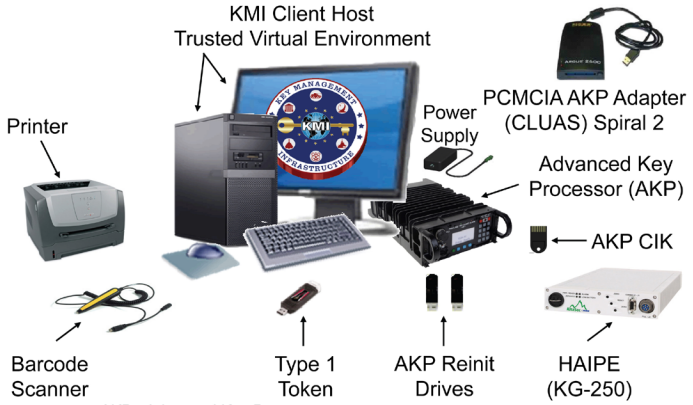
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an adequate Limited User Test (LUT) of Key Management Infrastructure (KMI) Spiral 2, Spin 2 capabilities in June/July 2017 in accordance with a DOT&E-approved test plan.
- DOT&E published its KMI Spiral 2, Spin 2 LUT Report in late September 2017 that found KMI to be operationally effective and operationally suitable for day-to-day operations, but not suitable for long-term sustainment.
- The KMI Program Management Office (PMO) should address the seven Priority 2 defects discovered during the LUT.
- Sustainment, manpower, KMI Training System (KMITS), configuration management, and documentation problems prevent KMI from being operationally suitable for long-term sustainment.
- The KMI PMO plans to eliminate some late Increment 2 requirements and interfaces (e.g., the Enterprise Service Bus that interoperates with the Dynamic Product Catalog, automating the Legacy Catalog Manager function for symmetric key generation requests). The KMI PMO should delay the KMI Increment 2 FOT&E until the system architecture, critical Spin 3 functionality, and interfaces are ready for test.

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 tools).
- KMI consists of core nodes that provide web operations at sites operated by the National Security Agency (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.
- 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)
- SafeNet – Belcamp, Maryland
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted an operational assessment (OA) of KMI Spiral 2, Spin 2 capabilities in January/February 2017 in accordance with a JITC-approved test plan. JITC approved the test plan in accordance with delegated authority in the DOT&E policy memorandum, "Guidelines for OT&E of Information and Business Systems," September 14, 2010.

To support agile acquisition and fielding approaches, DOT&E delegates test plan approval on an assessment of moderate or low overall risk to mission accomplishment of new software integration. The KMI Spiral 2, Spin 2 OA was assessed as low risk.

- DOT&E published its KMI Spiral 2, Spin 2 OA Report in early April 2017.
- The KMI PMO received new Model H KMI tokens in 2017 that need to be integrated and tested.
- JITC conducted a LUT of KMI Spiral 2, Spin 2 capabilities in June/July 2017 in accordance with a DOT&E-approved test plan.
- DOT&E published its KMI Spiral 2, Spin 2 LUT Report in late September 2017.
- During the LUT, JITC examined new KMI capabilities and enhancements for supporting:
  - F-22 Raptor
  - Advanced Extremely High Frequency and Mobile User Objective System 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
  - Site failover
  - EKMS and KMI client workstation transition procedures
- The KMI PMO and JITC plan to conduct a Spin 3 OA and an Increment 2 FOT&E in early FY18; however, some externally provided critical interfaces will not be ready to support this schedule.
- The KMI Program Manager deferred Window 10 client migration until after the projected KMI Increment 2 Full Deployment Decision projected for late March 2018.

Assessment

- KMI Spiral 2, Spin 2 builds upon the existing KMI operational baseline, and automates some key management and delivery actions. The Spin 2 software incorporates NSA-approved specifications and protocols that will allow commercial developers to create new KMI-aware devices with increased security to protect key material from compromise.
- KMI Spin 2 provides a Non-classified Internet Protocol Router Network capability that will allow the Service and agency key managers to complete the transition from the legacy EKMS to KMI for remote user sites.
- The KMI Program Manager delayed the start of the KMI Spiral 2, Spin 2 OA to correct deficiencies found during earlier developmental testing. The KMI team's troubleshooting efforts during the brief delay yielded a stable KMI client software baseline, notably reduced defects, and improved JITC's ability to accomplish all of the OA goals.
  - During the OA, all Spin 2 capabilities and enhancements performed as required, although JITC assessed some of the transformational capabilities using developer-provided emulators that JITC has not independently validated.
  - JITC discovered only three Priority 2 defects during the Spin 2 OA; none precluded KMI software deployment for the Spin 2 LUT. The positive OA results demonstrated that the KMI Spiral 2, Spin 2 software baseline was mature and posed low risk to operations to deploy into the production environment for the June 2017 LUT.
  - The KMI Spin 2 OA demonstrated that the KMI PMO did not adequately maintain the KMI Test Infrastructure, which the NSA uses for both system development and software maintenance testing, at the same level as the NSA does for the operational KMI system. This sustainment lapse led to unnecessary test interruptions and delays, with some users experiencing problems with system access because of a lack of reverification of their KMI roles. Because the NSA will use the KMI Test Infrastructure to test maintenance releases throughout the KMI system lifecycle, it is important from a sustainment perspective that the NSA give the same attention to configuration management for both the operational and test instantiations of the KMI system.
- The LUT demonstrated that KMI Spiral 2, Spin 2 is operationally effective and operationally suitable for day-to-day operations, but not suitable for long-term sustainment.
- JITC evaluated all of the new Spin 2 capabilities during the LUT that did not require the use of an emulator. All KMI capabilities in previous releases continued to function to support the operational missions. JITC discovered seven Priority 2 defects during the LUT.
- The LUT showed that sustainment, manpower, KMITS, configuration management, and documentation problems still exist that hamper long-term sustainment.
  - Service and agency Regional Sparing Warehouses are not yet fully established and provisioned as defined in published Service sustainment plans.
  - KMI staffing, especially at the alternate site and civil support facilities, is not sufficient to support all existing and planned new capabilities, networks, and users.
  - KMITS availability is insufficient to support user training because of excessive unplanned downtime. All Services reported KMITS availability shortfalls ranging from hours to days per 2-week class.
  - KMI did not have accurate universal key installation procedures and system configuration management to support asymmetric key ordering.
  - The KMI PMO was 2 months late in providing the Services with proper network change requests and KMI-related Authority to Operate documentation.
- The KMI PMO plans to eliminate some late Increment 2 requirements and interfaces (e.g., the Enterprise Service Bus that interoperates with the Dynamic Product Catalog, automating the Legacy Catalog Manager function for symmetric key generation requests). This will delay delivery of critical functionality, and leave the system architecture in an incomplete state for the Increment 2 FOT&E as currently scheduled by the PMO. The KMI PMO currently does not have plans to operationally test changes to the KMI system architecture and any NSA-deferred Increment 2 requirements and interfaces for the Services.
- KMI has 4 operational test events in 13 months from January 2017 through January 2018. The PMO is exhausting

the Service users and test team, trying to achieve a March 2018 Full Deployment Decision. Normally, two operational test events in a year is a major endeavor. The KMI PMO is not ready for the Increment 2 FOT&E, and it is deferring critical capabilities to maintain schedule.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed one of three previous FY16 recommendations. The following remain:
  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. Improve KMITS connectivity, software updating, and sustainment support for KMI courses and student training.
- FY17 Recommendations.
  1. The KMI PMO should:
     - Resolve all Priority 2 defects and verify acceptability to users prior to Spin 2 full deployment.
     - Maintain the KMITS to the same degree as the operational environment to support Service and agency training schedules.
     - Continue to improve token reliability and production quality control.
     - Provide network change and coordinating documentation to the Services with enough lead time for the Services to make those changes without using crisis management processes to support KMI efforts, particularly as it pertains to universal changeover.
     - Delay the KMI Increment 2 FOT&E until the system architecture, critical Spin 3 functionality, and interfaces are ready for test.
     - Plan for JITC to conduct a post-Increment 2 OA and LUT to evaluate KMI client upgrades to Windows 10, since the PMO delayed integrating that operating system until beyond Spin 3.
     - Establish a more realistic timeline for future KMI capability testing that supports revised milestone decisions, while managing expectations of those with KMI equities.
  2. NSA's KMI Operations should:
     - Improve KMI configuration management and develop procedures for loading universal keys for asymmetric key generation.
     - Reassess KMI Operations staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.
  3. Services and agencies should:
     - Establish and provision Regional Sparing Warehouses per their sustainment plans to meet client availability and Administrative and Logistics Delay Time requirements.
  4. JITC should:
     - Determine how and under what conditions transformation capabilities will be tested in a live operational environment.
     - Evaluate the new Model H KMI token for reliability during Spin 3 OA and Increment 2 FOT&E.