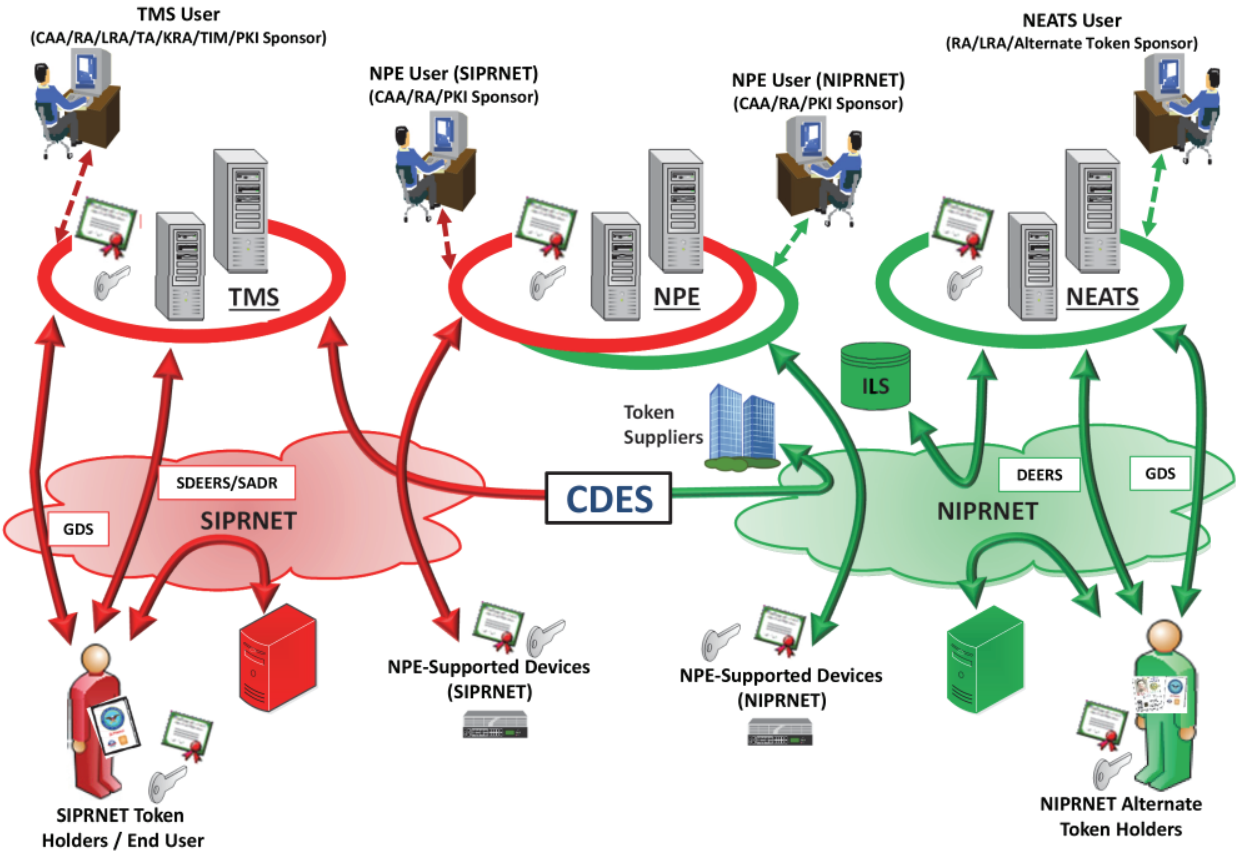
Public Key Infrastructure (PKI) Increment 2

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 based on DOT&E's PKI Increment 2 FOT&E Report published in November 2021. The NIPRNET Enterprise Alternate Token System (NEATS) and the Non-Person Entity (NPE) system are not survivable against moderate cyber threats.

SYSTEM DESCRIPTION

PKI Increment 2 enables the DOD to ensure only authorized individuals and devices have access to networks and data, thereby supporting the secure flow of information across DOD Information Networks and providing secure local storage of information. PKI Increment 2 provides the hardware, software, and services to generate, publish, revoke, and validate NIPRNET and SIPRNET PKI certificates.



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

MISSION

DOD users at all levels use DOD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, 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 Service and DOD Agency operators, communities of interest, and other authorized users use DOD PKI to securely access, process, store, transport, and use information, applications, and networks. 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 May 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. TMS, 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 FOT&E Report in November 2021 and a classified NPE finding memo in February 2022.

» MAJOR CONTRACTORS

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE)
- Peraton – Herndon, 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 and assess operational effectiveness and suitability of PKI capabilities for long-term sustainment and transition. JITC conducted FOT&E follow-up re-testing and verifications of fixes in late FY22, which were observed by DOT&E. JITC intends to continue cyber survivability testing and verifications of the DOD PKI Increment 2 NEATS and NPE in FY23 in support of a yet-to-be-determined date for a full deployment decision.

PERFORMANCE

» EFFECTIVENESS

NEATS, NPE, and TMS are operationally effective, with minor problems that the PKI Program Management Office (PMO) is working to remedy. JITC conducted verification of fixes for some PKI capabilities in late FY22 and will continue verifications as needed in FY23. The NPE auto-rekey functionality on devices using the Enrollment over Secure Transport (EST) protocol remained not operationally effective and has not been widely adopted as an enterprise capability. JITC has no plans to re-test the EST protocol at this time.

» SUITABILITY

NEATS and NPE are operationally suitable, though the DMDC NEATS help desk responsiveness is not satisfactory. TMS is not operationally suitable because the Central Management of Tokens system and processes resulted in a lack of token accountability. In June 2022, the PKI PMO introduced a PKI DISA Integration Lab (DIL) designed to test new token variants and device certificates with remote access to better support user needs. JITC reassessed TMS operational suitability, observed token ordering processes, and monitored NEATS help desk metrics from late FY22 into early FY23. The PKI PMO updated the lifecycle sustainment plan and transition plan in FY22. TMS capabilities were not ready for long-term sustainment and transition in FY22.

» SURVIVABILITY

TMS is survivable, while NPE and NEATS are not survivable against moderate capability nearsider and advanced capability outsider threats. In July 2021, JITC conducted TMS and NPE cyber survivability testing and then conducted focused NPE cyber survivability testing in October 2021 that identified problems. The PKI PMO partially mitigated the NPE problems in FY22, and JITC re-tested NPE in late FY22 into FY23. The PKI PMO and DMDC are working to mitigate NEATS and other architectural problems found in earlier cyber survivability testing, after which JITC will test NEATS in FY23. The PKI PMO and DMDC token supply chain risk management processes lack transparency and need improved monitoring of token manufacturer processes.

RECOMMENDATIONS

1. The PKI PMO and DMDC should establish a reproducible and accurate token ordering and accountability process for PKI tokens.
2. The PKI PMO, NSA Acquisition Security Office, and DMDC should improve their token supply chain risk management processes to inform Service and DOD Agency token purchasing and operational use decisions.

3. The PKI PMO and DISA should remediate and test the identified NPE vulnerabilities found during cyber survivability assessments in 2021 and 2022 to secure this system.
4. The PKI PMO and DMDC should remediate and test the identified NEATS vulnerabilities found during cyber survivability assessments over the past four years to secure this system and supporting environment.
5. The PKI PMO and JITC should conduct operational cyber survivability assessments of NPE and NEATS prior to full deployment.
6. The PKI PMO, DMDC, and DISA should correct long-term sustainment problems prior to full deployment.
7. The PKI PMO and DMDC should improve NEATS help desk support.
8. The NSA should determine the path forward for the EST capability.