ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

May 21, 2002

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARIES OF DEFENSE
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 SECRETARIES OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Public Key Infrastructure (PKI) Policy Update

References: (a) DoD Chief Information Officer Memorandum, subject: "Department of Defense (DoD) Public Key Infrastructure (PKI)," August 12, 2000
(b) DoD Chief Information Officer Memorandum, subject: "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)," May 17, 2001

This memorandum updates guidance in references (a) and (b) and outlines plans for reissuing DoD PKI policy. Reference (a) directs the development and implementation of the DoD PKI and provides specific guidelines for applying PKI services throughout the Department. It also mandates the Common Access Card (CAC) as the primary token platform for PKI certificates and designates the Real-time Automated Personnel Identification System (RAPIDS) as the primary registration platform. Reference (b) provides specific guidelines for enabling networks, web servers and client software applications to make use of the security services made available by the DoD PKI.

Key milestones of the policies are the completion of the PKI infrastructure and the subsequent completion of issuing PKI certificates to all eligible DoD personnel. Since the activation of DoD PKI Release 3 in late October 2001 CAC issuance has progressed smoothly and now exceeds a half million. The capacity to issue CACs is also increasing as the number of fielded RAPIDS capable of issuing the CAC continues to keep pace with the revised RAPIDS fielding schedule. Completion of RAPIDS fielding is now

expected to take place in May 2003 allowing for delivery of PKI certificates on the CAC to all eligible DoD personnel by October 2003.

Certificate issuance and other reference (a) and (b) requirements impacted by the revised RAPIDS fielding schedule and/or directed for completion by October 2002 are included in the following table along with revised implementation dates:

Applicable Policy	Existing October 2002 Requirement	Adjusted Milestone Date
Ref (a)	*Complete issuing Class 3 certs to all users*	October 2003
Ref (a), Ref (b) 4.2	*Client side authentication to DoD private web servers*	October 2003
Ref (a)	*Begin issuing Class 4 certificates*	October 2003
Ref (a) , Ref (b) 4.5	*All e-mail sent within DoD digitally signed*	October 2003
Ref (b) 4.5	*PK-enable web applications in unclassified environments*	October 2003
Ref (a), Ref (b) 4.1	*PK-enable DoD unclassified networks for hardware token, certificate-based access control*	October 2003

These tasks remain vital to the successful implementation of the DoD PKI and are expected to be completed without delay as infrastructure deployment progresses. All other PKI and PKE policy requirements not addressed in this memorandum remain in effect as specified in references (a) and (b).

A new policy document, updating and combining references (a) and (b) will be issued in June 2002, followed by a PKI directive later this year. It will include specific guidance and timelines for PKI implementation on the SIPRNET and in tactical environments.

Despite these necessary program adjustments, the DoD remains firmly committed to the CAC as the Department-wide standard implementation for PKI. Components should proceed with PKI implementations, taking into consideration delays in infrastructure deployment and CAC issuance in all related planning, programming, and budgeting activities. Components should also continue to support DoD PKI requirements, both CAC and non-CAC based, for specific programs and mission needs as they arise. I encourage active Commander in Chief, Service, Agency participation in the ongoing PKI policy revision to ensure PKI policy keeps pace with the evolution of technology, and serves the needs of the Department.

My point of contact for this memorandum and the PKI policy rewrite is Mr. Eric Moos, 703-614-2196 or email: Eric.Moos@osd.mil.

John P Stenbit

John P. Stenbit