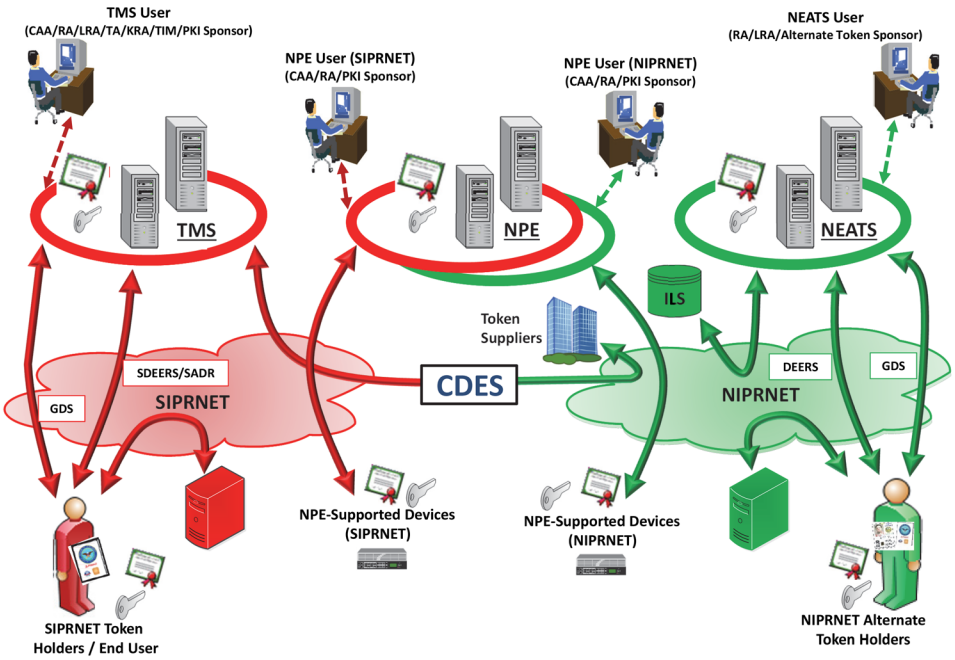
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- The Public Key Infrastructure (PKI) Program Management Office (PMO) and Defense Information Systems Agency (DISA) migrated PKI's Token Management System (TMS) from DISA physical hosting to a virtualized environment in February through March 2020.
- DOT&E published the PKI Increment 2, Spiral 4 Limited User Test (LUT) Report in April 2020.
- The PKI PMO and Joint Interoperability Test Command (JITC) had planned to conduct an Increment 2 FOT&E in FY20; however, the coronavirus (COVID-19) pandemic affected test planning and site participation, delaying the test event.
- DOT&E approved the PKI Increment 2 FOT&E plan in October 2020.



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

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. By controlling the distribution of encryption, identity, signing, and device certificates and keys, DOD PKI helps ensure only authorized individuals and devices have access to networks and data, which supports the secure flow of information across the DOD Information Network as well as secure local storage of information.
- The National Security Agency (NSA) deployed PKI Increment 1 on the NIPRNET with access control provided through Common Access Cards (CACs) issued to authorized personnel.
- 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. Spiral 4 is intended to deliver the NIPRNET Enterprise Alternate Token System (NEATS) and Non-Person Entity (NPE) NIPRNET and SIPRNET capabilities.
  - NEATS is intended to provide confidentiality, integrity, authentication, and non-repudiation services by providing a centralized system for the management of NIPRNET certificates on NEATS tokens for privileged users, which includes System Administrators, groups, roles, code signing, and individuals not eligible to receive CACs. NEATS provides token registration, issuance, personnel identification number reset, revocation, and key recovery. The private keys are stored on the token, which is a smartcard embedded with a microchip.
  - The NPE system issues certificates to large numbers of NPE devices (e.g., hardware and virtual devices and software applications) using both manual and automated methods. These certificates help ensure only authorized devices are allowed to access DOD networks. NPE provides authorized System Administrators and Registered Sponsors with the capability to obtain device certificates singularly or in bulk without the need for PKI registration authority approval.
  - The NSA developed the NEATS with the Defense Manpower Data Center (DMDC) and NPE with operational support from DISA, which provide PKI support for the DOD. DMDC also manages the Defense Enrollment Eligibility Reporting System for the NIPRNET and SECRET Defense Enrollment Eligibility Reporting System for the SIPRNET, the authoritative sources for personnel data.
  - NPE and NEATS use commercial and government off-the-shelf hardware and software hosted at DISA and DMDC operational sites.

Mission

- Commanders at all levels use DOD PKI to provide authenticated identity management via personal identification number-protected CACs 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.

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

Activity

- In accordance with a DOT&E-approved test plan, JITC conducted a LUT of PKI Increment 2 capabilities, including the Spiral 4 NPE and NEATS functionalities in September through November 2019. The LUT examined the NEATS on NIPRNET, the NPE enterprise certificate issuance and management system deployed in both the NIPRNET and SIPRNET environments, and TMS sustainment on SIPRNET.
- The PKI PMO updated the lifecycle sustainment plan and the transition plan with the Services and hosting organizations in FY20.
- The NSA established a token evaluation process and chartered a token evaluation working group to address token compatibility problems found in operational use and testing in FY20.
- The PKI PMO and DISA migrated PKI's TMS from DISA physical hosting to a virtualized environment in February through March 2020.
- DOT&E published the PKI Increment 2, Spiral 4 LUT Report in April 2020.
- The PKI PMO and JITC intended to conduct an Increment 2 FOT&E in FY20; however, COVID-19 affected test planning and site participation, which delayed the test event into FY21.
- DOT&E approved the PKI Increment 2 FOT&E plan in October 2020.
- The PKI PMO delayed the planned Increment 2 Full Deployment Decision from December 2020 to 4QFY21 due to COVID-19.

Assessment

- The DOT&E assessments from the PKI Increment 2, Spiral 4 LUT are as follows:
  - NEATS is:
    - Operationally effective for garrison forces, but not effective for naval afloat and forward operating tactical forces because of compatibility problems with deployed operating systems.
    - Progressing toward being operationally suitable, but is not long-term sustainable because of the lack of backwards compatibility and an architectural design that depends on other systems that do not failover.
    - Not survivable against moderate capability nearsider and advanced capability outsider cyber threats.
  - NPE is:
    - Operationally effective, except for inconsistent performance in the auto-rekey functionality on devices using Enrollment over Secure Transport (EST) protocol.
    - Operationally suitable except for EST protocol use with switches, which displayed a lack of operationalized capability that, along with insufficient user training, contributed to device setup delays and auto-rekey failures.
    - Survivable against limited capability nearsider and outsider threats. The NSA has yet to test NPE against advanced cyber threats.
- The DISA help desk needs improvement, and the DMDC help desk was not prepared to operationally support the PKI Spiral 4 capabilities.
- The NPE test effort and operational deployment is handicapped because vendors have not fully implemented protocols for device enrollment and auto-rekeying, which limits available devices for operational testing, and the DOD lacks enterprise NPE policy and implementation guidance.
- TMS long-term sustainment continues to mature; however, the NSA has yet to fully document or follow the formal security certification assessment process prior to deploying new PKI tokens.

Recommendations

- The PKI PMO, DISA, and DMDC should:
  1. Continue to resolve all high-priority defects and verify acceptability to users prior to the PKI Increment 2 Full Deployment Decision.
  2. Resolve sustainability, help desk training, and logistics problems through transition to DISA and DMDC.
  3. Fix or mitigate cybersecurity findings identified during the LUT.

4. Coordinate with the DOD Chief Information Officer to issue NPE guidance for the Services and Agencies on the intended NPE enterprise-wide implementation for devices, protocol, and portal use.
5. Complete full security certification testing for new PKI tokens, and rigorously follow the certification process for all future token variants to ensure that new tokens are secure prior to deploying them into the operational environment.
6. Conduct comprehensive operational testing of NEATS, NPE, and TMS in virtualized hosting, including cybersecurity adversarial assessments emulating advanced threats.