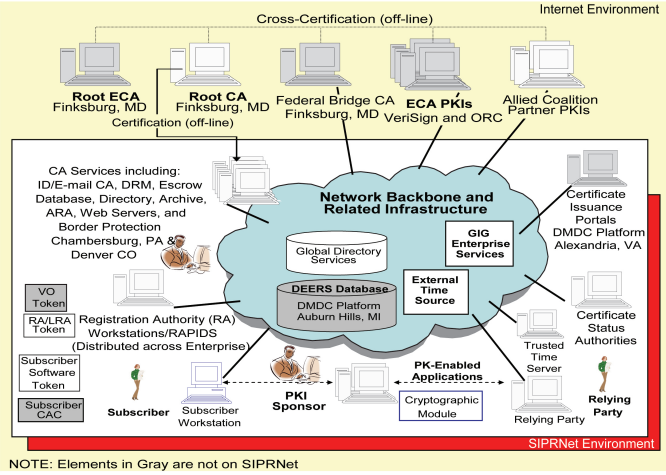
Public Key Infrastructure (PKI)

Executive Summary

- DoD Public Key Infrastructure (PKI) Increment 1 provides authenticated identity management via password-protected Common Access Card (CAC) to enable DoD members, coalition partners, and others to access restricted web sites, enroll in online services, and encrypt and digitally sign e-mail.
- The Joint Interoperability Test Command (JITC) conducted the DoD PKI Increment 1, Spiral 2 IOT&E in February and March 2008. DOT&E assessed the PKI system as operationally effective and operationally suitable for use in its intended operational environment.
- The DoD PKI Program Office should correct unresolved deficiencies identified during the IOT&E prior to the Full Deployment Decision at the end of Increment 1.

System

- DoD PKI is a critical-enabling technology for Information Assurance (IA) services to support seamless secure information flows across the Global Information Grid (GIG) or when stored locally.
- DoD PKI is the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of Public Key certificates and their corresponding private keys, and enables commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) applications to provide IA and e-business capabilities.
- Using authoritative data, obtained via face-to-face identity proofing, DoD PKI creates a credential that combines this identity information with cryptographic information that is non-forgeable and non-changeable. In this way, DoD PKI provides a standards-based representation of a physical identity in an electronic form.
- DoD PKI Certification Authorities (CA) reside in the Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECC) in Chambersburg, Pennsylvania, and Oklahoma City, Oklahoma.
  - DoD PKI is comprised of COTS hardware, COTS software, and the National Security Agency (NSA)-developed applications software.
  - Certificates are imprinted on the DoD CAC token for personnel identification using Defense Enrollment Eligibility Reporting System (DEERS) personnel data.
- DoD PKI is being developed jointly by DISA and the NSA using spiral acquisition in multiple increments. The current increment, Increment 1, is being deployed in five spirals, of which two have been operationally tested and deployed.



NOTE: Elements in Gray 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

Mission

- DoD PKI enables net-centric operations by allowing warfighters, 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 to enable DoD members, coalition partners, and others to access restricted web sites, 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, 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 provision of assured PKI-based credentials for any device on that network

Prime Contractor

- Government Integrator (DISA)

Activity

- JITC conducted the DoD PKI Increment 1, Spiral 2 IOT&E in February and March 2008. Testing was accomplished according to DOT&E-approved test plans and procedures. All or parts of 13 of the 14 Increment 1 enhancements were evaluated in the operational PKI environment, with typical users providing system support.
- Prior to the IOT&E, JITC observed developmental testing in the DISA PKI Laboratory at Fort Huachuca, Arizona. JITC observations were captured in a series of Letters of Observation submitted to DOT&E.
  - Early observation of this testing allowed JITC to identify issues that could impact operations.
  - The Program Office was able to correct areas of concern prior to the IOT&E, or schedule for their correction prior to deployment.

Assessment

- The testing conducted by JITC was adequate to assess the operational effectiveness and suitability of the DoD PKI Increment 1, Spiral 2 configuration. DOT&E concurred with the JITC assessment that the DoD PKI Increment 1, Spiral 2 capabilities provide an operationally effective and operationally suitable system.
- DoD PKI system IA controls were met, with the exception of physical access controls at the Chambersburg DECC at the Letterkenny Army Depot in Pennsylvania.
- Other deficiencies observed during the IOT&E include:
  - A single point of failure in the PKI system architecture
  - Training materials and system documentation did not reflect the current system under test
  - A system resource conflict occurred when generating the daily revocation list
- JITC's early observations of developmental testing were invaluable in reducing risk to the PKI operational mission when the baseline was deployed for IOT&E.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY08 Recommendations.
  1. DISA should coordinate with the Letterkenny Army Depot to eliminate the physical security vulnerability created by the lack of access control to the area surrounding the DECC.
  2. The PKI Program Management Office should resolve the single point of failure in the system, correct the resource allocation issue during creation of the revocation list, and provide system documentation and training materials that accurately describe the actual system configurations.