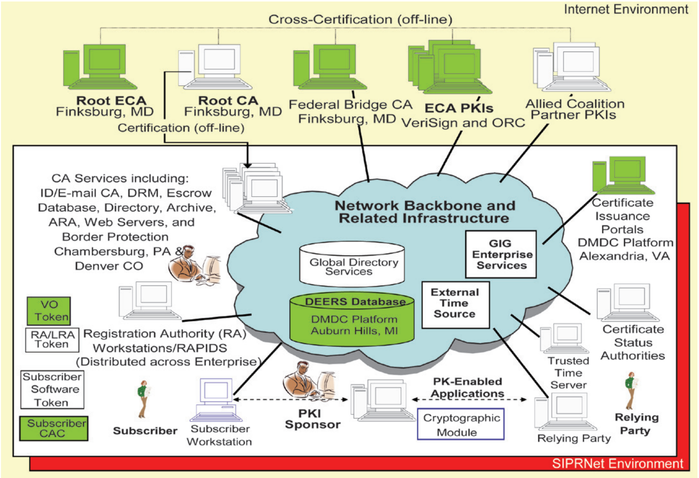
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- In September 2010, the National Security Agency (NSA) Senior Acquisition Executive approved the procurement of 25,001 Secret Internet Protocol Router Network (SIPRNET) tokens to support IOT&E. The NSA requested that an Accelerated Life Test (ALT) (independent laboratory testing) be conducted on the SIPRNET token to ensure the token reliability deficiencies, uncovered during the FY10 Operational Assessment of the DoD Public Key Infrastructure (PKI) Increment 2, Spiral 1were resolved.
- On January 26, 2011, following the successful completion of the ALT, the NSA Senior Acquisition Executive authorized deployment of the previously procured 25,001 tokens and the procurement and deployment of an additional 60,000 tokens to ensure an adequate number of tokens would be on-hand for IOT&E.
- The IOT&E was divided into two phases: Phase 1 issued tokens to establish a minimum required user base (16,500), while Phase 2 demonstrated scalability and sustainability as the user base continued to grow.
- During the IOT&E, the PKI Program Management Office (PMO) issued 17,194 tokens over a seven month span with only 58 token failures reported, meeting the reliability requirement that 91 percent of tokens will last for at least three years.
- The interim logistics process was evaluated and accepted for the distribution of 85,000 tokens.
- The IOT&E exposed significant logistics hurdles due to undefined processes for procuring, distributing, and tracking tokens. The Defense Manpower Data Center (DMDC), which currently handles the common access card (CAC) processes on the Non-secure Internet Protocol Router Network (NIPRNET), will take on similar responsibilities for the SIPRNET token in 3QFY12 to mitigate these deficiencies. However, detailed plans including assignment of roles and responsibilities and the establishment of token distribution sites are undefined.
- Currently, the PKI PMO and military Services' and Agencies' end-to-end token distribution and accountability processes are not fully defined and require testing. Given the IOT&E assessment of the current process, the lack of a clearly defined process is likely to lead to significant backlogs in getting SIPRNET PKI tokens out to the force, reducing overall network security and impeding the Services' ability to meet the OSD requirement of having tokens deployed for all SIPRNET account holders by the end of CY12.

System

- DoD PKI is a critical enabling technology for Information Assurance (IA). It supports the secure flow of information across the Global Information Grid (GIG) (both NIPRNET and SIPRNET), as well as secure local storage of information.


Internet Environment
Cross-Certification (off-line)
Root ECA Finksburg, MD
Root CA Finksburg, MD
Certification (off-line)
Federal Bridge CA Finksburg, MD
ECA PKIs VeriSign and ORC
Allied Coalition Partner PKIs
CA Services including: ID/E-mail CA, DRM, Escrow Database, Directory, Archive, ARA, Web Servers, and Border Protection Chambersburg, PA & Denver CO
Network Backbone and Related Infrastructure
Global Directory Services
GIG Enterprise Services
Certificate Issuance Portals DMDC Platform Alexandria, VA
DEERS Database DMDC Platform Auburn Hills, MI
External Time Source
VO Token
RA/LRA Token
Registration Authority (RA) Workstations/RAPIDS (Distributed across Enterprise)
Certificate Status Authorities
Trusted Time Server
Subscriber Software Token
Subscriber CAC
Subscriber
Subscriber Workstation
PKI Sponsor
PK-Enabled Applications
Cryptographic Module
Relying Party
Relying Party
SIPRNet Environment

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

- DoD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of Public Key certificates and their corresponding private keys. DoD PKI works with commercial off-the-shelf and government off-the-shelf applications to provide IA and e-business capabilities.
- PKI is a service of products that provide and manage X.509 certificates for public key cryptography. Using authoritative data, DoD PKI creates a credential that combines identity information with cryptographic information. The certificate identifies the individual PKI user and binds that person to a particular public/private key pair. In this way, DoD PKI provides a representation of physical identity in an electronic form.
- DoD PKI Certification Authorities for the NIPRNET and SIPRNET tokens reside in the Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs) in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma. Network Security Service PKI is now operational on the SIPRNET, and the Joint Interoperability Test Command (JITC) performed a system failover of the capability in early September 2011.
  - DoD PKI is comprised of commercial off-the-shelf hardware and software, and other applications developed by NSA.
  - Certificates are imprinted on the DoD CAC for NIPRNET personnel identification using data taken from the Defense Enrollment Eligibility Reporting System (DEERS). The

Secret DEERS provides the personnel data for certificates imprinted on a separate SIPRNET token.

- 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 (Federal and coalition capabilities). DoD PKI Increment 2 provides authenticated identity management via a personal identification number-protected token to enable DoD members and others to securely access the SIPRNET. Full implementation will enable authorized users to access restricted websites, enroll in online services, and encrypt and digitally sign email.

Mission

- Military operators, communities of interest, and other authorized users will use DoD PKI to enable net-centric operations, specifically, 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 email. Commanders will use specific PKI services to:
  - Enable and promote a common ubiquitous secure web services environment.
  - Enable the integrity of data/forms/orders moving within the GIG (both NIPRNET and SIPRNET), via use of digital signatures.
  - Enable management of identities operating in groups or certain roles within GIG systems.
  - Ensure the integrity and confidentiality of what is operating on a network by providing assured PKI-based credentials for any device on that network.

Major Contractors

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

Activity

- In September 2010, the NSA Senior Acquisition Executive decided to limit token production to 25,001 tokens due to token reliability problems discovered during the FY10 Operational Assessment of the PKI Increment 2, Spiral 1.
- To resolve the unacceptable token reliability, the NSA conducted and verified the accelerated three-year life testing (independent of the PKI PMO) in a controlled setting, including assessing the effects of temperature, humidity, salt, fog, and personal electrostatic discharge.
- In September 2010, the NSA Senior Acquisition Executive approved the procurement of 25,001 SIPRNET tokens to support IOT&E. The NSA requested that an ALT (independent laboratory testing) be conducted on the SIPRNET token to ensure the token reliability deficiencies uncovered during the FY10 Operational Assessment of the DoD PKI Increment 2, Spiral 1 were resolved.
- On January 26, 2011, following the successful completion of the ALT, the NSA Senior Acquisition Executive authorized deployment of the previously procured 25,001 tokens and the procurement and deployment of an additional 60,000 tokens to ensure an adequate number of tokens would be on-hand for rapid distribution for IOT&E.
- Due to delays in identifying users, configuring networks, and issuing tokens, the IOT&E was divided into two phases: Phase 1 issued tokens to establish a minimum required user base (16,500), while Phase 2 demonstrated scalability and sustainability as the user base continued to grow.
- JITC conducted Phase 1 IOT&E for DoD PKI Increment 2, Spirals 1 and 2 from March 1 to August 8, 2011, in accordance with the DOT&E-approved test plan. Typical users from a variety of operational environments participated in the test event.
  - Testing evaluated infrastructure processes supporting the distribution and management of 16,500 SIPRNET tokens. Testing also assessed sustainability of the tokens in the operational environment.
  - JITC and the DISA Field Security Office conducted Penetration Testing on the DECCs in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma, from June 6 to July 31, 2011.
- JITC conducted Phase 2 of the IOT&E from August 8 to September 21, 2011.
  - The JITC testing examined token reliability to validate the data from the NSA accelerated life testing, while the overall PKI system capacity was tested under heavier usage conditions to determine if it could handle the processing load.
  - The middleware patching and software upgrading processes were supposed to be thoroughly examined to ensure the PKI system could be maintained; however, the processes were not ready for testing during the IOT&E.
  - Additionally, the PKI PMO and JITC conducted a failover of the PKI system between Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma, to demonstrate its initial continuity of operations capabilities.

Assessment

- The independent ALT conducted and verified by NSA indicated the tokens meet reliability requirements for the required three-year service life. One exception was a risk of damage from moderate exposure to personal electrostatic discharge. Testing did not address reliability in tactical environments. SIPRNET tokens, unlike the CAC, can be reused by being reissued to new users. Testing did not address impacts to reliability caused by token reuse.
- Token reliability has improved significantly since the FY10 Operational Assessment. During the IOT&E, the PKI PMO issued 17,194 tokens over a seven month span with only 58 token failures reported, meeting the reliability requirement that 91 percent of tokens will last for at least three years.
- The IOT&E was adequate to make an assessment and was conducted in accordance with the DOT&E-approved test plan.
- The interim logistics process was evaluated and accepted for the distribution of 85,000 tokens.
- The IOT&E exposed significant logistics hurdles due to undefined processes for procuring, distributing, and tracking tokens. The DMDC, which currently handles the CAC processes on the NIPRNET, will take on similar responsibilities for the SIPRNET in 3QFY12 to mitigate these deficiencies. However, detailed plans including assignment of roles and responsibilities and the establishment of token distribution sites are yet undefined.
- Currently, the military Services' and Agencies' token distribution processes are not well-defined and may lead to reduced overall network security and the Services being unable to meet the OSD requirement of having tokens deployed for all SIPRNET account holders by the end of CY12. The affect of IA deficiencies is that SIPRNET users will be required to use multiple passwords for authentication to gain system access instead of the streamlined PKI access to the network and public/private key-enabled capabilities.
- Penetration testing examined PKI to assess Prevent, Detect, React, and Restore system capabilities and procedures and indicated that NIPRNET PKI is secure with some minor limitations, including physical vulnerabilities and detection shortfalls. SIPRNET PKI penetration testing results are classified.
- Middleware patching and software upgrading processes were insufficiently documented to be adequately tested at IOT&E, which affects PKI system security and supportability.
- Overall, the PKI system and technical capabilities are sound, but the SIPRNET standard operating procedures, training, logistical support, lifecycle sustainment, and continuity of operations planning lack maturity and documentation. Once these supporting infrastructures and documentation are defined and established, user and system administrator-level training can be adequately accomplished for the system to properly and securely operate.
- The SIPRNET PKI system load balancing and failover capabilities, processes, and documentation need refinement. These capabilities are critical for proper operation within the GIG and will affect the overall system performance and restoral abilities in the event of problems at the DECCs in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma.
- Operational testing did not identify any significant problems that were missed by developmental testing nor were there preexisting developmental testing problems that will preclude PKI Increment 2 from moving forward.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed one of two recommendations from the FY10 annual report for Increment 2, Spirals 1 and 2. The recommendation concerning correction of physical security vulnerability at Letterkenny Army Depot remains.
- FY11 Recommendations.
  1. Additional testing, post IOT&E should assess system scalability as the user population continues to grow. The PMO should complete a life cycle sustainment plan and define the role of the DMDC in future sustainment. Prior to procurement of additional tokens, DOT&E recommends additional tests to assess the effectiveness and suitability of the DMDC supportability and sustainment processes. The PMO should update and build upon the life cycle sustainment plan and develop a logistical support concept of operations to clarify Agencies' and Services' roles and responsibilities.
  2. The DoD Chief Information Officer, U.S. Cyber Command, PMO, and the Services should work closely together to develop the necessary policies, processes, and procedures to increase the ability to accountably distribute tokens to end users.
  3. The PMO should provide a written continuity of operations plan and ensure the alternate SIPRNET site is operational and that load balancing and automated system failover capabilities are in place and tested as part of future T&E events.
  4. The PMO should provide refined PKI standard operating procedures, training, and system documentation for users, helpdesk personnel, and system administrators.
  5. The PMO should fully develop and document PKI middleware patching and upgrading processes to ensure the system is able to be maintained and secured.
  6. Testing is needed to assess sustainability of tokens in all operating environments, including tactical environments. Further testing is needed to establish bounds for token reuse and to assess impacts to reliability from reissuing tokens to users.
  7. Overly aggressive testing event dates waste critical test resources for assessing PKI capabilities that are not ready to be assessed. The PMO should work to establish a more realistic timeline for future PKI development, capability testing, and milestone decisions, while managing expectations of those with PKI equities.