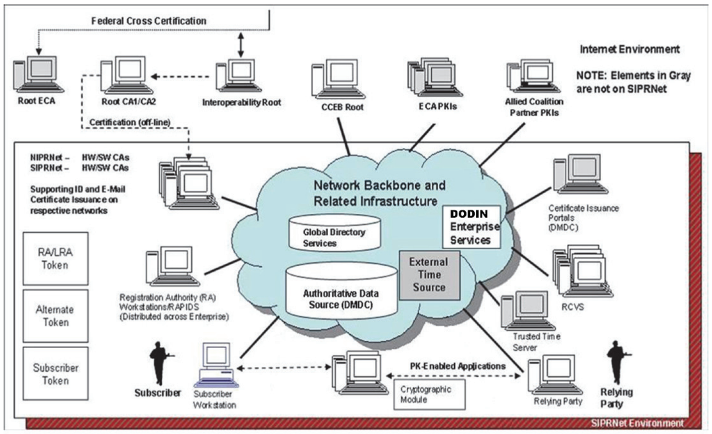
Public Key Infrastructure (PKI)

Executive Summary

- The FOT&Es I and II, conducted in January 2013, revealed effectiveness and suitability problems. Although no independent operational testing has been completed since then, the program manager has been actively addressing the requirements definition and system engineering problems that led to these deficiencies, while making program personnel and contract management process changes to improve the program. An expert token reliability team is currently addressing ongoing token reliability problems in the field.
- In October 2013, the DOD Public Key Infrastructure (PKI) program manager notified the Milestone Decision Authority, then DOD Chief Information Officer but now USD(AT&L), that it would exceed the criteria established for a critical change as defined in Title 10, United States Code (U.S.C.), section 2445c, and would be unable to achieve a Full Deployment Decision (FDD) within five years of the selection of the preferred alternative. The National Security Agency (NSA) Senior Acquisition Executive declared a schedule-related PKI program critical change in October 2013, and subsequently a cost-related change in March 2014.
- In July 2014, USD(AT&L) recertified the PKI program to Congress in accordance with 10, U.S.C., section 2445c(d), and in an Acquisition Decision Memorandum (ADM) further approved the PKI Program Management Office's (PMO's) funding obligation authorities for $10 Million through September 2014 to ensure no disruption of PKI Increment 2 program service while restructuring following the critical change.
- Due to program delays resulting from the critical change, the PKI PMO did not conduct any operational testing in FY14.
- The DOD PKI program manager has drafted an Acquisition Strategy that focuses the remaining Increment 2 Spirals (3 and 4) on 15 user-prioritized capabilities. These capabilities will improve Secret Internet Protocol Router Network (SIPRNET) token management and reporting, improve system availability, and will provide new infrastructures for the provisioning and management of the Non-secure Internet Protocol Router Network (NIPRNET) Enterprise Alternate Token System (NEATS) and certificates to Non-Person Entities (NPEs) (e.g., workstations, web servers, and mobile devices).

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.


Federal Cross Certification
Internet Environment
NOTE: Elements in Gray are not on SIPRNet
Root ECA
Root CA1/CA2
Interoperability Root
CCEB Root
ECA PKIs
Allied Coalition Partner PKIs
Certification (off-line)
NIPRNet – HW/SW CAs
SIPRNet – HW/SW CAs
Supporting ID and E-Mail Certificate Issuance on respective networks
Network Backbone and Related Infrastructure
Global Directory Services
DODIN Enterprise Services
Certificate Issuance Portals (DMDC)
RA/LRA Token
Alternate Token
Subscriber Token
Registration Authority (RA) Workstations/RAPIDS (Distributed across Enterprise)
Authoritative Data Source (DMDC)
External Time Source
RCVS
Trusted Time Server
PK-Enabled Applications
Subscriber
Subscriber Workstation
Cryptographic Module
Relying Party
Relying Party
SIPRNet Environment

CA – Certificate Authority
CCEB – Combined Communications Electronic Board
DMDC – Defense Enrollment Eligibility Reporting System
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

- 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 PKI Increment 2, and the Defense Information Systems Agency is supporting PKI operations, enablement, and security solutions.
- Increment 2 is being developed and deployed 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 the 15 user-prioritized capabilities.

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 NPE certificates 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
- Red Hat – Richmond, Virginia

Activity
- In October 2013, the PKI program manager notified the Milestone Decision Authority that it would exceed the criteria established for a critical change as defined in Title 10, U.S.C., section 2445c, and would be unable to achieve an FDD within five years of the selection of the preferred alternative. The NSA Senior Acquisition Executive declared a schedule-related PKI program critical change in October 2013, and subsequently for cost in March 2014.
- The program was unable to achieve the FDD objective date of March 2013 established in the Major Automated Information System original estimate to Congress. The one-year breach occurred in March 2014, and the five-year breach occurred in April 2014.
- At the Defense Acquisition Executive Summary review in April 2014, the PKI program manager identified problems with PKI requirements, Acquisition Strategy, funding, and schedule supportability.
- In May 2014, the PKI PMO conducted initial vendor developmental tests for planned Token Management System (TMS) Release 3.0 enhancements.
- In July 2014, the USD(AT&L) recertified the PKI program to Congress in accordance with Title 10, U.S.C., section 2445c(d), and in an ADM, which further approved the PKI PMO funding obligation authorities for $10 Million through September 2014 to ensure no disruption of PKI Increment 2 program service while restructuring following the critical change.
- The PKI PMO is currently revising the PKI Acquisition Strategy and plans to complete Spirals 3 and 4 by 3QFY17.
- The PMO is also updating the PKI System Engineering Plan, Spiral 3 Test and Evaluation Master Plan (TEMP) Addendum, Life Cycle Sustainment Plan, and Transition Plan.
- In late September 2014, the USD(AT&L) signed a PKI Increment 2 restructure ADM that restored the PMO's obligation authorities and provided directives for updating important-planning documents, including the Spiral 3 and 4 TEMP Addenda.
- The PKI PMO did not conduct any operational testing in FY14. JITC will examine interoperability and information security during Limited User Tests and subsequent FOT&E events tentatively scheduled for 2015 and later.

Assessment
- The PKI PMO's contractor-led TMS Release 3.0 developmental test and evaluations (DT&Es) demonstrated increased planning and execution rigor. The PMO is planning additional government DT&Es in September and November 2014, but will not conduct TMS operational testing until September 2015.
- The FOT&Es I and II, conducted in January 2013, revealed effectiveness and suitability problems. Although no independent 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 making program personnel and contract management process changes to improve the program's ability to achieve current restructured goals. An expert token reliability team is currently addressing ongoing token reliability problems in the field.
- The NSA Information Assurance Directorate (IAD) continues efforts to improve PKI token reliability. The PKI PMO's token vendor recently developed token version 3.2 that is intended to correct several known faults in the token's operating system. However, the NSA IAD will not certify the 3.2 token's operating system prior to distributing 65,000 new tokens to the Marine Corps and Air Force by the end of September 2014. It is possible more may be distributed before the next token version 3.3 is certified.
- System reliability, availability, and maintainability of the core PKI infrastructure continue to present problems as reported by users in the field. The PMO has implemented changes to improve overall system reliability; however, these changes have not been independently verified through operational testing.
- Currently, the draft PKI Spiral 3 TEMP Addendum is improved but still has missing information, including reliability growth curves needed for planning tests to assess improvements in the reliability of SIPRNET tokens and supporting PKI infrastructure. For example, token inventory management, reporting tools, and processes are still not in place and associated requirements are not clearly defined. With infrastructure in DOD-wide use and tokens in the hands of a majority of SIPRNET users, and with the need for replacement cards for a large fraction of users whose tokens

are expiring, there is clearly a need for a robust inventory logistics management system.

- The DOD PKI program manager has drafted an Acquisition Strategy that focuses the remaining Increment 2 Spirals (3 and 4) on 15 user-prioritized capabilities. These capabilities are intended to improve SIPRNET token management and reporting, improve system availability, and will provide new infrastructures for the provisioning and management of the NEATS and certificates to NPEs (e.g., workstations, web servers, and mobile devices).
- NSA IAD is conducting formal token certification tests for version 3.3 to ensure that no vulnerabilities are exposed.
- The PKI PMO adopted a Spiral 3 and 4 approach in the program's Acquisition Strategy that more logically aligns with the capability development and testing efforts. Spiral 3 will include the TMS 3.0 through 6.0 releases, and Spiral 4 will include separate releases for NPE and NEATS.
- The PKI PMO, Service representatives, and test community are working together to refine the schedule; however, additional effort is needed to establish an event-driven test approach (versus a schedule-driven approach) that supports the draft Acquisition Strategy.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed the four previous recommendations.
- FY14 Recommendations. The PKI PMO should:
  1. Update the TEMP in accordance with the redefined PKI Increment 2 Acquisition Strategy to prepare stakeholders for the remaining deliveries, resource commitments, and test and evaluation goals.
     - Clearly define the strategy to address token reliability and growth in the System Engineering Plan and Spiral 3 and 4 TEMP Addenda to ensure SIPRNET token fielding decisions are informed by thorough testing.
     - Establish a reliability growth program for the PKI system's infrastructure.
     - Operationally test new SIPRNET token releases prior to fielding decisions.
     - Develop a supportable, resourced, event-driven schedule to guide both the capability development and the testing approach.
  2. Create a 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 capabilities.