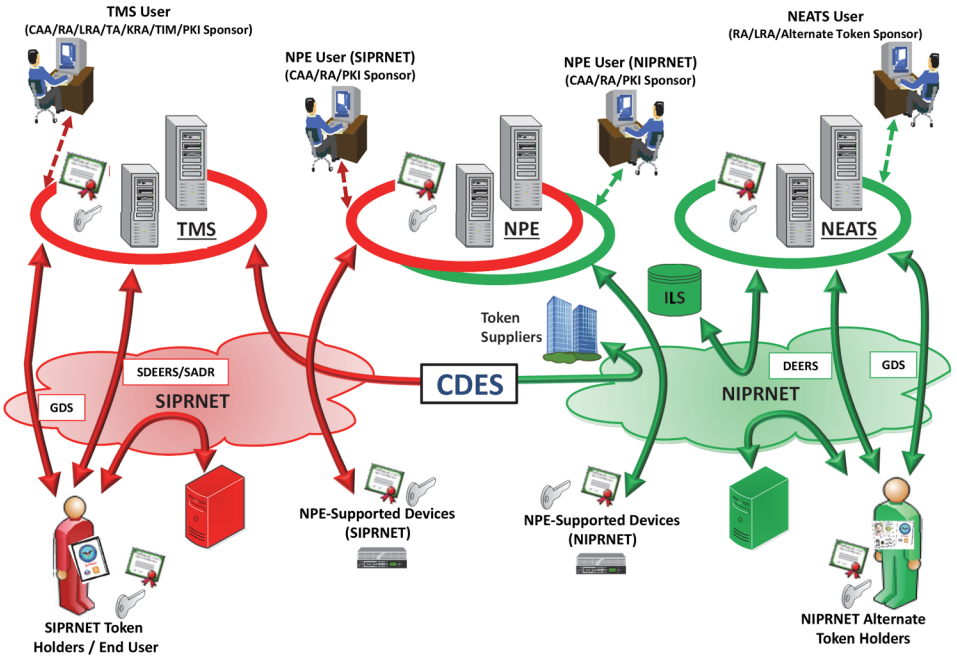
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an FOT&E of the Increment 2 Spiral 3 Public Key Infrastructure (PKI) capabilities in August and September 2017 in accordance with a DOT&E-approved test plan.
- The Spiral 3 FOT&E examined enhancements to the Token Management System (TMS) including a new Central Management of Tokens (CMT) capability, end-user certificate rekey, an Advanced Reporting System (ARS), and the ability to terminate expired certificates in batches. The FOT&E also examined sustainability processes including help desk, system administration, failover, training, and documentation.
- Preliminary PKI FOT&E findings and observations indicate the Spiral 3 TMS, CMT, and ARS capabilities are working with a few problems pertaining to second source tokens, certificate rekey and revocation, and help desk processes.
- DOT&E published the PKI Spiral 3 FOT&E Report in December 2017.



System

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. DOD PKI supports the secure flow of information across the DOD Information Network as well as secure local storage of information.
- The primary purpose of the SECRET Internet Protocol Router Network (SIPRNET) TMS is to issue tokens and certificates to end users. The private keys are encoded on the token, which is a smartcard embedded with a microchip.
  - The National Security Agency (NSA) manages TMS with operational support from the Defense Information Systems Agency (DISA), which hosts the infrastructure and provides PK-enabling support for DOD. TMS uses the Defense Manpower Data Center's Secure Defense Enrollment Eligibility Reporting System (SDEERS) as the authoritative data source for personnel data and provides capabilities for token formatting, user registration, token enrollment, token personal identification number reset, token suspension and restoration, token revocation, and encryption private key escrow and recovery.
  - TMS uses commercial off-the-shelf hardware and software components using Linux-based operating systems hosted at the DISA Enterprise Service Centers in Mechanicsburg, Pennsylvania, and Oklahoma City, Oklahoma.
- The NSA deployed PKI Increment 1 on the Non-classified Internet Protocol Router Network (NIPRNET) with access control provided through Common Access Cards (CACs). The NSA is developing and deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA deployed Spirals 1 and 2, while Spirals 3 and 4 will deliver TMS enhancements, inventory logistics tools, an enterprise-level alternate token issuance and management system (for system administrators) on the NIPRNET, and an enterprise-level Non-Person Entity (NPE) (e.g., workstations, routers, and web servers) for certificate issuance and system management.

Mission

- Commanders at all levels will use DOD PKI to provide authenticated identity management via personal identification number-protected CACs or SIPRNET 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 mobile devices to create secure network domains, which will facilitate intrusion protection and detection.

Major Contractors
- General Dynamics Mission Systems – Dedham, Massachusetts (Prime)
- 90Meter – Newport Beach, California
- SafeNet Assured Technologies – Abington, Maryland

Activity
- USD(AT&L) approved the fielding of the PKI Spiral 3, Release 4 TMS capabilities in January 2017 for DOD-wide use.
- The PKI Program Management Office (PMO) procured 566,500 second source Giesecke and Devrient (G&D) tokens for the DOD, that the Services and agencies later discovered were not interoperable with some thin and zero client environments.
- The PKI PMO developed a SIPRNET DISA Integration Lab (DIL) in March 2017 that provided limited system capacity and did not adequately represent the operational environment.
- The PKI PMO conducted a 2-week sustainment review in July 2017 to address problems with token failure tracking, help desk processes, token inventory logistics, and new token deployment processes.
- JITC conducted an FOT&E of the Spiral 3 PKI capabilities in August/September 2017 in accordance with a DOT&E-approved test plan. DOT&E published the PKI Spiral 3 FOT&E Report in December 2017.
- The Spiral 3 FOT&E examined enhancements to TMS including a new CMT capability, end-user certificate rekey, an ARS, and the ability to terminate expired certificates in batches. The FOT&E also examined sustainability processes including help desk, system administration, failover, training, and documentation.
- DOT&E approved the PKI Spiral 4 Test and Evaluation Master Plan (TEMP) Addendum in October 2017. The PKI Spiral 4 TEMP Addendum covers NPE automated device certificate issuance system and NIPRNET Enterprise Alternate Token System (NEATS).
- JITC plans to conduct a Spiral 4 operational assessment of NPE and NEATS in February 2018 and an Increment 2 FOT&E from May to June 2018.

Assessment
- CMT, ARS, and Nagios system health and monitoring capabilities operate properly but testing revealed that during routine failovers between the two TMS sites, ARS and CMT did not fail over correctly, requiring manual troubleshooting.
- The PKI PMO made improvements to training and documentation through classroom and on-demand, web-based training modules.
- The preliminary PKI Spiral 3 FOT&E findings are:
  - The Spiral 3 capabilities work. However, some deficiencies across the PKI capability set remain.
    - Registration Authorities successfully configured CMT to accept new tokens into their inventories, transfer tokens to affiliated sites, and place token orders. Token Inventory Managers confirmed that their inventories automatically updated as tokens transitioned between states (e.g., issued, blacklisted, and failed).
    - A small set of 50 end users demonstrated the ability to rekey their tokens within 60 days of expiration. However, in some cases, network configuration changes were required and Registration Authorities needed to confirm revocation of the users' original certificates.
    - An automated token termination server-side process terminated approximately 8,000 expired tokens in bulk, allowing Registration Authorities to reuse stacks of tokens without manually revoking each token individually.
    - Registration Authorities experienced sporadic problems revoking certificates, and end users with newly issued tokens experienced intermittent problems logging on, or digitally signing and encrypting emails.
    - The newly deployed second source G&D tokens do not work in many thin and zero client environments. The PKI PMO has been aware of the token problem since December 2016, but did not initiate a root cause analysis effort. Services and agencies only became aware of the problem when they employed the G&D tokens in the operational environment.
  - Some new Spiral 3 and long-standing Increment 2 deficiencies across the PKI capability set remain.
    - Token failure estimates as reported through TMS may prove to be inaccurate despite the inclusion of a token failure reporting mechanism. Services and agencies track internal failures and do not uniformly use the new TMS reporting process.
    - The PKI PMO piloted a new SIPRNET DIL in February 2017 to support developmental testing; however, the DIL lacked the necessary operational relevance to avert problems discovered after deployment.
    - A token reliability test, conducted using a sample of 365 users, concluded that second source tokens achieved a Mean Time to Failure (MTTF) of 26,605 hours whereas the SafeNet version 4.0c tokens achieved a MTTF of 1,175 hours at the 80 percent confidence level. Both tokens failed to meet the target MTTF of 43,000 hours, which assumes a 3-year life span and an 8-hour per day

usage profile. The existing requirement is in question because usage profiles of the sample population indicate tokens may be used for less than 1 hour per day for the majority of users and for much longer durations per day for a small subset of users. The data confirms that the G&D tokens can support the required 3-year life span given a 5-hour usage per day profile whereas the SafeNet 4.0c tokens can support approximately 13 minutes per day over the required 3 years.

- The PKI PMO deployed the second source token types without adequate beta testing in realistic operational environments resulting in interoperability findings with existing thin and zero clients across the DOD.
- Help desk processes remain inadequate because Registration Authorities continue to contact the PKI PMO directly for Tier III support, therefore losing the benefit of a trouble ticket tracking and reporting system.
- ARS is more widely used since the 2016 Limited User Test but remains difficult to use without assistance from experienced users.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed two of three previous FY16 recommendations. The PKI PMO still should provide periodic reports of token reliability, failure rates, and root cause analyses.
- FY17 Recommendations. The PKI PMO should:
  1. Implement a sustainable token reliability testing and certification process to ensure new tokens work in existing DOD thick, thin, and zero client environments.
  2. Establish an operationally representative DIL to properly examine TMS and NPE capabilities in a test environment. To support long-term sustainment, ensure the DIL is available for the Services and agencies to interconnect and test device and middleware variants.
  3. Establish an integrated product team to address sustainability problems through transition of the program to DISA.