Public Key Infrastructure (PKI) Increment 2

The DOD Public Key Infrastructure (PKI) Increment 2 is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DOD users and network devices. PKI's Token Management System (TMS) is not operationally suitable due to significant problems with SIPRNET token ordering processes and accountability, with over 143,000 unaccounted for tokens worth over $1.4 million. The NIPRNET Enterprise Alternate Token System (NEATS) is not secure against moderate cyber threats.

System Description

PKI Increment 2 provides the hardware, software, and services to generate, publish, revoke, and validate NIPRNET and SIPRNET public and private key certificates. Specifically, PKI Increment 2 delivers the NEATS, Non-person Entity (NPE), and TMS capabilities. Commanders at all levels use DOD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards or SIPRNET or NEATS tokens to enable DOD members, coalition partners, and other authorized users to access restricted websites, enroll in online services, and encrypt/decrypt and digitally sign email. Military operators, communities of interest, and other authorized users use DOD PKI to securely access, process, store, transport, and use information, applications, and networks. Military network operators use NPE certificates for workstations, web servers, and devices to create secure network domains, which facilitate intrusion protection and detection.

Program

The National Security Agency (NSA) has developed and is deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA delivered the SIPRNET TMS in Spirals 1, 2, and 3 prior to late August 2018. Spiral 4 is intended to deliver NEATS and NPE NIPRNET and SIPRNET capabilities. DOT&E approved the PKI Spiral 4 Test and Evaluation Master Plan Addendum in October 2017. The NSA developed the NEATS with the Defense Manpower Data Center (DMDC), and NPE with operational support from the Defense Information Systems Agency (DISA), which provide PKI support for the DOD. NPE and NEATS use commercial and government off-the-shelf hardware and software hosted at DISA and DMDC operational sites. DOT&E approved the PKI Increment 2 FOT&E plan in October 2020 and Cybersecurity Annex in November 2020. DOT&E published the PKI Increment 2 Report in September 2021 in support of a full deployment decision projected in mid-2023.

Major Contractors

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE).
- Global Connections to Employment – Lorton, Virginia (Prime for NEATS).
- SafeNet Assured Technologies – Abingdon, Maryland.
- Giesecke and Devrient America – Twinsburg, Ohio.

Test Adequacy

The Joint Interoperability Test Command (JITC) conducted the PKI Increment 2 FOT&E from late November 2020 through March 2021, in accordance with a DOT&E-approved test plan. Testing was adequate to verify system fixes, assess operational effectiveness and suitability of PKI capabilities for long-term sustainment and transition, and inform a full deployment decision for PKI Increment 2.

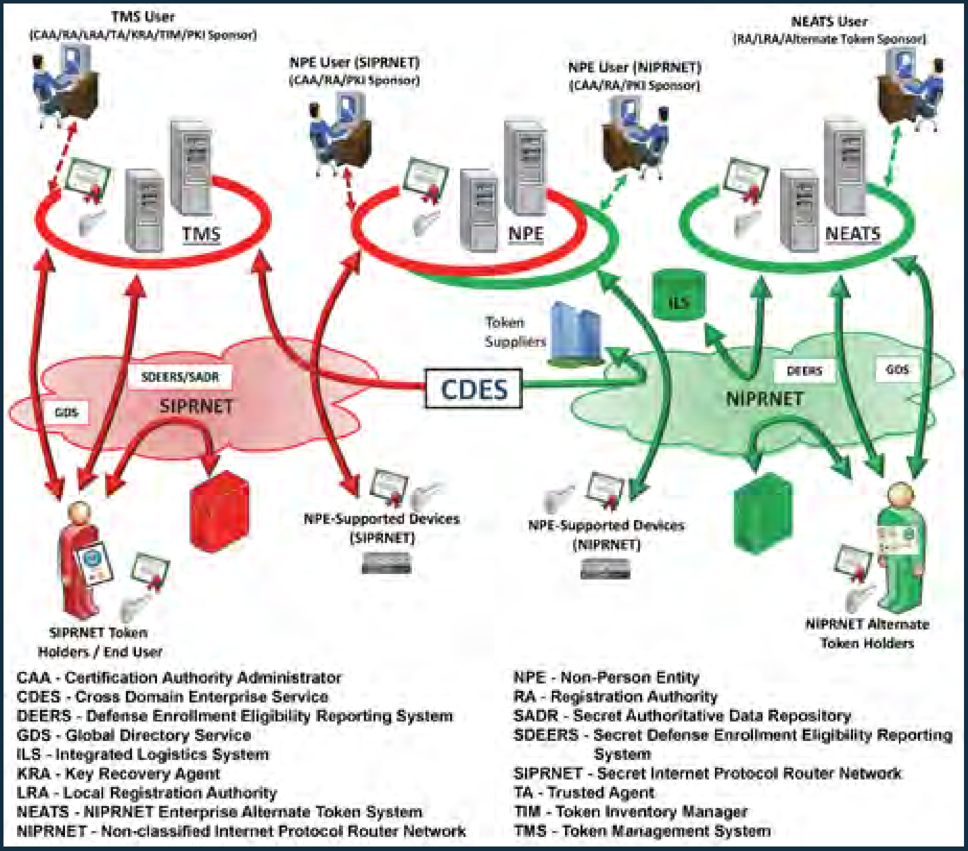
The PKI Program Management Office (PMO) interfered with test data collection and investigative processes, which is antithetical to the DOD's independent operational testing approach. While such actions did not ultimately affect DOT&E's and JITC's ability to assess the system, PMO test interference is a problem that DOT&E addressed in a separate memorandum to NSA leadership to prevent such actions from happening in the future.

Performance

Effectiveness

NEATS, NPE, and TMS are operationally effective, with a caveat that all three systems experienced problems accessing the Certificate Revocation List using the Robust Certificate Validation System within the required timelines, which potentially allows users to access restricted systems using revoked certificates. Additionally, the NPE auto-rekey functionality on devices using the Enrollment over Secure Transport

PKI Increment 2 delivers the NEATS, NPE, and TMS capabilities.



CAA - Certification Authority Administrator
CDES - Cross Domain Enterprise Service
DEERS - Defense Enrollment Eligibility Reporting System
GDS - Global Directory Service
ILS - Integrated Logistics System
KRA - Key Recovery Agent
LRA - Local Registration Authority
NEATS - NIPRNET Enterprise Alternate Token System
NIPRNET - Non-classified Internet Protocol Router Network
NPE - Non-Person Entity
RA - Registration Authority
SADR - Secret Authoritative Data Repository
SDEERS - Secret Defense Enrollment Eligibility Reporting System
SIPRNET - Secret Internet Protocol Router Network
TA - Trusted Agent
TIM - Token Inventory Manager
TMS - Token Management System

(EST) protocol performed inconsistently and remains not operationally effective as an enterprise capability.

Suitability

NEATS and NPE are operationally suitable, with a caveat that the DMDC NEATS help desk responsiveness is not satisfactory and the application experienced unexplained brief outages on the client that affected token processing. TMS is not operationally suitable because the Central Management of Tokens system and processes resulted in a lack of token accountability, with over 143,000 unaccounted for tokens worth over $1.4 million. JITC also uncovered critical token ordering and logistics problems with TMS. The PKI DISA Integration Lab (DIL) designed to test new token variants and device certificates does not support user needs. The PKI lifecycle sustainment plan and transition plan remained not finalized or ready for assessment five months after the test. TMS capabilities are not ready for long-term sustainment and transition.

Survivability

NEATS is not secure against moderate capability nearsider and advanced capability outsider threats. JITC conducted NPE and TMS cyber survivability testing in July 2021; however, the systems' cyber survivability status remains undetermined, pending completion of operational cybersecurity test analyses and classified reporting in late 2021.

Recommendations

1. The PKI PMO, DMDC, and DISA should establish a reproducible and accurate token ordering and accountability process for TMS, correct software compatibility and long-term sustainment problems, and improve training and help desk support.
2. The PKI PMO and DMDC should remediate the identified NEATS vulnerabilities found during cyber assessments over the past two years to secure this system and supporting environment.
3. The NSA and JITC should conduct comprehensive, independent, operational capability testing with advanced threat-representative cybersecurity cooperative and adversarial assessments of NEATS to improve cyber survivability prior to full deployment in mid-2023.
4. The PKI PMO should fix EST protocol-related auto-rekey problems before fielding and coordinate with other device manufacturers to assist with NPE EST protocol configuration to improve usefulness and reliability.
5. The PKI PMO and DISA should ensure the PKI DIL supports Service and Agency TMS and NPE functional testing and remote access.