



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G 6

16 MAR 2004

NETC-EST-A

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Common Access Card (CAC) and Public Key Enabling (PKE) Mandates

1. References:

a. Memorandum, USD (Personnel & Readiness), 25 Sep 03, subject: Common Access Card Issuance Mandate. AKO Document ID Number: 567449

b. Message, CIO/G-6, 02 Sep 03, subject: ALARACT 114/2003: Army Public Key Infrastructure (PKI) Usage Guidance for Encryption and Digital Signing of E-mail Messages. AKO Document ID Number: 532226

c. Message, CIO/G-6, 29 Jul 02, subject: ALARACT 0077/2002: Update for Implementation of Public Key Infrastructure and Common Access Card and the Public Key Enabling of Applications, Web Servers, and Networks in the Department of the Army. AKO Document ID Number: 272498

d. Memorandum, DoD CIO, 07 Oct 03, subject: Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Update. AKO Document ID Number: 592956

e. Memorandum, CIO/G-6, 10 Sep 03, subject: Update to Common Access Card/ Public Key Infrastructure Mandate. AKO Document ID Number: 542701

2. This memorandum provides Army guidance to implement CAC/PKE in a realistic, achievable manner. The Army CIO/G-6 office has engaged OSD to reassess program direction and planning to ensure PKI is implemented in a reliable, achievable fashion.

3. PKI is a fundamental component in reaching the Army's Net Centric Enterprise Service (NCES) technical objectives, and is essential in providing enhanced security, information assurance, and identity authentication. The DoD-wide program has encountered several challenges. Contributing to the challenges are the sheer size of the infrastructure and the OPTEMPO of the DoD overall. Additional policy and guidance will be forthcoming as collaboration continues with OSD. During this effort, the following actions must be taken in support of PKI milestones:

a. CAC/PKI Issuance – Army organizations will continue to issue CACs with PKI certificates by Apr 04, consistent with reference 1a.

NETC-EST-A

SUBJECT: Common Access Card (CAC) and Public Key Enabling (PKE) Mandates

b. Digitally Signing and Encrypting of Emails

(1) All Army organizations will continue installation of CAC readers and associated middleware. All PKI points-of-contact (POCs) will report CAC reader installation progress weekly via the following website: <https://setdweb.setd.army.mil>. The Army mandate for completion and reporting by units not deployed are as follows:

(a) 50% completion by Jun 04

(b) 75% completion by Aug 04

(c) 100% completion by Oct 04

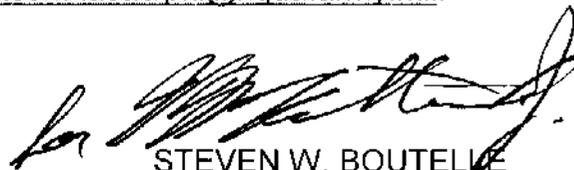
(d) Deployed units have six months from date of return to complete reader and middleware installations.

(2) As they are provided this capability, IAW reference 1b, Army users will digitally sign official email, which requires non-repudiation and data integrity, and will encrypt emails containing Sensitive information, i.e. information that is FOUO or protected by The Privacy Act of 1974.

c. PK-enabled Applications – Current efforts to PK-enable applications and networks shall continue as planned.

4. This policy will be updated as required. Until updated policy is issued, with the exception of those listed above, the implementation mandates published in reference 1c, as modified IAW references 1d and 1e, will be held in abeyance. I am committed to our development of an implementable program plan for PKI. While OCIO/G-6 continues to work with OSD to establish this plan, I request your continued command involvement in ensuring the building blocks of this program, defined in this memo, are put in place pending final delivery of a robust, reliable PKI.

5. The POC for this announcement is Jim Lynch, Army CAC/PKI, DSN: 329-1942, Comm: 703-601-1942, Email: netcom-iacac/pki@hqda.army.mil.



STEVEN W. BOUTELLE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY
(CONT)

NETC-EST-A

SUBJECT: Common Access Card (CAC) and Public Key Enabling (PKE) Mandates

DISTRIBUTION: (CONT)

COMMANDER

- U.S. ARMY EUROPE AND SEVENTH ARMY
- EIGHTH U.S. ARMY
- U.S. ARMY FORCES COMMAND
- U.S. ARMY TRAINING AND DOCTRINE COMMAND
- U.S. ARMY MATERIEL COMMAND
- U.S. ARMY CORPS OF ENGINEERS
- U.S. ARMY SPECIAL OPERATIONS COMMAND
- U.S. ARMY PACIFIC
- U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
- U.S. ARMY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
- U.S. ARMY CRIMINAL INVESTIGATION COMMAND
- U.S. ARMY MEDICAL COMMAND
- U.S. ARMY MILITARY DISTRICT OF WASHINGTON
- U.S. ARMY SOUTH
- U.S. ARMY TEST AND EVALUATION COMMAND
- U.S. ARMY SAFETY CENTER
- U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND

PROGRAM EXECUTIVE OFFICER

- AIR AND MISSILE DEFENSE
- AMMUNITION
- AVIATION
- COMMAND, CONTROL, AND COMMUNICATIONS (TACTICAL)
- CHEMICAL AND BIOLOGICAL DEFENSE
- COMBAT SUPPORT AND COMBAT SERVICE SUPPORT
- ENTERPRISE INFORMATION SYSTEMS
- GROUND COMBAT SYSTEMS
- INTELLIGENCE, ELECTRONIC WARFARE AND SENSORS
- SOLDIER
- SIMULATION, TRAINING AND INSTRUMENTATION
- TACTICAL MISSILES

PROGRAM MANAGERS

- CHEMICAL DEMILITARIZATION
- INFORMATION SYSTEMS
- JOINT SIMULATION SYSTEMS
- MISSILE DEFENSE AGENCY

DIRECTOR

- ARMY ACQUISITION EXECUTIVE SUPPORT AGENCY
- ARMY RESEARCH LABORATORY

(CONT)

NETC-EST-A

SUBJECT: Common Access Card (CAC) and Public Key Enabling (PKE) Mandates

DISTRIBUTION: (CONT)

INSTALLATION MANAGEMENT AGENCY

CF:

PRODUCT MANAGER, SECURE ELECTRONIC TRANSACTIONS-DEVICES

U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH ARMY

SIGNAL COMMAND

HUMAN RESOURCES COMMAND

COMMANDANT

U.S. ARMY LOGISTICS MANAGEMENT COLLEGE

U.S. MILITARY ACADEMY