Key Management Infrastructure (KMI)

The Key Management Infrastructure (KMI) Program Management Office (PMO) began Capability Increment 3 (CI-3) development in FY21. The National Security Agency (NSA) awarded a major contract modification in FY23 that increased the KMI CI-3 scope to address additional technical requirements packages in 10 Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late FY23. The KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy and the TEMP in FY25 to support a full deployment decision (FDD) in FY27. DOT&E intends to publish a preliminary performance assessment following completion of the KMI CI-3 multi-release operational testing in FY25.

SYSTEM DESCRIPTION

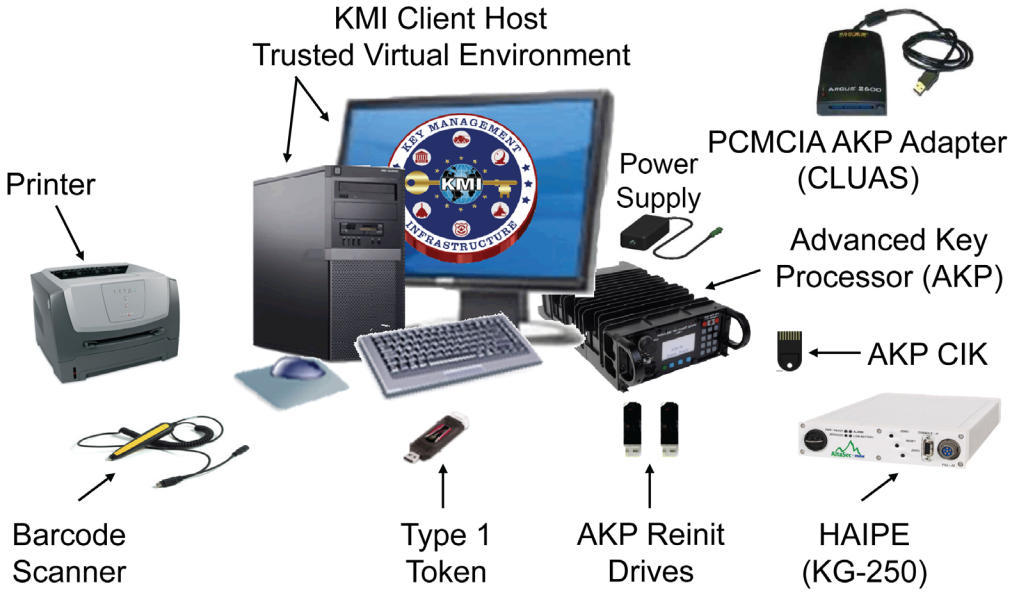
KMI provides a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products, to include encryption keys, cryptographic applications, and account management tools. KMI consists of core nodes that provide web operations at sites operated by the NSA, as 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. The KMI CI-3 delivery will enhance the deployed KMI CI-2 capabilities with a combination of custom software development and commercial off-the-shelf computer components, which include a client host computer with monitor and peripherals, 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 Network, and initiatives such as Cryptographic Modernization.

Service members will use KMI cryptographic products and services to enable security (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.



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

PROGRAM

The NSA intended to deliver KMI CI-3 in eight planned Agile releases to enhance existing capabilities. The KMI CI-3 PMO began capability development in FY21 and announced a schedule delay in FY22, due to hardware technical refresh, supply chain delivery delays, system configuration problems, and expanded requirements. The NSA awarded a major contract modification in FY23 that increased the KMI CI-3 scope to address additional technical requirements in 10 total Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late FY23, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy in FY25 to support an FDD in FY27.

» MAJOR CONTRACTORS

- Leidos – Columbia, Maryland (Prime)
- SafeNet Inc., a subsidiary of Thales Group – Belcamp, Maryland

TEST ADEQUACY

In FY20, DOT&E approved the initial KMI CI-3 TEMP that defined an adequate operational test strategy for the KMI program release testing through IOT&E. The KMI CI-3 PMO incurred a major TEMP deviation in FY23, due to the NSA needing to provide a hardware and software technical refresh before delivering KMI CI-3 software releases. The KMI CI-3 PMO and the Joint Interoperability Command (JITC) are updating the KMI CI-3 TEMP to address test strategy, capability scope, and integrated schedule changes with submission to DOT&E now expected in FY25. JITC continues to develop an operational test plan to support KMI CI-3 technical refresh release testing in the production environment, which is now expected to commence in FY25. The KMI CI-3 PMO and JITC intend to operationally test the initial seven KMI capability releases later in FY25. DOT&E intends to publish an assessment of the initial KMI CI-3 capabilities in FY25.

The current Key Management Enterprise (KME) schedule includes concurrent test planning, execution, and reporting between KMI CI-3, Symmetric Catalog Synchronization, Enterprise Service Bus, and legacy Electronic Key Management System efforts. This many parallel activities adds risk

to the program, as evidenced by the schedule delays over the past three years. While the KMI Test Infrastructure provides a safe environment for evaluating KMI software builds, it is currently not in the same configuration as the operational KMI. This may limit the KMI Test Infrastructure users' ability to identify problems prior to deploying a new KMI release to the operational system.

PERFORMANCE

DOT&E will provide a preliminary performance assessment after completion of the KMI CI-3 multi-release testing for the initial Agile releases, scheduled for FY25.

RECOMMENDATIONS

1. The KMI CI-3 PMO should reassess the release cadence and content to reduce test and delivery concurrency to make the integrated schedule more achievable, as recommended in the FY22 and FY23 Annual Reports.
2. The KMI CI-3 PMO and JITC should complete the KMI CI-3 TEMP updates to align the test strategy with the revised acquisition strategy, program baseline, and integrated schedule, as recommended in the FY23 Annual Report.
3. The NSA should mirror the KMI Test Infrastructure configuration to be the same as the operational environment, as recommended in the FY22 and FY23 Annual Reports.