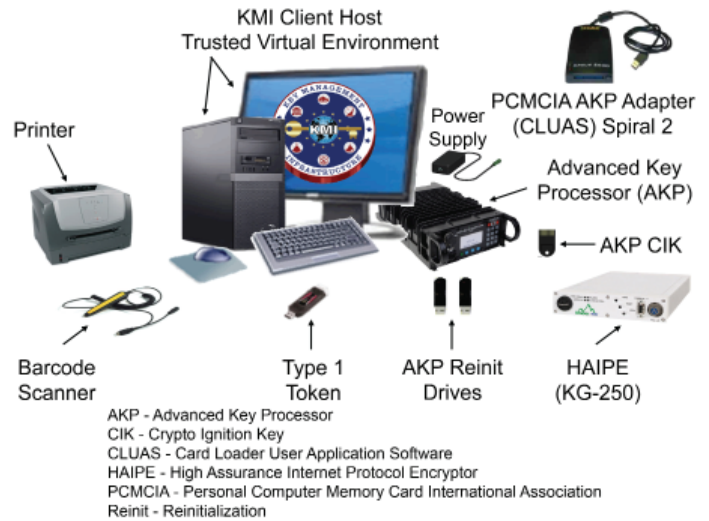# Key Management Infrastructure (KMI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an Operational Assessment (OA) of Key Management Infrastructure (KMI) Increment 2 Spiral 2, Spin 3 capabilities in October/November 2017.
- DOT&E published its KMI Spiral 2, Spin 3 OA Report in March 2018 that found system stability, usability, and maturity continue to improve. However, some high-priority defects remained in the KMI Spiral 2, Spin 3 software. Sustainment, KMI Operations staffing, KMI Test Infrastructure, and configuration management problems prevent KMI from being operationally suitable for long-term sustainment.
- The USD(A&S) delegated Milestone Decision Authority for the KMI Increment 2 program to the National Security Agency (NSA) Senior Acquisition Executive in March 2018.
- JITC conducted an FOT&E of KMI Increment 2 that included Spin 3 capabilities in April/June 2018. The FOT&E examined KMI regression capabilities, enhancements to existing functionality, the NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- During the KMI Increment 2 FOT&E, the KMI Spin 3 capabilities did not perform successfully. JITC did not fully test the NATO capabilities due to a high-priority finding that halted the planned NATO account transition. Also, a large number of high-priority system findings led the KMI Program Management Office (PMO) to fix the problems and plan to re-test the FOT&E in January/February 2019. DOT&E will make operational effectiveness, suitability, and survivability/cybersecurity determinations after the FOT&E re-test.

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 tools).
- 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.
- 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.

KMI Client Host Trusted Virtual Environment
Printer
PCMCIA AKP Adapter (CLUAS) Spiral 2
Power Supply
Advanced Key Processor (AKP)
AKP CIK
Barcode Scanner
Type 1 Token
AKP Reinit Drives
HAIPE (KG-250)

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

The COTS components include a client host computer with monitor and peripherals, printer, and barcode scanner.

- The NSA is delivering KMI Increment 2 in two spirals with Spiral 2 having three development spins. The NSA previously delivered KMI Increment 2, Spiral 1 and Spiral 2, Spin 1 and Spin 2. KMI Increment 2 Spiral 2, Spin 3 is the final capability delivery for the increment.

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 Network, 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, and Advanced Extremely High Frequency Satellite System.

Major Contractors

- Leidos – Columbia, Maryland (Spiral 2 Prime)
- General Dynamics Information Technology – Dedham, Massachusetts
- SafeNet – Belcamp, Maryland
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted an OA of KMI Increment 2 Spiral 2, Spin 3 capabilities in October/November 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. DOT&E and JITC assessed the KMI Spiral 2, Spin 3 OA as low risk.
- The USD(AT&L) published the KMI Spiral 2, Spin 2 limited fielding Acquisition Decision Memorandum in November 2017 that directed the NSA and the Services to resolve the long-term sustainability problems to include staffing levels, training infrastructure availability, adequacy of spares, and help desk operations prior to the Increment 2 FOT&E.
- The USD(A&S) delegated Milestone Decision Authority for the KMI Increment 2 program to the NSA Senior Acquisition Executive in March 2018.
- JITC conducted a KMI Spiral 2, Spin 3 defect resolution verification test in January 2018.
- DOT&E published its KMI Spiral 2, Spin 3 OA Report in March 2018.
- JITC conducted an FOT&E of KMI Increment 2 capabilities in April/June 2018 in accordance with a DOT&E-approved test plan. Due to KMI Spin 3 capabilities performance and configuration management problems in FOT&E, the KMI PMO intends to re-test the Increment 2 FOT&E in January/February 2019.
- The KMI PMO changed the estimated Increment 2 Full Deployment Decision to late April 2019.

Assessment

- The KMI Spiral 2, Spin 3 OA indicated system stability, usability, and maturity continue to improve. However, some high-priority defects remained in the KMI Spiral 2, Spin 3 software. Sustainment, KMI Operations staffing, KMI Test Infrastructure, and configuration management problems prevent KMI from being operationally suitable for long-term sustainment.
- JITC evaluated all of the new Spin 3 capabilities during the OA, and all KMI capabilities in previous releases continued to function to support the operational missions. JITC discovered 15 high-priority defects during the OA.
- The Increment 2 FOT&E examined KMI regression capabilities, enhancements to existing functionality, the NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- The KMI Spin 3 capabilities did not perform successfully in FOT&E. JITC did not fully test the NATO capabilities due to a high-priority finding that halted the planned NATO account transition. The large numbers of high-priority system findings led the KMI PMO to fix the problems and plan the future re-test for the Increment 2 FOT&E. DOT&E will make operational effectiveness, suitability, and survivability/cybersecurity determinations after the FOT&E re-test.
- The NSA KMI Operations continues to surge manning for operational test events and has reoccurring staffing shortages that affect long-term system sustainment.
- The KMI PMO now has an executable schedule to fix and operationally test/re-test the remaining Increment 2 capabilities, including system maintenance releases and Windows 10 client integration.

Recommendations

- The KMI PMO should:
  1. Continue to resolve all high-priority defects and verify acceptability on the integrated Windows 10 KMI client to users prior to Increment 2 FOT&E re-test and full deployment.
  2. Maintain the KMI Test Infrastructure to the same degree as the operational environment.
- The NSA KMI Operations should:
  1. Improve KMI configuration management and long-term sustainment.
  2. Reassess KMI Operations staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.