



INSTITUTE FOR DEFENSE ANALYSES

**Public Key Infrastructure (PKI)
Increment 2 Root Cause Analysis (RCA)
for Performance Assessments and Root
Cause Analyses (PARCA)**

Brandon R. Gould
Benjamin S. Aronin
Patricia F. Bronson, Project Leader

May 2015

Approved for public release;
distribution is unlimited.

IDA Paper P-5209

Log: H 14-001179

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882



The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Project AY-7-357815, "Root Cause Analysis and Performance Assessment Methods and Analyses (Public Key Infrastructure)," for the Director, Performance Assessments and Root Cause Analyses. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Thank you to Lawrence N. Goeller, Stanley A. Horowitz, and Shanti Satyapal for performing technical review of this document.

Copyright Notice

© 2014, 2015 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-5209

**Public Key Infrastructure (PKI)
Increment 2 Root Cause Analysis (RCA)
for Performance Assessments and Root
Cause Analyses (PARCA)**

Brandon R. Gould
Benjamin S. Aronin
Patricia F. Bronson, Project Leader

Executive Summary

The Public Key Infrastructure (PKI) program is a Department of Defense (DoD) Major Automated Information System (MAIS) acquisition effort. “PKI” refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of Public Key certificates, and their corresponding private keys. PKI certificates provide the Information Assurance (IA) that enables Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) applications to securely perform their e-business functions.

On October 31, 2013, the National Security Agency (NSA) Senior Acquisition Executive (SAE) declared a Critical Change to the PKI Increment 2 program. (A Critical Change for an MAIS program is analogous to a Critical Nunn-McCurdy Breach for a Major Defense Acquisition Program.) NSA provided two reasons for issuing this critical change:

- Inability to achieve PKI Increment 2 Full Deployment Decision (FDD) within five years of program initiation (March 1, 2014 deadline), and
- Delay of over one year in the original FDD estimate provided to the Congress (1 March 2014 deadline).

The proximate cause of the Critical Change, reported in the DoD PKI Critical Change Executive Leadership Update dated December 18, 2013, was that “Initial and Follow-on Operational Test and Evaluations resulted in not operationally suitable and not operationally effective ratings that were not resolved in time to support a 1 March 2014 FDD.”

The Director, Performance Assessments and Root Cause Analyses (PARCA), asked the Institute for Defense Analyses (IDA) to conduct an RCA on the PKI Increment 2 Critical Change. This paper summarizes IDA’s understanding of the problem, our methodology, and our findings.

IDA concludes that the root cause of the Critical Change in the PKI Increment 2 program is the lack of understanding, from the beginning of the program, of the scope of the work that needed to be done to track and manage the Secure Internet Protocol Router Network (SIPRNet) tokens. We attribute this lack of understanding to poor performance by government personnel. From the beginning, the Services and Agencies (S/As), Program Executive Office (PEO), Program Management Office (PMO),¹ and Identity Protection and Management Senior Coordinating Group (IPMSCG) should have

understood the scope of the requirement, but did not. Once the problems became apparent, these organizations did not find and fix them in a timely fashion.

The IDA team also found there were unrealistic estimates for cost and schedule, the root cause of which was also a lack of understanding of the scope of work. Substantial work associated with Spiral 2 (Tactical) and Spiral 3 (Enhanced Status Quo) was deferred to later increments and are not part of this Critical Change. Additional resources will be needed to complete the deferred and unmet scope of work from Increment 2, but that will be for a future increment and will likely not be treated as a Critical Change for Increment 2.

We believe that the MAIS process itself is a contributor to this Critical Change. We do not believe the best resource planning can be accomplished in an environment in which the user decides the content of a program that has a fixed five-year development cycle. For this strategy to succeed, the user must develop and maintain a resource-loaded schedule for every item on their list of priorities. Each item has to be described well enough to demonstrate that the requirements are understood, and each item must have a cost estimate based on those requirements. We did not find evidence of well-documented resource-loaded schedules in the documentation we examined (including Acquisition Strategy, Systems Engineering Plan, or Life Cycle Cost Estimate Summary) for the PKI effort.

¹ PMO includes both program management and systems engineering functions.

Contents

1.	Introduction	1
2.	Methodology.....	3
3.	PKI Increment 2 System Description	5
	A. Description from the MAR.....	5
	B. High Level Description of the Capabilities from the Systems Engineering Plan.....	6
	1. SIPRNet Expansion	6
	2. Tactical Environments.....	6
	3. Homeland Security Presidential Directive (HSPD) 12	7
	4. Enhancing the Status Quo Capabilities	7
	C. Management Structure and Roles and Responsibilities	8
4.	Description of the Critical Change	11
5.	Proximate Causes for Schedule Growth.....	13
6.	Timeline Leading Up to the Critical Change	15
	A. 2008	15
	B. 2009	16
	C. 2010	16
	D. 2011	16
	E. 2012	17
	F. 2013	18
7.	Root Cause Narrative	19
	A. Logistics Shortfalls and Missing ILS Functionality.....	19
	B. Configuration Management.....	21
	C. Token Reliability Issues	22
	D. Priority toward Token Issuance.....	23
	E. Failing to Meet the Requirements	24
	F. Deferral of Requirements	26
	G. WSARA 2009 Root Cause Categories.....	27
8.	Root Cause Analysis.....	31
	A. Lack of Understanding of the Logistics Support Requirement	31
	B. Faulty Baseline	34
	C. Oversight	35
9.	Conclusions	39
	Appendix A. DoD CIO Issuance Mandate October 14, 2011.....	A-1
	Appendix B. Full Fielding ADM Jan 2012.....	B-1

Illustrations	C-1
References.....	D-1
Abbreviations.....	E-1

1. Introduction

The Director, Performance Assessments and Root Cause Analyses (PARCA), is responsible for conducting root cause analyses (RCAs) for Major Defense Acquisition Programs (MDAPs) when required by the Weapon Systems Acquisition Reform Act (WSARA) of 2009¹ or when requested by the Secretary of Defense, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), the Secretary of a military department, or the head of a Defense Agency.²

PARCA requested that the Institute for Defense Analyses (IDA) conduct a root cause analysis of the PKI Increment 2 program based on the 31 October 2013 Critical Change declared by the National Security Agency (NSA) Senior Acquisition Executive (SAE). This was a discretionary RCA for PARCA. This paper summarizes IDA's understanding of the problem, our methodology, and our findings.

Chapter 2 presents IDA's methodology for conducting RCAs for PARCA. Chapter 3 contains the Program Description for Public Key Infrastructure (PKI) Increment 2 from the Major Automated Information System (MAIS) Annual Report (MAR) of December 2013. Chapter 4 provides the official description of the Critical Change. Chapter 5 reports reasons for the breach as provided by the Program Management Office (PMO), the Program Executive Office (PEO) or other stakeholders. Chapter 6 provides the timeline of events leading up to the critical change. Chapter 7 starts with the Critical Change and works backwards, identifying its root causes aligned with WSARA taxonomy. Chapter 8 provides IDA's findings on the root causes of the PKI Increment 2 Critical Change and other findings. Chapter 9 provides IDA's conclusions on the root cause of the Critical Change for the PKI Increment 2 program.

¹ *Weapon Systems Acquisition Reform Act*, Pub. L. 111-23, 123 Stat. 1704 (2009), § 103(b)(2).

² *Ibid.*, § 103(b)(1).

2. Methodology

PKI Increment 2 is a MAIS. A Critical Change for an MAIS program is analogous to a critical Nunn-McCurdy breach for an MDAP. Accordingly, IDA's methodology for PKI Increment 2's Critical Change is identical to that of an MDAP experiencing a critical Nunn-McCurdy breach.

The methodology is composed of an official statement of the critical change, proximate causes for the Critical Change, a timeline of events leading up to the Critical Change, a root cause narrative that works backward from the Critical Change, and identification of root causes of the Critical Change.

The official statement of the breach is recorded in a program deviation report from the SAE to the Milestone Decision Authority (MDA). It is also recorded in the MAR. The MAR documents the Critical Change and includes the program office's position on the Critical Change and its causes in the Executive Summary.

The timeline of events identifies the important events leading up to the breach. The IDA research team constructs the initial version of the timeline from the program's historical MARs, but all sources are considered for the timeline of events leading up to the breach.

The Root Cause Narrative is a method for classifying the events identified in the "Timeline of Events" according to the WSARA root cause categories. WSARA provides seven specific root causes, but does not exclude the possibility that there may be others. The WSARA categories are:

- Unrealistic performance expectations
- Unrealistic baseline estimates for cost or schedule
- Immature technologies or excessive manufacturing or integration risk
- Unanticipated design, engineering, manufacturing, or technology integration issues arising during program performance
- Changes in procurement quantities
- Inadequate program funding or funding instability
- Poor performance by government or contractor personnel responsible for program management
- Any other matters

The Root Cause Narrative begins with the statement of the breach and proceeds backward in time, linking contributing factors. Ultimately, the contributing factors are classified as symptoms; proximate causes; root causes; and factors unrelated to cost or schedule growth. Graphs and data (as opposed to bullets and text) are provided as evidence without comment and conclusion. The evidence stands by itself and each reader is free to infer his or her own meaning.

The Root Cause Analysis identifies the root causes and allocates the contributing factors from the root cause narrative to these root causes. The root cause analysis also addresses whether the root causes reflect inception or execution problems and distinguishes between root causes that are exogenous and endogenous to the program.

3. PKI Increment 2 System Description

Figure 1 is the PKI logo taken from the 2013 MAR.

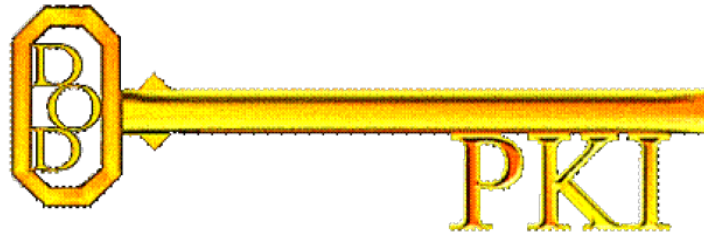


Figure 1. Department of Defense (DoD) PKI Program

A. Description from the MAR

Public Key Infrastructure (PKI) refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of Public Key certificates and their corresponding private keys and enabling Commercial Off the Shelf and Government Off the Shelf applications that provide Information Assurance and e-business capabilities. PKI will issue and manage electronic/digital identities and associated credentials and key materials for users, applications, servers, and network components.

The DoD PKI, Increment 2 was baselined to complete three development spirals to be implemented from FY 2009 through FY 2014. Increment 2 initiatives include the use of a hardware token on Secure Internet Protocol Router Network (SIPRNet), expansion of PKI into tactical low-bandwidth constrained environments, and compliance with Homeland Security Presidential Directive 12. The Program received a Milestone B Decision in April 2009 to enter the Engineering and Manufacturing Development phase.

The Program achieved a Milestone C decision in February 2011 to enter into Initial Operational Test and Evaluation (IOT&E) for Spirals 1 and 2. The Program completed IOT&E in September 2011 and declared Initial Operational Capability in November 2011. The Program achieved a Fielding Decision for Spiral 1 (SIPRNet) and Spiral 2 (Tactical) in

January 2012. Spiral 3 (Enhanced Status Quo) of the DoD PKI Program is in development.³

B. High Level Description of the Capabilities from the Systems Engineering Plan

The DoD PKI refers to the core framework and services that provide for the generation, production, distribution, control, revocation, recovery, storage, destruction, and accounting of public and private key certificates.

DoD PKI system components include Certificate Authorities (CAs) and a certificate repository; documentation, including a Certificate Policy document; Certification Practice Statements; and trained personnel performing trusted roles to operate and maintain the system. The DoD PKI framework is designed to provide the critically needed support for a broad range of human and Non Person Entities (NPEs) (e.g., applications, network devices, processes, etc.).

DoD PKI enables secure encryption, authentication of network transactions, data integrity, and non-repudiation to a broad range of government- and commercially based, security-enabled applications. DoD PKI supports the DoD's Defense-in-Depth layered Information Assurance (IA) strategy and provides for secure interoperability within DoD and with its Federal, Coalition, Allied partners and Non-Government Organizations.

The following paragraphs provide a high-level description of the four capabilities provided by DoD PKI Increment Two. These descriptions are from Increment 2's Systems Engineering Plan (SEP).

1. SIPRNet Expansion

The Increment Two SIPRNet expansion will provide support for the issuance of hardware tokens to support all SIPRNet users. In addition to providing support for a hardware token, the Increment Two SIPRNet expansion will provide support for interoperability between DoD SIPRNet users and Federal, State, and Coalition Partners and Allies in compatible environments. Finally, to maintain parity between the SIPRNet and Non-secure Internet Protocol Router Network (NIPRNet) PKI implementations, any enhancements integrated into the NIPRNet PKI implementation as a result of Increment Two will also be incorporated into the SIPRNet infrastructure.

2. Tactical Environments

The DoD PKI must be able to provide CA services that support certificate management, issuance, revocation, suspension, restoration, and validation in Tactical

³ Program Description for PKI Increment 2 from MAR, December 2013.

environments. Four development activities were identified to meet the requirements for expansion of the DoD PKI into Tactical environments:

- Deployed Certificate Authority (DCA)⁴
- Tactical Registration Authority (TRA)⁵
- Alternative token form factors⁶
- Joint Tactical IA Concept of Operations (CONOPS)

3. Homeland Security Presidential Directive (HSPD) 12

The following describes the HSPD-12 solution:

- Establish an Interoperability Root CA to support HSPD-12 requirement to participate with Federal Bridge Certificate Authority (FBCA)/ common policy Object Identifiers (OIDs).
- Transition to Server-based Certificate Validation Protocol (SCVP) utilizing existing Online Certificate Status Protocol (OCSP) Infrastructure.
- Transition PKI Infrastructure to support Personal Identity Verification (PIV) Authentication Certificates.
- Implement Rivest, Shamir, and Adelman (RSA) 2048 when viable and transition to Secure Hash Algorithm (SHA)-256 and/or Suite B (Elliptic Curve Cryptography [ECC] & SHA) when systems and applications ubiquitously support ECC & SHA-256.

4. Enhancing the Status Quo Capabilities

The Enhanced Status Quo architecture will provide the means to establish centralized trust and visibility of all aspects of the DoD enterprise to include the full scope of auto-enrollment and auto-renewal services as required by the enterprise. This includes support for, but is not limited to, all certificates issued, various protocols (i.e., Simplified Certificate Enrollment Protocol [SCEP]) and applications fielded in DoD (i.e., Microsoft). Suspension provides a capability to suspend certificates either singly or as a group. Certificate suspension will be used to invalidate (without permanently revoking) a single certificate or groups of certificates.

⁴ In cryptography, a **certificate authority** or **certification authority (CA)** is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

⁵ A **registration authority (RA)** is an authority in a network that verifies user requests for a digital certificate and tells the CA to issue it.

⁶ Physical **form factors** are tangible devices that users carry and use when authenticating.

Auto-enrollment and auto-renewal refer to the capability of automatically issuing and renewing PKI certificates to NPEs, most specifically Microsoft (MS) domain controller certificates, but to other NPEs as well.⁷

C. Management Structure and Roles and Responsibilities

The DoD PKI Organization Structure from the PKI SEP is shown in Figure 2.⁸

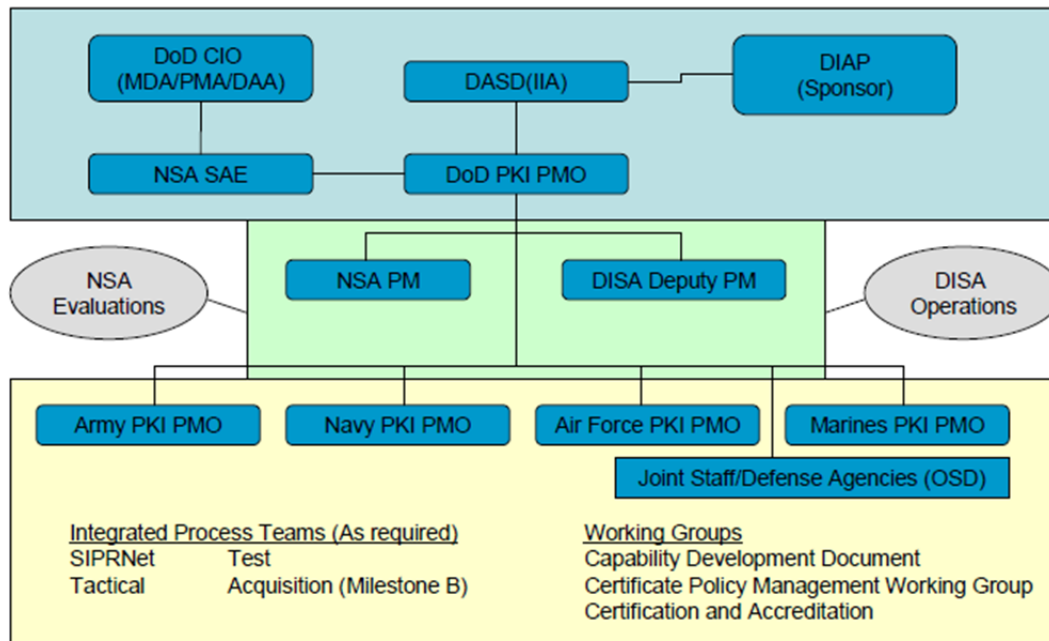


Figure 2. DoD PKI Increment 2 Organizational Structure

The NSA SAE provides acquisition assistance, oversight, and review as the program proceeds through its acquisition life cycle. NSA is responsible for PKI Increment 2 and the Defense Information Systems Agency (DISA) provides operational support. NSA and DISA established a central PMO, for which NSA provides the Program Manager (PM) and DISA the Deputy PM. NSA serves mainly as the materiel developer for the core infrastructure.⁹ DISA provides for the centralized PKI operational aspects, including the Global Directory Service (GDS).¹⁰

⁷ DoD PKI Program Management Office (PMO) Increment Two Systems Engineering Plan (SEP) Milestone B, Version 1.5, April 21, 2009.

⁸ Ibid.

⁹ Increment 2 Capabilities Development Document (CDD) Addendum.

¹⁰ Ibid.

The Defense Manpower Data Center (DMDC) supports the Real-Time Automated Personnel Identification System (RAPIDS) registration and Defense Enrollment Eligibility Reporting System (DEERS) database.¹¹ As time passed, DMDC also assumed other responsibilities in PKI Increment 2 that were not anticipated in the original plans.

The Military Services and other DoD Agencies provide the local registration, training, and key recovery capabilities.¹²

Until recently, the DoD Chief Information Officer (CIO) was the MDA for PKI Increment 2.

The Identity Protection and Management Senior Coordinating Group (IPMSCG) provides inter-Service/Agency (S/A) senior oversight of the DoD PKI. The members of the IPMSCG represent the Assistant Secretary of Defense, Networks & Information Integration (ASD(NII)), NSA, DISA, the DoD General Counsel, and the DoD Service CIO. The Department of the Navy CIO (DoN CIO) serves as the chairperson. The group provides a forum to address DoD-wide identity management issues and coordinates implementation across Combatant Commanders, S/As. The IPMSCG formulates identity management strategies with the S/As and conveys these strategies to the PKI PMO for execution.

In January 2012, the ASD(NII) authorities, responsibilities, personnel, and resources transferred to the DoD CIO. The acquisition-specific functions and resources related to Command, Control, and Communications (C3), non-intelligence space matters, and MAISs transferred from the DoD CIO to the USD(AT&L) and are in Deputy Assistant Secretary of Defense (DASD), Command, Control, and Communication (C3), Cyber, and Business Systems (C3CB). The DoD CIO is Principal Staff Assistant to SecDef and DepSecDef in information resource management matters.

¹¹ Ibid.

¹² Ibid.

4. Description of the Critical Change

The December 31, 2013 MAR provides a description of the critical change.

- Per 10 United States Code (U.S.C.) Chapter 144A, on October 31, 2013, the Senior Official declared a Critical Change based on two schedule-related criteria:
 - Inability to achieve Increment 2 FDD [Full Deployment Decision] within 5 years (1 March 2014 deadline)
 - Delay of over one year in original FDD estimate provided to Congress (1 March 2014 deadline)

Furthermore, the program status in the 2013 MAR also indicates there is cost growth to come:

The Critical Change Life Cycle Cost Estimate revealed the program had exceeded the cost by greater than 25% of the total life program cost as estimated in the (OE) [original estimate]. The OE did not include the appropriate 10 year sustainment costs. Based on the results of the Critical Change Report, the program will submit a revised OE to Congress as allowed by 10 U.S.C. 2445b(c)(2). Therefore, the Original Estimate Cost and Schedule parameters remain unchanged in this report.

Table 1 shows the change in schedule milestones reported in the 2013 MAR.

Table 1. Schedule Milestones

Schedule

Schedule Milestones		
Milestones	Original Estimate Objective	Current Estimate (Or Actual)
Funds First Obligated	Mar 2009	Mar 2009
Milestone A ¹	N/A	N/A
Milestone B	May 2009	Apr 2009
Milestone C	Jan 2011	Feb 2011
Full Deployment Decision ²	Mar 2013	Sep 2017
Full Deployment	TBD	TBD

In accordance with 10 U.S.C. Chapter 144A, the Full Deployment date is TBD until defined in the Full Deployment Decision Acquisition Decision Memorandum.

Memo

- 1/ The DoD PKI Increment 2 entered the acquisition process at Milestone B.
- 2/ The Full Deployment Decision date will be rebaselined as part of the critical change process.

Acronyms and Abbreviations

N/A - Not Applicable
TBD - To Be Determined

5. Proximate Causes for Schedule Growth

The Department of Defense PKI Critical Change Executive Leadership Update of December 18, 2013 provides a reason for the program not meeting its FDD date, which resulted in the Critical Change:

Initial and Follow-on Operational Test and Evaluations resulted in not operationally suitable and not operationally effective ratings that were not resolved in time to support a 1 March 2014 FDD.¹³

This statement points to the IOT&E and Follow-on Operational Test and Evaluation (FOT&E) reports for reasons the FDD had to be delayed.

¹³ Jason McCaskey, *Department of Defense Public Key Infrastructure: Critical Change Executive Leadership Update*. (December 18, 2013), 3.

6. Timeline Leading Up to the Critical Change

Figure 3 is a timeline for PKI Increment 2 showing events leading up to the critical change.

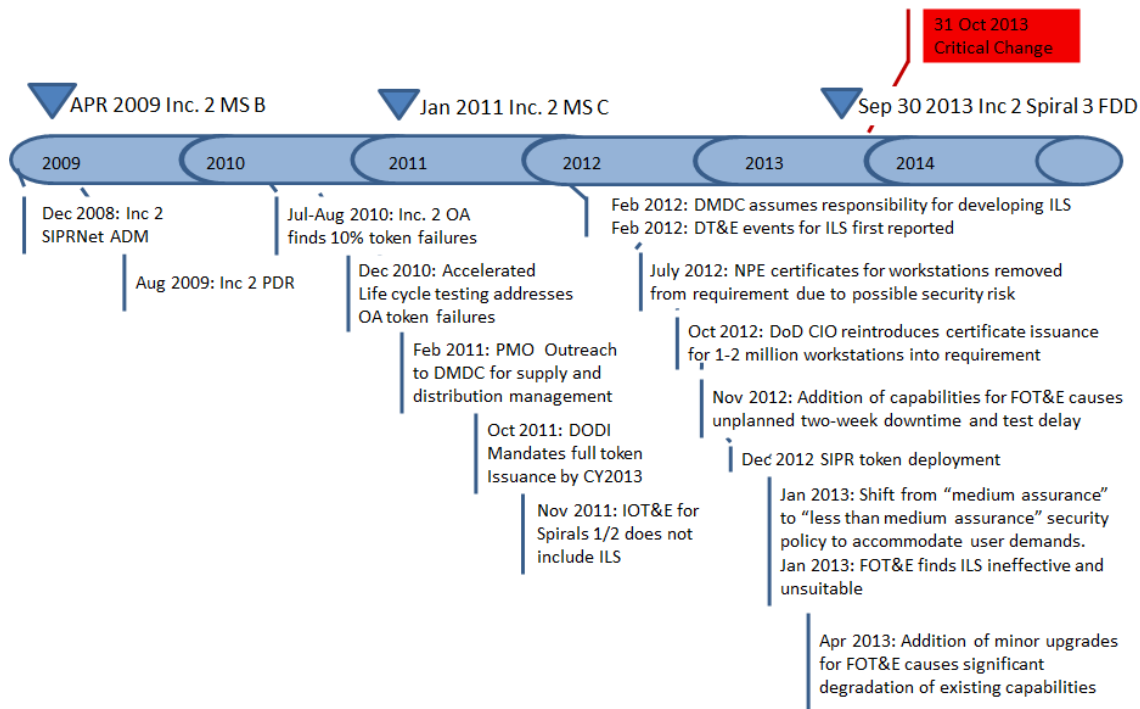


Figure 3. Program Events Leading to Critical Change

The following sections provide a descriptive timeline by year.

A. 2008

The PKI Increment 2 Acquisition Decision Memorandum (ADM) was signed in December 2008.¹⁴ The ADM schedule for Increment 2 includes a Spiral 1 and 2 Full Fielding Decision (FFD) objective of July 2011 and threshold January 2012, and a Spiral 3 Deployment Decision objective of March 2013 and threshold September 2013. The PKI Increment 2 PMO was stood up with an NSA PM and a DISA deputy PM.

¹⁴ MAR for PKI Increment 2, December 2013.

B. 2009

The Milestone (MS) B Review followed four months after the ADM was signed, in April 2009, and the Preliminary Design Review occurred in August 2009.

C. 2010

The June 2010 Operational Assessment (OA) of PKI Increment 2, Spiral 1 uncovered SIPRNet token reliability deficiencies.¹⁵ The OA for Increment 2, Spiral 1 showed that Registration Authorities (RAs) were able to efficiently issue SIPRNet tokens, and end users were able to use those tokens to facilitate missions through digital signing, encryption, and web-server authentication. However, reliability of the tokens was unacceptable, with approximately ten percent of those distributed during the OA found to be defective.

Findings from accelerated life cycle testing,¹⁶ necessitated by the problems identified in the OA, subsequently show token reliability was satisfactory.

D. 2011

The Program achieved an MS C decision in February 2011. This decision cleared the program to enter the Production and Deployment Phase for Spiral 2, and to enter into Initial Operational Test and Evaluation (IOT&E) for Spirals 1 and 2.¹⁷

The IOT&E test plan was approved on February 24, 2011. IOT&E tested the “interim” logistics process with the intent to test the final logistics solution (which had yet to be finalized in discussions with DMDC) during a later spiral.¹⁸

The Joint Interoperability Test Command (JITC) conducted Phase 1 IOT&E for DoD PKI Increment 2, Spirals 1 and 2, from March 1 to August 8, 2011. Phase 1 issued tokens to establish a minimum required user base (16,500).

JITC conducted Phase 2 of the IOT&E, which focused on overall system performance, scalability, information assurance, and tactical deployment, from August 8 to September 21, 2011. The IOT&E exposed significant logistics hurdles due to undefined processes for procuring, distributing, and tracking tokens.

¹⁵ 2011 DOT&E Annual Report.

¹⁶ Shanti Satyapal. The accelerated life cycle testing placed heavy emphasis on non-office-like conditions and poor handling practices (e.g., excessive heat, moisture) and not on repeated insertions of the card into the reader. This repetitive mechanical stress is now suspected of being a leading failure mode causing the increased observed token failures. New guidelines are being developed that will require use of sleeves to protect cards.

¹⁷ MAR, December 2013.

¹⁸ DAES Assessment, February 2011.

The Director, Operational Test & Evaluation (DOT&E) rated PKI Increment 2 as operationally effective with limitations, but not operationally suitable.

On October 14, 2011, the DoD CIO issued guidance to eliminate user anonymity on the SIPRNet by requesting the issuance of PKI tokens across the SIPRNet environments be completed by December 31, 2012 and software applications and infrastructure be fully enabled with PKI capabilities by June 30, 2013 (see Appendix A).

The PMO finalized the Memorandum of Agreement (MOA) with the DMDC to manage the token Inventory Logistics System (ILS) in November 2011.¹⁹

The program declared Initial Operational Capability (IOC) in November 2011.²⁰

E. 2012

The DoD CIO issued the PKI Increment 2 ADM for Full Fielding to SIPRNet and Tactical Environments in a memorandum dated January 20, 2012.²¹ The ADM approved full fielding of PKI to SIPRNet and Tactical Environments and the acquisition of tokens, card readers, and software to support full fielding. The ADM also directed NSA to resolve issues that contributed to the “Unsuitable” rating identified by the IOT&E, accelerate the procurement of the bulk formatter with issuance capability, and operationally test capability with the end-to-end logistical process (see Appendix B).

In February 2012, the DMDC demonstrated the ILS in the developmental environment for the S/As. The ILS is a key component for automating and tracking the bulk ordering and shipment of SIPRNet tokens in support of the end-to-end logistics process.²² The token ILS was made available for use in June 2012.²³

FOT&Es, originally scheduled for April–June 2012, were postponed to October 2012 due to system development delays and unanticipated system downtime caused by capability updates. (FOT&Es were eventually conducted in January 2013.)²⁴

July 2012 – NPE certificates for workstations were removed from requirement due to possible security risk.

¹⁹ DAES Assessment by PM, November 2011.

²⁰ MAR, December 2013.

²¹ MAR, December 2013; Teresa Takai, Public Key Infrastructure (PKI) Increment 2 Acquisition Decision Memorandum (ADM)—Full Fielding to Secret Internet Protocol Router Network (SIPRNet) and Tactical Environment, Memorandum (January 20, 2012).

²² DAES Assessment, February 2012.

²³ DAES Assessment, August 2012.

²⁴ DOT&E AR 2013.

October 2012 – DoD CIO reintroduced NPE certificate issuance for 1–2 million workstations into the requirement.

December 2012 – Systemic configuration management problems resulted in a stop-test.

The S/As largely met the December 2012 deadline for SIPRNet token deployment set by the DoD CIO in October 2011.

F. 2013

JITC conducted a delayed combined FOT&E I and II in January 2013 on the SIPRNet environment to address suitability shortcomings (see 2012 above).²⁵

In January 2013, the program’s security policy was changed from “medium assurance” to “less than medium assurance” to accommodate user demands (over NPE issues).

DOT&E issued the PKI Increment 2 FOT&E I and II Report on May 10, 2013. The report rated Increment 2 as both operationally ineffective and unsuitable. On July 25, 2013, the IPMSCG approved the removal of the following capabilities and their associated thresholds from the DoD PKI Increment 2 CDD:

- Transition to Internet Protocol version (IPv6),
- Server-based Certificate Validation Protocol (SCVP),
- Deployable Certification Authorities,
- Synchronization of Disconnected PKI Nodes,
- Tactical Registration Authority, and
- Tactical Certificate Revocation Information.

On October 31, 2013, the program experienced a Critical Change as declared by the NSA SAE.

²⁵ Ibid.

7. Root Cause Narrative

On October 31, 2013, the NSA SAE for the PKI Increment 2 program declared a Critical Change based on two schedule-related criteria: the inability to achieve an FDD within five years and a delay of the FDD by one year or more from the original estimate provided to the Congress. Subsequently, during development of the Critical Change Life Cycle Cost Estimate, it was determined that the program had exceeded the cost by greater than 25 percent of the total life program cost as estimated in the original estimate (MAR, December 2013).

In a subsequent update to program leadership, the Critical Change Team Lead reported that DOT&E findings of “not operationally suitable” and “not operationally effective” ratings would not be resolved in time to support a March 1, 2014 System Design and Development.²⁶ In addition to the suitability and effectiveness ratings, the DOT&E Memorandum on PKI Increment 2 FOT&E I and II,²⁷ dated May 10, 2013, identifies logistics shortfalls and missing Inventory Logistics System (ILS) functionality, as well as poor configuration management and token reliability, as reasons for their findings.

In the sections below, we discuss each of these topics.

A. Logistics Shortfalls and Missing ILS Functionality

The logistics shortfalls identified in the DOT&E report involve aspects of distribution, tracking, and general management of the SIPRNet Token. DOT&E reports:

The ILS was not designed to address logistics shortfalls identified in the IOT&E including token failure tracking and token statistics reporting, such as reporting of token issuance numbers by geographic region and Service affiliation...and does not provide necessary functions such as the ability to ship between issuance sites and the ability to terminate bad tokens in a stack.²⁸

²⁶ Critical Change Team Lead, “PKI Critical Change Executive Leadership Update” (December 18, 2013), 3.

²⁷ Public Key Infrastructure (PKI) Capability Increment 2 Follow-on Test and Evaluation (FOT&E) I and II Report. Memorandum (May 10, 2013).

²⁸ 10 May 2013 OT&E Memo on PKI Increment 2 FOT&E (conducted by JITC).

The PMO started discussions with DMDC to develop a centralized inventory management system in February 2011. These discussions led to DMDC taking on development of the SIPRNet ILS. DOT&E's unsuitable rating, prompted by its evaluation of the "interim" logistics management system, confirmed this need following IOT&E in September 2011.

In February 2012, DMDC demonstrated the ILS to the S/As in a developmental environment, and in June it was made available for use.²⁹ Unfortunately, requirements for the ILS were put on contract without adequate S/A or systems engineering (SE) participation, and user needs that could have been captured prior to or during development were not.³⁰

The ILS developed by DMDC covered token shipments to distribution locations but lacked the capability to track tokens to the individual user level and did not track data needed to calculate reliability.³¹ The PMO and the users missed the opportunity to incorporate the users' requirements for tracking tokens to the individual users in the DMDC-developed ILS. (For the purpose of this study PMO includes both program management and SE functions.) Both the users and systems engineers could have been more assertive in the requirements decomposition process on this issue.

Before the development and delivery of the ILS, DOT&E evaluated the S/A methods for managing tokens during IOT&E. Named the "interim" logistics process, these S/A methods included functionality for token delivery to distribution sites and token issuance, return, and reissuance of reusable tokens to individuals. The S/A interim process varied by Service and location. Often, S/A processes involved tracking tokens via manually entered spreadsheets. DOT&E approved the S/A methods to support the initial distribution of 85,000 tokens for IOT&E as a temporary measure, but noted that additional testing was needed to assess the scalability and suitability of the DMDC's logistics solution.³² Because the ILS was designed only to cover token shipments to distribution sites, the manually intensive process for token tracking persisted into FOT&E and was evaluated along with the DMDC-developed ILS. Neither the S/A issuance

²⁹ DAES Assessment, Aug 2012.

³⁰ J. Michael Gilmore, *Public Key Infrastructure (PKI) Capability Increment 2 Follow-on Test and Evaluation (FOT&E) I and II Report*. Memorandum (May 10, 2013). DOT&E reports that "user prioritized requirements, based on mission need, were not developed adequately" for the ILS. Furthermore DOT&E instructs that "[t]he users need to provide feedback into capability design, development, test, and deployment."

³¹ The requirement for tracking tokens through the ILS and the Token Management System (TMS) is complex because the two systems are separate and on separate networks. The ability to synchronize the information as tokens transition between various states was not only a technical challenge but a procedural challenge as well. The processes to employ the two-headed tracking system added manually intensive steps to an already over-burdened and undermanned workforce.

³² DOT&E Annual Report. *Public Key Infrastructure (PKI) Increment 2* (2011).

processes nor the ILS enabled automated tracking of token failure and statistics reporting. Shortfalls in both the interim logistics process and the ILS raised concerns that the system would not scale up to enable token management for the full population of 500,000 SIPRNet users.

The problems with ILS and interim logistics processes discussed above relate to shortcomings in defining the user requirements and the subsequent requirements decomposition process.

B. Configuration Management

In its FOT&E report, DOT&E found that configuration management had degraded since IOT&E and provided the following observations:

- Introduction of the capability to blacklist tokens and Auto-key recovery also introduced new software problems.
- New requirements are not clearly traced to original approved requirements documents.
- Lack of a process for inserting adequately tested, user-prioritized capabilities and fixes into the field.
- Documentation on ILS procedures was found inadequate.
- Software updates do not track deficiency reports.
- Change requests do not track to fixes or enhancements.
- Users are not notified of planned or unplanned outages and were not provided the assistance necessary to identify the root cause of outages or system degradation.

These configuration management issues delayed FOT&E from October 2012 to January 2013 (three months) due to unplanned outages. At FOT&E, configuration management issues became evident with the introduction of new Spiral 3 capabilities that degraded the performance of existing capabilities.

These events suggest that the PMO and SE did not establish and maintain an adequate configuration management process. Whether inadequate configuration management contributed to the critical change is another question. In total, the delays to FOT&E from October 2012 to January 2013 resulting directly from poor configuration management amounted to three months. As of the time of this writing in September 2014, the program has not achieved FDD six months after the Critical Change threshold and is not expected to do so in the near future. This suggests that even using the maximum estimate of schedule delays from configuration management difficulties, the Critical Change still would likely have occurred.

C. Token Reliability Issues

The DOT&E FOT&E report discusses two token reliability problems. The first is a direct problem with the reliability of the tokens and the second concerns shortfalls in the way the system tracks data that would permit accurate calculation of the reliability of the tokens and the disposition of the shortfalls.

Reliability issues with the SIPRNet token surfaced during the OA in June 2010. The DAES Assessment in August of that year describes the problem:

NII/Acquisition rating reflects quality control concerns reported by the Operational Test Agency (OTA) in their August 2010 report and from discussions with a user regarding problems they encountered in both formatting and failures after issuance. The OTA recommended a retest to verify resolution of the quality control issues before the procurement decision for 50,000 SIPRNet PKI items. While the failure rate was approximately 10 percent...³³

Token reliability has been a recurring problem throughout the history of PKI Increment 2. In the 2010 OA, the token experienced failure rates approaching 10 percent. By February 2011, the reliability issue was thought to be resolved when the SIPRNet tokens successfully completed an accelerated life-cycle test. In the DAES Assessments, DOT&E wrote “The SIPRNet tokens successfully completed the accelerated life-cycle testing. These results provide confidence the reliability issues that occurred during the Operational Assessment last summer will not be repeated during the IOT&E.”³⁴ Subsequently, the PKI Increment 2 program proceeded through IOT&E without encountering significant reliability problems.

Token reliability reemerged as a problem during FOT&E but the problem reported was with the tracking of reliability data, not the demonstrated reliability of the tokens. DOT&E reported that “token reliability is not accurately tracked or reported and does not reflect user reports of growing failure rates in the field (as much as 15 percent).”³⁵

By various accounts, token reliability continued to deteriorate after declaration of the Critical Change. In a February 2014 DAES Assessment, Assistant Secretary of Defense for Acquisition/Command, Control, and Communication, Cyber, and Business Systems (ASD(A)/C3CB)³⁶ reported “In Afghanistan, there are reports that numerous

³³ DAES Assessments, August 2010.

³⁴ DAES Assessments, February 2011.

³⁵ Gilmore, *Public Key Infrastructure (PKI) Capability Increment 2*.

³⁶ The office of C3CB provides the leadership for functional and acquisition oversight of all critical warfighting communications, command and control, and cyberspace capabilities in DoD. Additionally, the office performs the responsibilities of the Principal Staff Assistant for non-intelligence space systems supporting DoD leadership.

locations have lost SIPR access due to PKI token reliability issue. Individuals at camps are forced to travel to a location to get a new tokens [sic]. In [Jordan] there has been up to a 50 percent rate of failure of SIPRNet tokens. SOUTHCOM reports a 30 percent rate of failure.”

While token reliability may be a persistent problem, we do not believe it contributed considerably to the schedule slip in particular or the Critical Change in general. Indeed, token reliability (as opposed to token reliability tracking) reemerged as a problem only after the program declared a Critical Change in October 2013. However, the shortcomings in requirements definition for token management (and the ILS) continue to exacerbate tracking of the data needed to calculate token reliability accurately. This is a failure to manage requirements, specifically a failure to incorporate the requirements for tracking token reliability data. The Increment 2 Addendum to the CDD does not provide reliability or operational availability requirements that would drive development of a system capable of providing the statistics from operational data.

D. Priority toward Token Issuance

It has been suggested that the priority given to token issuance versus other activities channeled resources away from the infrastructure components of PKI Increment 2. However, the facts of the case do not support this as a contributor to the Critical Change schedule delay.

Figure 4 shows, for Spiral 1, the Integration of Infrastructure Components and Token Issuance were planned to be complete by March 2013.³⁷

³⁷ Schedule from the SEP and Acquisition Strategy (AS) (c. 2009).

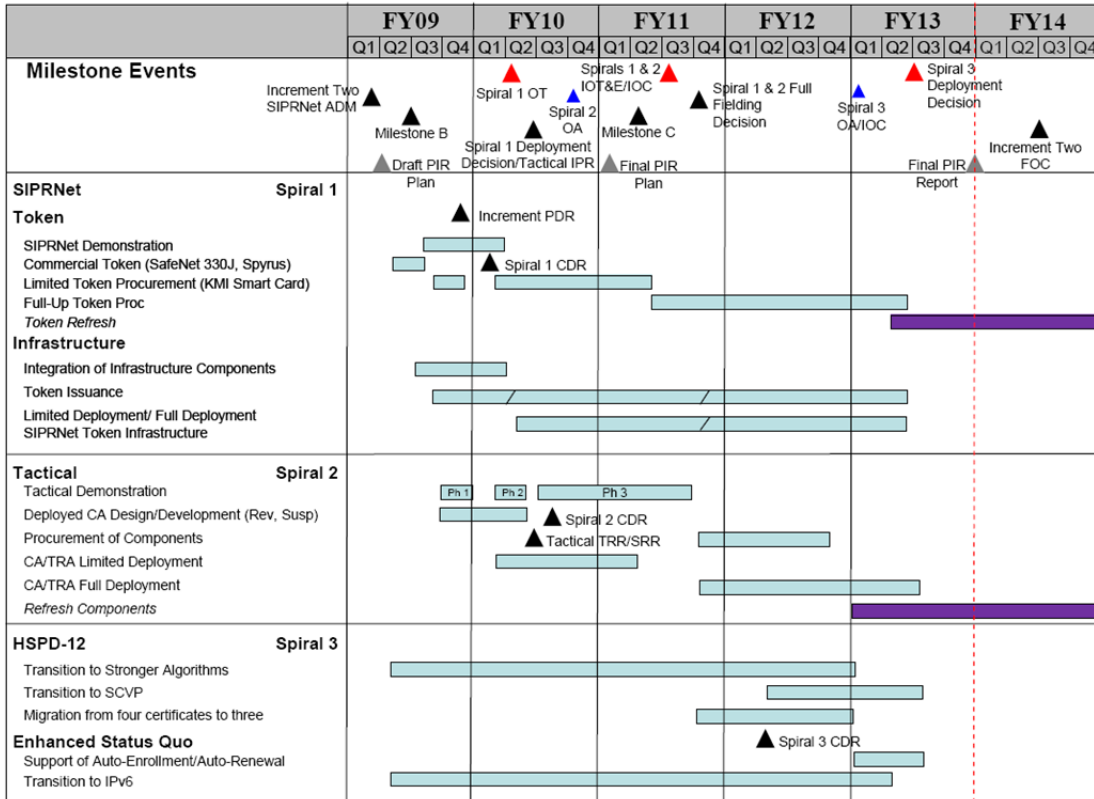


Figure 4. Integrated Program Schedule (2009)

The October 4, 2011 mandate from the DoD CIO accelerated the completion date for the issuance of SIPRNet tokens by only three months (December 31, 2012) compared to the plan. This minor acceleration should not have had a meaningful impact on other ongoing program activities, such as the development of the ILS or changes to baseline configurations. Indeed, even if other activities were deferred by an offsetting three months, the program still would have incurred a Critical Change by the date of this writing.

However, priority toward token issuance may have interfered with the schedule of major programmatic events. We infer that the program proceeded with operational testing before it was ready because of the pressures of meeting the issuance mandate. This rush to test resulted in requirements not met, capabilities not tested, and deferral of requirements to later spirals and increments. Conducting IOT&E with the “interim” logistics system, rather than the to-be-developed ILS, also marked a missed opportunity to diagnose the insufficiency of the ILS in addressing user requirements.

E. Failing to Meet the Requirements

Figure 5 shows the outcome of FOT&E by Measures of Effectiveness (MOE) and Measures of Suitability (MOS) ratings from IOT&E and FOT&E I and II.

		COI	IOT&E	FOT&E I and II
Effectiveness	COI 2 Validation		MOEs 2.1. Certificate validation on the SIPRNet	MOE 2.1. Blacklisting capability upgrade
			MOE 2.2. Austere SIPRNet environment support	MOE 2.2. Not Tested (per Test Plan)
	COI 4 Recover/Restore/Reset		MOE 4.1. Key recovery, restoration, and PIN reset on the SIPRNet	MOE 4.1. Auto-Key Recovery capability upgrade
			MOE 4.2. Austere SIPRNET environment support	MOE 4.2. Not Tested (per Test Plan)
	COI 6 Interoperate		MOE 6.1. Must interoperate with required DoD and non-DOD operational networks	MOE 6.1. Interface between TMS and ILS
	Suitability	COI 7 Usability		MOS 7.1. Training
			MOS 7.2. Documentation	MOS 7.2. Documentation for ILS and TMS Updates
			MOS 7.1. Help Desk	MOS 7.3. ILS and TMS Help Desk
			N/A	MOS 7.4. ILS for token management
COI 8 Sustainability			MOS 8.1. System Reliability	MOS 8.1. System Reliability
			MOS 8.2. Token Reliability	MOS 8.2. Token Reliability
			MOS 8.3. System Availability	MOS 8.3. System Availability
			MOS 8.4. System Maintainability	MOS 8.4. System Maintainability
			MOS 8.5	MOS 8.5. Scalability. PKI will accommodate an increasing number of users.
		MOS 8.1	MOS 8.7. Token distribution process	
Security	COI 9 Information Assurance		MOEs 9.1 – 9.4: Protect, Detect, React, Restore	Not Tested (per Test Plan)

Figure 5. DOT&E Comparison of IOT&E and FOT&E Results

The DOT&E FOT&E I and II results shown in Figure 5 indicate the following:

- The Blacklisting capability upgrade did not meet its MOE. Blacklisting is a Spiral 3 capability allowing RAs and Local Registration Authorities (LRAs) to identify tokens that are either lost or damaged and therefore cannot be reissued. Apparently, the modification to blacklist tokens kept not only those tokens that were reported lost or damaged from being reformatted but other tokens that were returned for reuse. On this topic, DOT&E reported:

The capability to allow blacklisting of tokens that should not be allowed reentry into the token management system resulted in field operators being unable to reformat valid tokens returned for reuse, lengthening the process to reissue expiring tokens by requiring RA intervention in the existing process.... All 23 tokens that were blacklisted failed to reformat through Token Management System (TMS), as expected. However, an unintended consequence was that LRAs and TAs could not reformat valid cards returned for reuse. The consequence was discovered through day-to-day real-world operations during the test, but it should have been

discovered through more rigorous developmental testing that verifies all functions continue to work for all user roles.³⁸

- Failure to meet MOSs occurred in the capabilities for ILS and TMS update training, ILS for token management, System Reliability, Token Reliability, System Availability, System Maintainability, and the token distribution process. The token distribution process has already been discussed with respect to the ILS. Reliability was also previously discussed and not identified as a likely root cause of the Critical Change.
- Several MOEs were not tested according to plan, and Critical Operation Issue (COI) 9 Information Assurance was not tested.
- System monitoring, automated failover (backup), and load-balancing capabilities were supposed to be added before Full Deployment.³⁹ Today, system health and monitoring, upgrades to automated failover, and load balancing are still issues. The PKI Critical Change Executive Leadership Update of December 18, 2013 reports that “COOP failover works but global load balancing is still in development” and that “System Health and Monitoring” is being developed and deployed by DISA independent of the acquisition development program.

All of these testing shortfalls contributed to DOT&E’s rating of operationally ineffective and unsuitable. However, each of these shortfalls was itself the product of another underlying cause. For example, blacklisting failures relate to deficient configuration management; ILS, token distribution, and reliability shortcomings stem from a flawed requirements development process for logistics; and deferrals of system monitoring, failover, and load-balancing stem from an unachievable program definition at MS B (discussed in Section 8.B).

F. Deferral of Requirements

As the program sought approval for Spiral 3 IOC and Full Operational Capability (FOC) (in May 2011), three non-Key Performance Parameter (KPP) attributes were identified for deferment to a future increment of the DoD PKI program (if a future increment is approved via the acquisition process). These are:

- Certificate Authority (CA) Services (from Spiral 2)
- Alternative Token Form Factors
- Tactical Registration Authority (TRA) (from Spiral 2)

³⁸ Public Key Infrastructure (PKI) Capability Increment 2 FOT&E I and II Report.

³⁹ The DOT&E FOT&E.

The IPMSCG subsequently approved the removal of the following capabilities and their associated thresholds from the DoD PKI Increment 2 CDD on July 25, 2013:⁴⁰

- Transition to Internet Protocol version 6 (IPv6) (from Spiral 3)
- Server-based Certificate Validation Protocol (SCVP) (from Spiral 3)
- Deployable Certification Authorities (from Spiral 2)
- Synchronization of Disconnected PKI Nodes
- Tactical Registration Authority (from Spiral 2)
- Tactical Certificate Revocation Information (from Spiral 2)

In addition, prior to the Critical Change, the PMO petitioned the IPMSCG to defer delivery of NPE (from Spiral 3)⁴¹ and Non-secure Internet Protocol Router Network (NIPRNet) Enterprise Alternative Token System (NEATS) past FDD.⁴²

The substantial amount of program content deferred or removed suggests an unrealistic initial program baseline that was never achievable within the five-year MAIS timeframe. Had requirements not been deferred or removed, the Critical Change might have been declared earlier, as the PMO may have had to acknowledge its inability to deliver the deferred content within the five years.⁴³

G. WSARA 2009 Root Cause Categories

Table 2 maps to the WSARA root cause categories the possible reasons we considered for schedule delays that caused the critical change. Chapter 8 provides the analysis for our root cause findings.

⁴⁰ Critical Change Executive Leadership Update, December 18, 2013.

⁴¹ The NPE capability is for the Auto-enrollment and Auto-renewal of PKI certificates for NPEs. NPE was initially an Increment 1 Spiral 3 requirement. A non-automated rudimentary capability for NPE was made available during PKI Increment 1, but the more robust and automated capability was deferred to Increment 2, Spiral 3. Because of a Microsoft Windows Server trust issue, NPE certificates for workstations were removed from the Increment 2, Spiral 3 requirement in July 2012. In October of the same year, the DoD CIO reintroduced the requirement, and in January 2013, the program's security policy was changed from "medium assurance" to "less than medium assurance" to accommodate user demands.

⁴² DAES Assessment, August 2013.

⁴³ "The DASD C3 & Cyber has also raised concerns with the schedule since the program's strategy is to request a Full Deployment Decision in April 2013 (after Spiral 2) and then deliver the content of Spiral 3 via a series of pre-planned productive improvements (P3I) that would not warrant MDA decision review. A program breach and congressional thresholds for a Significant Change would be triggered if Spiral 3 required an MDA review instead of the fielding via P3Is." From DAES Review, October 2012.

Working our way across the columns of Table 2:

1. Logistics shortfalls and ILS functionality could be a result of technical issues. However, the S/A opted for a decentralized model in which each Component would manage their own SIPRNet token registration and distribution. There is sufficient evidence to consider that the decentralized model is the problem, and the technical issues encountered are the consequences of the model. There is also sufficient evidence to consider poor performance of government personnel as a root cause.
2. We allocate configuration management to the poor performance of government personnel.
3. The token reliability problems could be rooted in unanticipated technical issues, but reliability is almost always an issue and should not be unanticipated. In addition, poor reliability of a commercial item can be avoided with a contract that ties payment to the results of acceptance testing. There is also sufficient evidence to consider poor performance of government personnel as a root cause.
4. and 5. We consider unanticipated design, engineering, manufacturing, or technical issues and performance of government personnel as root causes for both failing to meet requirements and deferral of requirements.

Table 2. Alignment with WSARA Root Cause Categories

WSARA Root Cause Categories	Logistics Shortfalls and ILS Functionality	Configuration Management	Token Reliability/ Not Tracked	Failing to Meet Requirements	Deferral of Requirements
Unrealistic estimates for cost or schedule	-	-	-	Maybe	Maybe
Immature technology, excessive manufacturing, integration risk	-	-	-	-	-
Unrealistic performance Expectations	-	-	-	-	-
Changes in Procurement Quantity	-	-	-	-	-
Inadequate funding/funding instability	-	-	-	-	-
Unanticipated design, engineering, manufacturing or technical issues	Maybe	-	Yes for token reliability	Yes	Yes, NPE
Poor performance of Government or contract personnel	Yes	Yes	Yes for not tracked	Yes	Yes

8. Root Cause Analysis

The primary proximate cause of the Critical Change is the inability to resolve the unsuitability ratings from IOT&E and FOT&E. The absence of a centralized logistics process during IOT&E and the inadequacy of the DMDC's ILS at FOT&E are the leading causes of this shortfall. It appears that, from the beginning of the program, neither the S/As, the PMO (including program management and SE), the PEO DoD CIO, nor the IPMSCG understood the scope of the work that needed to be done to track and manage the SIPRNet tokens. This lack of understanding led to S/A-specific ad hoc development of manually intensive logistics processes. Even when this S/A-specific process was recognized as inadequate, the PMO, S/As, and DoD CIO did not take the necessary steps to communicate the requirements for and develop a suitable centralized logistics system. This allowed logistics problems to persist past FOT&E, ultimately prompting the Critical Change.

A. Lack of Understanding of the Logistics Support Requirement

Logistics requirements development issues have their roots embedded early in the program. Evidence from the Material Availability KPP and the CDD Addendum for Increment 2 is presented below.

1. The Material Availability KPP is about services for and tracking of certificates. It does not mention tokens or tracking tokens.

The DoD PKI shall be available 24/7 to provide all services to both strategic and bandwidth constrained (i.e., tactical environment) users with no single points of failure. PKI operational availability is defined as the time that PKI is prepared to:

- a. Respond to requests to register subscribers;
- b. Generate new, modified or re-keyed certificates;
- c. Process revocation requests;
- d. Generate Certification Revocation Lists (CRLs);
- e. Provide certificate status checking; and
- f. Respond to key recovery requests.

PKI shall provide an automated ability to archive and retrieve PKI-generated security objects on demand. Assured management of PKI-generated security objects that are automatically archived and recoverable on demand to prove subscriber's recognition of compliance to policies and validity of PKI enabled transactions.

2. The capability statement in the CDD Addendum for Increment 2, approved January 25, 2011, supports the initial PMO and S/A position that only the issuance of the token needed to be centralized.

The ability to provide enhanced PKI services (e.g., stronger algorithms, etc.), bring[s] flexibility to defensive capabilities supporting all environments (national, strategic, operational, and Tactical), and maintain PKI services in degraded operations in protecting the GIG [global information grid], similar to weapon systems.

- Centralize Visibility/Trust with decentralized management
- Identify and implement hardware token based PKI on the SIPRNet using a centralized issuance system
- Issue a hardware token for use on SIPRNet
- Migrate to stronger algorithms by Dec 2010

3. The Increment 2 Addendum further identifies a sufficiently vague requirement for “Centralized Trust for Token Management System (TMS) for issuing and managing Alternate Tokens.” The requirement identifies the existence of a centralized token issuance and management system but is only explicit that the TMS must track certificates placed in the hardware token.

The Alternate Token shall be issued and managed by a centralized issuance and token management system. The TMS shall only issue and manage hardware tokens that are registered to and valid in the TMS. The TMS must track or record each certificate issued on a hardware token. Certificates issued on the Alternate Token shall include the appropriate hardware policy OIDs allowable by the DoD Certificate Policy.

These baseline requirements suggest some role for logistics management in the issuance and tracking of tokens but do not even hint at the scope of work. Furthermore, as implemented, the TMS did track certificates but did not contribute much to the management of tokens. It is interesting to note that the functions for tracking the token are now within the ILS not the TMS.

From these requirements, the PMO determined that the S/As would take responsibility for token distribution and management. The S/As executed this responsibility by developing Service-specific systems for distributing and managing token inventories. Many of these systems involved manually populated spreadsheets that proved difficult to reconcile across S/As.

As experience in the field accumulated, both the S/As and the PMO realized there were requirements for token management that had been overlooked. The PMO acknowledged these deficiencies when it began discussions with DMDC for a centralized logistics capability in February 2011. DOT&E’s unsuitable rating from IOT&E further

confirmed the need for a long-term, scalable, and centralized solution to logistics management.

The PMO and the S/As, however, held different views about the design of that TMS. The PMO realized the need for central management of the tokens but maintained the position that central management needed only cover distribution of the tokens to their initial distribution site. The S/As realized that the spreadsheet processes they developed were manually intensive and would not scale up to full operations. For the S/As, a centralized system would need the capability to track tokens to the individual user level to sufficiently replace the management capabilities that their interim processes already delivered.

The IDA team found no evidence that the PMO consulted with the S/As or that the S/As articulated their functional needs for a centralized TMS before the ILS design was finalized.

The fact that the eventual DMDC ILS solution did not include the S/A requirements for token management at the user level allowed this problem to continue through FOT&E.

The PMO, S/As, IPMSCG, and SAE could have known and acted earlier, but they did not. In a meeting with the PEO and NSA, PARCA and IDA representatives were told that the PMO did not use their experience on PKI Increment 1 as an analogy because the PMO did not think it applied. IDA disagrees with the idea that Increment 1 as an analogy does not apply. An analysis of the content of PKI Increment 1 as it relates to Increment 2 could have provided valuable insight into the scope of the Increment 2 Spiral 1 development activity. PKI Increment 1 improvements were fielded on the NIPRNet with the preexisting Common Access Card (CAC) system, which relied on DMDC's RAPIDS⁴⁴ infrastructure for CAC issuance and management. Accordingly, DMDC covered the end-to-end logistics process for the CAC,⁴⁵ to which Increment 1 added NIPRNet PKI capability enhancements. Neither the procurement of the CAC nor the end-to-end logistics were part of Increment 1 because the CAC and its logistics system already existed. Had the PKI PMO, S/As, and IPMSCG spent time with PKI Increment 1 as an analogy they might have realized they needed a SIPRNet equivalent of the CAC system and a SIPRNet equivalent of RAPIDS as the infrastructure upon which to field the Increment 2 PKI token on the SIPRNet. Furthermore, because the SIPRNet token was

⁴⁴ DEERS is the primary personnel database for the DoD. DEERS and RAPIDS are operational programs in support of resources/benefits management, critical defense missions, the Uniformed Services Identification Card program, and awareness regarding benefits to which Uniformed Services personnel and their family members are entitled.

⁴⁵ DMDC handles CAC supply and distribution inventory management through the preexisting RAPIDS infrastructure for CAC issuance.

reusable, Increment 2 had functionality not paralleled in Increment 1 that required greater attention to end-to-end token management. In essence, all of Spiral 1 of Increment 2 was new, and the decomposition of the requirements to the individual user level and the building of the system that met those requirements were an added development activity for which there was no comparable experience on Increment 1. The limited number of users for Increment 2 on SIPRNet compared to Increment 1 on NIPRNet may have mitigated the size of the effort, but did not imply that additional development work on end-to-end logistics was unnecessary.

The initial interpretation for distributed token management provided a false start for the program. The failure of the users, the PMO, and acquisition oversight to come to consensus on logistics management once the need for a centralized system was recognized during the development of the ILS allowed this shortcoming to persist. If one begins counting at the Preliminary Design Review (PDR) in July 2009 and ends when DMDC demonstrated the ILS in the development environment for the S/As in February 2012, the program went an estimated two and a half years without an enterprise logistics process.

By itself, the lack of understanding of the requirements to track and manage the tokens could be the sole cause for the Critical Change and the inability of the PKI Increment 2 program to achieve FDD within five years. But that is not the end of the story. The Critical Change did not include cost growth realized by not meeting and deferring a substantial number of capabilities.

B. Faulty Baseline

During execution of the PKI Increment 2 program the PMO, PEO, S/As, and IPMSCG could have more accurately anticipated or promptly mitigated the issues that led to the schedule delays, but there is sufficient evidence to say the Increment 2 program began with a faulty baseline.

In June 2008, the PKI PMO conducted an Economic Analysis (EA). The purpose of the EA was to examine the costs, benefits, schedule, and risks associated with the preferred alternative identified in the DoD PKI Increment Two Analysis of Alternatives (AoA).

Evidence suggests the magnitude of the development effort (as described in the preferred alternative of the EA) associated with Increment 2 was not adequately assessed at inception. The bar chart in Figure 6 shows funding for Increments 1 and 2. Development funding for both increments are roughly equivalent. Procurement funding for Increment 2 is greater than for Increment 1 because Increment 2 purchased the tokens and the bulk formatters, while Increment 1 used existing resources (the CAC).

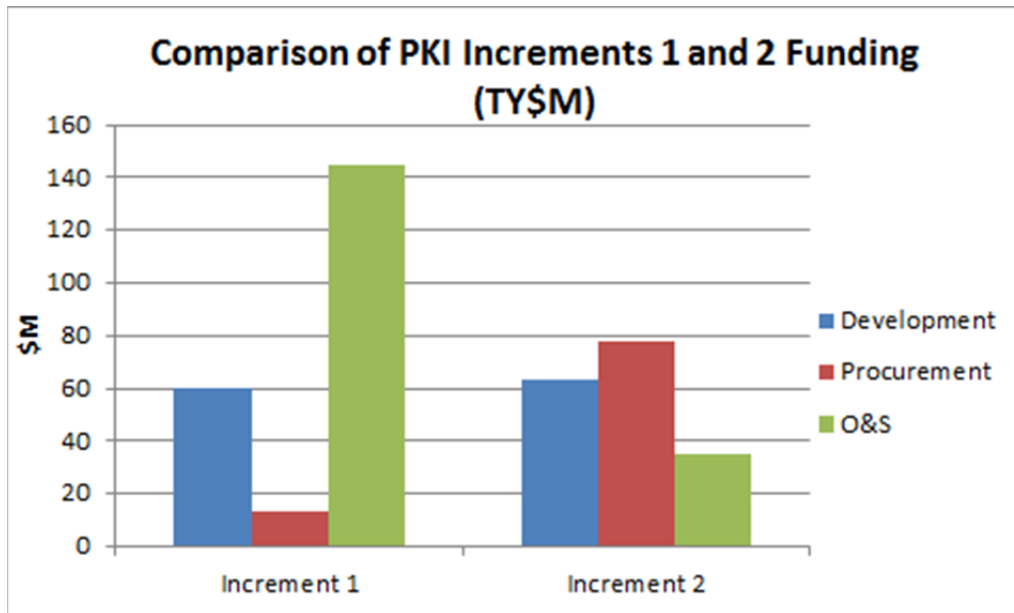


Figure 6. Funding for PKI Increment 1 and PKI Increment 2

Despite the equal development funding and schedule resources provided to the two Increments, Increment 2 was responsible for a vastly more ambitious set of capabilities. Whereas Increment 1 implemented a series of improvements to preexisting PKI capabilities on NIPRNet, Increment 2 was responsible for developing new PKI capabilities on SIPRNet, in Tactical environments, and for NPE users. Furthermore, whereas Increment 1 relied on the preexisting CAC token and its RAPIDS issuance and management infrastructure, Increment 2 had to develop new tokens (at least three, if one counts the since-deferred alternative Tactical and NEATS NIPRNet tokens) and an integrated system for distributing and managing those tokens and their certificates. Finally, the different operational concepts for Increment 1 (NIPRNet) and Increment 2 (SIPRNet and tactical) demanded greater security and functionality (i.e., reuse capabilities) for Increment 2 than for Increment 1. Accordingly, allocating the same time and resources to Increment 2 as Increment 1 may have been inappropriate from the beginning.

In the Root Cause Narrative section, we identified requirements that were not met in FOT&E and capabilities originally assigned to Increment 2 that were deferred to a later increment. Both lists are substantial, and, we assert, are additional evidence that the Increment 2 capabilities were not understood well enough to be resourced properly at inception.

C. Oversight

The IDA research team found substantial evidence of ineffective oversight.

Despite known logistics shortfalls and deficient centralized management infrastructure, the Increment 2 program was permitted to proceed past MS C in February 2011. The program was then allowed to enter IOT&E with an “interim” logistics process in November 2011—before DMDC began developing what would become the ILS.

Even once stakeholders realized that DMDC’s ILS development efforts were underway, oversight entities like the IPMSCG or the NSA SAE did not create an environment in which users and the PMO were kept aware of each other’s development plans and functional requirements, inhibiting the development of capabilities needed in the ILS. According to an AT&L team assessing the Critical Change, the IPMSCG did not serve as a forum to adjudicate/clarify/prioritize requirements or serve as the ultimate escalation path for requirements issues.⁴⁶

The DoD CIO, on behalf of the IPMSCG, approved the use of the CDD with the Increment 2 Addendum in place of a Capabilities Production Document (CPD) for the MS C decision. The Increment 2 Addendum does not approach the level of detail provided in most CPDs. Several of the people we talked to (particularly from DOT&E and Developmental Test and Evaluation (DT&E)) thought this represented a missed opportunity for doing a functional requirements analysis with S/A participants. Had the program been required to submit a CPD, it might have put more work into flowing down requirements for logistics up front, avoiding some of the problems that would arise later. Alternatively, a deficient CPD (had one been required) could have given acquisition oversight or the users another opportunity to catch the underlying requirements development issues that the program was experiencing.

PKI Increment 2 did not have a DAES review until October 2012, even though DOT&E, AT&L/SE, and other organizations provided detailed comments about significant problems causing schedule delays that started in 2010.

The DoD CIO and NSA SAE let the program proceed without a timely Test and Evaluation Master Plan (TEMP) Addendum to support OT&E for Spiral 3. DOT&E wrote a memorandum to the DoD CIO and NSA SAE on April 19, 2013 expressing concern that the PKI PMO had not yet provided an Increment 2 TEMP Addendum for Spiral 3 as agreed, even though OT&E for Spiral 3 was scheduled in FY 2013.

The Functional Capabilities Board (FCB) did not ensure that PKI Increment 2 capabilities were conceived and developed in the joint warfighting context. The FCB, chartered by the Joint Requirements Oversight Council (JROC), is the lead coordinating body to ensure that the joint force is best served throughout the Joint Capabilities Integration & Development System (JCIDS) and acquisition processes. The JCIDS process encourages early and continuous collaboration between the warfighter and

⁴⁶ PKI Critical Change Review (CCR) R4 mid Term Briefing, December 17, 2013.

acquisition communities to ensure that new capabilities are conceived and developed in the joint warfighting context. This did not happen on PKI Increment 2 with regard to logistics shortfalls and ILS functionality.

9. Conclusions

IDA concludes that the root cause of the Critical Change for the PKI Increment 2 program is the lack of understanding, from the beginning of the program, of the scope of the work that needed to be done to track and manage the SIPRNet tokens. This is supported most prominently by the failure to adequately decompose functional requirements for a logistics management system and the subsequent neglect to reach consensus between the PMO, S/As, and oversight organizations on the design of the ILS. We attribute this lack of understanding to poor performance by government personnel. From the beginning the PMO, PEO, and IPMSCG should have understood the scope of the requirement, but apparently did not. Subsequently the PMO, PEO, and IPMSCG did not find and fix the problem in a timely fashion. The PM and SE organizations are responsible for extracting validated testable requirements from users; for token management, this was not done. The users should have had a more active role in decomposing the requirements; they should have spoken up, but apparently did not.

There are two mitigating factors to the finding of poor performance on the part of the PMO, PEO, IPMSCG, and S/As.

First, the ASD(NII) at the time, now the DoD CIO, made NSA the material developer. NSA predominantly acquires goods and services. In our opinion, they were not the correct organization to be PMO for PKI Increment 2, which had development and enterprise characteristics.

Second, it is difficult to decide if our finding for a Faulty Baseline is an inception issue or an execution issue. The *Defense Acquisition Guidebook* states that an MAIS should be structured so that each increment can achieve FDD within five years from the MS A decision, or, if there was no MS A decision, the date when the preferred alternative was selected and approved by the MDA.

It is not clear if the content of Increment 2 was decided in June 2008 with the EA or when the DoD PKI Increment 2 Addendum Version 2 was signed in January 2011. In any event, unrealistic schedule and performance expectations existed, based on a lack of understanding of scope at inception and seriously exacerbated by poor management during execution.

We believe that the MAIS process itself is a contributor to this Critical Change. We do not believe the best resource planning can be accomplished in an environment in which the user decides the content of a program that has a fixed five-year development

cycle. For this strategy to succeed, the user must develop and maintain a resource-loaded schedule for every item on its list of priorities. Each item must be described well enough to demonstrate that the requirements are understood, and each item must have a cost estimate based on those requirements. We did not find evidence of well-documented resource-loaded schedules in the documentation we examined (including the Acquisition Strategy, SEP, or Life Cycle Cost Estimate Summary) for the PKI effort.

Appendix A.

DoD CIO Issuance Mandate October 14, 2011

Figure A-1 is a screen shot of the October 14, 2011 DoD CIO Issuance Mandate memorandum.

DOT&E



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

OCT 14 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD SIPRNet Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNet Applications and Web Servers

Reference: DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011

The Department of Defense (DoD) must eliminate user anonymity on the SIPRNet and other interconnected classified networks. Access control, responsible sharing and safeguarding of classified information must be enforced. Strong accountability for information access is key to deterring unauthorized activity by malicious insiders.

Per reference, the Department will be issuing a PKI cyber identity on a hardware token to every DoD SIPRNet user and require the use of this credential to access SIPRNet-based information. DoD Components should begin to use the hardware token for cryptographic logon and access to applications and information on the SIPRNet beginning with its issuance, and in accordance with the timeline stated below. DoD Components should upon receipt of this memorandum:

- Continue to issue the DoD SIPRNet PKI hardware token to their users, and complete the issuance to all users by December 31, 2012.
- Continue to configure user accounts on secret networks to support cryptographic logon using the PKI hardware token, and complete configurations no later than March 31, 2013.
- Implement user cryptographic network logon with PKI hardware tokens on SIPRNet accounts as they are configured, with all users required to log in using tokens by April 1, 2013.

- Public Key enable all SIPRNet applications and web servers to support cryptographic authentication, and complete Public Key enablement by June 29, 2013.
- Implement Public Key enablement (cryptographic authentication) of all SIPRNet applications and web servers as they are enabled, with all access requiring PKI credentials NLT June 30, 2013.

U.S. Cyber Command will establish a reporting process to track compliance and progress towards meeting the June 30, 2013 date, at which time all authentication to classified network accounts, and applications and web servers operating on the DoD SIPRNet shall require use of the SIPRNet PKI hardware token. Technical support can be obtained from the PKE Information Assurance Web site at <http://iase.disa.mil/pki-pke> or from pke_support@disa.mil. A SIPRNet presence of this support will be available later this year.

The DoD CIO point of contact is Mr. Tim Fong, timothy.fong@osd.mil or (703) 614-1991. The DISA lead for this effort is Ms. Patricia Janssen, trish.janssen@disa.mil or (301) 225-8740.



Teresa M. Takai

Figure A-1. October 14, 2011 DoD CIO Issuance Mandate Memorandum

Appendix B.

Full Fielding ADM Jan 2012

Figure B-1 is a screen shot of the January 20, 2012 DoD CIO PKI Increment 2 ADM.



DEPARTMENT OF DEFENSE
8000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-8000

JAN 20 2012

MEMORANDUM FOR THE SECRETARIES OF THE MILITARY SERVICES
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Public Key Infrastructure (PKI) Increment 2 Acquisition Decision
Memorandum (ADM) – Full Fielding to Secret Internet Protocol Router Network
(SIPRNet) and Tactical Environments

Purpose: A PKI Increment 2 Overarching Integrated Product Team (OIPT) was conducted on January 6, 2012; the objective was to review the readiness of whether the Department should deploy PKI to the SIPRNet and tactical environments involving the procurement of 856,499 tokens and associated card readers and software to support Services, Components, and Agencies implementation. The Program Manager (PM) is Ms. Denise Holmes; the Program Executive Officer is Mr. Charles Stein; and the Senior Acquisition Executive is Ms. Jennifer Walsmith.

Decisions:

- I approve full fielding of PKI to the SIPRNet and tactical environments.
- I approve the PM to acquire the necessary tokens, card readers, and software to support the full fielding requirements.


Tasking/Action Items:

- The National Security Agency shall:
 - Resolve and operationally retest the outstanding issues and test limitations that contributed to the "Unsuitable" rating identified by the Initial Operational Test and Evaluation. Accelerate the procurement of the bulk formatter with issuance capability and operationally test capability along with the end-to-end logistical process.
 - Address the outstanding risks associated with the fielding decision; the National Security Agency Senior Acquisition Executive shall conduct a review following the implementation of corrective actions and appropriate retesting.
 - Address the Program Protection Plan considerations by completing a criticality analysis to identify associated components (hardware, software, and firmware) requiring protection, identify vulnerabilities, analyze risks and develop a list of potential countermeasures, and provide the Deputy Assistant Secretary of Defense (System Engineering) draft results within 180 days from the date of this ADM.

- o In coordination with Deputy CIO for Identity and Information Assurance (DCIO (IIA)) and the Military Services, complete a Post Implementation Review Plan and perform baseline metrics collection. This plan shall be approved by the DCIO(IIA) within 120 days from the date of this ADM. The Post Implementation Review (PIR) shall be conducted in accordance with the PIR Plan and completed after the Increment 2 Initial Operational Capability.
- The Deputy CIO for Identity and Information Assurance shall:
 - o In concert with the DoD Components, implement a capability to track the implementation of PKI across the SIPRNet and tactical environments supporting DoD CIO guidance.

Discussion: On October 14, 2011, the DoD CIO issued guidance to eliminate user anonymity on the SIPRNet by requesting the issuance of PKI tokens across the SIPRNet environments be completed by December 31, 2012 and software applications and infrastructure be fully enabled with PKI capabilities by June 30, 2013. The readiness of PKI Increment 2 to support this objective was assessed in a six-month operational assessment involving 17,000 users that concluded in September 2011. Results of the test concluded the system was operationally effective. However, it also indicated the system was “Operationally Unsuitable” given the need for additional infrastructure enhancements and an enhanced Integrated Logistics System to support full deployment. The National Security Agency and the DoD Components have implemented an interim logistics support process and have taken action to mitigate the other risks to allow full fielding.

Points of Contact: Acquisition matters, Mr. Don Johnson at email: don.johnson@osd.mil, (703) 614-5839 or functional sponsor matters, Ms. Gail Lindsay at email: gail.lindsay@osd.mil, (703) 614-2137.


Teresa M. Takai

cc:
PKI OIPT Members

Figure B-1. January 20, 2012 DoD CIO PKI Increment 2 Memorandum

Illustrations

Figures

Figure 1. Department of Defense (DoD) PKI Program	5
Figure 2. DoD PKI Increment 2 Organizational Structure	8
Figure 3. Program Events Leading to Critical Change	15
Figure 4. Integrated Program Schedule (2009).....	24
Figure 5. DOT&E Comparison of IOT&E and FOT&E Results.....	25
Figure 6. Funding for PKI Increment 1 and PKI Increment 2	35

Tables

Table 1. Schedule Milestones	12
Table 2. Alignment with WSARA Root Cause Categories	29

References

- 2011 DOT&E Annual Report.
- Critical Change Executive Leadership Update (December 18, 2013).
- DAES Assessment (August 2012).
- DAES Assessment (August 2013).
- DAES Assessment by PM (November 2011).
- DAES Assessments (February 2011).
- DAES Assessments (February 2012).
- DoD PKI Program Management Office (PMO) Increment Two Systems Engineering Plan (SEP), Version 1.5, April 21, 2009.
- DOT&E AR (2013).
- Gilmore, J. Michael. "Public Key Infrastructure (PKI) Capability Increment 2 Follow-on Test and Evaluation (FOT&E) I and II Report." Memorandum, May 10, 2013.
- Increment 2 Capabilities Development Document (CDD) Addendum.
- MAR (Dec 2013).
- MAR for PKI Increment 2 (December 2013).
- McCaskey, Jason. "Department of Defense Public Key Infrastructure: Critical Change Executive Leadership," Update. (December 18, 2013).
- OT&E Memo on PKI Increment 2 FOT&E (conducted by JITC), May 10, 2013.
- PKI CCR R4 Mid Term Briefing (December 17, 2013).
- PKI Critical Change Executive Leadership Update 18. Critical Change Team Lead, (December 2013).
- Program Description for PKI Increment 2 from MAR (December 2013).
- Public Key Infrastructure (PKI) Increment 2. DOT&E Annual Report, 2011.
- Public Key Infrastructure Increment 1 Capability Development Document. January 25, 2006.
- Satyapal, Shanti. "PKI Increment 2 LCSP." Memorandum to Timothy Buennemeyer, DOT&E (July 6, 2012).
- Takai, Teresa. MAR December 2013, Public Key Infrastructure (PKI) Increment 2 Acquisition Decision Memorandum (ADM)—Full Fielding to Secret Internet Protocol Router Network (SIPRNet) Tactical Environment, Memorandum (January 20, 2012).

Weapon Systems Acquisition Reform Act, Pub. L. 111-23, 123 Stat. 1704 (2009).
§ 103(b)(1) and § 103(b)(2).

Abbreviations

ADM	Acquisition Decision Memorandum
AoA	Analysis of Alternatives
AS	Acquisition Strategy
ASD(A)	Assistant Secretary of Defense for Acquisition
ASD(NII)	Assistant Secretary of Defense, Networks & Information Integration
C3	Command, Control, and Communications
C3CB	Command, Control, Communications, Cyber, and Business Systems
C4	Command, Control, Communications, Computers
CA	Certificate Authority
CAC	Common Access Card
CC	Critical Change
CCR	Critical Change Review
CDD	Capabilities Development Document
CDR	Critical Design Review
CIO	Chief Information Officer
COI	Critical Operational Issue
CONOPS	Concept of Operations
COTS	Commercial Off the Shelf
CPD	Capabilities Production Document
CRL	Certification Revocation List
DAA	Designated Accrediting Authority
DAES	Defense Acquisition Executive Summary
DASD(IIA)	Deputy Assistant Secretary of Defense (Information and Identity Assurance)
DCA	Deployed Certificate Authority
DEERS	Defense Enrollment Eligibility Reporting System
DepSecDef	Deputy Secretary of Defense
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DODI	Department of Defense Instruction
DoN	Department of Navy
DOT&E	Director, Operational Test & Evaluation
DT&E	Developmental Test and Evaluation

EA	Economic Analysis
ECC	Elliptic Curve Cryptography
FBCA	Federal Bridge Certificate Authority
FCB	Functional Capabilities Board
FDD	Full Deployment Decision
FFD	Full Fielding Decision
FOC	Full Operational Capability
FOT&E	Follow-on Operational Test and Evaluation
GDS	Global Directory Service
GIG	Global Information Grid
GOTS	Government Off the Shelf
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IDA	Institute for Defense Analyses
IIA	Information and Identity Assurance
ILS	Inventory Logistics System
IOC	Initial Operational Capability
IOT&E	Initial Operational Test and Evaluation
IPMSCG	Identity Protection and Management Senior Coordinating Group
IPR	Integrated Program Review
IPv	Internet Protocol version
JCIDS	Joint Capabilities Integration & Development System
JITC	Joint Interoperability Test Command
JROC	Joint Requirements Oversight Council
KPP	Key Performance Parameter
LCSP	Life Cycle Support Plan
LRA	Local Registration Authority
M	Millions
MAIS	Major Automated Information System
MAR	MAIS Annual Report
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MOA	Memorandum of Agreement
MOE	Measure of Effectiveness
MOS	Measure of Suitability
MS	Microsoft
MS	Milestone
NEATS	NIPRNET Enterprise Alternative Token System
NII	Network & Information Integration
NIPRNet	Non-secure Internet Protocol Router Network
NLT	No Later Than

NPE	Non-Person Entity
NSA	National Security Agency
OA	Operational Assessment
OCSP	Online Certificate Status Protocol
OE	Original Estimate
OID	Object Identifier
OIPT	Overarching Integrated Product Team
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
P3I	Pre-Planned Productive Improvements
PARCA	Performance Assessments and Root Cause Analyses
PDR	Preliminary Design Review
PEO	Program Executive Office
PIR	Post Implementation Review
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Program Manager
PMA	Program Management Agreement
PMO	Program Management Office
RAPIDS	Real-Time Automated Personnel Identification System
RA	Registration Authority
RCA	Root Cause Analysis
RSA	Rivest, Shamir, and Adelman
S/A	Service/Agency
SAE	Senior Acquisition Executive
SCEP	Simplified Certificate Enrollment Protocol
SCVP	Server-based Certificate Validation Protocol
SE	Systems Engineering
SecDef	Secretary of Defense
SEP	Systems Engineering Plan
SHA	Secure Hash Algorithm
SIPRNet	Secure Internet Protocol Router Network
SOUTHCOM	United States Southern Command
SRR	System Requirements Review
TEMP	Test and Evaluation Master Plan
TMS	Token Management System
TRA	Tactical Registration Authority
TRR	Test Readiness Review
TY\$M	Then-Year Cost in Millions

U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
WSARA	Weapon Systems Acquisition Reform Act

REPORT DOCUMENTATION PAGE*Form Approved
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)

