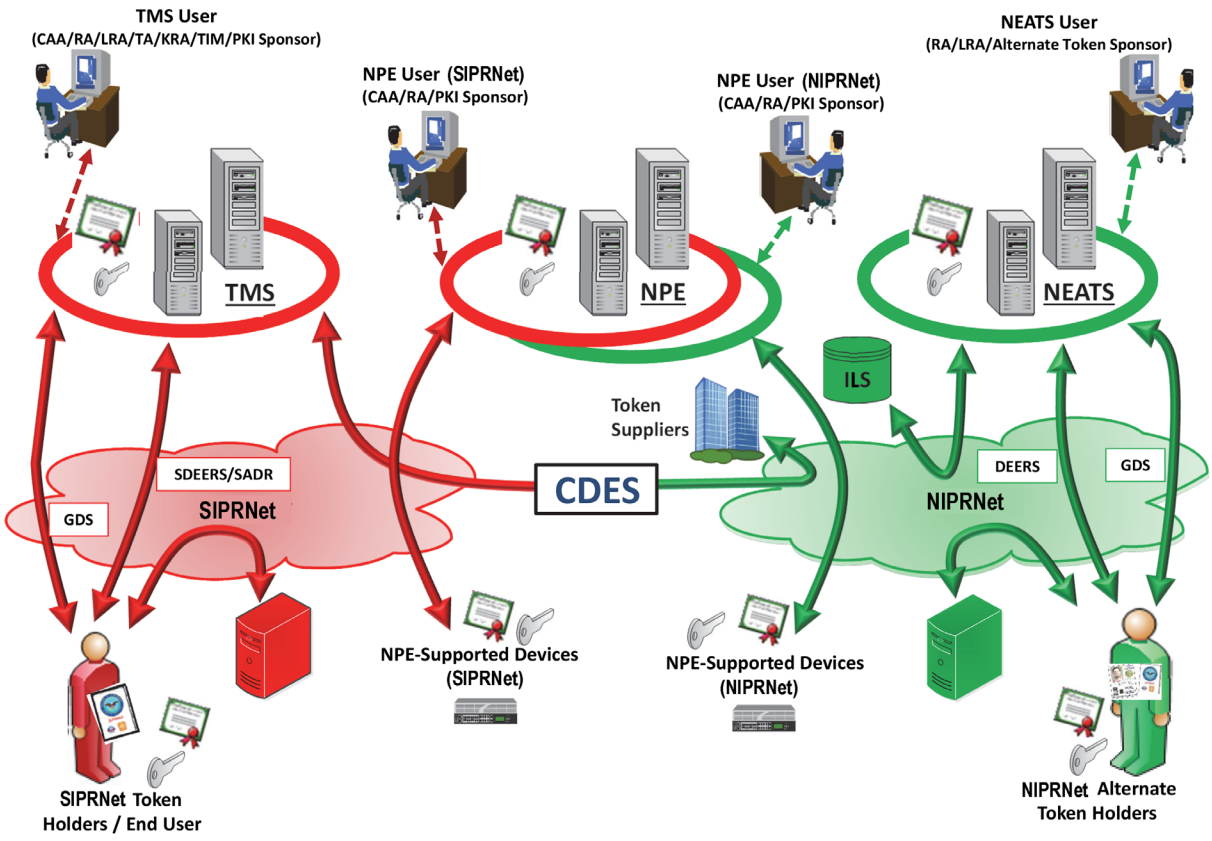
Public Key Infrastructure (PKI) Increment 2

The DoD Public Key Infrastructure (PKI) Increment 2 (consisting of Token Management System (TMS), NIPRNet Enterprise Alternate Token System (NEATS), and Non-Person Entity (NPE)) is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DoD users and network devices. In FY24, the Joint Interoperability Test Command (JITC) completed the TMS operational suitability and token ordering process reassessment and the NEATS cyber assessment. DOT&E intends to publish a TMS suitability and NEATS cyber survivability assessment in 1QFY25. 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 continue to address cyber vulnerabilities and conduct periodic independent cyber 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, and 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 on classified and unclassified workstations, web servers, and devices to create secure network domains, which facilitate intrusion protection and detection.

PROGRAM

The NSA has developed and deployed PKI Increment 2 in four spirals on SIPRNet and NIPRNet. DOT&E approved the PKI Spiral

4 TEMP Addendum in October 2017, the PKI Increment 2 FOT&E plan in October 2020, and the Cybersecurity Annex in November 2020. The NSA delivered the SIPRNet TMS in Spirals 1, 2, and 3 prior to late May 2018. Spiral 4 delivered NEATS and NPE NIPRNet and SIPRNet capabilities in late September 2024. The NSA developed 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 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. DOT&E intends to publish a classified PKI Increment 2 Suitability and Cyber Survivability Annex Update in 1QFY25 to support the full deployment decision (FDD).

» 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
- IDEMIA – Reston, Virginia
- 90Meter – Newport Beach, California

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 FY24, 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 Program Management Office (PMO) implemented partial NPE cyber mitigations in FY22, which were observed by JITC and DOT&E. JITC completed cyber survivability testing of NEATS in July 2024, in accordance with a DOT&E-approved test plan annex update from October 2023 to support the DoD PKI Increment 2 FDD. DOT&E intends to publish a classified PKI Increment 2 Suitability and Cyber Survivability Annex Update that captures FY24 testing in 1QFY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E assessed PKI Increment 2 NEATS, NPE, and TMS are operationally effective in the DOT&E PKI Increment 2 FOT&E Report published in November 2021. JITC completed verification of fixes for PKI capabilities in FY23 with no additional effectiveness testing required in FY24.

» SUITABILITY

DOT&E assessed PKI Increment 2 NEATS and NPE as operationally suitable in the DOT&E PKI Increment 2 FOT&E Report published in November 2021, and DOT&E intends to publish an updated assessment of TMS operational suitability in 1QFY25. The PKI PMO updated the TMS baseline with improvements in Enterprise Central Management of Tokens (CMT) order tracking to provide for better token accountability in FY23. JITC completed the follow-on assessment in FY24 that showed significant improvement with Enterprise CMT, Service, and Defense Agency token tracking, accountability, and reconciliation processes.

» SURVIVABILITY

DOT&E assessed TMS as survivable and NPE as not survivable against moderate capability cyber threats in the DOT&E PKI Increment 2 FOT&E Report published in November 2021 and the classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023. DOT&E intends to publish a NEATS cyber survivability assessment in 1QFY25. The PKI PMO mitigated all but one of the NPE problems but did not mitigate the remaining problem or conduct further NPE operational cyber testing prior to FDD. The PKI PMO and DMDC mitigated many NEATS findings and other architectural problems found in previous

cyber survivability testing. As NSA, DISA, and DMDC migrate PKI capabilities to cloud hosting environments, operational cyber testing will be needed to maintain and improve survivability. The PKI PMO, NSA Acquisition Security Office, and DMDC token supply chain risk management processes need to improve monitoring of token manufacturer processes.

RECOMMENDATIONS

The PKI PMO should:

1. Address remaining cyber vulnerabilities and conduct periodic operational cyber survivability assessments of PKI capabilities after FDD.
2. Improve token supply chain risk management processes to inform Service and Defense Agency token purchasing and operational use decisions.