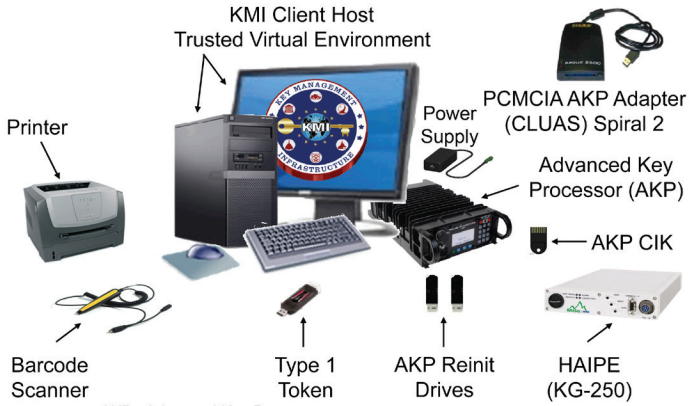
Key Management Infrastructure (KMI)

Executive Summary

- The Key Management Infrastructure (KMI) Program Management Office (PMO) and Joint Interoperability Test Command (JITC) conducted an FOT&E in accordance with a DOT&E-approved test plan from January 14 through February 1, 2013, which included infrastructure and 13 separate Service and agency locations across the United States.
- In April 2013, DOT&E reported that KMI significantly improved from the IOT&E and is now operationally effective, suitable, secure, and remains interoperable; however, the FOT&E demonstrated continued problems with token reliability and revealed some minor shortfalls in system availability and sustainment. Transition procedures improved but need further refinement.
- Subsequent to the DOT&E report, the DoD Chief Information Officer published the KMI Acquisition Decision Memorandum on June 19, 2013, approving full-rate production and deployment of Spiral 1 to DoD Services and agencies.

System

- KMI is intended to replace the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., asymmetric keys, symmetric keys, manual cryptographic systems, and cryptographic applications).
- KMI Spiral 1 consists of core nodes that provide web operations at a single site operated by the National Security Agency, as well as individual client nodes distributed globally to provide secure key and software provisioning services for the DoD, intelligence community, and agencies. Spiral 2 will provide improved capability through software enhancements to the Spiral 1 baseline.
- KMI combines substantial custom software and hardware development with commercial off-the-shelf computer components. The custom hardware includes an Advanced Key Processor for autonomous cryptographic key generation and a Type 1 user token for role-based user authentication. The commercial off-the-shelf components providing user operations include a client host computer, High Assurance Internet Protocol Encryptor (KG-250), monitor, keyboard, mouse, printer, and barcode scanner.



AKP - Advanced Key Processor
CIK - Crypto Ignition Key
CLUAS - Card Loader User Application Software
HAIPE - High Assurance Internet Protocol Encryptor
PCMCIA - Personal Computer Memory Card International Association
Reinit - Reinitialization

Mission

- Combatant Commands, Services, DoD agencies, other Federal Government agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the Global Information Grid, and initiatives such as Cryptographic Modernization.
- Service members will use KMI cryptographic products and services to enable security services (confidentiality, non-repudiation, authentication, and source authentication) for diverse systems such as Identification Friend or Foe, GPS, Advanced Extremely High Frequency Satellite System, and Warfighter Information Network – Tactical.

Major Contractors

- Leidos (formerly SAIC) – Columbia, Maryland (Spiral 2 Prime)
- General Dynamics Information Assurance Division – Needham, Massachusetts (Spiral 1 Prime)
- BAE Systems – Linthicum, Maryland
- L3 Systems – Camden, New Jersey
- SafeNet – Belcamp, Maryland
- Praxis Engineering – Annapolis Junction, Maryland

Activity

- The KMI PMO and JITC conducted an FOT&E in accordance with a DOT&E-approved test plan January 14 through February 1, 2013, which included infrastructure and 13 separate Service and agency locations across the United States.
- DOT&E issued a classified FOT&E report in April 2013.

- Subsequent to the DOT&E report, the DoD Chief Information Officer published the KMI Acquisition Decision Memorandum on June 19, 2013, approving full-rate production and deployment of Spiral 1 to DoD Services and agencies.
- The PMO and Operations Manager completed the facility Uninterruptable Power Supply (UPS) expansion in July 2013 to support the resiliency of KMI Storefront (which provides backend processing for generation of cryptographic products; also called core nodes) and redundant systems.
- The PMO and JITC are updating the Spiral 2 Test and Evaluation Master Plan (expected in March 2014) that will describe the test and evaluation strategy to support planned program activities to support a Full Deployment Decision by April 2017.

Assessment

- KMI is operationally effective. The PMO and Networking Tiger Team corrected EKMS-to-KMI transition problems previously encountered in the 2012 IOT&E. Once accounts transitioned, KMI supported required operational tasks with no difficulties in product key ordering and account management, and Service and agency user feedback was positive regarding KMI's effectiveness versus the legacy EKMS.
- KMI is operationally suitable; however, the FOT&E demonstrated continued problems with token reliability and revealed some minor shortfalls in system availability and sustainment. Transition procedures improved but still need further refinement.
  - While the PMO conducted extensive analysis to determine the underlying token failure modes, the KMI tokens redesigned to correct the problems were not available for the FOT&E.
  - The program's custom-designed Advanced Key Processor performed well and continued to meet reliability expectations.
  - The facility UPS was inadequate to support the KMI Storefront and redundant systems, contributing to availability problems observed during the FOT&E that the PMO subsequently resolved in July 2013.
  - KMI and Service-level help desk support was adequate in providing required user support during transition, routine activities, and subsequent mission operations.
  - Configuration management procedures matured significantly and are now adequate for operations.
  - The Configuration Control Board efficiently prioritized discrepancy reports logged against the system and approved build changes.
- KMI is secure. The detailed Information Assurance assessment results are classified and can be found in the annex to the April 2013 DOT&E report.
- The discussion of continuity of operations planning and facility preparations is classified and can be found in the April 2013 DOT&E report.
- KMI remains interoperable. The system continued to successfully exchange critical information with all external interfaces (fill devices, end cryptographic units, and EKMS) accurately and without failure during the FOT&E.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed the five previous recommendations.
- FY13 Recommendations. The KMI PMO should:
  1. Verify increased KMI token reliability through a combination of laboratory and operational testing with automated data collection from system logs for accurate reliability and usage analysis.
  2. Stress test the facility's UPS for the Storefront systems to include pertinent nodes and execute routine planned failover tests periodically to ensure necessary data synchronization between redundant equipment.
  3. Complete the Spiral 2 Test and Evaluation Master Plan update to support future operational testing by March 2014.
  4. Follow the recommendations for the KMI continuity of operations plan listed in the classified April 2013 DOT&E report.