

PENTAGON TELECOMMUNICATIONS CENTER

 * UNCLASSIFIED *

NAVAL MESSAGE
 DEPT OF NAVY

FOR COMPLYING WITH SUBJ IMPLEMENTATION. REF B DRAFT NAVY DOD CLASS 3 PKT IMPLEMENTATION PLAN.//
 POC/SAMIR OTHMAN/CIV/COMSPAWARSYSKOM/-/TEL:(619)524-7369
 /TEL:DSN: 524-7369/EMAIL:OTHMAN@SPAWAR.NAVY.MIL//
 POC/NICK VALDEZ/CIV/COMSPAWARSYSKOM/-/TEL:(619)524-7520
 /TEL:DSN: 524-7520/EMAIL:VALDEZN@SPAWAR.NAVY.MIL//
 RMKS/1. DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI) ENABLES ENTERPRISES TO PROTECT THE SECURITY OF THEIR COMMUNICATIONS AND BUSINESS TRANSACTIONS ON THE INTERNET. IMPLEMENTATION OF DOD PKI CAPABILITY WILL FACILITATE SECURE ELECTRONIC COMMERCE AND ALLOW CONTROLLED ACCESS TO DOD INFORMATION AND RESOURCES. ALL NAVY COMMANDS ARE REQUIRED TO UTILIZE DOD PKI TO DIGITALLY SIGN DEPARTMENT EMAIL MESSAGES BY OCTOBER 2002 TO MEET THE MANDATES IN REF A. A RELIEF MEMO IS EXPECTED TO EXTEND THIS DUE DATE. THE INTENT OF THIS MESSAGE IS TO PROVIDE GUIDANCE FOR SUCCESSFUL IMPLEMENTATION OF NAVY DOD PKI. FOLLOWING PARAGRAPHS DISCUSS RESPONSIBILITIES, RECOMMENDED HARDWARE/SOFTWARE REQUIREMENTS, AND OUTLOOK CLIENT CONFIGURATION ASSOCIATED WITH NAVY DOD PKI IMPLEMENTATION.

2. SPAWAR PMW 161 RESPONSIBILITY: THE COMMON ACCESS CARD (CAC) IS THE DOD PKI HARDWARE TOKEN FOR PKI COMMUNICATIONS. AS SUCH, THIS MESSAGE DEALS WITH THE IMPLEMENTATION OF THE CAC AS THE PREFERRED DOD PKI OPTION. SPAWAR PMW 161 WILL PROVIDE MIDDLEWARE AND SMART CARD READERS TO THE FLEET CINCS, NON-NMCI OCONUS COMMANDS, AND THE AFLOAT COMMUNITY. IAW REF B, TRAINING TEAMS FROM SPAWAR PMW 161 WILL BE SENT TO OCONUS REGIONAL SITES TO PROVIDE CARD READER AND MIDDLEWARE INSTALLATION TRAINING FOR THE SYSTEM ADMINISTRATORS WHO WILL ASSIST COMMANDS WITH DOD PKI IMPLEMENTATION.

3. AFLOAT PKI UPGRADE: IN ORDER TO EXPEDITE THE AFLOAT PKI IMPLEMENTATION, IT WILL BE ACCOMPLISHED UNDER A TWO-PART PROCESS. THE FIRST PART WILL CONSIST OF A GOTS DELTA PKI MAINTENANCE RELEASE THAT WILL SUPPORT AN INTERIM SOLUTION OF EITHER SOFTWARE CERTIFICATES OR THE CAC, WITH THE CAC BEING THE OPTIMUM SOLUTION. THE SECOND PART WILL BE THE DEPLOYMENT OF THE IT-21/GOTS DELTA 4.1.1.2 UPGRADE OR COMPOSE ROLLOUT THROUGH THE REGULAR ISNS/IT-21 UPGRADE SCHEDULE WITH THE CAC BEING THE PRIMARY HARDWARE TOKEN FOR DOD PKI FUNCTIONALITY.

4. HARDWARE/SOFTWARE: THE FOLLOWING OPTIMAL COMPONENTS ARE RECOMMENDED TO SUPPORT DOD PKI AND THE CAC:

- WINDOWS NT 4.0 SP6A / WINDOWS 2000 SP2 - PROVIDED BY COMMANDS.
- ACTIVCARD GOLD 2.1 - PROVIDED BY SPAWAR PMW 161.
- INTERNET EXPLORER 5.5 SP2 - PROVIDED BY COMMANDS.
- NETSCAPE COMMUNICATOR 4.76 OR HIGHER (U.S. 128 BIT ONLY) (EXCLUDING NETSCAPE V6.X) - PROVIDED UNDER THE DISA ENTERPRISE LICENSE.
- OUTLOOK 98 OR OUTLOOK 2000 SR1 - PROVIDED BY COMMANDS.
- EXCHANGE SERVER 5.5 SP4 - PROVIDED BY COMMANDS.

PENTAGON TELECOMMUNICATIONS CENTER

 * UNCLASSIFIED *

N A V A L M E S S A G E
 D E P T O F N A V Y

-ACTIVCARD SMART CARD READERS OR CHERRY INTEGRATED SMART CARD
 KEYBOARD - PROVIDED BY SPAWAR PMW 161.

5. OUTLOOK CLIENT CONFIGURATION: THERE ARE CURRENTLY A NUMBER OF
 APPLICATIONS IN THE DOD THAT DO NOT SUPPORT S/MIME. DUE TO THIS
 NON-HOMOGENOUS S/MIME ENVIRONMENT, IT IS NECESSARY TO PROPERLY
 CONFIGURE THE OUTLOOK EMAIL CLIENT TO ENSURE DIGITALLY SIGNED EMAIL
 CAN BE READ BY NON-S/MIME APPLICATIONS. TO DIGITALLY SIGN AN EMAIL
 MESSAGE IN OUTLOOK 98 OR OUTLOOK 2000, THE FOLLOWING CONFIGURATION
 CHANGES MUST BE MADE AT THE USER WORKSTATION:

-SELECT "TOOLS" FROM THE MENU BAR.

-SELECT "OPTIONS" FROM THE PULL DOWN MENU.

-SELECT THE "SECURITY TAB" FROM THE OPTIONS SCREEN.

-ENSURE THE "ADD DIGITAL SIGNATURE TO OUTGOING MESSAGE" AND "SEND
 CLEAR TEXT SIGNED MESSAGE WHEN SENDING SIGNED MESSAGES" BOXES ARE
 CHECKED.

TO ADD THE E-MAIL SIGNING CERTIFICATE:

-CLICK ON "SETTINGS" UNDER THE "SECURE E-MAIL" SECTION.

-TYPE "DOD PKI" UNDER THE "SECURITY SETTING NAME."

-SELECT "S/MIME" FROM THE "SECURE MESSAGE FORMAT" PULL DOWN MENU.

-ENSURE THE "DEFAULT SECURITY SETTING FOR THIS SECURE MESSAGE
 FORMAT" AND THE "DEFAULT SECURITY SETTING FOR ALL SECURE MESSAGE"
 BOXES ARE CHECKED.

-CLICK THE "CHOOSE" BUTTON NEAR THE "SIGNING CERTIFICATE" SECTION.

-SELECT THE CERTIFICATE THAT HAS "DOD CLASS 3 CAC EMAIL CA" IN THE
 "ISSUED BY" FIELD; THEN CLICK "OK."

-SELECT "SHA1" FROM THE "HASH ALGORITHM" PULL DOWN MENU.

-NEXT, CLICK THE "CHOOSE" BUTTON NEAR THE "ENCRYPTION ALGORITHM"
 SECTION.

-SELECT THE CERTIFICATE THAT HAS "DOD CLASS 3 CAC EMAIL CA" IN THE
 "ISSUED BY" FIELD; THEN CLICK "OK."

-SELECT "3DES" FROM THE "ENCRYPTION ALGORITHM" PULL DOWN MENU.

THEN CLICK "OK" TO CLOSE THE "SETTINGS" SCREEN.

-CLICK ON "APPLY."

-CLICK ON "OK" TO CLOSE THE "OPTIONS" SCREEN.

OUTLOOK 98 OR OUTLOOK 2000 IS NOW PROPERLY CONFIGURED TO UTILIZE THE
 CAC AND TO DIGITALLY SIGN ALL OUTGOING EMAIL MESSAGES.

6. EXCHANGE SERVER CONFIGURATION: THERE ARE A COUPLE OF
 CONFIGURATION CHANGES THAT MUST BE PERFORMED ON THE EXCHANGE SERVER
 TO ALLOW EMAIL MESSAGES WITH DIGITAL SIGNATURES TO REACH THE
 RECIPIENT. FIRST, THE EXCHANGE SERVER MUST BE CONFIGURED TO ALLOW
 FOR "CLIENTS SUPPORT S/MIME MESSAGES." SECOND, IF THE EXCHANGE
 SERVER IS CONFIGURED TO STRIP ATTACHMENTS WITH THE EXTENSIONS P7M OR
 P7S, THEN THE EXCHANGE SERVER MUST BE CONFIGURED TO ALLOW THESE FILE
 EXTENSIONS TO PASS THROUGH.

7. ANTI-VIRUS: IF THE ANTI-VIRUS CONTENT CHECKING IS STRIPPING
 FILE EXTENSIONS ENDING IN P7M OR P7S, THEN THE ANTI-VIRUS PROGRAM

PENTAGON TELECOMMUNICATIONS CENTER

* UNCLASSIFIED *

NAVAL MESSAGE
DEPT OF NAVY

PROGRAM.

8. FOR MORE INFORMATION ABOUT DOD PKI CLICK ON THE PUBLIC KEY INFRASTRUCTURE TAB AT [HTTPS://INFOSEC.NAVY.MIL](https://infosec.navy.mil).

9. NAVY POCS FOR DOD PKI IMPLEMENTATION IS SAMIR OTHMAN, SPAWAR PMW 161-2A; EMAIL ADDRESS: OTHMAN@SPAWAR.NAVY.MIL, COMM (619) 524-7369 OR DSN 524-7369 AND NICK VALDEZ, SPAWAR PMW 161-2A3; EMAIL ADDRESS: VALDEZN@SPAWAR.NAVY.MIL, COMM (619) 524-7520 OR DSN 524-7520.

10. REQUEST WIDEST POSSIBLE DISSEMINATION OF THIS MESSAGE.// BT