



REPLY TO
ATTENTION OF

DEPARTMENT OF DEFENSE
UNITED STATES SOUTHERN COMMAND
3511 NW 91ST AVENUE
MIAMI, FL 33172-1217

SCCS

27 September 2002

POLICY MEMORANDUM: 11-02

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: USSOUTHCOM Information Assurance Program, Policy for Public Key Infrastructure (PKI)

References:

- a. Memorandum, DEPSECDEF, 6 May 1999, Sub: Department of Defense (DOD) Public Key Infrastructure (PKI)
- b. Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0, 29 October 1999
- c. U.S. Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999
- d. Public Key Infrastructure Implementation Plan for the Department of Defense, Version 2.0, 29 October 1999
- e. Memorandum, DEPSECDEF, 10 November 1999, Sub: Smart Card Adoption and Implementation
- f. Message, HQDA SAIS-ZA, DTG 101256Z MAY 00, Subject: Public Key Enabling of Private Web Servers - 30 June 2000
- g. Message, Joint staff, J6, Sub: Firewall Policy

1. Purpose: The purpose of this memorandum is to establish the policy for the implementation of Public Key Infrastructure for the United States Southern Command (USSOUTHCOM).

2. General: PKI is being implemented as part of the Defense In-Depth Strategy to achieve information superiority by protecting information vital to combatant commanders and business operations. In addition, PKI provides the necessary authentication, confidentiality, integrity, and non-repudiation needed to migrate business operations to a paperless environment. PKI includes the integrated Defense Enrollment Eligibility Reporting System/Real Time Automated

SCCS

SUBJECT: USSOUTHCOM Information Assurance Program, Policy for Public Key Infrastructure (PKI)

Personnel Identification System (DEERS/RAPIDS) Workstations, Department of Defense (DOD) Certificate Authority and Root Authority, the Local Registration Authorities (LRA), and Verification Officials (VO) who staff the DEERS/RAPIDS workstations.

3. Application: This policy 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, USSOUTHCOM user and application requirements for PKI on encrypted networks and in the tactical environment will be handled on a case-by-case basis.

4. Policy:

a. All implementations of PKI within USSOUTHCOM shall use the standard DOD PKI Medium Assurance Infrastructure. The existing and planned infrastructure provided by DEERS/RAPIDS will become the DOD PKI Medium Assurance Infrastructure component for issuing PKI Certificates.

b. The Class 3 PKI token for Identity and Encryption Certificates issued to USSOUTHCOM users for use on unencrypted networks will be contained on the DOD Common Access Card (CAC).

c. All new procurement actions that require Public Key Cryptography will include in the solicitation process the requirements to use the PKI Certificates and Keys issued by the DOD PKI Medium Assurance Infrastructure.

d. Any current USSOUTHCOM pilot programs, initiatives, and systems that may be using Public Key Cryptography must migrate to the use of the PKI Certificates.

e. The standard DOD PKI Medium Assurance Identity Certificates contained on the CAC will be the primary set of PKI Certificates used for Digital Signature capability within USSOUTHCOM. Any USSOUTHCOM personnel who have software certificates issued to them should transfer over to the set of PKI Certificates on their CAC.

f. The PKI Identity Certificates contained on the CAC will be used to access USSOUTHCOM unclassified networks and will be capable of verifying a user's access through use of the DOD PKI Identity Certificates contained on the DOD CAC.

g. The Standard DOD PKI Medium Assurance Identity Certificates will be used to digitally sign messages that are created and sent from any unclassified USSOUTHCOM E-mail system other than the Defense Message System (DMS). By October 2003, all unclassified E-mail messages sent shall be digitally signed using the DOD PKI Medium Assurance Encryption Certificates contained on the CAC. Until that DOD milestone occurs, E-mails shall be

SCCS

SUBJECT: USSOUTHCOM Information Assurance Program, Policy for Public Key Infrastructure (PKI)

digitally signed only when non-repudiation and/or authentication of the E-mail sender is required due to USSOUTHCOM bandwidth considerations.

h. All E-mail messages created and sent from an unclassified E-mail System other than DMS and that require encryption shall be encrypted using the DOD PKI Medium Assurance Encryption Certificates contained on the CAC.

i. All USSOUTHCOM's Web Servers will become Secure Socket Layer (SSL) enabled via the DOD Medium Assurance PKI.

j. Army Signal Activity (ASA) will install the CAC readers (hardware). Additionally, all training and Operations and Maintenance (O&M) will be the responsibility of ASA. The initial New Equipment Training (NET) and equipment delivery was conducted the week of 10 June 2002. The Information Management Officers, System Administrators, and Help Desk personnel received training during this fielding. In the future, training on CAC and CAC reader use will be incorporated as part of the ASA sponsored Network User's Course.

k. All USSOUTHCOM firewalls will uniquely identify and authenticate the claimed identity of any user before granting access to the firewall's administration interface. All authentication requests will be PKI enabled by July 2003.

5. The USSOUTHCOM point of contact is SCJ621, DSN 567-3207 and COMM (305) 437-3207.

FOR THE COMBATANT COMMANDER:

A handwritten signature in black ink, appearing to read 'R. A. Huck', with a long horizontal flourish extending to the right.

R. A. HUCK

Brigadier General, U.S. Marine Corps
Chief of Staff, U.S. Southern Command

DISTRIBUTION:

D