

UNCLASSIFIED

DEPARTMENT OF DEFENSE
TARGET PUBLIC KEY INFRASTRUCTURE
OPERATIONAL REQUIREMENTS DOCUMENT
20 AUGUST 2001

V51
NATIONAL SECURITY AGENCY
9800 SAVAGE ROAD, SUITE 6734
FT. GEORGE G. MEADE MD 20755-6734

UNCLASSIFIED

TABLE OF CONTENTS

PREFACE	1
1 GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY	4
1.1 SUMMARY OF MISSION NEED.....	4
1.2 OVERALL MISSION AREA.....	6
1.3 DESCRIPTION OF PROPOSED SYSTEM	6
1.4 SUMMARY OF OPERATIONS AND SUPPORT CONCEPTS	12
1.4.1 <i>Operations Concepts</i>	12
1.4.1.1 Subscriber Registration	12
1.4.1.2 PK-Enabled Application Operation.....	15
1.4.2 <i>Support Concepts</i>	16
1.5 BENEFITS OF EVOLUTIONARY ACQUISITION	17
2 THREAT AND PROJECTED THREAT ENVIRONMENT	19
3 SHORTCOMINGS OF EXISTING SYSTEMS AND C4ISR ARCHITECTURES	21
3.1 GENERAL DISCUSSION	21
3.2 SHORTCOMINGS	21
4 CAPABILITIES REQUIRED	23
4.1 SYSTEM PERFORMANCE	23
4.1.1 <i>Generate Public Key Certificates</i>	24
4.1.2 <i>Supply Public Key Certificates</i>	25
4.1.3 <i>Support Multiple Cryptographic Algorithms And Algorithm Migration</i>	25
4.1.4 <i>Provide Key Pairs And Certificates</i>	25
4.1.5 <i>Program Subscriber Tokens</i>	26
4.1.6 <i>Distribute PKI Root Certificate</i>	26
4.1.7 <i>Support Subscriber Mobility</i>	26
4.1.8 <i>Provide Registration Process</i>	26
4.1.9 <i>Provide Renewal, Update, & Re-key Processes</i>	27
4.1.10 <i>Provide Revocation Processes</i>	27
4.1.11 <i>Recover From Compromise</i>	28
4.1.12 <i>Provide Key Recovery Services</i>	29
4.1.13 <i>Support Tactical Operations and Environment</i>	29
4.1.13.1 <i>Support Connected Tactical Networks</i>	29
4.1.13.2 <i>Support Closed Tactical Networks</i>	30
4.1.13.3 <i>Support Subscriber Mobility For Tactical Requirements</i>	30
4.1.14 <i>Maintain PKI-Generated Security Objects Archive</i>	30
4.1.15 <i>Generate Trusted Time Stamps</i>	31
4.1.16 <i>Provide PKI Interoperability</i>	31
4.1.17 <i>Support Enterprise-Level Access Control</i>	31
4.1.18 <i>Provide Implementation Aids</i>	32
4.1.19 <i>Provide Help Support</i>	32
4.2 INFORMATION EXCHANGE REQUIREMENTS.....	32
4.2.1 <i>Interactions With Subscribers and Device Administrators</i>	33
4.2.2 <i>Interactions with Tokens and PK-Enabled Devices</i>	33
4.2.3 <i>Interactions with PK-Enabled Applications</i>	33
4.2.4 <i>Interactions with Other PKIs</i>	33
4.2.5 <i>Interactions with Authoritative Personnel Databases</i>	33
4.2.6 <i>Interactions with DII Directories</i>	33
4.2.7 <i>Interactions with Time Reference Sources</i>	33
4.2.8 <i>Interoperability KPP</i>	34
4.3 LOGISTICS AND READINESS.....	34
4.3.1 <i>CA Availability</i>	34
4.3.2 <i>Continuity of Operations</i>	34

UNCLASSIFIED
DoD Target PKI Operational Requirements Document

4.4	OTHER SYSTEM CHARACTERISTICS.....	35
5	PROGRAM SUPPORT.....	37
5.1	MAINTENANCE PLANNING	37
5.1.1	<i>PKI Server Hardware.....</i>	<i>37</i>
5.1.2	<i>PKI Software Maintenance.....</i>	<i>37</i>
5.1.3	<i>PKI Communications.....</i>	<i>37</i>
5.1.4	<i>Card Reader Maintenance.....</i>	<i>37</i>
5.2	SUPPORT EQUIPMENT.....	38
5.3	C4I/STANDARDIZATION, INTEROPERABILITY, AND COMMONALITY	38
5.3.1	<i>Integration into C4ISR Infrastructure</i>	<i>38</i>
5.3.2	<i>Data fusion</i>	<i>39</i>
5.3.3	<i>Unique Intelligence Information.....</i>	<i>39</i>
5.3.4	<i>Use with NATO and Allies.....</i>	<i>39</i>
5.3.5	<i>Technical and Procedural Interfaces.....</i>	<i>39</i>
5.3.6	<i>Compliance with DoD Joint Technical Architecture.....</i>	<i>40</i>
5.3.7	<i>Global Command and Control System (GCCS) and Common Operational Picture (COP).....</i>	<i>40</i>
5.3.8	<i>Information Assurance.....</i>	<i>40</i>
5.3.9	<i>Energy Standardization and Efficiency.....</i>	<i>41</i>
5.3.10	<i>Electronic Environmental Effects and Spectrum Support.....</i>	<i>41</i>
5.4	COMPUTER RESOURCES	41
5.5	HUMAN SYSTEMS INTEGRATION (HSI).....	41
5.5.1	<i>Training.....</i>	<i>42</i>
5.6	OTHER LOGISTICS AND FACILITIES CONSIDERATIONS	43
5.7	TRANSPORTATION AND BASING.....	43
5.8	GEOSPATIAL INFORMATION AND SERVICES	44
5.9	NATURAL ENVIRONMENTAL SUPPORT	44
6	FORCE STRUCTURE.....	45
7	SCHEDULE.....	46
8	PROGRAM AFFORDABILITY	48
	APPENDIX A: REFERENCES.....	48
	APPENDIX B: DISTRIBUTION LIST	52
	APPENDIX C: LIST OF ORD SUPPORTING ANALYSES.....	53
	FOCUS GROUPS.....	53
	SECURITY FUNCTIONS OF SUPPORTED APPLICATIONS	53
	GLOSSARY	57
	ABBREVIATIONS AND ACRONYMS	63
	TABLES	66
	ORD KPP SUMMARY.....	66
	IER MATRIX	68

LIST OF FIGURES

Figure 1: Elements of Defense In Depth.....	1
Figure 2: Elements of Public Key-Based Information Assurance	2
Figure 3: Components of the DoD PKI	7
Figure 4: PKI Operational View (OV-1 / SV-1).....	9
Figure 5: PKI Registration	13
Figure 6: PK-enabled Operations.....	15
Figure 7: Key PKI Dates and PKI Release Schedule	47

DEPARTMENT OF DEFENSE
 TARGET PUBLIC KEY INFRASTRUCTURE
 OPERATIONAL REQUIREMENTS DOCUMENT
 31 MAY 2001

Preface

This Operational Requirements Document (ORD) defines and describes the requirements for the Department of Defense (DoD) Target Public Key Infrastructure (PKI)¹. 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 war fighting 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. As shown in Figure 1, PKI is a supporting infrastructure in the Defense in Depth strategy. PKI is a vital element for a secure IA posture for the Defense Information Infrastructure (DII). PKI responds to the requirement in the IA Implementation Guidance for the Global Information Grid (GIG) [Reference 38] to “provide a cryptographic infrastructure that supports key, privilege and certificate management; and that enables positive identification of individuals utilizing network resources.”



Figure 1: Elements of Defense In Depth

¹ Throughout this document, the term “PKI,” unless otherwise qualified, refers to the DoD Target PKI as defined in the PKI Roadmap.

The DoD Target PKI will support a broad range of public key (PK) enabled applications and support cost effective security interoperability between DoD and its Federal, Allied and commercial partners while minimizing degradation to operations. The DoD Target PKI is intended to support both the Non-classified IP Router Network (NIPRNet) and Secret IP Router Network (SIPRNet) environments. Over time, applications currently supported by the DoD Class 3 PKI and the FORTEZZA PKI are expected to migrate to the Target PKI.

PKI supports the ability of PK-enabled applications and devices to identify and authenticate individual users, devices, or processes; to provide source authentication and integrity protection for information transactions; and to establish end-to-end encrypted channels between PKI subscribers; and, to provide information confidentiality and/or community of interest segregation. The security capabilities supported by PKI supplement, rather than replace, the protections provided by current encryption techniques, such as link encryption. PKI, of and by itself, is inadequate to protect classified information, and must be used with traditional Type 1 cryptographic systems for such implementations. Traditional Type 1 cryptographic systems and devices will continue to have broad applicability in DoD systems.

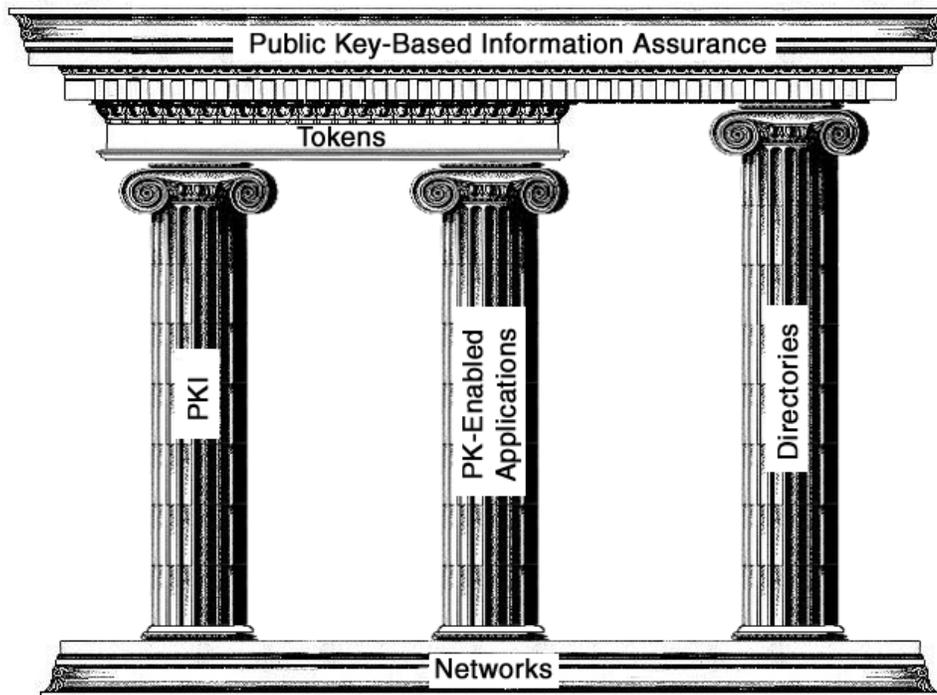


Figure 2: Elements of Public Key-Based Information Assurance

Figure 2 illustrates the four major elements involved in the implementation of public key-based information assurance. These elements are:

- **PKI.** PKI provides certificate management services, including subscriber registration, certificate generation, certificate revocation list (CRL) management, and archiving and recovery of private encryption keys. PKI also provides certain on-line security services, such as certificate status checking and generation of trusted time stamps, that may optionally be used by PK-enabled applications as part of their security processing.

- **DoD Directories.** PKI-generated information, such as public key certificates and CRLs, must be available to relying parties, in order for those relying parties to validate certificates. PK-enabled applications typically retrieve the information needed from the directories as part of their routine processing. The DoD PKI will use available directories (e.g., the DoD Global Directory Services [GDS]) as the primary means for publishing and distributing certificates and CRLs.
- **Tokens.** Tokens are used to store the subscriber's private key and certificate, and to perform cryptographic functions such as digital signature generation. DoD policy, documented in the X.509 Certificate Policy [Reference 2] requires the use of Federal Information Processing Standard (FIPS) Publication 140-1 [Reference 32], Level 2 cryptography for Class 4 assurance. The DoD intends to use smart card technology to fulfill this requirement. A Smart Card program is underway within DoD, and a Smart Card ORD is under development [Reference 39]. The DoD PKI will use the DoD Common Access Card (CAC) as the primary subscriber token for unclassified private key storage. A similar FIPS 140-1, Level 2-compliant smart card token will be used for NIPRNet subscribers who do not receive the CAC. SIPRNet subscribers will use a token that complies with FIPS 140-1, Level 2, in accordance with the DoD Certificate Policy. Devices certified by the DoD PKI may use alternate means to meet the FIPS 140-1, Level 2 requirement.
- **PK-enabled Applications and Devices.** The actual security processing) of subscriber information is performed by PK-enabled applications and devices, which invoke and control the cryptographic services of tokens in order to perform digital signature generation and verification, data encryption, data decryption, and other cryptographic functions. Because the DoD is seeking to implement a single, standards-based, broadly-used PKI, the enabling of applications and devices to implement public key-based security services is being handled as a separate initiative; the Assistant Secretary of Defense (Command, Control, Communications) (ASD C3I) published a memorandum on 17 May 2001 [Reference 42] specifying policy for development and deployment of PK-enabled applications. In implementing security services, PK-enabled applications and devices interface with directories to retrieve PKI-published information, with subscriber tokens to invoke cryptographic services, and (optionally) with PKI on-line services where those services meet a particular application's and/or device's performance and security requirements.

The PKI, directories, and PK-enabled applications and devices communicate via existing DoD communications networks such as NIPRNet and SIPRNet.

The PKI Program Management Office (PMO) is being restructured to add PKI integration and operations oversight to its current responsibilities for PKI implementation. This oversight responsibility will enable the Director of the PKI PMO to ensure PKI applications, directory services, middleware, tokens and readers, are in-place and tested to support the required operational timelines and customer expectations.

This document only addresses the requirements for the DoD PKI. Tokens, directories, and PK-enabled applications are treated as external components (for the purposes of this ORD), and appropriate requirements to interface with those components are included in this ORD. However, this ORD does not contain functional or performance requirements that apply only to tokens, directories, or PK-enabled applications.

1 General Description of Operational Capability

1.1 Summary of Mission Need

DoD is one of the world's largest users of electronic communications and transmitters of electronic message traffic. This electronic communication is transacted with a variety of organizations. Communications within a service and across the services are vital to all DoD missions. Additionally, communications with non-governmental organizations, state and local governments, and other federal agencies are increasingly common, especially when performing missions associated with military operations other than war. Technological advances giving rise to electronic commerce are leading to increased electronic communications with vendors and others outside of military-only data paths.

Numerous sources have identified threats to DoD information and documented attacks against DoD information systems. A May 1996 report [Reference 6] by the General Accounting Office (GAO) found: "Attacks on Defense computer systems are a serious and growing threat. ... [T]he number of attacks is doubling each year, as Internet use increases along with the sophistication of 'hackers' and their tools. ... At worst, [these attacks] are a serious threat to national security. ... The potential for catastrophic damage is great." In September 1998, the Deputy Secretary of Defense (DEPSECDEF) issued a policy memorandum regarding "Information Security and the World Wide Web" [Reference 40] that documented concerns about the security risks of DoD information on publicly accessible web sites, and directed the ASD(C3I) to "accelerate the development and implementation of an architecture which enhances the protection of sensitive but unclassified information."

Joint Vision 2020 is the guiding document for the evolution of America's Armed Forces to meet the challenges of the future. At the heart of Joint Vision 2020 is the concept of Full Spectrum Dominance, which depends heavily on Information Superiority. The Defense-wide Information Assurance Program (DIAP) annual report for Fiscal Year 2000 states:

Information superiority is at the very foundation of our vision of modern warfare, and Information Assurance (IA) is essential to achieve and maintain this superiority. IA is an integral part of Joint Vision 2020 and the ability to integrate intelligence, command and control, and battlefield awareness functions into joint and combined operations. IA is also an essential element in implementing protection of critical national infrastructures as mandated by the Presidential Decision Directive 63, Critical Infrastructure Protection.

The guiding vision of the ASD(C3I) is the establishment of information superiority, and ASD(C3I) has established a number of goals that support that vision. Among these goals are:

- Implement effective programs for establishing information assurance and critical infrastructure protection (ASD(C3I) Goal #2)
- Build a coherent Global Information Grid (ASD(C3I) Goal #3)

- Promote electronic business/electronic commerce (EB/EC) and business process change throughout DoD. (ASD(C3I) Goal #8)

PKI is an enabling technology that supports these goals. This is recognized in the GIG CRD, which calls for robust information assurance capabilities in GIG systems. In particular, the GIG CRD requires GIG systems to “utilize/interoperate with security management and the DoD public key infrastructure (Threshold),” and to “provide proof of origin and receipt as required (Threshold),” a capability for which public key cryptography is an enabler.

Responding to the threats to sensitive but unclassified information and the capabilities needed to achieve information superiority in support of Joint Vision 2020, DEPSECDEF issued a memorandum in May 1999, updated in August 2000 by the DoD Chief Information Officer (CIO) [Reference 1], regarding the development and implementation of a Department-wide PKI. The memorandum identifies a common, integrated, interoperable PKI as an important element of the Defense-in-Depth strategy for IA, serving as a foundation for IA capabilities across the Department, and providing general-purpose PKI services to a broad range of applications. Among the requirements set forth in that memorandum are the use of PKI to control access to private DoD and DoD-interest web servers and to unclassified networks hosting mission critical systems. The policy mandates a transition to a Class 4 level of assurance for that protection by December 2003. The policy also encourages wide-spread use of public-key enabled applications in both classified and unclassified environments. In response to the guidance in the memorandum, this ORD defines requirements for PKI support on NIPRNet and SIPRNet.

In today’s environment of sophisticated weaponry and rapid global force projections, the Defense Information Infrastructure (DII)’s highly interconnected nature dictates security measures be integrated across Commander in Chief (CINC), Service, Agency, regional command lines, and where necessary, privately owned resources, including the Internet. These security measures must be applied coherently to all of the DII’s individual elements. The PKI, when employed in conjunction with PK-enabled applications, security tokens such as the DoD CAC, and DoD network and directory infrastructures, supports the provision of security services by PK-enabled applications:

- Data integrity
- Digital signature capability
- Authentication of remote users
- Data confidentiality
- Non-repudiation

The infrastructure must support, among other technologies, email systems, file transfer functions, database transactions, access to Web servers, electronic file management, object code signing, multimedia collaboration, virtual private networking, network single sign-on, and other applications, including command and control (C2) systems and combat support systems. PKI provides the framework and services that provide for the secure creation, distribution, control, and management of public key products, primarily X.509 certificates. PKI includes the Registration Authority (RA) workstations, the Certification Authority (CA) servers, the archives for key retrieval, and the processes for subscriber registration and token programming. PKI is an enabling infrastructure and as such supports the operation of PK-

enabled software applications, and devices. A fully interoperable and functional PKI is the cornerstone of IA for the DII. Implementation of the DoD Target PKI will enable common security implementations among DoD information processing systems.

1.2 Overall Mission Area

PKI provides IA support services for the Command, Control, Communications, Computers, Intelligence (C4I) mission area. This operational requirements document supports the FY 2001-2005 Defense Planning Guidance (DPG), Part II, responding to Asymmetric and Transnational Threats. Specifically, this guidance requires, "Information technologies, including protection measures to control adversary access to critical information systems, countermeasures to contain adversary Information Operations (IO) effects, and restoration capabilities to reestablish information system functions." Additional DPG programming guidance is found in the IA portion of the Information Superiority Section of the Modernization area. This requirement is supported by Joint Publication 3-13 [Reference 9] and DoD Directive S-3600.1, [Reference 10].

1.3 Description of Proposed System

PKI, as defined in the DoD PKI Roadmap, refers to the framework and services that provide for the generation, production, distribution, control, revocation, recovery, and tracking² of PK certificates and their corresponding private keys. The DoD PKI, operating in concert with directories and tokens, will support registration of subscribers, dissemination of certificates, and a full range of certificate management services. 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.

PKI will provide an integrated public key infrastructure that supports a broad range of government and commercially-based, security-enabled applications, and shall provide for secure interoperability within DoD and with its federal, allied and commercial partners while minimizing overhead and impact to operations. It will be developed in accordance with DoD's Defense in Depth, layered IA strategy. To achieve these objectives, PKI will apply layered security which will enable DoD to minimize government off-the-shelf (GOTS) developments and leverage existing commercial PKI technology, standards, and services.

² Tracking here refers to maintaining record of issuance and ownership of public key certificates and public/private key pairs. It is needed, for example, to ensure that all certificates issued to a particular subscriber can be identified and revoked if necessary.

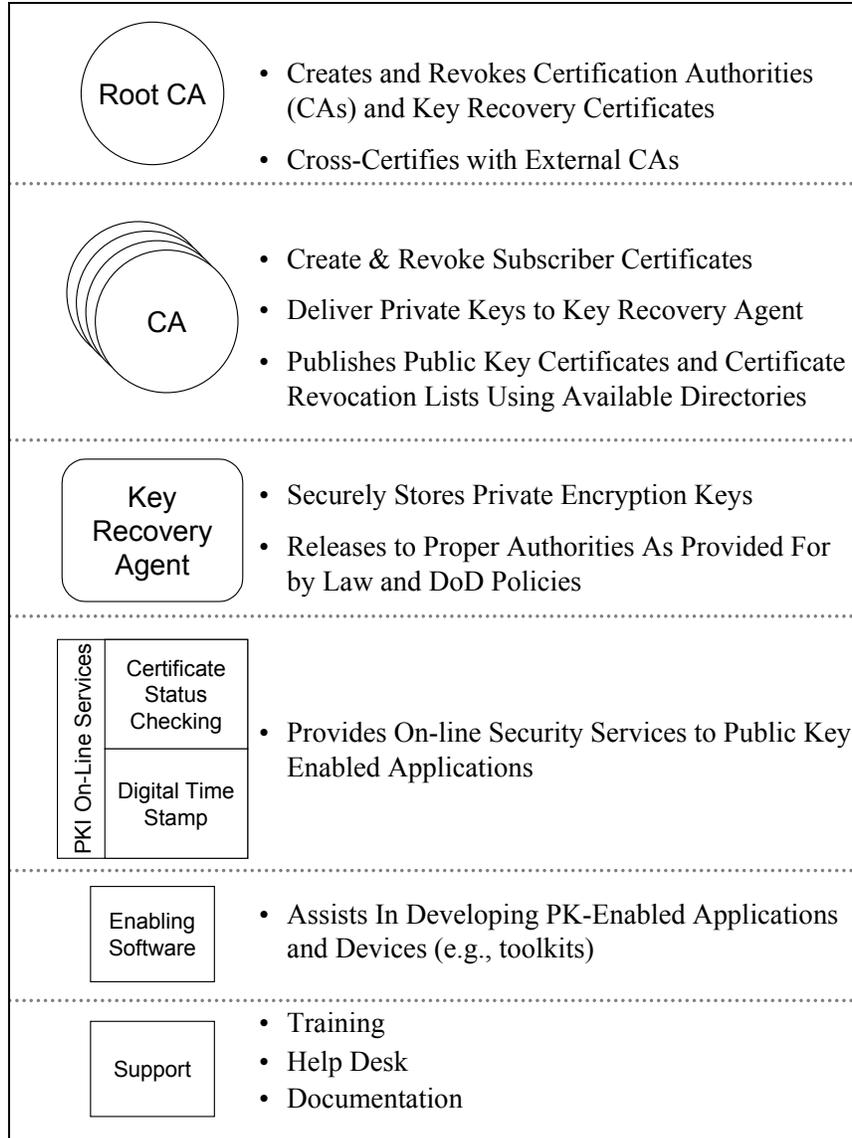


Figure 3: Components of the DoD PKI

The components of PKI are identified in Figure 3. The successful implementation, deployment, and use of PKI requires these elements, and also depends on the supporting components described in the Preface (i.e., tokens, directories, PK-enabled applications). This ORD presents the requirements for the PKI components identified in Figure 3:

- **Root Certification Authority.** The PKI root CA is an off-line element that certifies the on-line CAs that perform certificate and CRL management functions. A common root CA is used to certify the CAs for both the unclassified and classified domains (i.e., NIPRNet and SIPRNet).
- **Certification Authorities.** The CAs perform the core PKI functions: generation of public key certificates and CRLs. The CAs interact with registration management capabilities embedded in Real-time Automated Personnel Identification System (RAPIDS) workstations and with other registration authority workstations. The

certificates and CRLs generated by the PKI CAs are published using available directory services.

- **Key Recovery Agent (KRA).** The KRA provides secure storage for private encryption keys, and technical and procedural security measures to control the release of those keys. Key recovery may be needed both to reconstitute operational capabilities for PKI subscribers (e.g., if a token is damaged) and for law enforcement purposes.
- **On-line Services.** The on-line services provide capabilities that can be invoked by security-enabled applications, if appropriate to the needs of the application. These services provide an alternative means for certificate verification, and the ability to apply a verifiable time stamp to a block of data.
- **Enabling Software.** Enabling software (e.g., software toolkits) provides reusable implementations of common processing needed for PK-enabled applications. Examples of functions that may be supported by a toolkit are verification of a public key certificate, digital signature generation, and digital signature verification. The availability and use of common enabling software will facilitate the enabling of applications to take advantage of PKI, and will simplify the creation of interoperable PK-enabled applications.
- **Support.** PKI support includes training, documentation, and help desk capabilities to assist PKI subscribers, PKI operators, and PK-enabled application developers in taking maximum advantage of the security capabilities supported by PKI.

The requirements for tokens, directories, and PK-enabled applications are being developed separately from, but in concert with, the PKI requirements.

PKI will be implemented largely through the acquisition of commercial off-the-shelf (COTS) components to perform CA and KRA functions, provide on-line services, support help desk operations³, and supply enabling software for use in PK-enabling applications and implementing RA functionality. The CA, KRA and help-desk support functions will be integrated with a COTS web-based front-end interface that will be tailored to provide well-structured access to PKI capabilities and balance the operating load among the CAs. This collection of components will be replicated and deployed in multiple locations as needed to provide adequate PKI capacity and to support DoD elements worldwide. Initially, the CAs, and web front-end will be located in existing DoD facilities with strong physical security and high-capacity connectivity to NIPRNet and SIPRNet (e.g., a Defense Enterprise Computer Center - Detachment [DECC-D])⁴. The PKI components in a DECC-D will be replicated to provide parallel NIPRNet and SIPRNet support; for security reasons a single set of components will not be used to support both networks. Eventually, one or more sets of these components may be deployed in OCONUS locations or configured in a manner that can be deployed to support tactical operations.

³ If appropriate, the PKI help desk may be integrated with other, existing help desks rather than separately implemented.

⁴ The root CA is an off-line function and requires stringent physical security protections. The root CA will be located in an NSA-operated, high-security facility, rather than in a DECC-D.

COTS components used to implement the PKI and boundary protection between the PKI components and the network they support must be National Information Assurance Partnership (NIAP)-approved against applicable protection profiles for that component type. PKI components will interface to the NIPRNet and SIPRNet using DoD- and open, industry standard protocols, including Transmission Control Protocol and Internet Protocol (TCP/IP), hypertext transfer protocol (HTTP), network time protocols, and certificate enrollment, management and status protocols. PKI components will interface with available directories (e.g., GDS) using industry standard directory protocols, such as the X.500 family of protocols, Lightweight Directory Access Protocol (LDAP), or comparable protocols supported by the directories. PKI components, including boundary protection components used to ensure security isolation of the PKI components from the networks they support, must be NIAP-approved against appropriate protection profiles.

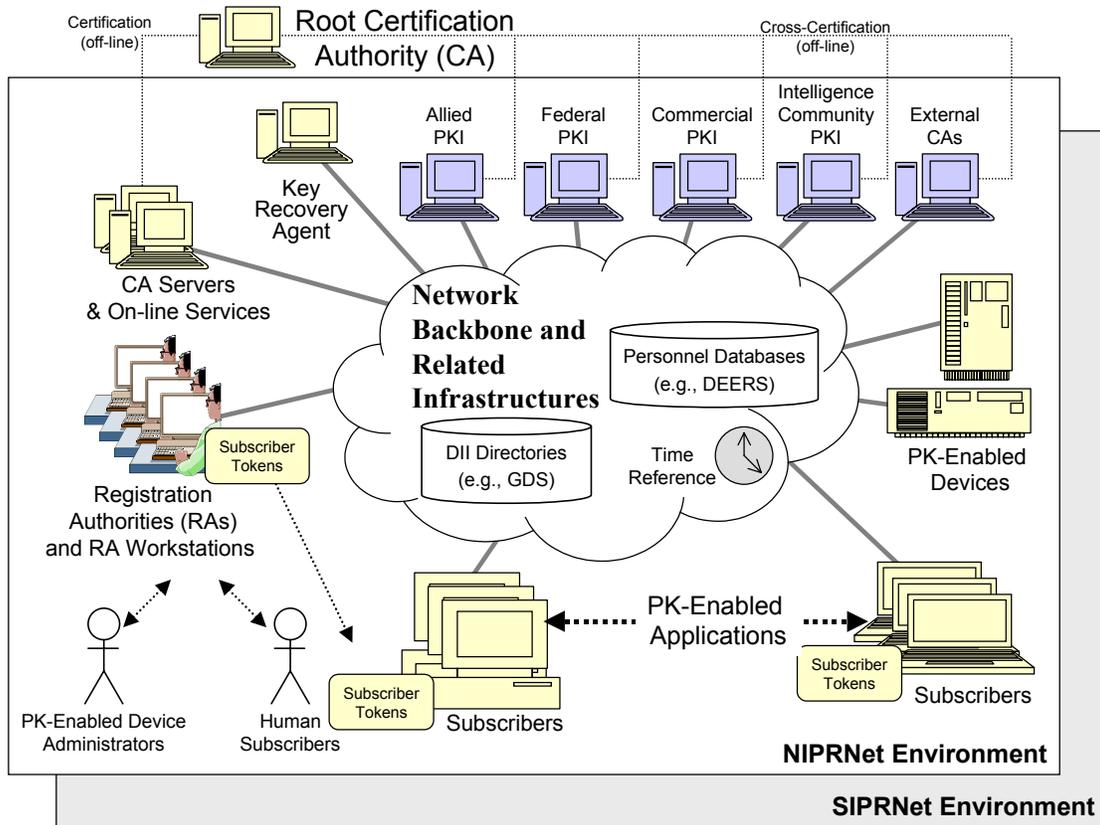


Figure 4: PKI Operational View (OV-1 / SV-1)

Figure 4 provides an operational view of the PKI. As shown, PKI will provide separate, parallel infrastructures in the unclassified and classified domains. The use of a common root and the movement, with suitable controls, of registration and path validation information between the two domains, will support PK-enabled applications that need to be interoperable across classification domains. The root CA can also certify and be certified by other PKIs, such as the Federal Bridge CA, and Allied, commercial, and Intelligence Community PKIs. Such cross-certifications will be implemented after review of the operational requirements

and security implications. Once implemented, the existence of the cross-certification enables the exchange of secured traffic. For example, a recipient operating under a Federal agency's PKI would be able to verify the digital signature on a message sent by a DoD PKI subscriber.

As show in the figure, CA servers and KRAs will be accessed via the network (i.e., NIPRNet or SIPRNet) backbone. Other PKI elements, such as RAs, will use the network backbone to gain access to CA services. The PKI will also connect to other infrastructures such as directories, personnel databases (e.g., DEERS), and time references via the network backbone. Since these other infrastructure elements are not part of the PKI, they are depicted within the network cloud.

Highly sensitive PKI elements such as the CAs and the KRAs may be located in centralized locations such as a Defense Enterprise Computer Center - Detachment (DECC-D), or in other locations as needed to support operational requirements. CA servers and KRAs must be located where they can be provided strong physical security protection.

PKI registration management will be decentralized. RAs and supporting workstations will be located where required, and will interact with the PKI CA servers through the network backbone. RAs will use their workstations to program subscriber tokens. PKI registration functions will be included in the RAPIDS workstation so that PKI registration can be integrated into the process of issuing DoD CACs. Other RA workstations will be used for registering subscribers who do not carry the CAC, and for registering applications and devices.

PKI subscribers use their tokens with PK-enabled applications. The tokens provide the cryptographic functions and access to private keys needed by PK-enabled applications to implement public key-based security services. Devices can also be registered and receive public key certificates, enabling public key-based security to be applied to interactions among devices and between devices and PK-enabled applications. The PKI will provide standards-based, general purpose identity and encryption certificates that can be used by a broad range of applications and devices. Over time, the PKI will evolve as dictated by operational need to provide additional certificate types such as network access certificates and possibly attribute certificates.

PK-enabled applications interact directly, applying public key-based security services to those interactions. Where appropriate and supportable by the operating environment of a particular application, the application may take advantage of one or more on-line services as part of the application's implementation of security for its information. These applications may include PKI-supplied enabling software as part of their implementation of public key-based security services.

For a PKI to be successful, it must have a number of basic characteristics:

- **Enhanced Security.** The DoD PKI will provide the security and assurance needed to ensure operational integrity for C2, Mission Support, and e-Business uses. The PKI will be built on authentic, universally accepted identities for all subscribers, operators, and devices, with standard toolkits that ensure the integrity of all PKI-relevant operations.

- **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 in all environments, including fixed facilities, garrison/office environments, afloat, aloft, and in deployed/tactical situations. The DoD PKI has to support all of these activities. The PKI must effectively and economically support multiple PK-enabled applications and devices.
- **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.
- **Scalability.** By capitalizing on scalability, economies in the deployment and operation of the infrastructure are achieved by allowing each subscriber to communicate with diverse and even remote parties.
- **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. Standards are essential to achieve many of the other requirements especially within a diverse and widespread infrastructure. PKI must employ, to the greatest extent possible, an open standards approach based on commercial products and services that can keep pace with technological rollover and the constantly evolving new applications and standards inherent in the information technology (IT) environment. PKI must comply with DoD standards included in the Joint Technical Architecture (JTA) [Reference 20] and other appropriate documents. PKI will support FIPS-compliance requirements. It must also comply with international standards, such as International Standards Organization (ISO)/International Telecommunications Union (ITU), and commercial standards, such as the IETF and World Wide Web Consortium (W3C), as appropriate.
- **Transparency.** PKI must function across a variety of hardware and software operating environments, and 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.
- **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, will be deployed in phases, introducing new

features and capabilities in an orderly fashion, consistent with commercial technology progression. Enhanced system capabilities will be introduced in parallel with existing operational capabilities, with no hard cutover whenever feasible.

- **Modular Design.** The DoD PKI has adopted the highly modular, nodal architecture of the evolving DoD Key Management Infrastructure (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.
- **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).

Eventually, nearly all DoD employees will need PKI services to support their daily activities. These services are becoming increasingly important in networked environments where communications and transactions occur over unsecured channels. The need for confidentiality and integrity for automated capabilities (e.g., attachments to emails, electronic exchange between classification levels, imagery, voice, video and digital signature) can be provided by cryptography, and those cryptographic mechanisms need the support of PKI.

1.4 Summary of Operations and Support Concepts

The core functions of PKI are subscriber registration and certificate management. This section provides a summary of the operational concepts for subscriber registration, and an illustration of the operation of a PK-enabled application. In the case of the PK-enabled application, depending on the specifics of its implementation of security services, there may be no direct interactions between the application and the PKI during the normal operations of the application. Further general information about PKI operational concepts can be found in the Class 3 PKI (Release 3.0) Concept of Operations (CONOP) [Reference 35], KMI 2012 Operational View for Capability Increment 1 (CI-1) [Reference 36], and KMI 2112 System Description for CI-1 [Reference 37].

1.4.1 Operations Concepts

1.4.1.1 Subscriber Registration

PKI employs centralized certificate management and decentralized registration. A primary goal of PKI is to integrate PKI registration into existing personnel processes to improve efficiency, minimize the number of specialized components or processes, and minimize the number of personnel needed to perform PKI registration functions. For example, PKI registration functions will be included in the RAPIDS workstation so that PKI registration can be integrated into the process of issuing DoD CACs⁵.

⁵ The PKI Program Management Office is working with the sponsor of RAPIDS to enhance the security of the RAPIDS workstation and to integrate it into the KMI environment so that it can properly meet the Class 4 PKI registration requirements.

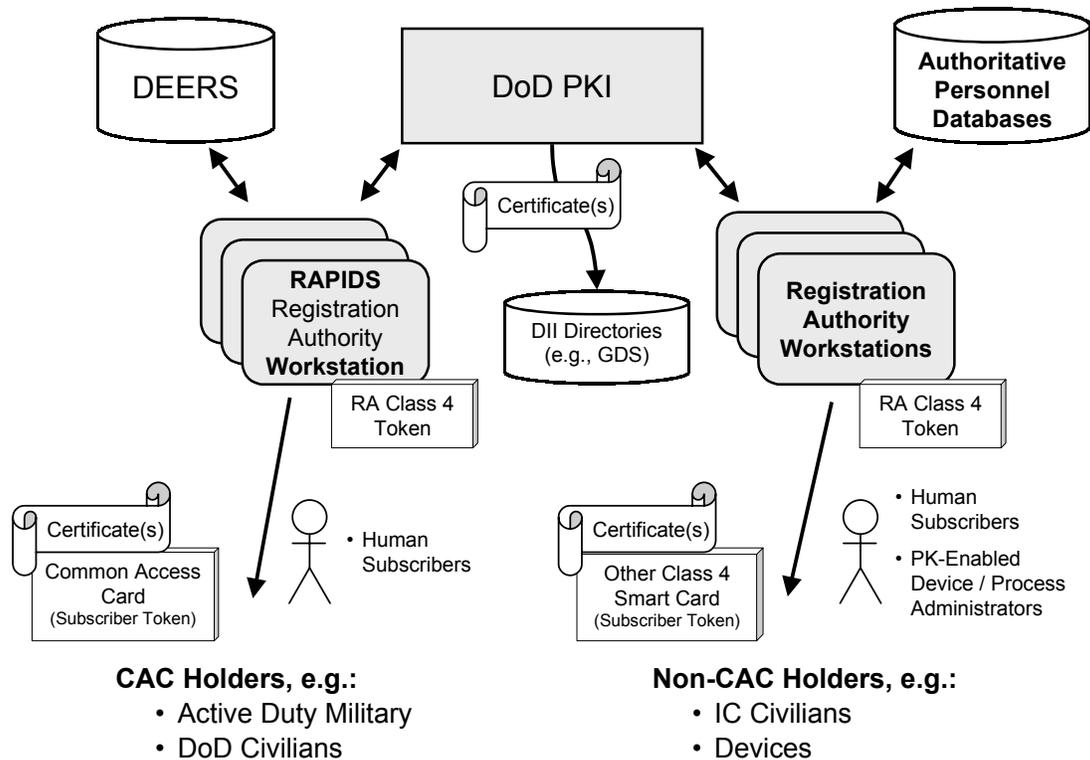


Figure 5: PKI Registration

Figure 5 provides a registration view of the PKI. DoD PKI subscribers present themselves in person to a RA in order to have their identity verified and to become enrolled in the PKI. Subscribers may be either human subscribers or devices (who will be represented to the RA by the appropriate responsible party). Which RA the subscriber interacts with depends on both the subscriber and the environment. PKI will provide registration capabilities in both the NIPRNet and SIPRNet environments.

- In the NIPRNet environment:
 - Human subscribers who are eligible to carry a DoD CAC (e.g., uniformed military personnel) will be registered at a RAPIDS workstation. Their identity verification will be based on the information in the Defense Enrollment Eligibility Reporting System (DEERS) database. Once the subscriber's identity has been verified, the RAPIDS workstation operator or verifying official (i.e., the RA) interacts via the RAPIDS workstation with a PKI CA and the subscriber's token to generate a public/private key pair and a corresponding public key certificate. This registration process results in an unclassified PKI identity certificate being issued, with the corresponding private key on the subscriber's CAC.
 - Human subscribers who do not carry a CAC (e.g., intelligence community personnel) will be registered through a PKI RA workstation that is not integrated into a RAPIDS terminal. Where available, authoritative personnel databases other than DEERS, such as agency-specific employee databases,

will be used to verify subscriber identities. Such use of personnel databases is not required, but is intended to facilitate the PKI registration process. This registration process results in an unclassified PKI identity certificate being issued, with the corresponding private key on the subscriber's smart card token.

- Devices are registered through a PKI RA workstation. Device registration procedures and the resulting products will depend both on the procedures used by the organization responsible for the device and the device type.
- In the SIPRNet environment:
 - All human subscribers will be registered through a PKI RA workstation. Where available, personnel databases other than DEERS will be used to verify subscriber identities. This process results in an unclassified⁶ SIPRNet PKI identity certificate being issued, with the corresponding private key on the subscriber's smart card token.
 - Devices are registered through a PKI RA workstation. Device registration procedures and the resulting products will depend both on the procedures used by the organization responsible for the device and the device type.

Separate tokens and identity certificates will be used for the NIPRNet and SIPRNet environments⁷. The certificates issued to the subscriber are published to the directory on the NIPRNet or SIPRNet. PKI will replicate NIPRNet certificate and revocation information to the SIPRNet to support applications that must operate through both environments.

Once the subscriber has received an identity certificate in an environment, he may use that to authenticate his identity to the PKI and request additional certificates, such as an encryption certificate, in the same environment. When PKI generates an encryption certificate, a copy of the corresponding private key is also delivered to a KRA to support key recovery requirements.

RA workstations can be deployed where needed to support PKI registration requirements. The RA workstation will need communications to a PKI CA. Registration can thus be conducted in both fixed and tactical / deployed environments, provided that adequate communications are available between the RA workstation and a CA. PKI must support PKI subscriber, and PK-enabled applications and devices worldwide in all DoD operational locations. To satisfy this requirement, CAs will be established in facilities and locations both with and outside the continental United States, as needed, to facilitate adequate connectivity and operational response/support. In addition, as PKI evolves, CAs may be fielded in tactical/deployed environments, as needed to facilitate adequate connectivity and operational response/support.

⁶ While SIPRNet certificates are used to protect classified information, the certificates themselves are unclassified.

⁷ The current DoD policy, documented in DoD 5200.28-STD, requires that the same certificate cannot be used for both classified and unclassified systems (even though a certificate is unclassified) and that the tokens will be separate (those used on classified and those used in unclassified systems). Tokens are "contaminated" through contact with the classified computer system, in accordance with DoD policy on classified computer media.

1.4.1.2 PK-Enabled Application Operation

The actual protection of information is handled by PK-enabled applications and systems, using the product that result from subscriber registration (e.g., certificates) and other PKI operations (e.g., CRLs). These PKI products facilitate the implementation of security services by PK-enabled applications to protect information while stored or transferred between systems. The availability of PKI facilitates the implementation of security services by PK-enabled applications and devices. The use of a common DoD PKI facilitates interoperability between different PK-enabled applications by providing a common foundation for the implementation of security services by those applications.

During the enabling of an application, the implementer must decide the most appropriate way for that application to use the capabilities enabled by PKI. These decisions are based on the application's operating environment, the nature of its information transactions, the sensitivity of the information processed, and other considerations. This section describes typical events during the operation of a PK-enabled application, but cannot take into account the requirements and environment of every potential PK-enabled application.

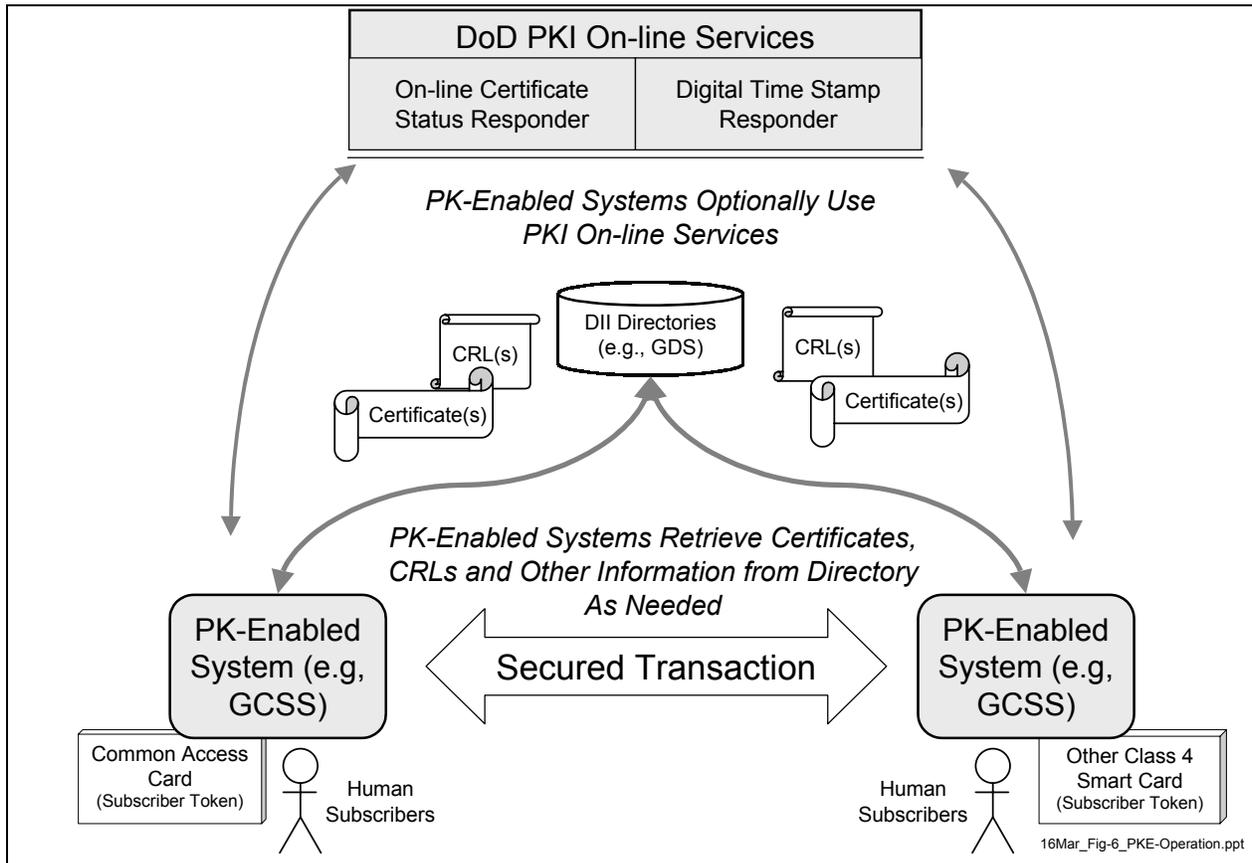


Figure 6: PK-enabled Operations

Figure 6 provides a view of PK-enabled application or devices operations, and the interactions that PK-enabled applications or devices may have with the PKI. During the operation of PK-enabled applications or systems, the primary interactions are among the application, the subscriber token, and the directory system:

- The application performs its information processing, formatting, and communications functions, and performs security processing as described in Appendix C.
- The token performs cryptographic functions, such as digital signature generation, that require use of the subscriber's public or private keys stored in the token.
- The directory serves as a source of information, such as certificates and CRLs, needed by the application to perform its security processing functions.

The application's information transactions (e.g., exchange of formatted information blocks or electronic mail messages) will be protected by the addition of public key-based security protections, such as the application of a digital signature, but are otherwise similar to the transactions the application would employ if not PK-enabled. The application implementer may elect to use one or more PKI on-line services such as certificate verification or trusted time stamp generation, if those services fit the requirements and operating environment of the application. The PKI does not, however, generate certificates or keys directly for the application as part of the application's normal transactions.

An application receiving digitally signed information needs to verify the identity certificate of the originator. An application needing to send encrypted information must retrieve and verify the encryption certificate of each recipient. When verifying certificates, the application is acting as a "relying party." As a relying party, the application will typically retrieve one or more certificates and CRLs from the directory in order to perform verification processing on the certificates of interest. The application may maintain copies of certificates and CRLs in a local cache to enhance performance and reduce network traffic. The implementer must determine if and how caching will be performed as part of PK enabling the application.

1.4.2 Support Concepts

PKI support considerations fall in two broad areas: CA and other centralized component support, and registration authority and subscriber support.

- CAs, KRAs and other core PKI components will primarily be located in fixed facilities (e.g., DECC-D Chambersburg and Denver) or in other locations with strong network connections and support infrastructures, such as network management centers. Support for these components will be obtained through the same mechanisms used to support other DoD information technology systems based in those locations.
- RA and subscriber support will be provided through a PKI help desk.

To minimize investment and overhead costs, consideration will be given to outsourcing PKI support for the protection of unclassified mission support, format sensitive, administrative, and selected mission critical data, to commercial service providers. Such providers must meet the DoD's security and functional requirements and be more cost effective than a DoD managed and operated system.

To ensure secure interoperability between DoD and its vendors and contractors, interoperability will be accomplished in the near term using External Certification

Authorities (ECAs). These ECAs will be established through a process that ensures a comparable level of trust to certificates issued by DoD PKI. ECAs will be approved by DoD CIO, in coordination with the DoD Comptroller and the Office of the Secretary of Defense (OSD) General Counsel in order to ensure this comparable level of trust. The DoD Target PKI will eventually achieve secure interoperability with non-DoD entities through a process called “direct cross certification,” which establishes a policy and process for recognizing third party CAs, or through an evolving concept like the Federal Public Key Infrastructure (FPKI) Bridge Certification Authority (BCA). Achieving this objective is dependent upon maturation of existing commercial applications and standards.

1.5 Benefits of Evolutionary Acquisition

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 IT environment. In addition, 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.

Notwithstanding the need for a commercially-based acquisition model, PKI strategy recognizes and takes into account the relatively immature state of commercial PKI products and standards. This translates into potential operational, cost, or schedule risks requiring workarounds to satisfy necessary security and operational functions. By definition, this implies an incremental, evolutionary approach to achieving PKI.

The benefits of such an approach are:

- Reduces up-front costs
- Allows incorporating emerging technologies as they appear
- Supports incremental adaptation to a new way of doing business
- Reduces the risk of major redesigns and the need for additional funding, as this technology matures
- Provides time for DoD community comment and buy-in

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 CIs every 18-24 months. The DoD PKI will be implemented as an integral part of DoD’s KMI evolution. Beginning with KMI CI-1, 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. The specifics of PKI evolution will be guided by operational

priorities, resources considerations, and the evolution of PKI technology. Current plans for the PKI capabilities to be provided at each PKI Release / KMI CI can be found in the DoD PKI Roadmap [Reference 3].

The PKI strategy is to pursue the earliest possible adoption, and to actively participate with industry to obtain the detailed technical understanding needed to fully specify requirements, resolve standards issues, and accelerate industry-wide convergence to a purely standards-based, interoperable capability which is not dependent on vendor-specific capabilities or technologies. Additionally, all PKI Commercial off-the-shelf (COTS)/GOTS acquisitions will comply with the National Telecommunications and Information Systems Security Committee's (NSTISSC) National Policy Governing the Acquisition of IA and IA-enabled IT Products [NSTISSP 11][Reference 11].

2 Threat and Projected Threat Environment

The threat posed to electronic communications within the DoD is varied and complex. The need for a PKI is derived from the need to defend our electronic communications and computing systems from acts such as blocking (denial of service), interception, tampering, destruction (data integrity), and forgery.

The nature of the threat varies widely across a wide spectrum of potential threat sources. These include hackers, disgruntled insiders, information warriors, foreign intelligence activities, terrorists, organized crime, industrial spies, etc. The actions of threat agents may be aided by careless or sloppy security behaviors of legitimate system users. Clearly, the nature and severity of the threat posed by these various communities varies with their motivations, resources, level of access, and risk tolerance. A successful attack against an electronic system will contain the following elements: 1) gather information on the system to identify exploitable vulnerabilities; 2) gain the necessary access to target the system; and 3) execute the attack. This scenario applies in general to the threat against all IT systems and to the electronic exchange of critical information in particular.

The typical way in which organizations prevent a potential threat's access to a target system is through the access control. Organizations must determine who, what, and why to grant access to its assets or information based on the trusted identity of the user and the user's assigned function in the organization. The trust in the identity of the user is currently based on paper documentation in possession of the users. In the virtual world, access control is ensured through layered security mechanisms such as passwords, file permissions, encrypting system information, boundary control and detection devices, etc. Unfortunately, password only-based measures to establish trust are not sufficient to establish the stronger trust relationships required in modern electronic operations / business models. In order to securely share information, conduct electronic commerce, etc., a more robust method of ensuring the trusted identity of the user is required. Without such trust, DoD electronic systems are vulnerable to the threat discussed above. The need for a PKI to facilitate trust is in response to this threat.

The threat environment for IT systems is abstract and difficult to define. The attack techniques vary by the different potential threat sources mentioned above. A typical/routine threat to everyday usage of IT systems to transmit critical information among DoD elements is the vulnerability to eavesdropping which denies confidentiality of data. Eavesdropping can be performed by industrial spies, hackers, or foreign intelligence gatherers. In times of crisis or confrontation, or if hostilities break out involving United States (US) forces, the threat environment would rapidly evolve to destructive information warfare targeted against IT systems and infrastructure, to include computer network attack (CNA), traditional electronic attack (EA) and destruction.

Commercial lines of communications and satellite resources (KA/KU/C Band) are placing increased vulnerabilities on DOD Information Systems. This increase will require additional requirements for protective measures. Specifically; deception/corruption, denial/loss of information, physical destruction/damage, and exploitation of system tasking/configuration all increase in an environment that relies heavily on COTS equipment and the utilization of

commercial satellite resources. Detailed information on the threat to military and commercial based IO and satellite systems can be found in:

- Naval Command, Control, Communications, Computers, Navigation, and IFF Systems (U), ONI-TA-099-99, April 2000 (SECRET/NOFORN), and
- Threats to Network Centric Warfare (U), ONI-1573-001-00, October 1999 (SECRET/NOFORN)."

Additional related Automated Information Systems (AIS) threats are addressed in:

- Automated Information Systems Threat Environment Description (TED), NAIC- 1574-0210-00, September 2000, (S/NF);
- Electronic Warfare Threat Environment Description (TED) NAIC-1574-0731-01, October 2000, (S/NF);
- Worldwide: Threats to Network centric Warfare (U) ONI-1573-001-00, (S//NF/X1).

Threats to military satellite communications segments can be found in the

- MILSATCOM System Threat Assessment Report (STAR) (U) , NAIC-1574-0367-00 October 2000, (S//NF), and
- NAVSTAR Global Positioning System (GPS) System Threat Assessment (STAR) (U), NAIC-1574-0407-00 October 2000.

Finally, regardless of the prevailing national security threat situation, IT systems are always vulnerable to alteration or destruction by disgruntled insiders or “non-traditional” threats such as organized crime or terrorists.

The PKI developed to address the threat laid out above must be capable of operating in a variety of usage and threat environments and withstanding a broad spectrum of attack styles.

3 Shortcomings of Existing Systems and C4ISR Architectures

3.1 General Discussion

Historically, DoD encryption requirements were developed independently of commercial efforts and implemented for a specific system. Today, it is recognized that a traditional, government-sponsored development and implementation process will not be able to keep pace with the DoD's commercially-based technology and services strategy. DoD must look to "employ an open standards approach, based on commercial products and services that can keep pace with the technology rollover . . . while still maintaining appropriate levels of security."⁸

With PKI being a new capability, the majority of current DoD systems are not PKI compatible. Information that needed to be protected was classified and the systems and networks handling classified and mission critical information were closed to public access and controlled exclusively by the Federal Government.

Today, there has been a dramatic increase of public access to DoD systems and mission critical information is often being handled on unclassified networks. These systems are managed by a variety of governmental and commercial personnel. The majority of DoD systems utilize commercial carriers for their primary communications path. Sensitive, unclassified information (e.g. Social Security numbers, privacy act, Freedom of Information Act [FOIA]-exempt) is being sent via NIPRNet and the Internet, with little or no protection.

3.2 Shortcomings

The DoD Chief Information Officer Memorandum, Department of Defense Public Key Infrastructure [Reference 1], mandates that DoD transition the existing PKI capabilities, remain focused on commercial technologies and continue to strive to reach Class 4 assurance levels for all appropriate DoD electronic transactions. The assurance levels are defined in the X.509 Certificate Policy (CP) for the United States Department of Defense [Reference 2].

Current PKI capabilities (Class 3) provides protection for handling unclassified medium value information in moderately protected environments, unclassified high value information in highly protected environments, and discretionary access control of classified information in highly protected environments. These capabilities do not meet the DoD security requirements for handling high value unclassified information (Mission Critical, National Security System Information [NSSI]) in minimally protected environments.⁹

Existing systems that perform PKI functions are highly diversified. The myriad of interfaces that are maintained, including those within DoD, government civilian agencies, vendors and contractors, foreign nationals, allies, and other non-governmental organizations, means there is no guarantee of system interoperability.

⁸ Public Key Infrastructure Roadmap for the Department of Defense [Reference 3], p. 9.

⁹ See "X.509 Certificate Policy for the United States Department of Defense" [Reference 2] for the definitions of low, medium, and high value information and minimally, moderately and highly protected environments.

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

With over 3.5 million DoD employees (active military, reservists, and civilians), current PKI capabilities do not provide DoD with a global access to specific user/device information. Additionally, current PKI capabilities do not provide digital signature services for unclassified mission critical or national security information in an unencrypted network. The capability to perform object signing (e.g., for mobile code) trusts between objects and their signatures does not exist under the current infrastructure. Technical non-repudiation for large value financial or electronic commerce applications are also not available under the current PKI.

Failure to field the PKI will significantly constrain the DoD's ability to provide flexible security and access control, particularly for unclassified but sensitive information on the NIPRNet. While PKI is not, and should not be seen as, a universal solution to network security challenges, it provides a uniquely flexible capability to identify and authenticate users prior to granting them access to information, as well as a basis for encrypting that information to protect its confidentiality in transit. In the absence of PKI, DoD lacks workable tools to enable routine cryptographic protection of electronic mail and world wide web communications that move enormous amounts of sensitive information on a daily basis.

4 Capabilities Required

PKI provides security objects and mechanisms used by public key-enabled systems and applications (hereinafter referred to as "PK-enabled applications") to provide the security services performed by the supported applications. PKI is being implemented because the security products it provides and the security services it supports mitigate the threats identified in Section 2. The primary products of PKI are public key certificates and other certified objects used in conjunction with public key certificates (e.g., CRLs). In addition to public key certificates, PKI provides on-line services (such as on-line certificate status checking), and can supply authenticated attributes in public key certificates and/or attribute certificates. PKI is one of a number of security solutions used to protect information in the DII, and is used in addition to other solutions (e.g., in-line network encryptors [INEs]) to implement the defense-in-depth concept. The development of new, or enhancement of existing, applications with security mechanisms, is another element of defense-in-depth, and is a separate issue and not part of this document. The directories in which PKI related information is stored and can be retrieved are also not considered part of the PKI itself and therefore are not included here.

In general, PK-enabled applications supported by PKI are responsible for implementing the security services of:

- User identification and authentication (I&A)
- Data confidentiality
- Data integrity
- Access control
- Non-repudiation.

PK-enabled applications implement these services using the security objects generated by PKI and, in some cases, on-line services provided by PKI. Functional requirements for PKI are contained in section 4.1. Appendix C provides an overview of the security functions performed by PK-enabled applications. The information in the appendix is provided to clarify the boundary between PKI and the supported applications and contains no PKI requirements.

4.1 System Performance

PKI must provide a variety of products and services used by PK-enabled applications to provide the security services listed above. The following are the specific products and services provided by PKI. Each item is identified with its Threshold and/or Objective requirement; some requirements are identified as Key Performance Parameters [KPP]¹⁰. Requirements without numerical performance parameters will be considered satisfied if the identified functional capability is provided. The performance parameter in these cases is "does" or "does not" "the PKI provide the capability." The terms Threshold and Objective are being used to distinguish the criticality to the PKI of the requirement. Requirements shown as [Threshold] are musts. Those shown as [Objective] are goals; where no [Objective] level of capability is specified, the objective is the same as the threshold.

¹⁰ The terms "threshold", "objective", and "key performance parameter" are used per their meaning in CJCSI 3170.01A, *Requirements Generation System*, 10 August 1999 [Reference 25]. The definitions are included in the glossary section of this document.

Any PKI functional requirements that are addressed in the DoD X.509 CP must be implemented in compliance with the requirements of that policy. In particular, the CP specifies the implementation standards for many PKI functions. For example, the CP provides specific guidance on what constitutes acceptable proof of identity when registering subscribers and issuing certificates at different assurance levels. The DoD CP is updated periodically to ensure that it adequately represents current security and assurance requirements.

In some instances system performance parameters are different depending on the environment in which the PKI is being used. Most notably, compromise notification response time is much more critical in a tactical environment. Although it is recognized that these differences exist, functionally the PKI being procured does not differ based on the environment to which it will be deployed. Other than revocation performance parameters (addressed in Section 4.1.10) a PKI deployed in the tactical environment has no special functional requirements. The effect the environment has on the PKI will be on how it is implemented.

4.1.1 Generate Public Key Certificates

[Threshold] [KPP] PKI must generate public key certificates formatted in accordance with ITU Recommendation X.509, as tailored in certificate profiles specified by DoD. PKI must generate certificates with lifetimes compliant with DoD CP. PKI must also be capable of generating certificates with shorter lifetimes when required by particular subscribers or applications. PKI must be able to generate certificates for organizations. PKI must generate certificates for devices (e.g., servers, routers, and firewalls). All certificates generated by PKI must be verifiable back to a trusted element known to the relying party. Public key certificates generated by PKI must be usable with PK-enabled commercial applications (e.g., web browsers, e-mail clients) to the degree supported by those applications.

PKI must generate two kinds of public key certificates: signature certificates and encryption certificates. Signature certificates must contain a public key that is used to establish the holder's identity (e.g., in combination with proof of possession of the private key when connecting to a server) or provide assurance of origin and integrity (e.g., when verifying a digital signature). Encryption certificates must contain a public key that is used to encrypt electronic message, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. Each individual public key certified by PKI will be used for I&A or confidentiality key establishment, but not both. This restriction is not intended to prohibit use of protocols (e.g., a Secure Sockets Layer) that provide authenticated connections using encryption certificates. All certificates contain information to identify the subscriber, and all certificates issued to each specific subscriber must contain the same identity information. PKI must generate certificates that can be used to verify digital signatures for source authentication and integrity protection of software objects. PKI must generate encryption certificates for roles (e.g., Watch Officer).

PKI must generate new certificates within the following time limits where response time is measured from reception of the request by the CA to the transmission of the

CA's response. This performance measure does not include communications delays outside the control of PKI.

- Threshold: 30 seconds
- Objective: 10 seconds.

4.1.2 Supply Public Key Certificates

[Threshold][KPP] PKI must supply public key certificates to uniformed military personnel, DoD civilian employees, and members of the ready reserves, and DoD-sponsored foreign national and contractor personnel. PKI must be able to supply organizational certificates to authorized organizations. PKI must supply certificates for devices (e.g., servers, routers, and firewalls). PKI must supply certificates for PK-enabled applications (e.g., back-end databases accessed via intermediate servers). PKI must supply encryption certificates for roles (e.g., Watch Officer) and the corresponding private keys to the set of individuals who operate in that role. In addition, PKI may deliver certificates generated by external CAs (including other US Government CAs, State CAs, commercial CAs, and allied CAs) to DoD PKI subscribers. The methods for delivery of the certificates will be stipulated by the Certificate Practice Statement (CPS) and will be in accordance with the CP.

4.1.3 Support Multiple Cryptographic Algorithms And Algorithm Migration

[Threshold] [KPP] PKI must support a variety of public key cryptographic algorithms both in the public/private keys pairs created and certified by PKI, and in the algorithms used to apply digital signatures to certificates and other PKI products. PKI must support the concurrent use of several digital signature algorithms for issuing certificates and must be able to migrate over time to using new signature algorithms. PKI products will be used in protecting information in the NIPRNet environment, and at the unclassified and secret level in the SIPRNet environment. PKI must support public key cryptographic algorithms that have been approved for protecting information in those environments.

4.1.4 Provide Key Pairs And Certificates

[Threshold] [KPP] For each public key certificate PKI produces there must be a corresponding private key. When the PKI generates the public/private key pair for hardware implementations, the key pairs and the corresponding public key certificates must be generated in a form such that supported applications can load the keys and certificates and use them with hardware cryptographic implementations. PKI must support generation of key pairs both centrally and locally. In all cases where private keys are generated by PKI, the distribution of private keys must be protected with authentication, integrity and confidentiality controls to ensure that the private key is delivered to the correct subscriber, unchanged and without compromise. PKI must ensure that subscribers have control over the use of their private keys. PKI must ensure that subscriber private keys are never exposed in plaintext form, and that private

encryption key copies held by a CA for key recovery purposes are never released without proper authorization and under proper controls.

4.1.5 Program Subscriber Tokens

[Threshold] [KPP] PKI must program hardware tokens with public/private key pairs (or control the generation of key pairs by the token) and the corresponding public key certificates. PKI must support standardized delivery protocols so that it can program any token selected by DoD. PKI must support remote programming of tokens in circumstances where there is significant geographic separation between the subscriber holding the token and the element(s) of PKI supporting that subscriber. It should be noted that token procurement is not a function of this ORD.

4.1.6 Distribute PKI Root Certificate

[Threshold] [KPP] PKI must have the means to distribute the public key certificate of the trusted root to all subscribers and relying parties in a authenticated manner.

4.1.7 Support Subscriber Mobility

[Threshold] [KPP] PKI subscribers need to use their token(s) and public/private key pairs with any DoD computer/platform, regardless of the operating system of the computer. PKI must supply public/private key pairs, and public key certificates that are, to the maximum extent possible, computer platform- and operating system-independent. PKI must not impose any restrictions on the ability of multiple subscribers to use the same platform or application. PKI must allow subscribers to invoke certificate revocation and renewal services without requiring direct, local contact between the subscriber and the CA or RA who performed the initial registration of that subscriber. PKI must incorporate mechanisms to efficiently accommodate changes in subscriber data, such as subscriber name, phone number, location information; and changes in subscriber addressing for groups of subscribers with common characteristics (e.g., a unit moved to a new base location). PKI must accommodate changes of status, location, and unit affiliation of military reserve personnel, active military personnel, DoD civilians, DoD sponsored contractors, and other subscribers of the Target PKI.

4.1.8 Provide Registration Process

[Threshold] [KPP] PKI must provide processes that handle the registration of subscribers so that they can be issued certificates. The registration process must ensure that each subscriber, of any type, registered under PKI is assigned a unique identifier that is both human usable and unambiguous when used by automated decision processes. The registration processes, and other certificate management processes, must support the issuing and management of device (e.g., web server, router) and application subscriber certificates as well as human subscriber certificates. The registration processes must facilitate the request of device and application subscriber certificates by the parties responsible for the device being registered. PKI registration must be implemented in a simple and efficient manner such that it can be integrated into other, related, operational processes and supported by DoD organizations with minimal additional manpower. PKI registration processes must be designed to ensure that there is continuous accountability for any physical materials (e.g., one-time password letter)

associated with subscriber registration from the point of creation of those materials until they are delivered to the subscriber. Human subscriber PKI registration processes must take advantage of authoritative databases of personnel information, where available, to enhance process accuracy, trustworthiness, and efficiency.

4.1.9 Provide Renewal, Update, & Re-key Processes

[Threshold] [KPP] PKI must provide processes for the renewal, update, and re-key of certificates. In each case a new certificate with a new serial number is issued. Renewing means creating a new certificate with the same name, key, and authorizations as the old certificate, but with a new, extended validity period. Updating means creating a new certificate that has the same or a different key, and differs in one or more other fields (e.g., subscriber authorizations), from the old certificate. Re-keying means creating a new certificate identical to the old one, except with a different public key corresponding to a different private key. A different validity period may also be assigned.

PKI must provide automated notification of impending certificate expiration to the subscriber and the responsible RA to facilitate these processes. In order to efficiently and effectively meet the needs of the supported applications, PKI must provide both procedural interfaces for these functions and, where possible, technical interfaces that can be used by supported systems to invoke and execute these processes.

PKI must generate renewal, updated, and re-keyed certificates within the following time limits, where response time is measured from the reception of the request by the CA to the transmission of the CA's response. This performance measure does not include communications delays outside the control of PKI.

- Threshold: 30 seconds
- Objective: 10 seconds

4.1.10 Provide Revocation Processes

[Threshold] [KPP] Public key certificates have a specified validity period (i.e., a "lifetime") encoded into them, however PKI must provide the capability to revoke a certificate (i.e., declare it invalid) prior to its expiration. Each certificate is a distinct object, and PKI must be able to revoke any individual subscriber certificate without affecting other certificates associated with that subscriber. PKI must be able to revoke certificates issued to PKI elements such as CAs and RAs. PKI must make certificate revocation information widely available so that supported applications can determine the validity of individual certificates before relying on them. PKI must comply with the requirements of the DoD CP regarding CRLs. PKI must generate and publish CRLs, which are the standard mechanism for disseminating revocation information, formatted in accordance with X.509 and applicable profiles specified by DoD.¹¹ PKI must be able to publish CRLs in forms that take into account the constrained communications and

¹¹ PKI publishes CRLs via the directory system. Complete "distribution" of CRLs requires the participation of supported applications to retrieve the published CRLs from the directory system.

directory access capabilities of some supported applications (e.g., partitioned CRL, delta CRL).

For some supported applications, CRLs will be an inappropriate or ineffective means of promulgating revocation information. PKI must support alternative means for supported applications to check certificate validity via an on-line, interactive capability. This capability must be based on commercial standards such as the On-line Certificate Status Protocol (OCSP).

PKI must provide processes for the revocation of certificates that become invalid prior to the end of their expressed validity period. The process of revoking certificates must be protected at levels commensurate with its criticality. RAs must be able to request the revocation of a certificate on behalf of a PKI subscriber. PKI must be able to identify currently valid certificates based on the citizenship of the corresponding subscribers and must be able to revoke groups of certificates based on the citizenship of the corresponding subscribers. PKI must provide a capability for mass revocation of certificates (e.g., if a military unit is captured, all certificates issued to personnel in that unit must be revoked).

In order to efficiently and effectively meet the needs of the supported applications, PKI must provide both procedural interfaces for these functions and, where possible, technical interfaces that can be used by supported systems to invoke and execute these processes.

PKI must issue a new CRL in response to notice of a private key compromise within the following time limits, where the response time is measured from reception of compromise notification by the CA to the posting of the new CRL to the directory. This performance measure does not include communications delays outside the control of PKI.

Level	Non-tactical	Tactical
Threshold	Once a day and within 6 hours of compromise notice being received by CA	Once a day and within 1 hour of compromise notice being received by CA, for compromises within the tactical area of operations
Objective	Once a day and within 15 minutes of compromise notice being received by CA	Once a day and within 10 minutes of compromise notice being received by CA, for compromises within the tactical area of operations

4.1.11 Recover From Compromise

[Threshold] [KPP] PKI must be able to recover from the compromise of private keys, including the private keys of human and device subscribers, and of PKI components such as CAs and RAs. Because of the large impact if a CA's private key is compromised, recovery procedures for such an occurrence must be detailed, explicit, and thoroughly tested. The process for compromise recovery and the procedures to be

followed in case of a compromise must be well documented and readily available to PKI operators, subscribers, and relying parties.

4.1.12 Provide Key Recovery Services

[Threshold] [KPP] There will be circumstances where subscribers or their organizations need to gain access to information that has been encrypted using PKI-issued encryption keys. PKI must provide for recovery of private encryption keys to aid organizations in recovering encrypted information in cases such as accidental destruction of a private key or a malicious attempt by a DoD employee to deny access to information placed in their charge. PKI must be able to prevent archiving of selected private keys for recovery (e.g., in order to not archive private keys of subscribers from coalition partner forces). PKI must not provide key recovery services for private digital signature keys, and must ensure that private signature keys are not archived or escrowed. PKI must provide for two-party control over stored key recovery information, including support for situations where the two parties must be from separate organizations (e.g., to meet the needs of special access programs). PKI must publish the policies, procedures, and interfaces associated with gaining access to stored key recovery information.

4.1.13 Support Tactical Operations and Environment

[Threshold] PKI must support PK-enabled applications operating in tactical environments. All basic PKI functions, including subscriber registration and renewal, key pair generation, issuing public key certificates, programming subscriber tokens, publishing CRLs, compromise recovery, key recovery services, and help desk support, must be supported in tactical environments.

4.1.13.1 Support Connected Tactical Networks

[Threshold] PKI must support subscribers, relying parties, and PK-enabled applications operating on tactical networks connected to NIPRNet and SIPRNet. Due to the stringent communications bandwidth limitations of tactical networks and their reach-back connections, PKI for tactical networks must be able to provide continuous support despite interruptions in communications to fixed networks. PKI support to connected tactical networks must provide a full range of capabilities to register subscribers; generate key pairs; program tokens; issue, renew and revoke certificates; archive and provide recovery services for private encryption keys; and disseminate PKI-generated objects. PKI must be able to provide revocation information in a condensed form (e.g., using delta CRLs) to minimize the communications load on limited tactical communications circuits. PKI supporting tactical networks must be able to locally (i.e., in theater) generate and disseminate revocation information of interest to the tactical area of operations (e.g., due to the overrun of a unit command post), in accordance with the performance requirements specified in Section 4.1.10. PKI support to tactical networks must accommodate situations involving the partial deployment of a unit from its home base to the tactical area of operations. On-line PKI elements, such as OCSP responders, used to implement support for tactical networks must be interoperable with the Joint

Network Management System and associated service-specific network management systems for status reporting.

4.1.13.2 Support Closed Tactical Networks

[Threshold] PKI must provide a capability that can be implemented in closed command and control networks established for service, joint, combined and coalition operations. These networks are not interconnected with the NIPRNet or SIPRNet, and require network-specific PKI support for PK-enabled applications operating on the closed network. PKI support to closed networks must provide a full range of capabilities to register subscribers; generate key pairs; program tokens; issue, renew and revoke certificates; archive and provide recovery services for private encryption keys; and disseminate PKI-generated objects. PKI supporting closed tactical networks must provide interoperability with allied systems used in that operational environment. PKI must support all tokens used by DoD in tactical environments. PKI support to closed networks must not depend on any form of reach-back communications or other connectivity to fixed networks such as NIPRNet or SIPRNet. On-line PKI elements, such as OCSP responders, used to implement support for closed networks must be interoperable with the Joint Network Management System and associated service-specific network management systems for status reporting.

4.1.13.3 Support Subscriber Mobility For Tactical Requirements

Mobile subscribers must be supported in all tactical situations, to include service, joint, allied, and coalition environments. PKI must be able to accommodate changes in identities, location information, or subscriber addressing in a timely, efficient manner to ensure continuity of PKI support to subscribers during deployment and redeployment.

4.1.14 Maintain PKI-Generated Security Objects Archive

[Threshold] [KPP] Information protected by PK-enabled applications may need to be processed or verified long after its original creation or use. This is particularly true in the case of digital signatures, which may need to be verified many times over a period of years. PKI must establish and maintain an archive of the security objects it generates (e.g., public key certificates, CRLs) to facilitate long-term use of information protected by PK-enabled applications it supports. The storage of information in PKI archive must meet the requirements of existing Records Management laws, rules and guidelines, and of the DoD CP. PKI must publish guidelines and procedures for access to, and use of the objects stored by, the archive. PKI archive must provide a well-documented interface to enable supported applications to access, search, and retrieve objects from the archive.

[Objective] The PKI archive must comply with Information Dissemination Management (IDM) requirements for semantic tagging, search accuracy, and relevance of information returned from a search, as identified in the IDM Capstone Requirements Document (CRD). IDM semantic tagging and search accuracy and relevance requirements shall be applied to that portion of the PKI archive that is accessible on-line for search and retrieval of information, as appropriate.

4.1.15 Generate Trusted Time Stamps

[Objective] PKI must provide a means of generating and returning to a supported application a trusted time stamp for a data object. Such a time stamp provides evidence that a particular data object existed at a specific date and time. PKI time stamp service must operate based on universal time so that time zone differences between supported system elements using the time stamp do not create interoperability or verification problems. PKI time stamp service must be an on-line service that may be invoked on an as-needed basis by supported applications. The time stamp service must be available to all subscribers, including those that access the service via wireless or intermittent communications networks. The time stamp must be generated based on a time source (e.g., NIST or the Naval Observatory) other than the system's internal clock.

PKI must generate a trusted time stamp within the following time limits, where response time is measured from reception of the request to the transmission of the time stamping result. This performance measure does not include communications delays outside the control of PKI.

- Threshold: 30 seconds
- Objective: 10 seconds

4.1.16 Provide PKI Interoperability

[Threshold] [KPP] DoD PKI subscribers require secure exchanges of information with subscribers of other PKIs. CINCs require protected information exchange with coalition partners on classified and unclassified networks during non-crisis/contingency periods. PKI must support interoperability (e.g., by establishing cross-certifications) with other PKIs such as the US Federal PKI, State PKIs, and PKIs supporting the intelligence community, the medical community, and allied and coalition military forces. Interoperability provisions must provide a means for subscribers certified under different PKIs to verify and thereby accept one another's certificates. PKI must implement technical and policy controls on interoperability provisions to limit the risk assumed by PKI and its subscribers to acceptable levels.

- Threshold: Federal PKI interoperability
- Objective: Interoperability with other PKIs

4.1.17 Support Enterprise-Level Access Control

[Objective] PKI must provide products and services that aid supported applications in implementing enterprise-level access control by providing an authenticated source of subscriber attributes (i.e., structured information about subscriber characteristics). Such attributes can be used, as desired, by supported applications, as a partial or complete basis for access control decisions. To support enterprise-level access control, PKI must

- Support attributes identifying subscriber privileges/permissions. These attribute definitions must be flexible to support role-based, clearance/privilege-based and other access control approaches. The attribute definitions must also support network-oriented access control requirements
- Support attributes in public key certificates

- Support attributes in attribute certificates linked to subscriber public key certificates¹²
- Support attributes that provide the ability to logically discriminate US citizens from foreign nationals on an individual basis.
- Support Security Policy Information Files (SPIFs) in accordance with ISO/IEC 15816 | ITU-T X.841.
- Generate and distribute information (e.g., integrity-protected objects) specifying the interpretation of subscriber attributes;
- Provide means for appropriate authorities to request attributes and their inclusion in public key certificates and/or attribute certificates.

4.1.18 Provide Implementation Aids

[Threshold] PKI must assist the developers of supported applications in the implementation of PK-enabled features. This assistance must be provided both through documentation and training, and through tools such as software toolkits or "middleware" libraries. Training must include clear guidance on the requirements for relying party applications to properly provide public key-based security services. Such toolkits and libraries must provide standard, tested, reusable implementations of PK-enabled security services, such as digital signature creation and verification, that can be used directly by supported application developers. PKI must also publish an implementation schedule for infrastructure capabilities and services, and provide a central repository of information regarding PK-enabled applications, and approved COTS and GOTS products that developers, implementers, and subscribers can use with certificates issued by PKI.

4.1.19 Provide Help Support

[Threshold] PKI must provide help services to assist PKI operators, supported application developers, and subscribers in resolving PKI technical and operational issues. These services include, but are not limited to help desk support. PKI help desk support must readily assist subscribers with common problems, including (but not limited to) lost or damaged tokens, and forgotten authenticating codes (e.g., personal identification numbers).

For any of the above products and services covered in the DoD CP, PKI must implement those products and services in compliance with the requirements of that policy.

4.2 Information Exchange Requirements

An operational view of the PKI was previously shown in Figure 4. PKI is an infrastructure system that will interface, directly or indirectly, with every PK-enabled

¹² In general, public key certificates are more likely to be used to convey long-lived attributes such as citizenship, and attribute certificates are more likely to be used to convey short-lived attributes such as user roles within a particular supported application. The US is working with a number of our allies to identify a standard set of attributes to be included on public key certificates.

supported application operating as part of the DII. To support the long-term goal of establishing an integrated KMI, the KMI architecture will be used for the DoD PKI.

The exchanges of information between PKI and other entities, including PK-enabled applications and devices, tokens, and other infrastructures must be based on standard protocols and formats. As part of the process of implementing PK-enabled security features, supported applications will need to use the standard interfaces provided by the PKI for interactions with CAs, RAs, the time stamp service, etc. The interfaces and capabilities of PKI will not be tailored to fit specific supported application characteristics.

The following sections describe the information exchange requirements (IERs) between PKI and other entities. An IER matrix is provided in the tables. Critical IERs are identified in the IER matrix.

4.2.1 Interactions With Subscribers and Device Administrators

PKI must interact with PKI subscribers and the administrators of PK-enabled devices for initial registration of PKI subscribers and subsequent actions to renew, update, re-key and revoke existing certificates and issue new certificates.

4.2.2 Interactions with Tokens and PK-Enabled Devices

PKI must interact with subscriber tokens and PK-enabled devices to program those entities with public key certificates and corresponding private keys. In some cases, PKI must program tokens with authentication information to support I&A of the subscriber to the token.

4.2.3 Interactions with PK-Enabled Applications

PKI must interact with PK-enabled applications to provide trusted timestamp and on-line certificate status checking services.

4.2.4 Interactions with Other PKIs

PKI must interact with other PKIs to establish cross-certifications. These cross-certifications are required to enable interoperability of PK-enabled applications and devices with peer applications and devices that are subscribers of other PKIs.

4.2.5 Interactions with Authoritative Personnel Databases

PKI must interact with authoritative personnel databases to support subscriber verification.

4.2.6 Interactions with DII Directories

PKI must interact with DII directories (e.g., GDS) to determine the correct naming for PKI subscribers, and to publish certificates and CRLs so that they are available to PK-enabled applications and devices.

4.2.7 Interactions with Time Reference Sources

PKI must interact with time reference sources (e.g., NIST, the Naval Observatory) to obtain precise, coordinated, authoritative time information. Time reference information is used in providing trusted time stamp services.

4.2.8 Interoperability KPP

Key Performance Parameter	Threshold (T)	Objective (O)
All IERs will be satisfied to the Standards specified in the Threshold & Objective values.	100% of IERs designated critical	100% of IERs

Critical IERs are identified in the IER matrix.

4.3 Logistics and Readiness

The entire PKI system must have no single points-of-failure that would make CA services unavailable at any time.

4.3.1 CA Availability

An individual CA must have an availability of 164 hours out of a 168 hour period and must provide the services as specified in Section 4.1 within the response times of the KPPs within that section.

Individual CA availability is defined as the time that a specific PKI CA is prepared to respond to requests for new certificates, certificate renewals, revocation notifications, CRLs, certificate status checking, etc.:

- Threshold: single CA 164 hours per 168 hour period of availability
- Objective: single CA 168 hours per 168 hour period of availability

The maximum non-availability period of any individual CA within a seven day time period must be less than 4 hours. PKI must incorporate local and regional back-up CA capabilities in order to support very critical missions with high assurance. PKI must have no single points-of-failure that would make CA services unavailable. In particular, the non-availability of an individual CA must not prevent the PKI from meeting the operational availability requirements specified in Section 4.3.2.

4.3.2 Continuity of Operations

The PKI must be designed to maintain continuity of operations. A disaster recovery plan must be established for PKI as a whole and for individual system elements (e.g., each CA, each RA). This plan must deal with the corruption, destruction, loss, and compromise of PKI components, as well as the impact of natural disasters and man-made disruptions of system operations.

PKI must be designed to operate 24 hours per day, 7 days per week. PKI operational availability is defined as the time that PKI is prepared to respond to requests to register subscribers; generate new, renewed or re-keyed certificates; process revocation requests; generate CRLs; provide certificate status checking; and respond to key recovery requests. The PKI operational availability requirement is:

- [Threshold] [KPP] PKI must be operationally available 99.9% of the time; PKI must have no single points-of-failure that would make CA services unavailable.

- [Objective] [KPP] PKI must be operationally available 99.99% of the time; PKI must be able to restore any non-available services within 4 hours of a non-catastrophic failure.

4.4 Other System Characteristics

a) EA and Wartime Reserve Modes (WARM) Requirements.

PKI has no requirements related to EA or WARM.

b) Conventional, initial nuclear weapons effects, Nuclear, Biological, Chemical Contamination (NBCC) survivability.

Deployable PKI components must be able to survive and operate in NBCC environments, and must be operable by personnel in protective clothing.

c) Unplanned stimuli (e.g., fast cook-off, bullet impact, sympathetic detonation).

- Not applicable

d) Safety issues (e.g., Hazards of Electromagnetic Radiation to Ordnance [HERO]).

- Not applicable

e) Natural environmental factors (e.g., climatic, terrain, oceanographic factors)

Deployable portions of PKI must be able to maintain operational capability in tactical operating environments, subject to the constraints imposed by the communications capabilities available in those environments.

f) Expected mission capability in various environments.

Deployable portions of PKI must be able to maintain operational capability in tactical operating environments, subject to the constraints imposed by the communications capabilities available in those environments.

g) Physical and operational security needs.

PKI will require a mixture of centralized fixed CAs (e.g., root CA), geographically distributed CAs, and deployable CAs. In addition, RAs, and other components may be deployed to meet specific operational needs in both fixed facilities and in tactical situations. All PKI system components must receive appropriate physical and operational security protection in accordance with the requirements of the DoD CP. PKI must undergo certification and accreditation in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

PKI must be designed to operate in the face of network attacks such as denial-of-service attacks. PKI must integrate with available DoD standard systems for network monitoring and defense. PKI core components must be protected by a standard suite of network security components and protections (e.g., firewall, malicious code detection, network- and host-based intrusion detection systems).

PKI components and facilities must be protected against damage from electrical transients (e.g., due to lightning strikes or utility switching operations) and other power abnormalities. Surge protection must be provided for both communications and power

connections, and must be consistent with common industry practices and applicable electrical codes. Surge protection devices used for PKI must meet the requirements of applicable industry standards.

PKI must be designed to protect and assure the integrity of the operation of PKI components. PKI must provide for identification and authentication of component operators, integrity verification of component software, and auditing of component operations.

PKI must develop and publish procedures for recovery from compromise of a PKI operational node (e.g., CA, RA). PKI must develop and publish procedures for subscribers to follow in the event of suspected or actual compromise of one or more of the subscriber's private keys.

5 Program Support

The joint potential designator for PKI is “Joint.”

5.1 Maintenance Planning

The following sub paragraphs describe the maintenance planning for PKI. An integrated logistics support plan must be developed for PKI. The PKI Program as envisioned, does not provide any end user hardware, therefore, user-level maintenance considerations are not applicable. End user hardware for this program consists of tokens and card readers. The Services will be required to procure and maintain these elements both of which are considered computer peripherals. No maintenance is envisioned for the Token. Card reader maintenance will be added to the current local maintenance of the host computer system. Maintenance planning for PKI must be consistent with normal and emergency maintenance concepts for military backbone communications systems and general-purpose computer equipment. PKI will be highly integrated with the DII, and must be supported and maintained in a like manner as backbone communications systems and equipment. Availability of PKI-generated objects to PK-enabled applications is dependent on DII backbone networks (e.g., NIPRNet) and directory systems whose maintenance is beyond the scope of PKI. Dependency on the DII (which will evolve to the GIG) and the tactical extensions to carry PKI requires coordination with DISA and Services’ communications commands. The capability of the DII/GIG and tactical extensions to provide connectivity to support PKI requirements must be ensured or identification of an alternate solution is required.”

5.1.1 PKI Server Hardware.

Server maintenance will be available from commercial sources. With the risk of outages affecting hundreds of subscribers, redundant systems in hot standby mode will be considered in the design to meet system availability requirements.

5.1.2 PKI Software Maintenance.

PKI software must be controlled by formal configuration management procedures. The PKI PMO will centrally control the software maintenance support.

5.1.3 PKI Communications.

Maintenance of supporting communications will be the responsibility of the Defense Information Systems Network (DISN) office to arrange and the respective CINC or Service components to fund. DISN-leased commercial communications support is assumed for fixed, peacetime locations. Organic DoD tactical communications support is assumed for deployed locations.

5.1.4 Card Reader Maintenance.

Card readers are associated with a user procured personnel computer or workstation. As such the card reader should be added to the local support program associated with these devices.

5.2 Support Equipment

The DoD PKI PMO has been formed to oversee the development and fielding of PKI for DoD. The PMO envisions incremental fielding of a PKI capability in a series of three incremental installations over a period of 5 years in which the capability will have a planned evolution. No new support or maintenance equipment shall be developed for PKI. This does not preclude the development of required, operational technology such as biometric authentication systems. PKI must be designed to be maintained by standard test equipment and must include fault isolation capabilities to diagnose failures at a level commensurate with the final support concept. Standard equipment is required to identify faults on COTS computer systems and software.

To facilitate the implementation of PK-enabled applications and systems, PKI must provide software toolkits, operating system libraries and other building block components that can be used by developers.

5.3 C4I/Standardization, Interoperability, and Commonality

5.3.1 Integration into C4ISR Infrastructure

PKI must be connected to and support subscribers, relying parties, and PK-enabled applications operating on all standard DoD networks, including NIPRNet and SIPRNet. It must be accessible to and support current and future PK-enabled DoD automated information systems, as specified in DoD PKI Memorandum [Reference 1].

PKI must be connected to and support subscribers, relying parties, and PK-enabled applications operating on National Guard and reserve forces networks, including (but not limited to):

- Guardnet XXI
- WarriorNet
- Reserve Component Automation System (RCAS)

PKI provides the infrastructure to enable security service support to both SIPRNet and NIPRNet. Applications on these networks like Global Command and Control System (GCCS), Global Combat Support System (GCSS), and others then may be PK-enabled such that access control may be granted by virtue of the permissions assigned to the subscriber and a digital signature certificate and personal identification number (PIN) being presented. GCSS Commander in Chief/Joint Task Force (CINC/JTF) is already using web-based PKI technology to achieve unitary logon to a variety of web-based resources.. Additionally, the subscriber's digital encryption key may then be used to encrypt transmissions user-to-user for PK-enabled applications.

PKI is one of the two support infrastructures identified in the Information Assurance Technical Framework, Release 3.0, September 2000. This framework was developed to support the Defense in Depth strategy for protecting DoD networks. There are two factors that have implications for the communications backbone infrastructure; a support factor and the subscriber community factor.

The support factor is comprised of the certificate registration activity and the certificate management activity. Each and every location involved in registering

subscribers and issuing certificates will have to have a registration workstation configured for this purpose connected to the specific network (NIPRNet or SIPRNet). A certificate management activity will have to interact over the network with the individual registration authorities for the issuing of the appropriate certificates. The subscriber information must then be sent to the network directory services and posted. All this activity requires network connectivity and bandwidth. The subscriber community will also impact the bandwidth with the insertion of digital certificates adding additional length to e-mails and with the need to exchange keys used for encryption. In general, the fixed plant infrastructure can easily be sized to accommodate the increased bandwidth consumption. The tactical infrastructure down to the Joint Task Force (JTF) level and into the service component levels needs to be examined according to how far down into the infrastructure the service decides to field and employ PK-enabled applications.

5.3.2 Data fusion

PKI has no data fusion requirements or anti-jam requirements. PKI will use basic communications support from DoD network.

5.3.3 Unique Intelligence Information

PKI has no unique intelligence information requirements. Target and threat databases may be PK-enabled to grant access permission based on individual user profiles. PKI must support a writer-to-reader encryption capability in PK-enabled applications.

5.3.4 Use with NATO and Allies

PKI must be interoperable to the maximum extent possible with commercial, Federal, State, and allied nation PKIs. It must support interoperability of the information systems used by US forces participating in joint and combined operations. PKI interoperability is a means to enable interoperability of PK-enabled applications. Products and services provided by PKI must support interoperability of DoD PK-enabled applications with PK-enabled applications supported by these other PKIs unless interoperability must be constrained for security reasons.

PKI must adhere to commercial PKI standards to facilitate interoperability negotiations with the appropriate standards committees of North American Treaty Organization (NATO) and Allied countries.

5.3.5 Technical and Procedural Interfaces

PKI must provide vendor-neutral interoperability across all elements of PKI and the supported applications. PKI must support PK-enabled applications in a manner independent of the communications media used by those applications. DoD PKI certificates must be usable with security services implemented in all protocols of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. DoD PKI certificates must be compliant with industry standards so that they will be usable in future operational systems. PKI certificates must be usable with PK-enabled commercial applications that are widely-used in DoD, including (but not limited to):

- Office automation suites
- Electronic mail packages
- Web browsers
- Electronic publishing applications (e.g., portable documents)
- Forms automation / work-flow applications
- Electronic commerce applications
- Financial management applications
- Electronic file management applications

All PKI components must be certified under the National Information Assurance Partnership (NIAP) program. Cryptographic components of PKI must meet the requirements for Class 4 assurance specified in the DoD CP [Reference 2].

PKI must make maximum use of and integrate seamlessly with COTS products and technology. PKI must be implemented in a manner that permits readily incorporating advances in data management, communications, networking, and security technology. It must be designed to facilitate the incorporation of new technology so that it can be kept technologically current at affordable cost. PKI must pass interoperability testing performed by the Joint Interoperability Test Command.

5.3.6 Compliance with DoD Joint Technical Architecture

The Target PKI is an infrastructure system. It must support a broad range of existing and future DoD information systems (all or near all DoD information systems). PKI must provide well-documented interfaces for its products and services, and those products and services must be implemented in accordance with the Joint Technical Architecture (JTA) V3.1, 31 March 2000 [Reference 20] and the DII Common Operating Environment (COE) [Reference 22].

5.3.7 Global Command and Control System (GCCS) and Common Operational Picture (COP)

With PKI fielded, applications supporting the GCCS and the COP may be PK-enabled to make use of the security services PKI supports. As a pilot SIPRNet PKI initiative, the GCCS (CINC/JTF) has already PK-enabled its Web based applications which supporting unitary logon and encrypted transactions.

5.3.8 Information Assurance

PKI must support PK-enabled applications in providing integrity, authentication, confidentiality, and support non-repudiation for the information processed by those applications. PKI must provide integrity, authentication, confidentiality, and support non-repudiation for the information it processes in the course of PKI operations.

PKI must support the DoD IA objectives for building the IA support infrastructure. DoD has adopted a defense-in-depth strategy approach for providing IA. This strategy has four objectives:

- Defend the Computing Environment
- Defend the Enclave Boundary
- Defend the Network Infrastructure

- Provide a Supporting Infrastructure

Separate steps are being implemented for the first three items above. The defense-in-depth strategy provides a supporting infrastructure that has the following three objectives:

- Provide a cryptographic infrastructure that supports key, privilege, and certificate management and that enables positive identification of individuals using network services.
- Provide an intrusion detection, reporting, analysis, assessment, and response infrastructure that enables rapid detection and response to intrusions and other anomalous events, and that enables operational situation awareness.
- Plan execution and reporting requirements for contingencies and reconstitution.

5.3.9 Energy Standardization and Efficiency

PKI components must be able to operate on available power conforming to local power standards in the area of operation. Depending on the location of operation of any particular component, this includes, but is not limited to, US standard power (110 VAC, 60Hz), European standard power (220 VAC, 50 Hz), Japanese standard (110/50) and Korean standard (220/60) for fixed location use. In some European areas (new NATO countries in particular) consideration must be given to fluctuating organic power systems caused by aging infrastructures. Deployable PKI components must be able to operate using the same power used by the associated deployed forces for their organic communications and information systems equipment.

5.3.10 Electronic Environmental Effects and Spectrum Support

PKI has no Electronic Environmental Effects nor does PKI require Spectrum Support.

5.4 Computer Resources

PKI subscriber clients must be usable on different hardware/software platforms commonly fielded by customer departments, agencies and organizations. PKI must be compliant with the DII COE, with a threshold requirement of level 6 compliance, and an objective requirement of level 8 compliance, per ASD C3I Memorandum, "Implementation of Defense Information Infrastructure Common Operating Environment Compliance", 23 May 1997.

5.5 Human Systems Integration (HSI)

[Threshold] PKI must provide training programs, including both classroom training and computer-based or on-line training for subscribers, relying parties, and PKI operations. PKI must be designed to minimize the number of distinct operational and management roles and corresponding manpower requirements at subscriber locations. It must also be designed to minimize the need for workstations dedicated to performing PKI functions, except where security dictates a need for separation. PKI must not require the use of multiple CA or RA workstations to provide PKI support at an installation simply because it has tenants from

multiple CINCs, Services, and/or Agencies. PKI must meet the requirements of Section 508 of the Rehabilitation Act of 1973, as amended and codified at Title 29, United States Code 794(d), and the Electronic and Information Technology Accessibility Standards, 36 C.F.R. Part 1194 (published at 65 Fed. Reg. 80500, Thursday, December 21, 2000).

5.5.1 Training

[Threshold] PKI must assist the developers of supported applications in the implementation of PK-enabled features. This assistance must be provided both through documentation and training, and through tools such as software toolkits or "middleware" libraries. Training must include clear guidance on the requirements for relying party applications to properly provide public key-based security services. Such toolkits and libraries must provide standard, tested, reusable implementations of PK-enabled security services, such as digital signature creation and verification, that can be used directly by supported application developers. PKI must also publish an implementation schedule for infrastructure capabilities and services, and provide a central repository of information regarding PK-enabled applications, and approved COTS and GOTS products that developers, implementers, and subscribers can use with certificates issued by PKI.

[Threshold] PKI must provide training programs, including both classroom training and computer-based or on-line training, for subscribers, relying parties and PKI operators.

The DoD PKI PMO must develop PKI training material. PKI will be operated and used by a mixture of PKI trained personnel, system administrators, and subscriber personnel. These personnel may be a mixture of government and contractor employees. PKI trained personnel (e.g., CAs, RAs, application component [e.g., guard] administrators) will require training consistent with the software and equipment they are expected to operate and the policies they are expected to enforce (grade requirements for these personnel are contained in Reference 2). System developers and administrators will require a more detailed understanding of PKI operations and functions than will DoD personnel in general, but will not be actual operators of PKI. In addition, all DoD personnel may interact with PKI (e.g., for certificate renewal). PKI information for all types of operators, subscribers, and developers must be readily available via the DII.

A PKI training plan must be developed in accordance with applicable Joint and DoD guidance. The training plan must address the training requirements of:

- **Executives.** This training must explain the impacts of PKI on organizational processes, AISs, and communications networks.
- **Human subscribers** (including foreign nationals and contractor personnel). This training must address basic subscriber functions including requesting and receiving a signature (i.e., identity) certificate, requesting and receiving encryption certificates, certificate use, certificate replacement/renewal, key recovery and requesting certificate revocation.
- **Application and device subscriber administrators.** This training must address the same basic subscriber functions as for human subscribers while addressing the unique aspects of managing a PK-enabled application or device.

- **Application Program Managers.** This training must address the use of PKI and the process of PK-enabling an application.
- **Developers.** This training must provide information needed by developers to PK-enable new and existing applications.
- **PKI operators.** This training must provide the information needed by CA and RA operators to operate the PKI in accordance with the DoD CP.

Portions of PKI may be operated or supported by contractors. Contractor personnel must be fully trained in the technology, policies, and operating procedures of PKI, and must be fully cognizant of their responsibilities under the DoD CP. All DOD personnel must receive general information regarding the use of their keys and certificates, and specific guidance regarding their obligations for protection of their security tokens and private keys.

5.6 Other Logistics and Facilities Considerations

Hardware and software to support the PKI must be deployed to an undetermined number of locations to support the millions of potential subscribers with up to several hundred thousand workstations. PKI infrastructure implementation will use existing building space and not require construction of new facilities. PKI must be operated in a mixture of fixed facility and forward-deployed environments. PKI must be designed to allow deployed military forces to take advantage of host nation facilities/resources (e.g., power, and communications) to access PKI. Host nation approval and SOFA for deployment of PKI will be done on a case-by-case basis as needed.

Portions of PKI will be operated by military personnel operating in deployed or tactical environments, afloat, or aloft. Deployable components will be operated at times by personnel in protective clothing, such as NBCC protection garments or arctic clothing. PKI components intended for such situations must be capable of operating in tactical environmental conditions (e.g., temperature range, moisture range, vibration and shock, etc.), and must be designed to require little or no specialized or dedicated hardware for routine operations. These deployable components must be operable by personnel in protective clothing, and be designed to operate reliably in such environments.

PKI components will require physical security protection. Critical PKI components such as CAs must be housed in facilities with strong physical security protections. Some PKI components will be fielded to and operated in user facilities. These PKI components must be designed to minimize the degree to which additional physical security requirements are placed on the facilities where such components are operated.

5.7 Transportation and Basing

PKI will operate from a mixture of fixed and mobile facilities. While the majority of PKI is likely to be operated from fixed facilities, a portion of PKI must be deployable to support the needs of operational military forces. Those portions of PKI that are deployable must be transportable using the organic assets or normal transport means of the units with which they are associated.

5.8 Geospatial Information and Services

PKI has no requirement for cartographic materials, digital topographic data, or geodetic data.

PKI requires access to a reference time source, such as that maintained by the U.S. Naval Observatory or provide through the Global Positioning System, to support synchronization. Such information will be obtained from the local DISN node supporting the network. Therefore, PKI will not have to develop this requirement.

5.9 Natural Environmental Support

PKI has no requirement for weather, oceanographic, or astrogeophysical support.

6 Force Structure

Hardware and software to support the PKI will be deployed to an undetermined number of locations to support over 3.5 million potential DoD subscribers with up to several hundred thousand workstations. CINCs, Services and Agencies will integrate the management and operation of the DoD PKI registration components onto common platforms.

Services, and Agencies will procure local infrastructure elements and RA workstations in accordance with the IA Framework, PKI technical specifications and guidance. 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 DoD PMO, working with the Services, will develop the training material for any equipment that they develop.

NSA will manage and operate the DoD Root CA(s). DISA will lead the integration and operations of the centralized certificate management services. The CINCs, Services, and Agencies will initialize and operate the RAs and LRAs. NSA (or PMO) support will include

- Registration
- Audit review
- Maintenance
- Policy enforcement
- Operating a help desk
- Compromise recovery
- Rekey, and
- Key recovery.

The CINCs, Services, and Agencies will provide manning and workstations at the registration sites. The RA is envisioned to be a single person operation, but may require backups to provide continuous coverage in the event of illness or vacations. The PMO will ensure that adequate help desk capabilities exist, consistent with the deployment of PKI services across the Department. It is expected that help desk capabilities will be decentralized.

Manning required for the operations, and maintenance of the DOD PKI Infrastructure will possibly consist of military, government employees, and contractor personnel. However, the Services are not mandated to increase their end strengths to control, operate, and maintain the infrastructure.

7 Schedule

Detailed schedule information for DoD PKI will be prepared by the PKI Program Management Office. The following key dates are based on the policy guidance in "Department of Defense (DoD) Public Key Infrastructure", Deputy Secretary of Defense Memorandum dated 12 Aug 00 [Reference 1], with the exception of certain SIPRNet-related dates; the latter are identified as "(not yet approved)".

December 2000:

- Unclassified, private web servers, i.e., those not accessible to the general public, shall be issued a Class 3 (at a minimum) DoD PKI server certificate.
- DoD unclassified networks begin migrating to hardware token, certificate-based access control.

December 2001:

- Registration capability for the Class 3 PKI shall be implemented.

June 2002:

- Private SIPRNet web servers PK-enabled for server-side authentication (not yet approved).

October 2002:

- All DoD Users issued a class 3 certificate.
- Issuing of Class 3 certificates on software tokens ends.
- Protection of Mission critical systems operating on unclassified networks and employing public key technology must be via Class 3 certificates at a minimum.
- Registration capability upgrades for Class 4 implemented.
- DoD organizations begin to issue Target Class 4 certificates.
- All private DoD and DoD-interest web servers located on unclassified networks shall require client identification and authentication using Class 3 user certificates.
- All electronic mail ... sent within the Department will be digitally signed.
- DoD unclassified networks shall be enabled for hardware token, certificate-based access control.

October 2003:

- Deployment of SIPRNet registration capability completed (not yet approved).

December 2003:

- Unclassified Mission Critical systems that operate on unclassified networks and employ public key technology must migrate to Target Class 4 certificates and tokens.
- For access to Mission Critical web servers on unencrypted networks ... transition from a Class 3 to a Target Class 4 certificates is required for client identification and authentication.

DoD Target PKI Operational Requirements Document

- Unclassified networks hosting mission critical systems shall migrate to certificate-based access control using Target Class 4 tokens.

October 2004:

- Certificates issued to all SIPRNet users (not yet approved).
- All SIPRNet e-mail digitally signed (not yet approved).

December 2004:

- Issuance of Class 3 certificates ends.

Figure 7 shows these key dates and the anticipated schedule of PKI releases through Release 5.0 in Gantt chart form.

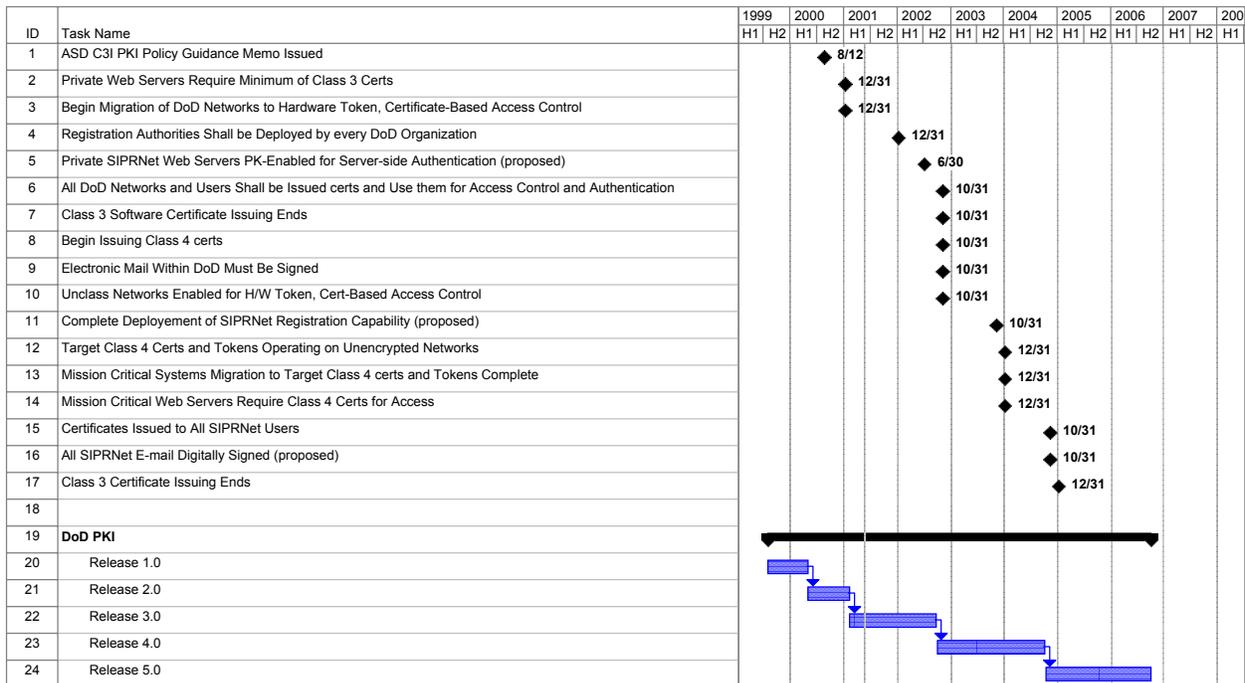


Figure 7: Key PKI Dates and PKI Release Schedule

8 Program Affordability

The Target PKI will be implemented as an integral part of DoD's KMI evolution. The capabilities of the existing Class 3 PKI serve as a baseline for the functionality of the DoD Target PKI. The Target PKI will be implemented to support the Class 4 PKI requirements across the Department as set forth in the recent ASD C3I policy [Reference 1]. While the Target is being developed and deployed, the existing Class 3 and FORTEZZA-based interim Class 4 PKI capabilities will remain operational to facilitate an efficient transition.

8.1 Threshold and Objective Costs

The threshold amount for acquisition of the capabilities described in this ORD is \$598.3M [T], with an objective amount of \$554.4M [O]. These amounts are distributed across fiscal years and PKI elements as follows:

Objective

	FY01	FY02	FY03	FY04	FY05	Totals
Root, CA	34.9	33.6	28.6	26.2	26.2	149.5
RA/LRA	4.0	13.7	15.9	7.4	9.0	50.0
O&M	77.0	94.4	70.1	57.1	56.3	354.9
Totals	115.9	141.7	114.6	90.7	91.5	554.4

Threshold

	FY01	FY02	FY03	FY04	FY05	Totals
Totals	115.9	155.9	126.1	99.8	100.7	598.3

These amounts purchase the following:

- 1) Class 4 Root CA and Operational CAs
- 2) RA/LRA Software and fielding
- 3) Tokens, readers, and middleware sufficient to establish the PKI
- 4) O&M support for above.

DISA and NSA are responsible for the development of the Target DoD PKI, and procurement, installation and operation/maintenance of the Root and CA. The Services and Agencies are responsible for the procurement of RA/LRA hardware, with software being centrally provided by DISA, and the associated operations and support. DMDC is responsible for the procurement, installation and maintenance support of the RAPIDS terminals. The Services and Agencies are responsible for the manpower required to operate these terminals.

8.2 Funding Status

The FY01 – FY05 DoD budget for all PKI initiatives in this ORD is \$466.4M. These funds are in the budgets of NSA, DISA, Army, Navy, Air Force, and the various DoD agencies, and is broken out as follows (\$M):

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

	FY01	FY02	FY03	FY04	FY05	Totals
Root, CA	34.9	33.6	28.6	26.2	26.2	149.5
RA/LRA	4.0	3.9	4.4	4.1	4.2	20.6
O&M	77.0	78.2	56.0	42.7	42.4	296.3
Totals	115.9	115.7	89.0	73.0	72.8	466.4

This amount is enough to cover all of the threshold requirements listed in this document. Essentially, it represents the development and procurement costs of a Target DoD PKI with full NIPRNet and an initial SIPRNet deployment.

In addition to the above funds, the PKI PMO has identified several areas where some additional funds may be required. These funds are needed to meet the objective requirements called out in this ORD plus the funds needed for PK enabling of specific service or department applications. PK enabling is not currently part of the overall budget. The objective level requirements addressed by these additional funds are in the areas of Tactical PKI components, full PKI on SIPRNet, OCONUS deployment & Allied interoperability. The need for the additional funds begins in FY02; FY01 is fully funded. The following chart summarizes the objective level funding requirements (\$M):

	FY02	FY03	FY04	FY05	Totals
Root, CA	0.0	0.0	0.0	0.0	0.0
RA/LRA	9.8	11.5	3.3	4.8	29.4
O&M	16.2	14.1	14.4	13.9	58.6
PK Enabling of Apps	83.0	51.0	47.0	3.0	184.0
Totals	109.0	76.6	64.7	21.7	272.0

The DoD PKI PMO is working with ASD C3I and the Services to further assess the shortfalls in order to program for these funds in out years.

Appendix A: References

1. Deputy Secretary of Defense Memorandum, subject: "Department of Defense (DoD) Public Key Infrastructure," 12 August 2000
2. U.S. Department of Defense Certificate Policy, Version 5.2, 13 November 2000
3. "Public Key Infrastructure Roadmap for the Department of Defense," Version 4.0, 4 December 2000
4. "KMI 2004: Threat Assessment Report (DRAFT)," National Security Agency (V5), KMI Security Architecture Team, 21 June 1999.
5. "Threat and Vulnerability Model for a Public Key Infrastructure within the Department of Defense," National Security Agency, Informal Technical Report, Date Unknown.
6. United States General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risk," GAO/AMID-96-84, May 1996 available at <http://frwebgate.access.gpo.gov>
7. "Smart Card Adoption and Implementation", Deputy Secretary of Defense Memorandum, 10 November 1999
8. "FY 2001-2005 Defense Planning Guidance", Department of Defense
9. Joint Publication 3-13, "Information Operations"
10. DoD Directive S-3600.1, 5 May 1995, "Information Warfare"
11. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Information Assurance Acquisition Policy dated January 2000.
12. DOD Directive 4630.5, 12 November 1992, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems" <http://web1.deskbook.osd.mil/>
13. DOD Instruction 4630.8, 18 November 1992, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems" <http://web1.deskbook.osd.mil/>
14. DOD Directive 5000.1, 23 October 2000, "The Defense Acquisition System" <http://www.acq.osd.mil/ar/doc/dodd5000-1.pdf>
15. DOD Instruction 5000.2, 23 October 2000, "Operation of the Defense Acquisition System" <http://www.acq.osd.mil/ar/doc/dodi5000-2.pdf>
16. USD (AT&L), ASD(C3I) and DOT&E Memorandum (Interim), 23 October 2000, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs" <http://www.acq.osd.mil/ar/doc/dodd5000-1-int-reg.pdf>
17. DOD Electronic Desk Reference Set, "Defense Acquisition DeskBook," December 1999 <http://www.deskbook.osd.mil/>
18. CJCS Instruction 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems, and Information Technology Systems" <http://www.dtic.mil/doctrine/jel/cjcsd/cjsi.htm>

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

19. C4ISR Architecture Framework, Version 2.0, 18 December 1997
http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/index.htm
20. DOD Joint Technical Architecture, Version 3.1, of 31 March 2000 (<http://www-jta.itsi.disa.mil/>)
21. DOD Instruction 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)"
22. Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 4.0, October 1999 <http://dod-ead.mont.disa.mil/cm/general.html>
23. DOD Technical Reference Model (TRM), Version 1.0, 5 November 1999 <http://www-trm.itsi.disa.mil/>
24. The Defense Information Infrastructure (DII) Master Plan, Version 8, "Implementing the Global Information Grid," 29 April 1999 see SIPRNet - <http://199.208.165.20/diimp/dii.htm>
25. CJCSI 3170.01A, 10 August 1999, "Requirements Generation System"
26. CJCSI 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems, and Information Technology Systems"
27. DOD Directive 5000.1, 15 March 1996, "Defense Acquisition"
28. DOD Directive 4630.5, 12 November 1992, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems"
29. DOD Instruction 4630.8, 18 November 1992, "Procedures for Compatibility, Interoperability, C4I Supportability of Command, Control, Communications, and Intelligence Systems"
30. ASD (C3I) memorandum, 20 March 1997, "Secret and Below Interoperability (SABI)"
31. GCSS Capstone Requirements Document, 5 June 2000
32. FIPS 140-1, January 11, 1994, "Security Requirements for Cryptographic Modules"
33. ITU-T Recommendation X.509, August 1997
34. CJSCI 3170.01A, "Requirements Generation System", 10 August 1999
35. Class 3 Public Key Infrastructure Release 3.0 Concept of Operations, Draft, December 2000
36. KMI 2012 Operational View (CONOP), 19 Jan 2000
37. KMI 2112 System Description for Capability Increment 1 (CI-1), 28 Feb 2001
38. Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance", 16 June 2000
39. Operational Requirements Document for the DoD Smart Card, 8 January 2001
40. Deputy Secretary of Defense Memorandum, "Information Vulnerability and the World Wide Web", 24 September 1998
41. Information Dissemination Management Capstone Requirements Document, 22 January 2001
42. ASD (C3I) memorandum, 17 May 2001, "Public Key Enabling (PKE) of Applications, Web Servers and Networks for the Department of Defense (DoD)"

Appendix B: Distribution List

TBSL

Appendix C: List of ORD Supporting Analyses

Focus Groups

The requirements contained in this ORD are based on a series of focus group conducted by the NSA and the DISA between August 1999 and June 2000. A broad spectrum of users, system architects, policy personnel, and IA specialists participated in these focus groups. In total, eight focus groups were conducted, with participation from 142 different individuals representing over 95 organizations.

Security Functions of Supported Applications

An enumeration of the security functions performed by PK-enabled applications was generated to clarify the boundaries of PKI. That analysis is attached here to assist the reader in understanding the allocation of security functions between PKI, which is a supporting infrastructure service, and the applications, which are responsible for the security protection of their information.

PKI support enables the implementation of security services by supported applications in a common, interoperable manner. Supported applications are responsible for proper use of the security object supplied by PKI. In particular, supported applications are responsible for proper verification of certificates and other PKI-generated objects prior to relying on information contained in those objects.

The following examples illustrate ways in which supported applications can employ PKI products and services to increase security of their operations, and provide enhanced capabilities to their users. These examples are intended to be illustrative, do not constitute an exhaustive list of the ways PKI support might be used by DoD applications, and do not impose any PKI-related requirements on any existing, under-development, or future application. The imposition of requirements to implement the security services identified in these examples in any particular application must be handled through the requirements development process for that application.

The security services described in this attachment are performed by the supported applications, and do not represent requirements for the PKI.

- *Perform user I&A.* Virtually all DoD information systems need to identify their users, in order to check access rights, maintain audit trails, and for a variety of other functions. Identity certificates issued by PKI provide a basis to authenticate the identity of the user presenting the certificate. This authentication may be used to
 - Verify the identity of the sender of an electronic mail (e-mail) message
 - Determine the identity of a user requesting information from a web server
 - Provide confirmation of a server's identity to a user requesting information from that server
 - Provide a single sign-on capability to multiple information systems based on the presentation of the public key certificate as proof of identity
 - Verify the sources of contract solicitations and bids transferred electronically

- Prove the identity of the originator of an electronic prescription
- Verify that the clearance information associated with a facility visit request was sent by the security office of the visitor's home facility
- *Provide data confidentiality.* The large volume of sensitive and classified information handled with DoD information systems must be protected, particularly when in-transit between information systems. In addition, the sender of information often needs some level of confidence that only the intended recipient receives the information in a usable form. Encryption certificates issued by PKI provide supported applications with a basis for implementing encrypted connections on an as-needed basis. These encrypted channels may be used to:
 - Protect the content of an e-mail message from being read by anyone other than the intended recipient(s), thereby providing writer-to-reader confidentiality of the message content
 - Protect sensitive medical information transiting DoD and connected networks (e.g., encryption of sensitive test results back to the individual tested, encryption of test results being transferred to a consulting physician)
 - Provide confidentiality of C4I information exchanged among tactical and strategic military information systems
 - Prevent the content of web pages delivered by a server from being read by anyone other than the authenticated user who requested the information
 - Provide need-to-know separation of information on secure networks by segregating that information cryptographically
 - Prevent viewing of force readiness information being transferred between military headquarters by unauthorized or foreign parties
 - Prevent competing vendors bidding on a military procurement from reading one another's proposals
 - Encrypt targeting information sent to weapons systems to ensure opposing forces cannot determine where US weapons are aimed
 - Protect the privacy of personal information pertaining to DoD personnel such as salaries, promotion and disciplinary actions, and humanitarian information exchanges between DoD and organizations such as the Salvation Army and the Red Cross
- *Protect data integrity.* Virtually all DoD information systems require the ability to transfer and store information with confidence that it is not modified during transmission or while in storage. PKI will support data integrity validation by providing the keys and related information necessary to apply integrity protections to information, permitting a supported application to use verification mechanisms to detect modifications to the information. Such integrity protection is useful in numerous applications:
 - Ensuring orders and other forms of command and control information are not modified during transmission between echelons of command

- Verifying that contract solicitations and responses are received exactly as sent, without information modifications obstructing fair, competitive procurement processes
 - Protecting patients against potential in-transit modifications of the medication or dosage specified in an electronic prescription
 - Ensure that medical test results are not tampered with for either the benefit or the harm of the subject of the tests
 - Ensure detection of modifications to geospatial or targeting information being disseminated to weapons systems
 - Ensure that software updates delivered in electronic form are in-fact unmodified and came from the proper source
 - Protect network routing information as it is disseminated to the backbone routers in the DISN
 - Ensure information stored on media (e.g., tape, floppy disk, optical media) has not been altered during storage
- *Provide non-repudiation of origin and/or receipt.* In many applications, it is necessary for one or both of the participants in an exchange to have positive confirmation of the involvement of the other party¹³. The security services enabled by PKI products such as certificates and CRLs make such non-repudiation possible. This security capability can be used to:
 - Prove that orders to employ US weapons against specific targets were actually given, and came from a legitimate source
 - Provide contractors bidding on a procurement a positive confirmation that their proposal was received by the appropriate contracting office prior to the specified deadline for proposal submissions
 - Support the tracking of medical test results and analyses as they are exchanged among medical facilities and personnel
 - Provide positive confirmation to a commander that orders he has issued were received by a subordinate unit
 - *Perform access control.* The control of access to data objects and other network resources is a supported application responsibility, and each application designer must incorporate a suitable access control approach. Within DoD, access control will often require a mixture of enterprise-level and lower-level access control process. Access control at the application level may include the creation, protection, interpretation, and display of labels indicating the sensitivity of information, and the restriction of access to the labeled information to users

¹³ Non-Repudiation blocks the sender's false denial that the sender sent a particular message. Whereas authentication of identity may be sufficient for applications where the sender needs only to convince the recipient of her identity, the legal requirements of many applications require non-repudiation sufficiently robust for the recipient to prove to a third party such as a judge that the sender's denial was false.

who possess the necessary authorizations. Supported applications can take advantage of PKI support for enterprise-level access control by:¹⁴

- Using authenticated user identities as a basis for retrieving the security attributes of that user from a directory or other data store
- Processing PKI-generated objects containing attributes and attribute definition and interpretation information
- Recognizing and verifying associations between attribute certificates and public key identity certificates
- Making and enforcing access control decisions based on user attributes and information and/or resource sensitivities, supported by PKI-disseminated objects supplying interpretation information for user security attributes.

¹⁴ The items here are intended as examples, and are in no way intended to imply that supported applications are obliged to base any portion of their access control solution on the use of PKI-certified attributes.

Glossary

Assurance Levels: The level of assurance of a public key 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 defined in the US DoD X.509 CP document the following four levels:

Class 2: (Formerly Basic) This level is intended for applications handling information of low value (Unclassified) or protection of system high information in a low to medium risk environment such as SIPRNet. This assurance level does not require that the end user register in person and their cryptography can be software based. Note: DoD will use Class 3 certificates to support Class 2 applications.

Class 3: (Formerly Medium) This level is intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that typically require identification of an entity as a legal person, rather than merely as a member of an organization. This assurance level requires that the end user register in person and their cryptography can be software based.

Class 4: (Formerly High) This level is intended for applications handling medium to high value information in any environment. These applications typically require identification of an entity as a legal person, rather than merely a member of an organization. This level requires a hardware token for protection of the private key material. This assurance level requires that the end user register in person, and that the cryptography be hardware based.

Class 5: This level is intended for applications handling classified information in a high-risk environment (over an open or unprotected network). This assurance level requires NSA-approved Type I cryptography.

Attribute: Information of a particular type. Certificates can contain attributes that convey information about their subjects. An attribute normally has a type, which indicates the class of information it conveys, and one or more values that are the actual information.

Attribute Certificate: A set of attributes of a user together with some other information, rendered unforgeable by the digital signature created using the private key of the certification authority which issued it.

Authentication: A process used to ascertain the identity of a person, process, or component.

Certificate: A computer-generated record that ties the user's identification with the user's public key in a trusted bond. The certificate contains the following (*at a minimum*): identity of the issuing Certification Authority and the user, and the user's public key.

Certificate Policy (CP): Defines requirements for the creation and management of public-key certificates for use in PKI capable applications.

Certification Authority (CA): The CA is an entity authorized by the Policy Management Authority (PMA) to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process,

publication of certificates, revocation of certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under the DoD X.509 Certificate Policy are performed in accordance with the requirements, representations, and warranties of that Policy.

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing certificates.

Certificate Revocation List (CRL): A computer-generated record that identifies certificates that have been revoked or suspended prior to their expiration dates. It is periodically issued by each certification authority and posted to the directory.

Confidentiality: A security service that protects information from unauthorized disclosure.

Digital Signatures: 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.

Electronic Attack: That division of electronic warfare involving the use of electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

Electronic Warfare: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

Encryption: The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (*one-way encryption*) or cannot be obtained without using the inverse decryption process.

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.

Evolutionary Acquisition: Evolutionary acquisition is a streamlined acquisition strategy that fields a core capability, with a modular open structure and provides for additional future increments in capability upgrades.

Format Sensitive Information: Unclassified information regarding DoD capabilities, infrastructure, personnel and/or operational procedures when electronically aggregated in significant volume that could adversely affect the national interest, the conduct of federal programs or the privacy of an individual if lost, misused, accessed, or modified in an

unauthorized way. Includes information that may be subject to public disclosure but requires protection when in electronic format.

Global Combat Support System (GCSS): The essential capabilities, functions, activities, and tasks necessary to support and sustain all elements of military forces engaged in military operations. Within the national and theater logistics systems, it includes that support rendered by service forces in ensuring the aspects of supply, maintenance, transportation, forces health protection, engineering and other services required by aerospace, naval, and ground combat troops to permit those units to accomplish their missions. GCSS is both a strategy and material solution(s) that provides information interoperability across combat support functions and between combat service support and command and control functions (GCCS) in support of the Joint War Fighter.

Global Combat Support System (Commander in Chief/Joint Task Force): A GCCS application provided the CINC and JTF commanders with combat support information. The components of GCSS (CINC/JTF) provide a fully integrated, scaleable, seamless, user-friendly information technology capability that provides near real-time access to information for mission planning and operation to any authorized user, any place, any time. GCSS (CINC/JTF) utilizes current technologies and integration strategies to access disparate source systems to fuse data that will allow the warfighter to make timely, informed decisions.

Information Assurance (IA): Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Exchange Requirements: The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as why the information is necessary and how that information will be used. The quality (i.e. frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement.

Interoperability: (1) The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to make use the services, units, or forces and to use the services so exchanged to enable them to operate effectively together. (2) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.

Integrity (Data Integrity): The service that protects information from unauthorized and undetected modification.

Joint Technical Architecture (JTA): The JTA provides DoD systems with the basis for the needed seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or improved systems throughout DoD. The JTA is structured into service areas based on the DoD Technical Reference Model (TRM). The DoD TRM originated from the Technical Architecture Framework for Information Management

(TAFIM), and was developed to show which interfaces and content needed to be identified. The JTA consists of two main parts: the JTA core, and the JTA Annexes. The JTA core contains the minimum set of JTA elements applicable to all DoD systems to support interoperability.

Key Management Infrastructure (KMI): The framework and services that provide for the generation, production, distribution, control, accounting and destruction for all cryptographic key material, symmetric keys as well as public keys and public key certificates.

Key Performance Parameters (KPPs): Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a ORD KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the Joint Requirements Oversight Committee (JROC). ORD KPPs are included in the APB.

Local Registration Authority (LRA): *See Registration Authority.*

Materiel Solution: A defense acquisition program (non-developmental, modification of existing systems, or new program) that satisfies identified mission needs.

Mission Need: A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance existing capabilities) through the use of new technologies. They are expressed in broad operational terms by the DoD components.

Mission Need Statement (MNS): A formatted non-system-specific statement containing operational capability needs and written in broad operational terms. It describes required operational capabilities and constraints to be studied during the Concept Exploration and Definition Phase.

Mission Performance Measurement: The assessment of effectiveness and efficiency of PKI in support of the achievement of an organization's missions, goals, and quantitative objectives through the application of outcome-based, measurable and quantifiable criteria compared against an established baseline to activities, operations and processes.

Non-materiel Solution: Changes in doctrine, tactics, training, or organization to satisfy identified mission needs. MNSs with an identified non-materiel solution are sent to the Military Departments for consideration and action.

Non-Repudiation: Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

Objective: An operationally significant increment above the threshold. An objective value may be the same as the threshold when an operationally significant increment above the threshold is not significant or useful.

Operational Requirements: A system capability or characteristic required to accomplish approved mission needs. Operational (including supportability) requirements are typically performance parameters, but they may also be derived from cost and schedule. For each parameter, an objective and threshold value must also be established.

Operational Requirements Document (ORD): A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each milestone beginning with Milestone I.

Operator: An operational command or agency that employs the acquired system for the benefit of users. Operators may also be users.

Organizational Registration Authority (ORA): *See Registration Authority.*

Policy Management Authority (PMA): A body established by the Department of Defense to oversee the creation and update of certificate policies; provide timely, responsive, DOD Service and Agency coordination to the DOD CP through a consensus-building process; review the Certification Practice Statements (CPS) of DOD operated CAs; review the results of CA compliance audits; and make recommendations to the CAs and to the PMA regarding corrective actions, or other measures that might be appropriate. This body also establishes the suitability of non-DOD policies for use within the DOD and offers recommendations to the DOD Program and Project Managers and DOD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the DOD certificate policies for specific applications.

Private Key: The part of a key pair to be safeguarded by the owner. A private key is used to generate a digital signature. Private keys are used to decrypt information, including key encryption keys during key exchange. It is computationally infeasible to determine a private key given the associated public key.

Public Key: The part of a key pair released to the public. The signer's public key is used to verify a digital signature. Public keys are used for encryption, including the encryption of privacy keys during key exchange.

Public Key-Enabled (PK-enabled) Application: A software application that uses public key technology to: authenticate its users, ensure information is not changed or modified either during transmission or storage, hold users responsible and accountable for their actions and representation, or encrypt information between parties where prior arrangement is neither known nor practical.

Public Key-Enabled (PK-enabled) Device: A device that uses public key technology to authenticate its interactions with other PK-enabled devices, authenticate users requesting services, provide integrity and/or confidentiality for information it transmits and receives, or otherwise provide security protection for its operation.

Public Key Infrastructure (PKI): The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates.

Registration Authority (RA): Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates. The terms local registration authority (LRA) and organizational registration authority (ORA) are also used.

Registration Manager (RM): KMI term for role granted to those KMI users responsible for authenticating and submitting identity credential requests. This role is similar in scope to the role of RA in the existing DoD Class 3 PKI. RMs are also able to request key establishment certificates, revoke certificates and request recovery of a key establishment key.

Relying Party (RP): A Relying Party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of a certificate, relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.

Requirement: The need of an operational user, initially expressed in broad operational capability terms in the format of a MNS. It progressively evolves to system-specific performance requirements in the ORD.

Root Certification Authority: The Root CA is a trusted entity responsible for establishing and managing a PKI domain by issuing CA certificates to entities authorized and trusted to perform CA functions.

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.

Security Policy Information File: A file that contains domain-specific security policy information, such as classification and labeling information.

System Capabilities: Measures of performance such as range, lethality, maneuverability, and survivability.

System Characteristics: Design features such as weight, fuel capacity, and size. Characteristics are usually traceable to capabilities (e.g. hardening characteristics are derived from a survival capability) and are frequently dictated by operational constraints (e.g., carrier compatibility) and/or the intended operational environment (e.g., NBCC).

Tactical Environment: Geographic area of operation in which actual or simulated combat, or VIP activity is occurring. This excludes strategic or fixed-base facilities.

Threshold: A minimum acceptable operational value below which the utility of the system becomes questionable.

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.

Type 1 Product: Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services, or controls. Type 1 products contain classified NSA algorithms. They are available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

User: An operational command or agency that receives or will receive benefit from the acquired system. CINCs and their Service component commands are the users. There may be more than one user for a system. The Service component commands are seen as users for systems required to organize, equip, and train forces for the CINCs. The Chiefs of the Services and heads of other DoD components are validation and approval authorities and are not viewed as users.

Abbreviations and Acronyms

AIS	Automated Information System
ASC C3I	Assistance Secretary of Defense (Command, Control, Communications and Intelligence)
BCA	Bridge Certification Authority
C2	Command and Control
C4I	Command, Control, Communications, Computers and Intelligence
CA	Certification Authority
CAC	Common Access Card
CI	Capability Increment
CINC	Commander in Chief
CIO	Chief Information Officer
CNA	Computer Network Attack
COE	Common Operating Environment
COP	Common Operational Picture
COTS	Commercial off-the-shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRD	Capstone Requirements Document
CRL	Certificate Revocation List
DECC-D	Defense Enterprise Computer Center - Detachment
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DPG	Defense Planning Guidance
EA	Electronic Attack
ECA	External Certification Authority
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
FPKI	Federal Public Key Infrastructure
GAO	General Accounting Office
GCCS	Global Command and Control System
GCSS	Global Combat Support system
GCSS (CINC/JTF)	Global Combat Support System (Commander in Chief/Joint Task Force)
GDS	Global Directory Services

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

GIG	Global Information Grid
GOTS	Government Off-The-Shelf
GPS	Global Positioning System
HERO	Hazards of Electromagnetic Radiation to Ordnance
HSI	Human Systems Integration
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IA	Information Assurance
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
INE	In-Line Network Encryptors
INFOSEC	Information Systems Security
IO	Information Operations
ISO	International Standards Organization
IT	Information Technology
ITU	International Telecommunications Union
IW	Information Warfare
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JTF	Joint Task Force
KMI	Key Management Infrastructure
KPP	Key Performance Parameter
KRA	Key Recovery Archive
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MILSATCOM	Military Satellite Communications
MNS	Mission Need Statement
NATO	North Atlantic Treaty Organization
NBCC	Nuclear, Biological, Chemical Contamination
NIAP	National Information Assurance Partnership
NIPNet	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSSI	National System Security Information
NSTISSC	National Telecommunications and Information Systems Security Committee
O&M	Operations and Maintenance
OCSP	On-line Certificate Status Protocol
ORA	Organizational Registration Authority
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
PC	Personal Computer

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PMO	Program Management Office
RA	Registration Authority
RAPIDS	Real-time Automated Personnel Identification System
RCAS	Reserve Component Automation System
RM	Registration Manager
RP	Relying Party
SIPRNet	Secret Internet Protocol Router Network
SPIF	Security Policy Information File
TAFIM	Technical Architecture Framework for Information Management
TCP/IP	Transmission Control Protocol / Internet Protocol
TED	Threat Environment Description
TRM	Technical Reference Model
UJTL	Uniform Joint Task List
US	United States
VAC	Volts – Alternating Current
W3C	World Wide Web Consortium
WARM	Wartime Reserve Modes

Tables

ORD KPP Summary

Section	Requirement Area	Threshold	Objective
4.1.1	Generate public key certificates.	Provide the specified functionality; Respond to certificate requests within 30 seconds, exclusive of communications delays	Provide the specified functionality; Respond to certificate requests within 10 seconds, exclusive of communications delays
4.1.2	Supply public key certificates	Provide the specified functionality	Provide the specified functionality
4.1.3	Support multiple cryptographic algorithms and algorithm migration	Provide the specified functionality	Provide the specified functionality
4.1.4	Provide key pairs and certificates	Provide the specified functionality	Provide the specified functionality
4.1.5	Program subscriber tokens.	Provide the specified functionality	Provide the specified functionality
4.1.6	Distribute PKI Root Certificate	Provide the specified functionality	Provide the specified functionality
4.1.7	Support subscriber mobility	Provide the specified functionality	Provide the specified functionality
4.1.8	Provide registration process.	Provide the specified functionality	Provide the specified functionality
4.1.9	Provide renewal, update, & re-key processes.	Provide the specified functionality; Respond to certificate requests within 30 seconds, exclusive of communications delays	Provide the specified functionality; Respond to certificate requests within 10 seconds, exclusive of communications delays
4.1.10	Provide revocation processes	Provide the specified functionality; Post CRLs once daily and within 6 hours of compromise notice being received by the CA (non-tactical); Post CRLs one daily and within 1 hour of compromise notice being received by the CA, for compromises within the tactical area of operationa (tactical)	Provide the specified functionality; Post CRLs once daily and within 15 minutes of compromise notice being received by the CA (non-tactical); Post CRLs one daily and within 10 minutes of compromise notice being received by the CA, for compromises within the tactical area of operationa (tactical)
4.1.11	Recover from compromise.	Provide the specified functionality	Provide the specified functionality

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

Section	Requirement Area	Threshold	Objective
4.1.12	Provide key recovery services.	Provide the specified functionality	Provide the specified functionality
4.1.14	Maintain of PKI-generated security objects archive.	Provide the specified functionality	Provide the specified functionality
4.1.16	Provide PKI interoperability.	Provide the specified functionality; Interoperate with the Federal PKI	Provide the specified functionality; Interoperate with other PKIs in addition to the Federal PKI
4.2.8	Interoperability KPP	Satisfy 100% of IERS designated critical to the specified standards	Satisfy 100% of IERS to the specified standards

IER Matrix

UJTL Entries Selected for Rationale. Since all of the IERs for the PKI involve support for information assurance, Uniform Joint Task List (UJTL) entries that emphasize information operations, information warfare, or infrastructure protection were selected for the rationale column of the IER matrix.

- **SN 3.4.4 Protect National Strategic Capabilities.** To safeguard strategic forces, critical facilities (political, economic, informational, military), national strategic center(s) of gravity, and force potential by reducing or avoiding the effects of enemy strategic level actions (lethal or non-lethal). This task includes hardening or fortifying facilities or construction for forces, removing hazards affecting execution of the national military strategy, and ensuring friendly effective use of the electromagnetic spectrum. (JP 3-01.1, 3-01.5 (*JP 3-10, 3-10.1, 6-0*))
- **SN 5.5 Coordinate Worldwide Information Warfare (IW).** To integrate the elements of offensive and defensive IW such as physical destruction, military deception, psychological operations, electronic attack, operations security, and other IW capabilities in order to affect an adversary's information, information-based processes, and information systems while defending one's own. This task includes military support to attacking and defending IW aspects of national military, political, and economic power. (JP 3-13.1, CJCSI 3210.01 (*JP 2-0, 3-0*))
- **ST 6.3.5 Protect Theater Information Systems.** To coordinate theater-wide activities to protect information and defend information systems. This task includes integrating and synchronizing indigenous and national IW defensive capabilities with joint force capabilities, ranging from technical security measures (such as Information Security [INFOSEC]) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes). Information protection includes producing the theater policies and procedures designed to ensure integrity, authenticity, availability, and confidentiality of information. Information system defense includes defensive measures, detection and reporting of attacks or intrusions, and the initiation of restoration and response processes. (JP 3-0, 3-13.1, 3-54, 3-58, 6-0 (*JP 1-02, CJCSI 3210.01*))

Selection of Critical Items in IER Matrix. The basic rationale for selection of critical information exchanges in the IER matrix was the identification of exchanges without which the basic role of the PKI cannot be fulfilled. Exchanges involving human beings were excluded; only exchanges between information systems were considered as candidates to be critical exchanges. Information exchanges that correspond to objective-level capabilities of the PKI (e.g., trusted time stamp request/response) were also excluded as critical exchanges. There are intra-PKI exchanges that would logically be considered critical (e.g., a RA requesting a certificate revocation by a CA), however the IER matrix only addresses exchanges between the PKI and external entities so the intra-PKI exchanges do not appear¹⁵.

¹⁵ Per CJCSI 6212.01B, Enclosure B, paragraph 3.b: "For ORDs, top-level IERs are defined as those information exchanges that are external to the system."

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

Rationale / UJTL Number	Event/Action	Information Characterization	Sending Node	Receiving Node	Critical	Format/Protocol	Frequency / Timeliness	Classification / Information Protection	Optional Notes
SN 3.4.4, SN 5.5, ST 6.3.5	Human User Registration	Subscriber identity and authentication	Human PKI User	PKI Registration Authority	No	Face-to-face interaction	Goal is for PKI interactions to occur quickly enough for overall registration to occur within time to issue a Common Access Card (< n minutes [T/O]).	Unclass to Secret	This happens at initial registration, and re-registration at a frequency as required by the DoD CP. Suitable documentation of individual identity is also per DoD CP requirements. Information is typically unclassified but may be classified SECRET under some circumstances.
SN 3.4.4, SN 5.5, ST 6.3.5	PK-Enabled Device Registration	Device identity and characteristics	PK-Enabled Device Administrator	PKI Registration Authority	No	Face-to-face interaction	Goal is for PKI interactions to occur quickly enough for overall registration to occur within < n minutes [T/O]+H10.	Unclass to Secret	This happens at initial registration, and re-registration at a frequency as required by the DoD CP. Suitable documentation of the device is also per DoD CP requirements. Information is typically unclassified but may be classified SECRET under some circumstances.
SN 3.4.4, SN 5.5, ST 6.3.5	User identity and attribute confirmation request / response	Name of subscriber, attributes of subscriber	PKI Registration Authority Workstation (embedded in RAPIDS workstation)	DEERS Database	Yes	HL7 / X12 / TCP-IP, per DEERS Specifications	Request / response processing time <60 seconds (T), <30 seconds (O), not including communications delays	Unclass	Routine, bi-directional interaction. This interaction will take place with each user registration verified through DEERS. Security protections will be determined by capabilities of the DEERS interface. Integrity protection of request and response will be provided if supported by the DEERS database interface.
SN 3.4.4, SN 5.5, ST 6.3.5	User identity and attribute confirmation request / response	Name of subscriber, attributes of subscriber	PKI Registration Authority Workstation	Other Authoritative Databases	No	Per Defined Interfaces of Existing Databases	Request / response processing time <60 seconds (T), <30 seconds (O), not including communications delays	Unclass to Secret	Routine, bi-directional interaction. This interaction will take place with each user registration verified through a personnel database. Security protections will be determined by capabilities of database. Integrity protection of request and response will be provided if supported by the database interface. Information is typically unclassified but may be SECRET under some circumstances. This interface supports verification of users whose information does not appear in DEERS but exists in other personnel information databases.

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

Rationale / UJTL Number	Event/Action	Information Characterization	Sending Node	Receiving Node	Critical	Format/Protocol	Frequency / Timeliness	Classification / Information Protection	Optional Notes
SN 3.4.4, SN 5.5, ST 6.3.5	Public Key Certificate request	Subscriber (human, device, application) identity and characteristics; public key if generated by RA WS or subscriber token or device.	PKI Registration Authority Workstation	CA	Yes	Industry-standard certificate enrollment protocol (e.g., ...)	Request / response processing time <30 seconds (T), <10 seconds (O), not including communications delays	Unclass to Secret	PKI internal interface. Requires I&A of PKI RA to CA, integrity protection of request, confidentiality protection of private key (if any). Request / response processing needs to support integration into routine administrative procedures (e.g., personnel in-processing)
SN 3.4.4, SN 5.5, ST 6.3.5	Public Key Certificate	Public key certificate; encrypted private key if key pair generated by CA	CA	PKI Registration Authority Workstation	Yes	Industry-standard certificate enrollment protocol (e.g., ...)	Request / response processing time <30 seconds (T), <10 seconds (O), not including communications delays	Unclass to Secret	PKI internal interface. Requires I&A of PKI CA to RA, integrity protection of request, confidentiality protection of private key (if any). Request / response processing needs to support integration into routine administrative procedures (e.g., personnel in-processing)
SN 3.4.4, SN 5.5, ST 6.3.5	Certificate delivery	Public key certificate; encrypted private key if key pair not generated by token.	PKI Registration Authority Workstation	Token	Yes	Industry-standard token interface protocol (e.g., ...)	<1 minute (T), <10 seconds (O) to program token with certificate (and private key if not generated by token)	Unclass to Secret	Protected by security protections supported by token interface protocols. Must protect confidentiality of private key if transferred via this interface.
SN 3.4.4, SN 5.5, ST 6.3.5	Certificate delivery	Public key certificate; encrypted private key if key pair not generated by device.	PKI Registration Authority Workstation or CA	PK-Enabled device	Yes	Industry-standard device interface protocol (e.g., ...)	<1 minute (T), <10 seconds (O) to program device with certificate (and private key if not generated by device)	Unclass to Secret	Protected by security protections supported by token/device interface protocols. Must protect confidentiality of private key if transferred via this interface.
SN 3.4.4, SN 5.5, ST 6.3.5	Human User Certificate Revocation	Certificate revocation request / information	Human Subscriber	PKI Registration Authority	No	Face-to-face or authenticated communication per DoD CP requirements	No timeliness requirements on this human/PKI interaction	Unclass to Secret	Revocation request needs source authentication, integrity protection, and ideally non-repudiation.
SN 3.4.4, SN 5.5, ST 6.3.5	PK-Enabled Device Certificate Revocation	Certificate revocation request / information	PK-Enabled Device Administrator	PKI Registration Authority	No	Face-to-face or authenticated communication per DoD CP requirements	No timeliness requirements on this human/PKI interaction	Unclass to Secret	Revocation request needs source authentication, integrity protection, and ideally non-repudiation.

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

Rationale / UJTL Number	Event/Action	Information Characterization	Sending Node	Receiving Node	Critical	Format/Protocol	Frequency / Timeliness	Classification / Information Protection	Optional Notes
SN 3.4.4, SN 5.5, ST 6.3.5	Certificate Revocation	Certificate revocation request / information	PKI Registration Authority Workstation	CA	No	Industry-standard certificate management protocol (e.g., ...)	Request / response processing time <60 seconds (T), <30 seconds (O), not including communications delays	Unclass to Secret	PKI internal interface. Requires I&A of PKI RA to CA, integrity protection of revocation request. Notifies CA of subscriber request for revocation, initiates CA action to place revoked certificate(s) on CRL.
SN 3.4.4, SN 5.5, ST 6.3.5	Publish PKI-generated objects	Certificates (including cross-certificates), CRLs	CA	DII Directories (e.g., GDS)	Yes	Industry-standard directory interface protocol (e.g., X.500 DAP, LDAP)	Each PKI object published to directory in <60 seconds (T), <30 seconds (O), not including communications delays	Unclass to Secret	Security protections will be determined by capabilities of directory. Time for updated PKI objects to be disseminated throughout the directory is a directory performance issue beyond the scope of PKI.
SN 3.4.4, SN 5.5, ST 6.3.5	Certificate status information	Certificate status information	CA	On-line status responder	No	Industry-standard interface protocol (TBD)	Updated revocation information published to on-line responder in <6 hours (T), <15 minutes (O) of compromise notice reception by CA. For tactical environments, these times are <1 hour (T), <10 minutes (O) for compromises within the area of operations.	Unclass to Secret	Security protections will be determined by capabilities of status protocol. Protocols may vary by device vendor.
SN 3.4.4, SN 5.5, ST 6.3.5	Cross-certification Establishment	Certificate request / response information	Root CA	Other PKI CAs	No	Industry-standard certificate enrollment protocol (e.g., ...) or off-line on media	No timeliness requirements on this interaction	Unclass to Secret	Bi-directional interface. Very infrequent event. Cross-certification typically involves a high degree of procedural security in addition to technical security protections of the data. Cross-certifications must be implemented IAW DoD CP. Cross-certification is not complete unless both CAs have received and processed a certificate request. This is not a time-critical or performance critical interface.

UNCLASSIFIED

DoD Target PKI Operational Requirements Document

Rationale / UJTL Number	Event/Action	Information Characterization	Sending Node	Receiving Node	Critical	Format/Protocol	Frequency / Timeliness	Classification / Information Protection	Optional Notes
SN 3.4.4, SN 5.5, ST 6.3.5	Time synchronization	Time request / response	PKI elements (any of CA, RA, time stamping service, digital notarization service)	External Time Reference Source	No	Industry-standard time synchronization protocol (e.g., ...)	Request / response processing time <30 seconds (T), not including communications delays	Unclass	Bi-directional interface. Example time source would be master clocks at the U.S. Naval Observatory.
SN 3.4.4, SN 5.5, ST 6.3.5	On-line Certificate Status Verification	Certificate status request (certificate to be verified), Certificate Status	PK-enabled applications	On-line status responder	Yes	Industry standard certificate status protocol (e.g., OCSP)	Request / response processing time <30 seconds (T), <10 seconds (O), not including communications delays	Unclass to Secret	Bi-directional interface. Classification depends on environment (e.g., NIPRNet, SIPRNet). Security protections will be those supported by certificate status protocol.
SN 3.4.4, SN 5.5, ST 6.3.5	Time stamp creation	Time stamp request (data [or hash]) to be stamped, Time stamp response	PK-enabled applications	Timestamp service	No	Industry-standard protocol (e.g., ...)	Request / response processing time <30 seconds (T), <10 seconds (O), not including communications delays	Unclass to Secret	Bi-directional interface. Classification depends on environment (e.g., NIPRNet, SIPRNet). Security protections will be those supported by time stamp protocol.
SN 3.4.4, SN 5.5, ST 6.3.5	Notarization	Notarization request (data [or hash]) to be notarized, Notarization response	PK-enabled applications	Digital notary service	No	Industry-standard protocol (e.g., ...)	Request / response processing time <30 seconds (T), <10 seconds (O), not including communications delays	Unclass to Secret	Bi-directional interface. Classification depends on environment (e.g., NIPRNet, SIPRNet). Security protections will be those supported by notarization protocol.

Example Candidate Protocols

- Network Time Protocol, Version 3, RFC 1305, March 1992
- Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, March 1999
- Internet X.509 Certificate Request Message Format, RFC 2511, March 1999
- PKCS 10: Certification Request Syntax Version 1.5, RFC 2314, March 1998
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 2560, June 1999

- X.500 Directory Access Protocol (DAP)
- Lightweight Directory Access Protocol (LDAP) (v3), RFC 2251, December 1997
- PKCS #11, Cryptographic Token Interface Standard, v2.10, December 1999
- PKCS #12, Personal Information Exchange Syntax Standard, v1.0, June 1999
- PKCS #15: Cryptographic Token Information Format Standard, v1.1, June 2000