

Public Key Infrastructure, the Common Access Card, and NMCI

The implementation of Public Key Infrastructure (PKI) is an important piece of the Defense in Depth strategy of NMCI. PKI technology significantly enhances the security posture of DoD networks by enabling the following desirable Information Assurance functions: non-repudiation, integrity, authenticity, and confidentiality.

PKI on NMCI consists of three primary elements: the tokens (Common Access Card (CAC) and Remote Access Service (RAS) software certificate); the middleware & card reader; and the infrastructure.

CAC issuance and maintenance is a government responsibility. Users should contact their local Information Systems Security Manager (ISSM) or the NMCI Help Desk if they have operational problems with their CAC. NMCI PKI training is provided by EDS.

CAC user training can be obtained via the eLearning catalog on the NMCI Homeport website at <http://homeport/>.

NMCI PKI component installation and maintenance is the contractor's responsibility. Users should report any difficulty with PKI functions directly to the NMCI Help Desk. A PKI User Guide and CAC Quick Reference Guide are available via the Homeport User Information page. The latter explains how to configure your NMCI seat to enable email encryption and digital signing.

Users employing the Alcatel RAS solution will require a soft (floppy disk) certificate issued by an EDS/Raytheon Local Registration Authority (LRA). A list of LRAs, a RAS User Guide, and a Quick Reference Guide are also available via the Homeport. An impending upgrade to the RAS solution will support CAC-based digital certificates.

Command-approved Outlook Web Access (OWA) users will need to register an identity certificate with the browser from which they are accessing their mailbox. An OWA User Guide, a Quick Reference, and links to the eLearning training required for approval are available on the Homeport.

DoD Policy on PKI

The DoD CIO has directed by 1 April 2004:

- ✓ All DoD users shall be issued DoD PKI certificates on the primary token platform, the CAC
- ✓ All DoD unclassified private web servers shall require client side authentication using DoD PKI identity certificates
- ✓ All official e-mail sent within DoD shall be digitally signed
- ✓ DoD unclassified networks will be Public Key enabled for hardware



Visit our NMCI website at www.nmci.navy.mil

Site transition Support - NMCI Integrated Support Center at 877-ISC-NMCI

User Support - EDS Help Desk at 866-843-6624

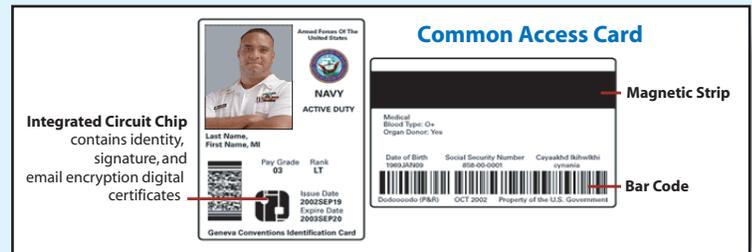
NMCI

bringing secure information technology to the warfighter

Preparing for PKI

End User Responsibilities

- ✓ Update CAC at local RAPIDS workstation - If certificates on a user's CAC were issued prior to 19 May 2002, the user must acquire new certificates to perform cryptographic logon. Users must also ensure their CAC carries their NMCI email account address to ensure full interoperability with networks outside of NMCI. Currently, this can only be accomplished by visiting a RAPIDS location. Users can find the nearest RAPIDS by accessing the DoD RAPIDS Site Locator at <http://www.dmdc.osd.mil/rsl>
- ✓ Complete eLearning on Homeport – An interactive, comprehensive overview of CAC and PKI is available from within the Intranet at <http://training/>. Users are issued a certificate upon completing the 30-minute course. This module can be counted towards a user's annual Information Assurance training requirement.
- ✓ Remember Personal Identification Number (PIN) – This protects the user's private information on the CAC and is assigned by the user at the time of CAC issuance. A user is prompted for the CAC PIN when logging onto the NMCI network with the CAC. Users who have locked themselves out of their CAC by entering an incorrect PIN on three successive attempts must visit a RAPIDS workstation to have their CAC unlocked and PIN reset.
- ✓ Configure NMCI seat for PKI – Users should download the CAC Quick Reference Guide available on the Homeport's User Information page and follow step-by-step instructions.
- ✓ Read and comply with applicable NMCI User Alerts and Information Advisories – These communiqués contain important information and guidance on NMCI policy and user actions.
- ✓ Employ CAC-based (i.e., cryptographic) logon to access NMCI – When directed, users will be forced to discontinue username/password network authentication and use the CAC to access NMCI. Once the username/password option is turned off, users must contact the NMCI Help Desk for temporary network access in the event that they have forgotten their PIN or misplaced their CAC.
- ✓ Sign and encrypt email – Current policy mandates digital signing of official email and encrypting messages containing potentially sensitive material; provided both email encryption and digital signature certificates are on a user's CAC and the seat has been properly configured for PKI, this capability is currently supported by Microsoft Outlook on NMCI.



PKI User Components

- ✓ CAC – Primary storage device for private keys and certificates.
- ✓ Digital Certificate – File containing user's identity data and public key; certificates bind identity to the private key.
- ✓ Private Key – Privately held string used to decrypt data.
- ✓ Public Key – Publicly available string used to encrypt data.
- ✓ Card Reader – Computer's hardware interface for the CAC; integrated with keyboard for desktops, card slot found on the side of portables.
- ✓ Middleware – Current version, ActiveCard Gold 2.2, has a utility through which users can view their CAC certificates.
- ✓ Certificate Validation Software – Verifies certificates are trusted, not expired, and not revoked; users may experience some delay in opening signed email and authenticating to PKI-enabled websites.

