DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

19 May 2003

MEMORANDUM FOR DISTRIBUTION

Subj: SMART CARD AND PUBLIC KEY INFRASTRUCTURE (PKI) POLICY

Ref: (a) Under Secretary of the Navy Memorandum, Subj: "Department of the Navy Leadership for Smart Card," 02 April 1999
(b) Under Secretary of Defense Personnel and Readiness (P&R)/Department of Defense Chief Information Officer (CIO) Memorandum, Subj: "Common Access Card (CAC)," 16 January 2001
(c) Assistant Secretary Defense Command, Control, Communications, and Intelligence (C3I) Memorandum, Subj: "Public Key Infrastructure (PKI) Policy Update," 21 May 2002
(d) Department of Defense (DoD) Directive 8190.3, Subj: "Smart Card Technology," 31 August 02
(e) DoD Configuration Management Plan for the Common Access Card v1.1, 17 Sep 01

Purpose. To issue Department of the Navy (DON) policy for the coordination, management, and implementation of smart card and public key infrastructure (PKI) technologies.

Scope and Applicability. In accordance with references (a) through (e), this document governs the use of smart card and public key infrastructure technologies for the DON. Although the most prolific smart card is the Common Access Card (CAC), other card systems such as financial smart cards used for stored value or electronic purses and contactless radio frequency cards used for physical access are also covered by this memorandum. Smart Card Technology (SCT) will be integrated into IT systems to provide Public Key Infrastructure (PKI) access to information resources and services for all Department of Defense (DoD) personnel. The CAC is the DoD's primary physical access badge, principal DoD PKI token carrier for unclassified systems, and new DoD identification card for military, DoD civilian, and designated DoD contractors. This document establishes SCT and PKI guidance associated with implementation, coordination, and configuration management.

Definitions

a. Common Access Card: A type of smart card that is the DoD military identification card, personnel identification card for civilian and selected contractor personnel, principal DoD PKI token carrier, and principal physical access badge.

b. 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.

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

d. Smart Card reader: A device used to exchange information between smart cards and computers.

e. Smart Card Middleware: A software product needed to communicate between smart cards and computers applications (i.e. Internet browsers and electronic mail applications). Typically this communications is conducted through smart card readers.

f. 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.

Discussion. The organization, functions, and services provided by DON information technology systems are undergoing significant changes. This is due in part to the rapid growth in the Department's need to process vast amounts of information in a timely and secure manner. The use of Smart Card and PKI technologies are key components of the DON's strategy to meet its information challenges by providing streamlined business processes and strong authentication. It is the Department's vision to use smart cards as authentication tools for web-based transactions. We will strive to minimize the amount of data stored on cards rather than use them as extensive portable data carriers.

In accordance with references (a) and (d), the Department of the Navy Chief Information Officer (DON CIO) serves as the senior official in the DON for CAC-SCT strategic direction, policy guidance, and oversight; represents the DON at DoD and federal CAC-SCT committees, workgroups, standards development bodies, and consortia; and coordinates DON participation in DoD, national, international and interdepartmental boards, committees, and other organizations involving CAC-SCT matters. Additionally, DON CIO represents the Secretary of the Navy as chairman of the DoD Smart Card Senior Coordinating Group (SCSCG), the statutory body responsible for overseeing smart card activities.

Policy. This policy governs the use of the smart cards and PKI for cyber and physical access as well as any other uses (e.g. financial transaction cards) within the DON. It is DON policy that:

a. The CAC and DoD PKI shall be used on unclassified networks to logon, sign all unclassified electronic mail (e-mail), and access all DOD unclassified private web sites in accordance with the items below.

(1) Every DON user, upon receipt of his or her CAC and availability of the required SCT, shall use the CAC for identification and authentication to unclassified networks and access to properly configured DOD private web sites.

(2) Once applicable organizations become NMCI enabled, including client smart card middleware and reader, the Director NMCI shall ensure the NMCI configuration supports this policy.

(3) Director, Space Information Warfare Command, & Control Division (CNO (N61)) and Director, Headquarters Marine Corps Command, Control, Communications, and Computers (HQMC C4) shall ensure that non-NMCI ashore (CONUS and OCONUS) activities receive the required SCT to comply with this policy.

(4) CNO (N61) and HQMC C4 shall incrementally implement PKI in the tactical environment, as the capability and resources to support and sustain tactical PKI and SCT-CAC infrastructures becomes available.

(5) As workstations are CAC-enabled, the CAC will be used as the token for all applications requiring digital signatures.

(6) Reference (c) currently requires all DON ashore (CONUS and OCONUS) activities, except for tactical networks, to comply with (1) through (5) above, by October 2003. This is a very aggressive timeline. Where possible, all DON ashore (CONUS and OCONUS) activities will strive to meet this mandate within the required timeframe.

(7) All DON tactical networks shall comply as soon as practicable.

b. The CAC shall be the principal card enabling physical access to DON facilities for those DON populations covered by the CAC in accordance with reference (c) section 4.5.3.

c. The configuration of all DON smart cards shall be managed to ensure Department-wide interoperability as set forth below.

(1) The DON Smart Card Configuration Control Board (SC CCB) consisting of members from DON EBUSOPOFF, CNO (N61), and HQMC C4 shall provide oversight for smart card configuration management and ensure consistency among DON smart cards.

(a) The DON EBUSOPOFF shall chair and facilitate the activities of the DON SC CCB.

(b) This board shall report to the DON CIO. Any issues not resolved by the DON SC CCB that require further attention shall be brought to the DON CIO for resolution.

(c) Requests for space allocations shall be submitted through the appropriate chain-of-command to the DON EBUSOPOFF. All allocation requests shall contain required assessment material to include, but not limited to, information on the purpose of the request, a business case analysis of initiative, the name of initiative sponsor, a risk assessment, and an illustration of the funding baseline. The DON EBUSOPOFF shall provide space allocation request material and recommendations to members of the DON SC CCB for review and approval.

(d) The Chair of the DON SC CCB shall coordinate with DON CIO a review of all approved space allocation requests prior to submission to DoD, in accordance with reference (d).

(e) The Chair of the DON SC CCB shall provide periodic updates on the CCB's activities to the DON CIO, DON Deputy CIO (Navy), and DON Deputy CIO (Marine Corps).

(2) Chip memory may be allocated for DON enterprise, USN-specific, or USMC-specific initiatives. The DON SC CCB shall focus and champion the migration of any duplicative Service-unique allocation requests towards DON enterprise initiatives. All DON enterprise initiatives shall require unanimous consent from the SC CCB members.

(3) No space shall be allocated without allocation requests being coordinated in accordance with above section c.1.d.

(4) The USN and USMC may establish Service-specific configuration management processes. These processes must comply with the overall DON Configuration Management Plan, and the results of any Service-specific process will be an allocation request submitted to the SC CCB via the DON EBUSOPOFF.

(5) USN or USMC functional managers and/or DON Functional Area Managers (FAM) that desire to utilize the CAC in their business areas should contact the appropriate SC CCB member for inclusion in the configuration management process.

d. DON CIO with the DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall conduct an annual flag-level review of the Department's progress in complying with this policy. Members of CNO (N61), HQMC C4, and DON EBUSOPOFF shall participate in this review.

Action

a. Within 60 days of this memorandum, all CNO Echelon II Commands and USMC Major Commands shall designate their smart card technology central point of contact (POC) to coordinate command activities and requirements. The designated POC information should be sent to CNO (N61) (ATTN: Bob Weilminster, COMM 703 601 1296, Robert.weilminster1@navy.mil) or HQMC C4 (ATTN: LtCol Brady, DSN 223-9970,

bradyfx@hqmc.usmc.mil). CNO (N61) and HQMC C4 shall provide all appropriate POCs in a consolidated list to the DON EBUSOPOFF (ATTN: Bonnie Armstrong, DSN 707-3420, bonita.Armstrong@navy.mil). The list shall become the Department's network of smart card technology managers.

b. Within 90 days of this memorandum, the DON EBUSOPOFF shall develop, implement, and disseminate a smart card configuration management plan based on the roles and responsibilities contained in this memorandum and complementary to reference (e). The plan shall outline a process in which configuration management requests and key issues can be vetted by Department stakeholders and raised to DON CIO. This shall be coordinated with CNO (N61) and HQMC C4, and approved by DON CIO.

Responsibilities

a. DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall:

(1) Receive periodic updates from the Chair of the DON SC CCB on the progress of the DON configuration management activities.

(2) Review material and participate in discussions about any unresolved DON configuration management item.

(3) Participate in an annual review of the Department's progress towards implementing this policy.

b. DON EBUSOPOFF shall:

(1) Serve as the DON smart card advocate to promote and develop implementation plans for:

(a) Exploiting the capability of SCT to enhance readiness and improve business processes;

(b) Interfacing, in coordination with DON CIO, with the DOD smart card program to:

1. Represent Component-unique smart card requirements within their mission/functional areas' integrated architectures

2. Allocate smart card storage and physical designs as prescribed by the ASD (C3I), DOD CIO and USD (P&R).

(c) Coordinating applicable portions of these implementation plans with DON CIO, HQMC C4, and CNO (N61).

(2) Implement DON CAC-SCT and *e*Business efforts to make DON IT and business processes more efficient and effective.

(3) Provide Smart Card-CAC pilot, prototype coordination and technical support.

(4) Manage CAC-SCT fielding and provide technical direction and integration support to assist field activities with implementing SCT.

(5) Serve as the Chair of the Smart Card Configuration Control Board (SC CCB).

(6) Publish and implement an approved DON smart card configuration management plan.

(7) Maintain technical documentation on SCT and document all aspects of the DON-specific space on the CAC.

(8) Working with the Chief of Information (CHINFO), provide Public Affairs guidance and material to DON sites receiving the CAC.

(9) Provide advisory services to the Department on CAC-SCT by conducting market research and environmental scanning; cataloguing industry and Government CAC-SCT solutions and best practices; and developing a process to identify and invest in pilot projects to foster the implementation of innovative CAC-SCT solutions throughout DON.

(10) Recommend configurations of smart card technologies and integrated solutions to DON CIO, DON policy makers and functional managers.

(11) Create and maintain a SCT information website containing items such as current SCT trends, guidance, frequently asked questions (FAQs), and more. This site should serve as a focal point where smart card users can direct questions and concerns.

c. CNO (N61) and HQMC C4 shall:

(1) Be the central liaison for smart card policy and oversight for their respective Service. Coordinating all relevant SCT-PKI activities within their chain of command to include:

(a) Coordinate CAC-SCT best practices to the maximum extent practical to improve both combat support capabilities and DON business operations.

(b) Ensure the insertion of CAC-SCT capabilities into the development, modernization, expansion or prototype of applicable unclassified systems.

(c) Support the development and updating of the DON CAC-SCT Strategic

and Implementation Plans.

(d) Develop, coordinate, and promulgate any additional CNO or CMC specific guidance needed to successfully implement CAC-SCT.

(e) Identify a subordinate command responsible for assisting activities in the Public Key Enabling of applications to use PKI credentials stored on the CAC.

(f) Participate and serve as member of the Smart Card Configuration Control Board (SC CCB).

(2) Assure representatives from CNO and HQMC personnel and manpower areas participate in CAC-related configuration management and policy activities.

(3) Assure representatives from CNO and HQMC physical security areas participate in CAC-related configuration management and policy activities.

(4) Designate a General Officer/Flag Officer or SES equivalent to represent their organizations on the Smart Card Senior Coordinating Group (SCSCG).

d. CNO Echelon II Commands and USMC Major Commands shall:

(1) Designate their smart card technology central point of contact (POC) to coordinate command activities and requirements.

(a) The designee may be required to liaise with the DON EBUSOPOFF and participate in Department-wide stakeholders meetings.

(b) Develop, coordinate, and promulgate any additional Echelon II or Major Command specific guidance needed to successfully implement CAC-SCT.

Effective date. This memorandum is effective immediately and will be incorporated in a SECNAV instruction.

The DON CIO point of contact for smart card technology policy is Mr. Robert Carey, 703-607-3420, DSN 327-4320, or Robert.carey@navy.mil.

D.M. Wennergren

Distribution: (see page 8)

Subj: SMART CARD AND PUBLIC KEY INFRASTRUCTURE (PKI) POLICY

Distribution:
Immediate Office of the Secretary (ASN (M&RA), ASN (RD&A), ASN (I&E), ASN (FM&C), AAUSN, GC)
Dept of the Navy Staff Offices (JAG, OLA, CHINFO, NAVINSGEN)
CNO (N09, N09B, N091, N093, N095, N096, N1, N2, N3/N5, N4, N6/N7, N8)
CMC (ACMC, C4, PP&O, M&RA, I&L, P&R, AVN, I, PA, AR)
COMPACFLT
COMLANTFLT
COMUSNAVEUR
COMSC
COMNETWARCOM
COMNAVAIRSYSCOM
COMNAVSUPSYSCOM
COMNAVSEASYSCOM
COMSPAWARSYSCOM
COMNAVNETSPAOPSCOM
COMNAVFACENGCOM
COMNAVSECGRU
CNET
BUMED
BUPERS
ONI
ONR
NAVOBSY
NAVPGSCOL
COMNAVLEGSVCCOM
COMNAVMETOCCOM
COMNAVPERSCOM
COMNAVRESFOR
DIRSSP
FLDSUPPACT
DIR NMCI
DON EBUSOPOFF
COMMARFORPAC
COMMARFORLANT
COMMARFORRES
COMMARFOREUR
CG MCCDC
COMARCORMATCOM
CG MCRC
CG TECOM
COMMARCORSYSCOM