ASTRO DATA ENCRYPTION UNIT

The Data Encryption Unit provides encryption/decryption of P25 data within ASTRO® radio systems. This tamper resistant encryption unit, with integrated physical security, is certified to the National Institute of Standards and Technology FIPS 140-2 Level 3 certification, a very stringent standard for cryptographic modules. The data encryption keys can be centrally managed using a Motorola Key Management Facility (KMF) via Over the Ethernet Keying (OTEK). The encryption unit is available for either ASTRO trunked or conventional radio systems. The CAI Data Encryption Module (CDEM) unit can only be used in a conventional system and the Packet Data Encryption Gateway (PDEG) can only be used in a trunked system. One device cannot be used for both types of radio systems.

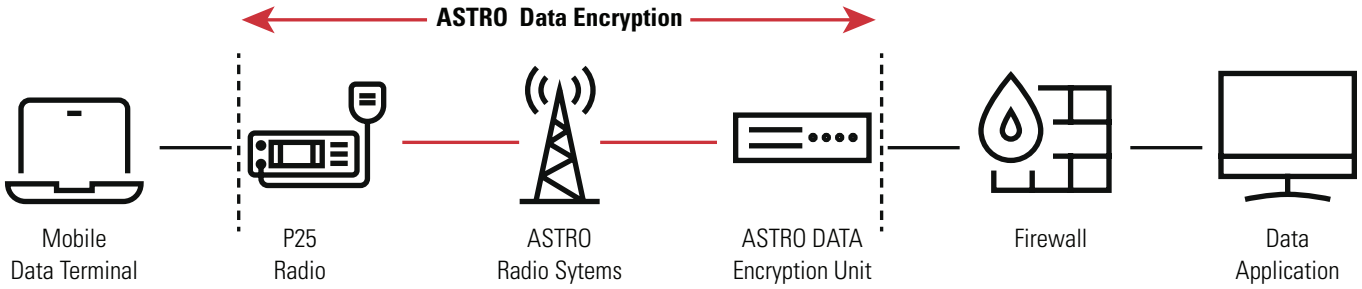
MOTOROLA SOLUTIONS

TRUNKING SYSTEMS

In an ASTRO trunking system the encryption unit is referred to as a Packet Data Encryption Gateway (PDEG). It is a component of the ASTRO Data Trunked IV&D Encrypted Integrated Data (EID) system feature, and is located within the Customer Enterprise Network (CEN) providing protection over-the-air and in the radio network infrastructure. The EID feature uses IPsec to provide AES encryption, decryption and authentication of packet data between each EID enabled P25 radio and a PDEG Encryption Unit. Using the EID feature, users can secure data sent between CEN applications and the P25 radio's internal or external applications like location information or a personnel look up.

CONVENTIONAL SYSTEMS

In an ASTRO conventional system the encryption unit is referred to as a CAI Data Encryption Module (CDEM). It is located in the Radio Network Infrastructure (RNI) and connects to the Packet Data Gateway (PDG) performing packet data encryption and decryption for inbound and outbound datagrams using either DES-OFB or AES 256 encryption algorithms or both simultaneously. This unit in a conventional system, provides secure communication between the endpoints of the P25 radio and the PDG. Packt data is in the form of Common-Air-Interface datagrams.



SPECIFICATIONS

Specifications apply to both trunked and conventional systems unless noted.

ELECTRICAL AND PHYSICAL	
Power	12 VDC @ 500 mA
Interfaces	2xRJ45 Ethernet, Key Fill, 2xRS-232 Serial
Dimensions (mm) ca.	29.5 x 92 x142 mm
Weight (typical) g ca.	300 g
ENVIRONMENTAL	
Operating Temperature (ºC)	-0ºC to +50ºCHz
Storage Temperature (ºC)	-10ºC to +60ºC
Humidity	Up to 90% RH at Upper Limit Operating Temperature
SECURITY AND PERFORMANCE	
Security: FIPS 140-2 Level 3	
Performance: Sensitive but Confidential Unclassified Information (CUI)	
Performance trunked system: 520KPS	
Performance conventional systems: 600K message an hour	
OVER THE AIR ENCRYPTION ALGORITHMS	
AES256	Applicable Standard Document: AES Advanced Encryption Standard: FIPS 197
DES-OFB	Data Encryption Standard - output feedback mode; FIPS 81 (Conventional systems only)
WIRELINE PROTOCOLS	
IPv4	Internet Protocol version Four
IPSEC	Internet Protocol Security (Trunked systems only)
ENCRYPTION KEY PROVISIONING, KEYLOADING AND KEY MANAGEMENT	
Configured through RS-232 console port	
Encryption key provisioning and key loading using the Motorola Key Variable Loader KVL 4000 and KVL 5000	
Manage Encryption Key using Over-the-Ethernet-Keying (OTEK) through the Key Management Facility	
STANDARD COMPLIANCE	
NIST FIPS 140-2	National Institute of Standards and Technology NIST FIPS 140-2 Level 3 compliant FIPS 140-2; Security Requirement for Cryptographic Modules

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**