PDEG Encryption Unit are:

- Integrated physical security
- Highly tamper resistant

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

- ASTRO® 25 IV&D Broadcast Data traffic
- Transit 25 Data

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

1.1.1 Key Features

The following are the key features of the PDEG Encryption Unit:

- Ease of configuration
- Low power consumption
- Active Internal Tamper Shield
- FIPS 140-3 Mandated Environmental Detectors
- Small size/light weight

- High Assurance Software
- Enhanced Fault Tolerance
- Integrated Physical Security
- FIPS 140-3 Level 3 Security
- Interoperable with other networks and gateways

1.1.2 Key Applications

The following are the key applications of the PDEG Encryption Unit:

- Simple point-to-point encryption
- End-to-end encryption on multi-link networks
- Wired to Wireless Networks
- Secured Tunnels/VPN over Bulk networks

1.2 PDEG Encryption Unit Components

Table 1: Major Components of the PDEG Encryption Unit

Item	Part Number	Function
PDEG Encryption Unit	T7539A	PDEG Encryption Unit
Infrastructure Power Cable/Adapter (AC-DC)	0171925M01	Provided with PDEG Encryption Unit
Straight Ethernet Cables (2)	3071813M01	Used to connect the PDEG Encryption Unit to the PC and to the network
RS232 Cable	30009259001	Used for loading configuration parameters
Key load Cable	TKN8531C	Used for key loading
Infrastructure Mounting Bracket	6471176M01	For Rack Mounting
Cable Retention Bracket	0771174M01	For Desktop or Rack Mounting

1.3 PDEG Encryption Unit Accessories

This section lists accessories used for the PDEG Encryption Unit in an infrastructure configuration.

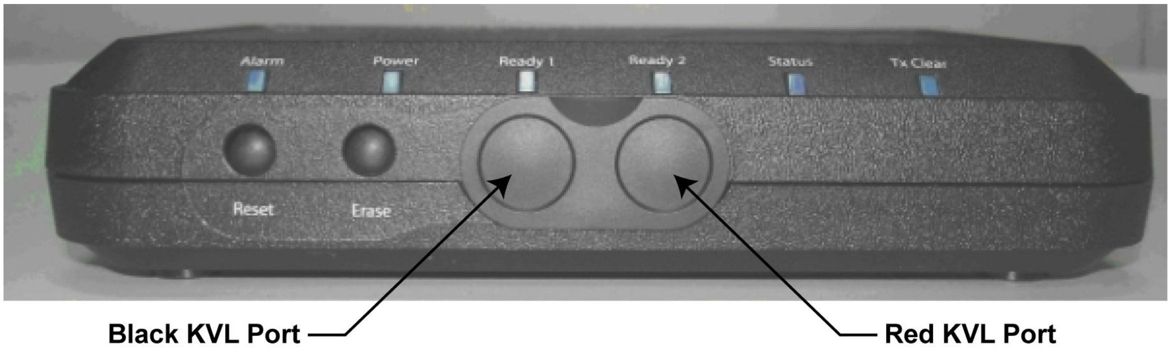
Table 2: Infrastructure Accessories for the PDEG Encryption Unit

Part Number	Accessory
TKN9282	Rack Support Bracket
TKN9283	Rack Mounting Plate
DLN6693	RS232 Cable for PDEG Encryption Unit

Part Number	Accessory
TKN8531C	Key loading Cable

1.4 Physical Description

Figure 1: PDEG Encryption Unit Front View



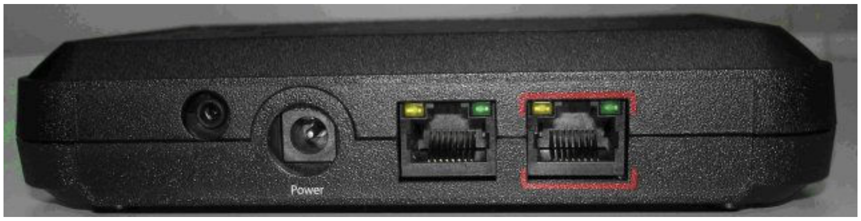
ph_CryptR_FrontView1

The front panel is equipped with the following:

1. Reset button
2. Erase button
3. Two Key Variable Loader (KVL) ports (with protective covers)
4. Alarm LED
5. Power LED
6. Ready1 LED
7. Ready2 LED
8. Tx Clear LED
9. Status LED

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

Figure 2: PDEG Encryption Unit Rear View



The rear panel is equipped with the following:

- Mini Jack
- Power Jack
- Two RJ–45 ports

1.5

Product Specifications

This section lists specifications for the PDEG Encryption Unit.

1.5.1

Security and Performance Specifications

Table 3: PDEG Encryption Unit – Security and Performance Specifications

Characteristic	Value
FIPS Level 3	Sensitive but Unclassified (SBU) Operation
Performance	520 Kbps

1.5.2

Electrical and Physical Specifications

Table 4: PDEG Encryption Unit – Electrical and Physical Specifications

Characteristic	Value
Power	12 V DC @ 500 mA
Interfaces	2x RJ–45 Ethernet, Key Fill, 2x RS232 Serial
Dimensions (mm) ca.	29.5 x 92 x 142 mm
Weight (typical) g ca.	300 g

1.5.3

Environmental Specifications

Table 5: PDEG Router – Environmental Specifications

Characteristic	Value
Operating Temperature	0° to 0° C
Storage Temperature	–10° to 60° C
Humidity	Up to 90% RH at Upper Limit Operating Temperature

1.5.4

Protocols and Encryption Algorithms

Table 6: PDEG Encryption Unit – Protocols and Encryption Algorithms

Characteristic	Value
AES256	Applicable Standard Document: AES – Advanced Encryption Standard: FIPS 197

Characteristic	Value
IPsec	Internet Protocol Security
IPv4	Internet Protocol version Four

1.5.5

Provisioning and Key Management for Encrypted Integrated Data

The following describes encryption key provisioning, key loading, and key management for the PDEG Encryption Unit:

- Configured through an RS232 console port
- Manual provisioning and loading of encryption keys using the Key Variable Loader (KVL)
- Manage Encryption Key using Over-the-Ethernet-Keying (OTEK) through the Key Management Facility (KMF), if your system includes a KMF.

1.5.6

Standards Compliance

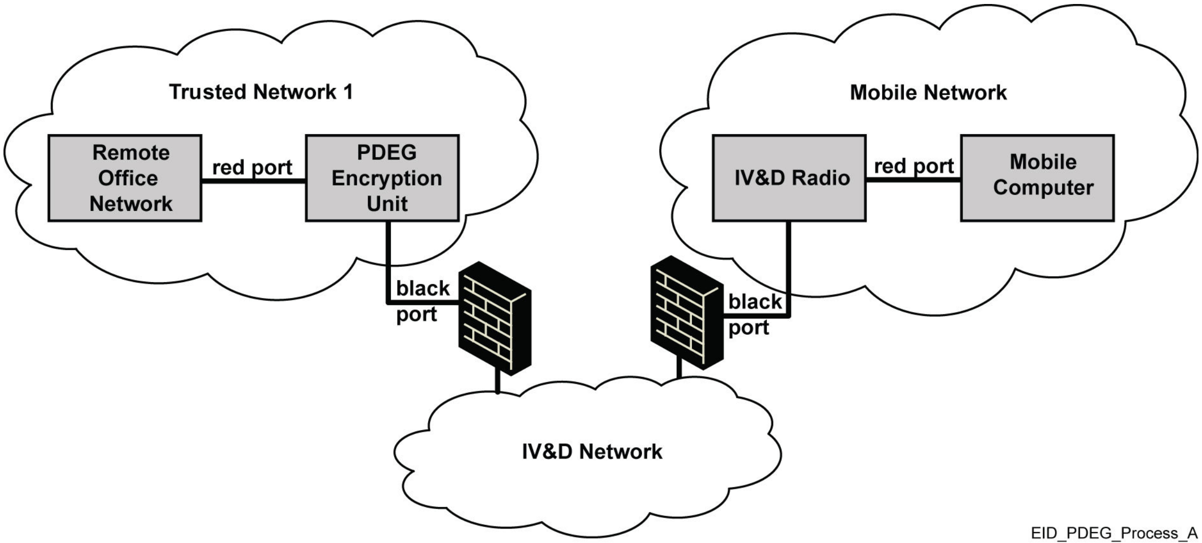
The PDEG Encryption Unit complies with National Institute of Standards and Technology FIPS 140-3 (Security Requirement for Cryptographic Modules) Level 3. For a reference, go to https://csrc.nist.gov/projects/cryptographic-module-validation-program.

Chapter 2

PDEG Encryption Unit Theory of Operations

This chapter explains how the PDEG Encryption Unit works in the context of your system. The following figure shows the basic process for secure communication using the PDEG Encryption Unit.

Figure 3: Secure Communication with the PDEG Encryption Unit



2.1 How PDEG Works

When a message is sent by an application host in the CEN red subnet to a subscriber radio, the CEN red subnet routing fabric 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. The result is to either process (encrypt, authenticate, encapsulate, and forward to the subscriber radio), bypass unprocessed, or discard. “Discard” is the default data association policy rule for the PDEG Encryption Unit.

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. The result is to either process (decrypt, authenticate, and forward to the destination), bypass unprocessed, or discard.

When a subscriber radio receives a message from the air interface, it inspects the message “selectors”, including its source address, and compares them against the configured and default data association/policy rules to determine what to do with the message. The result is to either process (decrypt, authenticate, and forward to the destination), bypass unprocessed or discard. A subscriber radio always discards an IPsec ESP/IP message if it is not sourced from the PDEG Encryption Unit the subscriber radio is configured to communicate with. A configurable option to allow all clear outbound data (CEN to subscriber) to bypass EID processing is also available.

When a subscriber radio receives a message from an external or internal application interface, it inspects the message “selectors”, including its destination address, and compares them against the configured and default data association/policy rules to determine what to do with the message. The result is to either process (encrypt, authenticate, and forward to the destination), bypass unprocessed, or discard. For incoming messages, there is a “process bypass” option that enables the PDEG Encryption Unit to accept both encrypted and unencrypted data at the same time (for example, when a system upgrade is in process, meaning that some radios are upgraded to support encryption but some radios are not).

NOTE: The default policy of the subscriber radio is to process all messages. Therefore, no specific data association/policy rules are needed to encrypt data messages; they are only needed to bypass data messages if desired.

2.2 Encrypted Integrated Data (EID)

The Encrypted Integrated Data (EID) feature adds security to data sent between a radio and a customer data application. In other words, any packet data flowing to or from a radio are ciphered and then deciphered in the radio and Customer Enterprise Network (CEN) premises. This solution ensures that data is secure and immune to compromise throughout the entire route.

EID provides data encryption services to ASTRO® 25 IV&D IP Bearer services between the Customer Enterprise Network (CEN) and subscriber radios. The 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, using IPsec. The encryption algorithm used is Advanced Encryption Standard (AES). The PDEG Encryption Unit and subscriber radio encryption modules are certified to FIPS Level 3. The subscriber radio and PDEG Encryption Unit data encryption keys can be centrally managed using a Key Management Facility server (KMF) in the CEN.

Using the EID feature, your organization can secure data sent using the 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 endpoint within the subscriber radio and the IPsec endpoint within the PDEG located in the CEN.

EID services are not applicable to Broadcast Messaging services.

2.2.1 EID Architecture

The EID feature involves adding one or more PDEG Encryption Units in the CEN. Although a redundant PDEG Encryption Unit pair is shown, redundancy is optional. 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 CEN red subnet and the CEN black subnet. The red subnet is considered the trusted subnet and the black subnet is considered untrusted. Thus, data is encrypted when passing through the black subnet. It is required that the PDEG Encryption Unit red and black subnet interfaces 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 CEN red and black subnets. 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. Specifics on determining application host subnet location are described in the *Encrypted Integrated Data Feature Guide*. Creating separate red and black subnets 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.

2.2.1.1 Key Management

Key management of EID endpoints can be done either manually, using a Key Variable Loader (KVL), or centrally, using a Key Management Facility (KMF). 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.

The KMF server should be in the black subnet of the CEN. Since the KMF, subscriber radio and PDEG Encryption Unit 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 Encryption Unit and consuming a portion of its capacity. However, locating the KMF in the red subnet is also supported if desired but requires EID bypass rules to be configured in the PDEG Encryption Unit for KMF traffic with subscriber radios and consoles. Specifics on determining KMF subnet location are described in the *Encrypted Integrated Data Feature Guide*.

Chapter 3

PDEG Encryption Unit Installation

This chapter provides instructions for installing the PDEG Encryption Unit hardware.

3.1 PDEG Hardware Installation Overview

Process:

1. Unpack the PDEG Encryption Unit. See Unpacking the PDEG Encryption Unit on page 21.
2. Install the hardware (the battery is pre-installed). See Mechanical Installation on page 21.
3. Attach the Ethernet cable. See Attaching Ethernet Cables to the PDEG Encryption Unit on page 26.
4. Configure the PDEG Encryption Unit. See PDEG Encryption Unit Configuration on page 28.

3.2 Unpacking the PDEG Encryption Unit

Procedure:

1. When you open the box, the pre-packed Ethernet Cables are in a plastic bag on the top.
2. Take out the cables and remove the top foam.
3. Take out the mounting plate.
4. At the bottom, you have:
   - Fasteners in the plastic bag
   - Power Adapter
   - Cable Retention Bracket
   - PDEG Encryption Unit

3.3 Mechanical Installation

The PDEG Encryption Unit can be mounted on a desk, in an equipment rack, or on a mobile base application.

3.3.1 Rack Mounting (Optional)

There are two types of rack mounting:

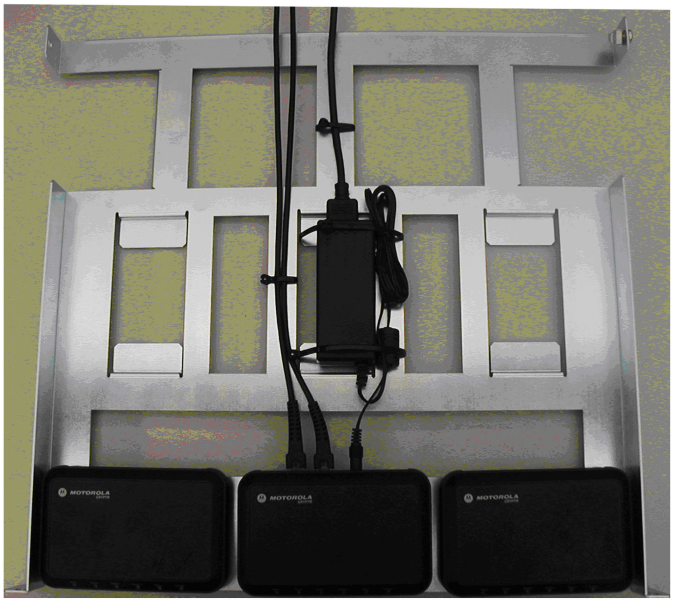
- cabinet mount
- open rack mount

3.3.1.1 Cabinet Mount

If you mount the PDEG Encryption Units in an infrastructure cabinet, then use the Motorola Solutions mounting bracket (Part No. 6471176M01) with the following parts:

- six bolts (Part No. 0310909C91)
- nuts (Part No. 0285504U01)
- cable ties (Part No. 4210217A04)

Figure 4: PDEG Encryption Unit in Cabinet Mount



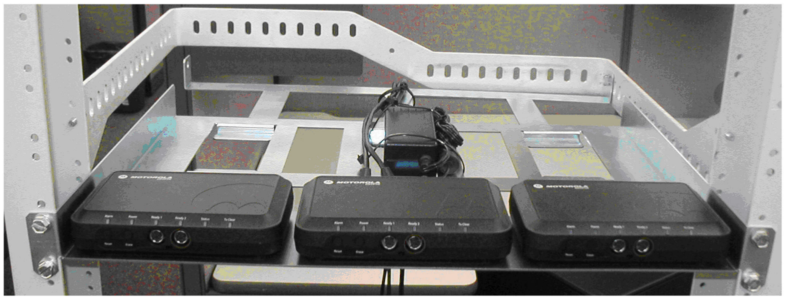
B_IP_CryptR_cabinet_mount

3.3.1.2 Open Rack Mount

If you mount the PDEG Encryption Units in an infrastructure open rack, use the Motorola Solutions mounting bracket (part no. 6471176M01) and Motorola Solutions support bracket (part no. 0784469Y02) with the following parts:

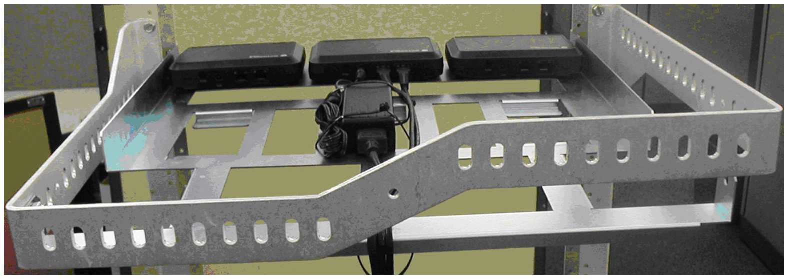
- eight screws (part no. 0309660A01)
- one bolt (part no. 0310909C91)
- one nut (part no. 0285504U01)
- cable ties (part no. 4210217A04)

Figure 5: Front View of PDEG Encryption Unit in Open Rack Mount



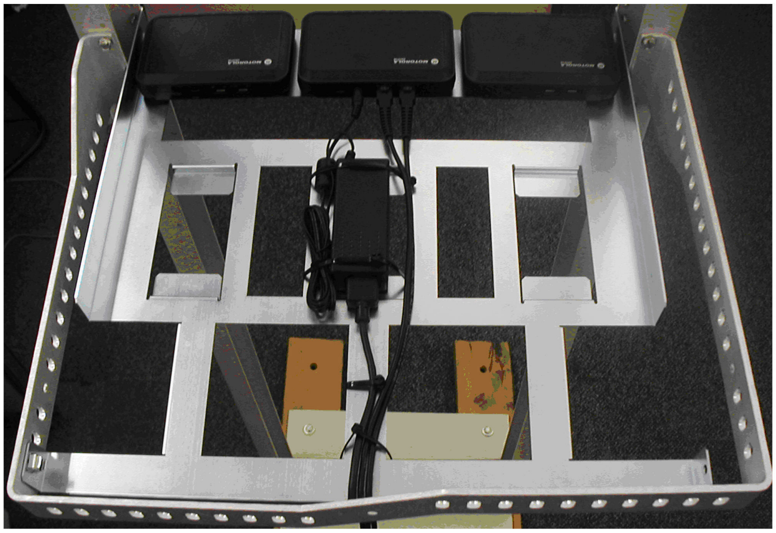
B_IPCryptR_Rack_Mount_Rear_View

Figure 6: Rear View of PDEG Encryption Unit in Open Rack Mount



B_IPCryptR_Rack_Mount_Front_View

Figure 7: Overhead View of PDEG Encryption Unit in Open Rack Mount



B_IPCryptR_Rack_Mount_From_Above

3.3.2 Desk Mount

Secure the PDEG Encryption Unit to the desk with a mounting plate, as shown in the following figures.

Figure 8: PDEG Encryption Unit with Mounting Plate

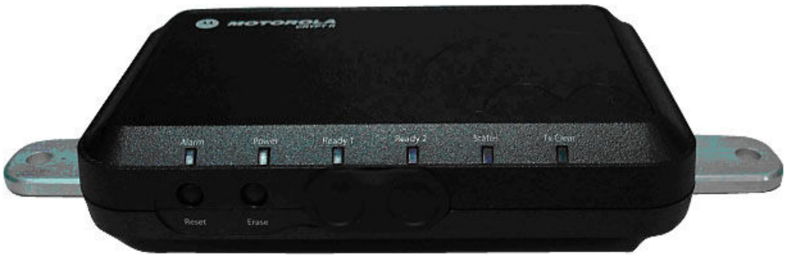
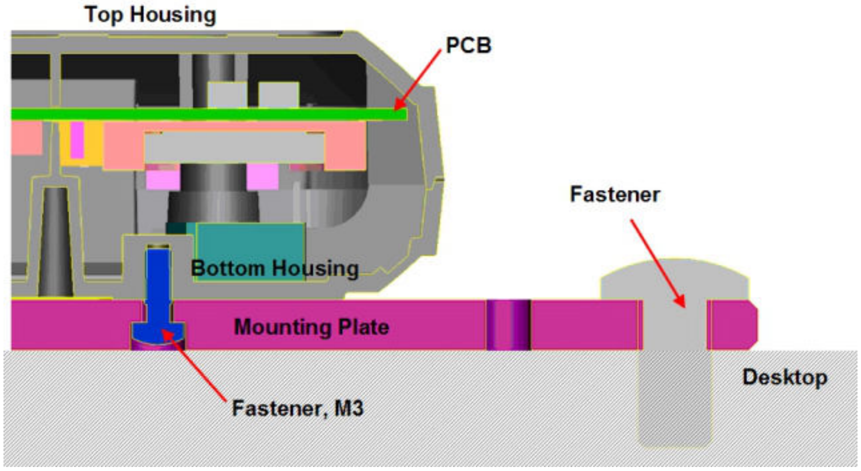


Figure 9: Mounting for Single PDEG Encryption Unit

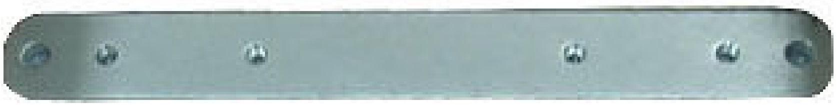


3.3.2.1

Mounting Plate

The PDEG Encryption Unit package has a mounting plate, shown in the following figure. The mounting plate allows modular installation and allows a PDEG Encryption Unit to be installed on a desk.

Figure 10: PDEG Encryption Unit Mounting Plate



3.3.2.2

Cable Retention Bracket

A retention bracket prevents the accidental loosening of a cable connection. It can be provided for desktop mounting. The cable retention bracket is mounted between the PDEG Encryption Unit and the table mounting plate. See the following figures for installation guidelines.

Figure 11: Cable Retention Bracket Mounting

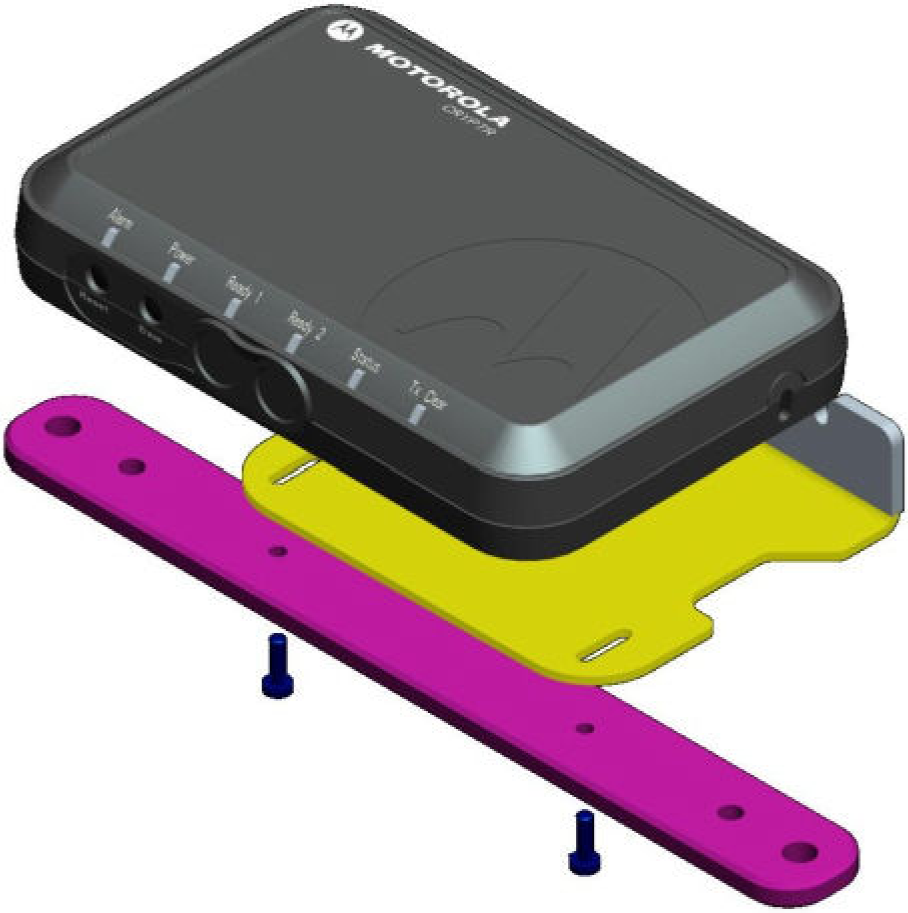
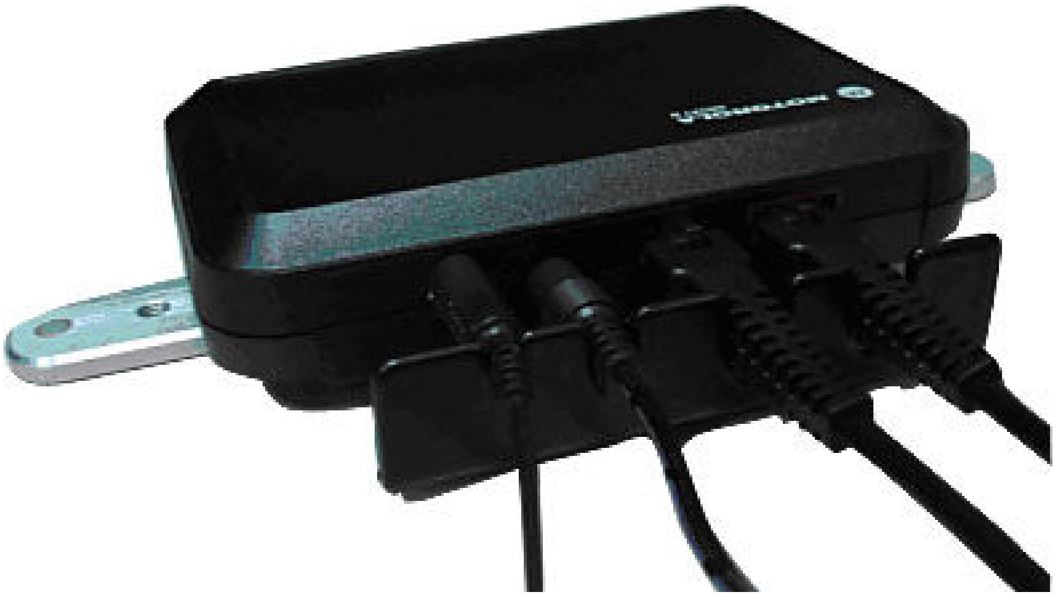


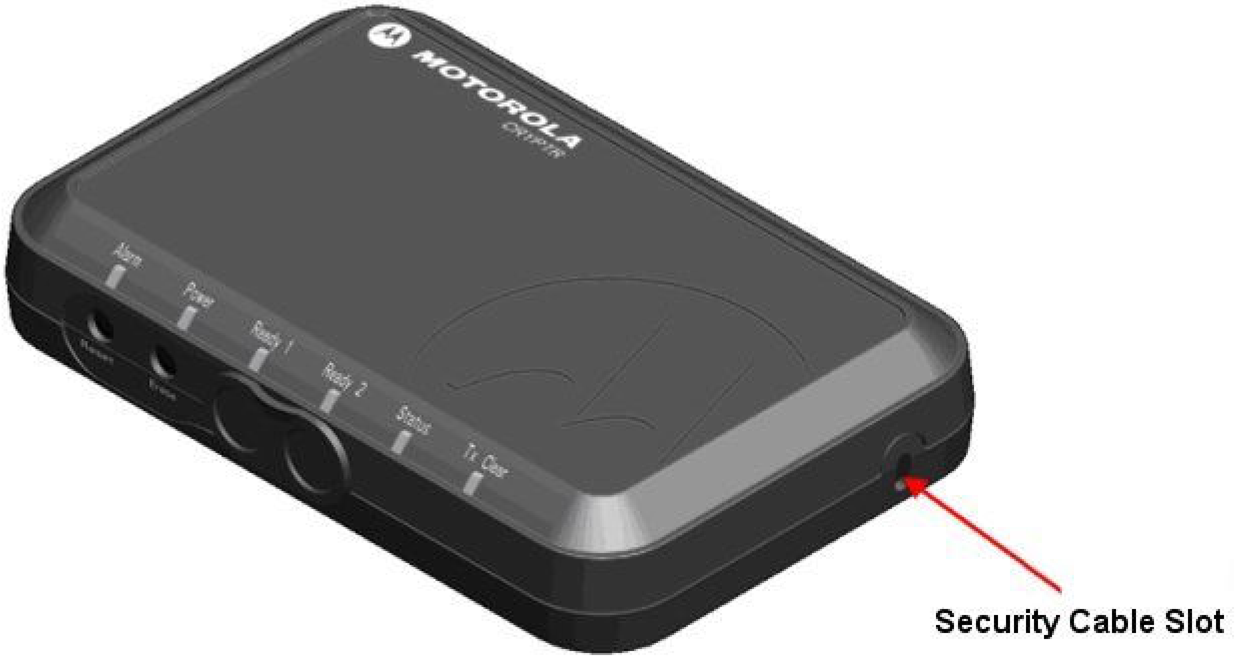
Figure 12: Cable Retention Bracket Rear View



3.3.2.3 Cable Lock

The PDEG Encryption Unit has a security cable slot, compatible with most standard computer security cables.

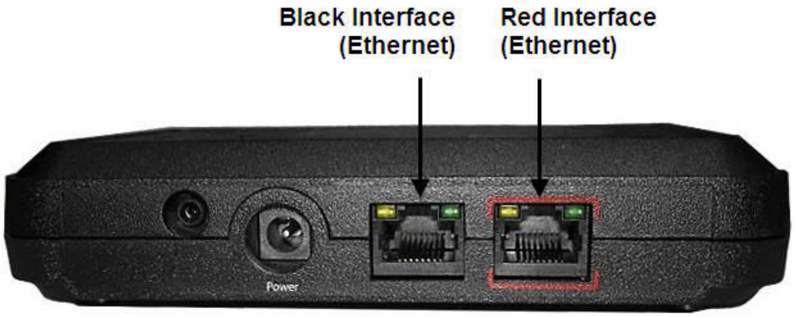
Figure 13: PDEG Encryption Unit Security Cable Slot



3.4 Attaching Ethernet Cables to the PDEG Encryption Unit

Both the red and black Ethernet ports on the PDEG Encryption Unit must be connected with Ethernet cables, as shown in the following figure.

Figure 14: Ethernet Connections on the PDEG Encryption Unit



3.4.1 Wiring for Infrastructure Configuration

Powering of the PDEG Encryption Unit in the infrastructure environment requires no third party conditioning/ filtering devices. All that is needed is the supplied AC/DC converter cable. For ordering information, contact your Motorola Solutions representative.

3.4.1.1 Power Configuration

Table 7: Desktop Power Configuration

AC Source	Power Cable
100–240 V at 50/60 Hz	0171925M01

3.4.1.2 Wiring for Setup

Table 8: Communication Wiring for Desktop/Rackmount Setup

Desktop Cable	Function	Port on PDEG Encryption Unit
RS232 cable (part number DLN6693A)	Loading IP information	Red RS232/Keyload Port
Key load cable (kit number TKN8531C)	Key loading	

3.4.1.3 Wiring for Operation

Table 9: Communication Wiring for Desktop/Rackmount Operation

Device	Cable	Port on PDEG Encryption Unit
PC	Crossover Ethernet cable (part number 3071813M02)	Red Ethernet port
Remote device	Either straight Ethernet cable (part number 3071813M01) or Crossover Ethernet cable (part number 3071813M02), depending on the configuration	Black Ethernet port

Chapter 4

PDEG Encryption Unit Configuration

This chapter describes an example of how the Encrypted Integrated Data (EID) feature should be designed and configured, thus it should be read as a guideline. Consider your own setup when deploying this feature. It is possible for the proposed solution to be further customized, depending on your specific needs.

4.1 Initiating a Serial Shell Connection

The PDEG Encryption Unit software monitors its serial port for a connection. To connect to the PDEG Encryption Unit, use a laptop computer running a terminal emulator application and a serial cable.

Prerequisites:

Ensure that a terminal emulator application is installed on your laptop.

Obtain an RS232 cable with a Hirose round connector and a DB-9 connector used to connect to the laptop. See Table 1: Major Components of the PDEG Encryption Unit on page 14.

If necessary, obtain a secure password from Motorola Solutions.

Procedure:

1. Connect the PDEG Encryption Unit via the serial cable to the laptop computer and start a terminal emulation session on that computer with the following session parameters:
   - Baud rate: 9600
   - Parity: none
   - Data bits: 8
   - Stop bits: 1
   - Flow control: none
2. Perform one of the following actions:
   - If the PDEG Encryption Unit is already initialized when the terminal emulation session is started, press ENTER to notify the PDEG Encryption Unit of the connection.
   - If the PDEG Encryption Unit is powered up after the terminal emulation session is started, go to step 3.
3. Type your login name and password.

   Ten consecutive unsuccessful attempts to log on are considered tampering with the PDEG Encryption Unit. If the PDEG Encryption Unit detects tampering, it erases the pre-shared key, erases the user password, restores the default password, and must be power-cycled.

   The PDEG does not allow any other commands until the login and the password are verified.
4. Change the password after logging on for the first time.

   A password change from the default password will be required for the first login. The new password cannot be one of the last five previous passwords, must be 15 or 16 characters long, and contain three of the following four attributes:
   - At least one upper case letter
   - At least one lower case letter
   - At least one number

- At least one special character (!@#$^&*()-/?,.=+)

4.2 Logon Session and User Authentication

After verifying the logon name and password, the PDEG Encryption Unit displays the following command prompt: `ASTRO PDEG>`

The PDEG Encryption Unit displays the command prompt after each successful or unsuccessful command, until you log out.

Table 10: Logon Session Commands

Command	Description
`exit`	This command causes the PDEG Encryption Unit to display the logon prompt. No other command is allowed until the user authenticates with a username and password again.
`passwd`	This command causes the PDEG Encryption Unit to prompt the user for the existing password and then for a new password. If the previous password is entered correctly, the new password is stored within the PDEG Encryption Unit and retained even when the PDEG Encryption Unit is powered down and restarted. ● If the password is not entered correctly, the PDEG Encryption Unit displays the error message and returns to the prompt. No changes to the stored password are made in this case. ● If the PDEG Encryption Unit detects no user activity for 10 minutes during a logon session, the PDEG Encryption Unit terminates the logon session and prompts for username and password. ● Removing the battery from the PDEG Encryption Unit does not reset the password and must be done explicitly with 10 failed logon attempts.
`banner`	This command changes the text of the logon banner. The maximum length of banner text is 274 characters, including white space. A maximum of 80 characters is recommended for proper display. ● Use `\n\r` (line feed, carriage return) for new lines if needed. You can escape `\n` and `\r` in the serial shell by pressing the Esc key and then sending the appropriate carriage return or line feed character. This can require a SHIFT + ENTER or CTRL + ENTER, depending on your operating system and terminal emulation program. ● Customizing the banner overwrites the default banner permanently. The only way to restore the default banner, if necessary, is to manually enter the default banner text: `Use of this device and any related service is your consent to all associated terms, conditions, including consent to monitoring and disclosure provisions.`

4.3

Configuring the PDEG Encryption Unit for Encrypted Integrated Data

The configuration process is an important stage that consists of many procedures. This process is also the most flexible. Configuration details can differ depending on the required setup.

Process:

1. If your system includes a Key Management Facility (KMF) for centralized key management, configure the KMF for the Encrypted Integrated Data (EID) feature.

   See “Configuring the KMF for Encrypted Integrated Data” in the *Key Management Facility User Guide*.
2. Set up a serial connection for the PDEG Encryption Unit.

   See Setting Up a Serial Connection for the PDEG Encryption Unit on page 30.
3. Assign IP addresses for the PDEG Encryption Unit.

   See Assigning IP Addresses for the PDEG Encryption Unit on page 31.
4. Load encryption keys to the PDEG Encryption Unit.

   See Loading Encryption Keys to the PDEG Encryption Unit on page 32.
5. If your system includes a KMF, configure each PDEG Encryption Unit for Over The Ethernet Keying (OTEK).

   See Configuring the PDEG Encryption Unit for OTEK on page 32.
6. If your system includes optional syslog for the Customer Enterprise Network (CEN), configure each PDEG Encryption Unit for syslog.

   See Configuring the PDEG Encryption Unit for Syslog on page 34.
7. If your system includes redundant PDEG Encryption Units, configure each unit for redundancy using Virtual Router Redundancy Protocol (VRRP).

   See Configuring PDEG Encryption Units for Redundancy on page 35.
8. Configure the associations and rules for each PDEG Encryption Unit.

   See Configuring Associations and Rules on page 38.
9. If your system includes a KMF, then set OTAR parameters for PDEG Encryption Unit for centralized key management. See the documentation for your KVL model.
10. Connect each PDEG Encryption Unit to the system.

    See Connecting the PDEG Encryption Unit to the System on page 38.

4.3.1

Setting Up a Serial Connection for the PDEG Encryption Unit

Perform this procedure on a service laptop, on which PuTTY, HyperTerminal, or another terminal emulator tool is installed.

Procedure:

1. Connect the serial cable (PN CLN8521A/3000925001) to the front red port of the PDEG Encryption Unit and to an RS232 or USB port of the service laptop.
2. Open a terminal emulator software (such as PuTTY or HyperTerminal) on the service laptop.

Postrequisites: Continue to Assigning IP Addresses for the PDEG Encryption Unit on page 31.

4.3.2 Assigning IP Addresses for the PDEG Encryption Unit

This procedure describes how to assign IP addresses for the PDEG Encryption Unit by using the `cryptrconfig` command.

As an alternative, you can assign IP addresses by using the `ifconfig` command. For more information, see Alternate Configuration Command Mode on page 39.

Procedure:

1. Log on to the PDEG Encryption Unit.
2. At the prompt, enter: `cryptrconfig`
3. Enter the black (public network) IP address:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.
4. Enter the black subnet mask:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.
5. Enter the black default gateway:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.
6. Enter the red (trusted network) IP address:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.
7. Enter the red subnet mask:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.
8. Enter the red default gateway:
   - To accept the IP address displayed, press ENTER.
   - To specify a different IP address, enter the address at the prompt.

   A message appears confirming the changes to the CRYPTR configuration.
9. **NOTE:** PDEG allows for up to 5 static Address Resolution Protocol (ARP) entries. Enter `none` for any that are not being used.

   Optional: Enter static ARPs in the following order:

   a. ARP1

   b. ARP2

   c. ARP3

   d. ARP4

   e. ARP5

   - To accept the static ARP entry, press ENTER.
   - To clear the static ARP entry, enter: `none`
   - To specify a different static ARP entry, enter: *`<IP Address>`*, *`<delimited MAC Address>`*

For example: `10.2.32.134,12:34:56:78:9A:BC`

NOTE: For systems with a geo or local redundant IMW, enter the *<IP Address>* and *<MAC Address>* of the IMW's virtual address. The IMW uses Windows load balancing which has special ARP requirements.

Postrequisites: Continue to Loading Encryption Keys to the PDEG Encryption Unit on page 32.

4.3.3 Loading Encryption Keys to the PDEG Encryption Unit

Use the Key Variable Loader (KVL) to load keys to the PDEG Encryption Unit for the first time, by performing the Store and Forward operation. Subsequent key loads can use Over-The-Ethernet Keying (OTEK).

When and where to use: Load the keys before you configure the associations.

Procedure:

1. Disconnect the serial cable and connect the KVL to the front red port. Load the initial encryption key (KEK).

   For more information, see the documentation for your KVL model.
2. Connect the serial configuration cable back to the PDEG Encryption Unit. See Setting Up a Serial Connection for the PDEG Encryption Unit on page 30.

Postrequisites: Continue to Configuring the PDEG Encryption Unit for OTEK on page 32.

4.3.4 Configuring the PDEG Encryption Unit for OTEK

If your system includes a Key Management Facility (KMF) for centralized key management, configure each PDEG Encryption Unit for Over-The-Ethernet Keying (OTEK).

This procedure describes how to configure the PDEG Encryption Unit for OTEK by using the `otekconfig` command.

IMPORTANT:

Prerequisites:
Contact your system administrator for information regarding IP addresses.

IMPORTANT:
Port numbers can be fixed values. Do **not** change port numbers without consulting your system administrator.

Procedure:

1. Log on to the PDEG Encryption Unit.
2. At the prompt, enter: `otekconfig`
3. At the `Enable OTEK Interface` prompt, perform one of the following actions:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
4. Enter the KMF network:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.

5. Enter the KMF IP address:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
6. Enter the KMF port number:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.

   IMPORTANT: The KMF port number value in the PDEG Encryption Unit must match the trunking system **Listening port** number value in the KMF. Do not assign the **OTEK Device Listening Port** number.
7. Enter the Tx security level:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
8. Enter the Rx security level:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
9. Enter the KMF inactivity timeout in hours:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
10. Enter the KMF registration delay in seconds:
    - To accept the value displayed, press ENTER.
    - To specify a different value, enter the value at the prompt.

    If any values were changed, a message confirming the changes appears. If no values were changed, a message appears confirming that the OTEK configuration is unchanged.

Postrequisites: Continue to Configuring the PDEG Encryption Unit for Syslog on page 34.

4.3.5 Syslog Levels

The syslog is a useful tool for monitoring the status of the PDEG Encryption Unit. Syslog configuration defines where syslog messages are sent and what level they have. The following list describes the syslog levels:

0 Emergency
System is unusable.

1 Alert
Action must be taken immediately.

2 Critical
Critical conditions.

3 Error
Error conditions.

4 Warning
Warning conditions.

5 Notice
Normal but significant condition.

6 Informational

Informational messages.

7 Debug

Debug-level messages.

4.3.6 Configuring the PDEG Encryption Unit for Syslog

If your system includes the optional syslog for the Customer Enterprise Network (CEN), configure the PDEG Encryption Unit for syslog.

This procedure describes how to configure the PDEG Encryption Unit for syslog by using the `sysconfig` command.

Procedure:

1. Log on to the PDEG Encryption Unit.
2. At the prompt, enter: `sysconfig`
3. At the `Enable Syslog Interface` prompt, perform one of the following actions:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
4. Enter the syslog network:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
5. Enter the syslog IP address:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
6. Enter the syslog port number:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
7. Enter the syslog level:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.

   If any values were changed, a message confirming the changes appears. If no values were changed, a message appears confirming that the syslog configuration is unchanged.

Postrequisites: Continue to Configuring PDEG Encryption Units for Redundancy on page 35.

4.3.7 Configuring PDEG Encryption Units for Redundancy

If your system includes redundant PDEG Encryption Units, configure each unit for redundancy using Virtual Router Redundancy Protocol (VRRP). Perform this procedure on each unit individually.

NOTE:
In a redundancy configuration, the primary PDEG Encryption Unit receives data by default. The non-primary unit receives data only if and when the primary unit fails to respond to messages verifying its availability. If the primary unit is disconnected from the system, the non-primary unit takes over processing of data after a delay of up to three seconds.

Transfers of function between primary and non-primary units occur automatically and no user action is required to initiate the switchover:

- The primary and non-primary units must be assigned the same VRRP IDs.
- Multiple groups of redundant PDEG Encryption Units are allowed. Each pair must have a unique Black and Red VRRP ID.
- If the VRRP IDs do not match, the non-primary unit takes up to 15 seconds to come up.

IMPORTANT: When configuring PDEG Encryption Unit using the Virtual Router Redundancy Protocol (VRRP), explicit protocols must be used in all security associations. The `ANY` option cannot be used (TCP, UDP, ICMP, etc., must be assigned their own associations.)

Procedure:

1. Log on to the PDEG Encryption Unit.
2. At the prompt, enter: `vrrpconfig`
3. At the `Enable VRRP Function` prompt, perform one of the following actions:
   - To accept the value displayed, press ENTER.
   - To specify a different value, enter the value at the prompt.
4. Enter the VRRP priority:
   - To designate this PDEG Encryption Unit as the primary unit, enter: `255`
   - To designate this PDEG Encryption Unit as a non-primary unit, enter any integer less than 255.
5. Enter the black VRRP IP address:
   - To accept the default IP address for the PDEG Encryption Unit on the black subnet, press ENTER.
   - To specify a different IP address, enter the desired address at the prompt.
6. Enter the black VRRP ID:
   - To accept the default device ID for the PDEG Encryption Unit on the black subnet, press ENTER.
   - To specify a different device ID, enter the device ID at the prompt.

   IMPORTANT: The black VRRP ID must be the same for the primary and non-primary PDEG Encryption Unit pair.
7. Enter the red VRRP IP address:
   - To accept default IP address for the PDEG Encryption Unit on the red subnet, press ENTER.
   - To specify a different IP address, enter the desired address at the prompt.
8. Enter the red VRRP ID:
   - To accept the default device ID for the PDEG Encryption Unit on the red subnet, press ENTER.

- To specify a different device ID, enter the device ID at the prompt.

IMPORTANT: The red VRRP ID must be the same for the primary and non-primary PDEG Encryption Unit pair. It is recommended that the red VRRP ID and black VRRP ID **not** use the same values.

If any values were changed, a message confirming the changes appears. If no values were changed, a message appears confirming that the VRRP configuration is unchanged.

Postrequisites:
Verify that redundancy configuration is functioning successfully. See Verifying Redundancy Configuration on page 47.

Continue to Configuring Associations and Rules on page 38.

4.3.8 Associations and Rules

Review this information before you configure associations between local and remote hosts in the PDEG Encryption Unit.

Association Command

Associations between local and remote hosts in the PDEG Encryption Unit are configured by using the `association` command. For guidance on the proper use of this command, contact your system administrator.

When executed, this command must include one of the following options:

`flush`
Starts a configuration session.

`add`
Adds an association and includes the following rules: *`<source IP address><destination IP address><remote IP address><protocol><action><direction><CKR>`*

`show active`
Displays the active configuration data.

`show new`
Displays the recently entered configuration data.

`show protocols`
Displays the list of available transport protocols.

`commit`
Reconfigures the PDEG with the already entered configuration data.

Associations include the following rules:

`<source IP address>`
The IPv4 address of the local end of the association.

`<destination IP address>`
The IPv4 address of the remote end of the association. For incoming security associations, the destination IP address of the endpoint device, that is the device receiving data from the red side of the PDEG Encryption Unit. For outgoing associations, the IP address of the subscriber or device receiving messaging in the Radio Network Interface (RNI).

<remote IP address>
The IPv4 address of the PDEG Encryption Unit from which a connection is accepted. For incoming security associations, the black IP address of the PDEG Encryption Unit. For outgoing associations, the IP address of the subscriber or device receiving messaging in the RNI.

<protocol>
The protocol that this rule acts on. The protocol is specified by ID (1-255) or name (for example, TCP).

<action>
The action to apply to the association (bypass, process, process_bypass, or discard). When configuring outgoing bypass rules with a remote IP address field value that is not on the same subnet as the PDEG Encryption Unit black network interface, the protocol (for example, TCP, UDP) must also be explicitly specified. Using `any`, does not allow packets to be bypassed. The `process_bypass` action will cause encrypted packets to be processed and non-encrypted packets to be bypassed. The `process_bypass` action is only valid for messages going in the black to red direction.

<direction>
The direction of flow (incoming or outgoing). Incoming messages are messages received at the black port of the PDEG Encryption Unit. Outgoing messages are messages received at the red port of the PDEG Encryption Unit.

<CKR>
The common key reference. Blank if action is bypass or discard.

Overlapping 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 another data association or that policy selectors can also apply to another data association. For example, an overlap exists when two data associations 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.

IMPORTANT:
To prevent overlapping data associations, use selectors that do not make the data associations overlap. If an unavoidable need to overlap data associations arises, contact the Centralized Managed Support Operations (CMSO) for assistance.

For example, to send data to the same subnet, such as a subscriber subnet, but with a different data association policy (process as opposed to bypass), make the source IP address specific and different between the two data associations. For example, use two different CEN host server IP addresses.

Another example concerns sending 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 bypass of broadcast data by placing broadcast data addresses in a different subnet than the subscriber destination subnet.

IMPORTANT: If the PDEG Encryption Unit is configured with an association with a most restricted rule combined with associations using the `any` rule and the same IP/subnet, the `any` rule is ignored. As a result, messages related to these associations are dropped instead of being subject to a more general rule.

If you set up the association rules as shown in the following example, the PDEG Encryption Unit only processes encrypted TCP messages on these IP configurations and all other protocol messages are dropped. The `any` rule used to generalize the behavior of all other protocols does not work.

```
association add 10.71.1.4/32 10.51.1.0/24 10.51.11.133 TCP process incoming 1
association add 10.71.1.4/32 10.51.1.0/24 10.51.11.133 any bypass incoming
```

Instead of using any protocol, you have to add a specific protocol for each association that requires it, as shown in the following example:

```
association add 10.71.1.4/32 10.51.1.0/24 10.51.11.133 TCP process incoming 1
association add 10.71.1.4/32 10.51.1.0/24 10.51.11.133 UDP bypass incoming
```

IMPORTANT: When configuring PDEG Encryption Unit using the Virtual Router Redundancy Protocol (VRRP), explicit protocols must be used in all security associations. The `ANY` option cannot be used (TCP, UDP, ICMP, etc., must be assigned their own associations.)

4.3.9

Configuring Associations and Rules

This procedure describes how to set up associations between local and remote hosts in the PDEG Encryption Unit by using the `association` command.

Prerequisites: Review the information about associations and rules. See Associations and Rules on page 36.

Procedure:

1. Log on to the PDEG Encryption Unit.
2. Enter: `association flush` to start a configuration session.
3. Enter: `association commit` to save the change made in step 2.
4. To add an association, enter:

   ```
   association add <source IP address><destination IP address><remote IP address><protocol><action><direction><CKR>
   ```

   The address fields can be appended with / *<XX>* where *<XX>* is a number ranging from zero to 32. This number is shorthand for a netmask.
5. To verify the added associations, enter: `association show new`

   The values for the newly added associations are displayed.
6. Repeat step 4 and step 5 for each association until all necessary associations are added.
7. To finish the configuration session, enter: `association commit`

   A message confirming the changes appears.

Postrequisites: Continue to Configuring the PDEG Encryption Unit for OTEK on page 32.

4.3.10

Connecting the PDEG Encryption Unit to the System

Prerequisites:

Ensure that all the necessary equipment in the black Customer Enterprise Network (CEN) and red CEN is properly configured.

If the PDEG Encryption Unit is deployed but not configured, there is no traffic to and from the red CEN.

Procedure:

1. Connect the Ethernet cables to the PDEG Encryption Unit. See Attaching Ethernet Cables to the PDEG Encryption Unit on page 26.

   Use straight or crossover Ethernet cables, depending on your installation.
2. Verify that PDEG Encryption Unit is properly connected to the system:
   a. Verify that the PDEG Encryption Unit can successfully communicate with KMF.
   b. Verify that the PDEG Encryption Unit can send logs to the logging server.
   c. Verify that the PDEG Encryption Unit can be reached from the red side by all intended hosts.

4.4 Alternate Configuration Command Mode

As an alternative, if the prompt mode configuration is unavailable, you can configure the PDEG Encryption Unit by using the `ifconf` command.

This command is used to configure both the Black and Red MACE interfaces. The command has the following syntax:

```
ifconf <MACE> <IP_Address> <Subnet_Mask> <Default_Gateway> <MTU> <ARP1> <ARP2> <ARP3>
<ARP4> <ARP5>
```

The following list describes the parameters for this command:

<MACE>
The available values are black or red.

<IP_Address>
The IP address of the specified MACE's interface.

<Subnet_Mask>
The subnet mask (typically 255.255.255.0).

<Default_Gateway>
The IP address of the default gateway.

<MTU>
The Maximum Transfer Unit (MTU) for this interface.

<ARP1> to *<ARP5>*
The static Address Resolution Protocol (ARP) in the format of *<IP Address>*, *<delimited MAC Address>*

For example, `192.168.0.100,12:34:56:78:90:AB`

PDEG allows for up to 5 static ARP entries. Enter `none` for any that are not being used.

Chapter 5

PDEG Encryption Unit Operation

This chapter describes operation of the PDEG Encryption Unit after it is installed and configured.

IMPORTANT:
If your system includes a Key Management Facility (KMF) for centralized key management, see the *Key Management Facility User Guide* for instructions on centralized key management using the KMF.

Otherwise, follow procedures in this section for manual key management using the Key Variable Loader (KVL). For more information, see the documentation for your KVL model.

5.1 Administering Keys on the KVL

For details on how to enter, edit, and delete encryption keys on the Key Variable Loader (KVL), see the documentation for your KVL model.

5.2 Managing Keys on the PDEG Encryption Unit

Keys that have been entered manually into the Key Variable Loader (KVL) can be loaded manually into the PDEG Encryption Unit or other target device. This method of key loading is typically used when a centralized key management facility (KMF) is not installed to manage keys, or when a device (such as a PDEG Encryption Unit) is not yet connected to a KMF.

If you do not have a KMF, track the keys loaded into devices on your system manually. The KVL includes log records that can be loaded to a PC to help you account for your key loading activity.

For instruction on loading and removing keys from target devices (PDEG), see the documentation for your KVL model.

5.2.1 Rotating Keysets

The PDEG Encryption Unit, like any device managed by a KMF in a system with centralized key management, has two keysets:

- Keyset 1, the active set, which the device uses to encrypt data before transmission
- Keyset 2, the inactive keyset

New keys are loaded into the inactive keyset so they do not interfere with communications using the active keyset while the keys are being sent (because rekeying multiple devices takes time). When all new keys have been delivered to all devices, the inactive keyset is ready for use. The devices active and inactive keyset can then be switched (which again with multiple devices takes time). While the switch is being distributed, devices have the same keys (new and previous) and use which ever keyset is active. When the switch is complete, all managed devices use the newly active keyset for communication. This process is known as keyset changeover.

Since switching can take time, the devices can decrypt data that comes from devices that have already switched and from devices that have not switched yet. For example:

- Radio 1 transmits with Keyset 1 (not switched over yet).
- Radio 2 transmits with Keyset 2 (it has already switched).

- Radio 3 can decrypt messages from both (no matter which keyset is active on Radio 3), because it has both sets of keys.

Chapter 6

PDEG Encryption Unit Maintenance

This chapter provides maintenance steps for the PDEG Encryption Unit.

6.1 Replacing Batteries in the PDEG Encryption Unit

When and where to use: The battery in the PDEG Encryption Unit is included for infinite key retention. The battery only needs replacement if the Status LED indicates that the battery is Low. See Interpreting Status Indicators on page 45 for details.

IMPORTANT:

A PDEG with a dead or missing battery will only retain its encryption keys for about one minute if the PDEG is not connected to power.

The battery replacement procedure below requires that the PDEG's bottom cover be removed. This action will activate the internal tamper mechanism, and all encryption keys will be erased. Be prepared to restore encryption keys using a KVL and/or a KMF.

Procedure:

1. Power down the PDEG Encryption Unit and remove the Ethernet cable.
2. Unscrew the four screws of the bottom cover to open the PDEG Encryption Unit.
3. Remove the existing coin-type battery using a small screwdriver to gently pry the battery out of the holder.
4. Insert a new +3.0 V lithium battery (DL2032) in the battery holder with the “+” side facing up.
5. Assemble to PDEG Encryption Unit bottom cover again.
6. Reconnect the Ethernet cable to the PDEG Encryption Unit, and power up the PDEG Encryption Unit.
7. Verify that the device powers up normally. The status LED will be yellow, indicating there are no encryption keys, due to the removal of the PDEG's bottom cover.
8. Load keys as described in PDEG Encryption Unit Configuration on page 28.

6.2 Upgrading PDEG Software or Algorithms

Use the KVL to upgrade the PDEG software or algorithms. See the documentation for your KVL model.

IMPORTANT:

With the new FIPS 140-3 certificate implementation, it is recommended to upgrade the Black processor first, then proceed to upgrade the Red processor.

In the case when PDEG Red processor has been upgraded first, and the KVL does not establish connection on the Black processor, press **Reset** button and wait 10 seconds for PDEG to establish a connection with the KVL. If the connection was still not established, press **Reset** button again.

NOTE:

The ASTRO PDEG upgrade procedure includes steps for upgrading both the Red and Black processors. It is important to complete both steps before attempting to bring the ASTRO PDEG back into service. A partially upgraded ASTRO PDEG may trigger an alarm during the power-up.

A PDEG downgrade to R02.05.02 or earlier firmware from R02.07.00 or later is only supported using the FIPS 140-3 certified KVL 5000.

WARNING: Do **not** attempt to downgrade from R03.01.01 or later to R02.07.05 or earlier. To perform such a downgrade, contact Centralized Managed Support Operations (CMSO).

After a downgrade of this type, the internal setting preventing Pre-FIPS-140-3 certified software from functioning with the upgraded internal database must be reset. See Resetting Internal Settings After Downgrade on page 43.

6.3 Resetting Internal Settings After Downgrade

IMPORTANT: A PDEG downgrade to R02.05.02 or earlier firmware from R02.07.00 or later is only supported by using the FIPS 140-3 certified KVL 5000. After such a downgrade, you must reset internal settings which prevent Pre-FIPS-140-3 certified software from functioning with the upgraded internal database. The procedure erases all keys and restores the default PDEG password.

Procedure:

1. Remove network cables and power cycle the PDEG.
2. Log on to the PDEG Shell.
3. Enter: `fips`
4. Note the `Encrypted only keyfill` configuration.

   It can be either `Enabled` or `Disabled`.
5. Toggle the FIPS setting by performing one of the following actions:
   - If the setting is `Disabled`, enter: `fips Enable`.
   - If the setting is `Enabled`, enter: `fips Disable`.
6. Restart the PDEG.
7. Log on the PDEG Shell with the default password.
8. Restore FIPS settings to the setting noted in step 4 by performing one of the following actions:
   - If the setting was Enabled, enter: `fips Enable`
   - If the setting was Disabled, enter:`fips Disable`
9. Restart the PDEG.

10. Log on to the PDEG Shell with the default password.
11. Change the default password.
12. Reconnect the network cables and reload any keys that were erased.

6.4 Cryptographic Algorithm Self-Test

The ASTRO PDEG offers the user the ability to execute the Cryptographic Algorithm Self-Test. This test exercises the cryptographic algorithms to ensure correct operation.

This test, as was written above, can be executed on demand, or configured for automatic periodic execution. Periodic self-testing should be disabled during normal operation. On-demand self-testing should only be executed during PDEG maintenance. Periodic self-testing is disabled by default.

For On-Demand Testing, you must use the `kat run` command.

To configure periodic test execution, you must use `kat configure` *`<0-720>`* where *`<1-720>`* indicates the number of hours between the scheduled tests. `0` indicates that periodic tests are disabled.

Chapter 7

PDEG Encryption Unit Troubleshooting

This chapter provides troubleshooting procedures for the PDEG Encryption Unit.

7.1 Interpreting Status Indicators

The set of Light Emitting Diodes (LEDs) on the front of the PDEG Encryption Unit indicate its status. See Figure 1: PDEG Encryption Unit Front View on page 15 and Figure 2: PDEG Encryption Unit Rear View on page 15 to view LED locations on the PDEG Encryption Unit.

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

Table 11: Front Panel LED Indicators

Item	LED	Status Description	User Action
1	Alarm	**Red** = a security alarm or fatal error detected	Use the `error_log` command to display volatile (severe) and non-volatile (debug information) errors that occurred. Volatile errors are stored in RAM and are erased if the PDEG Encryption Unit is power cycled. Non-volatile errors are stored in flash memory and are not erased if the PDEG Encryption Unit is power cycled. **NOTE:** To debug the errors, provide the software version number and the output from the command to the Centralized Managed Support Operations (CMSO).
2	Power	**Green** = LED lights when main power is supplied to the PDEG Encryption Unit. The battery in the PDEG Encryption Unit has no impact on this LED.	N/A
3	Ready 1	**Green** = the PDEG Encryption Unit is ready to communicate with a Key Variable Loader (KVL) on the black side.	N/A
4	Ready 2	**Green** = the PDEG Encryption Unit is ready to communicate with a KVL on the red side.	N/A
5	Tx Clear	**Yellow** = Outgoing bypass rules are set.	N/A
6	Status	**Green** = normal operation, good battery **Yellow** = no encryption keys, good battery	If the status LED is Yellow, encryption keys need to be reloaded.

Item	LED	Status Description	User Action
		Red = low or dead battery regardless of status	If the status LED is Red, the battery must be replaced. **NOTE:** For information related to key retention and battery replacement, see Replacing Batteries in the PDEG Encryption Unit on page 42.
7	Ethernet (2 LEDs)	**Green LED** displays link and activity. ● ON – Ethernet physical link established ● OFF – no link ● Flashing – link established, activity indicated by flashing off **Orange LED** displays 10/100 Mbit link status. ● ON – 100 Mbit ● OFF – 10 Mbit	N/A

7.2

Repairing a Connection

Repairing a connection can help in debugging or re-establishing a lost connection.

Procedure:

1. From the **Windows Control Panel**, open the **Network Connections** window.
2. In the **Network Connections** window, right-click the LAN connection that is connected to the red subnet of the PDEG Encryption Unit.
3. In the pop-up menu, click **Repair**.

   The repair service runs, terminating with a status message.

7.3

Troubleshooting Administrative Login Issues

- **Problem:** Unable to log on to the PDEG Encryption Unit Admin Account
- **Recovery Action:** 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 Centralized Managed Support Operations (CMSO) for assistance. You must re-configure the PDEG Encryption Unit. See PDEG Encryption Unit Configuration on page 28, for configuration procedures.

7.4 Verifying Redundancy Configuration

Procedure:

1. Initiate data traffic on a system configured with primary and non-primary PDEG Encryption Units.
2. Disconnect any of the following from a PDEG Encryption Unit that is configured as the primary unit:
   - Red Ethernet cable
   - Black Ethernet cable
   - Power cable
3. Wait for three seconds.

   If the redundancy configuration is functioning successfully, then the switchover from the primary unit to a non-primary unit occurs automatically.
4. Verify that the non-primary unit (or one of the non-primary units if the system is configured with more than one non-primary unit) is processing data.
5. Verify that the security associations are entered using explicit protocols (TCP, UDP, etc.) and that no `ALL` associations are entered.

   IMPORTANT: When configuring PDEG Encryption Unit using the Virtual Router Redundancy Protocol (VRRP), explicit protocols must be used in all security associations. The `ANY` option cannot be used (TCP, UDP, ICMP, etc., must be assigned their own associations.)

Chapter 8

PDEG Encryption Unit FRU/FRE Information

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) applicable to the PDEG Encryption Unit.

The PDEG Encryption Unit is considered a Field Replaceable Unit (FRU), 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. The faulty PDEG Encryption Unit must then be shipped to the Motorola for further troubleshooting and repair.

The following ordering guidelines apply to the PDEG Encryption Unit:

- Order one TKN9282A Rack Mount Plate for every three Rackmount Version PDEG units to be installed in a rack or cabinet.
- Order one TKN9283A Rack Mount Bracket for every six Rackmount Version PDEG units to be installed in open racks.
- Order at least one DLN6693A, RS232 Cable for programming the PDEG units (utilizing a standard PC, not included).
- Order at least one TKN8531C Key load Cable for loading encryption keys on PDEG units (utilizing the KVL).

IMPORTANT: A second unit should be ordered if redundancy is a requirement.

8.1 Hardware for the PDEG Encryption Unit

Table 12: PDEG Encryption Unit Hardware

Part Number	Description
T7539A	PDEG Encryption Unit Hardware
DLN6693A	RS232 Cable (must select at least one with the Encrypted Integrated Data Hardware Box)

8.2 Software for the PDEG Encryption Unit

Table 13: PDEG Encryption Unit Software

Part Number	Description
CA00182AC	AES Algorithm Kit (required)
CA01483AA	ASTRO® 25 Encrypted Integrated Data Operation (required)

8.3 Accessories for the PDEG Encryption Unit

Table 14: PDEG Encryption Unit Accessories

Part Number	Description
TKN8531C	Cable for RNC, DIU
TKN9282A	Rack Support Bracket
TKN9283A	Rack Mounting Plate
DLN6693A	RS232 Cable for PDEG

Chapter 9

PDEG Disaster Recovery

This chapter provides references and information that make it possible to recover the PDEG in the event of a failure.

9.1

Recovery Sequence for the PDEG Encryption Unit

When and where to use: Follow this process to replace the entire PDEG Encryption Unit.

Process:

1. Remove the existing PDEG Encryption Unit hardware. Install the new PDEG Encryption Unit hardware. See Mechanical Installation on page 21 in the *PDEG Encryption Unit Feature Guide*.
2. Perform basic device configuration through the serial port. See the following procedures in the *PDEG Encryption Unit Feature Guide*:
   - Assigning IP Addresses for the PDEG Encryption Unit on page 31
   - Configuring the PDEG Encryption Unit for Syslog on page 34
   - If your system includes redundant PDEG Encryption Units, configure each unit for redundancy using Virtual Router Redundancy Protocol (VRRP). See Configuring PDEG Encryption Units for Redundancy on page 35.
   - Configuring Associations and Rules on page 38
   - If your system includes a KMF, then configure each PDEG Encryption Unit for centralized key management. See Configuring the PDEG Encryption Unit for OTEK on page 32
3. Restore encryption keys. See the following procedures in the *PDEG Encryption Unit Feature Guide*:
   - Loading Encryption Keys to the PDEG Encryption Unit on page 32
   - Configuring the PDEG Encryption Unit for OTEK on page 32