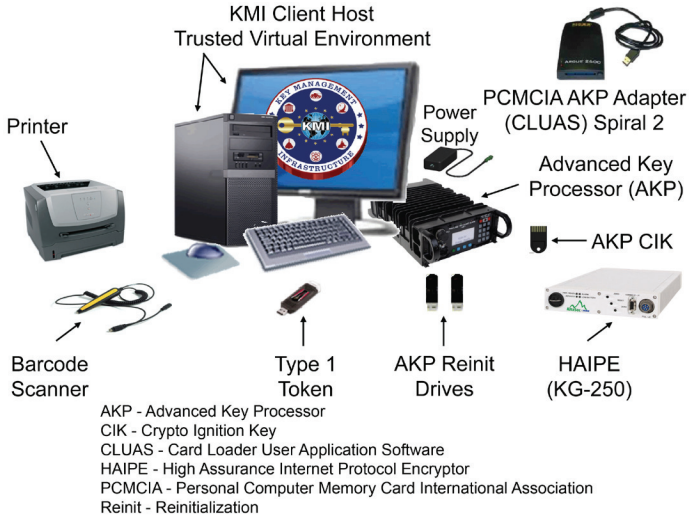
Key Management Infrastructure (KMI)

Executive Summary

- The Key Management Infrastructure (KMI) Program Management Office (PMO) and Joint Interoperability Test Command (JITC) completed the KMI Spiral 2 Test and Evaluation Master Plan (TEMP) Addendum, and DOT&E approved it on March 7, 2014.
- The National Security Agency (NSA) Senior Acquisition Executive declared a KMI program deviation on August 29, 2014, due to missing the Acquisition Program Baseline's Spiral 2, Spin 1 software release date in July 2014. The PMO's revised release date will be January 31, 2015.
- JITC conducted an operational assessment (OA) of Spiral 2, Spin 1 capabilities and the new KMI tokens in September 2014. DOT&E issued a classified OA report in November 2014.
- The OA successfully demonstrated new KMI capabilities for supporting F-22 Raptor, Advance Extremely High Frequency and Mobile User Objective System Satellite systems, Benign Keying, Secure Terminal Equipment enhanced cryptographic cards, new tokens, and transition procedures. The OA concluded with no high-priority discrepancies.
- While the OA was successful, DOT&E and JITC identified the following areas for improvement:
  - The KMI system executed the Secure Software Provisioning capability as designed; however, due to inadequate training and procedural problems, the KMI staff had difficulty uploading and titling the software packages for distribution to KMI operating accounts. Secure Software Provisioning did not perform properly for file uploads and downloads, and installation procedures were inadequate.
  - The NSA and Service help-desk manning and training observed during the OA is inadequate to meet KMI installation, network, and daily activities for Service worldwide transition and rollout of the Spiral 2, Spin 1 system.
  - Additional training and enhanced standard operating procedures are needed at the KMI sites to leverage the automated notifications in the KMI system. Those procedures need to be refined and rehearsed for routine and critical situations.

System

- KMI is intended to replace the legacy Electronic Key Management System to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., encryption keys, cryptographic applications, and account management).



- 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, intelligence community, and 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, High Assurance Internet Protocol Encryptor (KG-250), monitor, keyboard, mouse, printer, and barcode scanner.

Mission

- Combatant Commands, Services, DOD agencies, other Federal Government 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)
- General Dynamics Information Assurance Division – Needham, Massachusetts (Spiral 1 Prime)
- BAE Systems – Linthicum, Maryland
- L3 Communications – Camden, New Jersey
- SafeNet – Belcamp, Maryland
- Praxis Engineering – Annapolis Junction, Maryland

Activity
- The PMO and JITC completed the KMI Spiral 2 TEMP Addendum, and DOT&E approved it on March 7, 2014. The KMI TEMP Addendum describes the test and evaluation strategy to support planned Spiral 2 program activities. The PMO and JITC produced the TEMP Addendum to align the formal test program with the PMO's implementation of an Agile software development methodology. The PMO is planning four software releases (one spin per year) that will lead to a Full Deployment Decision by April 2017.
- The PMO rolled out new KMI tokens in May 2014 to reduce fault modes and improve reliability. The PMO conducted reliability growth tests to evaluate the tokens, and the JITC and Service representatives evaluated the new tokens in Spiral 2, Spin 1 Developmental Test and Evaluation (DT&E) events in June and July 2014.
- The NSA Senior Acquisition Executive declared a KMI program deviation on August 29, 2014, due to missing the Acquisition Program Baseline's Spiral 2, Spin 1 software release date in July 2014. The PMO's revised release date is January 31, 2015.
- JITC conducted an OA of Spiral 2, Spin 1 capabilities and the new KMI tokens in September 2014.
- DOT&E issued a classified OA report in November 2014.
- JITC is developing plans for a Spiral 2, Spin 1 Limited User Test to be conducted in 2QFY15 to demonstrate that the KMI system operates comparably in the operational environment as it did in the OA's representative environment, and to gain Service stakeholder acceptance.

Assessment
- Users are satisfied with the existing Spiral 1 performance and capabilities, and the overall KMI capability is significantly improved and stable.
- The KMI PMO and test community devised a sound test approach to support the program's Agile development methodology and planned capability releases, resulting in the Spiral 2 KMI TEMP Addendum's approval.
- At the recommendation of DOT&E, the KMI PMO adopted and implemented automated software testing, additional KMI token testing, and reliability growth efforts that yielded substantive improvements in system performance and stability as observed during the Spiral 2, Spin 1 OA.
- In the government-led DT&E-2 in June 2014, JITC and Service test participants identified high-priority deficiencies, and the KMI PMO directed the developer to correct the problems and release an updated baseline to the KMI system.
- The subsequent DT&E-2 retest in late June 2014 identified additional, high-priority deficiencies and structural problems in the KMI database. These problems were exacerbated by inadequate schedule allocation before and after the DT&Es. The PMO resolved problems found in the DT&E-2 retest by mid-August 2014. The KMI PMO delayed the start of the OA approximately 60 days until sufficient regression testing was conducted to ensure the system was ready to move to the next phase of testing.
- A combination of 22 operationally representative Air Force, Army, Marine Corps, Navy, and civil KMI accounts participated during the OA at geographically-dispersed sites.
- The OA concluded with no high-priority discrepancies. The OA successfully demonstrated new KMI capabilities for supporting F-22 Raptor, Advance Extremely High Frequency and Mobile User Objective System Satellite systems, Benign Keying, Secure Terminal Equipment enhanced cryptographic cards, new tokens, and transition procedures.
- While the OA was successful, DOT&E and JITC identified the follows areas for improvement:
  - The KMI system executed the Secure Software Provisioning capability as designed; however, due to inadequate training and procedural problems, the KMI staff had difficulty uploading and titling the software packages for distribution to KMI operating accounts. Secure Software Provisioning did not perform properly for file uploads and downloads, and installation procedures were inadequate.
  - The NSA and Service help desk manning and training observed during the OA is inadequate to meet KMI installation, network, and daily activities for Service worldwide transition and rollout of the Spiral 2, Spin 1 system.
  - Additional training and enhanced standard operating procedures are needed at the KMI sites to leverage the automated notifications in the KMI system. Those procedures need to be refined and rehearsed for routine and critical situations.
- JITC assessed interoperability for fill devices, end cryptographic units, and the Electronic Key Management System information exchanges. The KMI Spiral 2, Spin 1 system is on pace to achieve interoperability.
- Continuity of operations planning and facility preparations are nearing completion; continued efforts are necessary to refine and test those capabilities and procedures.

- JITC did not evaluate KMI Spiral 2 cybersecurity in the OA but will in future test events in accordance with the KMI TEMP Addendum approved in March 2014.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed the four FY13 recommendations.
- FY14 Recommendations. The KMI PMO should:
  1. Continue to improve the KMI software development and regression processes rigor to identify and resolve problems before entering operational test events.
  2. Ensure adequate schedule time is allocated to support test preparation, regression, post-test data analysis, verification of corrections, and reporting to support future deployment and fielding decisions.
  3. Develop, codify, and distribute standard operating procedures to KMI Storefront operators and users for functions that require routine to critical coordination across the enterprise.
  4. Continue to verify increased KMI token reliability through a combination of laboratory and operational testing with automated data collection from system logs for accurate reliability and usage analysis.
  5. Fully execute the continuity of operations plan to ensure procedures and redundant facilities are adequate.