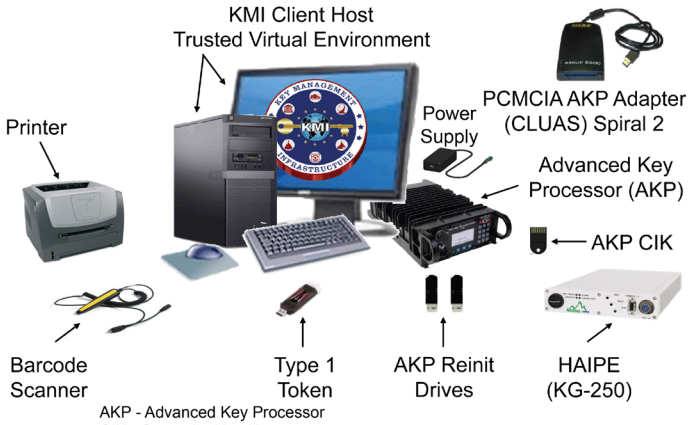
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- DOT&E published its Key Management Infrastructure (KMI) Spiral 2, Spin 1 Limited User Test (LUT) and LUT Retest Report in late October 2015 that found KMI to be operationally effective with some problems and not operationally suitable. The Joint Interoperability Test Command (JITC) conducted a LUT of KMI Spiral 2, Spin 1 capabilities; however, JITC could not fully assess KMI cybersecurity until an Adversarial Assessment is completed in Spin 2.
- Based on the LUT Retest results, USD(AT&L) authorized a limited DOD-wide KMI Spiral 2, Spin 1 fielding in December 2015 with guidance to the National Security Agency (NSA) and the Services to implement mitigation plans to resolve suitability problems discovered during the LUTs.
- Users are satisfied with Spiral 2, Spin 1 capabilities, performance, and system stability. Database management problems during the LUT and LUT Retest affected software downloading. Site failover, Advanced Extremely High Frequency keying, Card Loader, F-22, KMI tokens, benign fill (a cryptographic key wrapped within an encryption key known only between the device wrapping it and the end unit), and existing Spiral 1 functions worked. During the LUT Retest, some problems remained with Mobile User Objective System (MUOS), Secure Software Provisioning, and the Host-Based Security System (HBSS) and its supporting servers.
- In February 2016, the KMI Program Management Office (PMO) changed the Full Deployment Decision (FDD) estimate from April 2017 to February 2018, thus triggering a Significant Change.
- The KMI PMO and JITC conducted a government-led Developmental Test and Evaluation-2 (DT&E-2) of Spiral 2, Spin 2 capabilities in July 2016. Major problems with Spin 2 capabilities required the KMI PMO to delay the DT&E-2 regression event from August to October 2016.
- JITC conducted no KMI operational testing in FY16 due to Spin 2 schedule delays.

System

- KMI will 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., encryption keys, cryptographic applications, and account management).
- KMI consists of core nodes that provide web operations at sites operated by the NSA, as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies.



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 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 include a client host computer with monitor and peripherals, High Assurance Internet Protocol Encryptor (KG-250), printer, and barcode scanner.

Mission

- Combatant Commands, Services, DOD agencies, other Federal 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 DOD Information Networks, 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 – Columbia, Maryland (Spiral 2 Prime)
- General Dynamics Information Assurance Division – Needham, Massachusetts (Spiral 1 Prime)
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted a LUT in April 2015 of Spiral 2, Spin 1 capabilities in accordance with a DOT&E-approved test plan, and a LUT Retest in July 2015 to verify fixes to problems discovered during the LUT. JITC published its LUT Retest Report in October 2015. The LUT examined new KMI capabilities for supporting F-22 Raptor, Advanced Extremely High Frequency and MUOS satellite systems, benign fill (a cryptographic key wrapped within an encryption key known only between the device wrapping it and the end unit), Secure Terminal Equipment enhanced cryptographic cards, new KMI tokens, HBSS and ePolicy Orchestrator server, site failover, and EKMS and KMI client workstation transition procedures.
- DOT&E published its KMI Spiral 2, Spin 1 LUT and LUT Retest Report in late October 2015 that found KMI to be operationally effective with some problems and not operationally suitable. JITC conducted a LUT of KMI Spiral 2, Spin 1 capabilities; however, JITC could not fully assess KMI cybersecurity until an Adversarial Assessment is completed in Spin 2.
- Based on the LUT Retest results, USD(AT&L) authorized a limited DOD-wide KMI Spiral 2, Spin 1 fielding in December 2015 with guidance to the NSA and the Services to implement mitigation plans to resolve suitability problems discovered during the LUTs.
- In February 2016, the KMI PMO changed the original FDD estimate to February 2018, thus triggering a Significant Change.
- KMI Operations issued the Spiral 2, Spin 1 Maintenance Release 1 (MR1) in May 2016. Spin 1 MR2 completed developmental testing in June 2016, and the KMI Configuration Control Board approved Spin 1 MR2 for production in late August 2016.
- The KMI PMO and JITC conducted the government-led DT&E-2 of Spiral 2, Spin 2 capabilities in July 2016. Major problems with Spin 2 capabilities required the KMI PMO to delay the DT&E-2 regression event from August to October 2016.
- JITC conducted no KMI operational testing in FY16, due to Spin 2 schedule delays.
- The DOD Chief Information Officer convened KMI Executive Management Reviews that focused attention on significant problems with the KMI schedule, developer staffing, and shared test infrastructure resources. The KMI PMO, Service stakeholders, and test community met to help orchestrate the integrated Spin 2 and Spin 3 schedule that accounts for KMI development, KMI and EKMS sustainment, shared test infrastructure usage, and operational risk reduction with EKMS message server hardware and software upgrades.
- All Services are fielding KMI Spiral 2, Spin 1; account transitions as of October 2016 are:
  - Army - 97
  - Air Force - 192
  - Navy - 235
  - Defense Agencies - 25
- The Army will accelerate account transitions with the Spin 2 fielding decision projected for late 2017. The Army will be unable to transition all of its Non-secure Internet Protocol Router Network key managers to KMI before December 2017 and will need EKMS extended into 2018. The Navy indicated that some afloat accounts will not transition until 2018 and will need EKMS to accomplish the transition process.

Assessment

- Users are satisfied with Spiral 2, Spin 1 capabilities, performance, and system stability. Functionality improved for the LUT Retest, but some suitability problems remain unresolved.
- KMI Spiral 2, Spin 2 developmental and operational testing is at least 12 months behind schedule, and the program is at risk of not meeting its new FDD in 2018.
- Service users completed the Spin 2 DT&E-2 in July 2016, identifying numerous critical problems, some of which are process and procedural problems related to EKMS-to-KMI transition. PMO regression testing of the fixes to those defects began in September 2016.
- The KMI Spiral 2, Spin 2 test schedule is aggressive and high-risk based on the time required to integrate and test the previous spin's capabilities.
- The KMI PMO delayed the Spiral 2, Spin 2 Operational Assessment due to software integration problems found in the Spin 2 DT&E-2. Additionally, the KMI PMO experienced significant Spin 3 integration and developmental testing delays. Because of these delays, the KMI PMO can only develop, test, and field three of four spins prior to the desired EKMS end-of-life date in 2017.
- Problems observed in previous developmental testing, if not corrected during system development, could adversely affect the system's effectiveness, suitability, or survivability during the KMI Spiral 2, Spin 2 LUT, which the KMI PMO delayed from January 2017 to June 2017.
- The KMI training system (separate from the operational KMI system) has connection and updating problems that effect KMI courses and student training.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed one of the FY14 and FY15 recommendations. The following remain unresolved:
  1. Improve rigor of the KMI software development and regression process to identify and resolve problems before entering operational test events.
  2. Allot adequate schedule time to support test preparation, regression, post-test data analysis, verification of corrections, and reporting to support future deployment and fielding decisions.
  3. 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.
4. Demonstrate a regular maintenance release schedule and resolve the backlog of deficiencies.
5. Ensure that appropriate transition and funding plans are in place to continue development and support fielding efforts beyond FY17 target dates, since all Services will have some accounts that will not transition until FY18.
6. Resolve HBSS version management and re-verification process problems that obstruct autonomous operations.
7. Improve and institutionalize rigorous configuration management, software and security update processes, and version controls to properly sustain KMI.
8. Ensure adequate engineering, second echelon, system administrators, database managers, and NSA/Service Help Desk and transition staffs are available to support surge fielding and long-term KMI sustainment.

- FY16 Recommendations. The KMI PMO should:
  1. Ensure shared test resources are synchronized with competing NSA program and sustainment efforts, and continue to maintain an overall schedule that is executable with coordinated Service support and participation.
  2. Prepare to extend the EKMS end-of-life, as the Navy has indicated that some afloat accounts will not transition until 2018 and will need EKMS to accomplish the transition process. The Army will be unable to transition all of its Non-secure Internet Protocol Router Network key managers to KMI before December 2017 and will need EKMS extended into 2018.
  3. Improve KMI training system connectivity, software updating, and sustainment support for KMI courses and student training.