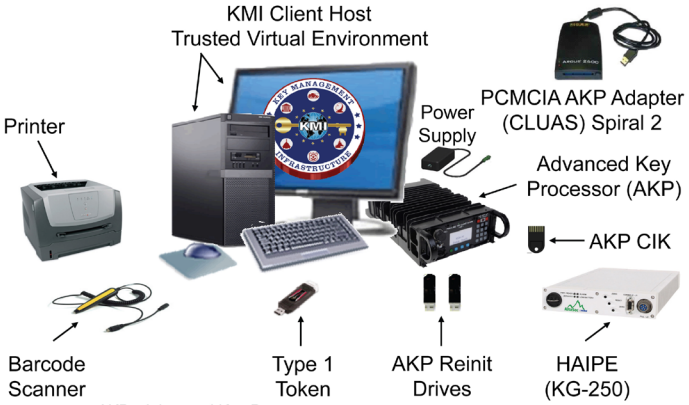
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- In coordination with the Key Management Infrastructure (KMI) Program Management Office (PMO), the Joint Interoperability Test Command (JITC) conducted a Limited User Test (LUT) of Spiral 2, Spin 1 capabilities in April 2015, and a LUT Retest in July 2015 to verify deficiency corrections. Testing was conducted in accordance with a DOT&E-approved test plan.
- 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, Advance Extremely High Frequency keying, card loader, F-22, KMI tokens, benign fill, and existing Spiral 1 functions worked. During the LUT Retest, some problems remained with Mobile User Objective System, Secure Software Provisioning, and the Host-Based Security System (HBSS) and its supporting servers.
- The National Security Agency's (NSA) KMI Help Desk and tiered engineering support personnel lacked specific transition-related knowledge and not enough experienced personnel were available to support extended coverage hours. NSA and Service Help Desks are not prepared for surge transition and sustainment.
- KMI Spiral 2, Spin 2 developmental and operational testing is at least 12 months behind schedule, and the program will probably not be able to meet its Full Deployment Decision in April 2017.
- JITC and Service test participants identified a growing backlog of high-priority deficiencies that remain unresolved. The Service leads requested that the PMO resolve the backlog of deficiencies before continuing new development.

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., 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, intelligence community, and agencies.
- 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 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 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

- In coordination with the KMI PMO, JITC conducted a LUT of Spiral 2, Spin 1 capabilities in April 2015, and a LUT Retest in July 2015 to verify deficiency corrections, in accordance with a DOT&E-approved test plan.
- Sixty-nine operationally representative Air Force, Army, Marine Corps, Navy, and civil KMI account users participated during the LUT and its retest at geographically dispersed sites.
- DOT&E submitted a classified report detailing results of the LUT and LUT Retest in October 2015.
- NSA and JITC evaluated KMI Spiral 2, Spin 1 cybersecurity in the LUT Retest; the results are classified.
- JITC is developing plans for a Spiral 2, Spin 2 Operational Assessment in 2QFY16 and a LUT to be conducted in 4QFY16.

Assessment

- Users are satisfied with Spiral 2, Spin 1 capabilities, performance, and system stability. Functionality improved for the LUT Retest but suitability problems remained.
- 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, and existing Spiral 1 functions worked. During the LUT Retest, some problems remained with Mobile User Objective System, Secure Software Provisioning, and the HBSS and its supporting server.
- The PMO's KMI token reliability growth program continues to identify fault modes and has demonstrated improved reliability.
- KMI Spiral 2, Spin 2 developmental and operational testing is at least 12 months behind schedule, and the program will probably not meet its Full Deployment Decision in April 2017.
- JITC and Service test participants identified a growing backlog of high-priority deficiencies that remain unresolved. The Service leads requested that the PMO resolve the backlog of deficiencies before continuing new development.
- The LUT Retest concluded with only one high-priority product inventory discrepancy.
- The KMI program implemented a re-verification process for account holders, Advanced Key Processor, tokens, and the client that creates unannounced service interruptions when re-verifications are missed. The re-verifications and HBSS-enforced software version controls prevent KMI from operating autonomously for 6-9 months as designed. NSA must address these process-related system-enforced conflicts, to enable the National Guard, Army Reserve, remotely-deployed units, and submarine forces to be able to operate with KMI.
- During the LUT, the Army identified 26 new KMI tokens at the depot that failed at initialization out-of-the box (10.4 percent failure rate), indicating problems with the manufacturing production process. The PMO corrected problems in manufacturing, which helped bring the overall depot failure rate for both the LUT and LUT Retest down to 2.6 percent (52 out of 1,978 tokens).
- The KMI PMO successfully demonstrated continuity of operations planning and execution, by conducting a failover to the backup site during live operations.
- The NSA Help Desk and tiered engineering support personnel lacked specific transition-related knowledge. In addition, not enough experienced KMI engineering, second echelon, system administrators, database management, and Help Desk personnel were available to support extended coverage hours; this problem was previously reported by DOT&E at the 2012 KMI IOT&E, 2013 FOT&E, and again at the 2014 Operational Assessment. The NSA and Service Help Desks are not prepared for surge transition and sustainment, as some new Help Desk technicians lack KMI experience and system knowledge. This was especially noticeable during transition support.
- Problems observed in previous 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 is scheduled to begin in 4QFY16.
  - There may be latent software flaws that could affect ongoing mission operations.
  - NSA and Service Help Desk manning may not be adequately staffed to support the pace of transition from EKMS to KMI.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed two of the five FY14 recommendations. The following remain unresolved:
  1. Continue to 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. Continue to 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.
- FY15 Recommendations. The KMI PMO should:
  1. Resolve the mounting backlog of deficiencies and establish a regular maintenance release schedule.
  2. Ensure that appropriate transition and funding plans are in-place to continue development and support fielding efforts beyond FY17 target dates.
  3. Resolve HBSS version management and re-verification process problems that obstruct autonomous operations.

4. Implement improved and rigorous configuration management, Configuration Control Board, Information Assurance Vulnerability Alert update processes and controls to properly sustain KMI.
5. Ensure adequate engineering, second echelon, system administrators, database managers, and NSA and Service Help Desk and transition staff are available to support surge fielding and long-term KMI sustainment.