COMMAND, CONTROL,
COMMUNICATIONS
AND INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

August 12, 2000

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: Department of Defense (DoD) Public Key Infrastructure (PKI)

References: (a) Deputy Secretary of Defense (DEPSECDEF) Memorandum, subject: "Department of Defense (DoD) Public Key Infrastructure (PKI)," May 6, 1999 (Hereby Canceled)
(b) DEPSECDEF Memorandum, subject: "Smart Card Adoption and Implementation," November 10, 1999
(c) DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," June 13, 1999
(d) "X.509 Certificate Policy for the United States Department of Defense," Version 5.0, December 13, 1999
(e) "Public Key Infrastructure Roadmap for the Department of Defense," Version 3.0, October 29, 1999

This memorandum reissues reference (a) to update DoD policies for the development and implementation of a Department-wide PKI. As authorized by reference (b), this memorandum aligns PKI activities and milestones with those of the DoD Common Access Card (CAC) program.

Achieving Information Superiority in a highly interconnected, shared-risk environment requires that DoD's Information Assurance (IA) capabilities address the pervasiveness of information as a vital aspect of warfighting and business operations. The technical strategy that underlies DoD IA is Defense-in-Depth, in which layers of defense are used to achieve our security objectives. This strategy recognizes the diversity of technologies, solutions, adversaries, and vulnerabilities that pervade our information systems and infrastructures. It seeks to maximize the use of COTS technology as appropriate in order to keep pace with technology evolution and to develop GOTS solutions only when necessary.

One element of the Defense-in-Depth strategy is the use of a common, integrated, interoperable DoD PKI to enable security services at multiple levels of assurance. The DoD PKI will provide a solid foundation for IA capabilities across the Department. The goal of this DoD-wide infrastructure is to provide general-purpose PKI services to a broad range of applications, at levels of assurance consistent with operational imperatives. The Department must take an aggressive approach in acquiring and using a PKI that meets our requirements for all IA services. This policy encourages widespread use of public key-enabled applications and provides the following specific guidelines for applying PKI services throughout the Department.

- **Applicability and Scope.**

  - 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 Definitions section); and the DoD field activities (hereafter referred to collectively as the "DoD Components.")

  - DoD PKI certificates shall be issued, as defined herein, to all active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractor personnel, who have access to a DoD Automated Information System (AIS). DoD PKI certificates may be issued to other personnel categories (retirees, dependents, eligible non-U.S. personnel, etc.) as necessary if access is required to a PKI-enabled DoD AIS. This memorandum applies to all DoD unclassified and classified information systems 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 reference (c).

  - Global Information Grid 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.

- **Selection of Appropriate DoD PKI Certificate Assurance Levels**. To ensure consistent, proper usage of different assurance levels across the Department, DoD PKI certificates will be issued with assurance levels in accordance with minimum criteria defined in reference (d), as summarized below:

  - **Class 3 Certificates:** All DoD users shall be issued a Class 3 certificate by October 2002. Class 3 is the minimum assurance level certificate provided by the DoD PKI. Protection of Mission Critical systems operating on unclassified networks <u>and employing public key technology</u> must be via Class 3 certificates at a minimum. These systems shall complete migration to Target Class 4 certificates and tokens by December 31, 2003. All other applications <u>that employ public key technology</u> (e.g., unclassified or classified Mission

Critical systems on encrypted networks using NSA Type 1 approved encryption, and system-high Mission Support/Administrative systems on any classification network) must use Class 3 certificates at a minimum.

- **Class 4 Certificates:** Unclassified Mission Critical systems that employ public key technology must migrate to Target Class 4 certificates and tokens by December 31, 2003.

- **Evolution of DoD certificates**. DoD's goal is a single, interoperable, high assurance PKI. Thus, in addition to the accelerated transition requirements for Mission Critical systems stated above, DoD will evolve to Target Class 4 certificates for all environments and applications that employ public key technology. DoD organizations shall begin to issue Target Class 4 certificates by October 2002. Class 3 will continue to be supported in parallel with Target Class 4 for a finite period to allow for natural expiration of certificates and graceful evolution of applications. Class 3 certificates may be issued through December 2004.

- **PKI Tokens.** The CAC will be the primary token platform for both Class 3 and Target Class 4 certificates used in unclassified environments for active duty military personnel, members of the Selected Reserve, DoD civilian employees, and eligible contractors. Class 3 certificates may be distributed on software tokens as necessary until October 2002 to meet near-term operating requirements. The DoD PKI Program Management Office (PMO) will define the assurance requirements for Class 3 and Target Class 4 hardware tokens.

- **Deployment of DoD PKI Registration Capability**. To meet DoD IA objectives on a widespread basis and to field interoperable public key cryptography within the Department as soon as possible, the registration capability (i.e., trained personnel and installed software/hardware for registration operations) for the Class 3 PKI shall be implemented in accordance with reference (d) by December 31, 2001, with upgrades for the Target Class 4 PKI implemented by October 2002. The user identification process shall meet the trust requirements for Class 3 and Class 4 in accordance with reference (d). Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) workstations integrated with PKI capability shall be the primary registration platform. PKI Local Registration Authorities (LRAs) will be needed to support requirements of classified systems and to provide device certificates. PKI LRAs also may be fielded as necessary to support near-term and tactical requirements. LRAs are available today to support limited near-term requirements. To support the requirements of reference (b), DEERS/RAPIDS initial operational capability will occur no later than December 2000.

- **The DoD PKI Certificate Types and Content**. The DoD PKI will issue identity certificates and encryption certificates. Note: The current Class 3 implementation includes "identity", "email signature", and "email encryption" certificates. To provide a data recovery capability, the DoD PKI will support key recovery for private keys associated with encryption certificates (includes only the "email encryption" certificate in the current Class 3

implementation.) So that certificates may be provided with common parameters throughout DoD, the Class 3 certificates will have a minimum/common set of attributes (e.g., citizenship, government/non-government employee, service, or agency affiliation). Additionally, some DoD programs (e.g., Defense Message System) will require attribute certificates.

- **External Certificate Authorities**. Secure interoperability between DoD and its vendors and contractors will be accomplished using External Certificate Authorities (ECAs). ECAs will operate under a process that delivers the level of assurance that is required to meet business and legal requirements. Operating requirements for ECAs will be approved by the DoD Chief Information Officer, in coordination with the DoD Comptroller and the DoD General Counsel. An Interim ECA (IECA) capability is currently available. Requirements for *interoperable PKI-enabled services with Industry partners* shall be met via certificates generated from an IECA or ECA.

- **Web Server Access Control via Public Key Techniques**. Protection of DoD information resident on private web servers must be improved. Unclassified, private web servers, i.e., those not accessible to the general public, (see Definitions section) shall be issued Class 3 (at a minimum) DOD PKI server certificates by December 31, 2000. The servers shall, by the same date, use this certificate for server authentication via the Secure Sockets Layer (SSL) protocol or better. By October 2002, all private DoD and DoD-interest web servers located on unclassified networks shall require client identification and authentication using Class 3 user certificates. For access to Mission Critical web servers on unencrypted networks, in accordance with the *Selection of Appropriate DoD PKI Certificate Assurance Levels* paragraph above, transition from a Class 3 certificate to a Target Class 4 certificate is required for client identification and authentication no later than December 31, 2003. Certificate-based access control for classified web servers is encouraged, and requirements for classified web servers in this area will be provided in future guidance pending further study of technical and resource issues.

- **Digitally Signed Electronic Mail**. To accelerate improved protection of information exchanged within the Department, all electronic mail (as distinct from organizational messaging) sent within the Department will be digitally signed by October 2002. Components are encouraged to encrypt e-mail within the Department. The certificates used for digital signature and encryption will be the identity and encryption certificates issued by the DoD PKI. Note: The current Class 3 implementation uses "email signature" and "email encryption" certificates for this purpose.

- **Enabling of Networks and Applications.** DoD unclassified networks shall be enabled for hardware token, certificate-based access control no later than October 2002, with organizations beginning this migration in December 2000, when Class 3 certificates on CACs will be available. Unclassified networks hosting mission critical systems shall migrate to certificate-based access control using Target Class 4 tokens no later than December 31, 2003. Further guidance on enabling applications will be provided in a separate

memorandum. Hardware token-based access control to classified networks is encouraged, and requirements for classified networks in this area will be provided in future guidance pending further study of technical and resource issues.

- **Responsibilities.**

  - **The DoD Chief Information Officer (CIO)** shall ensure that this policy is implemented in the context of the GIG Architecture. The DoD CIO shall manage the Defense-wide Information Assurance Program (DIAP), which shall perform the following activities: provide central oversight of DoD PKI activities; develop PKI planning guidance for inclusion within the DoD's planning, programming, budgeting, and execution system; provide guidance to the Department's functional communities on implementation and integration of PKI during business process reengineering; conduct a study of technical and resource issues and provide recommendations regarding PKI-enabled access control to classified DoD networks and classified DoD private web servers.

  - **The DoD Components** shall be responsible for planning, programming, and budgeting to implement the DoD PKI according to this policy and to develop the required policy and plans to ensure a standard implementation of the DoD PKI within their respective organizations; coordinate with the DoD PKI PMO and DIAP in these duties as required; immediately transition from use of any non-DoD PKI to the DoD PKI.

  - **The USD(P&R)** shall, in addition to responsibilities outlined for DoD Components, serve as the Department's focal point for issues related to the DEERS/RAPIDS infrastructure; develop and field the required DEERS/RAPIDS infrastructure to support the complete life cycle management activities of the DoD PKI certificates for Class 3 and Target Class 4; develop policies and plans to provide the required operational support to the aforementioned activities for the following PKI certificate subscribers: Active Duty Military, Selected Reserve, DoD Civilians, and Eligible Contractors.

  - **The Director DoD PKI PMO** shall serve as the program manager for all PKI-related actions and shall manage all centralized tasks involved in definition, development, installation, integration, integrated logistics support, training, and acceptance testing of the DoD PKI and DoD PKI products; provide guidance and oversight to organizational infrastructure implementation efforts as necessary to ensure consistency across DoD.

Implementation of this policy will ensure that future uses of public key cryptography as part of the Department's Defense-in-Depth strategy are consistent with threat and risk tolerance. The DoD PKI PMO shall update and coordinate references (d) and (e) as necessary within 90 days of this memorandum's issuance.

This policy memorandum is effective immediately and will be reviewed on an annual basis to ensure that the policy remains consistent with evolving technology and Department-wide

objectives. My point of contact for this action is Mr. Richard C. Schaeffer, Jr., Director, Infrastructure & Information Assurance, 703-695-8705.

Arthur L. Money
DoD Chief Information Officer

Attachment

ATTACHMENT

DEFINITIONS

Automated Information System (AIS). A combination of computer hardware and software, data, or telecommunications that performs functions such as collecting, processing, transmitting, and displaying information. This also encompasses an AIS environment that includes systems, applications, telecommunications, and other components of information technology.

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.

Digital Signature. "Digital signature" or "digitally signed" refers to a transformation of a message using an asymmetric cryptosystem such that a person who has the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made."

External Certificate Authority. An agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities.

Mission Category. (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 warfighter's combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

a. **Mission Critical**[1] 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).

[1] This definition of Mission Critical is operationally focused and differs from that in the Clinger-Cohen Act of 1996 as well as the one used for reporting to Congress under Section 8121 of the FY 2000 Defense Appropriations Act, both of which pertain to information technology procurement, not information or mission assurance support to deployed forces.

b. Mission Support. 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. Administrative. 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).

PKI Certificate. A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

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.) 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, userid and/or password authentication, encryption (i.e., DoD certificates), and physical isolation. 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. 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.

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.