

PAAUZYUW RUEOMFC2686 3492152-UUUU--RJASAPA READACS REASAIS.

ZNR UUUUU

P 142159Z DEC 00

FM PTC EMAIL SYSTEM WASH DC

TO RJASAMR/DA EMAIL
CUSTOMER//SAMR/SAPA/DAJA/DAMH/DASG/SAAG/

SAIS-SMTP/SAAA/SAGC/DACS-1-SMTP/SAIS-SMTP/SAIS-SMTP//

INFO RJASAMR/DA EMAIL CUSTOMER//8THARMYLNO-SMTP//

P 141430Z DEC 00

FM DA WASHINGTON DC//SAIS-ZA//

TO ALARACT

BT

UNCLAS ALARACT 0109/2000 SECTION 1 OF 3

SUBJECT: UNCLAS ALARACT 0109/2000, INTERIM POLICY AND
PROCEDURES FOR PUBLIC KEY INFRASTRUCTURE (PKI)
IMPLEMENTATION IN THE DEPARTMENT OF THE ARMY

THE DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL,
COMMUNICATIONS, AND COMPUTERS (DISC4) RELEASES THE FOLLOWING
POLICY EFFECTIVE 06 DECEMBER 2000.

REFERENCES:

A. MEMORANDUM, DOD ASD (C3I/CIO), DTD 12 AUGUST 2000, SUBJ:
DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI)

B. PUBLIC KEY INFRASTRUCTURE ROADMAP FOR THE DEPARTMENT OF
DEFENSE, VERSION, 3.0, DTD 29 OCTOBER 1999

C. U.S. DEPARTMENT OF DEFENSE X.509 CERTIFICATE POLICY,
VERSION 5.0, DTD 13 DECEMBER 1999.

D. PUBLIC KEY INFRASTRUCTURE IMPLEMENTATION PLAN FOR THE
DEPARTMENT OF DEFENSE, VERSION 3.0, DTD 13 NOVEMBER 2000.

E. DCID 6/3, DTD 05 JUNE 1999, PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS.

F. MEMORANDUM, DEPSECDEF, DTD 10 NOVEMBER 1999, SUBJ: SMART CARD ADOPTION AND IMPLEMENTATION.

G. MESSAGE, HQDA SAIS-ZA, DTG 101256MAY00, SUBJ: PUBLIC KEY ENABLING OF PRIVATE WEB SERVERS - S: 30 JUNE 2000.

H. HQDA LETTER 25-99-1, DTD 15 OCTOBER 1999, SUBJ: U.S. ARMY ELECTRONIC COMMERCE POLICY.

1. PURPOSE AND SCOPE

A. THIS MESSAGE ESTABLISHES POLICY AND PROCEDURES FOR THE IMPLEMENTATION OF PUBLIC KEY INFRASTRUCTURE (PKI) IN THE DEPARTMENT OF THE ARMY AND ASSIGNS ASSOCIATED ROLES AND RESPONSIBILITIES TO HQDA PROPONENTS, MAJOR ARMY COMMANDS (MACOMS), ARMY FUNCTIONAL PROPONENTS, ARMY MATERIEL DEVELOPERS, AND OPERATIONS AND MAINTENANCE {O&M} COMMANDS.

B. FOR THE PURPOSES OF THIS MESSAGE, PKI INCLUDES THE INTEGRATED DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM (DEERS) AND THE REAL TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM (RAPIDS) WORKSTATIONS; DOD CERTIFICATE AUTHORITY (CA) AND ROOT AUTHORITY; ARMY REGISTRATION AUTHORITY FOR INDIVIDUALS (RAI); ARMY REGISTRATION AUTHORITY FOR EQUIPMENT (RAE); AND THE VERIFICATION OFFICIALS (VO) / LOCAL REGISTRATION AUTHORITIES (LRA) PERSONNEL THAT STAFF THE DEERS/RAPIDS WORKSTATIONS.

C. PKI IS BEING IMPLEMENTED AS PART OF THE DEFENSE IN DEPTH STRATEGY TO ACHIEVE INFORMATION SUPERIORITY BY PROTECTING INFORMATION VITAL TO WARFIGHTING AND BUSINESS OPERATIONS. IN ADDITION, PKI IS AN ELECTRONIC BUSINESS/ELECTRONIC COMMERCE ENABLER THAT PROVIDES THE NECESSARY AUTHENTICATION, CONFIDENTIALITY, INTEGRITY, AND NON-REPUDIATION NEEDED TO MIGRATE BUSINESS OPERATIONS TO A PAPERLESS ENVIRONMENT.

D. THIS MESSAGE IS EFFECTIVE IMMEDIATELY AND APPLIES TO THE ACTIVE DUTY ARMY, THE ARMY NATIONAL GUARD, THE U.S. ARMY RESERVE, CIVIL SERVICE EMPLOYEES, AND ELIGIBLE CONTRACTORS WHO HAVE ACCESS TO A DOD AUTOMATED INFORMATION SYSTEM (AIS). THIS MESSAGE DOES NOT APPLY TO THE INTELLIGENCE

COMMUNITY (IC) SENSITIVE COMPARTMENTED INFORMATION (SCI) AND INFORMATION SYSTEMS OPERATED WITHIN THE DOD IC THAT FALL UNDER THE AUTHORITY OF THE DIRECTOR OF CENTRAL INTELLIGENCE IAW REFERENCE (REF) E ABOVE.

E. THIS MESSAGE DOES NOT APPLY TO USERS OR APPLICATIONS ON ENCRYPTED NETWORKS OR IN THE TACTICAL ENVIRONMENT. UNTIL DOD POLICY IS PUBLISHED FOR PKI ON ENCRYPTED NETWORKS AND IN THE TACTICAL ENVIRONMENT, ARMY USER AND APPLICATION REQUIREMENTS FOR PKI ON ENCRYPTED NETWORKS AND IN THE TACTICAL ENVIRONMENT WILL BE HANDLED ON A CASE BY CASE BASIS. WRITTEN REQUESTS WILL BE SUBMITTED (IAW THE FORMAT CONTAINED IN PARAGRAPHS FIVE(5)A THROUGH FIVE(5)G BELOW) THROUGH COMMAND CHANNELS TO THE OFFICE OF THE DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (ODISC4), ATTN: SAIS-IAS.

F. THIS POLICY DOES NOT ASSIGN ROLES AND RESPONSIBILITIES FOR THE FOLLOWING COMMON ACCESS CARD (CAC)/PKI FUNCTIONS AS THEY PERTAIN TO VO/LRA PERSONNEL (1) RECEIVING AND PROCESSING CERTIFICATE REVOCATIONS AND SUSPENSION REQUESTS; AND (2) RECEIVING AND PROCESSING CERTIFICATE RE-KEY REQUESTS. THE ROLES AND RESPONSIBILITIES RELATED TO THOSE FUNCTIONS WILL BE ADDRESSED AS A PART OF THE ARMY'S CAC BUSINESS PROCESS REENGINEERING (BPR)/ FUNCTIONAL ECONOMIC ANALYSIS (FEA) STUDY. UPON COMPLETION OF THE CAC BPR/FEA STUDY, A FUNCTIONAL PROPONENT WILL BE IDENTIFIED TO TAKE ON THESE ADDITIONAL ROLES AND RESPONSIBILITIES. IN THE EVENT THE BPR/FEA DECISION REQUIRES OTHER CHANGES IN ROLES AND RESPONSIBILITIES ASSIGNED HEREIN, AN AMENDMENT TO THIS POLICY WILL BE PUBLISHED.

2. IAW REFERENCES A-H ABOVE, IT IS ARMY POLICY THAT:

A. ALL IMPLEMENTATIONS OF PKI WITHIN THE DEPARTMENT OF THE ARMY SHALL USE THE STANDARD DOD PKI CLASS 3 INFRASTRUCTURE (ROOT AUTHORITIES, CERTIFICATE AUTHORITIES, REGISTRATION AUTHORITIES, AND VERIFYING OFFICIALS AND LOCAL REGISTRATION AUTHORITIES). FURTHER, IAW WITH REF F, THE EXISTING AND PLANNED INFRASTRUCTURE PROVIDED BY THE DEERS/RAPIDS WILL BECOME THE DOD PKI CLASS 3 INFRASTRUCTURE COMPONENT FOR ISSUING PKI CERTIFICATES. THE PROJECTED DATE FOR INITIAL OPERATIONAL CAPABILITY OF THE DEERS/RAPIDS INFRASTRUCTURE TO ISSUE PKI CERTIFICATES IS DECEMBER 2000; SUBSEQUENT FULL OPERATIONAL CAPABILITY IS PROJECTED FOR DECEMBER 2001.

B. ALL NEW PROCUREMENT ACTIONS THAT REQUIRE PUBLIC KEY CRYPTOGRAPHY WILL INCLUDE IN THE SOLICITATION PROCESS THE REQUIREMENT TO USE THE PKI CERTIFICATES AND KEYS ISSUED BY THE DOD PKI CLASS 3 INFRASTRUCTURE NLT OCTOBER 2002.

C. ARMY PILOT PROGRAMS, INITIATIVES, AND SYSTEMS THAT CURRENTLY USE PUBLIC KEY CRYPTOGRAPHY MUST MIGRATE TO USE THE PKI CERTIFICATES ISSUED BY THE DOD PKI CLASS 3 INFRASTRUCTURE BY OCTOBER 2002.

D. LEGACY SYSTEMS THAT CURRENTLY USE NON DOD STANDARD IMPLEMENTATIONS OF PKI AND ARE TARGETED FOR REPLACEMENT WITHIN THE NEXT 5 YEARS WILL NOT MIGRATE TO THE DOD PKI CLASS 3 INFRASTRUCTURE UNLESS THE MIGRATION TO THE DOD STANDARD PKI IS REQUIRED TO MAINTAIN CURRENT SYSTEM INTERFACES. IF NO CHANGES ARE REQUIRED, THEN THESE SYSTEMS WILL CONTINUE TO USE THEIR CURRENT PKI IMPLEMENTATION UNTIL UNCLAS ALARACT 0109/2000 SECTION 2 OF 3 THE SYSTEMS ARE RETIRED. IN ALL CASES, TARGETED REPLACEMENT SYSTEMS WILL BE REQUIRED TO USE THE PKI CERTIFICATES ISSUED BY THE DOD PKI CLASS 3 INFRASTRUCTURE.

E. THE STANDARD DOD PKI CLASS 3 CERTIFICATES WILL BE CONTAINED IN THE INTEGRATED CIRCUIT CHIP (ICC) ON THE DOD CAC. A SINGLE SET OF CLASS 3 PKI CERTIFICATES WILL BE USED FOR IDENTIFICATION, DIGITAL SIGNATURE, AND ENCRYPTION CAPABILITY ON UNCLASSIFIED NETWORKS WITHIN THE ARMY. ALL ARMY USERS SHALL BE ISSUED CLASS 3 CERTIFICATES BY OCTOBER 2002.

F. IAW REF F, THE DOD PKI IDENTITY CERTIFICATES CONTAINED ON THE CAC WILL BE USED TO ACCESS ALL ARMY UNCLASSIFIED NETWORKS. ALL ARMY UNCLASSIFIED NETWORKS WILL BE CAPABLE OF VERIFYING A USER'S ACCESS THROUGH USE OF THE DOD PKI CLASS 3 IDENTITY CERTIFICATES CONTAINED ON THE DOD CAC NLT OCTOBER 2002.

G. BY OCTOBER 2002, THE STANDARD DOD PKI CLASS 3 SIGNING CERTIFICATES WILL BE USED TO DIGITALLY SIGN MESSAGES THAT ARE CREATED AND SENT FROM ANY DEPARTMENT OF THE ARMY ELECTRONIC MAIL (EMAIL) SYSTEM OTHER THAN THE DEFENSE MESSAGE SYSTEM (DMS).

H. BY OCTOBER 2002, ALL EMAIL MESSAGES CREATED AND SENT FROM ANY DEPARTMENT OF THE ARMY EMAIL SYSTEM OTHER THAN THE DMS THAT REQUIRE ENCRYPTION BASED ON A BUSINESS ANALYSIS OR SENSITIVITY LEVEL OF THE INFORMATION SHALL BE ENCRYPTED

USING THE DOD PKI CLASS 3 ENCRYPTION CERTIFICATES CONTAINED ON THE CAC.

I. REF G PROVIDES THE POLICY AND PROCEDURES FOR PKI ENABLING ALL ARMY PRIVATE WEB SERVERS ON THE MILITARY DOMAIN (.MIL) DOMAIN TO BECOME SECURE SOCKET LAYER (SSL) ENABLED VIA THE DOD CLASS 3 PKI, EXCEPT THAT THE SUSPENSE DATE FOR THESE SERVERS WILL BE IAW REF A, 31 DECEMBER 2000. ALL OTHER ARMY PRIVATE WEB SERVERS LOCATED ON A DOMAIN OTHER THAN .MIL MUST MIGRATE TO THE .MIL DOMAIN WITHIN 120 DAYS OF THE DATE OF THIS MESSAGE AND BECOME SSL ENABLED IAW THE GUIDELINES PROVIDED IN REF G.

3. TO ENSURE A SMOOTH IMPLEMENTATION OF THE PKI POLICIES WITHIN THE DEPARTMENT OF THE ARMY, EFFECTIVE IMMEDIATELY THE FOLLOWING ROLES AND RESPONSIBILITIES ARE ASSIGNED:

A. THE OFFICE OF THE DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (ODISC4) SHALL:

(1) SERVE AS THE ARMY'S SINGLE FOCAL POINT FOR ALL PKI ISSUES

(2) PRODUCE ARMY PKI PLANNING GUIDANCE FOR INCLUSION WITHIN THE ARMY'S PLANNING, PROGRAMMING, BUDGETING, AND EXECUTION SYSTEM; THE ARMY MODERNIZATION PLAN; THE REQUIREMENTS DETERMINATION PROCESS; THE ARMY PLAN; AND, THE ARMY PROGRAM GUIDANCE MEMORANDUM

(3) DEVELOP AND/OR OVERSEE THE DEVELOPMENT OF AN ARMY-WIDE MASTER SCHEDULE OF EVENTS THAT, AT A MINIMUM, INCLUDES THE MILESTONES FOR THE RESEARCH, DEVELOPMENT, TESTING, EVALUATION AND ACQUISITION ACTIVITIES OF PKI, AND THE DEVELOPMENT OF OTHER ARMY DOCUMENTS, SUCH AS IMPLEMENTATION PLANS, CONFIGURATION MANAGEMENT PLANS, KEY RECOVERY POLICIES, CERTIFICATE PRACTICE STATEMENTS, PUBLIC KEY ENABLING POLICY, PKI ROADMAP, AND UPDATED PKI AND CAC POLICIES - TO INCLUDE ARMY REGULATION (AR) 25-1 AND DEPARTMENT OF THE ARMY PAMPHLET (DA PAM) 25-1-1

(4) REPRESENT THE ARMY AT DOD PKI WORKING GROUPS

(5) PROVIDE GUIDANCE TO THE ARMY FUNCTIONAL COMMUNITIES ON IMPLEMENTATION AND INTEGRATION OF PKI DURING BPR

(6) SERVE AS THE ARMY FUNCTIONAL PROPONENT FOR PKI AND THE RELATED PKI REQUIREMENTS, INCLUDING INITIATING BUSINESS PROCESS CHANGES NEEDED TO ACCOMMODATE THE IMPLEMENTATION OF PKI

(7) INITIATE ANALOGOUS WORKING GROUPS TO THE DOD PKI RELATED WORKING GROUPS AND COMMITTEES TO ADDRESS TECHNICAL AND BUSINESS-RELATED ISSUES

(8) IAW REF H, ENSURE THAT ALL PKI SOLUTIONS BE DESIGNED, DEVELOPED, IMPLEMENTED, AND MANAGED CONSISTENT WITH THE GENERAL RESPONSIBILITIES, SPECIFIC RESPONSIBILITIES, AND MANAGEMENT OVERSIGHT OF THE ARMY ELECTRONIC COMMERCE POLICY.

(9) ENSURE THAT THE PRODUCT MANAGER SECURE ELECTRONIC TRANSACTIONS-DEVICES (PM SET-D) ADDRESSES TOTAL PACKAGE FIELDING REQUIREMENTS, TO INCLUDE TRAINING, IMPLEMENTATION, AND SUSTAINMENT COSTS FOR INSTALLATIONS.

B. THE PM SET-D, UNDER DIRECT REPORTING CHANNELS TO THE PROGRAM EXECUTIVE OFFICE STANDARD ARMY MANAGEMENT INFORMATION SYSTEMS (PEO STAMIS), SHALL (1) COORDINATE WITH OTHER DEFENSE AND ARMY PROGRAM MANAGERS TO SUPPORT THE SYNCHRONIZED PLANNING, PROGRAMMING, DEVELOPMENT, PROCUREMENT, INTEGRATED LOGISTICS SUPPORT, TESTING, AND FIELDING OF TECHNOLOGY AND PRODUCTS REQUIRED TO SUPPORT PKI ON THE CAC AS DIRECTED BY THE DISC4; AND (2) MANAGE THE DAY-TO-DAY TASKS INVOLVED IN INSTALLATION, INTEGRATION, INTEGRATED LOGISTICS SUPPORT, TRAINING, AND ACCEPTANCE TESTING OF THE REQUIRED SMART CARD READER INFRASTRUCTURE NECESSARY TO SUPPORT THE IMPLEMENTATION OF NETWORK ACCESS VIA THE PKI ON THE CAC.

C. THE ODISC4 COMMUNICATIONS ELECTRONIC SERVICES OFFICE (CESO) SHALL

(1) SERVE AS THE ARMY'S RAI;

(2) REGISTER LRAS TO ISSUE PKI CERTIFICATES TO INDIVIDUALS;

(3) DEVELOP THE ARMY'S CERTIFICATE PRACTICE STATEMENTS (CPS) NECESSARY TO STANDARDIZE THE IMPLEMENTATION OF PKI WITHIN THE ARMY;

(4) EXECUTE REVOCATION REQUESTS RECEIVED FROM LRAS OR OTHER AUTHORIZED SOURCES; AND

(5) IAW REF B, MAINTAIN APPROPRIATE RECORDS TO SUPPORT ARCHIVAL AND AUDIT REQUIREMENTS.

D. THE ARMY NETWORK OPERATIONS CENTER (ANSOC), ARMY SIGNAL COMMAND, SHALL

(1) SERVE AS THE ARMY'S RAE;

(2) ISSUE CERTIFICATES TO DEVICES;

(3) REVOKE DEVICE CERTIFICATES AS REQUIRED; AND

(4) IAW REF B, MAINTAIN APPROPRIATE RECORDS TO SUPPORT ARCHIVAL AND AUDIT REQUIREMENTS.

E. THE OFFICE OF THE DEPUTY CHIEF OF STAFF FOR PERSONNEL (ODCSPER), AS THE ARMY'S FUNCTIONAL PROPONENT FOR DEERS/RAPIDS SHALL

(1) PROVIDE THE REQUIRED OPERATIONAL SUPPORT TO THE CAC/PKI INTEGRATED WORKSTATIONS; AND

(2) SUPPORT THE INITIAL ISSUANCE AND RENEWAL OF THE CAC, TO INCLUDE THE APPLICATION OF DOD CLASS 3 PKI CERTIFICATES TO THE CARDS AS PART OF THE ISSUANCE PROCESS.

F. THE ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY) SHALL INITIATE THE NECESSARY ACTION TO ENSURE THAT ARMY ACQUISITION AND LIFE CYCLE MANAGEMENT POLICIES ARE UPDATED TO REFLECT THE PKI POLICY CONTAINED IN THIS MESSAGE.

G. FUNCTIONAL PROPONENTS AND MAJOR ARMY COMMANDS SHALL

(1) PLAN, PROGRAM, AND BUDGET TO PUBLIC KEY ENABLE (PKE) THEIR APPLICATIONS AND NETWORKS IAW THIS POLICY;

(2) REENGINEER THEIR BUSINESS PROCESSES, IF APPLICABLE, TO ACCOMMODATE THE ARMY-WIDE IMPLEMENTATION OF PKI.

(NOTE: PENDING THE ESTABLISHMENT OF DOD PKE POLICY, SUBSEQUENT ARMY GUIDANCE AND POLICY ON PKE WILL FOLLOW IN A SEPARATE MESSAGE).

H. ARMY MATERIEL DEVELOPERS AND O&M COMMANDS SHALL IMPLEMENT PKI TECHNOLOGIES THAT COMPLY WITH THE POLICY MANDATES CONTAINED WITHIN THIS MESSAGE.

I. ARMY FUNCTIONAL PROPONENTS MAY USE THEIR DISCRETIONARY AUTHORITY AND RESOURCES TO FIELD OSD DIRECTED FUNCTIONAL SPECIFIC IMPLEMENTATIONS OF PKI TO ARMY INSTALLATIONS PRIOR TO THE MIGRATION TO THE STANDARD DOD CLASS 3 PKI CONTAINED ON THE CAC.

4. EFFECTIVE IMMEDIATELY, ALL ARMY ELEMENTS THAT HAVE IMPLEMENTED OR ARE PLANNING TO IMPLEMENT ANY PKI-RELATED TECHNOLOGY FOR DIGITAL SIGNATURE OR ENCRYPTION SERVICES WILL COMPLY WITH THE DOD GUIDANCE REFERENCED ABOVE AND ALL ADDITIONAL REQUIREMENTS ESTABLISHED IN PARAGRAPH FIVE (5) BELOW.

5. PRIOR TO IMPLEMENTATION OF PKI ON THE CAC, ARMY ACTIVITIES THAT INTEND TO USE THEIR DISCRETIONARY AUTHORITY AND RESOURCES TO IMPLEMENT A PKI SOLUTION THAT DOES NOT COMPLY WITH THE ARMY'S STANDARD PKI SOLUTION (PARAGRAPH 2A ABOVE) MUST SUBMIT A WRITTEN WAIVER REQUEST, THROUGH COMMAND CHANNELS, FOR APPROVAL TO THIS HEADQUARTERS (ODISC4, ATTN: SAIS-IAE) 120 DAYS PRIOR TO THEIR PLANNED NON-STANDARD PKI IMPLEMENTATION. SAIS-IAE WILL COORDINATE THE REQUESTS WITH ALL APPROPRIATE HQDA STAFF OFFICES AND WILL DEVELOP A RECOMMENDED COURSE OF ACTION FOR DISC4 APPROVAL. ALL WAIVER REQUESTS SUBMITTED TO SAIS-IAE WILL CONTAIN THE FOLLOWING INFORMATION:

A. THE NAME OF THE PROGRAM/PROJECT;

B. THE NAME AND FULL CONTACT INFORMATION OF KNOWLEDGEABLE PERSON (TELEPHONE, FAX, MESSAGE, E-MAIL, AND MAILING ADDRESS);

C. A DESCRIPTION OF THE PROGRAM/PROJECT - TO INCLUDE:

(1) REQUIRED NUMBER OF LRA WORKSTATIONS NEEDING TO BE IMPLEMENTED

(2) REQUIRED NUMBER OF CERTIFIED LRAS (PERSONNEL) NEEDED

(3) REQUIRED NUMBER OF TRUSTED AGENTS (IF ANY)

(4) REQUIRED TYPE OF PKI TOKENS PLANNING TO BE ISSUED DURING THE IMPLEMENTATION (SMART CARD OR FLOPPY DISK)

(5) REQUIRED NUMBER OF INDIVIDUAL CERTIFICATES TO BE ISSUED (I.E., NUMBER OF SUBSCRIBERS)

(6) REQUIRED TYPE OF PKI CERTIFICATE TO BE ISSUED (I.E., DIGITAL SIGNATURE, ENCRYPTION, AND IDENTIFICATION)

D. THE RATIONALE FOR NON-STANDARD IMPLEMENTATION OF PKI AND THE EXPECTED BENEFITS AND OUTCOMES TO BE ACHIEVED;

E. AN IMPACT STATEMENT ADDRESSING THE ADVERSE EFFECTS THAT WILL OCCUR TO THE PROGRAM IF EARLY IMPLEMENTATION OF PKI IS NOT ACHIEVED;

F. THE FUNDING AUTHORIZATION (FISCAL YEAR AND APPROPRIATION) FOR EARLY IMPLEMENTATION OF PKI (MANAGEMENT DECISION PACKAGE (MDEP) AND PROGRAM ELEMENT (PE));

G. A LIST OF THE EXTERNAL AGENCIES OR ACTIVITIES INVOLVED, INCLUDING FOREIGN PARTICIPATION.

6. THE CESO WILL NOT PROVIDE RAI SUPPORT TO ARMY NON-STANDARD PKI IMPLEMENTATIONS THAT HAVE NOT SUBMITTED WAIVERS AND RECEIVED DISC4 APPROVAL.

7. ARMY PKI PILOT PROGRAMS INITIATED PRIOR TO IMPLEMENTATION OF THE ARMY-SANCTIONED PKI ON THE CAC PLATFORM WILL NOT BE MAINTAINED BY THE PM SET-D.

8. UNLESS SUPERSEDED, POLICIES CONTAINED IN THIS MESSAGE WILL EXPIRE THREE YEARS FROM THE DATE OF THIS MESSAGE. ODISC4 POCs FOR THIS ACTION ARE MS. BARBARA.KNIEFF, DSN 227-4674, COMMERCIAL (703) 697-4674, EMAIL BARBARA.KNIEFF@HQDA.ARMY.MIL, AND MS. DEBORAH POFF, DSN 227-6158, COMMERCIAL (703) 697-6158, FAX (703)-697-4235, EMAIL DEBORAH.POFF@HQDA.ARMY.MIL

9. EXPIRATION DATE IS 13 DEC 2003.

BT

#2686

NNNN