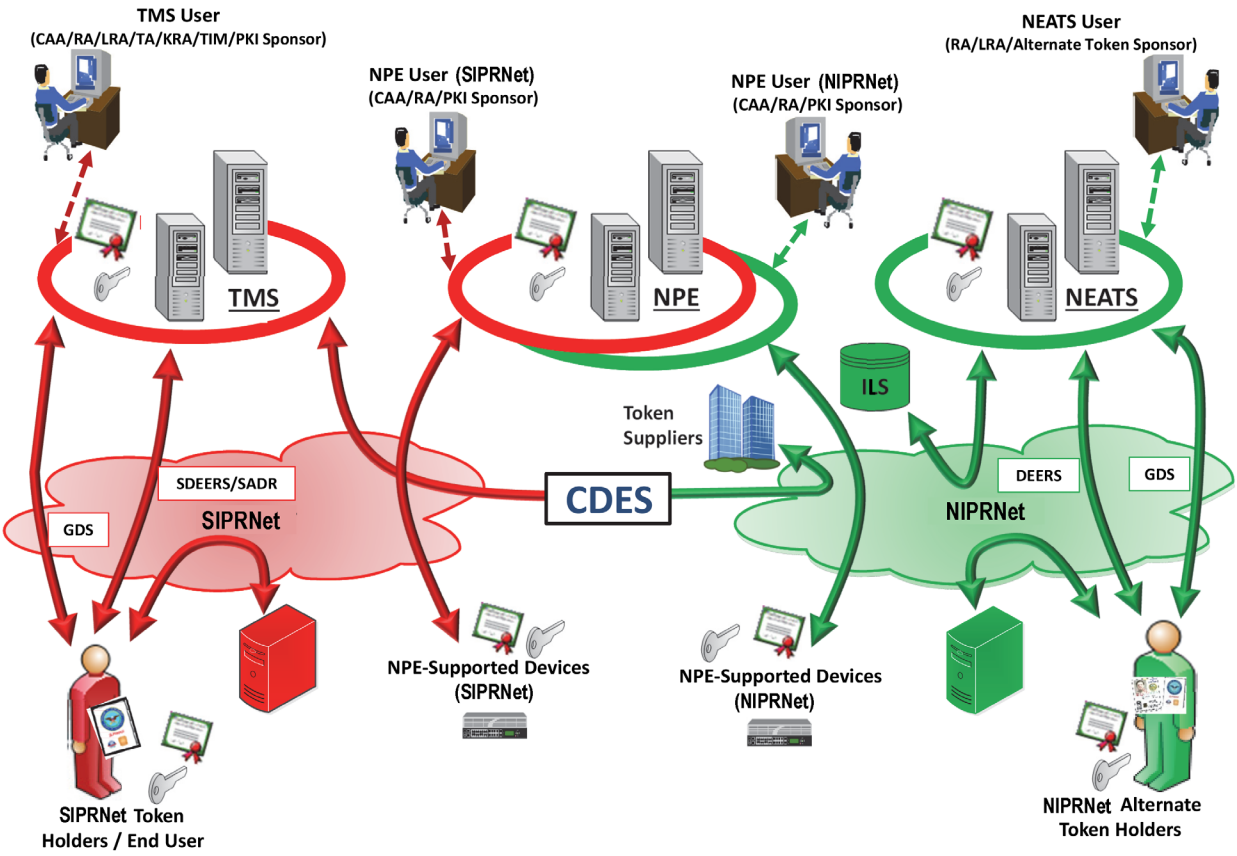
Public Key Infrastructure (PKI) Increment 2

The DoD Public Key Infrastructure (PKI) Increment 2 (consisting of Token Management System (TMS), NIPRNet Enterprise Alternate Token System (NEATS), and the Non-Person Entity (NPE)) is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DoD users and network devices. The PKI TMS is not operationally suitable due to problems with SIPRNet token ordering processes and accountability. The PKI Program Management Office (PMO) upgraded the TMS baseline and changed processes to enhance token order tracking for the Services and Agencies. The Joint Interoperability Test Command (JITC) reassessed TMS operational suitability and token ordering processes in FY23 and expects to complete the effort in FY24. TMS is survivable, while NEATS and NPE are not survivable against moderate cyber threats. Given the criticality of PKI to DoD's cyber posture, the National Security Agency (NSA), Defense Information Systems Agency (DISA) and Defense Manpower Data Center (DMDC) should remediate the cyber vulnerabilities to PKI as soon as possible and conduct operational testing to ensure PKI is survivable.



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

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.

MISSION

DoD users at all levels use DoD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, SIPRNet tokens, 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 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 DMDC, and NPE with operational support from the DISA. 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, a classified NPE finding memo in February 2022, and a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023.

» MAJOR CONTRACTORS

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE)
- Peraton, Inc. – Herndon, Virginia (Prime for NEATS)
- SafeNet Assured Technologies, a subsidiary of Thales Group – Abingdon, Maryland
- Giesecke and Devrient America – Twinsburg, Ohio

TEST ADEQUACY

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 Increment 2 capabilities for long-term sustainment and transition. JITC completed FOT&E re-testing and verifications of fixes for operational suitability issues in FY22 and FY23, which were observed by DOT&E. JITC conducted NPE and TMS cyber testing in FY21 and re-tested NPE cyber in late FY21 and FY22. The PKI PMO implemented partial NPE cyber mitigations in FY22 and intends to implement additional mitigations in FY24. JITC intends to continue cyber survivability testing and verifications of NEATS in FY24 in support of a DoD PKI Increment 2 full deployment decision in September 2024.

PERFORMANCE

» EFFECTIVENESS

NEATS, NPE, and TMS are operationally effective, with minor problems that the PKI PMO is working to remedy. JITC completed verification of fixes for some PKI capabilities in FY23. The NPE auto-rekey functionality on devices using the Enrollment over Secure Transport (EST) protocol remains not operationally effective and as a result, has not been widely adopted as an enterprise capability. The PKI PMO has no technical means to fix the EST protocol implementation for devices, and JITC has no plans to re-test the EST protocol.

» SUITABILITY

NEATS and NPE are operationally suitable. TMS is not operationally suitable because the Central Management of Tokens (CMT) system and processes resulted in a lack of token accountability. The PKI PMO updated the TMS baseline with improvements in CMT order tracking to support Service and Agency needs in FY23. JITC conducted follow-on TMS assessments in FY22 and FY23 to evaluate system changes and token ordering process improvements. JITC is reassessing TMS operational suitability and token ordering processes, with expected completion in FY24. TMS capabilities are still not ready for long-term sustainment and transition at the conclusion of FY23, a recurring issue.

» SURVIVABILITY

TMS is survivable, while NPE and NEATS are not survivable against moderate capability nearsider and advanced capability outsider threats. The PKI PMO partially mitigated the NPE problems in FY22; however, the PKI PMO has no plans to mitigate all the remaining problems in FY24 or conduct further NPE operational cyber testing and evaluation. DOT&E published a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023 that addressed NPE findings. The PKI PMO and DMDC are working to mitigate NEATS findings and other architectural problems found in previous cyber survivability testing, after which JITC will test NEATS in FY24. The PKI PMO, NSA Acquisition Security Office, and DMDC token supply chain risk management processes lack transparency and need improved monitoring of token manufacturer processes.

RECOMMENDATIONS

The PKI PMO and other organizations have yet to resolve the following recommendations from the FY22 Annual Report:

1. The PKI PMO and DISA should remediate the identified NPE vulnerabilities found during cyber survivability assessments and operationally test the system.
2. The PKI PMO and DMDC should remediate the identified NEATS vulnerabilities found during cyber survivability assessments to secure this system and the supporting environment, and then operationally test the system.
3. The PKI PMO and JITC should conduct operational cyber survivability assessments of NPE and NEATS prior to full deployment.
4. The PKI PMO and DMDC should establish a reproducible and accurate token ordering and accountability process for PKI tokens.
5. 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.
6. The PKI PMO, DMDC, and DISA should correct long-term sustainment problems prior to full deployment.