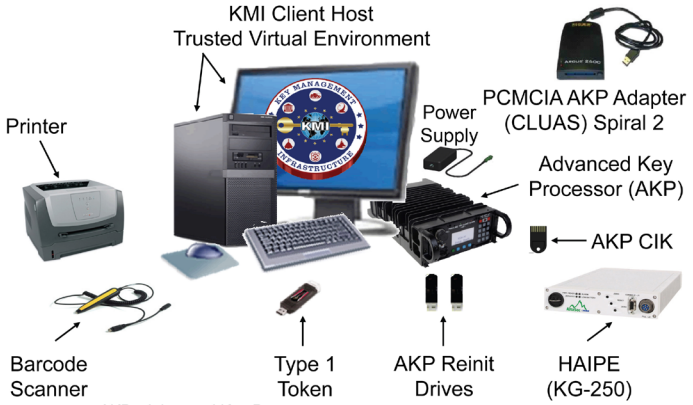
Key Management Infrastructure (KMI)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted FOT&E-2 of Key Management Infrastructure (KMI) Increment 2 that included new capabilities and enhanced functionality integrated with a Windows 10 upgrade in May/June 2019. The FOT&E-2 examined KMI enhancements to existing functionality, KMI's NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- The KMI FOT&E-2 demonstrated that the software baseline is operationally effective, suitable, and secure for continued operational deployment.
- DOT&E published the KMI Increment 2 FOT&E-2 report in September 2019 to inform a Full Deployment Decision in November 2019.

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 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 (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. 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 the 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 FOT&E-2 of KMI Increment 2 that included new Spin 3 capabilities and enhanced functionality integrated with a Windows 10 upgrade in May/June 2019 in accordance with a DOT&E-approved test plan.
- The FOT&E-2 examined KMI enhancements to existing functionality, KMI's NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- DOT&E published the KMI Increment 2 FOT&E-2 report in September 2019 to inform a Full Deployment Decision in November 2019.
- The KMI Program Management Office (PMO) and test community are developing a KMI Increment 3 Test and Evaluation Master Plan to support a projected Milestone B decision in FY20.

Assessment

- The KMI FOT&E-2 demonstrated that the software baseline is operationally effective, suitable, and secure for continued operational deployment. The KMI performance is summarized below:
  - The NSA included a Windows 10 upgrade and system integration in the FOT&E-2 using upgraded scripts that performed near flawlessly and were notably improved over previous installation scripts.
  - KMI system documentation, Service help desks, and training were adequate to support the mission.
  - KMI had problems synchronizing common account data for cryptographic product transfers from some Navy and all NATO accounts to non-KMI (manual) accounts.
  - The secure software provisioning capability that allows users to download information assurance vulnerability alerts had slow delivery.
  - NSA KMI Operations temporarily surged manning for the operational test and has recurring staffing shortages that affect long-term system sustainment.
  - The NSA KMI help desk, which supports DOD agency and external (non-DOD) users, lacks adequate knowledge of the system and is subject to high staff turnover rates.
  - Long-standing KMI configuration management problems remain that require experienced system and database administration, rigid process adherence, adequate staffing, and monitoring to sustain configuration consistency between core nodes throughout the KMI lifecycle.
- The KMI Test Infrastructure (TI) provides a safe laboratory for evaluating KMI software builds; however, the KMI TI is not maintained in the same configuration as the operational KMI. This limits the KMI TI's ability to accurately identify problems prior to deploying a new KMI version to the operational system.

Recommendations

- The KMI PMO should:
  1. Continue to resolve system defects and sustainment problems.
  2. Maintain the KMI TI 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 and help desk staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.