

AAUZELX RUEADWD6617 2452030-UUUU--RUEACOE.

ZNR UUUUU

P 031859Z SEP 03

FM PTC EMAIL SYSTEM WASH DC

INFO RUEACOE/DA EMAIL CUSTOMER//CEHECIM/COE//

P 022019Z SEP 03 ZEL

FM DA WASHINGTON DC//DCIO/G6//

TO ALARACT

BT

UNCLAS ALARACT 114/2003 SECTION 1 OF 2

SUBJECT: UNCLAS ALARACT 114/2003 ARMY PUBLIC KEY INFRASTRUCTURE
(PKI) USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL
SIGNING OF E-MAIL MESSAGES

OTHERORG

UNCLASSIFIED//

ALARACT 114/2003

THE CHIEF INFORMATION OFFICER/G-6 RELEASES THE FOLLOWING MESSAGE
EFFECTIVE IMMEDIATELY:

SUBJECT: ARMY PUBLIC KEY INFRASTRUCTURE (PKI) USAGE GUIDANCE FOR
ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES

REFERENCES

- A. MESSAGE, HQDA, SAIS-ZA, 031830Z MAY 02, SUBJECT: UNCLAS ALARACT 0048/2002, ARMY PUBLIC KEY INFRASTRUCTURE (PKI) USAGE GUIDANCE FOR ENCRYPTION AND DIGITAL SIGNING OF E-MAIL MESSAGES.
- B. AR 25-1, ARMY INFORMATION MANAGEMENT, 31 MAY 02.

PAGE 02 RUEADWD6617 UNCLAS

- C. MEMORANDUM, ASD(C3I), SUBJECT: DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI), 12 AUG 00.
- D. MEMORANDUM, ASD(C3I), SUBJECT: PUBLIC KEY INFRASTRUCTURE (PKI) POLICY UPDATE, 21 MAY 02.
- E. UNITED STATES CODE, TITLE 5, PART I, CHAPTER 5, SUBCHAPTER II, SUB SECTION 552A, THE PRIVACY ACT OF 1974, 27 SEP 75.
- F. 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 00.
- G. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA), SUBJECT: RECORDS MANAGEMENT GUIDANCE FOR AGENCIES IMPLEMENTING ELECTRONIC SIGNATURE TECHNOLOGIES, 18 OCT 00.
- H. NARA BULLETIN 2003-04, AVAILABILITY OF ELECTRONIC RECORDS MANAGEMENT GUIDANCE FOR PUBLIC KEY INFRASTRUCTURE (PKI)-RELATED ADMINISTRATIVE RECORDS, 27 MAR 03.
1. PURPOSE AND SCOPE. THIS MESSAGE SUPERCEDES REFERENCE A AND PROVIDES UPDATED ARMY GUIDANCE FOR THE USE OF BOTH HARDWARE BASED AND SOFTWARE BASED DOD PUBLIC KEY CERTIFICATES TO DIGITALLY SIGN AND/OR ENCRYPT E-MAIL MESSAGES IN ACCORDANCE

PAGE 03 RUEADWD6617 UNCLAS

- WITH (IAW) REFERENCES B, C, AND D.
2. USING DIGITAL SIGNATURES.

- A. SENDING DIGITALLY SIGNED E-MAILS. AS A GENERAL RULE IN THE ARMY, A PKI DIGITAL SIGNATURE SHOULD BE USED WHENEVER E-MAIL IS CONSIDERED OFFICIAL BUSINESS AND/OR CONTAINS SENSITIVE INFORMATION IAW REFERENCES E OR F. THE DIGITAL SIGNATURE PROVIDES ASSURANCES THAT THE INTEGRITY OF THE MESSAGE HAS REMAINED INTACT IN TRANSIT, AND PROVIDES FOR THE NON-REPUDIATION OF THE MESSAGE THAT THE SENDER CANNOT LATER DENY HAVING ORIGINATED THE E-MAIL.
- 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., EXTERNAL CERTIFICATE AUTHORITY). E-MAILS THAT ARE DIGITALLY SIGNED BY UNAPPROVED SOURCES SHOULD ONLY BE OPENED, READ, AND ACTED UPON WITH CAUTION.

PAGE 04 RUEADWD6617 UNCLAS

- C. RETAINING DIGITALLY SIGNED E-MAIL. AGENCIES MUST ACCOMMODATE THE PRESERVATION NEEDS IF A DIGITALLY SIGNED RECORD REQUIRES TEMPORARY OR PERMANENT PRESERVATION IAW REFERENCE G. 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) ARMY RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY HAS DETERMINED THE MINIMUM STANDARDS FOR PRESERVATION OF DIGITALLY SIGNED E-MAIL. ADDITIONAL INFORMATION REGARDING MINIMUM REQUIREMENTS MAY BE FOUND IN REFERENCES G AND H, AND AT THE US ARMY RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WEBSITE: [HTTPS://WWW.ARIMS.ARMY.MIL](https://www.arims.army.mil).
- 3. 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. IAW REFERENCE C, ALL DOD E-MAIL THAT REQUIRES ENCRYPTION MUST USE, AT A MINIMUM, DOD CLASS 3 ENCRYPTION CERTIFICATES. ENCRYPTION USES A GREATER AMOUNT OF BANDWIDTH THAN DIGITAL

PAGE 05 RUEADWD6617 UNCLAS

- SIGNATURE. THEREFORE, ENCRYPTED E-MAILS SHOULD BE THE EXCEPTION, NOT THE RULE AND SHOULD ONLY BE USED TO SEND (1) SENSITIVE INFORMATION; (2) INFORMATION PROTECTED BY THE PRIVACY ACT OF 1974 (REFERENCE E); (3) INFORMATION PROTECTED UNDER REFERENCE F, 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 INFORMATION THAT NEEDED TO BE PROTECTED DURING TRANSMISSION. ONCE IT HAS BEEN RECEIVED, THE NEED TO PROTECT THE INFORMATION REMAINS.

- C. RETAINING ENCRYPTED E-MAIL. E-MAILS THAT ARE RECEIVED IN ENCRYPTED FORM AND CONTAIN SENSITIVE INFORMATION NEED TO BE STORED IN 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. ENCRYPTED E-MAIL RECEIVED THAT DOES NOT CONTAIN SENSITIVE INFORMATION, OR

PAGE 06 RUEADWD6617 UNCLAS

INFORMATION PROTECTED BY REFERENCES E AND F, (THE PRIVACY ACT OR THE HIPAA PRIVACY RULE) SHOULD BE STORED UNENCRYPTED. INFORMATION ON DECRYPTING AND STORING UNENCRYPTED E-MAIL CAN BE FOUND AT

[HTTPS://SETDWEB.SETD.ARMY.MIL/SUPPORT/ADDLRESOURCES.HTM](https://setdweb.setd.army.mil/support/addlresources.htm).

FURTHER ASSISTANCE CAN OBTAINED BY CALLING THE ARMY SET-D HELP DESK AT (866) SET-DCAC (738-3222). IN ACCORDANCE WITH REFERENCE G, AGENCIES SHOULD DEVELOP RECORDS SCHEDULES AND PROPOSED RETENTION PERIODS FOR NEW RECORDS FOR NARA TO REVIEW; HOWEVER, IF THE RECORDS ARE ALREADY SCHEDULED, THEY WOULD NOT NEED TO BE RESCHEDULED BECAUSE THEY WERE ENCRYPTED THE SAME RETENTION WOULD APPLY IN BOTH CASES. THE ODCS/G-1, RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WILL DETERMINE APPROPRIATE RECORDS RETENTION ACTIONS REGARDING ENCRYPTED E-MAILS. USERS SHOULD BE AWARE THAT IF THEIR CAC OR SOFTWARE-BASED PKI TOKEN WERE LOST, OPENING STORED/SAVED-ENCRYPTED E-MAIL WOULD NOT BE POSSIBLE WITHOUT RECOVERY OF THEIR PRIVATE KEY.

UNCLAS ALARACT 114/2003 FINAL SECTION OF 2

SUBJECT: ARMY PUBLIC KEY INFRASTRUCTURE

DESK AT (866) SET-DCAC (738-3222). IN ACCORDANCE WITH REFERENCE G, AGENCIES SHOULD DEVELOP RECORDS SCHEDULES AND PROPOSED RETENTION PERIODS FOR NEW RECORDS FOR NARA TO REVIEW; HOWEVER, IF THE RECORDS ARE ALREADY SCHEDULED, THEY WOULD NOT NEED TO BE RESCHEDULED BECAUSE THEY WERE ENCRYPTED THE SAME RETENTION WOULD APPLY IN BOTH CASES. THE ODCS/G-1, RECORDS MANAGEMENT AND DECLASSIFICATION AGENCY WILL DETERMINE APPROPRIATE RECORDS RETENTION ACTIONS REGARDING ENCRYPTED E-MAILS. USERS SHOULD BE AWARE THAT IF THEIR CAC OR SOFTWARE-BASED PKI TOKEN WERE LOST, OPENING STORED/SAVED-ENCRYPTED E-MAIL WOULD NOT BE POSSIBLE WITHOUT RECOVERY OF THEIR PRIVATE KEY.

----- PROCESSED BY DECISION AGENT -----
DA MESSAGE ID: 304123

NNNN