

OPR: PENREN/C IT

1. References:

- a. Deputy Secretary of Defense memorandum, Department of Defense Public Key Infrastructure, dated 6 May 1999
- b. Deputy Secretary of Defense memorandum, Smart Card Adoption and Implementation, dated 10 November 1999
- c. DoD Chief Information Officer memorandum, Department of Defense (DoD) Public Key Infrastructure, dated 12 August 2000
- d. Under Secretary of Defense (Personnel and Readiness) memorandum, Common Access Card, dated 18 Apr 2003
- e. Under Secretary of Defense (Personnel and Readiness) memorandum, Common Access Card Issuance, dated 25 Sep 2003
- f. DoD 5400.7-R, DoD Freedom of Information Act (FOIA) Program, September 1998

2. Applicability: This policy applies to all government and contractor personnel performing duties for PENREN/C, both on-site and off-site.

3. Policy: This policy ensures that PENREN/C personnel are following DoD guidelines for digitally signing and encrypting (when necessary) e-mail. It outlines when digital signatures are required and what type of information must be encrypted when transmitted outside of the PENREN/C network.

4. Definitions:

- a. **Public Key Infrastructure (PKI):** PKI is a complex system that uses electronic documents known as digital certificates to verify an individual's identity, to ensure information isn't altered between sender and receiver, to encrypt information so that it is unreadable by anyone but the recipient, and to provide undeniable proof of the identity of the sender and receiver of information. PENREN/C participates in the DoD-wide PKI.
- b. **Common Access Card (CAC):** In November of 1999, the Deputy Secretary of Defense directed the military services to implement smart card technology for use in both physical and electronic access control. A smart card is a plastic card resembling a traditional credit or debit card that contains a computer chip, bar codes, and magnetic strips. The resulting DoD smart card is known as the Common Access Card. The CAC has numerous functions, literally combining several cards into one. At PENREN/C, the initial use of the CAC will only be for digitally signing and encrypting e-mail.

- c. External Certificate Authority (ECA): There are many external contractors and other organizations with which the DoD communicates that will not be issued DoD PKI certificates. The ECA PKI program was implemented by DoD to provide a mechanism for these external entities to obtain certificates and thereby comply with DoD directives.
- d. Digital Signature: A method to validate that a specific message was not altered during transmission. This process involves creating a message, encrypting it, and sending both the original message and the encrypted message together. Once received, the recipient compares the contents of the original message against the contents of the encrypted message to make sure the information has not been changed.
- e. Non-Repudiation: Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
- f. Digital Certificate: A digital certificate is an electronic means of establishing credentials when sending e-mail or connecting to a web server, issued by a certification authority (CA; PENREN/C digital certificates fall under a DoD-wide CA. A CA contains the user's name, a unique serial number, expiration dates, a copy of the certificate holder's public and private keys (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is genuine. DoD digital certificates reside on the CAC.
- g. Public/Private Key Pair: Two mathematically related files contained in a digital certificate. When the key pair is used for encryption, the sender uses the public key of the recipient to encrypt the message, and the recipient uses their private key to decrypt the message. When the key pair is used for signing, the signer uses their own private key to encrypt a representation of the message, and the recipient uses the sender's public key to decrypt the representation of the message for signature verification. DoD digital certificates contain three key pairs; one for digitally signing e-mail, one for encrypting e-mail, and one for identity verification, primarily to web servers.
- h. For Official Use Only (FOUO): FOUO information is unclassified information that is exempt from release to the public under the FOIA. Reference (f) outlines the nine exemption categories to the FOIA under which the FOUO information may fall. These exemption categories deal with sensitive information. Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, but do not meet the criteria for designation as classified material.

5. Responsibilities:

- a. PENREN/C Network Account Holders. All government and contractor employees supporting PENREN/C on-site (hereinafter referred to as 'internal users') will obtain a CAC from the Pentagon Badge Office or a designated alternate facility. These

individuals will use the CAC to digitally sign and, when required, encrypt e-mail, as well as authenticate themselves to PENREN/C or other DoD web servers.

- b. Off-site Contractors Supporting PENREN/C. Contractor employees who directly or indirectly support PENREN/C off-site (hereinafter referred to as 'external users') and regularly exchange e-mail with PENREN/C personnel or need to access PENREN/C private web servers, must obtain an ECA. These individuals will use the ECA to digitally sign and, when required, encrypt e-mail as well as authenticate themselves to PENREN/C web servers.

6. Procedures:

- a. Use of Digital Signatures: All e-mail sent by internal or external users related to official PENREN/C or other government business will be digitally signed using either a CAC or ECA.
- b. Use of encryption:
 - i. Internal users: All e-mail containing FOUO information will be encrypted with the public key of the recipient when transmitted anywhere outside of the PENREN/C network. If the recipient does not have a digital certificate, contact the PENREN/C Information Assurance Manager for further guidance.
 - ii. External users: All e-mail related to PENREN/C business that is FOUO shall be encrypted with the public key of the recipient when transmitted over the Internet. This includes all e-mail between prime contractors and their sub-contractors, as well as e-mail between sub-contractors. If the recipient does not have a digital certificate, contact the PENREN/C Information Assurance Manager for further guidance.
- c. Obtaining a Digital Certificate:
 - i. CAC: All internal users will obtain a CAC from the Pentagon Badge Office or designated alternate facility. Contractors will complete a DD Form 1172-2 and submit through the same channels used to obtain a Pentagon Building Badge. Military and government employees simply need to provide two forms of identification.
 - ii. ECA: ECA identity and encryption certificates are obtained through any one of three commercial vendors who have been certified by the DoD to provide this service. Each individual who sends e-mail to PENREN/C internal employees or connects to PENREN/C private web servers must obtain a unique ECA. In general, obtaining an ECA is a 3-step process:
 1. Provide the vendor with notarized paperwork proving your identity and the existence of your firm.
 2. Pay for and then download the ECA from the vendor.
 3. Configure the ECA on the recipient's PC.

The detailed process for obtaining and configuring these certificates is contained at the following address: <http://iase.disa.mil/pki/eca/>. This site also contains links to the three ECA vendors.

- iii. Other Transmission Methods: DoD PKI will be the primary security mechanism for e-mail. However, it is not always practical to apply PKI to other transmission methods such as web-based transactions. The rule of thumb for transmitting FOUO over the Internet over other transmission protocols is as follows:
 1. Transmission protocol will use a secure login method and a minimum of 128-bit encryption for data transmission.
 2. Unique login credentials for each user using DoD directives for password management.



Michael R. Sullivan
Director