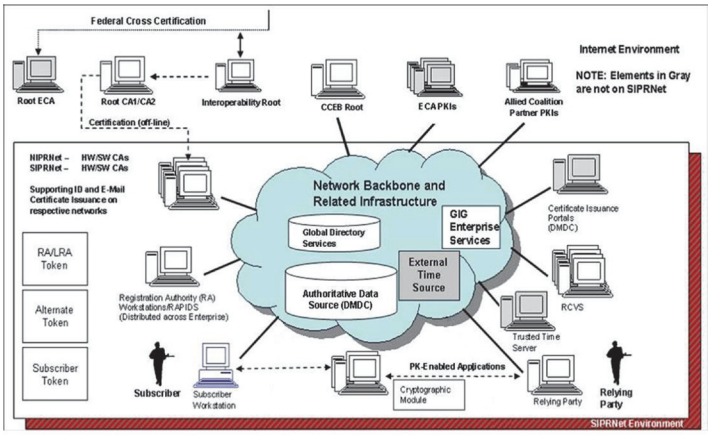
Public Key Infrastructure (PKI)

Executive Summary

- DoD Public Key Infrastructure (PKI) Increment 2 provides a cryptographic capability for DoD members and others to access the Secret Internet Protocol Router Network (SIPRNet) securely and to encrypt and digitally sign e-mail. Increment 1, which provided the Non-secure Internet Protocol Router Network (NIPRNet) PKI infrastructure with controlled access using Common Access Cards (CACs), is complete. The PKI infrastructure provides a personal identification number-protected SIPRNet token for electronically identifying individuals and managing access to resources over globally dispersed SIPRNet nodes. Full implementation will enable authorized users and Non-Person Entity (NPE)-enabled devices (e.g., servers and workstations) to access restricted websites and enroll in online services.
- The Joint Interoperability Test Command (JITC) conducted a combined FOT&E I and II in January 2013 on the SIPRNet environment to address suitability shortcomings discovered during the 2011 IOT&E and to evaluate preliminary Increment 2 Spiral 3 enhancements. The major suitability concerns cited in the IOT&E were not addressed in the FOT&Es and new findings were discovered including increased token failures in the field and inefficiencies in token management. However, the PKI Program Management Office (PMO) has taken steps to address these problems including changes to improve system stability. No completed operational testing to date confirms resolution of the effectiveness and suitability problems.
- An Inventory Logistics System (ILS) for managing SIPRNet token stock at each issuance site was not effective for tracking tokens returned for reuse, was cumbersome to use, and does not provide the necessary functions to replace existing spreadsheet tracking mechanisms. The capability to track reused tokens requires significant redesign and development investments as well as adoption of taxing procedures currently not required for NIPRNet CACs, which are not reusable. Given budget constraints, the Services and agencies opted to rely on workarounds to track returned tokens and requested that remaining Increment 2 resources be reserved for higher priority capabilities, such as group and role-based tokens. The ILS is not part of the original PKI baseline and was developed to support the end-to-end logistics of token distribution and tracking since no common system across the Services and agencies exists on the SIPRNet.
- The DoD Chief Information Officer directive requiring all SIPRNet users to be issued tokens was met for the initial target population. However, select user groups, including some DoD contractors, intelligence personnel, and users supporting tactical operations, have not yet received SIPRNet tokens.
- Increment 2 was originally intended to provide infrastructure upgrades to support DoD's transition to Internet Protocol version 6 (IPv6), migration to stronger PKI algorithms, and to provide the flexibility needed to expand PKI usage in tactical environments. Due to lack of infrastructure readiness across the DoD networks, these areas will not be tested and evaluated as part of Increment 2.
- The National Security Agency (NSA) Senior Acquisition Executive declared a PKI program significant change in September 2013 and a critical change in October 2013.



CA – Certificate Authority
CCEB – Combined Communications Electronic Board
DMDC – Defense Enrollment Eligibility Reporting System
ECA – External Certification Authority
GIG – Global Information Grid
LRA – Local Registration Authority
NIPRNet – Non-classified 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 is a critical enabling technology for Information Assurance. It supports the secure flow of information across the Global Information Grid as well as secure local storage of information.
- 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 is comprised of commercial off-the-shelf hardware and software and other applications developed by the NSA.
  - The Defense Enrollment Eligibility Reporting System (DEERS) and Secret DEERS provide the personnel data for certificates imprinted on NIPRNet CACs and SIPRNet tokens, respectively.
  - DoD PKI Certification Authorities for the NIPRNet and SIPRNet tokens reside in the Defense Information Systems Agency (DISA) Enterprise Service Centers in Oklahoma City, Oklahoma, and Mechanicsburg, Pennsylvania.
- DISA and NSA are jointly developing DoD PKI in multiple increments. Increment 1 is complete and deployed on the NIPRNet. Increment 2 is being developed and deployed

in three spirals on the SIPRNet and NIPRNet to deliver the infrastructure, PKI services and products, and logistical support.

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 regardless of technology, organization, or location.
- Commanders at all levels will use DoD PKI to provide authenticated identity management via personal identification number-protected CACs 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 fully identified network domains, which will facilitate intrusion protection and detection.

Major Contractors
- General Dynamics Information Technology – Needham, Massachusetts (Prime)
- 90Meter – Newport Beach, California
- SafeNet – Belcamp, Maryland

Activity
- DOT&E approved an Operational Assessment plan for the NPE capability in November 2012. However, the NPE technical solution has since evolved to support changes in operating constraints such as the need to support virtual web servers hosting multiple web sites. Furthermore, the PMO delayed the test indefinitely due to the lack of DoD policy defining the types of devices requiring DoD enterprise medium assurance certificates.
- The PKI PMO and JITC, in accordance with a DOT&E- approved test plan, conducted a combined FOT&E I and II of the PKI Increment 2 from January 8 through February 1, 2013, to verify correction of system deficiencies discovered during the IOT&E in 2011 for Spirals 1 and 2, and to evaluate preliminary Spiral 3 enhancements, respectively. The FOT&Es were originally scheduled for 3QFY12 but were postponed due to system development delays. Furthermore, a stop-test in December 2012 resulted from systemic configuration management problems.
- Delays in delivering the ILS capability for token ordering and shipping diverted resources and indirectly contributed to delays in the delivery of several key Spiral 3 capabilities, including the NPE and alternate token capabilities to support system administrator roles on the SIPRNet and NIPRNet.
- In June 2013, JITC conducted a Level II user test to assess improvements to Certificate Authority user management functions.
- In 4QFY13, DISA moved the PKI primary site from Chambersburg to Mechanicsburg, Pennsylvania, to address previous Information Assurance operational test findings.
- The NSA Senior Acquisition Executive declared a PKI program significant change in September 2013 and a critical change in October 2013.

Assessment
- The DOT&E report in May 2013 found PKI's Token Management System (TMS) and the ILS to be not operationally effective and not suitable.
- PKI Increment 2, Spiral 3 is not operationally effective. The Spiral 3 enhancements assessed during the FOT&E I and II degraded existing capabilities and lowered efficiency by increasing Service and agency workload. The initial Spiral 3 deployment of capabilities was intended to provide the following upgrades: (1) blacklisting of tokens, (2) auto-key recovery of private encryption keys escrowed by the core system, and (3) tracing of tokens to the original issuing Service or Local Registration Authority. Specific deficiencies include the following:
  - Blacklisting of tokens successfully identified tokens that should not be allowed reentry into the TMS but had the unintended consequence of lengthening the time to reformat valid user tokens because field operators lost the ability to reformat tokens returned for reuse.
  - The auto-key recovery capability allows end-users to recover private encryption keys through two methods: a self-service web-based capability and a third-party web-based capability requiring Key Recovery Agent approval before granting access to encryption keys. However, a system limitation in the underlying commercial off-the-shelf product prevented users from recovering encryption keys to a token and subsequently using those keys to retrieve encrypted messages.
  - Users were not able to view all potential encryption certificates they have the ability to self-recover or request Key Recovery Agent assistance to recover on their behalf. The failure to deliver needed upgrades while maintaining critical operational functionality underscores immature configuration management problems and a need for processes that incorporate user feedback into capability design, development, test, and deployment.
  - The users expected the ILS to ease the burden of tracking and accounting for tokens but it added more steps without providing significant benefit. A verification of deficiencies test in May 2013, however, confirmed three ILS deficiencies were corrected to improve warehouse managers' ability to leverage the ILS.
  - In summary, the Spiral 3 enhancements assessed during the FOT&E I and II were minor and instead of providing needed capability and enhancement, degraded existing capabilities, and lowered efficiency by increasing Service and agency workload.

- PKI Increment 2 is not operationally suitable. The end-to-end logistics processes continue to rely on manual, Service- and agency-specific methods for procuring, distributing, accounting, and tracking of tokens. Although over 45 bulk token formatters deployed across the DoD have helped increase token issuance rates, token reliability is not accurately tracked or reported and does not reflect user reports of growing failure rates in the field (as much as 15 percent).
  - The ILS was not designed to address logistics shortfalls identified in the IOT&E including token failure tracking and token statistics reporting, such as reporting of token issuance numbers by geographic region and Service affiliation.
  - The ILS has the potential to track shipments but was not effective for tracking tokens returned for reuse. It does not provide necessary functions such as the ability to ship between issuance sites and the ability to terminate bad tokens in a stack.
  - ILS procedures were cumbersome and confusing, and documentation and training were not adequate to improve usability.
- Critical capabilities including the capabilities to generate group and role-based certificates and NPE device certificates (on both SIPRNet and NIPRNet) have been delayed. Sustainment plans for ILS after calendar year 2014 are uncertain further hampering the development of long-term Service and agency logistics processes for token ordering and shipping. Hosting the logistics and token management systems on the same network should improve manpower and usability concerns. However, due to budget constraints, the ILS development schedule has been suspended.
- System reliability, availability, and maintainability of the core PKI infrastructure degraded since the IOT&E with two long unplanned downtimes (4 and 6 hours, respectively) and 12 days of system degradation as reported by users in the field. Configuration management problems persist, causing unannounced system degradations. The PMO has implemented changes to improve overall system reliability; however, these changes have not been independently verified through operational testing.
- Increment 2 also included a requirement to support interoperability with coalition PKI. The SIPRNet PKI infrastructure uses a common root Certificate Authority to ease certificate validation path processing; however, partner nations must stand up their own certificate issuance capabilities in order to make interoperability a reality. These efforts are ongoing, but no operational testing on the SIPRNet has been conducted to date.
- With continual changes to planned Spiral 3 capabilities, configuration management still lacks adequate processes for inserting user-prioritized capabilities and fixes into the field. Since the FOT&E I and II, the PMO has established a Configuration Control Board to address this issue; however, the process is still maturing.
- Based on the results of the June 2013 user test, trusted agents can now perform pin resets in the field, thereby shifting a significant burden off of the registration authorities' workflow. While this assessment was largely positive, the new release again caused unwanted changes to existing capabilities: unanticipated changes in the user interface hampered registration authorities from viewing the full history of transactions performed on each card that underwent a pin reset. More rigorous developmental testing is required to identify problems so user workflow is not negatively affected by capability releases.
- The NPE development efforts have been halted to allow time for a thorough assessment of current mission requirements and changes in technology. Until a requirements review is conducted, no further development or testing is planned for Increment 2.
- A transition plan to support post-2014 operations and maintenance is still undefined between NSA, DISA, and the Services and agencies. Given the inability to address IOT&E and FOT&E I and II suitability shortcomings, the initial PKI Spiral 3 deployment remains not operationally suitable.
- The developmental test program processes and procedures directed in both the Test and Evaluation Master Plan and System Engineering Plan were not implemented, which has resulted in limited visibility into actual performance of the system prior to OT&E.
- Further testing will be necessary of the recently moved PKI primary site in Mechanicsburg, Pennsylvania, to assess improvements in Information Assurance, operational availability, system health and monitoring, and continuity of operations plans.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed three of four recommendations from the FY12 Annual Report for Increment 2, Spirals 1 and 2. The recommendation for the PMO to establish a more realistic schedule for PKI development, delivery, and testing remains.
- FY13 Recommendations. The PKI PMO should:
  1. Address and independently verify fixes to operational effectiveness and operational suitability shortcomings in follow-on operational test activities. In particular, improve configuration management practices to ensure patches and releases do not impact critical mission functions and improve token failure tracking to more accurately reflect user experience.
  2. Update the Test and Evaluation Master Plan in accordance with the redefined PKI Increment 2 acquisition strategy to prepare stakeholders for the remaining deliveries, resource commitments, and test and evaluation goals.
  3. Create a transition plan defining roles and responsibilities for stakeholders once the program enters sustainment to support a smooth transition and ensure minimal impact to PKI operations.
  4. Conduct a follow-on operational test of the new Mechanicsburg, Pennsylvania, PKI hosting site to assess improvements in Information Assurance, operational availability, system health and monitoring, and continuity of operations plans.