Department of Defense

DIRECTIVE

NUMBER 8190.3
August 31, 2002
Certified Current as of November 21, 2003

ASD(C3I)/DoD CIO

SUBJECT: Smart Card Technology

References: (a) Deputy Secretary of Defense Memorandum, "Smart Card Adoption and Implementation," November 10, 1999 (hereby canceled)
(b) Section 113, Note, title 10, United States Code
(c) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," January 11, 2002
(d) Chapter 25 of title 40, United States Code, "Information Technology Management Reform"

1. PURPOSE

This Directive:

1.1. Supersedes reference (a) and establishes policy and assigns responsibilities regarding the use of smart card technology, as it applies to individuals, within the Department of Defense consistent with references (b) and (c).

1.2. Establishes the Smart Card Senior Coordinating Group (SCSCG), as directed by reference (b).

1.3. Disestablishes the Smart Card Configuration Management Control Board (SCCMCB), established in reference (a).

2. APPLICABILITY AND SCOPE

This Directive 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, the DoD Field

Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components"); the U.S. Coast Guard under agreement with the Department of Transportation (DoT), when not operating as a Military Service under the Department of the Navy; the Commissioned Officers Corps of the U.S. Public Health Service (USPHS) under agreement with the Department of Health and Human Services (DHHS); and the Commissioned Officers Corps of the National Oceanic and Atmospheric Administration (NOAA) under agreement with the Department of Commerce (DoC). The term "Uniformed Services" refers to the Army, the Navy, the Marine Corps, the Air Force, the Coast Guard, their respective National Guard and Reserve components, the Commissioned Corps of the USPHS, and the NOAA Corps.

3. DEFINITIONS

3.1. Integrated Circuit Chip. A small piece of semiconducting material (usually silicon) on which an integrated circuit is embedded. A typical chip can contain millions of electronic components (transistors).

3.2. Smart Card. A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuits and also may employ one or more of the following technologies: magnetic stripe, bar codes (linear and two-dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication, or photo identification.

3.3. Smart Card Technology. A smart card, together with all of the associated information technology hardware and software, that comprise the system for both support and operation.

3.4. Public Key Infrastructure (PKI). The framework and services that provide the generation, production, distribution, control, accounting, record keeping, and destruction of private key pairs for authentication, electronic signature, and encryption/decryption.

4. POLICY

It is DoD policy that:

4.1. DoD Chief Information Officer (CIO)-developed or approved Department-wide interoperability standards for use of smart card technology shall be implemented.

4.2. Smart card-based technology and systems shall be used to transform and improve security in DoD processes and mission performance thereby enhancing readiness while also improving business processes.

4.3. Smart card use and applications shall be based on open-system configuration, interoperable with commercial and Government use, consistent, to the maximum extent practical given security requirements of the Department of Defense, with commercial industry best practices and standards.

4.4. DoD security and information assurance programs shall support a secure operating environment for smart card technology and operations to ensure the confidentiality and integrity of information and the protection of sensitive data.

4.5. Smart card technology shall be applied in the form of a Department-wide common access card (CAC) that shall be:

4.5.1. The standard identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, [1] eligible contractor personnel, and eligible foreign nationals.

4.5.2. The Department's primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment.

4.5.3. The principal card enabling physical access to buildings, facilities, installations, and controlled spaces. This policy does not require the DoD Components to dismantle immediately current access systems, or preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC (e.g., such as entrance into a Sensitive Compartmentalized Information Facility (SCIF) or other high security space). However, the Heads of the DoD Components are to plan for migration to the CAC for general access control using the CAC's present or future access control capabilities.

4.6. The CAC shall be produced by the DoD Realtime Automated Personnel Identification System (RAPIDS) based on data supplied by the DoD Defense Enrollment Eligibility Reporting System (DEERS).

---

[1] Exception: Civilian employees of the Intelligence Community (e.g., National Security Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, and National Reconnaissance Office) are authorized a CAC from RAPIDS workstations when their appropriate personnel data has been submitted and verified in DEERS.

4.7. Consistent with reference (d), an SCSCG shall be established under the DoD CIO and shall be composed of senior representatives from each of the Armed Forces and DoD Components (enclosure 1) or organizations as identified and recommended by the SCSCG membership. The SCSCG shall be chaired by an official (Flag/SES) designated by the Secretary of the Navy, in accordance with reference (b). The SCSCG, in accordance with reference (b), shall:

4.7.1. Oversee the development of and recommend Department-wide interoperability standards for use of smart card technology.

4.7.2. Oversee the development of and recommend a plan to exploit smart card technology as a means for enhancing readiness and improving business processes.

4.8. The categories of individuals eligible for a CAC, as delineated in subparagraph 4.5.1., above, may expand when required and resources are available.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence/DoD Chief Information Officer, consistent with references (c) and (d), shall:

5.1.1. Serve as the Principal Staff Assistant for smart card technology and provide overall policy, oversight, and direction for applying smart card technology throughout DoD missions and functions.

5.1.2. Approve the appointment of the Chairperson of the SCSCG.

5.1.3. Ensure the integration and interoperability of cross-functional requirements and approve the allocation of space for data elements for joint applications and space for DoD Component use on CAC storage media based on recommendations from the SCSCG.

5.1.4. Coordinate with the Under Secretary of Defense (Personnel and Readiness) (USD(P&R)) on the DoD CAC design.

5.1.5. Oversee the development of the CAC, in coordination with the USD(P&R) and the DoD Components, and submit planning, programming, and budgeting documents necessary to support acquisition, sustainment, and implementation of DoD smart cards and smart card technology to the Under Secretary of Defense (Comptroller).

5.1.6. Provide guidance to the Department's functional communities on implementation of PKI and/or ICC in business process reengineering and electronic business.

5.1.7. Develop CAC interoperability guidance and standards as prescribed in reference (c) for inclusion within the DoD Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance architecture.

5.1.8. Develop and employ performance measures to ensure the CAC, its supporting network, and the PKI technology components perform as intended.

5.2. The Under Secretary of Defense (Personnel and Readiness) shall:

5.2.1. Develop, in coordination with the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))/DoD CIO and the DoD Components, the DoD CAC design.

5.2.2. Develop and field the required DEERS/RAPIDS infrastructure and all elements of field support to issue and sustain the CAC, and provide responsive technical support to fielded DEERS/RAPIDS installations to ensure the sustainability of quality CAC operations.

5.2.3. Provide technical support and program management to the ASD(C3I)/DoD CIO, and technical and executive secretariat support to the SCSCG on matters relating to smart card technology and use.

5.3. The Under Secretary of Defense (Comptroller) shall advise and assist the ASD(C3I)/DoD CIO in the development and coordination of planning, programming, and budgeting documents necessary to ensure the effective and efficient acquisition, sustainment, and funding of smart cards, smart card technology, interoperability, and related infrastructure within the Department of Defense.

5.4. The OSD Principal Staff Assistants, in executing their authority for assigned functional areas, shall:

5.4.1. Examine and advocate the applicability of smart card technology and systems in support of accomplishing assigned missions and functions.

5.4.2. Designate a smart card focal point to prioritize and integrate requirements for the implementation of smart card technologies, including the CAC, in support of this Directive and the SCSCG.

5.4.3. Sponsor and review funding requirements for the acquisition and use of smart card technology within their assigned missions and functions, recommending

appropriate adjustments and allocations, through the Planning, Programming, and Budgeting System process.

5.5. The Secretaries of the Departments of the Army, the Navy, and the Air Force, each shall establish a project office to develop implementation plans for exploiting the capability of smart card technology as a means for enhancing readiness and improving business processes in accordance with reference (b).

5.6. The Secretary of the Navy, as prescribed in reference (b), shall nominate a senior official (Flag/SES) to Chair the SCSCG.

5.7. The Heads of the DoD Components shall:

5.7.1. Designate an organizational entity to serve as the DoD Component smart card advocate to promote and develop implementation plans for exploiting the capability of smart card technology as a means for enhancing readiness and improving business processes in accordance with reference (b) and to interface with the DoD Smart Card Program, including representing their Component-unique smart card requirements within their mission/functional areas' integrated architectures, smart card storage allocations, and physical designs, respectively, as prescribed by the ASD(C3I)/DoD CIO and the USD(P&R).

5.7.2. Field the requisite infrastructure needed to use the CAC (i.e., smart card readers, middleware, office space for workstations, communications availability, etc.).

5.7.3. Implement Smart Card Technology policy consistent with this Directive and their labor relations' obligations.

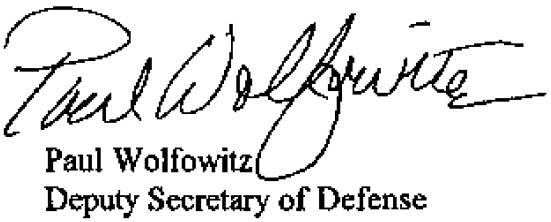
5.7.4. Provide sufficient personnel resources to ensure timely implementation and maintenance support of the CAC and its supporting infrastructures.

5.7.5. Submit reports on CAC performance, implementation progress, and quality of maintenance support consistent with the performance measures established by the DoD CIO.

5.8. The Director, Administration and Management, shall be responsible to carry out subparagraphs 5.7.1. through 5.7.3., above, within the Office of the Secretary of Defense.

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 1
E1. Smart Card Senior Coordination Group (SCSCG) Membership

E1. ENCLOSURE 1

SMART CARD SENIOR COORDINATING GROUP (SCSCG) MEMBERSHIP

E1.1.1. A General Officer/Flag Officer or SES representative from each of the following organizations, unless exempted by the Chair, are designated as members of the SCSCG:

E1.1.1.1. Military Departments and Coast Guard.

E1.1.1.2. Offices of the OSD Principal Staff Assistants.

E1.1.1.3. Other DoD Components, as necessary.

E1.1.1.4. Defense Manpower Data Center.

E1.1.1.5. DoD PKI Program Management Office.

E1.1.1.6. Other organizations as identified and approved by the SCSCG.