

Common Access Card (CAC) is a Cyber Security Ace in the Hole

December 2006



If you use your computer password to remember your spouse's birthday, you better find another way. There's a new card in the Army's deck of cyber security procedures and it's an Ace. The DoD Common Access Card (CAC), currently in roll out, will replace all those IDs and passwords and still increase information assurance and cyber security in a way that is efficient and easy to use.

All authorized personnel have, or will receive, a personal CAC with photo. Within each card is a chip that contains three digital certificates; signing, encrypting, and digital signature all used to protect your cyber identity. This information is encrypted, so a lost card does not mean a user's identity and data are compromised. Each card also has a corresponding Personal Identification Number (PIN) that you chose at the time of issuance. A user must use the correct PIN with the correct card in order to gain access to an Army applications or network. This double layer of security combines the physical, something you have, the card, and mental, something you know, the PIN and you need both working together to get in the cyber door. Special card readers and software are being added to all Army computers to allow access only by authorized card and PIN combinations.

Most people are already very familiar with the use of a CAC. It works similar to a bank ATM card or a credit card with a PIN that lets you access your accounts. By simply inserting the card into a reader and entering the correct PIN, an authorized user gains access to his or her cyber account.

While this is an easier and efficient way of protecting access to Army cyber resources, it still requires that card holders prevent unauthorized users from gaining access to both the CAC and the PIN. Protecting a CAC is the same as protecting a personal bank card. Keep the card in a safe place when not in use. If you must write down your PIN, never keep it with or near your CAC. Make sure that no one is watching when you enter your PIN, (Shoulder surfing).

Not only does a CAC increase access security it also makes our work environment a little easier. We have enough to deal with without remembering a continually changing and more complicated list of computer passwords. This list changes often because policy requires users to change their passwords frequently in order to add an extra layer of protection. Some networks even force users to do this. In addition, Army password regulations require a series of upper and lowercase letters with numbers and non-numeric symbols like dollar signs. Under stress or fatigue, these complex passwords and login IDs sometimes don't come to mind. That's why some people resort to the very unsafe practice of writing all their IDs and passwords down in an easily accessible location – easily accessible to prying eyes.

The CAC eliminates this problem. One card, one PIN means freeing up a few brain cells for more important work. It also means better security for the information and resources that ultimately protects all Army personnel, especially our troops in harm's way.

For more information on the CAC program visit the Army Information Assurance website: <https://informationassurance.us.army.mil/cacpki/> and click on the CAC/PKI Division link or click on the CAC PKI information link on the My Security web page.