

ADMINISTRATIVE MESSAGE

ROUTINE

R 011600Z MAY 03 ZYB PSN 704263M22

FM CNO WASHINGTON DC//N61//

TO COMLANTFLT NORFOLK VA//N00/N6//  
COMUSNAVEUR LONDON UK//N00/N6//  
COMPACFLT PEARL HARBOR HI//N00/N6/N69//  
OPNAVSUPPACT WASHINGTON DC//N00/N6//  
FLDSUPPACT WASHINGTON DC//N00/N6//  
COMNAVAIRSYSCOM PATUXENT RIVER MD//N00/N6//  
COMNAVAIRSYSCOM PATUXENT RIVER MD//N00/N6//  
COMUSNAVCENT BAHRAIN//N00/N6//  
COMNAVRESFOR NEW ORLEANS LA//N00/N6//  
COMNAVRESFOR NEW ORLEANS LA//N00/N6//  
CNET PENSACOLA FL//N00/N6//  
BUMED WASHINGTON DC//N00/N6//  
USNA ANNAPOLIS MD//N00/N6//  
USNA ANNAPOLIS MD//N00/N6//  
COMNAVSEASYSYSCOM WASHINGTON DC//N00/N6//  
CHNAVPER MEMPHIS TN//N00/N6//  
COMSC WASHINGTON DC//N00/N6//  
COMSC WASHINGTON DC//N00/N6//  
NAVWARCOL NEWPORT RI//N00/N6//  
NAVWARCOL NEWPORT RI//N00/N6//  
COMNAVSVPSYSCOM MECHANICSBURG PA//N00/N6//  
COMNAVLEGSVCCOM WASHINGTON DC//N00/N6//  
COMSPAWARSYSCOM SAN DIEGO CA//N00/N6/PMW161//  
NAVPGSCOL MONTEREY CA//N00/N6//  
COMNAVAFACENCOM WASHINGTON DC//N00/N6//  
COMNAVAFACENCOM WASHINGTON DC//N00/N6//  
NAVSTKAIRWARCEN FALLON NV//N00/N6//  
COMNAVSECGRU FT GEORGE G MEADE MD//N00/N6//  
DIRSSP WASHINGTON DC//N00/N6//  
COMNAVDIST WASHINGTON DC//N00/N6//  
COMNAVDIST WASHINGTON DC//N00/N6//  
PRESINSURV NORFOLK VA//N00/N6//  
ONI WASHINGTON DC//N00/N6//  
NAVOBSY WASHINGTON DC//N00/N6//  
COMNAVMETOCCOM STENNIS SPACE CENTER MS//N00/N6//  
COMNAVSPECWARCOM CORONADO CA//N00/N6//  
COMNAVSAFECEN NORFOLK VA//N00/N6//  
NAVHISTCEN WASHINGTON DC//N00/N6//  
NCTSI SAN DIEGO CA//N00/N6//  
COMNAVNETWARCOM NORFOLK VA//N00/N6/N64//  
COMNAVNETWARCOM NORFOLK VA//N00/N6/N64//  
  
INFO COMOPTEVFOR NORFOLK VA//N00/N6//  
HQUSMC WASHINGTON DC//C4//  
DON CIO WASHINGTON DC//IA//  
DCMS WASHINGTON DC//N00/N3/N5//  
DCMS WASHINGTON DC//N00/N3/N5//  
COMDT COGARD WASHINGTON DC//G-SCT//

BT  
UNCLAS //3420//

MSGID/GENADMIN/CNO WASH DC N61//

SUBJ/DOD PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION GUIDANCE//

REF/A/MEMO/ASD C3I/12AUG2000/-/NOTAL//

REF/B/MEMO/ASD C3I/17MAY2001/-/NOTAL//

REF/C/MEMO/ASD C3I/21MAY2002/-/NOTAL//

REF/D/RMG/CNO WASHINGTON DC/181413ZJUN2002//

NARR/REF A IS DOD PKI POLICY. REF B IS DOD POLICY FOR PUBLIC KEY (PK) ENABLING UNCLASSIFIED WEB SERVERS, APPLICATIONS, AND NETWORKS. REF C IS UPDATED DOD PKI POLICY MILESTONE MANDATES. REF D IS CNO GUIDANCE FOR THE IMPLEMENTATION OF REF A.//

POC/ROBERT WEILMINSTER/CIV/CNO N61424/LOC:WASHINGTON DC  
/EMAIL:WEILMINSTER.ROBERT@HQ.NAVY.MIL; (703)601-1296 [DSN:329-1296]//  
POC/SAMIR OTHMAN/CIV/CALLSIGN:PEO C4I AND SPACE PMW 161  
/LOC:SAN DIEGO CA  
/EMAIL:SAMIR.OTHMAN@NAVY.MIL; (619)524-7369 [DSN: 524-7369]//

RMKS/1. PURPOSE: THIS IS A PROGRAM EXECUTIVE OFFICE-COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE AND SPACE (PEO C4I AND SPACE) (PMW 161) AND CNO (N614) COORDINATED MESSAGE TO PROVIDE NAVY COMMANDS WITH GUIDANCE FOR THE IMPLEMENTATION OF DOD PKI. DOD PKI POLICY MANDATES ARE REITERATED TO ENSURE ALL COMMANDS ARE AWARE OF CURRENT PKI MILESTONES. THIS MESSAGE ALSO ANNOUNCES, IN PARAGRAPH 10 BELOW, THE DOD PKI USERS FORUM IN MYRTLE BEACH, SC ON 17-18-19 JUNE 2003 AND A NAVY BREAKOUT SESSION TO BE HELD IN CONJUNCTION WITH THE DOD FORUM ON 19-20 JUNE.

2. SCOPE: THIS GUIDANCE APPLIES TO ALL NAVY ACTIVITIES USING THE NIPRNET. POLICY AND GUIDANCE FOR THE USE OF DOD PKI ON THE SIPRNET IS STILL BEING DRAFTED AND WILL BE PROMULGATED BY SEPCOR.

### 3. BACKGROUND

A. THE OFFICE OF THE SECRETARY OF DEFENSE (OASD) DIRECTED THE IMPLEMENTATION OF A COMMON PKI ACROSS DOD TO ENHANCE THE DEPARTMENT'S INFORMATION ASSURANCE (IA) POSTURE. PKI PROVIDES THE SECURITY SERVICES OF AUTHENTICATION, IDENTIFICATION, CONFIDENTIALITY, DATA INTEGRITY, AND NON-REPUDIATION. PER REF A, DOD DIGITAL CERTIFICATES SHALL BE ISSUED TO AND USED BY ALL MILITARY, DOD CIVILIAN, ELIGIBLE DOD CONTRACTOR, AND ELIGIBLE NON-US PERSONNEL WHO ACCESS DOD COMPUTERS/NETWORKS. THE TOKEN WHICH HAS BEEN IDENTIFIED AS THE CARRIER FOR A USER'S PKI CREDENTIALS IS THE COMMON ACCESS CARD (CAC).

B. PKI IS A TECHNOLOGY THAT ENABLES SECURE TRANSMISSION OF DATA ACROSS COMPUTER NETWORKS AND PROVIDES THE FOLLOWING CAPABILITIES TO USERS:

- CONDUCT SECURE WEB TRANSACTIONS
- DIGITALLY SIGN EMAIL AND DOCUMENTS
- ENCRYPT EMAIL AND DOCUMENTS
- USE CREDENTIALS STRONGER THAN USERIDS AND PASSWORDS TO LOGIN TO

COMPUTER NETWORKS AND TO ACCESS APPLICATIONS

C. ALL NAVY USERS WILL BE REQUIRED TO USE DOD PKI CERTIFICATES TO AUTHENTICATE TO AND GAIN ACCESS TO NAVY INFORMATION RESOURCES (E.G., NETWORKS, APPLICATIONS, WEB SERVERS). ADDITIONALLY, NAVY PERSONNEL WILL USE DOD EMAIL SIGNING CERTIFICATES TO DIGITALLY SIGN OFFICIAL EMAIL. EMAIL ENCRYPTION CERTIFICATES CAN BE USED FOR PROVIDING CONFIDENTIALITY TO SENSITIVE BUT UNCLASSIFIED EMAIL.

4. DOD PKI MILESTONE MANDATES: REFS A THROUGH C ESTABLISH THE DOD PKI MILESTONES FOR THE USE OF PKI SECURITY SERVICES. INITIAL NAVY IMPLEMENTATION GUIDANCE WAS PROVIDED BY REF D. KEY NEAR TERM MILESTONES FOLLOW.

A. BY 01 OCTOBER 2003:

-ALL DOD USERS SHALL BE ISSUED DOD PKI CLASS 3 CERTIFICATES.

-ALL NAVY UNCLASSIFIED PRIVATE WEB SERVERS SHALL REQUIRE CLIENT-SIDE AUTHENTICATION USING DOD PKI IDENTITY CERTIFICATES.

-IT IS RECOMMENDED THAT PRIVATE WEB SERVERS POST A WARNING MESSAGE TO ADVISE USERS OF THIS UPCOMING REQUIREMENT. A WARNING SUCH AS "BEGINNING 01 OCTOBER 2003, ALL ACCESS TO THIS WEB SITE WILL BE RESTRICTED TO ONLY THOSE PERSONS POSSESSING VALID DOD PKI CERTIFICATES. SEE YOUR INFORMATION SYSTEM SECURITY MANAGER (ISSM)/INFORMATION SYSTEM SECURITY OFFICER (ISSO) FOR INFORMATION ON OBTAINING AND CONFIGURING YOUR DOD USER CERTIFICATES FOR WEB ACCESS."

-IT IS ALSO RECOMMENDED THAT PRIOR TO OCTOBER 2003 A GRADUAL IMPLEMENTATION OF THIS REQUIREMENT BE CONSIDERED. CONTACT THE PEO C4I AND SPACE POC FOR GUIDANCE.

-ALL OFFICIAL EMAIL SENT WITHIN DOD SHALL BE DIGITALLY SIGNED.

-DOD UNCLASSIFIED NETWORKS WILL BE PUBLIC KEY (PK) ENABLED FOR HARDWARE TOKEN CERTIFICATE-BASED ACCESS CONTROL.

B. BY 01 SEPTEMBER 2007:

ALL OTHER LEGACY APPLICATIONS IN ALL OTHER OPERATING ENVIRONMENTS THAT USE OR REQUIRE PK TECHNOLOGY SHALL BE PK ENABLED TO INTEROPERATE WITH DOD PKI.

5. THE FOLLOWING MILESTONE IS REITERATED TO ENSURE THAT ALL NAVY COMMANDS AND ACTIVITIES ARE AWARE OF AND HAVE IMPLEMENTED THE MANDATED SECURITY REQUIREMENT.

-BY 31 DECEMBER 2000: ALL UNCLASSIFIED NAVY PRIVATE WEB SERVERS SHALL HAVE IMPLEMENTED SERVER-SIDE AUTHENTICATION VIA DOD PKI SERVER CERTIFICATES AND SECURE SOCKETS LAYER (SSL).

CLARIFICATION: A PRIVATE WEB SERVER IS DEFINED AS A WEB SERVER THAT RESTRICTS OR ATTEMPTS TO RESTRICT GENERAL PUBLIC ACCESS TO THE WEB SERVER. ANY NAVY WEB SERVER THAT PROVIDES INFORMATION RESOURCES THAT ARE NOT INTENDED FOR THE GENERAL PUBLIC SHALL BE CONSIDERED A PRIVATE WEB SERVER AND IS SUBJECT TO THIS POLICY. THIS INCLUDES WEB SERVERS LOCATED BEHIND FIREWALLS AND/OR THOSE THAT ATTEMPT TO RESTRICT ACCESS BY USE OF PASSWORDS, IP ADDRESS/DOMAIN FILTERING, OR PHYSICAL ISOLATION.

6. PKI IMPLEMENTATION

A. NAVY ACTIVITIES WITH NIPRNET ACCESS AND A REQUIREMENT TO USE DOD EMAIL AND/OR DOD PRIVATE WEB SERVERS ARE DIRECTED BY DOD TO IMPLEMENT THE DOD PKI BY OCTOBER 2003. LOCAL PSDS OR SECURITY BADGING OFFICES WILL ISSUE USERS HARDWARE-BASED CLASS 3 PKI CERTIFICATES ON THE COMMON ACCESS CARD (CAC) IN TIME TO MEET THIS PKI MANDATE. AS A CONTINGENCY PLAN IN THE EVENT FULL DEPLOYMENT OF CARD READERS AND CACS IS NOT COMPLETED PRIOR TO THE OCTOBER 2003

DEADLINE, NAVY PERSONNEL MAY OBTAIN SOFTWARE CERTIFICATES (ON FLOPPY DISK) FROM A NON-NMCI LOCAL REGISTRATION AUTHORITY (LRA). COMMANDS SHOULD COORDINATE WITH THEIR CHAIN OF COMMAND TO ENSURE ACCESSIBILITY TO AN LRA FOR ISSUANCE OF SERVER AND/OR USER SOFTWARE-BASED CERTIFICATES. TRUSTED AGENTS (TAS) SHOULD BE ESTABLISHED WHERE LRAS ARE NOT READILY ACCESSIBLE. TAS DO NOT REQUIRE ANY SPECIAL SOFTWARE OR HARDWARE.

B. COMMANDING OFFICERS OF ACTIVITIES NOT SCHEDULED TO RECEIVE PKI THROUGH THE NAVY-MARINE CORPS INTRANET (NMCI) ROLLOUT, IN COORDINATION WITH THEIR CHAIN OF COMMAND AND PEO C4I AND SPACE, SHOULD SCHEDULE PKI IMPLEMENTATION FOR ALL THEIR ACTIVITIES. PEO C4I AND SPACE PKI ENGINEERS WILL ASSIST EACH NON-NMCI NAVY SHORE ACTIVITY WITH THEIR PKI IMPLEMENTATION. ASSISTANCE WILL INCLUDE INSTALLATION AND CONFIGURATION OF LRA WORKSTATIONS IF REQUIRED, ON-SITE PKI TRAINING FOR USERS AND SYSTEM ADMINISTRATORS, ON-SITE CARD READER AND MIDDLEWARE INSTALLATION TRAINING FOR SYSTEM ADMINISTRATORS, AND VALIDATION TESTING. A NAVY PKI HELP DESK WILL ALSO BE MAINTAINED TO ANSWER QUESTIONS.

C. THE ONLY APPROVED PKI IS THE DOD PKI. TO BE IN COMPLIANCE WITH DOD POLICY, NON-DOD PKIS MUST INITIATE TRANSITION TO DOD PKI. SUCH TRANSITIONS MUST BE COMPLETED BY OCTOBER 2003. PRETTY GOOD PRIVACY (PGP) SELF-GENERATED CERTIFICATES ARE NOT AUTHORIZED FOR USE ON THE NIPRNET. EXCEPTIONS, SUCH AS TO SUPPORT COALITION OPERATIONS, ARE MADE ON A CASE-BY-CASE BASIS.

#### 7. PKI OPERATIONS GUIDANCE

A. USE OF DOD PKI ENCRYPTION IS AT THE DISCRETION OF THE COMMAND BUT IS STRONGLY ENCOURAGED WHEN SENDING EMAIL CONTAINING INFORMATION THAT IS SENSITIVE BUT UNCLASSIFIED (SBU), FOR OFFICIAL USE ONLY (FOUO), OR CATEGORIZED AS PRIVACY ACT INFORMATION. DOD PKI IS NOT TYPE I ENCRYPTION AND SHOULD NEVER BE USED TO PROTECT CLASSIFIED INFORMATION.

B. HARDWARE-BASED (I.E., CAC) AND SOFTWARE CONFIDENTIALITY PRIVATE KEYS ARE AUTOMATICALLY ESCROWED AT THE CERTIFICATION AUTHORITY (CA) AND CAN BE RECOVERED THROUGH THE DOD KEY RECOVERY PROCESS.

C. ACTIVITIES SHOULD INCORPORATE CERTIFICATE ISSUANCE AND REVOCATION INTO THEIR CHECK-IN/CHECK-OUT PROCEDURES. LRAS ARE RESPONSIBLE FOR SUBMITTING CERTIFICATE REVOCATION REQUESTS TO THEIR SERVICING REGISTRATION AUTHORITY (RA). USER SOFTWARE-BASED EMAIL CERTIFICATES ARE REQUIRED TO BE REVOKED UPON DEPARTURE FROM THAT ACTIVITY. IN ADDITION, USER CERTIFICATES MUST BE REVOKED IF THE PRIVATE KEYS ARE LOST OR COMPROMISED.

#### 8. ROLES AND RESPONSIBILITIES

A. SPAWAR SYSTEM CENTER (SSC) SAN DIEGO AND SSC CHARLESTON HAVE THE RESPONSIBILITY FOR IMPLEMENTING THE DOD PKI FOR NAVY OCONUS COMMANDS AND NON-NMCI NAVY CONUS COMMANDS.

B. THE PROGRAM EXECUTIVE OFFICE-INFORMATION TECHNOLOGY (PEO-IT) HAS THE RESPONSIBILITY FOR IMPLEMENTING DOD PKI FOR ALL NAVY AND MARINE CORPS CONUS COMMANDS VIA THE NMCI ROLLOUT.

C. THE NAVY RA AT DCMS WILL PROVIDE SUPPORT TO LANT, NAVEUR, AND NAVCENT ACTIVITIES UNTIL THEATER RAS ARE ESTABLISHED IN THESE AORS. PLA: DCMS WASHINGTON DC/N35/N7/. CONTACT INFO: DONPKIRA@DCMS.NAVY.MIL. 202-764-0259, DSN 764-0259.

D. PAC ACTIVITIES SHALL USE THE PACIFIC THEATER RA AT COMPACFLT. PLA: COMPACFLT PEARL HARBOR HI/N69/. CONTACT INFO: PACRA@CPF.NAVY.MIL, PACRA@CPF.NAVY.SMIL.MIL. 808-471-8755, DSN

315-471-8755.

E. ISSMS ARE RESPONSIBLE FOR ESTABLISHING AND MAINTAINING PKI FOR THEIR ACTIVITIES. ISSMS ARE RESPONSIBLE FOR ENSURING THAT AN LRA CAPABILITY IS AVAILABLE TO USERS.

F. USERS ARE RESPONSIBLE FOR SAFEGUARDING THEIR PRIVATE KEYS AND REMEMBERING THEIR ASSOCIATED PASSWORDS/PERSONAL IDENTIFICATION NUMBERS (PINS). PRIVATE KEYS AND PASSWORDS/PINS SHALL REMAIN UNDER THE POSITIVE CONTROL OF THE USER, ONCE DELIVERED. EXCEPTION: THE USER'S SOFTWARE-BASED PRIVATE DECRYPTION KEY MAY BE COPIED FOR LOCAL KEY BACKUP PURPOSES. CONTACT PEO C4I AND SPACE (PMW 161) FOR GUIDANCE AND SPECIFIC REQUIREMENTS.

9. ACTION: EVERY NAVY COMMAND AND ACTIVITY MUST ENSURE THAT THEY HAVE TAKEN ALL ACTIONS REQUIRED TO COMPLY WITH THE MILESTONES DETAILED IN PARAGRAPH 4 ABOVE. DIRECT ANY QUESTIONS REGARDING THE ACTIONS WHICH MUST BE TAKEN TO IMPLEMENT PKI AT YOUR COMMAND TO THE PEO C4I AND SPACE POC, MR. SAMIR OTHMAN AT SAMIR.OTHMAN@NAVY.MIL. TO ENABLE NAVY TO MEET THE OCTOBER 2003 MILESTONE, ALL COMMANDS SHALL HAVE INITIATED PKI COMPLIANCE ACTIONS BY THE END OF 3RD QTR FY03.

10. THE DOD PKI PMO HAS SCHEDULED THE FOURTH ANNUAL PKI USERS FORUM FOR 17 THROUGH 19 JUNE 2003 IN MYRTLE BEACH, SC. THE FORUM AGENDA, REGISTRATION INFORMATION, AND HOTEL SPECIFICS CAN BE OBTAINED AT [HTTP://WWW.IAEVENTS.COM](http://www.iaevents.com). NAVY IS SPONSORING A BREAKOUT SESSION IN CONJUNCTION WITH THIS FORUM. THE NAVY SESSION WILL RUN FROM 1015 ON THURSDAY THE 19TH (AFTER THE DON CIO SESSION SCHEDULED FOR 0830 TO 1000) THROUGH 1230 ON FRIDAY THE 20TH. A DETAILED AGENDA FOR THE NAVY SESSION IS AVAILABLE AT [HTTPS://INFOSEC.NAVY.MIL/PKI](https://infosec.navy.mil/pki). THE GOAL OF THE NAVY SESSION IS TO PROVIDE IMPLEMENTATION INFORMATION, DISCUSS ISSUES, PROVIDE POLICY DIRECTION AND INITIATE AN EFFORT TO ENSURE PK ENABLING OF NAVY APPLICATIONS. ALL NAVY COMMANDS ARE ENCOURAGED TO ATTEND THIS BREAKOUT SESSION TO BECOME FAMILIAR WITH THE NAVY'S PKI ROLLOUT PLANS AND PROCEDURES AND TO INTERACT WITH THE PRESENTERS TO ENSURE MAXIMUM INFORMATION EXCHANGE. RECOMMENDATIONS FOR NAVY SESSION AGENDA ITEMS OR ISSUES SHOULD BE ADDRESSED TO ROBERT WEILMINSTER (CNO/N61424) AT WEILMINSTER.ROBERT@HQ.NAVY.MIL.

11. SUPPORT OF THIS IMPORTANT SECURITY INITIATIVE IS APPRECIATED. PKI WILL SERVE TO ENHANCE THE FORCE PROTECTION POSTURE OF THE FLEET. WAIVERS TO THIS POLICY SHOULD BE ADDRESSED VIA THE CHAIN OF COMMAND TO OPNAV N61.

12. MINIMIZE CONSIDERED. RELEASED BY RADM T.E. ZELIBOR.

BT  
#0894  
NNNN