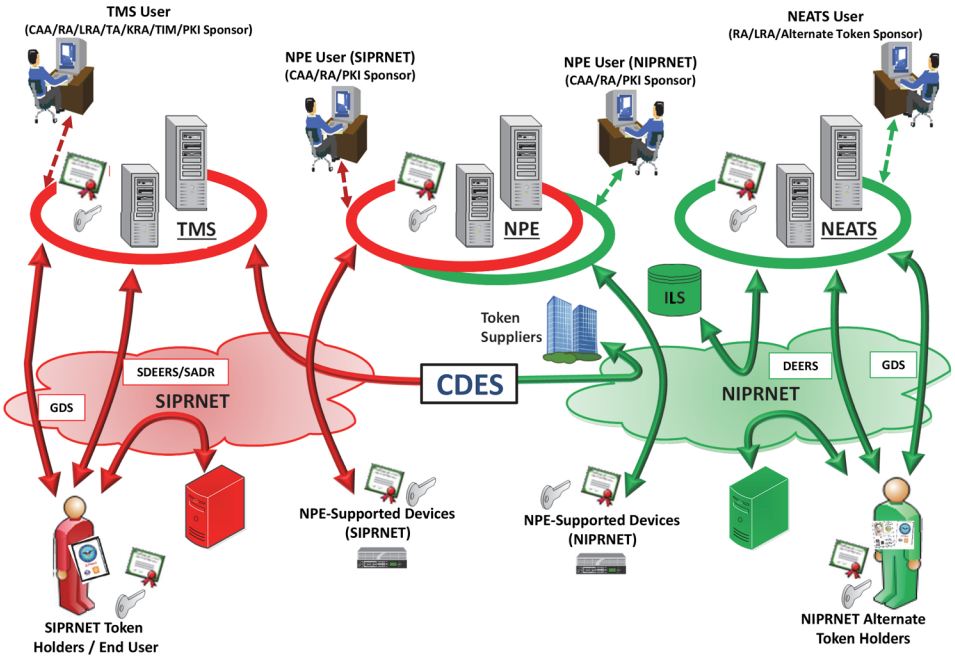
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted a Limited User Test (LUT) of the Public Key Infrastructure (PKI) Increment 2, focusing on Spiral 4 capabilities, in September/November 2019 to reduce risk and inform a planned Limited Deployment Decision in late February/March 2020.
- The PKI Program Management Office (PMO) and Defense Information Systems Agency (DISA) plan to migrate the Token Management System (TMS) from the DISA physical hosting to a virtualized environment in February/March 2020.
- JITC plans to conduct an OT&E of the new DISA virtual server solution for TMS in March/May 2020 to inform a decision to cutover to a new server.



CAA - Certificate 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 - Secure 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 is developing and 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) capabilities.
  - NEATS is intended to provide confidentiality, integrity, authentication, and nonrepudiation 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 will provide token registration, issuance, personnel identification number reset, revocation, and key recovery. The private keys are encoded on the token, which is a smartcard embedded with a microchip.
  - The NPE system issues certificates to large numbers of network devices (e.g., routers and web servers) 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 issue device certificates singularly or in bulk without the need for PKI registration authority approval.
  - The NSA manages the NEATS and NPE with operational support from DISA, which hosts the infrastructure and provides PKI support for the DOD, and the Defense Manpower Data Center (DMDC). DMDC also manages the Defense Enrollment Eligibility Reporting System for the NIPRNET and Secure 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 sites.

Mission

- Commanders at all levels will use DOD PKI to provide authenticated identity management via personal identification number-protected CACs, SIPRNET or NEATS tokens to enable DOD members, coalition partners, and other authorized users to access restricted websites, enroll in online services, and encrypt and digitally sign email.
- Military operators, communities of interest, and other authorized users will use DOD PKI to securely access, process, store, transport, and use information, applications, and networks.
- Military network operators will use NPE certificates for workstations, web servers, and devices to create secure network domains, which will 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 – Abington, Maryland
- Giesecke and Devrient America – Twinsburg, Ohio

Activity

- JITC conducted a PKI Increment 2 operational assessment in November/December 2018 as a risk reduction event to evaluate the Spiral 4 NPE and NEATS capabilities, but found the systems were not ready for the FOT&E.
- JITC conducted a cybersecurity verification of deficiency corrections of PKI Increment 2, Spiral 4 capabilities in December 2018.
- In February 2019, the PKI PMO delayed the PKI Increment 2 FOT&E to resolve high-priority Spiral 4 system defects and integration problems found in the operational assessment and subsequent continuous monitoring, as well as cybersecurity findings.
- In accordance with a DOT&E-approved test plan, JITC conducted a LUT of all Increment 2 capabilities, including the new Spiral 4 NPE and NEATS functionalities in September/November 2019. The LUT examined the NEATS on NIPRNET and the NPE enterprise certificate issuance and management system deployed in both the NIPRNET and SIPRNET environments.
- The PKI PMO changed the estimated Increment 2 Full Deployment Decision from October 2018 to late January 2020, but the PMO will likely change the Full Deployment Decision estimate to late 2020/2021.
- The PKI PMO and DISA plan to migrate TMS from the DISA physical hosting to a virtualized environment in February/March 2020.
- JITC intends to conduct an OT&E of the new DISA virtual server solution for TMS in March/May 2020 to inform a decision to cutover to a new server.

Assessment

- Problems associated with PKI Increment 2, Spiral 4 NPE and NEATS capabilities found in developmental and integrated testing, and the operational assessment events affected preparations for operational testing.
  - The NEATS and NPE functionality continues to improve; but processes, interfaces, and sustainment were immature and not ready for operational testing.
  - The DISA and DMDC help desks were not prepared to support the PKI Spiral 4 capabilities operationally.
- TMS stability, NPE and NEATS capability problems, and the lack of operationally representative NPE devices caused several test event schedule slips.
- The NPE test effort is handicapped because vendors have not fully implemented protocols for device enrollment, so the Key System Attribute to auto-rekey devices is unlikely to be met.
  - With assistance from the DOD Chief Information Officer (CIO), the PKI PMO continues investigating and identifying devices that will support the NPE protocols.
- The proposed NPE integration efforts provide limited, semi-automated protocol solutions that likely will not satisfy the greater NPE requirement needs of the DOD, which include an as yet unknown, and much broader, range of devices.
- 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; however, the NSA has yet to fully document or follow the formal security certification assessment process prior to deploying new PKI tokens.

Recommendations

- The DOD and Service CIOs should:
  1. Develop DOD enterprise NPE policy and implementation guidance for automated device enrollment.
- The PKI PMO and DISA should:
  1. Continue to resolve all high-priority defects and verify acceptability to users prior to the PKI Increment 2 Full Deployment Decision.
  2. Establish a dedicated transition working-level integrated product team to address sustainability and logistics problems through transition to DISA and DMDC.
  3. Coordinate with the DOD CIO to issue NPE guidance for the Services and Agencies on the intended NPE approach for enterprise-wide Certificate Authorities and devices.
  4. 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.