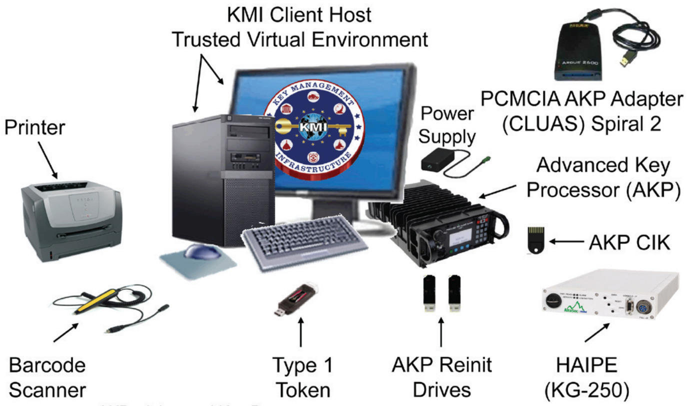
Key Management Infrastructure (KMI)

Executive Summary

- In January 2012, the Key Management Infrastructure (KMI) Program Management Office (PMO) and DoD Chief Information Officer (CIO) declared an acquisition cost and schedule threshold breach, resulting in a Critical Change Review of the program. Subsequently, the Chairman of the Joint Chiefs of Staff declared KMI essential to national security and OSD recertified the program to Congress.
- The Joint Interoperability Test Command (JITC) conducted an IOT&E from July until August 2012. The results were a marked improvement over previous operational assessments; however, there were still several operational effectiveness and suitability problems uncovered during the testing event that must be corrected before continued deployment.
- The KMI transition process and Services' fielding concepts must be matured to ensure an accurate and smooth migration from the legacy Electronic Key Management System (EKMS) to KMI. Configuration management controls and training of personnel at the KMI operational support site need improvement to eliminate system inconsistencies.
- The new Type 1 token hardware and its stability are an improvement over previous tokens, but its reliability is deficient and further product refinement and testing is necessary for a suitability determination.
- KMI is potentially operationally effective once significant transition problems are resolved. Security is undetermined, pending a Red Team's assessment. KMI is interoperable and received full certification for Spiral 1; however, KMI was determined to be unsuitable due to the lack of help desk preparedness for operational support, deficient token reliability, and immature Configuration Control Board and configuration management processes.
- Despite problems identified during operational testing, the KMI program continues to show progress toward delivering a useful cryptographic capability for system managers and users. Operational users in the IOT&E reviewed the system capabilities positively, once the transition process completed.

System

- KMI is intended to replace the legacy EKMS to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., asymmetric key, 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 (NSA), 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.



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

- KMI combines substantial custom software and hardware development with commercial off-the-shelf (COTS) 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 COTS components providing user operations include a client host computer, High Assurance Internet Protocol Encryptor (KG-250), monitor, keyboard, mouse, printer, and barcode scanner.

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, Joint Tactical Radio System, and Warfighter Information Network – Tactical.

Major Contractors

- 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

- DOT&E published the KMI Operational Assessment-2 report in mid-October 2011. Based on that report, the DoD CIO approved Milestone C and authorized the KMI program to enter the Production, Deployment, and Sustainment phase for Capability Increment 2 in late October 2011.
- In January 2012, the KMI PMO and DoD CIO declared an acquisition cost and schedule threshold breach, resulting in a Critical Change Review of the program. Subsequently, the Chairman of the Joint Chiefs of Staff declared KMI essential to national security and OSD recertified the program to Congress.
- With the DoD CIO certification of the program, the KMI Program Office moved forward with Spiral 1 IOT&E preparations and Spiral 2 Contract Award.
- In accordance with the Acquisition Decision Memorandum, the KMI program manager implemented a token reliability growth program and conducted accelerated life testing of 120 tokens in order to increase confidence in token reliability. The tokens achieved 86,000 combined hours of testing while undergoing temperature and vibration cycles to demonstrate a 10,000-hour Mean Time Between Failure with 80 percent confidence.
- The KMI program and JITC conducted an IOT&E in accordance with a DOT&E-approved plan from July 9 through August 10, 2012, at 17 separate Service and Agency locations across the United States.
- DOT&E published the KMI IOT&E report in mid-October 2012.

Assessment

- KMI is potentially operationally effective once significant transition problems are resolved. Security is undetermined, pending a Red Team's assessment. KMI is interoperable and received full certification for Spiral 1; however, KMI was determined to be unsuitable due to the lack of help desk preparedness for operational support, deficient token reliability, and immature Configuration Control Board and configuration management processes.
- Successful completion of IOT&E was required for a Spiral 1 client node fielding decision.
  - The program's major hardware developmental item, the Advanced Key Processor, is performing well and exceeds its expected reliability.
  - The Service and agency users perceived KMI as a major qualitative improvement over the legacy EKMS.
- KMI is significantly more stable and usable than in previous test events, although there are still effectiveness and suitability problems with transition and backend support.
- Based on the IOT&E, problems with system performance, data errors, manual KG-250 and virtual private network tunnel configurations, and network connectivity associated with account transition affected the efficacy and speed of migrating cryptographic products from EKMS to KMI. This caused significant delays in account migration across Services and agencies.
- The 5 percent token failure rate observed during the test period is not acceptable. While observations indicate that token reliability is improved, additional token reliability testing to gain more usage hours, square wave (power cycling), and mechanical insertion testing is required.
- Symmetric cryptographic key ordering is working well in KMI; however, asymmetric keys are ordered within KMI but their production is accomplished external to the system. While this is an early delivery solution to support Service needs, operational users can still effectively perform their duties.
- Suitability concerns persist with the system and logistical support documentation. These products are improved, but they require refinement to support a fully operational capability.
- KMI help desk and system administration personnel were not adequately prepared to support a fully operational KMI system.
  - The monitoring capabilities and knowledge base are immature and not well-exercised. Critical support personnel were not prepared to support the user community during transition and day-to-day operations.
  - The backend support is not prepared for a KMI full fielding effort. Significant effort must be made to refine the technical support processes before the system is fully deployed to hundreds of user accounts and client systems.
- The Configuration Control Board processes and procedures for updating and implementing system builds and maintaining a consistent software baseline are not refined or effectively implemented to support the Services and agencies.
- The KMI transition process and Services' fielding concepts must be matured to ensure an accurate and smooth migration from the legacy EKMS to KMI. Configuration management controls and training of personnel at the KMI operational support site needs improvement to eliminate system inconsistencies.
- KMI system documentation, procedures, and training for technical staff and help desk personnel are inadequate. However, KMI operational users indicated the training was thorough but too compressed. The Services have limited training blocks to two weeks because of Reservist and National Guard requirements.
- Despite some problems identified during operational testing, the KMI program continues to show steady progress toward delivering a useful cryptographic capability for system managers and users. Operational users in the IOT&E reviewed the system capabilities positively, once the transition process completed.
- Based on the IOT&E results, the KMI PMO scheduled an FOT&E for January 2013.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed seven of nine previous recommendations. Additional PMO effort is required to adequately address regression testing for system builds and their deployment and more time is necessary to provide adequate KMI training.
- FY12 Recommendations. The KMI PMO should:
  1. Require the developmental contractors to routinely demonstrate system readiness through regression testing before releasing software upgrades and system builds, and then only as approved by the Configuration Control Board for distribution to Services and agencies.
  2. Review Service and agency deployment methods and work jointly to automate transition functions, such as KG-250 and virtual private network tunnel configurations, to reduce problems and minimize network setup changes and remote troubleshooting from the KMI support site.
  3. Capture and refine documentation of all KMI process adjustments for incorporation in system and user-level operating guides.
  4. Assure that KMI training includes sufficient hands-on equipment time to allow users to gain more system familiarity, knowledge, and proficiency. Additional user and manager-level training is needed to ensure that users can understand the KMI processes and operate the system.
  5. Conduct additional token reliability testing incorporating more usage hours, square wave (power cycling), and mechanical insertion tests.