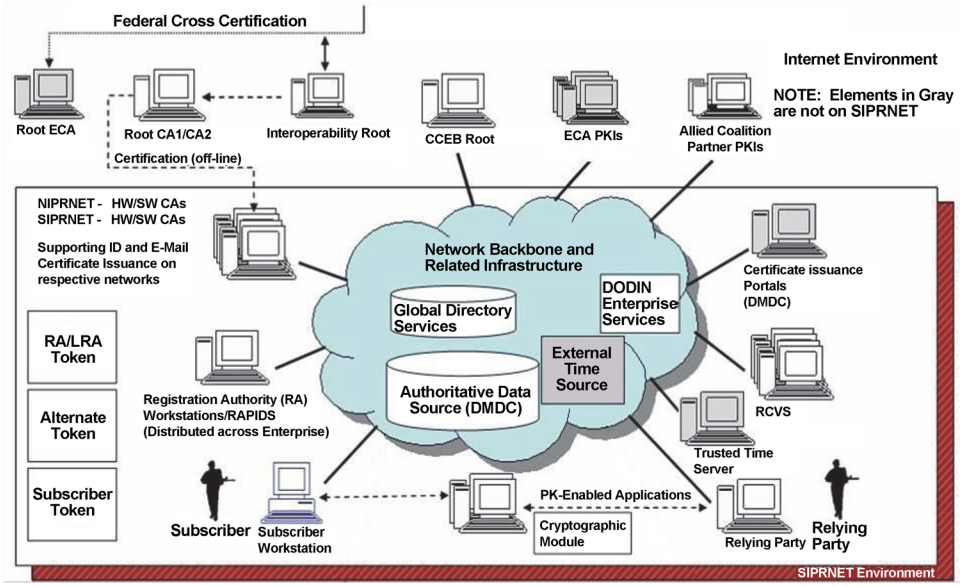
Public Key Infrastructure (PKI) Increment 2

Executive Summary

- DOT&E published a memo in late December 2015 noting that poor Secret Internet Protocol Router Network (SIPRNET) token reliability continues to impede operational missions requiring secure access to SIPRNET, and recommended that the Public Key Infrastructure (PKI) Program Management Office (PMO) address the problem. The PMO recently began issuing two new token types to the field, and deploying to a small set of users an automated token data logging capability to evaluate and improve token reliability. The new token types include a redesigned token from the existing manufacturer and a second source token type based on Common Access Card technology.
- In late February 2016, the PKI Program Manager changed his Full Deployment Decision (FDD) estimate to April 2018, triggering a Significant Change. The program manager subsequently changed his FDD estimate to July 2018.
- The Joint Interoperability Test Command (JITC) conducted a Limited User Test (LUT) of PKI Token Management System (TMS) releases 4.1, 4.2, and 4.3 from July 18 to August 11, 2016. New capabilities under test included Very Important Person (VIP) and Traditional Group, Role-based, and User-Identity tokens; recovery of past encryption keys to a token; TMS monitoring; and automatic failover between the primary and alternate sites. Test results revealed that DOD PKI Increment 2 Spiral 3 Releases 4.1, 4.2, and 4.3 are operationally effective, operationally suitable except for the Advanced Reporting System (ARS), and interoperable. Cybersecurity analyses are ongoing.
- JITC and National Security Agency (NSA) cybersecurity teams conducted a cooperative cybersecurity assessment of TMS in July 2016.
- DOT&E published the PKI TMS Release 4 LUT report in November 2016.
- A persistent cyber opposing force identified a significant PKI vulnerability during a DOT&E-sponsored cybersecurity assessment, and DOT&E is preparing a classified finding memo that will recommend remediations.
- The NSA PKI PMO delayed deployment of the Defense Information Systems Agency (DISA) Integration Lab (DIL), a key aspect of the program's late 2014 post-critical change way ahead. Without the DIL, the PKI Program Manager will continue to deploy potentially immature capabilities directly to the production environment, creating operational risk for users.
- JITC plans to conduct a Spiral 3 FOT&E from April to May 2017.



CA – Certificate Authority
CCEB – Combined Communications Electronic Board
DMDC – Defense Manpower Data Center
DODIN – Department of Defense Information Networks
ECA – External Certification Authority
LRA – Local Registration Authority
NIPRNET – Non-secure Internet Protocol Router Network
RA – Registration Authority
RAPIDS – Real-Time Automated Personnel Identification System
RCVS – Robust Certificate Validation Service
SIPRNET – SECRET Internet Protocol Router Network

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 Networks as well as secure local storage of information.
- The SIPRNET TMS's primary mission 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 NSA manages TMS with operational support from 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 (DEERS) 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 (COTS) 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-secure Internet Protocol Router Network (NIPRNET) with access control provided through Common Access Cards. 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 Common Access Cards 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
- The PKI PMO conducted multiple government-led TMS 4.1 and 4.2 developmental tests to resolve software deficiencies from December 2015 to June 2016.
- DOT&E published a memo in late December 2015 noting that poor SIPRNET token reliability continues to impede operational missions requiring secure access to SIPRNET, and recommended that the PKI PMO address the problem. The PMO recently began issuing two new token types to the field, and deploying to a small set of users an automated token data logging capability to evaluate and improve token reliability. The new token types include a redesigned token from the existing manufacturer (SafeNet) and a second source token type based on Common Access Card technology.
- DOT&E approved the PKI Spiral 3 Test and Evaluation Master Plan (TEMP) Addendum in February 2016.
- The PKI PMO and JITC began writing the Spiral 4 TEMP Addendum in late February 2016. Spiral 4 will support the NIPRNET Enterprise Alternate Token System (NEATS), NPE, and Secure Channel Protocol (SCP) 03 development efforts and testing.
- In late February 2016, the PKI Program Manager changed his FDD to April 2018, triggering a Significant Change. The program manager subsequently changed his FDD estimate to July 2018.
- JITC conducted a LUT of PKI TMS Releases 4.1, 4.2, and 4.3 from July to August 2016. These releases provide TMS privileged users with enhanced management and reporting functions, TMS system administrators with improved monitoring tools, and SIPRNET token end-users with more flexible ways to securely share information through group and role-based tokens. Additionally, TMS 4.3 implements an automated failover capability. TMS 4.1, 4.2, and 4.3 capabilities include:
  - TMS VIP, Traditional Group, role-based, and user-identity token processes and enrollments with encryption, identity, and signing certificate attributes.
  - ARS uses the Pentaho COTS tool to create data-object templates and ad hoc reports.
  - The Nagios COTS tool that provides the DISA system administrators with a system health and monitoring dashboard view of TMS performance metrics, server services, connections, storage, and data files.
- JITC and NSA cybersecurity teams conducted a cooperative cybersecurity assessment of TMS in July 2016.
- DOT&E published the PKI TMS Release 4 LUT report in November 2016.
- A persistent cyber opposing force identified a significant PKI vulnerability during a DOT&E-sponsored cybersecurity assessment, and DOT&E is preparing a classified finding memo that will recommend remediations.
- The PKI PMO plans to conduct developmental testing of TMS release 5.0 and 6.0, starting in December 2016.
- JITC plans to conduct the Spiral 3 FOT&E from April to May 2017.

Assessment
- Developmental testing conducted on the production environment in February, March, and June 2016 resulted in the identification and fixing of 11 high-priority software deficiencies. Four high-priority deficiencies were found during the four-week LUT, not including several high-risk cybersecurity vulnerabilities, which are still being evaluated. PMO delays in software delivery and the need for successive regression testing in the production environment have overtaxed the user community and further compressed the already aggressive Increment 2 schedule.

- Developmental test planning and process improvements since the critical change included an event-driven test approach, regression testing prior to proceeding to operational testing, and involving more Service and agency users in test events.
- From April to June 2016, there were ongoing TMS performance/latency problems impeding certificate issuance and revocation that affected PKI mission operations for all Services and agencies. The PKI PMO reduced those latency and failover problems with the hardware refresh completed at the DISA hosting sites in late June 2016.
- Services and agencies continue to experience SIPRNET token shortages that are a direct result of poor logistics supply planning, high token failure rates, and delays in provisioning and long lead time for new token types. Moreover, a surge of expiring SIPRNET PKI certificates (certificates expire after 3 years) require users to renew their certificates, which involves the time-consuming process of interfacing with a Registration Authority (RA).
- Significant PKI SIPRNET token shortages forced Services to institute rationing for FY16.
- PKI TMS release 4.1, 4.2, and 4.3 LUT assessment:
  - JITC examined TMS VIP, group, and role token processes and enrollments with encryption, identity, and signing certificate attributes. The TMS 4.1 and 4.2 functionality is working properly and provides operational benefits such as methods for encouraging adoption of secure authentication, encryption, and non-repudiation.
  - A new bulk revocation capability has been tested successfully by many Services and agencies, driven by the large stock of returned tokens that require proper handling for termination or reuse.
  - The PMO placed two new token types into circulation to address the poor reliability of existing tokens. JITC has not operationally tested these new token types, and the Services have yet to equip most sites with the required middleware version to utilize the new tokens. The Services are reporting few problems with the new token types.
  - JITC evaluated ARS, which uses the Pentaho tool to create data-object templates and ad hoc reports. The Service RAs stated that ARS is a powerful tool, but they need a tailored instruction guide and more training to better understand how to use ARS.
  - JITC tested TMS release 4.3 and the Nagios COTS tool that provides DISA system administrators with a system health and monitoring dashboard view of TMS performance metrics, server services, connections, storage, and data files. TMS 4.3 implements an automated failover capability, which worked during the LUT. The Nagios tool will be more useful once it is tailored to meet the system administrators' specific system monitoring needs with specific thresholds for generating alerts that are tuned and once the system administrators define the techniques, tactics, and procedures for the tool.
- PKI LUT findings revealed that DOD PKI Increment 2 Spiral 3 Release 4.1, 4.2, and 4.3 are operationally effective, operationally suitable except for ARS, and interoperable. Security data analyses are ongoing.
- PKI LUT results indicated the following:
  - Some users experienced intermittent connectivity problems when enrolling tokens; however, the extent to which this affects their productivity is unclear.
  - TMS granted excessive privileges to Trusted Agents, allowing them to inadvertently renew a certificate rather than simply resetting a Personal Identification Number.
  - While running a report using ARS, one RA discovered approximately 500 active certificates that TMS should have revoked when the RA terminated the associated tokens. This should not have occurred because TMS should automatically revoke certificates when an RA terminates a token.
  - Users liked VIP group tokens, which allow staff members of senior officials to better handle official encrypted email traffic.
  - PKI successfully demonstrated automatic failover between the primary and alternate sites during the LUT after JITC-identified system configuration problems were corrected.
  - DISA system administrators successfully used the Nagios monitoring capability to troubleshoot TMS failures; however, the volume and types of alerts need adjustment to allow system administrators to respond when required.
  - ARS provides a much needed token reporting capability; however, users require more focused training. Default templates for standard data objects (e.g., number of tokens issued per month by Service) would be beneficial to users who do not have access to focused training.
- DISA system administrators identified a TMS-related configuration management problem that prevented automatic failover and complete data replication between the two Enterprise Service Center hosting sites. During the LUT, RAs attempting to run ARS reports during the LUT discovered that the report data were incomplete. The PKI PMO found the root cause and fixed the problem during the test, and subsequent failovers and data replication between sites functioned properly.
- The NSA PKI PMO and DISA delayed deployment of the DIL, a key aspect of the program's late 2014 post-critical change way ahead, due to lack of DIL effort prioritization, funding shortfalls, and hardware procurement problems. Without the DIL, the PKI Program Manager will continue to deploy potentially immature capabilities directly to the production environment, creating operational risk to users.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed one of four previous FY15 recommendations. The following remain:
  1. Develop the Spiral 4 TEMP Addendum in accordance with the redefined PKI Increment 2 Acquisition Strategy to

prepare stakeholders for the remaining deliveries, resource commitments, and T&E goals.
2. Define and validate sustainment requirements for PKI Spiral 4 capabilities.
3. Provide periodic reports of token reliability, failure rates, and root cause analyses.

- FY16 Recommendations. The PKI PMO should:

1. Establish an operationally representative DIL to properly examine TMS and NPE capabilities in a test environment containing realistic token data, interfaces to user test laboratories, and an email server to improve test adequacy prior to deploying capabilities to production.
2. Implement the cybersecurity mitigating actions from the classified memo.