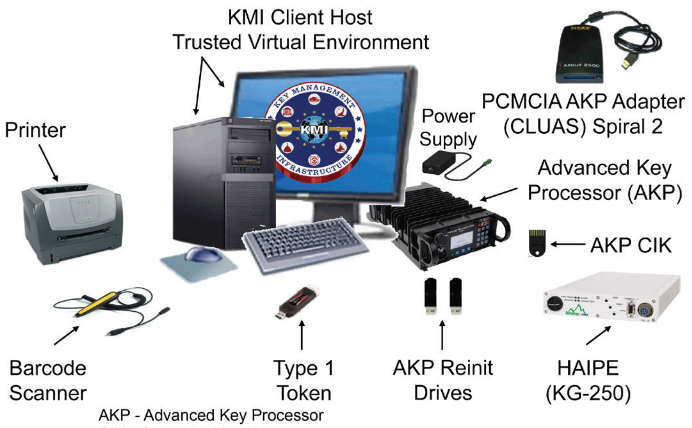
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- Key Management Infrastructure (KMI) is designed to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems for Combatant Commands, Services, DoD agencies, other Federal government agencies, coalition partners, and allies.
- The Operational Assessment Phase 2 (OA-2) began in late August 2011 with the National Security Agency (NSA) Protect Program Executive Office (PEO) certifying that it was ready for test. When the OA-2 testing completed in late September 2011, the results were a marked improvement over OA-1; however, there were still effectiveness and suitability problems uncovered during the testing event.
- The KMI Program Management Office (PMO) has not fully demonstrated the ability to provide a stable software release and supporting Type 1 token hardware to accomplish all aspects of operational testing. Additional verification of system readiness and usability procedures through an operational assessment are necessary.
- 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.

System

- KMI will provide a means for the secure ordering, generation, production, distribution, management, and auditing of cryptographic products (e.g., asymmetric key, symmetric keys, manual cryptographic systems, and cryptographic applications), and will replace the legacy Electronic Key Management System.
- KMI consists of core nodes that provide database storage, secure routing, and key generation and management services centrally located at an NSA location, as well as individual client nodes distributed throughout the world and used by cryptographic account custodians to order, manage, and distribute key material to Service members and other consumers.
- KMI is a combination of nearly 1,200,000 lines of contractor-developed software code, custom-developed hardware in the form of an Advanced Key Processor (AKP), AKP Crypto Ignition Key (CIK) and Type 1 token for user authentication, and commercial off-the-shelf (COTS) hardware and software. The KMI client node hardware components are comprised of a computer (client host), monitor, printer, AKP with power supply, AKP CIK, High Assurance Internet Protocol Encryptor (KG-250), ten Type 1 tokens, two AKP reinitialization drives, and a bar code scanner (as pictured above). A Personal Computer Memory Card International Association (PCMCIA) AKP Adapter Card Loader User Application Software (CLUAS) is also included with the hardware; however, the software capability to leverage this peripheral is not planned until Spiral 2.



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 such as 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 (IFF), Global Positioning System (GPS), Advanced Extremely High Frequency (AEHF) Satellite System, Joint Tactical Radio System (JTRS), and Warfighter Information Network – Tactical (WIN-T).

Major Contractors

- General Dynamics Computer Network Division – Needham, Massachusetts (Prime)
- General Dynamics Information Assurance Division – Needham, Massachusetts
- BAE Systems – Linthicum, Maryland
- SAIC – San Diego, California
- L3 Systems – Camden, New Jersey
- SafeNet – Belcamp, Maryland

Activity

- The KMI program completed developmental testing on each KMI node and the integrated system in March 2011. Although developmental testing indicated token reliability was lacking and software stability was unsuitable for operational use, the NSA PEO certified KMI for operational test readiness, and the program entered Operational Assessment Phase 1 (OA-1) in late March.
- OA-1 was a six-week test intended to be executed as a series of mission-based scenarios, with the Joint Interoperability Test Command (JITC) as the Operational Test Agency and Service key management subject matter experts executing the scenarios, with a focus on system performance.
  - The KMI PMO halted OA-1 after three weeks due to an inability to complete most of the required tasks.
  - Over 200 high-priority deficiencies were documented, and client node Mean Time Between Operational Mission Failure (MTBOMF) was significantly below target (3 hours versus 1,107 hours). In addition, token failures were significant and required vendor re-engineering to remedy the various problems.
  - During the OA-1, the KMI PMO requested permission from JITC to apply a new software version for the client nodes that would correct the need for frequent system reboots, but this new software code introduced problems in functions that had worked correctly in previous versions. The PMO declared this testing complete although only approximately 30 percent of the scenarios were successfully executed, while problems were continuing to be found, and new software builds were being produced at a rate of two per week.
  - Following these problems, the KMI PMO implemented testing of the OA scenarios at the contractor site for completion on all software releases.
- After suspending OA-1, JITC and the Service users continued to provide the PMO with regression test support in an effort to find errors and allow completion of all required scenarios. After six weeks of testing by the Services and the NSA, the PMO declared the testing complete.
- The PMO issued new tokens, updated the KMI software, and conducted a formal two week OA-1 regression test where the system demonstrated improved performance. In addition, the first account transition was demonstrated from the legacy Electronic Key Management System into KMI. Problems were still identified in the system performance, token reliability, and client node reliability, and there were suitability concerns with the system documentation.
- The KMI Training Working Group completed formal verification of the training materials in June 2011, presenting to training class participants for OA-2. After the Training Working Group meeting and review of the verification results in July 2011, the Service training leads accepted the training.
- Based on the results of the regression test, closure of the deficiency reports resulting from the OA-1 regression test, and user support for further operational testing, NSA Protect PEO authorized entrance into the OA-2 pilot testing in June 2011. Because problems resulted from the pilot testing (high failure rate of new tokens provided for OA-2, deficiency reports in early testing, problems with Secret Internet Protocol Router Network (SIPRNET) firewall configurations, and representative legacy and transition accounts and procedures), the KMI PMO deferred the formal start of OA-2 until the pilot problems were closed and the transition accounts established.
- The KMI program intended for OA-2 to be a four-week test performed at Service locations with typical users executing mission-based scenarios, with a focus on user readiness for operational deployment and the IOT&E.
  - JITC executed a pilot test the week prior to the official start of OA-2 during which high-priority system problems were discovered that precluded starting OA-2 as planned.
  - JITC conducted the OA-2 from August 24 to September 20, 2011.
  - New tokens were provided to the users for OA-2 that were intended to correct the low reliability seen in the previous batch of tokens, but the redesigned devices continued to have problems, although fewer and with different failure modes than the previous versions.
  - During the OA-2, a critical test, designed to ensure that conversion of the system of record from the legacy Electronic Key Management System to KMI could be accomplished, continued to fail, even after new software versions were produced to fix these problems.
  - The Service system experts again agreed to provide defect discovery support and regression test evaluations to the PMO, with the result being continued software baseline instability with multiple version releases per week.
- The DoD Chief Information Officer, as the Milestone Decision Authority, approved Milestone C and authorized the KMI program to enter the Production, Deployment, and Sustainment phase for Capability Increment 2 on October 28, 2011.

Assessment

- The KMI PMO has not demonstrated the ability to provide stable and reliable software or Type 1 token hardware to accomplish operational testing.
  - Software stability was initially found to be unsuitable for operational use with multiple high-priority deficiencies that would not allow for completion of required tasks.
  - Capabilities that worked in one release ceased to work in subsequent releases, indicating a lack of rigor in contractor regression testing.
  - Token reliability has not been demonstrated as sufficient for use in an operational environment with tokens failing to meet the 10,000-hour Mean Time Between Operational Mission Failure (MTBOMF) requirement.
- The KMI system was improved noticeably between OA-1 and OA-2. Although there are still some stability problems with the software, it is significantly more stable.
  - Notably, the program's major hardware developmental item, the Advanced Key Processor is performing well and exceeds its expected reliability.

  - Additionally, the test users like KMI, and the system is perceived as a major improvement over the legacy Electronic Key Management System.
- KMI system documentation, procedures, and training for technical staff, helpdesk personal, and users are inadequate. More hands-on training is necessary for users to gain experience and confidence with KMI.
- Operational testing identified some problems that were missed by developmental testing. The development test environment was initially limited because of no operational data from the legacy system; however, this has now been corrected. Pre-existing developmental testing problems will not preclude KMI from moving forward.
- Successful completion of OA-2 was required for the Milestone C decision and limited deployment to operational sites for IOT&E.
- Based on the improved system performance, PMO-initiated pilot program, and regression testing in October 2011, DOT&E recommended KMI for Milestone C and entrance into IOT&E with specific direction to correct all mission-critical deficiencies, documentation, training, and support services. However, currently, KMI is not sufficiently mature for deployment for full operational use.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY11 Recommendations.
  1. The KMI PMO should require the developmental contractors to demonstrate system readiness for operational assessment by executing mission-based scenarios with no critical discrepancy reports.
  2. After contractor verification of system capability and stability, JITC and Service subject matter experts should independently verify the KMI system's readiness for IOT&E prior to test execution.
  3. The readiness checklist for IOT&E should contain measureable criteria relating to software version stability, token and client MTBOMF metrics, and user-accepted workarounds for all system deficiencies that must be demonstrated prior to starting the test event.
  4. Documentation of all KMI process adjustments needs to be captured and refined for incorporation in system and user-level operating guides.
  5. Additional evaluation of user and manager-level training is needed to ensure that users can understand the KMI processes and operate the system.
  6. The PMO must assure that training for all personnel (users, administrators, core node staff, and helpdesk) includes sufficient hands-on equipment time to allow users to gain more system familiarity, knowledge, and proficiency with KMI.
  7. The KMI PMO should conduct an additional operational assessment to verify that the system is stable, reliable, and on the path to successful performance during IOT&E.
  8. A Red Team evaluation of the KMI core node security posture needs to be scheduled to coincide with the IOT&E, and be completed in time to influence the full deployment decision currently scheduled for June 2012.
  9. The PMO needs to establish a reliability improvement program for the tokens to ensure that progress is being made toward fielding a reliable token that will support the key management mission.