ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000
May 17, 2001

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)

References:
(a) DoD Chief Information Officer Memorandum, subject: "Department of Defense (DoD) Public Key Infrastructure (PKI)," August 12, 2000
(b) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 13, 1999
(c) "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, November 13, 2000
(d) NSTISSP No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," January 2000
(e) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
(f) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements, June 30, 1998," authorized by DoD Directive 8910.1, "Management and Control of Information Requirements," February 11, 1993
(g) DoD Directive 5100.3, "Support of the Headquarters of Combatant and Subordinate Joint Commands," November 15, 1999

1. PURPOSE

1.1. Public key cryptography is a critical element of the Department's Information Assurance (IA) Defense-in-Depth technical strategy. The DoD Public Key Infrastructure (PKI) provides a foundation for interoperable, public key enabled (PK-enabled) security services at multiple levels of assurance. Beyond security considerations, the DoD PKI also offers the opportunity for process improvements in many business areas. It seeks to maximize the use of

Commercial-Off-the-Shelf (COTS) technology as appropriate in order to keep pace with technology evolution and to develop Government-unique solutions only when necessary.

1.2. Ref (a) directs the development and implementation of the DoD PKI and provides specific guidelines for applying PKI services throughout the Department. Availability of an infrastructure alone is not sufficient to meet the milestones set forth in Ref (a). Applications that use or are required to use public key cryptography must be enabled with the functionality and interfaces necessary to take advantage of the security services available. This memorandum provides specific guidelines for PK-enabling networks, web servers, and client software applications (hereafter referred to as applications) to provide security services at appropriate assurance levels. These guidelines are consistent with the requirements identified and governed by Ref (a).

2. APPLICABILITY

2.1. This memorandum applies to the Office of the Secretary of Defense (OSD); the Military Departments; the Chairman of the Joint Chiefs of Staff; the Combatant Commands; the Inspector General of the Department of Defense; the Defense Agencies and Offices (see Attachment); and the DoD field activities (hereafter referred to collectively as the "DoD Components" or "Components.")

2.2. This memorandum applies to all DoD unclassified and classified information systems except where expressly noted, and with the exception of Intelligence Community Sensitive Compartmented Information and information systems operated within the DoD that fall under the authority of the Director of Central Intelligence as provided for in Ref (b).

2.3. Global Information Grid (see Attachment) implementation must comply with policy and responsibilities established herein and, wherever applicable, separate and coordinated Director of Central Intelligence Directives and Intelligence Community Policy. To the extent possible, the DoD and Intelligence Community Chief Information Officers have agreed to use similar PKI processes and infrastructures.

3. DEFINITIONS

The terms "Class 3" and "Class 4" in this memorandum refer to the assurance levels of certificates issued by the DoD PKI. These and other terms are defined in the Attachment. Ref (c) contains detailed information on assurance levels and the creation and management of DoD PKI certificates.

4. POLICY

It is DoD Policy that:

4.1. In accordance with Ref (a):

4.1.1. All DoD unclassified networks that authenticate users, except as specified in 4.1.2, shall be PK-enabled for Class 3 hardware token, certificate-based access control conditional with the following:

a. Availability of commercial certificate based access control applications compatible with the network operating system; and

b. DoD PKI issuance of access control application compatible certificates on hardware tokens (e.g. CACs) to all users of given network.

Unclassified networks hosting Mission Category I systems (see Attachment) shall be given highest priority.

4.1.2. Unclassified DoD networks whose user communities belong predominantly to personnel categories not required to receive DoD PKI certificates in accordance with Ref (a), e.g., retirees, dependents, academia, are exempt from 4.1.1.

4.1.3. Unclassified DoD networks hosting Mission Category I systems shall migrate to Class 4 certificate-based access control no later than December 31, 2003.

4.2. All unclassified, private DoD web servers (see Attachment), except as specified in 4.2.1, shall be enabled to use Class 3 and/or Class 4 certificates for server authentication and client/server authentication in accordance with the timelines and criteria set forth in Ref (a).

4.2.1. Any unclassified DoD web server providing non sensitive, "publicly releasable", information resources that is categorized as a private web server (see Attachment) because it limits access to a particular audience only for the purpose of:

a. Preserving copyright protection of the contained information resources; or

b. Facilitating its own development; or

c. Limiting access to link(s) to limited access site(s) (and not the information resources), is exempt from 4.2.

4.3. Procurement of COTS applications that use or require the use of public key cryptography shall include requirements for interoperability and compatibility with the evolving DoD PKI.

4.4. Development authorities for applications that use or require the use of public key cryptography shall ensure interoperability with the DoD PKI in accordance with standards developed by the DOD PKI Program Management Office (PMO). This includes incorporation of Class 3 (with DoD PKI hardware token) requirements as a minimum and, when published, Class 4 requirements.

4.5. Email in all operating environments and web applications in unclassified environments shall be PK-enabled by October 2002 for use with Class 3 certificates in accordance with Ref (a). Email applications to include web e-mail applications, shall support both digital signature and encryption services. All other web applications shall support client authentication to the applicable private web server at a minimum. Email and web applications also shall be PK-enabled for Class 4 operation per the following schedule:

- No later than December 31, 2003 for Mission Category I applications operating on unclassified networks. Exempt from this date is the Defense Messaging System (DMS) High Grade of Service (HGS) application. HGS shall begin transitioning to the DoD PKI as soon as the DoD PKI is capable of satisfying the HGS requirements.
- No later than September 30, 2007 for all other operating environments.

4.6. Legacy, Mission Category I applications not addressed in Sec 4.5 that operate on unclassified networks and that use or require the use of public key cryptography shall be PK-enabled for Class 4 operation by December 31, 2003. Legacy applications scheduled for phase-out or replacement by this suspense date may be exempted.

4.7. All other legacy applications not addressed in Sec 4.5 or 4.6, in all other operating environments, that use or require the use of public key cryptography shall be PK-enabled to interoperate with the DoD PKI no later than September 30, 2007. This end date allows cost effective incorporation of these capabilities in conjunction with planned maintenance/upgrade activities for applications. Legacy applications scheduled for phase-out or replacement by this suspense date may be exempted if warranted by an economic analysis.

4.8. Applications that do not use or require the use of public key cryptography do not require PK-enabling. However, applications that will benefit from the use of public key cryptography should be strongly considered for inclusion if warranted by an economic analysis.

4.9. PK-enabled applications shall be tested to ensure interoperability and compatibility with the DoD PKI (see 5.4.3). As with all security-enabled products, PK-enabled applications and systems shall be acquired, certified, accredited, and installed in accordance with applicable national and DoD policy and guidance, e.g., References (d) and (e). Assurance requirements for PK-enabled applications shall be commensurate with the assurance requirements of other components of the system (e.g., Certificate Authorities and tokens).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, ASD(C3I), as the DoD Chief Information Officer (CIO), shall ensure that this policy is implemented in the context of the Global Information Grid (GIG) architecture. The ASD(C3I) shall manage the Defense-wide Information Assurance Program (DIAP) Office, which shall:

5.1.1. Provide compliance oversight to this policy. This oversight includes synthesizing and validating annual DoD Component reports and producing a summary report that analyzes overall DoD compliance with this policy. The DIAP Office will coordinate the content requirements, period of performance and the schedule for submission of the Component reports. Data will be collected only after obtaining an appropriate Report Control Symbol in accordance with Ref (f).

5.1.2. Develop and refine costs models, as appropriate, for use by DoD Components.

5.1.3. Identify and reconcile redundancies and duplication of effort in PK-enabling activities, in coordination with the affected DoD Components.

5.1.4. Publish and maintain a list of PK-enabled DoD applications, including COTS products verified to be interoperable and compatible with the DoD PKI.

5.1.5. Publish guidance and provisions to Component CIOs in the development of their waiver processes.

5.2. The Heads of DoD Components shall:

5.2.1. Ensure compliance with this policy within their respective organizations, including all necessary planning, programming, and budgeting activities. Components shall apply the criteria set forth in Section 4 to identify, prioritize, and schedule the PK-enabling of networks, web servers, and applications.

5.2.2. Investigate additional applications that may benefit from the use of public key cryptography and conduct an appropriate level of economic analysis to justify the enabling of these applications. All Components have a responsibility to look beyond the mandates of this policy and identify opportunities to improve information services and business processes with cost-effective use of the services available from the DoD PKI.

5.2.3. Assume responsibility to PK-enable applications for Joint programs and systems for which the Component is the executive agent, program management office, or equivalent.

5.2.4. Ensure that applications are enabled for use with appropriate assurance levels in accordance with Ref (a) and implement a strategy for migration to Class 4 operation.

5.2.5. Provide an annual report to ASD(C3I)'s DIAP Office. This report shall summarize status of policy compliance, including identification, prioritization, and scheduling of applications and systems to be enabled, projected cost, cost basis, and actual cost (for those delivered). (See section 5.1.1.)

5.2.6. Ensure successful completion of interoperability testing for PK-enabled applications using the centralized testing capability established by the DoD PKI PMO or via alternate testing capabilities in accordance with guidelines established by the DOD PKI PMO. (See section 5.4.3.)

5.2.7. Ensure that Component CIOs grant waivers only if in accordance with Section 6.

5.3. The Chairman of the Joint Chiefs of Staff, in addition to Section 5.2 responsibilities, shall ensure that the Joint Staff identify, review, and validate PK-enabling requirements for

Combatant Commands and ensure that Combatant Commanders coordinate requirements to implement this policy with their host Military Departments in accordance with Ref (g).

5.4. The DoD PKI Program Management Office shall:

5.4.1. Define and maintain DoD PK-enabling performance requirements, including all functional, interface, and testing requirements necessary for system/network access control, digital signature, and encryption. The requirements shall address all assurance levels and token forms supported by the DoD PKI.

5.4.2. Provide guidance on issues governing application operation with multiple assurance levels and transition between assurance levels.

5.4.3. Establish an independent, centralized testing capability to ensure application interoperability with the DoD PKI and develop minimum requirements for the establishment of Component-wide or other alternate testing capabilities. The PKI PMO shall ensure that alternate testing capabilities are in compliance with minimum requirements.

5.4.4. Provide guidance on appropriate use of commercial toolkits and other mechanisms that aid the process of PK-enabling applications, servers, and networks.

5.4.5. Ensure that DoD registration mechanisms include appropriate hardware token interfaces to support communities not using the Common Access Card.

5.5. The National Security Agency shall:

5.5.1. In conjunction with the DoD components, define application security specifications that are commensurate with the Class 4 system assurance requirements.

6. WAIVERS

DoD Component CIOs have the authority to waive compliance to this policy for individual applications on a case-by-case basis, consistent with the waiver guidelines and provisions published by the DIAP. Waivers shall be granted only for the minimum length of time required to achieve compliance. Approved waivers shall be reported to the DoD CIO within 15 days of approval.

7. EFFECTIVE DATE: This policy memorandum is effective immediately.

8. SUMMARY

Implementation of this policy will help to ensure that technical capabilities are in place to allow the use of public key cryptography consistent with the Department's Defense-in-Depth strategy, opportunities for business process improvement, evolving technology, and security risk management.

This policy will be reviewed on an annual basis in conjunction with Ref (a), to ensure that it remains consistent with Department-wide objectives and to ensure that it remains supported by technological progress in the area.

My point of contact for this action is Mr. Robert F. Lentz, Director of Information Assurance, (703) 695-8705 or email: robert.lentz@osd.mil.

Linton Wells II
Acting DoD Chief Information Officer

Attachment

ATTACHMENT

DEFINITIONS

Assurance Level - 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. This memorandum references enabling requirements for the following 2 classes (See the DoD X.509 Certificate Policy, Ref (c), for detailed definitions and guidance on usage):

> Class 3 - intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that require identification of an entity as a legal person, rather than merely a member of an organization. This assurance level requires that the end user register in person. This assurance level has been subdivided into components distinguished by protection of the private key either in software or hardware tokens. Software storage of the private key is acceptable in some environments, but per Ref (a), DoD will be migrating near-term to protection of the private key on hardware tokens, particularly the Common Access Card. Hence, Class 3-enabled applications must include an interface to a hardware token supported by the DoD PKI. This hardware token based assurance level, designated "Class 3 Hardware" offers a higher degree of assurance and technical non-repudiation than software based Class 3.
>
> Class 4 - intended for applications handling medium to high value information in any environment. These applications 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 private key material. The combination of all security controls that contribute to this assurance level involves a higher level of robustness than that required for Class 3. Not all environments require Class 4 operation near-term, but in accordance with Ref (a), DoD will gradually migrate to Class 4 usage across the Department, so applications should ensure Class 4 interoperability when feasible to allow for migration strategies that are as transparent as possible for its user community.

Defense Agencies and Offices - All agencies and offices of the Department of Defense, including Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Contract Management Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency/Central Security Service.

Global Information Grid (GIG) - (A) The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing,

disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

(B) Includes any system, equipment, software, or service that meets one or more of the following criteria:

(1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software and services.

(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services

(3) Processes data or information for use by other equipment, software and services

(C) Non GIG IT – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

Legacy Application - For the purposes of this memorandum, a legacy application is either an existing application or one in development/procurement whose contract solicitation (Request for Proposal or equivalent) is released no later than 120 days after the date of this memorandum.

Mission Category[1] - (GIG IA 6-8510 G&PM) Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

[1] Information system mission categories under this policy are defined with regard to the need for integrity and availability services relative to direct support of combat operations. The definitions of mission critical and mission essential information systems provided in DoDI 5000.2, Change 1, dated January 2001, take a more general view. While the 5000.2 definition of a mission critical system implies that such systems must be available at all times, neither 5000.2 definition speaks to the need for integrity services. Further, the definition of mission essential only reflects the importance of information relative to accomplishment of the organizational mission, not the warfighter's. None-the-less, it is safe to say that all mission category I and II systems are mission critical under the 5000.2 definition and all mission category III systems are mission essential. Thus, the names Mission Category I, II, and III replace the mission category names used in the August 12, 2000 PKI policy in order to avoid confusion with the DoDI 5000.2 definitions.

a. Mission Category I - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).

b. Mission Category II - Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

c. Mission Category III - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

Network - A network is composed of a communications medium and all components attached to that medium, including two or more computers, whose responsibility is the electronic exchange of information using a cohesive set of protocols.

Private Web Server - A web server that is designed for and/or provides information resources that are limited to a particular audience (i.e., DoD) or a subset thereof. (This includes web servers that provide interfaces to e-mail systems.) Any DoD operated web server that provides any information resources that are not intended for the general public shall be considered a private web server and is subject to this policy. A private web server restricts or attempts to restrict general public access to it. The common means of restriction are by the use of domain restriction (e.g., .mil and/or .gov), filtering of specific Internet Protocol (IP) addresses, User ID and/or password authentication, encryption (i.e., DoD certificates), and physical isolation. Personal web servers (i.e., those that only allow one user and are only accessible from the machine to which it is installed) are not subject to this memorandum.

Public Key-Enabled Application/Web Server/Network - A Public Key-Enabled (PK-Enabled) application or web server or network is one that can accept and process a DoD PKI X.509 digital certificate to support one or more application, server, or network-specific functions (digital signature, data encryption support, system/network access) that provide security services. PK-enabled applications interoperate with the DoD PKI to access public key certificates, revocation information (e.g. Certificate Revocation List (CRL)), and general information in public directories or repositories.

Public Key Infrastructure - The framework and services that provide the generation, production, distribution, control, tracking and destruction of public key certificates.

Token - A device (e.g., floppy disk, Common Access Card, smart card, PC Card, Universal Serial Bus device, etc.) that is used to protect and transport the private keys of a user. Per Ref (a), the primary hardware token selected for DoD use is the Common Access Card.

Web Application - Web browser and other distributed applications characterized by a web interface and both back-end (server) and front-end (client) software.