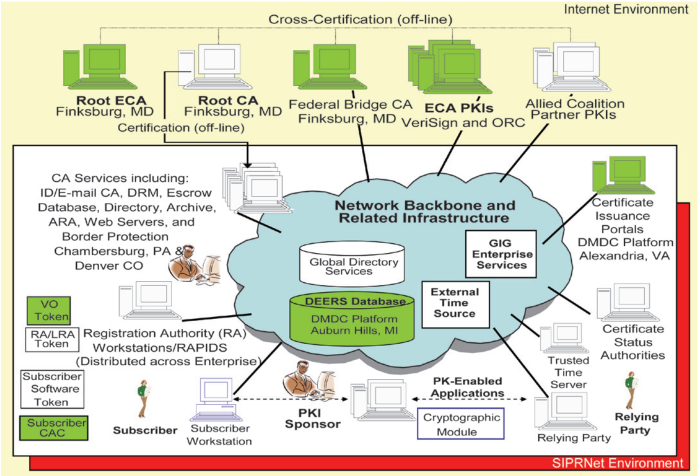
Public Key Infrastructure (PKI) Increments 1 and 2

Executive Summary

- DoD Public Key Infrastructure (PKI) Increments 1 and 2 provide authenticated identity management via a password-protected Common Access Card (CAC) and Secure Internet Protocol Routing Network (SIPRNet) token to enable DoD members, coalition partners, and others to access restricted websites, enroll in online services, and encrypt and digitally sign e-mail.
- JITC conducted separate FOT&Es for DoD PKI Increment 1, Spirals 3 and 4 in April 2010 and August 2010, respectively. The capabilities provided in the spirals were operationally effective, suitable, and survivable for deployment. However, Spiral 3 capabilities provided inaccurate reporting of certificate revocations that must be corrected.
- The Operational Assessment for Increment 2, Spiral 1 showed Registration Authorities (RAs) were able to efficiently issue SIPRNet tokens, and end users were able to use those tokens to facilitate missions through digital signing, encryption, and web-server authentication. However, reliability of the tokens was unacceptable when approximately ten percent of those distributed during the Operational Assessment were defective.



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 (GIG) (Non-Secure Internet Protocol Routing Network (NIPRNet) and SIPRNet), 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 works with commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) applications to provide IA and e-business capabilities.
- Using authoritative data, DoD PKI creates a credential that combines identity information with cryptographic information that is non-forgeable and non-changeable. In this way, DoD PKI provides a representation of physical identity in an electronic form.
- DoD PKI Certification Authorities (CAs) for the NIPRNet and SIPRNet software certifications reside in the Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECC) in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma. PKI CAs for issuance of the SIPRNet hardware tokens reside in the DECC in Chambersburg, Pennsylvania.
    - DoD PKI is comprised of COTS hardware, COTS software, and other applications software developed by the National Security Agency (NSA).
    - Certificates are imprinted on the DoD CAC token 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 broken into five spirals, four of which have been operationally tested and deployed on NIPRNet. Increment 2 is being developed and deployed in three spirals on the SIPRNet.

Mission

- DoD PKI enables net-centric operations by allowing military operators, communities of interest, and other authorized users 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 password-protected CAC or SIPRNet token to enable DoD members, coalition partners, and others to access restricted websites, enroll in online services, and encrypt and digitally sign e-mail. 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 Contractor

BAE Systems Incorporated – Arlington, Virginia

Activity

Increment 1 Spirals 3 and 4 (FOT&E)

- JITC conducted separate FOT&Es for DoD PKI Increment 1, Spirals 3 and 4 in April 2010 and August 2010, respectively. Integrated developmental and operational testing was accomplished according to DOT&E-approved test plans and procedures in the JITC PKI laboratory at Fort Huachuca, Arizona.
  - Spiral 3 testing evaluated software applications encompassing three new or improved capabilities: Local Registration Agent version 4 (LRA v4), Web Based Bulk Revocation (WBBR) server, and the Certificate History Repository Information Service (CHR-IS).
  - Spiral 4 testing evaluated system upgrades to the Robust Certificate Validation Service (RCVS), which includes migration to a new operating system and architecture enhancements.

Increment 2, Spiral 1 (Operational Assessment)

- For Increment 2, Spiral 1, JITC conducted an Operational Assessment in June and July 2010 in accordance with the DOT&E-approved test plan and procedures. Typical users from a variety of operational environments participated in the test event.
- The PKI Program Management Office (PMO) experimented with varying network conditions in February and September 2010 to better define problems with PKI use in tactical and austere environments.

Assessment

Increment 1, Spirals 3 and 4 (FOT&E)

- The testing conducted by JITC was adequate to assess the operational effectiveness and suitability of the DoD PKI Increment 1, Spirals 3 and 4 enhancements. The capabilities provided in the spirals were operationally effective, suitable, and survivable for deployment.
- Eleven deficiency reports (DRs) were opened during Spiral 3 testing, with no critical items identified. The two highest priority DRs involved certificate revocations. Inaccurate reporting of certificate revocations resulted in the RA concluding all certificates were revoked when that was not the case. These DRs must be resolved prior to deployment, or written guidelines must be given to users warning them of this potential reporting error.
- There are no outstanding issues with the Spiral 4 capabilities.

Increment 2, Spiral 1 (Operational Assessment)

- The testing conducted by JITC was adequate to assess the capabilities and limitations of DoD PKI Increment 2, Spiral 1.
- RAs were able to efficiently issue SIPRNet tokens and end users were able to use those tokens to facilitate missions through digital signing, encryption, and web-server authentication.
- Nearly ten percent of all tokens were found to be defective. Some tokens failed prior to or during the issuance process. A sizable fraction failed after issuance, having an adverse impact on the users. Problems with the software that formats tokens, inaccurate system documentation, and lack of a back-up system which prevents RAs from performing their duties when the system is down for maintenance also adversely affected operational suitability.
- Token problems must be resolved prior to starting the IOT&E.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed one of two recommendations from the FY08 annual report for Increment 1, Spirals 1 and 2. The recommendation concerning correction of a physical security vulnerability at Letterkenny Army Depot remains.
- FY10 Recommendations.

Increment 1, Spirals 3 and 4

1. The PKI PMO should provide data regarding the expected system load for Increment 1 at full deployment so an adequate capacity assessment can be done by DOT&E to support the full deployment decision following Increment 1, Spiral 5 testing in FY11.

Increment 2, Spiral 1

2. The PKI PMO should correct unresolved Increment 2, Spiral 1 SIPRNet token deficiencies identified during the Operational Assessment and confirm through testing that the fixes are operationally viable before purchasing more tokens in support of the Increment 2, Spiral 1 IOT&E.
3. The PMO should provide a written Continuity of Operations Plan for Increment 2 and ensure the alternate SIPRNet sight is operational; conduct IA testing during the IOT&E in accordance with DOT&E guidance to assess protect, detect, react, and restore capabilities; and develop a Life-Cycle Sustainment Plan.