Key Management Infrastructure (KMI)

The Key Management Infrastructure (KMI) Capability Increment 3 (CI-3) Program Management Office (PMO) began capability development in July 2021. The National Security Agency (NSA) awarded a major contract modification in late January 2023 that increases the KMI CI-3 scope to address additional technical requirements packages in ten Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late September 2023, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy and the Test and Evaluation Master Plan (TEMP) in early FY24 to support a full deployment decision (FDD) in FY27. A preliminary performance assessment will be available after completion of the KMI CI-3 multi-release testing in late FY24 or early 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.
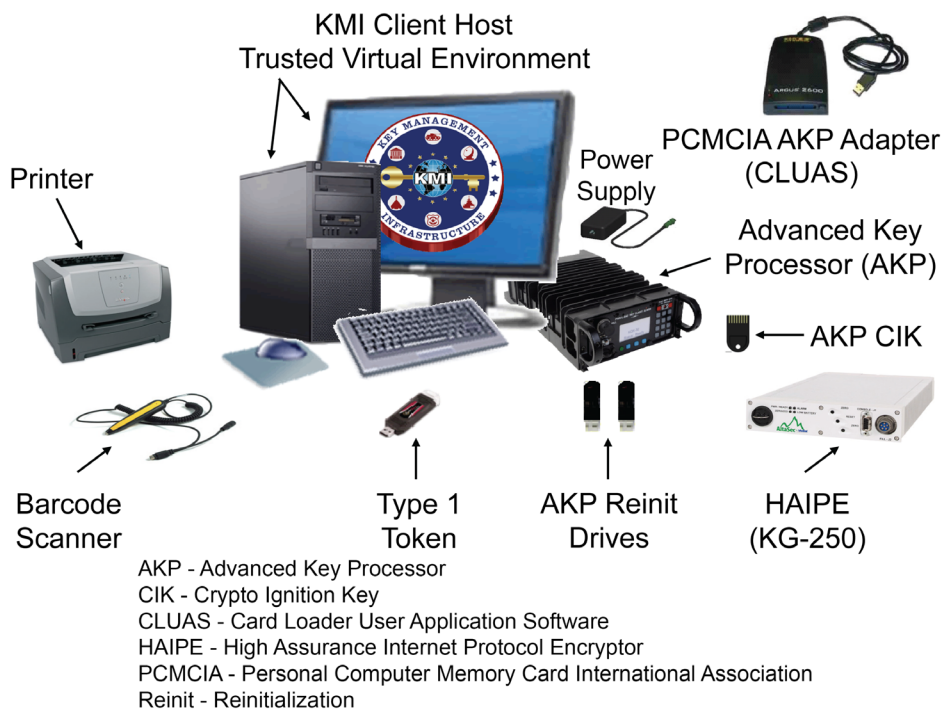
MISSION

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.

PROGRAM

The NSA intended to deliver KMI CI-3 in eight planned Agile releases to enhance existing capabilities and be transition capable for the legacy Electronic Key Management System (EKMS) Tier 0 and Tier 1 cryptographic product delivery into the infrastructure. The KMI CI-3 PMO began capability development in July 2021. The KMI CI-3 PMO announced a schedule delay in April 2022, due to hardware technical refresh, supply chain delivery delays, system configuration problems, and expanded requirements. The NSA awarded a major contract modification in late January 2023

KMI Client Host Trusted Virtual Environment

Printer

Power Supply

PCMCIA AKP Adapter (CLUAS)

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

that increased the KMI CI-3 scope to address additional technical requirements packages in ten total Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late September 2023, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy in early FY24 to support FDD in FY27.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

DOT&E approved the initial KMI CI-3 TEMP in August 2020 that defines 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 by not adhering to the approved test strategy, and the NSA had to provide a hardware technical refresh before delivering 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 expected in FY24. The JITC KMI test team will employ a multi-release test plan that can cover up to six of the initial Agile releases in an operational test plan. JITC is developing an operational test plan to support KMI CI-3 technical refresh release testing in the production environment that will commence in FY24. The KMI CI-3 PMO and JITC intend to operationally test the initial six KMI capability releases later in FY24 or early FY25.

PERFORMANCE

A preliminary performance assessment will be available after completion of the KMI CI-3 multi-release testing for the initial Agile releases scheduled for late FY24 or early 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 EKMS efforts. This many parallel activities adds risk to the program. In addition, 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. The KMI CI-3 PMO is in the process of a technical refresh for the KMI Test Infrastructure to mirror the production system.

RECOMMENDATIONS

1. The KMI CI-3 PMO should reassess the release cadence and content to reduce delivery and test concurrency to make the integrated schedule more achievable as recommended in the FY22 Annual Report.

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.

3. The NSA should mirror the KMI Test Infrastructure configuration to be the same as the operational environment as recommended in the FY22 Annual Report.