

FROM: DAMFITAYZ022(N)  
SENT: FRIDAY, MAY 03, 2002 3:25 PM  
TO: OCARAGENCYMAIL; OASA(FMC)STAFFACTIONOFCR;  
OFCOFCHIEFOFCHAPLAINSCHIEFOFCHAP; OCE; OCEEXECUTIVEDIR;  
ODISC4STRATEGICANDADVCOMPUTINGCE; odisc4disc4;  
OSAILEASINSTALLATIONSANDENVIRON; OACSIMOFCASSTCHIEFOFSTAFFINSTALM;  
OFCDIROFMGMTDIROFMGMT; ODCSINTDCSINT;  
ODISC4STRATEGICANDADVCOMPUTINGCE;  
ODISC4STRATEGICANDADVCOMPUTINGCE  
Cc: odisc4disc4; ODISC4CIOINTEGRATION; ODISC4ELECTRONICCOMMERCE;  
ODUSA(IA)REGINTEGRATIONANDASSESS; ODCSOPSWARPLANS;  
ODUSA(IA)SAPOLICYANDRESOURCES; IMCENCUSTOMERSUPPORT;  
OSAILEASINSTALLATIONSANDENVIRON; ODCSINTCIHUMINTSECURITY;  
ODCSINTINTELLIGENCEINFORMATIONMA  
SUBJECT: UNCLAS ALARACT 0048/2002, ARMY PUBLIC KEY INFRASTRUCTURE (PKI)  
IMPORTANCE: LOW

RAAUZYUW RUEOMFB6620 1231845-UUUU--RJAIPOL RJAENZC RJAIMCS RJASAIL  
RJASACW RJAISZA RJADAIM RJAMICH RJAMIIM RJASACC RJASIMC RJADACS  
RJASSWA RJASIAE RJAIEUR RJASAIS RJADAZC RJAINSE RJASAFM RJAOCAR  
RJAMIZA.

ZNR UUUUU

R 031922Z MAY 02

FM PTC EMAIL SYSTEM WASH DC

TO RJAOCAR/DA EMAIL CUSTOMER//OCAR/SAFM/DACH/DAEN-ZC-TEST/DAEN-ZC/  
SAIS-IM-SACC/SAIS/SAILE/SACW/DAIM/DACS-DMZ/DAMI-ZA/SAIS-IM-SACC/ SAIS-IM-  
SACC// INFO RJAOCAR/DA EMAIL CUSTOMER//SAIS-ZA/SAIS-IMC/SAIS-IAE/IA-IPR-  
EUR/DAMO-SSW/IA-DSA-EXPORT-POL/JDIM-CS/OSAILE/DAMI-CH/  
DAMI-IM//

**R 031830Z MAY 02**

FM DA WASHINGTON DC//SAIS-ZA//

TO ALARACT

RUEADWD/DA WASHINGTON DC

ZEN/OU=ARMY/OU=ORGANIZATIONS/OU=MAIL LISTS/CN=ML ALARACT(N)

BT

UNCLAS ALARACT 0048/2002 SECTION 1 OF 3

SUBJ: UNCLAS ALARACT 0048/2002, ARMY PUBLIC KEY INFRASTRUCTURE (PKI)  
USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES  
THE CHIEF INFORMATION OFFICER/G-6 RELEASES THE FOLLOWING MESSAGE  
EFFECTIVE IMMEDIATELY:

SUBJECT: UNCLAS ALARACT 0048/2002, ARMY PUBLIC KEY INFRASTRUCTURE  
(PKI) USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES  
REFERENCES

- A. ASD (C3I) MEMORANDUM, 12 AUGUST 2000, SUBJECT: DEPARTMENT OF DEFENSE (DOD) PKI.
- B. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA), SUBJECT: "RECORDS MANAGEMENT GUIDANCE FOR AGENCIES IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES," OCTOBER 18, 2000.
- C. DOD, SUBJECT: "X.509 CERTIFICATE POLICY" VERSION 5.2.2, 01 MARCH 2002.
- D. THE PRIVACY ACT, 5 USC 552.
- E. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, "STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION" [45 CFR PARTS 160 AND 164], FEDERAL REGISTER, VOL. 65, NO. 250, 28 DEC 2000.
- F. USD (P&R) MEMORANDUM, 22 OCTOBER 2001, SUBJECT: DOD TELEWORK POLICY AND GUIDE.

1. PURPOSE AND SCOPE. THIS MESSAGE PROVIDES ARMY GUIDANCE FOR THE USE OF BOTH HARDWARE BASED (COMMON ACCESS CARD (CAC)) AND SOFTWARE BASED DOD PUBLIC KEY CERTIFICATES TO DIGITALLY SIGN AND/OR ENCRYPT E-MAIL MESSAGES. THE GUIDANCE IS EFFECTIVE IMMEDIATELY AND APPLIES TO THE ACTIVE ARMY, THE ARMY NATIONAL GUARD, THE UNITED STATES ARMY RESERVE, ARMY CIVIL SERVICE EMPLOYEES, AND ELIGIBLE ARMY CONTRACTORS WHO ACCESS ARMY E-MAIL SYSTEMS. THIS GUIDANCE DOES NOT APPLY TO GENERAL OFFICERS (GO) OR SENIOR EXECUTIVE SERVICE (SES) EMPLOYEES. SPECIFIC GUIDANCE ON THE USE OF PKI CERTIFICATES BY GOS AND SESS HAS BEEN ISSUED BY THE CHIEF OF STAFF OF THE ARMY UNDER SEPARATE COVER. THE PKI USAGE GUIDANCE HEREIN SHOULD BE FOLLOWED UNLESS THE LOCAL COMMANDER DIRECTS STRICTER USAGE GUIDANCE.

2. BACKGROUND. ON 12 AUGUST 2000, THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (ASD (C3I)) ISSUED A MEMORANDUM (REFERENCE A) TO UPDATE DOD POLICIES RELATED TO DEVELOPING AND IMPLEMENTING PKI. THE MEMORANDUM STATES IN PART THAT PKI CERTIFICATES MUST BE ISSUED TO ALL ACTIVE-DUTY MILITARY PERSONNEL, MEMBERS OF THE SELECTED RESERVE, DOD CIVILIAN EMPLOYEES, AND ELIGIBLE CONTRACTOR PERSONNEL. FURTHER, THE MEMO STATES THAT ALL DOD USERS ARE TO BE ISSUED CACS WITH PKI CLASS 3 CERTIFICATES BY OCTOBER 2002.

3. USING DIGITAL SIGNATURES.

A. SENDING DIGITALLY SIGNED E-MAILS. UNTIL DOD PKI POLICY OFFICIALLY MANDATES THE USE OF PKI DIGITAL SIGNATURES, NON GO/SES ARMY E-MAIL USERS MAY ELECT TO USE DOD PKI CERTIFICATES TO DIGITALLY SIGN E-MAIL MESSAGES AT THEIR DISCRETION. EVERY TIME AN E-MAIL IS DIGITALLY SIGNED USING PKI, AN ATTACHMENT IS CREATED AND ADDED TO THE E-MAIL. THOSE ATTACHMENTS QUICKLY ADD UP AND CAUSE AN ADDITIONAL BURDEN ON ARMY BANDWIDTH USE. ACCORDINGLY, TO PRECLUDE UNNECESSARY USE OF ARMY BANDWIDTH AS WELL AS DIGITAL SIGNATURES, E-MAIL USERS SHOULD DIGITALLY SIGN THEIR E-MAIL MESSAGES ONLY WHEN NON-REPUDIATION SERVICES ARE REQUIRED. E-MAIL NON-REPUDIATION IS AN INHERENT SAFEGUARD AFFORDED BY THE USE OF PKI DIGITAL SIGNATURE CERTIFICATES. NON-REPUDIATION PROVIDES ASSURANCE TO THE RECIPIENT THAT THE SENDER CANNOT LATER DENY HAVING ORIGINATED THE EMAIL. AS A GENERAL RULE IN THE ARMY, UNLESS E-MAIL NON-REPUDIATION IS REQUIRED, A PKI DIGITAL SIGNATURE SHOULD NOT BE USED.

B. RECEIVING DIGITALLY SIGNED E-MAILS. PRIOR TO OPENING AN INCOMING PKI DIGITALLY SIGNED E-MAIL, ARMY E-MAIL USERS SHOULD ASSESS THE ATTACHED DIGITAL SIGNATURE'S LEVEL OF ASSURANCE. E-MAILS SIGNED USING REVOKED CERTIFICATES SHOULD BE TREATED AS NOT HAVING ORIGINATED FROM THE INDICATED SENDER. VALID PKI DIGITAL SIGNATURES ORIGINATING OUTSIDE DOD DOMAINS MUST BE GENERATED BY AN APPROVED DOD PKI CERTIFICATE SOURCE (E.G., INTERIM EXTERNAL CERTIFICATE AUTHORITY). E-MAILS DIGITALLY SIGNED BY UNAPPROVED SOURCES SHOULD ONLY BE OPENED, READ, AND ACTED UPON WITH CAUTION. FOR COMPLETE INFORMATION ON HOW TO CHECK THE VALIDITY OF E-MAIL CERTIFICATES, SEE FREQUENTLY ASKED QUESTIONS AT

<https://setdweb.belvoir.army.mil/INDEX3.HTML>

C. RETAINING DIGITALLY SIGNED E-MAIL. IN ACCORDANCE WITH REFERENCE B, IF A DIGITALLY SIGNED RECORD REQUIRES TEMPORARY OR PERMANENT PRESERVATION, AGENCIES MUST ACCOMMODATE THE PRESERVATION NEEDS. THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) REQUIRES THAT AN AGENCY CHOOSE AN APPROACH THAT IS PRACTICAL AND FITS BUSINESS NEEDS AND RISK ASSESSMENT. AS THE FUNCTIONAL PROPONENT FOR RECORDS MANAGEMENT, THE OFFICE OF THE DEPUTY CHIEF OF STAFF/G-1 (ODCS/G-1) WILL DETERMINE THE MINIMUM STANDARDS FOR PRESERVATION OF DIGITALLY SIGNED E-MAIL.

ADDITIONAL INFORMATION REGARDING MINIMUM REQUIREMENTS MAY BE FOUND IN REFERENCE C.

#### 4. ENCRYPTION OF E-MAILS.

A. SENDING ENCRYPTED E-MAILS. DATA IS ENCRYPTED TO ENSURE CONFIDENTIALITY. HOWEVER, DATA CONFIDENTIALITY RESULTS WHEN ONLY THE INTENDED RECIPIENT CAN DECRYPT ENCRYPTED INFORMATION. SENDING ENCRYPTED E-MAIL SHOULD BE THE EXCEPTION NOT THE RULE. IN ACCORDANCE WITH REFERENCE A, ALL DOD E-MAIL THAT REQUIRES ENCRYPTION MUST USE DOD CLASS 3 ENCRYPTION CERTIFICATES. GENERALLY, ENCRYPTED E-MAILS SHOULD BE USED TO SEND: (1) INFORMATION PROTECTED BY THE PRIVACY ACT (REFERENCE D); (2) INFORMATION CLASSIFIED AS "FOR OFFICIAL USE ONLY" (FOUO); AND (3) SENSITIVE BUT UNCLASSIFIED DATA OR INFORMATION PROTECTED UNDER REFERENCE E, THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA).

B. RECEIVING ENCRYPTED E-MAILS. WHEN AN ENCRYPTED E-MAIL IS RECEIVED WITHIN A DOD DOMAIN, RECIPIENTS MUST TAKE APPROPRIATE MEASURES TO PROTECT THE ENCRYPTED INFORMATION. IF A MESSAGE HAS BEEN ENCRYPTED, THE IMPLICATION IS THAT IT CONTAINS SENSITIVE BUT UNCLASSIFIED INFORMATION THAT NEEDED TO BE PROTECTED DURING TRANSMISSION. ONCE IT HAS BEEN RECEIVED, THE NEED TO PROTECT THE INFORMATION REMAINS. ACCORDINGLY, AS A GENERAL RULE, E-MAIL THAT IS RECEIVED ENCRYPTED SHOULD BE MAINTAINED IN ENCRYPTED FORM. AS A PRACTICAL MATTER, HOWEVER, E-MAIL RECIPIENTS SHOULD BE AWARE THAT A SENDER MAY HAVE UNINTENTIONALLY ENCRYPTED A MESSAGE THAT DOES NOT CONTAIN SENSITIVE BUT UNCLASSIFIED INFORMATION. THEREFORE, RECIPIENTS OF ENCRYPTED E-MAIL MESSAGES SHOULD TREAT THOSE E-MAILS AS IF THEY DO CONTAIN SENSITIVE BUT UNCLASSIFIED INFORMATION UNTIL IT CAN BE POSITIVELY DETERMINED THAT THE INFORMATION IS NOT SENSITIVE.

C. RETAINING ENCRYPTED E-MAIL. E-MAILS THAT ARE RECEIVED IN ENCRYPTED FORM AND CONTAIN SENSITIVE BUT UNCLASSIFIED INFORMATION NEED TO BE STORED IN AN ENCRYPTED FORM TO ENSURE APPROPRIATE PROTECTION OF THE INFORMATION. IT SHOULD BE NOTED THAT STORAGE (AND SUBSEQUENT RETRIEVAL) OF ENCRYPTED E-MAIL TAKES ADDITIONAL TIME AND SPACE AND MAY REQUIRE IMPROVED STORAGE DEVICES. USERS SHOULD BE AWARE THAT IF THE RECIPIENT'S CAC OR SOFTWARE BASED PKI TOKEN IS LOST, OPENING ENCRYPTED E-MAIL WILL NOT BE POSSIBLE WITHOUT RECOVERY OF THE PRIVATE KEY. AT THIS TIME, THE DOD IS WORKING TOWARD FINALIZING A KEY RECOVERY POLICY. WHEN THE POLICY IS FINAL, ARMY WILL IMPLEMENT A KEY RECOVERY PROCESS FOR E-MAIL USERS. UNTIL A STANDARD KEY RECOVERY PROCESS IS IMPLEMENTED, THE PROCESS OF RECOVERING LOST OR COMPROMISED KEYS WILL BE SLOW. ENCRYPTED E-MAIL SHOULD BE RETAINED IN ENCRYPTED FORM OR IF POSSIBLE, STORED UNENCRYPTED IF THE INFORMATION IS NOT SENSITIVE, FOUO, OR PROTECTED BY THE PRIVACY ACT OR THE HIPAA PRIVACY RULE. FOR INFORMATION ON HOW TO UNENCRYPT AN E-MAIL MESSAGE, CALL THE ARMY SET-D HELP DESK AT (866) SET-DCAC (738-3222). IN ACCORDANCE WITH REFERENCE B, AGENCIES SHOULD DEVELOP RECORDS, SCHEDULES, AND PROPOSED RETENTION PERIODS FOR NEW RECORDS FOR NARA TO REVIEW. THE ODGS/G-1 WILL DETERMINE APPROPRIATE RECORDS RETENTION ACTIONS REGARDING ENCRYPTED E-MAILS.

#### 5. OTHER PKI USAGE ISSUES.

A. USING PKI CERTIFICATES WHEN TELEWORKING. TELEWORK REFERS TO ANY ARRANGEMENT IN WHICH AN EMPLOYEE PERFORMS OFFICIALLY ASSIGNED DUTIES AT AN ALTERNATIVE WORK SITE ON EITHER A REGULAR AND RECURRING OR AD HOC BASIS (NOT INCLUDING WHILE ON OFFICIAL TRAVEL). IN ACCORDANCE WITH REFERENCE F, GOVERNMENT-FURNISHED COMPUTER EQUIPMENT, SOFTWARE, AND COMMUNICATIONS, WITH APPROPRIATE SECURITY MEASURES, ARE REQUIRED FOR ANY REGULAR AND RECURRING TELEWORK ARRANGEMENT THAT INVOLVES SENSITIVE BUT UNCLASSIFIED DATA, INCLUDING PRIVACY ACT, HIPAA, OR FOUO DATA. WITH THE EXCEPTION OF STORING ENCRYPTED DATA, THE GUIDANCE IN PARAGRAPHS 1 THROUGH 3 ABOVE PERTAINS TO USING PKI CERTIFICATES WHEN

TELEWORKING. WHEN GOVERNMENT EMPLOYEES TELEWORK ON AN AD HOC BASIS, PERSONAL COMPUTERS THAT HAVE BEEN APPROVED BY THE DESIGNATED ACCREDITING AUTHORITY (DAA) CAN BE USED TO WORK ON LIMITED AMOUNTS OF SENSITIVE BUT UNCLASSIFIED MATERIAL. THIS ARRANGEMENT, HOWEVER, IS CONTINGENT ON THE TELEWORKER TRANSFERRING SUCH MATERIAL TO THEIR DOD DOMAIN COMPUTERS AND THEN DELETING SUCH FILES FROM THEIR PERSONAL COMPUTERS AS SOON AS THEY ARE NO LONGER REQUIRED, AND VERIFYING IN WRITING, THAT HE OR SHE HAS DELETED ALL FILES CONTAINING DEPARTMENT INFORMATION FROM PERSONALLY OWNED COMPUTER HARD DRIVES. OTHER PKI CERTIFICATE GUIDANCE INCLUDES:

(1) IF A USER HAS A FORMAL TELEWORK ARRANGEMENT WITH THE ARMY UTILIZING GOVERNMENT-FURNISHED COMPUTER EQUIPMENT, FOUO, SENSITIVE BUT UNCLASSIFIED, AND PRIVACY ACT OR HIPAA-RELATED MATERIALS SHOULD BE STORED IN THEIR ENCRYPTED FORM.

(2) IN ACCORDANCE WITH REFERENCE F, WHEN EMPLOYEES TELEWORK ON AN AD HOC BASIS (USING PERSONAL EQUIPMENT), IT IS RECOMMENDED THAT FOUO, SENSITIVE BUT UNCLASSIFIED, AND PRIVACY ACT OR HIPAA-RELATED MATERIALS BE STORED IN THEIR ENCRYPTED FORM IF IT IS ABSOLUTELY NECESSARY TO RETAIN THEM. THESE FILES MUST BE DELETED FROM THEIR PERSONAL COMPUTER HARD DRIVES ONCE NO LONGER IN USE AND WRITTEN VERIFICATION THAT THEY HAVE BEEN DELETED MUST BE PROVIDED IAW REF F.

(3) IF A USER HAS NO FORMAL TELEWORK ARRANGEMENT, FOUO, SENSITIVE BUT UNCLASSIFIED, AND PRIVACY ACT OR HIPAA-RELATED E-MAIL RECEIVED SHOULD NOT BE STORED ON PERSONAL EQUIPMENT.

B. PKI USAGE WITH WIRELESS E-MAIL DEVICES. WIRELESS DEVICES ARE NOT YET COMPATIBLE WITH THE DOD PKI AND THEREFORE CANNOT BE USED TO SEND OR RECEIVE DIGITALLY SIGNED OR ENCRYPTED E-MAIL USING DOD PKI CERTIFICATES. THEREFORE, USERS OF WIRELESS DEVICES CANNOT ENCRYPT, DECRYPT, DIGITALLY SIGN, OR VALIDATE DIGITALLY SIGNED E-MAIL USING WIRELESS DEVICES.

C. PKI USAGE WITH WEBMAIL. CURRENTLY, WEBMAIL PRODUCTS, INCLUDING ARMY KNOWLEDGE ONLINE (AKO) WEBMAIL, ARE NOT DOD PKI COMPATIBLE. WHILE ARMY KNOWLEDGE MANAGEMENT POLICY MANDATES THAT E-MAIL USERS' PKI CERTIFICATES BE BOUND TO THEIR AKO E-MAIL ADDRESSES, IT IS IMPORTANT TO NOTE THAT AT THIS TIME THE WEB-BASED E-MAIL ACCESSED THROUGH AKO CANNOT DIGITALLY SIGN OR ENCRYPT E-MAILS. USERS CAN STILL DIGITALLY SIGN OR ENCRYPT EMAILS USING THE AKO EMAIL SYSTEM AS LONG AS THEY SETUP AND CONFIGURE AN EMAIL CLIENT SUCH AS MICROSOFT OUTLOOK OR NETSCAPE MESSENGER. ADDITIONAL GUIDANCE WILL BE PROVIDED TO USERS ONCE AKO WEBMAIL IS PUBLIC KEY ENABLED TO OPERATE WITH THE DOD PKI.

D. LEGAL ISSUES ASSOCIATED WITH PKI. WHILE DIGITAL SIGNATURES ARE CONSIDERED LEGALLY BINDING, THE LEVEL OF ASSURANCE REQUIRED FOR DIGITALLY SIGNED E-MAILS MUST BE BASED ON THE REQUIREMENTS OF THE BUSINESS PROCESSES. FOR EXAMPLE, IN ACQUISITION AND CONTRACTING PROCESSES, THE PKI CERTIFICATE USED TO DIGITALLY SIGN AN E-MAIL MUST BE A HARDWARE-BASED (I.E. CAC) PKI CERTIFICATE. HOWEVER, CLASS 3 SOFTWARE-BASED CERTIFICATES MAY BE SUITABLE FOR OTHER BUSINESS PROCESSES. THE LEGAL PURPOSES OF DIGITAL SIGNATURE INCLUDE:

(1) SIGNER AUTHENTICATION. IF A PUBLIC AND PRIVATE KEY PAIR IS ASSOCIATED WITH AN IDENTIFIED SIGNER, THE DIGITAL SIGNATURE ATTRIBUTES THE MESSAGE TO THE SIGNER. THE DIGITAL SIGNATURE CANNOT BE FORGED, UNLESS THE SIGNER LOSES CONTROL OF THE PRIVATE KEY (A "COMPROMISE" OF THE PRIVATE KEY), SUCH AS BY DIVULGING IT OR LOSING THE MEDIA OR DEVICE IN WHICH IT IS CONTAINED.

(2) MESSAGE AUTHENTICATION/INTEGRITY. THE DIGITAL SIGNATURE ALSO IDENTIFIES THE SIGNED MESSAGE, TYPICALLY WITH FAR GREATER CERTAINTY AND PRECISION THAN PAPER SIGNATURES. VERIFICATION REVEALS ANY TAMPERING,

SINCE THE COMPARISON OF THE HASH RESULTS (ONE MADE AT SIGNING AND THE OTHER MADE AT VERIFYING) SHOWS WHETHER THE MESSAGE IS THE SAME AS WHEN SIGNED.

(3) NON-REPUDIATION. CREATING A DIGITAL SIGNATURE REQUIRES THE SIGNER TO USE THE SIGNER'S PRIVATE KEY. THIS ACT CAN PERFORM THE "CEREMONIAL" FUNCTION OF ALERTING THE SIGNER TO THE FACT THAT THE SIGNER IS CONSUMMATING A TRANSACTION WITH LEGAL CONSEQUENCES (I.E., THE ORIGINATOR CANNOT DENY SIGNING THE FILE). THE PROCESSES OF CREATING AND VERIFYING A DIGITAL SIGNATURE PROVIDE A HIGH LEVEL OF ASSURANCE THAT THE DIGITAL SIGNATURE IS GENUINELY THE SIGNER'S.

E. EQUIPMENT NEEDED TO USE THE DOD PKI. TO USE THE DOD PKI, E-MAIL USERS ARE REQUIRED TO HAVE TWO ESSENTIAL COMPONENTS. THE FIRST COMPONENT IS THE CAC, WHICH SERVES AS THE USER'S PKI TOKEN (I.E., THE CAC'S INTEGRATED CIRCUIT CHIP STORES THE USER'S PRIVATE KEY IDENTITY TOGETHER WITH THE ELECTRONIC MAIL, IDENTITY AND ENCRYPTION CERTIFICATES). THE SECOND COMPONENT IS A CAC READER AND ASSOCIATED "MIDDLEWARE" SOFTWARE ON THE USER WORKSTATION. THE ARMY'S PRODUCT MANAGER FOR SECURE ELECTRONIC DEVICES (PM SET-D) WEB SITE, LOCATED AT [HTTPS://SETDWEB.BELVOIR.ARMY.MIL/](https://setdweb.belvoir.army.mil/), LISTS THE SUPPORTED SMART CARD READERS AND ASSOCIATED MIDDLEWARE, AND PROVIDES INFORMATION ON HOW THE READERS WILL BE FIELDDED AND INSTALLED AND HOW E-MAIL APPLICATIONS MUST BE CONFIGURED TO OPERATE WITH THE DOD PKI. WHEN USERS OBTAIN THESE PRIMARY COMPONENTS, THEY WILL BE ABLE TO USE PKI TO DIGITALLY SIGN AND/OR ENCRYPT E-MAIL MESSAGES.

6. POINTS OF CONTACT. THE CIO/G-6 POINTS OF CONTACT FOR THIS ACTION ARE MS. WENDY SEFERT, PHONE: 703-902-4149, E-MAIL: WENDY.SEFERT@US.ARMY.MIL OR MR. KEMP PRUGH, PHONE: 703-558-7861, E-MAIL: E.PRUGH@US.ARMY.MIL. ADDITIONAL INFORMATION ON THE USE OF PKI AND THE CAC CAN BE FOUND ON THE ARMY C4 ET WEB SITE AT [HTTPS://SECUREWEB.HQDA.PENTAGON.MIL/ARMYC4ETECH](https://secureweb.hqda.pentagon.mil/armyc4etech).

7. EXPIRATION DATE IS 02 MAY 2005.