

DON CIO Message: DTG: 122213Z MAY 08

UNCLASSIFIED//

SUBJ: PUBLIC KEY INFRASTRUCTURE SOFTWARE CERTIFICATE MINIMIZATION
EFFORT FOR DON UNCLASSIFIED ENVIRONMENTS - CORRECTED COPY

REF/A/ DOC/JTF-GNO/14DEC07//

AMP/REF A IS JOINT TASK FORCE ? GLOBAL NETWORK OPERATIONS
COMMUNICATIONS TASKING ORDER 07-015.

POCS/RICHARD ETTER/CIV/DONCIO/LOC:ARLINGTON, VA/TEL: 703-602-6882/E-
MAIL: RICHARD.ETTER@NAVY.MIL/

JAMES MAUCK/CTR/DONCIO/LOC:ARLINGTON, VA/TEL:703-601-0579/E-MAIL:
JAMES.MAUCK.CTR@NAVY.MIL/

RMKS/1. ISSUE: CRYPTOGRAPHIC AUTHENTICATION IS A PILLAR OF
DEPARTMENT OF DEFENSE (DOD) NETWORK SECURITY. PUBLIC KEY
INFRASTRUCTURE (PKI) CERTIFICATES GENERATED AND STORED ON A HARDWARE
TOKEN LIKE THE COMMON ACCESS CARD (CAC) PROVIDE HIGHER ASSURANCE LEVELS
BECAUSE THEIR PRIVATE KEYS ARE UNABLE TO BE EXTRACTED. FROM A PKI
PERSPECTIVE, PKI SOFTWARE CERTIFICATES ARE INHERENTLY NO LESS SECURE
THAN THEIR HARDWARE-BASED EQUIVALENT, WHEN USED CORRECTLY. HOWEVER,
WHEN SOFTWARE CERTIFICATES ARE IMPROPERLY STORED ON COMPUTERS,
INSTALLED, AND/OR CONFIGURED IN WEB BROWSERS, ADDITIONAL NETWORK
VULNERABILITIES MAY BE INTRODUCED.

2. TO MINIMIZE NETWORK RISK ASSOCIATED WITH IMPROPER HANDLING OF
SOFTWARE CERTIFICATES IN THE PAST, WHERE ALTERNATIVES EXIST, THE
DEPARTMENT MUST TRANSITION TO USE OF HARDWARE-BASED PKI. THE
DEPARTMENT OF NAVY (DON) CHIEF INFORMATION OFFICER (CIO) IS CONDUCTING
A DATA CALL AND IMPACT ASSESSMENT TO UNDERSTAND WHERE SOFTWARE
CERTIFICATES ARE CURRENTLY USED IN OUR UNCLASSIFIED ENVIRONMENTS AND
IDENTIFY POTENTIAL ALTERNATIVE PKI APPROACHES. ONCE THIS ASSESSMENT IS
COMPLETE, A DON WORKGROUP WILL BE CONVENED IN LATE MAY 2008 TO DEVELOP
A PLAN OF ACTION & MILESTONES (POA&M) AND THE ASSOCIATED POLICIES
REQUIRED FOR MINIMIZATION OF SOFTWARE CERTIFICATE USE AND TRANSITION TO
HARDWARE-BASED PKI CERTIFICATES WHERE PRACTICAL, WITH A GOAL OF
ACHIEVING TRANSITION BY 31 DECEMBER 09. THE DON WORKGROUP WILL ALSO
WORK WITHIN THE DOD PKI COMMUNITY ON ANY COMMUNITY-WIDE ISSUES
IDENTIFIED.

3. DON COMMANDS AND PERSONNEL THAT RELY ON SOFTWARE CERTIFICATES ARE
ENCOURAGED TO IMMEDIATELY BEGIN PREPARING FOR TRANSITION TO HARWARE
BASED PKI CERTIFICATE USE. THIS INCLUDES ENSURING INDIVIDUALS HAVE THE
APPROPRIATE HARDWARE (CAC READER) AND SOFTWARE (ACTIVE CLIENT
MIDDLEWARE) FOR USE WHERE REQUIRED. INDIVIDUALS REQUIRING MIDDLEWARE
SHOULD CONTACT THEIR COMMAND INFORMATION ASSURANCE MANAGER (IAM) FOR
FURTHER DIRECTION.

4. THE JOINT TASK FORCE: GLOBAL NETWORK OPERATIONS (JTF-GNO), IN REF
A, HAS PROVIDED SPECIFIC GUIDANCE FOR PROPER HANDLING, INSTALLATION,
AND MAINTENANCE OF PKI SOFTWARE CERTIFICATES. REF A IS AVAILABLE AT
[HTTPS:\(SLASH\)WWW.JTFGNO.MIL](https://(SLASH)WWW.JTFGNO.MIL).

5. CURRENTLY UNAFFECTED SOFTWARE CERTIFICATE USES: THIS MESSAGE IS NOT INTENDED TO CHANGE HOW THE DEPARTMENT CONDUCTS BUSINESS AND OPERATIONS FOR THE FOLLOWING:

A. EXTERNAL CERTIFICATION AUTHORITY (ECA) CERTIFICATES: THE DON CIO FULLY SUPPORTS THE DOD ECA PROGRAM AND ENCOURAGES THE USE OF ECA CERTIFICATES FOR DON INDUSTRY PARTNERS AND OTHER INDIVIDUALS WHO DO NOT REQUIRE A CAC FOR NETWORK LOGON ACCESS AND/OR PHYSICAL ACCESS.

B. NAVY AND MARINE CORPS ISSUED ALTERNATE TOKENS: CERTIFICATES ISSUED ON NAVY AND MARINE CORPS SMART CARD BASED ALTERNATE TOKENS CONTAIN INTERNAL IDENTIFIERS THAT INDICATE THEY ARE SOFTWARE CERTIFICATES. THIS EFFORT IS FOCUSED ON CERTIFICATES NOT GENERATED OR STORED ON A SMART CARD, AND THEREFORE DOES NOT APPLY TO CERTIFICATES CONTAINED ON THE ALTERNATE TOKEN.

C. COALITION PARTNERS: DON CIO RECOGNIZES THAT MANY OF DOD'S COALITION PARTNERS ARE DEVELOPING AND IMPLEMENTING THEIR OWN PKIS USING SOFTWARE CERTIFICATES. THESE CERTIFICATES MUST CONTINUE TO BE SUPPORTED.

D. REGISTRATION AUTHORITY/LOCAL REGISTRATION AUTHORITY CERTIFICATES: THESE CERTIFICATES, ALTHOUGH INTERNALLY IDENTIFIED AS SOFTWARE CERTIFICATES, DO NOT PRESENT THE SAME VULNERABILITIES AS A SOFTWARE CERTIFICATE WHICH IS ISSUED IN SOFTWARE AND INSTALLED BY A USER INTO THEIR BROWSER.

E. SERVER/WEB SERVER/DEVICE CERTIFICATES: DON CIO RECOGNIZES THAT MANY SERVER AND DEVICE CERTIFICATES ARE IMPLEMENTED USING SOFTWARE CERTIFICATES. THIS CATEGORY OF CERTIFICATES MAY BE FOCUSED ON IN FUTURE POLICY UPDATES.

F. GROUP/ROLE/WATCHSTANDER EMAIL CERTIFICATES: SOFTWARE CERTIFICATES USED FOR DIGITAL SIGNATURE AND ENCRYPTION OF EMAIL SENT FROM ACCOUNTS THAT ARE NOT ASSOCIATED WITH A SPECIFIC INDIVIDUAL WILL BE FOCUSED ON IN FUTURE POLICY UPDATES.

G. AFLOAT CONTINGENCY PLAN: AFLOAT USERS ON SHIPS THAT DO NOT HAVE THE ABILITY TO ISSUE OR MAINTAIN THE CAC MAY CONTINUE TO USE SOFTWARE CERTIFICATES AS A CONTINGENCY SHOULD A USER'S CAC BECOME LOST, STOLEN, LOCKED, DAMAGED OR OTHERWISE INOPERABLE. SOFTWARE CERTIFICATE INSTALLATION .P12 AND .PFX FILES MUST BE REMOVED FROM WORKSTATIONS IMMEDIATELY AFTER INSTALLATION IN WEB BROWSERS.

6. FUTURE POLICY AND GUIDANCE UPDATES RELATED TO SOFTWARE CERTIFICATES WILL BE RELEASED AS THE DON WORKGROUP MAKES PROGRESS AND SOFTWARE CERTIFICATE ALTERNATIVES ARE IDENTIFIED.

7. REQUEST WIDEST DISSEMINATION OF THIS MESSAGE.

8. RELEASED BY ROBERT J. CAREY, DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER.