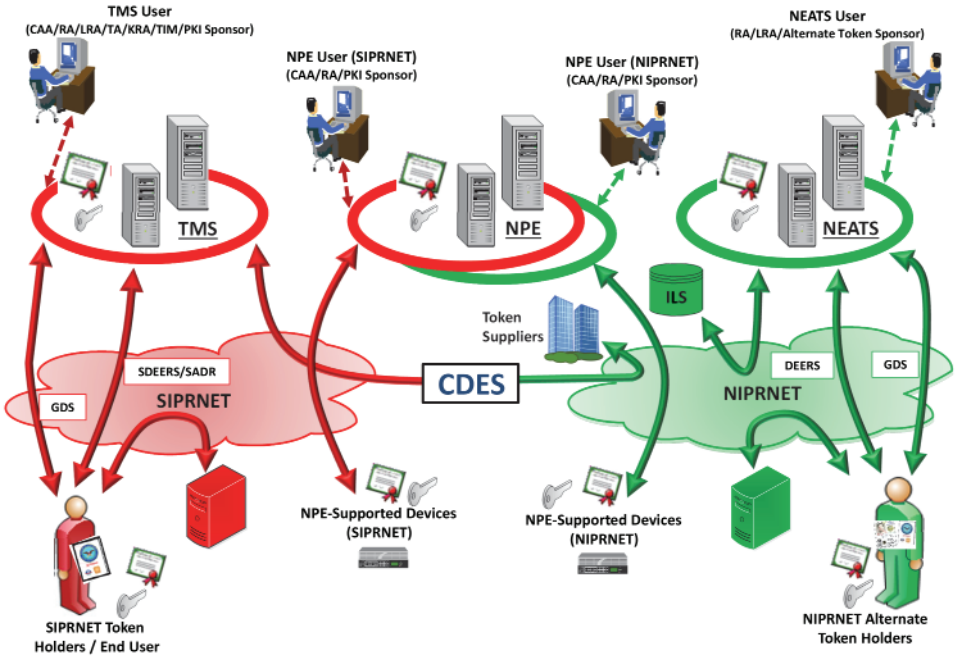
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- DOT&E published the Public Key Infrastructure (PKI) Increment 2, Spiral 3 FOT&E Report in December 2017 based on the test that the Joint Interoperability Test Command (JITC) conducted in August/September 2017.
  - Spiral 3 is operationally effective and suitable for day-to-day operations, but not suitable for long-term sustainment.
  - The National Security Agency (NSA) Senior Acquisition Executive (SAE) approved DOD-wide fielding of Spiral 3 in October 2018.
- The USD(A&S) delegated Milestone Decision Authority for the DOD PKI Increment 2 program to the NSA in March 2018.
- JITC began assessments of PKI Increment 2, Spiral 4 in 2018. In late July 2018, the PKI Program Management Office (PMO) delayed the Operational Assessment (OA) of the PKI Increment 2, Spiral 4 capabilities until November/ December 2018 to resolve high-priority system defects and integration problems.



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 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 Token Management System (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 the Defense Information Systems Agency (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 (DEERS) for the NIPRNET and Secure Defense Enrollment Eligibility Reporting System (SDEERS) for the SIPRNET, the authoritative sources for personnel data.

- NPE and NEATS use commercial and government off-the-shelf hardware and software hosted at respective DISA and DMDC sites.

Mission
- Commanders at all levels will 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 others 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
- In February 2018, DOT&E approved the combined test plan for the PKI Increment 2 OA and future FOT&E.
- The USD(A&S) delegated Milestone Decision Authority for the DOD PKI Increment 2 program to the NSA in March 2018.

Spiral 3
- DOT&E published the PKI Increment 2, Spiral 3 FOT&E Report in December 2017 based on a test that JITC conducted in August/September 2017.
- JITC verified Spiral 3 deficiency fixes in June 2018 and began a SIPRNET token reliability assessment in July 2018.
- The NSA SAE approved DOD-wide fielding of Spiral 3 in October 2018.

Spiral 4
- JITC conducted three cybersecurity assessments of PKI Increment 2, Spiral 4 capabilities in FY18 (the results are classified):
  - NPE Cooperative Vulnerability and Penetration Assessment (CVPA), February 2018
  - NEATS CVPA, March 2018
  - NPE Adversarial Assessment, June 2018
- JITC conducted the NPE and NEATS CVPA re-tests in October 2018.
- In late July 2018, the PKI PMO delayed the OA of the PKI Increment 2, Spiral 4 capabilities until November/December 2018 to resolve high-priority system defects and integration problems.
- JITC plans to conduct an FOT&E of all Increment 2 capabilities, including the new Spiral 4 NPE and NEATS functionalities, from March/April 2019. The FOT&E will examine the NEATS on NIPRNET and the NPE enterprise certificate issuance and management system deployed on both the NIPRNET and the SIPRNET.
- The PKI PMO changed the estimated Increment 2 Full Deployment Decision to late July 2019.

Assessment
- PKI Increment 2, Spiral 3 is operationally effective and suitable for day-to-day operations, but not suitable for long-term sustainment.
  - Testing revealed PKI process problems with tiered help desk coordination, configuration management, and token certification.
- Problems associated with Spiral 4 NPE and NEATS capabilities found in developmental and integrated testing events are affecting preparations for operational testing.
- NPE and NEATS capability problems and the lack of operationally representative NPE devices caused several test event slips.
- The Service and Agency NIPRNET System Administrators must be equipped with NEATS tokens in order to adequately demonstrate auto-provisioning of NPE certificates. Because of the significance of NEATS developmental test findings and initial classified findings stemming from the NEATS CVPA, the PKI PMO delayed the OA to resolve high-priority system defects and integration problems.
- 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.
  - The PKI PMO is still investigating and identifying devices that will support the NPE protocols.
- The proposed NPE integration efforts only 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 certainly much broader, range of devices.
- The NSA is responsible for certifying that tokens are secure in the operational environment. However, the NSA did not fully document or follow a formal assessment process for the Giesecke and Devrient tokens.
- The PKI PMO and DISA plan to migrate TMS from the DISA physical hosting to a virtualized, Next Generation environment after the planned Increment 2 FOT&E and currently do

not have plans to operationally test changes to the system architecture and any interfaces for the Services and Agencies.

Recommendations

- The DOD and Service Chief Information Officers should:
  1. Develop a 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 entering the PKI Increment 2, Spiral 4 OA and FOT&E.
  2. Establish a dedicated sustainability working-level integrated product team to address sustainability and logistics problems through transition to DISA and DMDC.
  3. Establish a more realistic, event-driven timeline for future PKI capability testing that better supports milestone decisions, while managing the expectations of those with PKI equities.
  4. Issue NPE procedures for implementation of auto-rekey protocols to assist Service and Agency System Administrators with device configurations.
  5. Coordinate with the DOD Chief Information Officer to issue NPE guidance for the Services and Agencies on the intended NPE approach for enterprise-wide Certificate Authorities and devices.
  6. Complete full security certification testing for existing Giesecke and Devrient tokens, and rigorously follow the certification process for all future token variants to ensure new tokens are secure prior to deploying them into the operational environment.
  7. Delay the PKI Increment 2 FOT&E until the system architecture, critical Spiral 4 functionality, and interfaces are ready for test.
  8. Plan for JITC to conduct a post-Increment 2 operational test to evaluate the TMS hosting and cybersecurity in the DISA Next Generation environment.