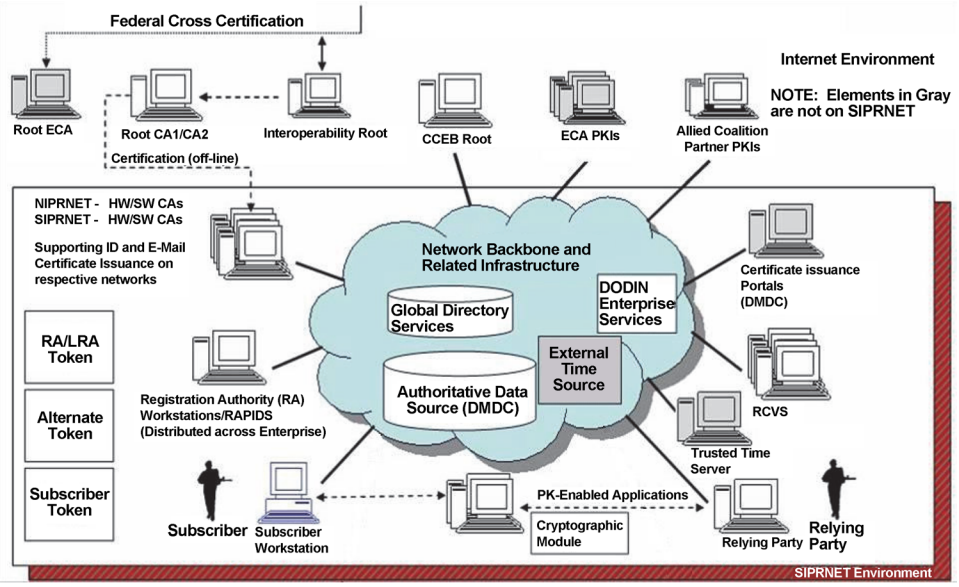
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- FOT&Es I and II, conducted in January 2013, revealed effectiveness and suitability problems. Although no operational testing has been completed since then, the program manager is addressing the requirements definition and system engineering problems that led to these deficiencies, while also making program personnel and contract management process changes to improve the program's ability to achieve restructured goals.
- In December 2014, the Public Key Infrastructure (PKI) Increment 2 Program Management Office (PMO) and the Joint Interoperability Test Command (JITC) conducted an integrated developmental test/operational test (DT/OT) for Token Management System (TMS) release 3.0 to examine code signing, token Personal Identification Number (PIN) reset, certificate recovery, and additional token issuance capabilities.
- USD(AT&L), guided by the recommendation of the Director of the National Security Agency (NSA), directed the PKI PMO to evaluate the viability of whether a one-token and/or one-infrastructure approach could achieve the DOD PKI mission requirements for both the classified and unclassified networks. This resulted in a program delay of six months.
- USD(AT&L) signed an Acquisition Decision Memorandum (ADM) in April 2015, which concluded that a one token/one-infrastructure approach would cost more money, take longer to develop, and would not improve cybersecurity. The ADM, in conjunction with the Joint Requirements Oversight Council memorandum, directed the NSA to resume development of the PKI Increment 2 program in accordance with plans developed prior to the strategic pause.
- In April and May 2015, JITC verified correction of deficiencies to resolve problems found in the integrated DT/OT for the TMS release 3.0.
- In July 2015, USD(AT&L) approved the revised PKI Acquisition Program Baseline, and approved the updated PKI Acquisition Strategy in September 2015 outlining the PKI PMO's plans to complete Spirals 3 and 4 by 2QFY18. The revised strategy focuses the remaining Increment 2 Spirals (3 and 4) on 15 user-prioritized capabilities. These capabilities are intended to improve the Secret Internet Protocol Router Network (SIPRNET) token management and reporting, improve system availability, and provide new infrastructures for the provisioning and management of the Non-classified Internet Protocol Router Network (NIPRNET) Enterprise Alternate Token System and Non-Person Entity certificates (e.g., workstations, web servers, and mobile devices).



CA – Certificate Authority
CCEB – Combined Communications Electronic Board
DMDC – Defense Manpower Data Center
DODIN – Department of Defense Information Networks
ECA – External Certification Authority
LRA – Local Registration Authority
NIPRNET – Non-secure Internet Protocol Router Network
RA – Registration Authority
RAPIDS – Real-Time Automated Personnel Identification System
RCVS – Robust Certificate Validation Service
SIPRNET – SECRET Internet Protocol Router Network

System

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. The private keys are encoded on a token, which is a credit card sized smartcard embedded with a microchip.
- DOD PKI supports the secure flow of information across the DOD Information Networks as well as secure local storage of information.
- DOD PKI uses commercial off-the-shelf hardware, software, and applications developed by the NSA.
  - The Defense Enrollment Eligibility Reporting System (DEERS) and Secure DEERS provide the personnel data for certificates imprinted on NIPRNET Common Access Cards and SIPRNET tokens, respectively.
  - DOD PKI Certification Authorities for the NIPRNET and SIPRNET tokens reside in the Defense Information Systems Agency Enterprise Service Centers in Oklahoma City, Oklahoma, and Mechanicsburg, Pennsylvania.
- Increment 1 is complete and deployed on the NIPRNET.
- The NSA is developing and deploying PKI Increment 2 in four spirals on the SIPRNET and NIPRNET. Spirals 1 and 2 are deployed, while Spirals 3 and 4 will deliver the

infrastructure, PKI services and products, and logistical support required by 15 user-prioritized capabilities.
- The Defense Information Systems Agency is supporting PKI operations, enablement, and security solutions.

Mission
- Military operators, communities of interest, and other authorized users will use DOD PKI to securely access, process, store, transport, and use information, applications, and networks.
- Commanders at all levels will use DOD PKI to provide authenticated identity management via personal identification, number-protected Common Access Cards or SIPRNET tokens to enable DOD members, coalition partners, and others to access restricted websites, enroll in online services, and encrypt and digitally sign e-mail.
- Military network operators will use Non-Person Entity certificates (e.g., workstations, web servers, and mobile devices) to create secure network domains, which will facilitate intrusion protection and detection.

Major Contractors
- General Dynamics C4 Systems – Scottsdale, Arizona (Prime)
- 90Meter – Newport Beach, California
- SafeNet – Belcamp, Maryland

Activity
- In December 2014, the PKI PMO and JITC conducted an integrated DT/OT for TMS release 3.0 to examine code signing, token PIN reset, certificate recovery, and additional token issuance capabilities.
- USD(AT&L), guided by the recommendation of the Director of NSA, directed the PKI Increment 2 PMO to evaluate the viability of whether a one-token and/or one-infrastructure approach could achieve the DOD PKI mission requirements for both the classified and unclassified networks. This resulted in a program delay of six months.
- USD(AT&L) signed an ADM in April 2015, which concluded that a one-token/one-infrastructure approach would cost more money, take longer to develop, and would not improve cybersecurity. The ADM, in conjunction with the Joint Requirements Oversight Council memorandum, directed the NSA to resume development of the PKI Increment 2 Program in accordance with previous plans developed prior to the strategic pause.
- In April and May 2015, JITC conducted a correction of deficiency verification test to resolve problems found in the integrated DT/OT for the TMS release 3.0.
- USD(AT&L) convened an Integrated Product Team to evaluate TMS release 3.0 in June 2015 and issued a fielding ADM in September 2015.
- USD(AT&L) approved the revised PKI Acquisition Program Baseline in July 2015, and approved the updated PKI Acquisition Strategy in September 2015 outlining the PKI PMO's plans to complete Spirals 3 and 4 by 2QFY18. The revised strategy focuses the remaining Increment 2 Spirals (3 and 4) on 15 user-prioritized capabilities. These capabilities are intended to improve the SIPRNET token management and reporting, improve system availability, and provide new infrastructures for the provisioning and management of the NIPRNET Enterprise Alternate Token System and Non-Person Entity certificates.
- The PMO and test community are finalizing the Spiral 3 Test and Evaluation Master Plan (TEMP) Addendum in November 2015 for signature approval in January 2016.
- The PMO is also updating the PKI System Engineering Plan, Life Cycle Sustainment Plan, and Transition Plan.
- The PMO had no major operational test events scheduled in FY15, but does have test events scheduled for 2QFY16 for TMS 4.1, 4.2, and 4.3 capabilities.

Assessment
- Delaying the capability deliveries until FY16, which were due to the six-month one-token/one-infrastructure strategic pause, negatively affected developmental and operational test planning and execution. TMS release 3.0 is a minor FY15 release that will not change the overall not effective/not suitable evaluations.
- FOT&Es I and II, conducted in January 2013, revealed effectiveness and suitability problems. Although no operational testing has been completed since then, the program manager is addressing the requirements definition and system engineering problems that led to these deficiencies, while also making program personnel and contract management process changes to improve the program's ability to achieve restructured goals.
- The PKI PMO's and JITC's integrated DT/OT, combined with the subsequent correction of deficiencies verification of TMS release 3.0 capabilities in April and May 2015, confirmed that Spiral 3 is adequate for DOD-wide fielding. USD(AT&L) issued a fielding ADM in September 2015 to authorize the use of the new capabilities including token PIN resets, encryption certificate key recovery, and issuance of new token types (Unique Identification-based and Administrator Identity-only certificates).
- The PKI PMO's methodology for measuring token reliability lacks sufficient rigor and focus. The PMO should focus their long-term reliability growth plan and testing on the end-state token. Furthermore, the current token reliability requirement requires 6,000 hours over 3 years, which equates to 35 hours a week. Many DOD users require a higher reliability. The DOD Chief Information Officer directed the PKI PMO to define a

higher reliability requirement for the tokens in August 2014 that remains unresolved.
- DOT&E conducted a Spiral 3 TEMP Addendum early review in September 2015, and the document is on track for approval in January 2016.

Recommendations
- Status of Previous Recommendations. The PKI PMO satisfactorily addressed the three previous FY14 recommendations.
- FY15 Recommendations. The PKI PMO should:
  1. Develop the Spiral 4 TEMP Addendum in accordance with the redefined PKI Increment 2 Acquisition Strategy to prepare stakeholders for the remaining deliveries, resource commitments, and T&E goals.
  2. Create a Spiral 4 transition plan defining roles and responsibilities for stakeholders to support a smooth transition and ensure minimal impact to PKI operations once the program enters sustainment.
  3. Define and validate sustainment requirements for PKI Spiral 4 capabilities.
  4. Provide periodic reports of token reliability, failure rates, and root cause analyses.