INTERTALK™

InterTalk P25 AES Encryption Dongle

ENCRYPTION MEETING FIPS 140-2 STANDARD

InterTalk's P25 AES Encryption Dongle is a 28 mm x 25 mm single-board security module, designed to conform to FIPS 140-2 standards and targeted for mobiles and base stations. It provides encryption, decryption, key management and key storage services, and can be used with radio and network equipment. The module supports KFD management implementations, including a dedicated 3-wire KFD interface. It includes a complete key storage and critical security material management function for Traffic Encryption Keys (TEK) and Key Encryption Keys (KEK) in non-volatile memory within the dongle, with protection from unauthorised disclosure or modification.

FEATURES

- Single multi-chip embedded 28 mm x 25 mm board
- 24 simultaneous cryptographic channels
- Voice and data encryption and decryption support
- P25 OTAR (Over the Air Rekeying) support
- Key Fill Device (KFD) interface
- Key generation support
- High capacity key and security material storage
- High speed serial host interface
- Multi-level zeroisation capability
- Full zeroisation via direct hardware control
- Firmware integrity and cryptographic power-up tests

PHASE 1 VOICE AND DATA SUPPORT

The P25 AES Encryption Dongle supports encryption and decryption of Phase 1 voice and data traffic, Trunking Control Keystream and OTAR Message Authentication Code (MAC) operations. It implements the following FIPS 140-2 approved algorithms:

- AES-256 ECB
- AES-256 OFB
- AES-256 CBC
- PRNG1
- SHA-12
- DSA
- HMAC

FIPS SECURITY LEVEL

The P25 Encryption Dongle meets the following security levels, as defined in FIPS 140-2:

AREA FIPS 140-2	*SECURITY LEVEL*
Cryptographic Module Specification	Level 1
Cryptographic Module Ports and Interfaces	Level 1
Roles, Services, and Authentication	Level 1
Finite State Model	Level 1
Physical Security	Level 1
Cryptographic Key Management	Level 1
EMI / EMC	Level 1
Power-up Self Tests	Level 1
Design Assurance Level	Level 1

P25 AES Encryption Dongle
Specifications

MAIN COMPONENTS

STARTUP MANAGER
The Startup Manager initialises the Crypto Module software and invokes self-test of the cryptographic algorithms.

HOST INTERFACE
The Host Interface performs common message processing for incoming and outgoing host messages.

HOST MESSAGE HANDLERS
The Host Message Handlers process specific incoming host messages. They request the necessary actions within the Crypto Module, and prepare the appropriate response messages for the host.

KFD INTERFACE
The KFD Interface performs common message processing for incoming and outgoing KFD messages.

KMM HANDLERS
The KMM Handlers process specific incoming key management messages (KMMs). They request the necessary actions within the Crypto Module, and prepare the appropriate response KMMs for the KFD.

DATABASE
The Database allows the other entities to store and retrieve information in a high-level form appropriate to that entity. It translates between this high level form and its storage format, and organises stored information into logical pages.

DATABASE STORAGE MANAGER
The Database Storage Manager is responsible for mapping the logical pages of database information to its physical storage, and for managing failsafe update operations.

CHANNEL ROUTER
The Channel Router coordinates cryptographic channels and routes channel operation messages to and from the individual channels.

CHANNELS
The Channels are the individual cryptographic channels. They implement the specific behaviour of each channel type, and maintain channel state for the life of each channel instance. A Channel invokes the cryptographic algorithms required for its operation using unwrapped (plaintext) key material obtained from the Key Wrapper.

WARM START GENERATOR
The Warm Start Generator is responsible for generation of Warm Start Segment information when requested by the host, including generation of the temporary key using an appropriate Pseudo Random Number Generator algorithm.

KEY WRAPPER
The Key Wrapper performs wrapping and unwrapping operations on keys stored in the database, or received or transmitted over the air. It invokes the appropriate cryptographic algorithms to perform the wrapping and unwrapping, and handles plaintext versions of both the keys being wrapped/unwrapped and the Key Encryption Key with which the wrapping is performed.

ZEROISING AND INTEGRITY
A multi-leveled zeroise feature ensures all the Critical Security Parameters (CSPs) are completely and securely deleted when required. Also digital signatures utilising the SHA-1 and DSA are used to digitally sign and verify software modules during power up self test and when new software versions are uploaded. The module also includes cryptographically sound pseudorandom number generation for key generation.

INTERTALK PART NUMBER	
P25 AES ENCRYPTION DONGLE	830-4001-01