

# FIPS P25 Crypto Module

**The Nexus FIPS P25 Crypto Module is a single-board security module designed to conform to FIPS140-2 standards and targeted for APCO P25 mobiles and base stations. It provides all the encryption, decryption, key management and key storage services required for use in an APCO Project 25 communications system, and meets the Security Requirements for Cryptographic Modules standard from the National Institute of Standards and Technology.**

## Overview

The FIPS P25 Crypto Module is a 28 x 25 mm board based around a TI C5509 DSP. The module supports both KFD and KMF management implementations, including a dedicated 3-wire KFD interface. It includes a complete key storage and critical security material management function for TEK, KEK, UKEK, CKEK and KSKEK keys in non-volatile memory within the FIPS module, with protection from unauthorized disclosure or modification.

The FIPS Module executes encryption and decryption of P25 Phase 1 voice and data traffic, Trunking Control Keystream and OTAR MAC operations. Full support is provided for the following FIPS 140-2 Approved Operational Modes:

- DES ECB
- DES OFB
- DES CBC
- DES 1-bit CFB
- AES-256 ECB
- AES-256 OFB
- AES-256 CBC

## Main Module Components

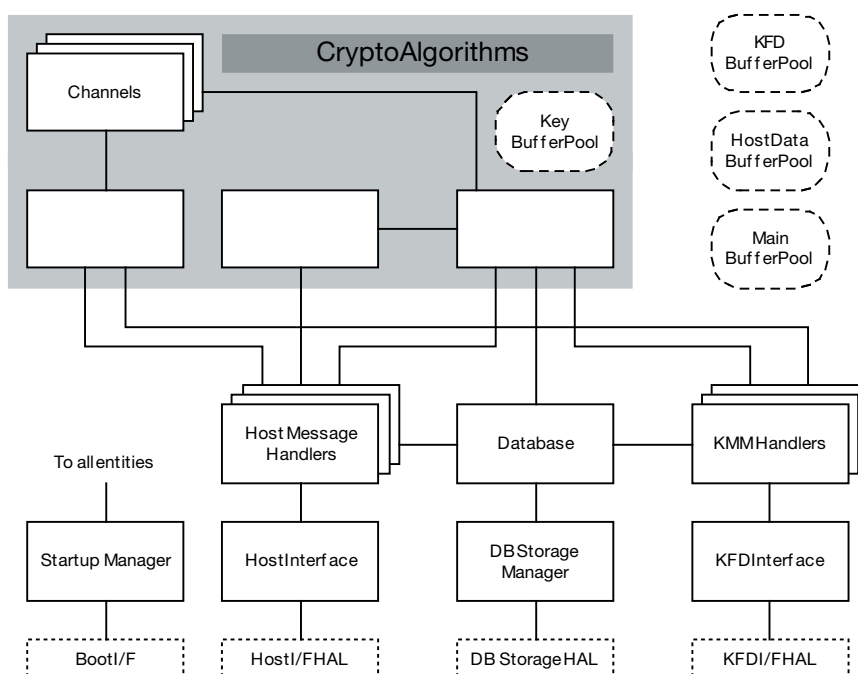
The Startup Manager initializes the Crypto Module software and invokes self-test of the cryptographic algorithms.

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

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

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

The Channels are the individual



cryptographic channels. They implement the behavior 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.

## FIPS Security Level

The Nexus FIPS Module meets the following security levels, as defined in FIPS140-2:

- 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
- Operational Environment Level 1

- Cryptographic Key Management Level 1
- EMI / EMC Level 1
- Power-up Self Tests Level 1
- Design Assurance Level Level 1
- Mitigation of Other Attacks N/A

## Zeroize Capability

A multi-levelled zeroize feature ensures all the Critical Security Parameters (CSPs) are completely and securely deleted when required. Also digital signatures utilizing 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.