

UNCLAS

PRECEDENCE TO: ROUTINE DTG: 061525Z OCT 04
PRECEDENCE CC: ROUTINE
TYPE: DMS SIGNED/ENCRYPTED
FROM PLA: DON CIO WASHINGTON DC
FROM D/N: C:US,O:U.S. Government,OU:DoD,OU:NAVY,OU:ORGANIZATIONS(uc),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:DON CIO
WASHINGTON DC(uc)
SUBJECT: DON PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION GUIDANCE
UPDATE

TEXT:

UNCLASSIFIED//

PASS TO OFFICE CODES:

FM DON CIO WASHINGTON DC

TO ASSTSECNAV FM WASHINGTON DC//00//

ASSTSECNAV IE WASHINGTON DC//00//

ASSTSECNAV MRA WASHINGTON DC//00//

ASSTSECNAV RDA WASHINGTON DC//00//

UNSECNAV WASHINGTON DC//AAUSN//

OGC WASHINGTON DC//00//

NAVY JAG WASHINGTON DC//00//

OLA WASHINGTON DC//00//

CHINFO WASHINGTON DC//00//

NAVINSGEN WASHINGTON DC//00//

NAVAUDSVC WASHINGTON DC//00//

DIRNAVCRIMINVSERV WASHINGTON DC//00//

CNO WASHINGTON DC//N6F//

CMC WASHINGTON DC//C4//

INFO DON CIO WASHINGTON DC//00//

UNCLAS

MSGID/GENADMIN/DON CIO WASHINGTON DC/-/OCT//

SUBJ/DON PUBLIC KEY INFRASTRUCTURE (PKI) IMPLEMENTATION GUIDANCE
/UPDATE//

REF/A/DOC/DOD INSTRUCTION 8520.2/01APR2004//

REF/B/MSG/DON CIO WASHINGTON DC/052157ZMAR2004//

REF/C/DOC/DOD WASHINGTON DC/24OCT2002//

REF/D/MSG/DON CIO WASHINGTON DC/031700ZNOV2003//

NARR/REF A IS DOD INSTRUCTION 8520.2 OF 1 APR 04, PUBLIC KEY
INFRASTRUCTURE (PKI) AND PUBLIC KEY ENABLING (PKE). REF B UPDATES
DON PKI MILESTONES AND RE-CONFIRMS MONTHLY COMPLIANCE REPORTING
REQUIREMENTS. REF C IS THE DOD INFORMATION ASSURANCE DIRECTIVE.
REF D ESTABLISHED PKI IMPLEMENTATION REPORTING GUIDANCE ON PROGRESS
TOWARD FULL COMPLIANCE.//

POC/LAWRENCE PEMBERTON/CDR/DON CIO/LOC:WASHINGTON DC

/EMAIL:LAWRENCE.PEMBERTON@NAVY.MIL PHONE: 703-601-0120//

POC/JAMES MAUCK/CIV/DON CIO/LOC:WASHINGTON DC

/EMAIL:JAMES.MAUCK@NAVY.MIL PHONE: 703-601-0579//

RMKS/

1. THIS MESSAGE PROVIDES AMPLIFYING IMPLEMENTATION GUIDANCE TO REF A AND RE-CONFIRMS COMPLIANCE REPORTING REQUIREMENTS OF REF B.
2. PKI PROVIDES ENHANCED IDENTITY AUTHENTICATION AND IS A FUNDAMENTAL COMPONENT OF OUR NETWORK INFORMATION ASSURANCE STRATEGY.

THE ENTIRE DEPARTMENT OF THE NAVY (DON) TEAM CONTINUES TO MAKE SIGNIFICANT STRIDES IN SECURING OUR NETWORKS AND INFORMATION SYSTEMS BY FIELDING AND IMPLEMENTING PKI.

3. 3. REF B SETS THE FOLLOWING DON PKI MILESTONES
 - A. CAC/PKI ISSUANCE
 - B. CAC READER AND MIDDLEWARE DEPLOYMENT
 - C. CLIENT SIDE AUTHENTICATION TO DOD PRIVATE WEB SERVERS
 - D. E-MAIL SIGNING AND ENCRYPTION
 - E. PK-ENABLE DOD UNCLASSIFIED NETWORKS FOR HARDWARE TOKEN CERTIFICATE BASED ACCESS CONTROL
 - F. DON INDUSTRY PARTNERS OBTAIN DOD PKI DIGITAL CERTIFICATES OR EXTERNAL CERTIFICATE AUTHORITY (ECA) PKI DIGITAL CERTIFICATES.
4. THE DEADLINE IS EXTENDED FOR IMPLEMENTATION OF REF B ACTIONS, SINCE SOME OF THE INFRASTRUCTURE COMPONENTS REQUIRED TO ACHIEVE THE PKI MILESTONES ARE NOT COMPLETE. WE MUST ALL CONTINUE TO WORK TOWARDS ACHIEVING THESE IMPORTANT MILESTONES, AS SOON AS POSSIBLE.

THE FOLLOWING ACTIONS SHALL BE TAKEN IN SUPPORT OF PKI/PKE MILESTONES:

 - A. CAC/PKI ISSUANCE: ALL DON ORGANIZATIONS SHALL CONTINUE TO ISSUE CACS WITH THREE PKI CERTIFICATES.
 - B. CAC READER AND MIDDLEWARE DEPLOYMENT: ALL DON ORGANIZATIONS SHALL CONTINUE TO INSTALL CAC READERS AND ASSOCIATED MIDDLEWARE. NMCI, CONUS NON-NMCI, BLII AND MCEN NETWORKS SHALL COMPLETE DEPLOYMENT OF CAC READERS AND MIDDLEWARE BY APR 2005. IT-21 DEPLOYMENTS SHALL CONTINUE ON THEIR CURRENT ACCELERATED SCHEDULE UNTIL COMPLETE. NOTE: DON ORGANIZATIONS SCHEDULED TO TRANSITION TO NMCI (I.E. IN ASSUMPTION OF RESPONSIBILITY (AOR) OR PRE-AOR) SHALL WAIT UNTIL NMCI CUTOVER TO DEPLOY CARD READERS AND MIDDLEWARE, PER THE NMCI DEPLOYMENT SCHEDULE.
 - C. CLIENT SIDE AUTHENTICATION TO DOD PRIVATE WEB SERVERS: ALL DON ORGANIZATIONS SHALL CONTINUE TO PK-ENABLE PRIVATE WEB SERVERS AS PLANNED. PRIVATE WEB SERVERS THAT HAVE A USER BASE WITHOUT CAC READERS AND MIDDLEWARE ARE AUTHORIZED TO MAINTAIN BOTH CAC BASED AND NON-CAC BASED METHODS OF AUTHENTICATION UNTIL USER BASE HAS MIGRATED.
 - D. E-MAIL SIGNING AND ENCRYPTION: AS CAC READERS AND MIDDLEWARE ARE DEPLOYED, DON USERS SHALL DIGITALLY SIGN E-MAIL MESSAGES REQUIRING EITHER MESSAGE INTEGRITY AND/OR NON-REPUDIATION, AND ENCRYPT MESSAGES CONTAINING SENSITIVE INFORMATION, PER REF C. E-MAIL THAT IS ROUTINE, PERSONAL OR NON-OFFICIAL IN NATURE (E.G., SAILOR MAIL) SHOULD NOT BE DIGITALLY SIGNED.
 - E. CRYPTOGRAPHIC BASED NETWORK LOGON: NMCI SHALL CONTINUE TO DEPLOY INFRASTRUCTURE COMPONENTS REQUIRED TO SUPPORT THIS CAPABILITY. ALL DON ORGANIZATIONS SHALL CONTINUE TO ENABLE ALL NON-NMCI NETWORKS FOR CRYPTOGRAPHIC BASED NETWORK LOGON AS PLANNED. WE MUST CONTINUE TO AGGRESSIVELY PURSUE THE SIGNIFICANT SECURITY ENHANCEMENTS ASSOCIATED WITH CRYPTOGRAPHIC BASED NETWORK LOGON.

- F. DON INDUSTRY PARTNERS SHALL CONTINUE TO OBTAIN EXTERNAL CERTIFICATE AUTHORITY (ECA) PKI DIGITAL CERTIFICATES.
5. THIS POLICY WILL BE UPDATED AS REQUIRED. WE WILL CONTINUE TO WORK ACROSS DOD TO REFINE FUNCTIONAL CAPABILITIES OF THE DOD PKI, DEVELOP A CAPABILITIES EVOLUTION STRATEGY, AND DEVELOP A PKI/PKE IMPLEMENTATION MILESTONE POLICY THAT IS BETTER ALIGNED WITH THE DOD PKI CAPABILITIES EVOLUTION STRATEGY. THIS UPDATE IN PKI/PKE IMPLEMENTATION MILESTONES WILL HELP TO ENSURE A REASONABLE IMPLEMENTATION, HOWEVER, WE MUST CONTINUE TO AGGRESSIVELY PURSUE CAC AND CERTIFICATE ISSUANCE, AND PK-ENABLING ACTIONS.
 6. BY 01 FEB 2005, ACTION ADDEES SHALL IDENTIFY ALL PRIVATE WEB SERVERS AND NETWORKS, UNDER THEIR COGNIZANCE WHICH HAVE NOT BEEN PK-ENABLED, AND DEVELOP A COMPREHENSIVE PK-ENABLING PLAN OF ACTION AND MILESTONE (POA&M). ACTION ADDEES SHALL DISCONTINUE USE OF PRIVATE WEB SERVERS AND NETWORKS THAT DO NOT MEET THE ABOVE REQUIREMENT, UNTIL A POA&M IS DEVELOPED. ACTION ADDEES SHALL CONTINUE TO PROVIDE DON CIO MONTHLY PKI IMPLEMENTATION STATUS REPORTS PER REFS B AND D, AND PROVIDE UPDATES TO POA&M(S) AS THEY EVALUATE THEIR RESPECTIVE PKE IMPLEMENTATION STRATEGIES AND MOVE FORWARD. WE MUST CONTINUE TO MONITOR AND TRACK DON PROGRESS IN REACHING OUR PKI IMPLEMENTATION GOALS.
 7. THE DEPARTMENT OF THE NAVY IS FIRMLY COMMITTED TO ACCOMPLISHING DOD PKI MILESTONES, AS QUICKLY AS IS REASONABLE, IN ORDER TO STRENGTHEN THE SECURITY OF OUR INFORMATION SYSTEMS BY USING PUBLIC KEY TECHNOLOGY AND REALIZE THE BENEFITS OF WEB-BASED SELF SERVICE TRANSACTIONS FOR OUR NAVY-MARINE CORPS TEAM.
 8. RELEASED BY D. M. WENNERGREN, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER./

=====

ORIGINAL TO RECIPIENTS:

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
 L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:CNO WASHINGTON DC(UC)
 [CNO WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:USMC,OU:ORGANIZATIONS,L:HQMC
 WASHINGTON DC,OU:CMC WASHINGTON DC(UC)
 [CMC WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
 L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:CHINFO WASHINGTON DC(UC)
 [CHINFO WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
 L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:OLA WASHINGTON DC(UC)
 [OLA WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
 L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:NAVINGEN WASHINGTON DC(UC)
 [NAVINGEN WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
 L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:OGC WASHINGTON DC(UC)
 [OGC WASHINGTON DC]

C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),

L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:ASSTSECNAV FM WASHINGTON DC(UC)
[ASSTSECNAV FM WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:ASSTSECNAV IE WASHINGTON DC(UC)
[ASSTSECNAV IE WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:ASSTSECNAV MRA WASHINGTON DC(UC)
[ASSTSECNAV MRA WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:ASSTSECNAV RDA WASHINGTON DC(UC)
[ASSTSECNAV RDA WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:UNSECNAV WASHINGTON DC(UC)
[UNSECNAV WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:NAVY JAG WASHINGTON DC(UC)
[NAVY JAG WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:NAVAUDSVC WASHINGTON DC(UC)
[NAVAUDSVC WASHINGTON DC]
ORIGINAL CC RECIPIENTS:
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:CNO WASHINGTON DC(UC)
[CNO WASHINGTON DC]
C:US,O:U.S. GOVERNMENT,OU:DOD,OU:NAVY,OU:ORGANIZATIONS(UC),
L:DISTRICT OF COLUMBIA,L:WASHINGTON,OU:DON CIO WASHINGTON DC(UC)
[DON CIO WASHINGTON DC]
PROFILED DISSEMINEEES:
PTC WASHINGTON DC @ CNONTS(UC) (CC)
DMSFOROCT@PTSC.PENTAGON.MIL (CC)
NAVSTAT@HQ.NAVY.MIL (CC)
NAVY-HQ-NAVSTAT@NAVY.MIL (CC)
ADPMESSAGES@HQ.NAVY.MIL (CC)
DONNA.BURCHTURNER@NAVY.MIL (CC)
FSA_MDS@NAVY.MIL (CC)
M09B172-MSG@US.MED.NAVY.MIL (CC)
MICHAEL.VANSICKEL@NAVY.MIL (CC)
MSGRCV@140.185.74.193 (CC)
N00MESSAGES@HQ.NAVY.MIL (CC)
N091MESSAGES@HQ.NAVY.MIL (CC)
N09B1BMESSAGES@HQ.NAVY.MIL (CC)
N09B20MESSAGES@HQ.NAVY.MIL (CC)
N09B3MESSAGES@HQ.NAVY.MIL (CC)
N09BCMESSAGES@HQ.NAVY.MIL (CC)
N09BFTRAFFIC@HQ.NAVY.MIL (CC)
N09GMESSAGES@HQ.NAVY.MIL (CC)
N20MESSAGES@HQ.NAVY.MIL (CC)
N22MESSAGES@HQ.NAVY.MIL (CC)
N23MESSAGES@HQ.NAVY.MIL (CC)
N2CMESSAGES@HQ.NAVY.MIL (CC)
N2MESSAGES@HQ.NAVY.MIL (CC)
N3N5NCCINFO@HQ.NAVY.MIL (CC)

N43MESSAGES@HQ.NAVY.MIL (CC)
N44MESSAGES@HQ.NAVY.MIL (CC)
N46MESSAGES@HQ.NAVY.MIL (CC)
N4MESSAGES@HQ.NAVY.MIL (CC)
N61ACTION@HQ.NAVY.MIL (CC)
N61MESSAGES@HQ.NAVY.MIL (CC)
N74ACTION@HQ.NAVY.MIL (CC)
N7INFO@HQ.NAVY.MIL (CC)
N8INFO@HQ.NAVY.MIL (CC)
NAVY-HQ-ADPMESSAGES@NAVY.MIL (CC)
NAVY-HQ-M09B172@NAVY.MIL (CC)
NAVY-HQ-N00FMESSAGES@NAVY.MIL (CC)
NAVY-HQ-N00MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N091MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09B1BMESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09B20MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09B3MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09BCMESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09BFTRAFFIC@NAVY.MIL (CC)
NAVY-HQ-N09GMESSAGES@NAVY.MIL (CC)
NAVY-HQ-N09WACTION@NAVY.MIL (CC)
NAVY-HQ-N09WINFO@NAVY.MIL (CC)
NAVY-HQ-N12MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N130MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N131MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N132MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N133MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N134MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N13MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N1MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N20MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N22MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N23MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N2CMESSAGES@NAVY.MIL (CC)
NAVY-HQ-N2MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N3N5NCCINFO@NAVY.MIL (CC)
NAVY-HQ-N43MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N44MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N46MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N4MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N61ACTION@NAVY.MIL (CC)
NAVY-HQ-N61MESSAGES@NAVY.MIL (CC)
NAVY-HQ-N74ACTION@NAVY.MIL (CC)
NAVY-HQ-N7INFO@NAVY.MIL (CC)
NAVY-HQ-N8INFO@NAVY.MIL (CC)
NAVY-HQ-OARDECMESSAGES@NAVY.MIL (CC)
NAVY-HQ-OGCMESSAGES@NAVY.MIL (CC)
NAVY-HQ-OLAMEESSAGES@NAVY.MIL (CC)
NAVY-HQ-SSMESSAGES@NAVY.MIL (CC)
OGCMESSAGES@HQ.NAVY.MIL (CC)
OLAMEESSAGES@HQ.NAVY.MIL (CC)
SSMESSAGES@HQ.NAVY.MIL (CC)
DA ID: 304645
MTSID: c=US;a=DMS;p=GOV+DMS+NIPR;l=AVTAYZ05-041006152638Z-48516
SIGNED BY: /C=US/O=U.S. Government/OU=DoD/OU=NAVY/
OU=ORGANIZATIONS(uc)/L=DISTRICT OF COLUMBIA/

L=WASHINGTON/OU=DON CIO WASHINGTON DC(uc) ***
VALIDATED ***
ENCRYPTED BY: /C=US/O=U.S. Government/OU=DoD/OU=NAVY/
OU=ORGANIZATIONS(uc)/L=DISTRICT OF COLUMBIA/
L=WASHINGTON/OU=DON CIO WASHINGTON DC(uc) ***
VALIDATED ***
MESSAGE TYPE: OTHERORG
OTHER TO RECIPIENTS:
DIRNAVCRIMINVSERV WASHINGTON DC

UNCLAS