Public Key Infrastructure Roadmap for the Department of Defense

18 December, 2000
Version 5.0

Prepared By:

DoD Public Key Infrastructure Program Management Office

Approved:

_____

Assistant Secretary of Defense
(Command, Control, Communications, and Intelligence)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 DEC 2000		**00-00-2000 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Public key Infrastructure Roadmap for the Department of Defense	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) **Assistant Secretary for Defense Command, Control Communications and Intelligence,DoD Public Key Infrastructure Program Managment Office,Washington,DC**	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
Approved for public release; distribution unlimited

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			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**42**	

Table of Contents

List of Figures

Executive Summary

The Public Key Infrastructure (PKI) Roadmap establishes the enterprise-wide end-state for the Department of Defense (DoD) PKI and outlines the evolution strategy and timeline for the availability of the Department's PKI capabilities. Also, it identifies critical risk areas that must be addressed, summarizes measures that will be undertaken to mitigate those risks, and highlights roles and responsibilities of organizations involved with its realization. This document is an update to the DoD PKI Roadmap (Version 3.0). It provides an updated perspective on the overall evolution of the Department's PKI program, and addresses new requirements identified in the 12 August 2000 ASD C^3I Memorandum including integration with the Common Access Card (CAC).

Achieving Information Superiority in the highly interconnected, interdependent, shared-risk DoD environment requires that the Department's Information Assurance (IA) capabilities be applied within a management framework that considers the pervasiveness of information as a vital aspect of warfighting and business operations. The technical strategy that underlies DoD IA is Defense in Depth, in which layers of defense are used to achieve our security objectives. The DoD PKI is a supporting layer of this strategy, providing a vital element for a secure IA posture for the Defense Information Infrastructure (DII).

The DoD PKI strategy recognizes that a traditional, Government-developed implementation will not be able to keep pace with a strategy based on commercial technology and services. It recognizes that the DoD PKI must employ an incremental, evolutionary approach using open standards, based on commercially available products and services that can keep pace with the technology rollover and constantly evolving applications and standards inherent in the Information Technology (IT) environment. With that, it must still maintain appropriate levels of security, embracing secure interoperability both within the DoD and externally with Federal and international counterparts and with business partners.

It is imperative that the Department takes an aggressive approach in establishing a PKI that provides public key products and services needed to support the Department's diverse set of missions and operations. The DoD PKI will also enhance the Department's capability for tactical, joint, and combined operations, as well as improved interoperability with allies, coalition forces, civil agencies, and business partners. To ensure operational effectiveness, the DoD PKI will provide these products and services transparent to subscribers. Thus, as the infrastructure is upgraded through phased releases, these upgrades will be transparent to subscribers. However, in some cases, achieving transparency will require enhancements to user devices and mission planning systems so they take full advantage of the features offered by the DoD PKI.

The DoD PKI will support directly the Department's desire to encourage the widespread use of public key (PK)-enabled applications throughout the Department's activities. The DoD PKI will evolve as an essential element of the overall Key Management Infrastructure (KMI) and will be realized as an integral part of DoD's KMI evolution. The National Security Agency (NSA) has initiated a DoD KMI program, with the support of the Defense Information Systems Agency (DISA), the Services and Agencies, Joint Staff, and the DoD contractor community. The DoD KMI will enable the provisioning of cryptographic key products, symmetric and asymmetric (public) keys, and security services. The DoD KMI will be implemented through a phased evolution delivering Capability Increments (CIs) every 18-24 months. The PKI is the primary component of the first CI, CI-1.

1. INTRODUCTION

This PKI Roadmap establishes the Department's plan for the implementation of the DoD PKI and outlines the DoD strategy and timeline for the availability of PKI capabilities. It provides a perspective on the Department's existing PKI capabilities, the evolution to a DoD PKI, and the transition of existing PKI capabilities to the DoD PKI. It also identifies critical issues and challenges that must be addressed concurrent with the implementation of the strategy and highlights roles and responsibilities associated with its implementation. It is important to note that the PKI Roadmap is a strategic planning document. Formal commitments for the delivery of infrastructure products and services will be made via the DoD PKI (and KMI) planning processes.

This document is one of three major planning documents for the PKI evolution. It complements the DoD PKI Implementation Plan (Reference A) that identifies tasks, schedules, dependencies, and responsibilities across the Department for realizing the PKI evolution and operation. It is also supported by the DoD X.509 Certificate Policy (CP) (Reference B) that identifies the applicability of certificate assurance levels, and the personnel, physical, procedural, and technical security controls needed to achieve those levels. The Roadmap represents a long-term guide for high level planning and budgeting. Together these documents provide a framework for the Department's realization of an effective PKI capability. These documents will be updated periodically to reflect actual implementations, updates to requirements, and advances in PKI-relevant technologies.

1.1 Background

The individuals, programs, and systems that carry out or support the broad range of missions and operations of the DoD perform a variety of activities. These diverse activities, highlighted in Figure 1, represent an ever-expanding need for IA capabilities in DoD operations.

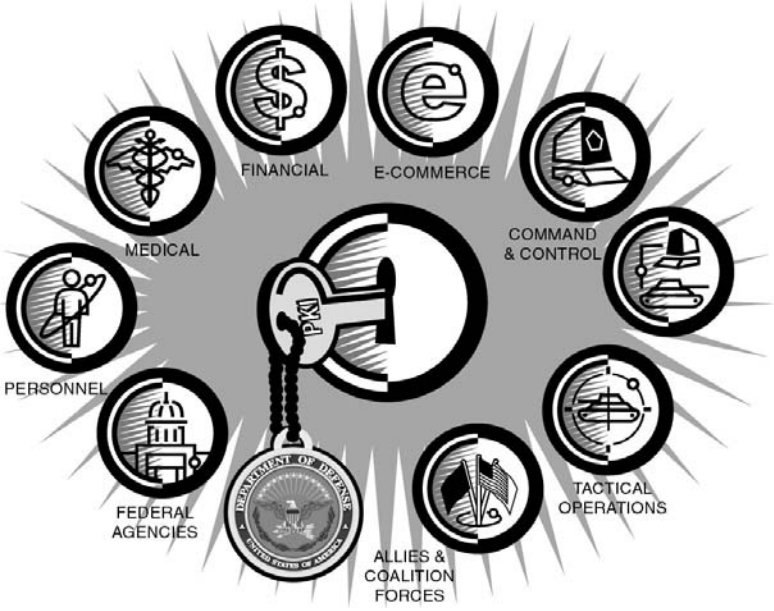

Figure 1. DoD Missions and Operations Relying on PKI

Traditionally, DoD has satisfied these needs with stand-alone cryptographic components. In today's IT-rich environment, DoD's IA needs are being addressed with security features integrated into the many communications and information processing system components that comprise the DII. PK technology is rapidly becoming the technology of choice to enable security services within these systems. These security services include: identification and authentication; data integrity; confidentiality of information and transactions; and non-repudiation to facilitate mission-related and eBusiness transactions internal to the Department and with external organizations.

In a memorandum dated 9 April 1999 (Reference C), the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C^3I) assigned NSA program management responsibility for the Department's efforts to implement a PKI and DISA to provide a Deputy Program Manager. In response NSA and DISA have established a Program Management Office (PMO) that will ensure the DoD PKI supports validated and endorsed PK-enabled systems and applications that meet the broad spectrum of DoD mission and business needs.

1.2 Defense in Depth Strategy

The Department's IA strategy recognizes that no single element can provide adequate assurance independently, and that layers of defenses of varying strength and assurance levels can be deployed to provide multiple roadblocks between our sensitive information systems and those internal and external adversaries who would try to exploit them. This layering allows the use of multiple solutions of varying assurance levels and, upon failure of deterrence or prevention, the containment of the consequences of a breach in security to achieve a balanced overall IA posture. Critical Defense in Depth layers include:

- *Defense of Computing Environments* including the hosts, servers, applications, and operating systems used within DoD local area networks (LANs),

- *Defense of Enclave Boundaries/External Connections* at which DoD LANs connect to the wide area networks (WANs) by deploying boundary protection measures to control and monitor access to the internal LANs,

- *Defense of Networks and Infrastructure,* including the WANs that are used to interconnect DoD systems and those of its allies and business partners, to ensure the confidentiality of DoD communications and protection against Denial of Service attacks that could disrupt DoD's ability to communicate prior to or during operational deployments,

- *Attack Sensing, Warning, and Response* to protect, analyze, and respond to unauthorized access, intrusions, and cyber attacks at local, regional, and national levels, and

- *Key Management Infrastructure* services including key management for DoD traditional, and more recently public key systems, as well as physical products such as codebooks and authenticators.

Thus, PKI is identified within this strategy as an element of the KMI, providing PK products and services that support, and thus enable security services in DoD applications, devices, and systems.

1.3 PKI Products and Services

PKI, as defined herein, refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking of PK certificates and their corresponding private keys. The DoD PKI will support registration of users, dissemination of certificates, and a full range of certificate management services as discussed in Section 2.4.3. This provides the critically needed support to individuals, applications, and network devices that provide secure encryption and authentication of network transactions as well as data integrity and non-repudiation.

Certificates are instruments used to convey trust. The initial deployment of the DoD PKI will provide two types of certificates: identity certificates (used for authenticated access and digital signatures) and key establishment (confidentiality) certificates. There are profiles within these types that will support certificates for servers, e-mail signature services, and e-mail confidentiality services. To achieve common certificates across the entire DoD, the DoD PKI identity, e-mail signing, server (device), and encryption certificates will have a minimum/common set of attributes as specified in the certificate profile section of the DoD X.509 CP. Unique e-mail certificates are needed to support current versions of the commercial S/MIME protocol that requires an e-mail address to be embedded in certificates. These e-mail-specific certificates will not be required with the next version of the S/MIME protocol, so these will be phased out once the Department transitions to the updated version of S/MIME. This still requires each subscriber to have identity and key establishment certificates. As the PKI evolves, it is possible that additional certificate types will have to be provided. Other types of certificates such as network access and object-signing certificates will be supported by the PKI as operational requirements dictate.

1.4 Existing PKI Capabilities

Since the mid 1980s, NSA has used PK technologies in a number of large deployment programs including the Secure Terminal Equipment (STE), its predecessor, the Secure Telephone Unit (STU-III), and a number of secure wireless terminal initiatives. In the early 1990s, these activities were expanded with the development of a hardware token (FORTEZZA) and an operational PKI under the Multilevel Information Systems Security Initiative (MISSI) to support organizational messaging under the Defense Messaging System (DMS) using Government-off-the-shelf (GOTS) technologies. It was based on the use of FORTEZZA hardware tokens and a Government-developed Certificate Authority capability, which required the use of Certificate Authority Workstations (CAWs) to register and issue certificates on the FORTEZZA token. What resulted was the FORTEZZA-based Class 4 PKI designed primarily to support DMS, which was approved for operational use in March 1995. In January 1998, the infrastructure was updated to CAW version 3.1 to support subsequent releases of DMS. The CAW has been updated to version 4.2.1 to support DMS Release 3.0 scheduled for operation during FY2001. This latest update provides the capability to support X.509 version 3 certificates, key recovery for private confidentiality keys, and security labeling compatible with DMS Release 3.0.

In the mid 1990s, the Department recognized that while there were indeed mission-critical operational requirements that at the time could only be satisfied with developmental (GOTS) solutions, the push toward eBusiness in the commercial sector created technologies that offered tremendous potential benefit to non-mission critical DoD operations and missions. The Department decided to assess the value of the rapidly evolving commercial PKI technologies by deploying a commercial, Medium Assurance PKI and a series of application pilot programs that relied on it.

Based on the success of these pilots, what was then the Medium Assurance PKI (renamed Class 3 PKI Release 1.0) was upgraded to Release 2.0 and approved as an operational capability in July 2000. Plans are currently underway for Class 3 PKI Release 3.0, scheduled for the 2nd Quarter of FY2001, that will integrate PKI registration capabilities into the DoD Real-time Automated Personnel Identification System (RAPIDS). RAPIDS terminals, which will be used to issue CACs for the Department, have been enhanced to serve as Local Registration Authorities (LRAs), providing PKI certificates on the CACs for many DoD subscribers. Traditional PKI LRAs will be used to support device owners as well as those users that cannot obtain service from RAPIDS.

1.5 Planned Evolution

Stemming from a Deputy Secretary of Defense policy memorandum in 1999 (Reference D), efforts were initiated to plan for and implement an evolutionary approach for an effective PKI capability that would serve the Department overall. It called for making the Medium Assurance PKI pilot an operational (Class 3) capability, sustaining the existing DMS (Class 4) PKI, and planning for an evolution to the DoD PKI that would eventually replace both of these systems. On August 12, 2000, ASD C3I issued an update to this policy (Reference E). While it adjusts milestone dates for its implementation, it still mandates that the Department transition the existing capabilities, remain focused on commercial technologies, and continue to strive to reach Class 4 assurance levels for all appropriate DoD electronic transactions. The DoD PKI will be implemented as an integral part of DoD's KMI evolution. Beginning with Release 4.0, PKI releases will be integrated as part of the appropriate KMI capability increments. The DoD PKI will be implemented to support the Class 4 requirements across the Department as set forth in the recent ASD C3I policy, building on the functionality of the existing Class 3 PKI services as a baseline. While the DoD PKI continues to evolve, existing PKI capabilities will remain operational to facilitate an efficient transition.

2. The DoD PKI

The DoD PKI strategy recognizes that a traditional, government-sponsored development and implementation will not be able to keep pace with a strategy based on commercial technology and services. It recognizes that the DoD PKI must employ an open standards approach, based on commercial products and services that can keep pace with the technology rollover and constantly evolving applications and standards inherent in the IT environment, while still maintaining appropriate levels of security. It embraces secure interoperability both within the DoD and externally with Federal and international counterparts and business partners. The DoD PKI strategy also recognizes and takes into account the evolving state of commercial secure network products and standards, and employs an incremental, evolutionary approach to achieving the DoD PKI.

2.1 Goals and Objectives

The DoD PKI provides the products and services that enable effective use of PK technology. Historically, key management services associated with an infrastructure of this nature have been expensive to develop and manpower intensive to operate. We recognize that the only practical way to extend IA features to over 3.5 million DoD employees (active military, reservists, and civilians) and to the hundreds of software applications and the thousands of network devices across the Department is to deploy a modern, commercially-based infrastructure that offers:

- ***Broad Operational Support*** – The individuals, programs, and systems that conduct or support the broad range of DoD missions perform a variety of activities. These diverse activities represent an ever-expanding need and role for IA capabilities in DoD operations. The DoD PKI has to support ALL of these activities.

- ***Interoperability –*** The Department relies heavily on interactions and coordination with external communities. These include military operations with Allies and Coalition forces; close working relationships with the Intelligence Community; coordinated operations with other federal Government agencies; and day-to-day transactions with our business partners in the U.S. and abroad. Interoperability is fundamental to our mission success.

- ***Transparency –*** The DoD PKI is designed to be compatible with the most popular, commercial software packages. Commercial PKI vendors have spent considerable resources building plug-ins and "toolkits" (i.e., software that adds security features compatible with PKI services) to give applications the ability to work with their PKI solutions. The PKI PMO is building on this base of toolkits to ensure that the Department has the capability to integrate (or PK-enable) DoD's custom software so it will interact effectively with the PKI, transparent to the user.[1]

- ***Ease of Operation –*** PKI operator interactions that are manpower-intensive are being upgraded to be more operator-friendly and as transparent as is practical. Toolkits are also

[1] While the PKI can provide infrastructure capabilities to enable this transparency, modifications to PKI-aware devices are also required to add functionality that can realize this transparency.

being identified to enable the DoD to tightly integrate PKI capabilities into mission planning system capabilities.[2]

- ***Enhanced Security –*** The DoD PKI will provide the security and assurance needed to ensure operational integrity for Command and Control, Mission Support, and e-Business uses. The PKI will be built on authentic, universally accepted identities for all users, operators, and devices, with standard toolkits that ensure the integrity of all PKI-relevant operations.

- ***Evolutionary Roll Out –*** The DoD PKI is structured to take advantage of the steady pace of advances in technology available from Industry. The DoD PKI, based on commercial industry standards, is being deployed in phases, introducing new features and capabilities in an orderly fashion, consistent with commercial technology progression.

The Department is harnessing rapidly advancing commercial technologies to realize these objectives.

2.2 General Features of the DoD PKI

There are several pervasive characteristics of the DoD PKI. These include the following:

- ***Modular Design –*** The DoD PKI has adopted the highly modular, nodal architecture of the evolving DoD KMI. By enforcing this modularity and maintaining control of both physical and functional interfaces, PKI features and capabilities will evolve over time in a structured and cost effective manner.

- ***Standards Based –*** The DoD PKI is based on the use of commercial standards to the maximum extent feasible. The DoD PKI program will ensure that DoD specifications are consistent with the emerging commercial and National Institute of Standards and Technology (NIST) Federal standards, and will continue to track new and evolving Internet Engineering Task Force (IETF) standards to ensure the most viable commercial standards are fully leveraged.

- ***An Integral Component of the DoD KMI –*** DoD's PKI capability will be realized as an integral aspect of the overall DoD KMI evolution. The DoD PKI will be integrated into the common management processes defined for the broader KMI capabilities, as discussed in the DoD KMI Roadmap (Reference F). The PKI is the primary component of the first KMI CI.

- ***Focused on a Single (Class 4) Assurance Level –*** DoD's goal is a single, interoperable, high assurance (Class 4) PKI for all environments and applications that employ PK technologies (except for protection of classified information over otherwise unprotected networks.)

- ***Phased Transition –*** The PKI structure will evolve over time. Enhanced system capabilities will be introduced in parallel with existing operational capabilities, with NO hard cutover whenever feasible.

[2] This goal too can only be realized with enhancements to mission planning and system management components.

2.3 System Context

The PKI interacts with a number of external components and systems to perform its intended functions, as highlighted in Figure 2. One of the primary capabilities is to interact with the individuals, applications, and devices it is intended to serve. The DoD PKI interacts with external Federal and commercial PKIs to achieve the broad base of interoperability that must be supported. It also interacts with External Certification Authorities (ECAs) that provide acceptable levels of assurance for DoD-compatible certificates used by commercial business partners and others that are not served directly by the DoD PKI.

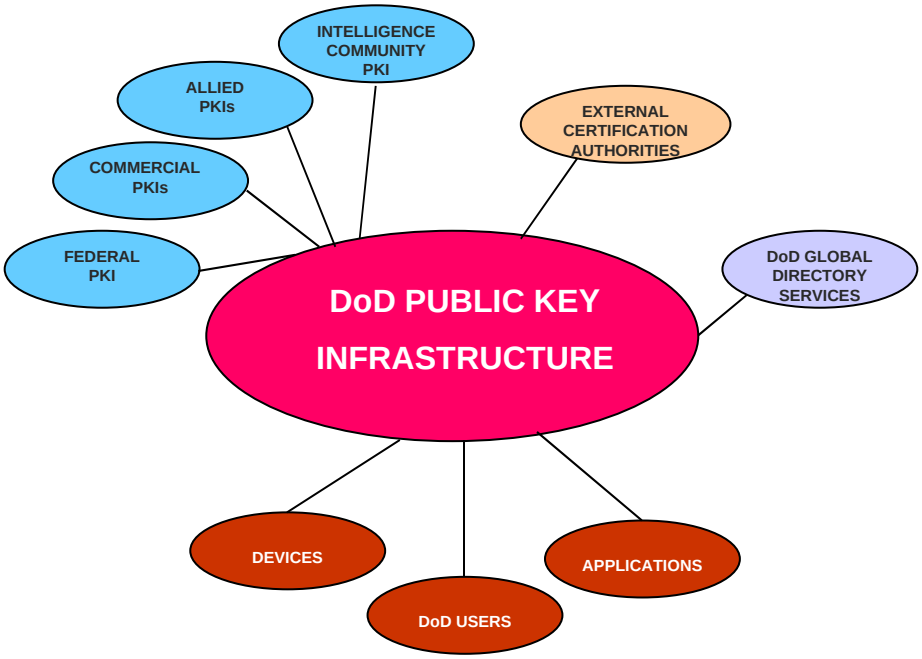

Figure 2. DoD PKI System Context

The DoD PKI interfaces to the DoD Global Directory Services that will offer a DoD-wide repository of specific user information contained within the many DoD local directories deployed worldwide.

2.4 PKI System Elements

As shown in Figure 3, there are three major elements of a PK enabled system that must work together to achieve secure functionality: registration, certificate management, and subscribers (that include individuals, their PK-enabled applications, servers, and network devices that use public keys to support their operations).

2.4.1 Subscribers and Relying Parties

Subscribers are the consumers of the products and services provided by a PKI. Clearly individuals are consumers. However, software applications and hardware devices (such as firewalls and routers) can also use the PKI to support their operations. A *relying party* refers to anyone that will use (rely on) PKI products and services and their implied trust to verify the identity of the source of a transaction, check the integrity of a message, or establish a confidential communication.

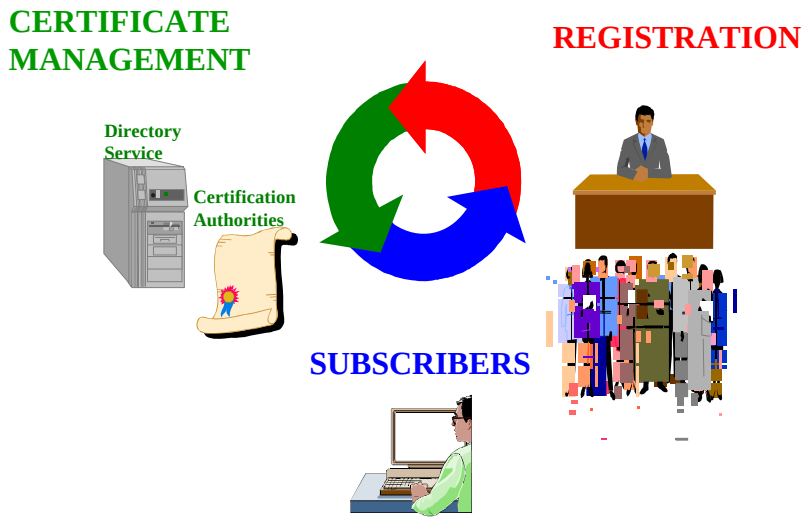

Figure 3. Major PKI System Elements

The PKI supports the employment of cryptographic security services by providing subscribers with valid PK certificates that are bound to the corresponding private key and certificate revocation information. The subscribers actually encrypt and decrypt data and/or sign and verify signatures. Information contained in the certificate includes an issuer's public key, an X.509 certificate version number, the issuer's name, a serial number, the individual's (or subscriber) name, the subscriber's public key, and validity period for use. Future certificate types may offer information such as attributes or privileges as requirements mandate.

2.4.2 Registration

Registration is the process that subscribers use to identify themselves to the PKI and to request certificates. The level of trust in any PKI stems directly from the integrity of the registration process. The requirements for this process are defined in the DoD X.509 CP. Registration Authorities (RAs) are responsible for verifying the identities of subscribers and information that is entered into PK certificates, and for requesting the certificate management services discussed below. RAs are also responsible for verifying any additional subscriber information that may also be contained in a subscriber's certificate. LRAs can be designated by an RA to assume responsibilities for registration of local community subscribers. These RAs and LRAs provide registration services for all subscribers, including those needing certificates for servers and devices, and for subscribers that are on SIPRNet.

RAPIDS Verifying Officials (VOs) are specialized versions of LRAs. RAPIDS workstations have been upgraded to support RA and LRA functions. RAPIDS terminals interact with the Defense Eligibility Enrollment Reporting System (DEERS) database that contains personnel information to ensure proper identification during registration of most subscribers. RAPIDS VOs will register DoD subscribers who have already been enrolled into the DEERS system into the PKI, using DEERS as an authoritative source, and to issue CACs containing PK certificates. RAPIDS Super Verifying Officials (SVOs) are the RA counterparts for the VOs.

2.4.3 Certificate Management

Certificate Management involves the generation, production, distribution, control, tracking and destruction of public/private keys and associated PK certificates. Certificate management functions are performed by Certification Authorities (CAs). Central to the certificate management

element is a trusted third party that certifies the identity of the subscriber that possesses a private key used for digital signature or key exchange. CAs serve as trusted third parties. CAs are responsible for all aspects of the PKI certificate management process, ensuring that its operation and the services it provides are performed in accordance with the requirements, representations, and warranties of the DoD X.509 CP. Within the DoD PKI, the certificate management process is responsible for:

- Generating and digitally signing each certificate, thereby binding the association of the public key to the corresponding subscriber,
- Delivering the X.509 certificate to the subscriber (typically on a token) and publishing the certificate to a repository (e.g., directory) that is accessible by other subscribers,
- Managing the revocation of certificates. DoD will use two methods to manage the revocation of certificates: (1) Publishing and posting certificate revocation information to the directory, and (2) Providing a mechanism for a real-time check of the revocation status,
- Archiving of the required certificate management information (e.g. registration information, certificates, and certificate revocation information) to support non-repudiation of digital signatures ,
- Supporting authorized recovery of cryptographic keys that are needed to gain access to encrypted information when the intended decryption key is not available, and
- Providing certificates, tools, and procedures for personnel responsible for subscriber registration.

2.5 DoD PKI Architecture

While the DoD PKI evolves, it will be enhanced in conjunction with the DoD KMI evolution. The KMI has adopted a modular structure to allow adequate flexibility to ensure it can evolve over time. The architecture is built on four types of nodes.

- The Client Nodes represent the subscribers that require products and services from the KMI (and PKI). These include the consumers (i.e., individuals, software applications, and hardware devices as discussed in section 2.4.1). Client nodes also include the managers (e.g., RAs, LRAs) that interact with the PKI to register and request certificate management services discussed in section 2.4.2.
- The Primary Services Node (PRSN) is the core element of the KMI (and PKI) structure, providing common management functions in a server-based architecture. It offers end entities (client nodes) unified and transparent access to the production sources, providing direct delivery of PKI products and services to consuming applications. It also handles subscriber access control and manages the interfaces between the other nodes.
- The Production Source Nodes (PSNs) interface to the common management functions of the PRSN. One type of PSN is the PKI CA, that provides the certificate management functions discussed in section 2.4.3, including key pair generation; certificate creation, posting, rekey, and revocation. The Root CA can be considered a special type of PSN, however, for security reasons, it is not networked to the PRSN (or other PSNs).
- The Central Services Node (CSN) provides overall system management and configuration management functions for the infrastructure, including the long-term system archive and the master KMI database. The CSN will also handle system health monitoring and overall

infrastructure security management, including intrusion detection security oversight and audit data and analysis.

The majority of the PKI components within this architecture are available as COTS products. The PRSN functionality is currently envisioned as a government-sponsored capability that will be developed under the DoD KMI initiative. The functionality and general relationship of these nodes is highlighted in Figure 4. It utilizes a communications fabric encompassing a variety of existing networks and workstations to satisfy its mission requirements.

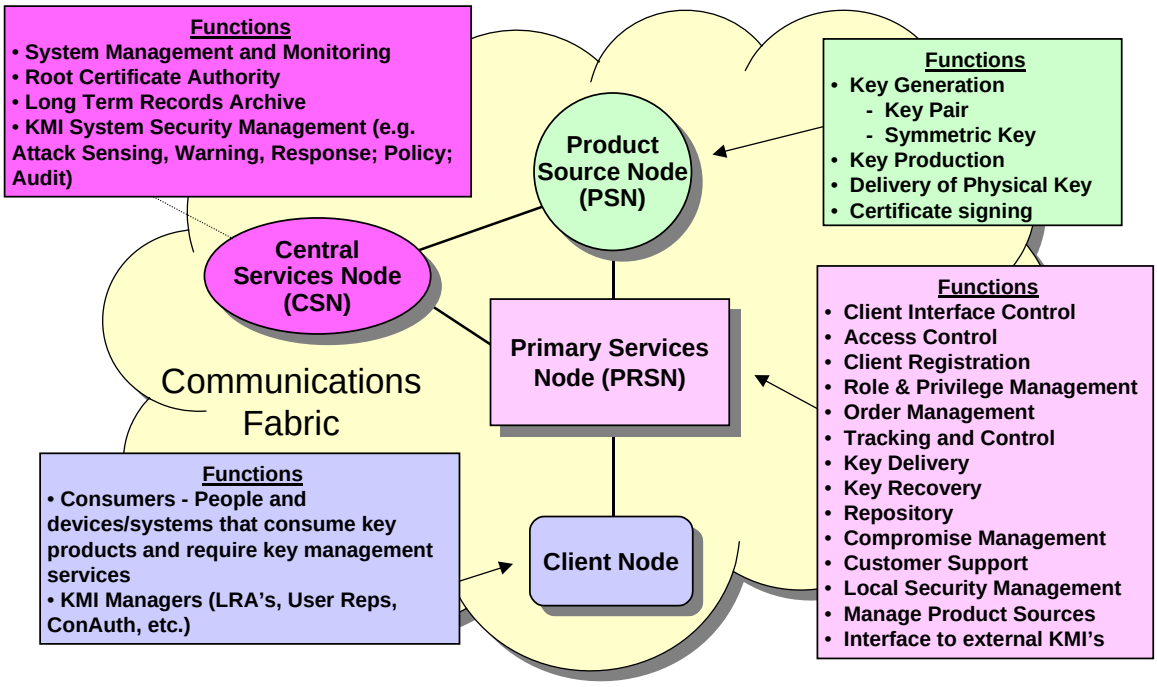

Figure 4. Nodal View of the DoD PKI

2.6 General Deployment Considerations

The DoD PKI will be deployed as modular sites consistent with the nodal architecture discussed above. While the exact nature of the final deployment is still under consideration, there is a conceptual deployment for the DoD PKI defined as a baseline, as depicted in Figure 5. Separate, but parallel PRSNs will be deployed for PKI and other KMI services. In early phases, separate PRSN configurations will be established to serve different security domains; future security enhancements are envisioned to allow subsequent integration of these functions across domains. There are also plans for future deployments in regional areas where the operational need dictates, and deployable sites to support tactical elements.

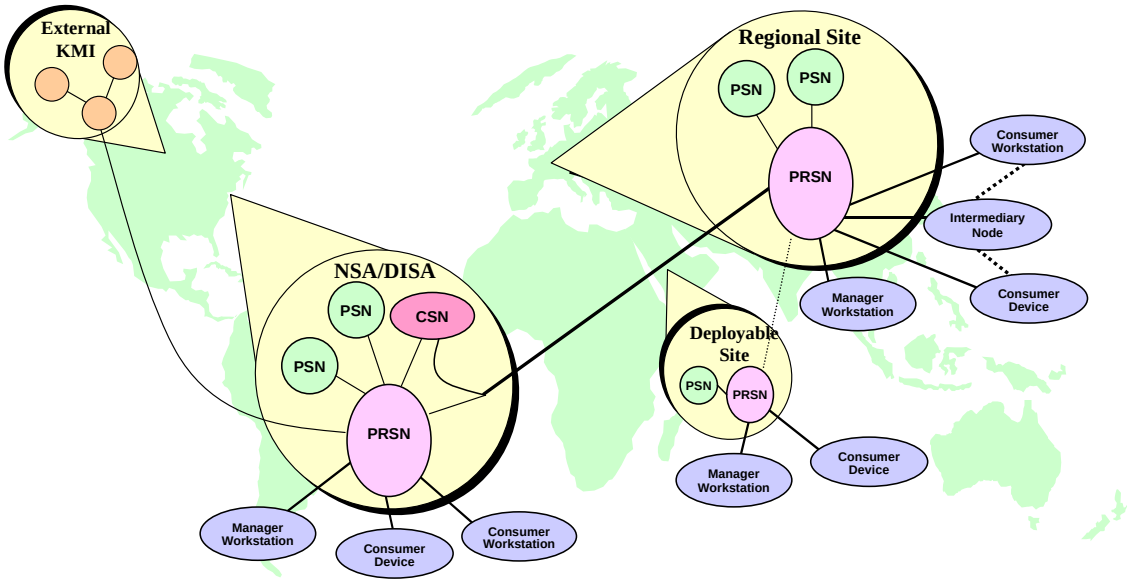

Figure 5. PKI Deployments

There will be several PRSN sites in strategic locations across CONUS. PSNs (CAs) will be co-located with several of the PRSNs. The current plan is for PKI PRSNs (and CAs) to be located at the Defense Enterprise Engineering Center Detachments at Chambersburg, PA and Denver, CO, the sites of the existing Class 3 PKI CAs. Each will be capable of serving as a back-up capability to other PRSNs, with automated cutover capabilities available to ensure uninterrupted service to PKI clients. The Root CA for the DoD PKI will be located at NSA, and will not be networked.

Requirements have been identified for regional sites (PRSNs and PSNs) outside CONUS (in both the European and Pacific theaters.) Efforts are underway to determine how these requirements can be satisfied. Typically, these sites will reach back to the CSN located in CONUS. These regional PRSNs will also have to include basic CSN provisions to facilitate operations when connectivity back to CONUS is impaired or unavailable.

As indicated earlier, the current Class 3 PKI includes directory services used to post certificates, certificate revocation, and other PKI information. The DoD PKI will transition to the use of the DoD Global Directory Services when it is available. Currently, NSA and DISA are establishing a formal service level agreement to identify the functional capabilities and interfaces needed to ensure that the Global Directory Services will incorporate the features necessary to support the DoD PKI.

The DoD PKI will not deploy networks of its own, but will rely on the communication channels already serving its customers in other capacities. The PKI will rely on existing communications paths for connectivity within the system. The dominant paths will be the Unclassified IP Router Network (NIPRNet) and Secret IP Router Network (SIPRNet).

3. STRATEGY TO ACHIEVE THE DoD PKI

The PKI strategy is to leverage existing IA policies, IA capabilities of commercial technologies, existing DoD PKI implementations, and Defense in Depth concepts, to satisfy the DoD PKI needs and the goals established for its evolution. An incremental strategy will allow a phased evolution, providing the means for integrating requirements that can be satisfied in an orderly manner, reducing development cost and schedule risk, and allowing the PKI to take advantage of viable technology advances as they become available. While the PKI will only offer value to the Department if PK-enabled applications are available that take advantage of the products and services it offers, the activities associated with this enabling is outside the scope of the PKI program, and is not addressed in the PKI strategy. The risks associated with this availability are discussed in section 4.3.

The strategy to achieve the DoD PKI is linked to the overall DoD strategy for achieving IA. The IA strategy, as defined in DoD Policy Memorandum No. 6-8510, Information Assurance for the DoD Global Information Grid, (Reference G) provides a framework as well as guidance for the acquisition of IA-relevant technologies. A companion document, the IA Technology Framework, IATF (Reference H) offers detailed technology recommendations and guidance for its effective use, consistent with 6-8510. This framework is augmented by a series of technical specifications, called Protection Profiles, delineating the technical, performance, and best practice standards for system functions that support the Defense in Depth layers. These security specifications, written in accordance with the International Common Criteria for Information Technology Security (Reference I), will serve as the basis against which IA products/services can be assessed and evaluated to determine their effectiveness for use in securing DoD systems. These documents are also compatible with the National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11 (Reference J) that governs the acquisition of IA and IA-enabled IT products for national security systems and networks.

A major activity in the DoD PKI arena has focused on understanding the technology, standards, operational policy, and procedural issues, and establishing the role of PKI relative to the rest of the IA Defense in Depth model. The experiences gained from the two major DoD PKI initiatives (the existing Class 4 PKI that supports DMS and other FORTEZZA-enabled applications, and the Medium Assurance PKI pilot that was recently transitioned to a fully operational Class 3 PKI), have been instrumental in the development of the DoD PKI architecture.

While based on Government-developed technology and protocols, the decentralized, FORTEZZA-based Class 4 PKI provided a means for establishing a PKI technology baseline, developing the knowledge and expertise to influence commercial standards bodies, creating PKI policy and procedures, and obtaining an understanding and appreciation of their operational impacts and issues. Similarly, the existing Class 3 PKI (and its predecessor Medium Assurance PKI pilot) offered an initial appreciation of the benefits and shortfalls of a centralized PKI architecture based on commercial technology, policy, and procedures, and helped DoD to influence applications developers in the direction of standards-based PK-enabled applications. Both of these PKIs resulted in architectural and technical specifications, supporting policy and procedural documents, and critical lessons learned that enabled the Department to address DoD PKI development activities more effectively.

Accordingly, the DoD PKI will be designed with adequate flexibility to ensure that it can evolve over time. It will immediately leverage existing commercial capabilities in the baseline

implementation and incrementally evolve the capability as commercial technology matures. The strategy mandates significant DoD involvement in commercial standards organizations to influence the direction and maturation of technology to address DoD PKI requirements.

3.1 Overall PKI Rollout Strategy

As indicated earlier, the DoD PKI evolution is designed to offer PKI products and services with a transition transparent to subscribers. The evolution of the infrastructure components is integrated into the KMI CIs. The detailed design and planning for this evolution is extensive and complex, but the evolutionary strategy is fairly straightforward. In the near term, the existing Class 3 and the Class 4 (DMS) PKI capabilities will be maintained. The Class 4 (DMS) PKI is currently being enhanced with the deployment of the updated CAW software Release 4.2.1 capability. The FORTEZZA-based Class 4 (DMS) PKI was updated to incorporate CAW version 4.2.1 in September 2000. This latest update provides the capability to support X.509 version 3 certificates, key recovery for encryption keys, and security labeling compatible with DMS release 3.0. There are approximately 500 CAWs currently deployed. Efforts are underway to evaluate the feasibility of consolidating the operations and reducing the numbers of CAW operators needed to support this infrastructure, as well as to determine the steps that are needed to transition to the next release of the DoD PKI. A segment of the DMS user population will transition to the DoD PKI under the Medium Grade Services initiative. The evolution to the DoD PKI will provide the long-term infrastructure solution for the remaining DMS subscribers.

3.1.1 Existing DoD PKI Releases

The Medium Assurance PKI pilot was transitioned to the Class 3 PKI (Release 1.0) in April 1998. In July 2000, the DoD Class 3 PKI (Release 2.0) which introduced the use of X.509 version 3 Certificates was approved for operational use. Efforts are underway to incorporate Class 3 PKI LRA functionality into RAPIDS terminals. Currently scheduled for the 2nd Quarter FY2001, these updated RAPIDS terminals will be introduced in Class 3 PKI Release 3.0 to provide a means for registering users enrolled in DEERS into the PKI and issuing CACs (smart cards) that serve as PKI hardware tokens. The Class 3 PKI Release 3.0 will also continue to support certificates in software.

The functionality of the existing Class 3 PKI capability serves as a baseline for the DoD PKI, being implemented as an integral segment within what is emerging as the unified DoD KMI. NSA, in conjunction with DISA, the Services, and industry partners is currently defining the strategy that merges the existing KMI capabilities (that support DoD and the rest of the national security community), other relevant key management initiatives, and the functionality for the DoD PKI. The DoD PKI will be implemented to support the Class 4 PKI requirements across the Department as set forth in the recent ASD C3I policy.

CIs represent the build, integrate, and test philosophy used to implement the DoD KMI. The DoD PKI Releases align with the KMI CIs. The remainder of this section provides an overview of specific PKI capabilities planned within each DoD PKI release.

3.1.2 DoD PKI – Release 4.0

Consistent with the KMI CI-1, PKI Release 4.0 will provide an initial set of Class 4 PKI products and services consistent with those provided by the existing Class 3 PKI. This will enable the transitioning of the infrastructure components from the existing Class 3 PKI capability to the DoD PKI. Again, this transition is planned to be transparent to the subscribers. Specifically Release 4.0 will include the following products and services for the DoD PKI:

- Identity certificates and key pairs, which are used for digital signatures and to provide identification and authentication of a party in an electronic transaction
- Class 4 certificates needed to support network servers
- For subscribers who require them, key establishment (i.e., confidentiality) certificates to support encryption services and key pairs used to encrypt electronic communications with either hardware or software cryptography. A certificate to support encryption can be provided on the same token as the ID certificate. Also, e-mail certificates to support signatures and encryption services will also be available in this timeframe.
- Corresponding certificate management functions, such as re-key, validation, revocation, and tracking. The services provided for certificates in Release 4.0 will be comparable to those that are provided in the existing Release 3.0 (Class 3) PKI.

The major transactions include registration, enrollment, key distribution, rekeying, certificate revocation, and order management. In addition to those functions, the PRSN will provide local system and security management, help desk support to subscribers, a local data repository (directory), a library from which documents can be downloaded, and support for tracking of PKI products. In the Release 4.0 timeframe, CSN functionality will be included in each separate classification domain, and will be collocated with the PRSNs.

Release 4.0 will also provide the following infrastructure management functions:

- An integrated registration process for individuals, devices, and systems including those in the DEERS system
- Enrollment of individuals authorized to perform PKI management functions in Release 4.0 based on a static set of roles and privileges that the infrastructure associates with the subscriber's identity (established via the subscriber's PKI certificate)[3]
- PKI Help Desk extended from the existing Class 3 PKI Help Desk
- External interoperability, specifically with the Federal PKI using the Federal Bridge CA
- ECAs to extend PKI products and services to business partners and others (e.g., commercial business partners, and when appropriate, dependents and retirees) external to the DoD PKI
- Operator and subscriber training and implementation aids

Technology Prototyping and Anticipatory Developments

There are a number of additional PKI-related activities for the Release 4.0 timeframe that have been identified at this time to mitigate what are considered to be significant technical or operational risk issues. These activities, which are intended to ensure the smooth progression of PKI capabilities in future releases, include the following:

- Capacity modeling and scalability test environment
- Scalability choke point identification
- Cross-vendor CA subordination in hierarchical PKIs
- Advanced on-line certificate status processing capabilities
- Advanced key recovery capabilities
- Prototype on-line ordering for devices
- Simulator for access control mechanisms that could support DMS evolution
- PKI device simulator

[3] Note: Role and privilege information is not included in identity and encryption certificates.

Specific prototyping activities are subject to the availability of funding and the priorities that are established when activities are to be initiated.

3.1.3 DoD PKI – Release 5.0

While the detailed functionality of the PKI releases is not fully established, the PKI Program has defined a basic definition for DoD PKI Releases 5.0 and 6.0. Proposed features for Release 5.0 are dependent on the availability of funding and the results of detailed system engineering activities that will be conducted prior to its acquisition or development. It is important to recognize that these definitions are subject to refinement and adjustment during the appropriate system engineering activities associated with their definition and development. Planned capabilities for this release currently include the following:

- Support for access control mechanisms that enables the transition of DMS organizational messaging subscribers to the DoD PKI
- Introduction of an initial set of trusted date and trusted time stamp services
- Initial capability for integrity/software download certificates
- Additional support for new Key Exchange and DSA algorithms
- Toolkits for PKI-aware applications

Release 5.0 will also provide the following infrastructure management functions:

- Regional deployments of PKI PRSNs
- The ability to create new roles and dynamic mapping of privileges to roles
- PKI Help Desk features including an expanded repository of PKI information with on-line access available to authorized users
- External interoperability expanded to approved Allied and coalition partner PKIs
- Integrated PRSN structures for Class 3 and Class 4 PKI functions
- Independent CSN with electronic access to all PRSNs

Technology Prototyping and Anticipatory Developments

There are a number of additional PKI-related activities for the Release 5.0 timeframe that have been identified at this time to mitigate what are considered to be significant technical or operational risk issues. These activities, which are intended to ensure the smooth progression of PKI capabilities in future releases, include the following:

- Audit reduction tool development
- Elliptic Curve algorithm implementation
- Development of a KMI Applications Programming Interface (API)
- Time stamp application and processing
- Prototype automated accounting and archive capabilities
- Tactical network model
- Tactical protocol simulator
- Tactical demand simulator
- Prototype deployable PRSN
- PSN simulator for new Type 1 algorithm(s)
- Prototype Class 5 PKI PRSN and PSN capabilities

Specific prototyping activities are subject to the availability of funding and the priorities that are established when activities are to be initiated.

3.1.4 DoD PKI – Release 6.0

As with Release 5.0, proposed features for Release 6.0 are similarly dependent on the availability of funding and the results of detailed system engineering activities that will be conducted prior to its acquisition or development. It is important to recognize that these definitions are also subject to refinement and adjustment during the appropriate system engineering activities associated with their definition and development. Current plans are for Release 6.0 to introduce capabilities for new Class 5 algorithms needed for planned cryptographic system modernization. The DoD PKI capabilities will be expanded to offer trusted notary services.

A summary of the basic set of features introduced during Release 6.0 include the following:

- Prototype Class 5 PKI PRSN and PSN
- Full support for a trusted date/trusted time stamp service
- Full support for integrity/software download certificates
- An initial prototype for an accurate date/time service
- Introduction of notary services

Release 6.0 will also provide the following infrastructure management functions:

- Security filters to enable integration of automated PRSN functions across classification security domains
- Initial support for new Type 1 Crypto Modernization algorithms
- Enhanced external interoperability capabilities

Technology Prototyping and Anticipatory Developments

There are a number of additional PKI-related activities for the Release 6.0 timeframe that have been identified at this time to mitigate what are considered to be significant technical or operational risk issues. These activities, which are intended to ensure the smooth progression of PKI capabilities in future releases, include the following:

- Prototype PSN to support regional deployments
- Prototypes for field-deployable PKI managers and (battlefield) PKI-aware devices
- Prototype PSN for new Type 1 algorithms
- Delegated certificate path development.
- Display of Certificate Policy information to relying parties (so that per message policy information can be viewed by the relying parties)
- Biometric cryptographic tokens
- Additional advanced PKI features that will be determined at that time

Specific prototyping activities are subject to the availability of funding and the priorities that are established when activities are to be initiated.

3.2 Transition

While the actual DoD PKI structure will evolve over time, the PKI Program has established a fundamental philosophy for transition. Enhanced system capabilities will be introduced in parallel with existing operational capabilities. As indicated earlier, every effort will be made to ease any operational impact to subscribers resulting from the evolution of the infrastructure capabilities. The transition strategy will be based on NO hard cutover whenever feasible. This

will allow subscribers to plan and implement effective transition of their operations to take advantage of new capabilities.

The transition from the existing Class 3 PKI is straightforward, since the DoD PKI will offer the same services in a compatible framework during the transition phase. The existing Class 4 (DMS) PKI will be sustained until an effective transition is completed. A DISA and NSA working group has been tasked to establish and coordinate an effective overall transition for DMS subscribers. Currently, some DMS subscribers have determined that they do not require organizational messaging services (ala DMS) to satisfy their mission needs are being transitioned to use COTS e-mail services supported by the existing Class 3 PKI under the DMS Medium Grade Services (MGS) initiative. The transition of the broader community will be addressed by the working group.

Interim External Certification Authorities (IECAs) have been established to serve DoD business partners and others that cannot be supported by the existing DoD Class 3 PKI. IECAs are commercial certificate providers that provide certificate services, interoperable with those of the DoD Class 3 PKI, with a satisfactory assurance level to enable a trust relationship with the DoD PKI. IECAs were established as an interim capability to determine if the concept was viable legally and commercially. Once a final determination is made, ECAs will be established, transitioning from, and possibly adding additional providers beyond the existing IECA contractors. As with the IECAs, ECAs will be established through a process that encourages competition and ensures a commensurate level of trust with the DoD PKI. They will be approved by the DoD Chief Information Officer (CIO), in coordination with the DoD Comptroller and the Office of the Secretary of Defense (OSD) General Counsel.

If deemed necessary by the Department and when industry is able to support it, ECAs will migrate to a Class 4 level. If and when this transition occurs, the migration will again be transparent to subscribers and relying parties as existing Class 3 certificates issued by ECAs will be used until they expire, and will be replaced with higher assurance (Class 4 certificates) when they are normally replaced

The Department has not currently identified operational requirements for a PKI service to protect applications handling high value (e.g., classified) information in minimally protected (i.e., high-risk) environments such as NIPRNet or the Internet. Currently, these transactions are protected by conventional Type 1 cryptography for the transport mechanism, using Class 3 or Class 4 PKI services to operate within this stronger protection. The evolution of a higher assurance DoD Class 5 PKI capability will be driven by future operational and mission needs.

The PKI utilizes a wide variety of existing networks and workstations to fulfill its mission and is being designed based on commercial standards and commercially available products and service offerings. Initial deployments of the DoD PKI will be structured as separate functions for the Unclassified/SBU and Secret classification domains, however as the system evolves, it will transition to a structure that allows the transfers of appropriate data between domains. Using this approach, most PKI functions will operate on a single-level (commercial) System High platform at RA and LRA nodes. RAPIDS terminals, which require access to DEERS, will only operate over unclassified networks.

3.3 DoD PKI Schedule

The August 12, 2000 ASD C^{3}I policy directs specific events and milestone dates for the evolution of the DoD PKI. As highlighted in Figure 6, the PKI program is structured to provide a

transparent transition from the existing Class 3 PKI capabilities to the DoD PKI. While the infrastructure elements will be updated, every effort is being made to ensure that the impact to subscribers will be minimal (if not transparent). Existing Class 3 certificates and tokens will be retained until they expire normally. They will be replaced with Class 4 certificates when they are normally updated or replaced.

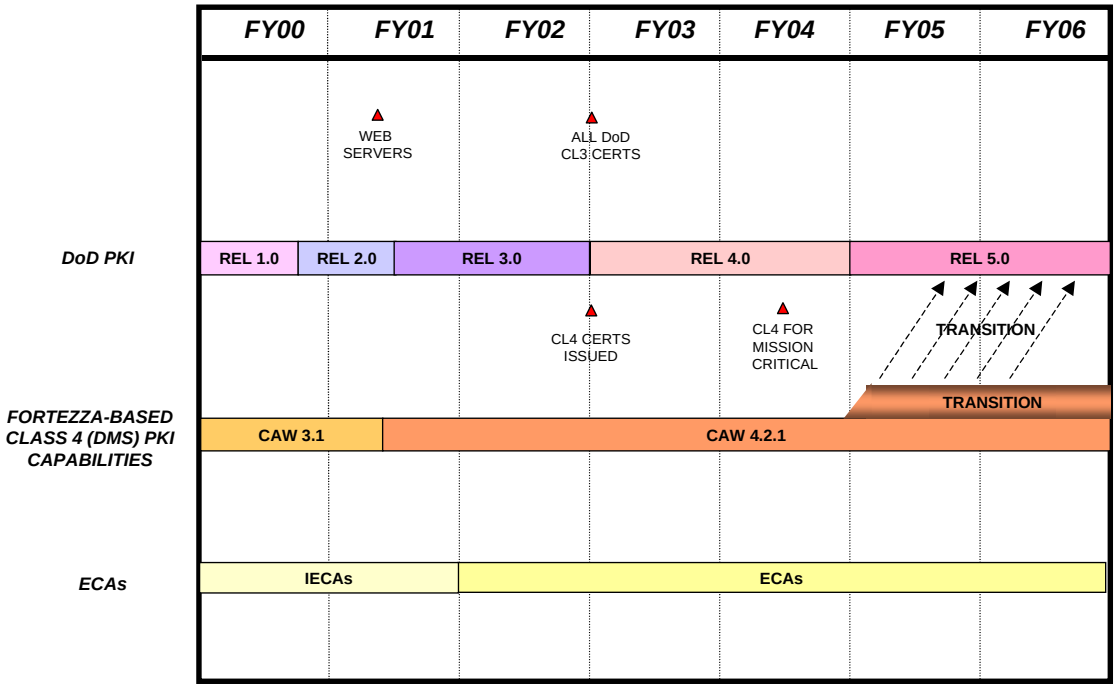

Figure 6. Operational View of the PKI Schedule

The PKI architecture is planning to use commercial, web-based clients for all PKI registration (RA and LRA) workstations (except RAPIDS), allowing them to remain unchanged, while the web servers that support them are updated to accommodate any additional features. RAPIDS terminals will be upgraded as appropriate. The shift from IECAs to ECAs will again be transparent to subscribers and relying parties. When the shift first occurs, it will have no operational impact on PKI subscribers and relying parties. If and when the ECAs migrate to a Class 4 level, certificates issued up to that point (at the Class 3 level) can be used until they expire, and will be replaced with higher assurance (Class 4 certificates) when they are normally replaced. The transition of users on the Current Class 4 (DMS) PKI will go through a structured transition. Efforts are underway to identify the exact transition strategy for the FORTEZZA-based users, and every effort will be made to ease any operational burden associated with the shift.

3.4 Critical Milestones

The August 12, 2000 ASD C³I policy memorandum established the timetable for the PKI evolution, and mandates a number of milestones for its realization. Several of these milestones are shown in the figure above to indicate their relationship to the major PKI activities. The schedule established for the PKI rollout is aggressive, and meeting the critical milestones associated with that schedule depends on a number of critical elements that have to be accomplished in a timely fashion. Critical milestones associated with this schedule are highlighted below:

1. Development, coordination and promulgation of the PKI user requirements,

2. Timely updates, coordination, approvals, and releases of the PKI (and KMI) requirement documents, the PKI Roadmap, PKI Implementation Plan, and the DoD X.509 CP,

3. Completion of the RAPIDS terminal upgrades to ensure that DoD LRA registration capabilities are in place in concert with the rollout of new PKI capabilities,

4. Completion of the registration and distribution of Class 3 certificates to all DoD subscribers,

5. Completion of the preparation, coordination, and approval of the specifications and related documentation to support each release of the DoD PKI,

6. Completion of the development, integration, test, security assessment, and deployment of each DoD PKI release, and

7. Establishment of ECAs, for interoperability with DoD business partners.

The PKI PMO has established detailed schedules, work breakdown structures, and tracking tools to monitor closely the progress of each element of the PKI program. The DoD PKI Implementation Plan contains the complete list of tasks required to meet these high level milestones and dates associated with each.

4. RISKS AND THEIR MITIGATION

Managing risks is a critical factor for the success of the DoD PKI program. Risk management involves two fundamental steps: risk assessment (to identify, analyze, and prioritize risks) and risk mitigation (to develop plans for risk resolution/mitigation/monitoring and to report their status). PKI risk management is an ongoing process, where the PMO will conduct periodic reviews to identify potential risks early enough to be able to mitigate their effects, and to monitor the progress on mitigating risks that were identified previously. This section identifies potential high-risk areas associated with the development, deployment, and operation of the DoD PKI, and steps that have been identified to address those risks.

4.1 Funding/Resources

As with any major program, availability of funding is a potential risk, particularly since the responsibility for funding of the DoD PKI will be shared between the NSA, DISA, Services, and Agencies according to their responsibilities as delineated in the PKI Implementation Plan. To ensure that funding is available and allocated effectively toward PKI-specific activities, the PKI PMO will assume the following responsibilities:

- Coordinate with NSA to identify resources needed to complete the development of the DoD PKI architecture, perform the security analysis and testing of the system and components, and procure and operate the Root CA(s),
- Coordinate with DISA to identify resources needed to integrate, implement and operate the centralized PKI components (e.g., the centralized CA Servers), and
- Coordinate with the Services and Agencies to identify funding and/or manpower resources needed to procure, deploy, and operate (or outsource the operation of) the local infrastructure elements.

4.2 Schedule

The schedule established for the PKI rollout is aggressive, and there is risk that it cannot be maintained. Meeting the critical milestones associated with that schedule depends on the Department's ability to accomplish a number of activities in a timely fashion. The PKI Implementation Plan establishes detailed schedules, work breakdown structures, and tracking tools to monitor closely the progress of each element of the PKI program. The Program has been structured to allow adjustment in the implementation of features for each release to carefully balance the Department's needs for the PKI, technology risks associated with satisfying those needs, and resource constraints. This will allow the PKI program to tailor its focus and ensure delivery of needed operational capabilities in a timely manner, and with a minimum of schedule risk.

4.3 PK-Enabled Applications Development

There is a risk that there will not be usable and/or interoperable PK-enabled applications available. There is no inherent value in the deployment of any PKI unless the Department implements applications that use the resulting capabilities to improve the effectiveness of their overall operations. To use PK technology, application developers must understand the supporting infrastructure's policies, usage, and interfaces. There are a growing number of

applications today which come ready off-the-shelf to accept PK certificates. Because PKI standards and products continue to evolve, functional and interoperability problems between vendors' applications are possible. ASD C³I is in the process of issuing a policy on PK-enabling of applications.

While the PKI program is NOT responsible for the PK-enabling of applications across the Department, it is developing the tools and capabilities that will be needed to support these activities. Toolkits will be selected from commercial offerings (or developed when necessary) to enable user devices to determine what PKI products and services they require, and interact directly with the PKI to obtain them. The PKI PMO has established a Government-operated test facility at the DISA Joint Interoperability Test Command (JITC), where DoD organizations that do PK-enable their applications can verify (on a fee-for service basis) that the enabled applications are compatible with DoD's PKI capabilities. It will be necessary for developing organizations across the Department to take the initiative to enable their applications using these toolkits and test capabilities so that the Department can reach the full benefit that PK technology offers.

4.4 Technical Risks

The DoD PKI in particular, and the IA strategy overall, are predicated on the availability of acceptable COTS products and services. PK technology and commercial application standards are still evolving. This leads to increased technical risk that the DoD will not be able to meet all of its operational requirements, and that it will have cost and schedule impacts. Areas of technical risk are addressed below.

4.4.1 Scalability

As a PKI becomes larger, there is a risk that the PKI functions are not sufficiently extensible to satisfy DoD's large base of users, applications, and devices. The technology is still evolving, and solid technical data that describes how increasing the number of users affects the characteristics of the PKI does not exist. Certificate revocation, key recovery, registration, and directory access and management are functions that may become progressively more time consuming, more expensive, or less secure as the number of subscribers increases.

DISA and NSA are developing computer models to aid in the engineering, planning, and testing of the DoD PKI system. This modeling effort is being used to identify the scalability choke points for the basic PKI functions. Multiple sets of performance data will be analyzed to develop projections of the performance of the PKI during peak and average time periods. Performance reports, utilizing data collected from pilot efforts and automatic system performance reports will provide insight into the operational performance of the system for sizing and analysis purposes.

4.4.2 Interoperability

DoD relies heavily on interactions and coordination with external communities: military operations with Allies and Coalition partners; close working relationships with the Intelligence Community; coordinated operations with other federal Government agencies; and day-to-day business transactions with our business partners in the U.S. and abroad. Interoperability is fundamental to the Department's mission success, and since many of these communities operate their own PKIs, there is a risk that the PKI will not support the requisite interoperability. There are two basic issues associated with this interoperability: assessing the security implications of allowing two communities to interoperate, and the mechanisms that facilitate that interoperation (once it has been approved).

A Policy Management Authority (PMA) has been established to review the policies, practices, and procedures of external PKIs to determine if there is acceptable risk associated with enabling interoperability with them. The PMA has the authority to authorize interoperability. The existing IECAs (and the subsequent ECAs) are approved by the PMA to issue certificates, compatible with the DoD PKI to business partners and others outside DoD that are authorized.

Beyond that, the PKI established a number of elements to achieve interoperability. The DoD Class 3 PKI and the DoD PKI design is based on commercial standards, algorithms, and protocols to facilitate operation with external PKIs approved by the PMA. The Federal Bridge Certification Authority (BCA) is being developed as a component to interconnect to a broad range of PKIs that employ various commercial standards. Currently, it is envisioned that this capability will be incorporated into DoD's PKI capabilities. However, the BCA requires support from the Department of Commerce and NIST. NSA is supporting these activities to ensure that the operational capability will be available in the CI-1 timeframe.

DISA and NSA are actively working with the vendors and the standards communities to achieve standard specifications and implementations to improve interoperability. The DoD will ensure that DoD specifications are consistent with the emerging commercial and NIST Federal standards to support DoD interoperability requirements. The DoD PKI program will continue to track new and evolving IETF standards to ensure the most viable commercial standards are fully leveraged to support maximum interoperability in the future.

4.4.3 Transparency

Transparency has a direct bearing on user acceptance of the PK-enabled functions, as well as impacting the level of manpower needed to operate and sustain the infrastructure itself. Thus, the potential for not achieving transparency risks the acceptability of PKI technology across the Department. To ease any impact to operations, the security services associated with the use of the PKI should be as transparent as possible to subscribers and relying parties. The most effective way to reduce the manpower required to operate and support the PKI is for the PKI is to provide as much transparency of operations as is technically feasible and operationally acceptable. While some PKI operations will have to retain manual intervention (to ensure adequate security), transparency is being addressed in a number of areas. One such operation is the automation of the traditionally manpower-intensive accounting and auditing.

Beyond registration, much of the subscriber interaction can be assumed by PK-enabled applications. The PKI architecture recognizes PK-enabled applications that are capable of performing security functions using the certificates and related products available from the PKI. It also recognizes PK-aware applications that are capable of interacting directly (e.g., on-line) with the PKI to obtain requisite products and services automatically. This level of transparency requires that applications be configured appropriately, and that users accept that PKI interactions should be performed automatically (or perhaps with notification and approval of subscribers).

4.4.4 Security

Fundamental to the PKI is the need to ensure the overall security and assurance of its operations. As such, this is a fundamental focus to all aspects of its realization. There is a major risk that COTS components will not satisfy the Department's security requirements. NSA has established a Security Engineering Working Group specifically responsible for ensuring that the KMI/PKI architecture and concepts of operations are adequate to maintain that security and assurance. As the PKI architecture evolves, this group will establish security requirements, validate that the architecture appropriately addresses those requirements, and ensure that System Security Analyses are conducted on components and the overall system. The group will also verify that

components and the overall system (as required) are certified and accredited in accordance with DITSCAP, the DoD Information Technology Security Certification and Accreditation Process (Reference K).

The DoD X.509 CP is the overall security requirements document, identifying specific personnel, physical, procedural and technical security controls needed to achieve adequate levels of assurance. Certification Practice Statements (CPSs) are established to document the manner in which each element of the PKI will satisfy the requirements of the CP. The CPMWG, in support of the PMA, as discussed in Appendix A, retains technical responsibility for the analysis of the CP and CPSs. The PMA is responsible for evaluating the acceptability of CPs and CPSs of external PKIs to determine if interoperability is prudent. They are also responsible for evaluating similar capabilities for potential ECAs.

4.4.5 Directories

Applications may use directories to locate and retrieve certificates and certificate revocation information, and must be available and reliable at all times. The possibility of not having effective directory services risks the utility of PK technologies across the Department. The PKI and directory components must be designed, implemented, and deployed to support efficient population of the directories with PKI information. There are multiple directory efforts within the Department, and the PKI relies on access to them for its operation. These directories are also used to make other subscriber information (e.g., e-mail addresses, telephone numbers, and applicable policies) available. The DoD Class 3 PKI has established a directory for making available certificates and certificate revocation information. The existing PKIs each have established their own directory capabilities, with linkages to local directories where appropriate.

DISA has undertaken the Global Directory Services initiative to ensure that these multiple directory systems are integrated into an interoperable directory infrastructure and architecture that can be used across the DoD. It is intended that the DoD PKI will transition to the evolving DoD Global Directory Services when it is available, continuing to use the existing directory for the Class 3 PKI in the interim. The DoD Global Directory Services is an enterprise-level "meta-directory" system, currently in pilot implementation, that provides integrated access to these directory systems while allowing the owners to retain control of their data. While this effort is independent of the PKI initiative per se, this represents an area of potential risk. NSA and DISA are working closely together to ensure that the resultant directory structure offers adequate security features and functionality to properly support the DoD PKI needs. NSA and DISA are currently in the process of establishing a service level agreement for the interaction of the DoD PKI and the Global Directory Services to ensure that the security provisions and availability of operational capabilities remains compatible with the overall PKI evolution. The PKI PMO will continue to conduct periodic reviews of the Global Directory Service evolution to monitor its progress. Meanwhile, the existing Class 3 PKI directory capability will be sustained to support DoD PKI operations if necessary.

4.4.6 Transition

The risk of a cumbersome, demanding transition again jeopardizes the acceptability of PK technology within DoD. Ease of transition is a critical. The transition to the DoD PKI architecture will be evolutionary, as standards and technologies in the PKI area continue to evolve. Available technology and lessons learned from the current PKI activities (pilot medium assurance and FORTEZZA PKI efforts) will be inputs into the transition planning. Both the Class 3 and the existing (FORTEZZA-based) Class 4 PKIs will be maintained and service will be continuous until all of their subscribers are transitioned to the DoD PKI. Interoperability across the various

releases of the PKI will be maintained to ensure a smooth transition rather than a hard cutover from one release to the next.

4.4.7 Support for Tactical Operations

Tactical operations drive some of the most demanding requirements for PKI. There is a risk that the PKI capabilities cannot satisfy the requirements of this operational environment. These may include rapid mobilization, rapid compromise recovery, rapid addition of personnel, rapid changing of roles and granting of privileges, key recovery, support for remote subscribers and operations over low bandwidth communications, and radio silence required by tactical operations. While the DoD PKI supports many tactical requirements through the use of local CA servers, there are a number of issues concerning the completeness of the services provided by these capabilities. Since the tactical environment does not always provide easy access to the infrastructure elements (e.g., CA Servers, directory), services requiring such access may suffer.

Requirements for tactical operations are still being coordinated. Currently, the PKI PMO is considering concepts for reduced functionality versions (perhaps in different packaging or form factors) of PKI components, manager workstations, and related devices to support tactical operations. While the same basic functional and physical modularity will be retained for these nodes, it is likely that tailored features, protocols, and techniques may be needed to ensure that the PKI is fully responsive to the demands created by these environments. Architectures, concepts of operations, and where necessary, tailored capabilities and components will be provided by the PKI to ensure that it provides appropriate support for tactical operations. These engineering efforts are just now getting underway, and will be integrated as part of the overall PKI evolution as appropriate.

4.4.8 Support to OCONUS/Theater Operations

There are unique requirements associated with operating overseas, in potentially bandwidth-limited and security-challenged environments. There is a risk that the PKI cannot support mission operations in these theaters. To satisfy operational requirements, the PKI program must be able to deploy and operate capabilities in these theaters to ensure availability of services and maintain the integrity and security posture of the PKI products and services, and the infrastructure overall. DISA and NSA are currently studying this critical need and developing a strategy for satisfying these critical requirements.

4.4.9 Communications Capabilities

Currently there is limited communications bandwidth available within the networks used by the Department to support existing mission-critical operations. There is a risk that communications bandwidth that is needed to support PKI functions will not be available within the current communications infrastructure. While the PKI is designed to minimize any communications overhead associated with its use, there are a number of functions that inherently require some communications capability.

Both NSA and DISA are currently performing modeling and simulations of their operating scenarios with anticipated traffic projections to establish specific communications bandwidth requirements and assess the impact of the DoD PKI on the telecommunication/network infrastructure. Multiple sets of performance data will be sampled at different frequencies and will be analyzed to develop projections of the performance of the PKI during peak and average time periods. Analyses will continue to be performed to identify possible bottlenecks of the current system and ways to improve its performance. Scenarios such as user projections, stressed environments (e.g., crisis, wartime workloads), application projections, and the like will be modeled and performance data captured.

The PKI Program Team is also evaluating the use of commercial communications transport services that can reduce or eliminate demands on the available communications capacity. The Program will continue to work with DISA and other operational forces to ensure that the PKI is able to offer the services that are required without degrading mission critical operations across the Department.

5. ROLES AND RESPONSIBILITIES

There are a number of organizations involved in the design, development, acquisition, deployment, and operation of the evolving DoD PKI. This section highlights the roles and responsibilities for major activities associated with the PKI implementation, operations, and support. The DoD PKI Implementation Plan identifies detailed tasks and responsibilities associated with the realization of the PKI. This chapter highlights overall responsibilities.

5.1 Program Management

NSA, supported by DISA will continue to serve as the DoD PKI PMO, as directed by ASD C^3I, and provide coordination of activities across DoD to define and implement the DoD PKI. The PMO provides the leadership and coordination for all PKI activities across the Department, and is the single point of responsibility for all DoD PKI planning, development, and implementation activities. The DoD PKI PMO is responsible for overall program management of all DoD efforts required to execute this DoD PKI Roadmap. The PMO is also responsible for raising awareness across the Department of the value of PKI capabilities, the status of ongoing and planned PKI-related activities, and the support that is available for its effective use.

5.2 System Engineering

5.2.1 Security

NSA is responsible for defining the security architecture and security criteria for the DoD PKI. This includes defining the security criteria for the DoD PKI components and the overall operation. Commercial security products will be evaluated prior to acquisition consistent with the provisions of the NSTISSP Number 11 DoD CIO Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for Department of Defense Global Information Grid Information Assurance that references NSTISSP 11. These policies mandate that effective January 2001, preference be given to products that are in compliance with one of the following:

- International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement,
- National Security Agency/National Institute of Standards and Technology (NSA/NIST) National Information Assurance Partnership (NIAP) certified commercial laboratories, or
- NIST Federal Information Processing Standard (FIPS) validation program (Reference L).

By July 1, 2002, this requirement is mandated. Occasionally, NSA will perform security evaluations of commercial products. These evaluations are an acceptable replacement for any of the other compliance tests cited above.

As part of an overall Certification and Accreditation (C&A) process, NSA will conduct a System Security Assessment of each system configuration being deployed. This assessment will provide technical information needed to support the system certification, and will provide an important input to final accreditation and Approval to Operate. Operational commands will assume responsibility for maintaining the proper security configurations and adhering to the security requirements derived from the DoD X.509 CP for their specific capabilities. Periodically, NSA and DISA will coordinate to conduct independent audits of CAs, RAs, and LRAs to ensure their operations are in compliance with the requirements of the DoD X.509 CP and their approved

CPS(s), and in accordance with the DOD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

5.2.2 Functional and Operational

The PMO has ultimate responsibility for the establishment and coordination of PKI requirements. The PMO will coordinate with CINCs, Services, and Agencies to ensure that services required by users are available in a timeframe consistent with their needs. To ensure accurate documentation of user requirements, NSA and DISA will engage local and overseas representatives of the CINCs, Military Departments, subordinate commands, and other DoD Agencies to capture PKI requirements. DoD PKI user requirements have been documented and are being coordinated across the Department.

The PMO will be responsible for ensuring that the PKI is capable of delivering products and services in a timeframe consistent with subscriber needs. NSA, working with DISA, will coordinate with CINCs, Services, and Agencies to ensure that KMI (and PKI) services needed by users are available. NSA and DISA, supported by various members of the DoD community, will provide technical leadership to develop and maintain the PKI architecture, standards, specifications, and related documentation for the DoD PKI.

5.3 Interoperability

The DoD PKI PMO will ensure that the DoD PKI is able to interoperate securely both within DoD and externally with other Federal Government organizations, Allies, coalition forces, and business partners. The PMO must address technical challenges, as well as ensure that the necessary policies, practices, and procedures are in place to advance interoperability.

NSA and DISA will participate in various standards bodies and consortia in the commercial sector and with external constituents including the Intelligence Community, NATO, other Allies, and those of Federal Government Agencies to ensure that an effective means is available to provide interoperability when the need dictates.

5.4 Development, Integration, and Test

NSA will lead any required research and development efforts for the PRSN, CSN, and PSNs associated with the PKI. DISA will provide PKI technical leadership for specific PKI elements of the KMI architecture. These include the Root, CAs, RAs, and LRAs. Additionally, NSA in conjunction with DISA, the Services and industry partners will develop specifications for commercial PKI products that may be used in the DoD PKI.

NSA will lead the integration of the PKI Root. DISA will lead integration of the remaining centralized components, the CA servers and PKI-specific Directory components. Additionally, DISA will also retain responsibility for the DoD Global Directory Services that will provide a critical capability for the PKI evolution, but is external to the PKI evolution itself. DMDC will continue to take responsibility for upgrades to the RAPIDS LRAs (and associated enhancements to the DEERS system).

Development of PK-enabled applications is not within the purview of the PKI program; however, they are critical for the success of the overall PKI investment by the Department. The Services and Agencies are responsible for PK enabling of their specific custom applications. These applications must adhere to the DoD PKI specifications to utilize the DoD's PKI services. The PMO is responsible for ensuring the availability of requirements documentation, toolkits,

technical guidance and a facility for conducting interoperability testing of PK-enabled applications. Support beyond this, and funding are not included within the scope of the DoD PKI initiative.

The PKI PMO will identify toolkits (or ensure they are available) to facilitate this enabling and customer support for programs and vendors that are actually performing the enabling. DISA will lead activities to identify and evaluate the effectiveness of commercial PKI toolkits. NSA will take the lead for developing specialized toolkits needed to address specific requirements that cannot be satisfied by commercial offerings. DISA JITC has been established as a PK-enabled applications test facility for developers and integrators to verify compliance and compatibility of their implementations with the PKI. The DoD Services and Agencies will retain responsible for enabling of their applications and devices to be compatible with the PKI capabilities, including the funding needed to maintain and operate the test facilities.

The DoD Access Card Office (ACO) is responsible for the development and upgrade of RAPIDS terminals to incorporate the functionality and establish operations needed for them to serve as LRAs for the PKI. The Defense Manpower Data Center (DMDC) performs the RAPIDS development activities for the ACO.

5.5 Procurement/Acquisition

The PKI PMO will assume overall responsibility for procuring, or directing the procurement of the centrally operated infrastructure elements. The PKI PMO will develop the acquisition strategy for the DoD PKI. NSA, working in conjunction with the DoD PKI PMO and DISA will procure, develop, or direct the procurement of the centrally operated infrastructure elements of the KMI. NSA is responsible for the procurement and deployment of the KMI Type 1 functionality. DISA will be responsible for the procurement and deployment of centralized Directory elements of the PKI. The DoD PKI PMO will develop the acquisition strategy for the DoD PKI, the certificate management components and services. DISA will lead integration of the centralized components of the PKI, including the CA servers and Directory components. The Services and Agencies will procure local infrastructure elements, PKI RA and LRA workstations and local directories.

5.6 Operations

The DoD PKI allows for flexibility in management and operation of the related PKI components. Although placement of the centralized and decentralized components needs to be finalized, the requirements for their management and operations are detailed in the DoD X.509 CP. The CINCs, Services, and Agencies that operate PKI equipment will acquire appropriate operator training on the policies and proper use of the equipment. CINCs, Services, and Agencies that operate PKI equipment will acquire appropriate training for their operators on the policy and proper use of the equipment. The PMO, working with the Services, will develop the training material for any equipment that they develop.

5.6.1 Root CA(s) and the CSN

NSA will manage and operate the DoD Root, its associated PSN, and the CSN.

5.6.2 CA Servers and Other Centralized PKI Components

DISA will be responsible for the operation of the centralized certificate management and directory services (with the exception of the PKI Root). Responsibility for the operation of PRSNs

and the PSNs will be shared between NSA and DISA. DISA will lead the integration and operations of the centralized certificate management and directory services. For CINC, Service, and Agency unique or tactical applications, management and operation of those specific CA Servers is the responsibility of the appropriate CINC, Service, or Agency. Operational responsibilities for the regional and deployable PRSNs and PSNs have yet to be established.

5.6.3 RAs, LRAs and Other Local PKI Components

The CINCs, Services, and Agencies will be responsible for manning the registration sites, including the RAs, LRAs, SVOs, and VOs as well as any CINC, Service, and Agency local directories. Support will include registration, audit review, maintenance, and policy enforcement, operating a help desk, compromise recovery, re-key, and key recovery.

5.6.4 Help Desk

The PMO will ensure that adequate Help Desk capabilities exist, consistent with the deployment of PKI products and services across the Department. The help desk capabilities will build on existing help desk facilities available within each organization. NSA, DISA, and DMDC will augment those capabilities to ensure that adequate customer support capabilities exist. It is expected that customer support capabilities will be both manned and unmanned. An additional (manned) help desk capability will be established at JTIC to provide assistance to organizations that are PK-enabling applications.

5.7 Oversight

In February 1999, the DoD CIO approved the implementation plan for the Defense-wide Information Assurance Program (DIAP). The DIAP forms the Department's core organizing element for achieving a more comprehensive, coherent, and consistent IA program. It implements a process designed to provide for centralized planning, coordination, integration, and oversight of the Department's IA resources while retaining decentralized execution to realize continuous improvement in our IA posture. The DIAP's central coordination and oversight activities enable the Department to develop, validate, and prioritize DoD-wide IA requirements, determine the overall return of our IA investments, and objectively assess DoD's Defense-in-Depth efforts to protect information assets critical to the Department. This oversight will apply to all DoD PKI activities.

The DoD PKI Senior Steering Committee, previously referred to as the DoD PKI Steering Group, is the Department's PKI implementation authority. Reporting directly to ASD C^3I, they perform the functions highlighted in Appendix A. Currently there is a separate Joint Key Management Infrastructure Working Group (JKMIWG) that performs similar functions for what has been traditionally the Department's Electronic Key Management System (EKMS). Recognizing the close linkage of PKI within the broader KMI, these groups will be merged during 2001 to ensure that high level planning for both of these critical capabilities remain coordinated across the Department.

Appendix A – Policy Management

The Policy Management process described in this appendix defines the manner in which DoD certificate policies will be approved and modified, and ensure that the policies are correctly implemented. This process is depicted pictorially in Figure A-1.

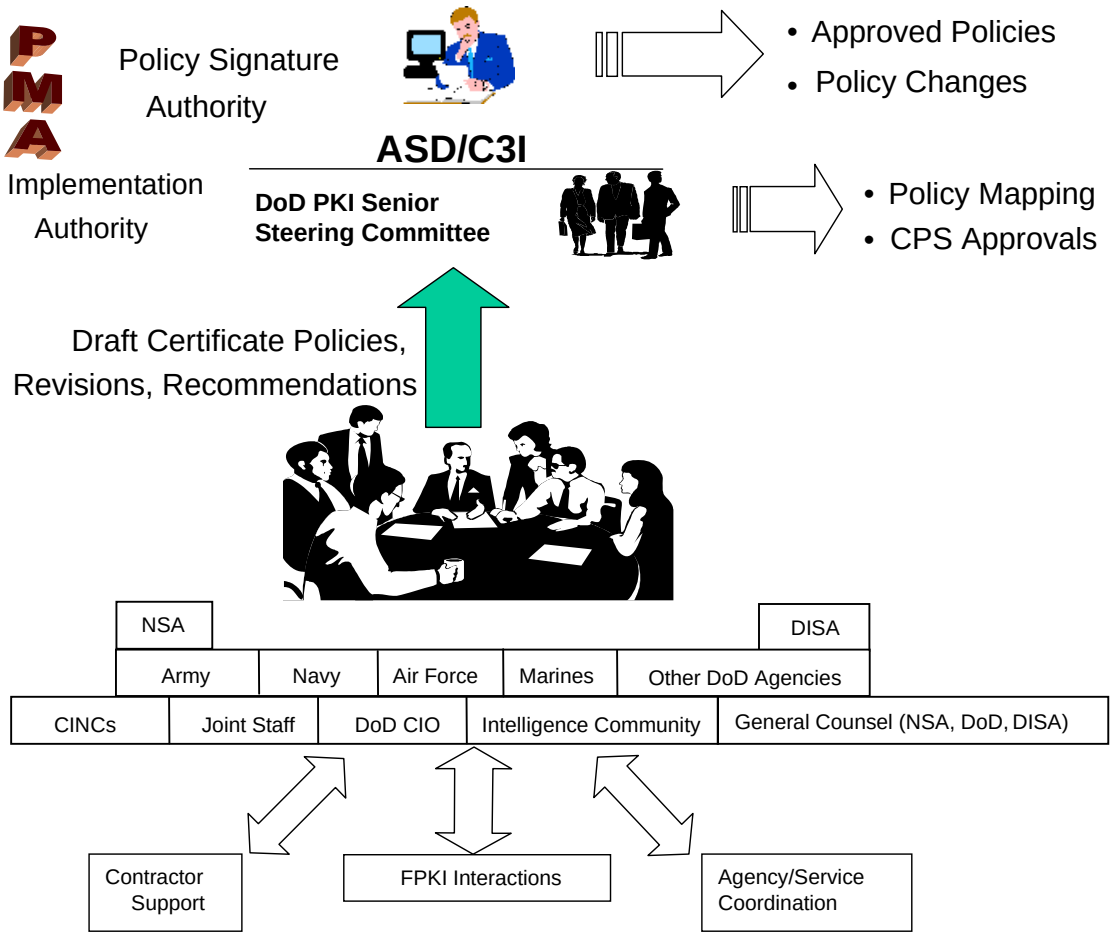

Figure A-1. DoD Certificate Management Process

Policy Management Authority

ASD C³I is the Department of Defense PK Certificate Policy Management Authority (PMA) for the DoD Certificate Policies (CPs). NSA has been designated as the Program Manager for the DoD PKI with DISA as the Deputy Program Manager.

Specifically, **ASD C³I** will:

- Approve the DoD CPs
- Review, coordinate, and promulgate changes to the DoD CPs.

The DoD PKI Senior Steering Committee will:

- Draft DoD CPs and any recommended changes to the CPs;
- Review Certification Practice Statements (CPSs) to ensure that they meet the requirements of DoD CPs;
- Review the CPs of external organizations with which the DoD PKI is considering cross-certification or otherwise certifying and make recommendations to the ASD C³I concerning which external security policies may be considered equivalent to DoD policies;
- Recommend to higher-echelon CAs that certain CA certificates be revoked, based on non-compliance with the CPs; and
- Issue formal statements to CAs to cease issuing certificates asserting DoD policies, should these CAs not comply with the DoD CPs.

The DoD PKI Program Manager will chair the DoD Steering Group. The following organizations shall be represented: NSA, DISA, Services, JCS, and ASD C³I.

Certificate Policy Management Working Group (CPMWG)

The DoD PMA will establish a Certificate Policy Management Working Group that will be responsible for advising the PMA to ensure that the DoD Certificate Policies are appropriate to the needs of the Department, and evolve to meet new operational and technical developments. Specifically, the CPMWG will:

- Evaluate suggested modifications to the policies from the DoD, Services and Agencies
- Generate, coordinate, and maintain a Certificate Policy Planning Document that describes the DoD approach to evolving the DoD Certificate Policy
- Provide a mechanism to facilitate the timely, responsive, DoD, Service and Agency coordination and buy-in to the DoD CP through a consensus-building process
- Ensure legal review is obtained for the CP and any modifications
- Review the Certification Practice Statements (CPS) of DoD-operated CAs and commercial CAs that offer to provide services to the DoD. The CPMWG will analyze the CPS documents to ensure that the practices of CAs serving the DoD comply with the DoD CP, and provide the analysis to DOD PKI Steering Committee
- Analyze Federal, allied, commercial and other certificate policies with respect to DoD certificate policies for purposes of establishing the suitability of the non-DoD policies for use within the DoD (for example, in cases where the technical mechanism of "policy mapping" is being considered) or for purposes of determining the possible interoperability of the DoD and the non-DoD system
- Ensure that DoD certificate policies evolve to remain consistent with appropriate Federal, commercial, allied and international standards and practices. In particular, the DoD CPMWG will establish a liaison with the Federal PKI Legal and Policy Management Working Group
- Review the results of CA audits to determine if the CAs are adequately meeting the requirements of approved CPS documents. Make recommendations to the CAs and to the DOD PKI Steering Committee regarding corrective actions or other measures that might be

appropriate, such as revocation of CA certificates

- Offer recommendations to DOD PKI Steering Committee, DoD Program and Project Managers, and DoD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the various DoD certificate policies for specific applications
- Otherwise respond to the direction of the DOD PKI Steering Committee to provide CP advice as required.

The DoD PKI Program Management Office will chair the CPMWG. The following organizations shall be represented on the CPMWG: NSA, DISA, the Intelligence Community, General Counsel, CINCs, Services, and Agencies, Office of the Joint Staff, Office of the DoD Chief Information Officer and other organizations as the PMA may direct.

Each organization may optionally provide operational, legal and technical representatives to the CPMWG as requested by the PMA or the CPMWG. Each member of the CPMWG (*except for the Legal Counsel*) represents all of the interests of their agency or department, and is responsible for coordinating a unified agency/department position on issues being considered by the CPMWG. CPMWG members must have the authority to speak on behalf of their agency or department.

The CPMWG will be expected to rely on the support of working-level personnel within the agencies represented on the CPMWG. Contractor support provided by the organizations represented on the CPMWG may also be used for such tasks as evaluating CPSs against the requirements of CPs, and evaluating policies of potential cross-certification partners. The CPMWG will meet on an as-needed basis. CPMWG recommendations will be by consensus. If consensus cannot be achieved, then the CPMWG will prepare a position paper and/or briefing for the PMA describing the issues involved, and the various points of view, and the PMA will make the final decision.

Appendix B – Definitions

Access	Ability to make use of any information system resource.
Access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Assurance levels	The level of assurance of a PK certificate is the degree of confidence in the binding of the identity to the public keys and privileges. Personnel, physical, procedural and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. DoD has identified the following assurance levels. *Class 3*: This level is intended for applications handling medium value information in a low to medium risk environment. *Class 4:* This level is intended for applications handling medium to high value information in any environment. *Class 5:* This level is intended for applications handling high value information in a high-risk environment.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Binding	Process of associating two related elements of information.
Certification Authority (CA)	An entity authorized to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate. Additionally the CA is responsible for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certification Practice Statement (CPS)	A statement of the practices that a certification authority employs in managing and issuing certificates in relation to a specific Certificate Policy.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Digital Signature	A transformation of a message using an asymmetric cryptographic system and a hash function such that a person having the initial message and the signer's public key can accurately determine if the transformation was created using the corresponding signer's private key. In addition, it can be determined if the initial message has been altered since the transformation was made.
Directory	The directory is a repository or database of certificates, CRLs, and other information available online to users.
Encryption Certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Integrity	Protection against unauthorized modification or destruction of information.
Key Management Infrastructure (KMI)	The framework and services that provide the generation, production, distribution, control, tracking and destruction for all cryptographic key material, symmetric keys as well as public keys and public key certificates.
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	The person who is responsible to the CA for local (onsite) identification of users' identity.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate.
Technical Non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
Token	A physical device (e.g. floppy diskette, smart card, PC Card, etc.) which is used to protect and transport the private keys of a user.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific object existed at a particular time.

References

A. Public Key Infrastructure Implementation Plan for the Department of Defense, Version 3.1, dated 18 December 2000.

B. U.S. DoD X.500 Certificate Policy (CP), Version 5.2, dated 13 November 2000.

C. OASD (C3I) Memorandum, Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI), dated April 9, 1999, Washington, D.C.

D. Deputy Secretary of Defense Memorandum, Department of Defense (DoD) Public Key Infrastructure (PKI), dated May 6, 1999, Washington, D.C.

E. DoD Chief Information Officer Memorandum, Department of Defense (DoD) Public Key Infrastructure (PKI), dated August 12, 2000, Washington, D.C.

F. KMI 1011: Key Management Infrastructure Roadmap for the Department of Defense, Draft, dated October 30, 2000.

G. Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for Department of Defense Global Information Grid Information Assurance

H. IA Technology Framework (Companion Document to Reference G, above).

I The Common Criteria for Information Technology Security Evaluation (CC), Version 2.1 / ISO IS 15408, dated October 5, 1999.

J National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products. January 2000.

K. Department of Defense DoD Instruction 5200.40, DoD Information Technology Security Certification & Accreditation Process (DITSCAP), dated 10 February 1998.

L. Federal Information Processing Standard (FIPS) Publication 140-1, dated January 11, 1994.

Abbreviations and Acronyms

ACO	Access Card Office
API	Applications Programming Interface
ASD C^3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
BCA	Bridge Certification Authority
C&A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CAW	Certification Authority Workstation
CI	Capability Increment
CINC	Commanders-in-Chief
CIO	Chief Information Officer
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPMWG	Certificate Policy Management Working Group
CPS	Certification Practice Statement
CSN	Central Services Node
DEERS	Defense Eligibility Enrollment Reporting System
DIAP	Defense-wide Information Assurance Program
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMDC	Defense Manpower Data Center
DMS	Defense Messaging System
DoD	Department of Defense
ECA	External Certification Authority
EKMS	Electronic Key Management System
FIPS	Federal Information Processing Standard
IA	Information Assurance
IATF	Information Assurance Technology Framework
IECA	Interim External Certification Authority
IETF	Internet Engineering Task Force
IT	Information Technology
JCS	Joint Chiefs of Staff
JKMIWG	Joint Key Management Infrastructure Working Group
JITC	Joint Interoperability Test Center
KMI	Key Management Infrastructure

LAN	Local Area Network
LRA	Local Registration Authority
MGS	Medium Grade Services
MISSI	Multilevel Information Systems Security Initiative
NIAP	National Information Assurance Partnership
NIPRNet	Unclassified IP Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMO	Program Management Office
PRSN	Primary Services Node
PSN	Production Source Node
RAPIDS	Real-time Automated Personnel Identification System
RA	Registration Authority
S/MIME	Secure Multipurpose Internet Mail Extension
SIPRNet	Secret IP Router Network
STE	Secure Terminal Equipment
STU-III	Secure Telephone Unit – Third Generation
SVO	Super Verifying Official
VO	Verifying Official
WAN	Wide Area Network