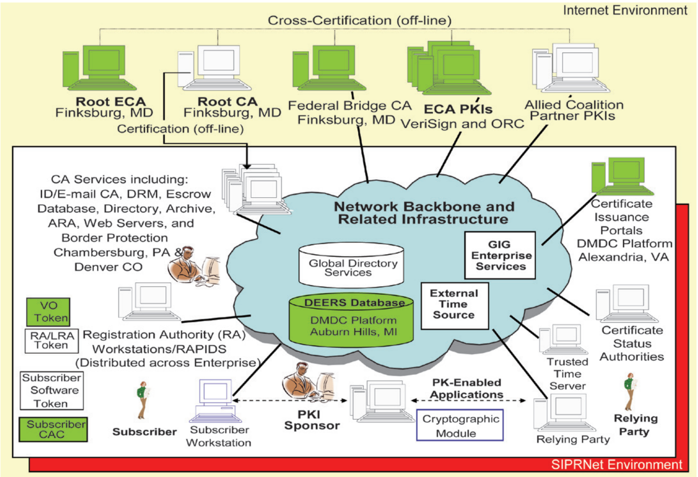
Public Key Infrastructure (PKI)

Executive Summary

- DoD Public Key Infrastructure (PKI) Increment 2 provides authenticated identity management via password-protected Secret Internet Protocol Routing Network (SIPRNET) tokens to enable DoD members and others to access the SIPRNET securely and encrypt and digitally sign e-mail. 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.
- An IOT&E in 2011 exposed significant logistics deficiencies due to undefined processes for procuring, distributing, and tracking SIPRNET tokens. The Defense Manpower Data Center, which currently handles the common access card (CAC) logistical processes on the Non-secure Internet Protocol Router Network (NIPRNET), is actively working with the DoD PKI Program Management Office (PMO) to take on similar responsibilities for the SIPRNET tokens.
- In October 2011, the DoD Chief Information Officer (CIO) directed the military Services and agencies to implement PKI on the SIPRNET and deploy tokens DoD-wide to approximately 500,000 users by December 31, 2012. As of mid-October 2012, military Services and agencies had issued approximately 78,300 tokens to users, falling far short of the pace needed to achieve the 500,000 goal by end of year. This status reflects growing backlogs in registering, enrolling, and getting SIPRNET tokens out to users, suggesting only nominal improvements toward overall SIPRNET security.
- In January 2012, the DoD CIO approved full fielding of PKI to the SIPRNET and tactical environments and the acquisition of the necessary tokens, card readers, and software to support fielding. The DoD CIO called for an operational retest of end-to-end logistical processes to address outstanding suitability deficiencies.
- In September 2012, the Joint Interoperability Test Command (JITC) conducted an operational test of a bulk token formatting and issuance capability intended to improve the speed of token issuance. JITC found the formatter to be effective and suitable, fulfilling its intended purpose by providing the Registration Authorities the ability to simultaneously complete multiple tasks. Fifteen SIPRNET token bulk formatters are currently being used by the Services and an additional 35 units are being procured.
- Capabilities to correct logistic shortfalls with token inventory and accounting are delayed and awaiting operational testing. A previously scheduled FOT&E slipped from 3QFY12 until 2QFY13 to verify correction of logistics deficiencies found during the IOT&E. JITC intends to conduct an operational test to verify whether the new Inventory Logistics System (ILS) can successfully track tokens by serial number and location throughout their lifecycle from ordering, through shipping, issuing, and return. Future enhanced reporting capabilities to improve token accounting and reporting will not be available for operational testing until 1QFY14.



NOTE: Elements in Green are not on SIPRNet

ARA - Auto-key Recovery Agent
CA - Certification Authority
CAC - Commom Access Card
DEERS - Defense Enrollment Eligibility Reporting System
DMDC - Defense Manpower Data Center
DRM - Data Recovery Manager
ECA - Enterprise Certification Authority
GIG - Global Information Grid
ID - Identification
LRA - Local Registration Authority
ORC - Operational Research Consultants, Inc.
PK - Public Key
RA - Registration Authority
RAPIDS - Real-Time Automated Personnel Identification System
SIPRNet - SECRET Internet Protocol Router Network
VO - Verifying Official

System

- DoD PKI is a critical enabling technology for Information Assurance (IA). 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.
- DoD PKI is comprised of commercial off-the-shelf hardware and software, and other applications developed by the National Security Agency (NSA).
  - The Defense Enrollment Eligibility Reporting System (DEERS) and the 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 Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma.
  - 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 for Spiral 1 (tokens), Spiral 2 (tactical and austere environments), and Spiral 3 (NPE PKI, Federal and coalition capabilities).

- The NPE development effort provides certificates for devices, automated and manual enrollment, and the infrastructure means for credential checking to insure NPE-enabled devices (e.g., domain controllers, web servers, and workstations) are authorized to exist on DoD networks.

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.

Major Contractors

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

Activity

- In September 2011, the PKI PMO signed a Memorandum of Agreement with the Defense Manpower Data Center to develop an ILS to handle SIPRNET token ordering, shipping, and distribution.
- In October 2011, the DoD CIO directed the military Services and Agencies to implement PKI on the SIPRNET and deploy tokens DoD-wide to all users by December 31, 2012.
- The JITC and PMO executed an automated failover in December 2011. The failover between the PKI systems in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma, demonstrated continuity of operations after the planned failover.
- DOT&E issued the PKI Increment 1, Spirals 1 and 2 IOT&E report on December 6, 2011.
- In January 2012, the DoD CIO approved full fielding of PKI to the SIPRNET and tactical environments and the acquisition of the necessary tokens, card readers, and software to support fielding. The DoD CIO called for an operational retest of end-to-end logistical processes to address outstanding suitability deficiencies.
- The PKI PMO continues to work on the underlying suitability problems, focusing on the ILS and Token Management System to address scalability. However, no significant PKI capabilities were delivered and operationally tested in FY12. Suitability retesting is ready but on hold due to errors in reconciling token inventory status for tokens already issued.
- Test planning and preparations are ongoing for conducting an operational test of Increment 2, Spiral 3 backend capabilities in December 2012.
- With approval from the DoD CIO, the PKI PMO further delayed the NPE capability delivery and operational assessment until 3QFY13 due to security and user concerns that the proposed capability will not satisfy current mission requirements. Security mitigations are being developed and plans for testing the proposed NPE capability are being put in place.

Assessment

- The PKI Increment 2, Spirals 1 and 2 IOT&E were conducted in 4QFY11 in accordance with a DOT&E-approved test plan.
- The DOT&E report in December 2011 found the system to be operationally effective and secure, but not operationally suitable with logistical improvements needed to support full deployment. The system was available, reliable, maintainable, and relatively easy to use. However, critical logistical support deficiencies were found in the processes for distributing and accounting for hardware tokens, token readers, and middleware. Specific logistics deficiencies found include the following:
  - The lack of a robust token reliability tracking program for ensuring failure rates are acceptable.
  - A centralized token inventory system for ensuring tokens are procured and distributed according to Service and agency demands and for tracking tokens that are reissued to different users.
  - The need for more customized searching and reporting through the Token Management System portal interface to enable Services and Agencies to better report on token issuance status.
  - The lack of bulk formatting and issuance capabilities to improve token distribution time and reduce manpower costs.
- While logistics improvements have been made since the IOT&E report, to include delivery of a bulk formatting and issuance capability, a final tested robust logistics process for token procuring, distributing, tracking, and reporting is not in place. Delays in the delivery of the centralized logistics inventory system coupled with the Services' need to meet the DoD CIO's SIPRNET token deployment directive are hampering the transition from previous operations.
- There are over 530,000 SIPRNET tokens distributed to the Services and Agencies but only 78,300 tokens in use as of mid-October 2012. This status reflects the significant backlog in registering, enrolling, and deploying SIPRNET tokens. The

Service and agency registration authorities responsible for issuing tokens currently do not have the manpower needed to support the FY13 NPE operational test activities. Additionally, stakeholders do not have enough confidence in the NPE capability because it has not been adequately demonstrated via developmental testing. Ongoing missions and operations are precluding the Services and agencies from being able to commit critical devices to operational assessments and testing.

- Overall, the PKI system and technical capabilities are sound, but the SIPRNET standard operating procedures, training, logistical support, and lifecycle sustainment lack maturity. While procedures for middleware and card reader distribution and support have improved, the new process supporting the token ILS has not yet been demonstrated. Additional duties are being defined within the PKI program for Service and agency token warehouse and issuance site managers to ensure that tokens are properly tracked by the new system. With more than 100 issuance sites, there is a significant risk that the ILS process will not be uniformly adopted in a timely manner, which is necessary to provide a complete and accurate inventory status and to enable production of tokens based on issuance site requirements.
- The NPE capability delays continue to plague the Program Office. The NPE delivery is now amassed into the Increment 2, Spiral 3 set of capabilities, which also include enhancements to the existing SIPRNET and NIPRNET infrastructures. While the NPE Release 3 provides some automation improvements, it adds a substantial manpower support requirement for the Services to accomplish the large volume of DoD NPE devices, especially given the loose DoD guidance stating that all devices require medium assurance certificates. The registration authorities and system administrators ultimately responsible for approving and enrolling devices into the system have major concerns with the system and the workload it will entail. Although the PKI PMO has attempted to refine guidance to enable NPE certificate deployment to be prioritized based on risk that a device can be compromised by information attacks, the community has not established a clear path forward for deploying NPE certificates across DoD devices.
- The developmental test program is inadequate to support integrated test planning efforts. Processes and procedures directed in both the Test and Evaluation Master Plan and System Engineering Plan have not been implemented, which has resulted in limited visibility into actual performance of the system. Better coordination between the test teams, and improved test planning and reporting are required to support operational test readiness assessments.
- Overly aggressive testing event dates continue to waste critical user and test resources by forcing the assessment of PKI capabilities that are not ready to be assessed.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed five of seven recommendations from the FY11 Annual Report for Increment 2, Spirals 1 and 2. The recommendations concerning correction of token testing and scheduling deficiencies remain.
- FY12 Recommendations.
  1. The PKI program needs to improve coordination with the stakeholders, provide better capability definition, and recognize schedule impossibilities early to provide sound acquisition management for testing and delivering the PKI capabilities for the DoD.
  2. The PKI program needs to adhere to both the System Engineering Plan and Test and Evaluation Master Plan, which provide specific direction on how the development and testing of the PKI capabilities should be executed.
  3. The PKI acquisition community needs clear guidance on the intended NPE devices. Any directives for issuing NPE certificates must take into consideration Service and agency manpower and resource constraints. If such guidance is not timely, the PKI acquisition program baseline should be restructured such that tests are driven based on capability maturity, readiness, and mission need and not to satisfy program schedule requirements.
  4. The PMO should work to establish a more realistic timeline for PKI development, delivery, and capability testing that better supports milestone decisions. The program must better manage expectations of those with PKI equities by avoiding recurring schedule slips caused by capability delivery delays.