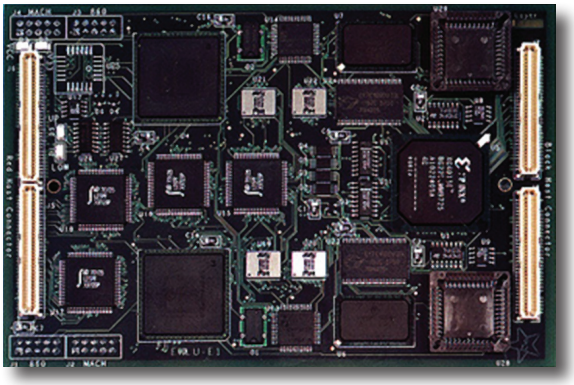
PEIP II

PROGRAMMABLE EMBEDDABLE INFOSEC PRODUCT



PEIP II Cryptographic Engine

Key Features:

- *NSA certified Type 1 programmable crypto engine*
- *Crypto Modernization compliant*
- *Key and Crypto Application Agile*
- *Support Suite A & B crypto applications*
- *Software based cryptography – fully programmable*
- *Secure software download*
- *10 channels emulate up to 10 crypto devices*
- *Robust key management features:*
  - *Black key fill*
  - *Benign keying and fill*
  - *Basic and enhanced FIREFLY*
  - *ACCORDION 1.3 and 3.0*
  - *Key update*
  - *Over-the-air distribution*
- *Multiple Independent Levels of Security (MILS) certified for data processing*
- *Radiation hardened version available*
- *Designed to support foreign releasability*

Description

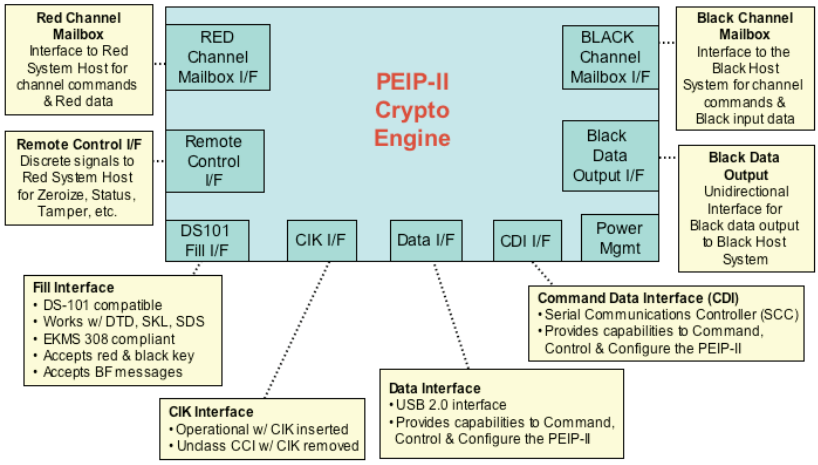
The PEIP family of cryptographic engines is designed and developed by the Naval Research Laboratory, in support of the NSA Crypto Modernization Program. The PEIP-II is implemented as a pluggable cryptographic engine that supports a wide array of functions. To lessen the required COMSEC functionality on the host system, the PEIP-II includes as many cryptographic and key management functions as possible. This includes key and crypto application storage, support for key decryption, and relevant public key exchange algorithms and protocols implemented to support infrastructure to End Crypto Unit (ECU) as well as ECU-to-ECU messaging.

Applications

The PEIP-II development, sponsored by the NSA Crypto Modernization Program Office, has been embedded in various ECU systems on platforms ranging from sub-surface to strategic air platforms to ground elements. The programs using PEIP-II as a core cryptographic technology are: KG-3x Modernization Program (Increment 1 & 2), Ground Element MEECN System (GEMS), and Modular Integrated Link Electronics System (MILES). As an inexpensive Type 1 Government-off-the-Shelf (GOTS) solution, the PEIP-II serves as an enabling cryptographic technology for Crypto Modernization.

PEIP Characteristics

Certification	NSA Type 1 certified and MILS certified for processing information up through TS Code-word and allowing simultaneous processing of information classified at different levels.
Dimensions	Currently 6"W x 4"H industry mezzanine card.
Power	Standard 3.3V and 5V, consuming on average 5 Watts.
Data Throughput	Varies by crypto application; 133 MHz clock.
Operating Temperature	Sheltered shore version 0°C to 50°C, and airborne version –40°C to 90°C.
Status Indicators	Remote Control Interface (RCI) signals available to host system.
Fill Interface	DS-101; compatible with DTD, SDS, and SKL.
Key Storage	100 TEKs per Key Bank (10 Key Banks in the PEIP) and multiple KEK locations.
Crypto Application Storage	Storage provided for up to 20.
Crypto Applications	Supports Suite A and Suite B crypto applications.
Crypto Device Emulation	Through 10 channels, up to 10 individual crypto devices can be simultaneously emulated on one PEIP.
Field-Reprogrammable	Secure software download for crypto applications and operational software.
Crypto Ignition Key (CIK)	Industry standard Serial Peripheral Interface (SPI); supports one master CIK device and up to 9 unique secondary user CIK devices.
Randomizer	On-board NSA approved randomizer.
Cost	Low-cost solution, specific cost based on operating temperature requirements and packaging.
Classification	Unclassified when not keyed, unclassified when in the CIK mode and the CIK is removed.



The **Communications Security (COMSEC) Systems Section**, a component of the Center for High Assurance Computer Systems (CHACS) at the U.S. Naval Research Laboratory, focuses on research and development of cryptographic technologies.

Current Projects:

- Programmable crypto engine development
  - PEIP II
- Host development
  - KOV-17 and 17-1, KG-334
- Crypto application development
  - KG-38, MEDLEY, BATON, KEESEE, JOSEKI, AES
- Security engineering

For Additional Information:

U.S. Naval Research Laboratory
Attn: Code 5541
4555 Overlook Ave., SW
Washington, DC 20375

Fax: (202) 767-1060
Email: 5541info@chacs.nrl.navy.mil