



# Security Made Easy with the NMCI, PKI, and the CAC

By Josephine Smidt with Rebecca Nielsen

You have heard of the Navy Marine Corps Intranet (NMCI), the Department of Defense (DoD) Public Key Infrastructure (PKI), and the Common Access Card (CAC). You may even have heard about Public Key Enabled (PKE) applications. Here at the Department of the Navy Chief Information Officer (DON CIO), these aren't abstract concepts. They are woven into daily workplace activities, ensuring that DoD Defense in Depth information assurance requirements are met. One of the benefits of working in my office is that we test the technology that will be deployed to the DON community. This is both good and bad: we use all the cool, new technology, but we have to work out the bugs prior to deployment.

I'll explain how implementation of the new PKI technology has helped me do my job better as a member of the Information Assurance Team at DON CIO. The PKI provides digital certificates to subscribers — people and computer systems. Digital certificates and their associated keys are credentials, similar to photo identification. Unlike a photo ID, however, digital certificates can also be used for electronic signatures and encryption — assuring secure communications between users. By itself, PKI doesn't do anything. However, the security services that PKI provides: authentication, data integrity, confidentiality, and non-repudiation (described in the text box above), transform time-consuming, insecure paper processes into streamlined, secure electronic systems. Applications like e-mail and the Defense Travel System (DTS), that are programmed to use digital certificates are PK Enabled.

Like any credential, my digital certificates are only useful if I have them when I need them. So, I carry them with me on my CAC. The CAC contains a small chip (almost as powerful as the first personal computers) that not only contains my certificates and associated keys, but also the processing power to use the keys and to protect them

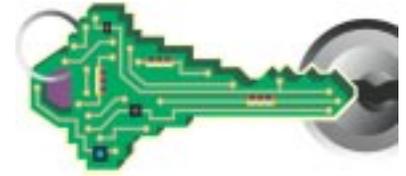
*The National Information Systems Security (Infosec) Glossary defines the following five security services. PKI provides all but authorization.*

- **Authentication:** Establish the validity of a transmission, message or originator.
- **Authorization:** Access privileges granted to a user, program or process.
- **Confidentiality:** Assurance that information is not disclosed to unauthorized persons, processes or devices.
- **Data Integrity:** Data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- **Non-Repudiation:** Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

from unauthorized disclosure. The CAC also has other technologies, including a photo (for visual identification), a magnetic stripe and a bar code. Since all of these are on the same card, I will soon only have to carry one card and remember one password — the one that tells the computer chip that I am the authorized user. There is an icon at the bottom of my screen that changes color when my CAC is being used to verify or authorize something. This is especially helpful, when your workstation seems to take longer than usual to do something, as the verification process sometimes takes a couple of seconds.

I use my CAC and PKI on a daily basis. My office has recently been designated as classified, and as a result, we decided to test how easily the CAC can work with biometrics to enter the secure area. When I arrive in the morning, I swipe my CAC and put my thumb on the reader and the door opens. Right next to the reader that we currently use is one that we will be using in the not-too-distant future. This reader doesn't require swiping, but reads my CAC from the chain around my neck as I press my finger. How cool is that?

Our office has not switched over to NMCI yet, but we have been using the CAC to log



on to the network — the CAC contains our userid and password. Some personnel use PKI to log on by inserting the CAC into a card reader located on the side of their laptop and typing in the CAC Personal Identification Number (PIN). The chip on the card communicates with PKE Microsoft Windows 2000 to authenticate the identity certificate. Since the PIN is useless without the card, they don't even have to change it every 90 days. We will all be using this method when we switch over to NMCI.

I digitally sign each e-mail I send so that the recipient will know that the e-mail came from me, and that the contents have not changed since I sent it. The NMCI workstation comes with both Outlook and the middleware needed for Outlook to work with the CAC. All I have to know is the PIN. Someone who wants to send me an encrypted e-mail, either can retrieve my e-mail encryption certificate from the Global Address List or from a signed e-mail I have already sent. This certificate can encrypt information that is sensitive and should not be sent in a manner that allows anyone to read it. When I receive an encrypted e-mail, Outlook communicates with my CAC to decrypt the information.

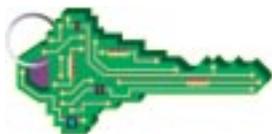
Since I used the CAC to log onto the workstation, if I have to step away from my desk, all I have to do is remove the CAC from the reader and my desktop is automatically locked so that no one else can access it. When I return, I put the card back into the reader and enter my PIN to return to where I left off. Since unattended workstations are not secure, and security is a primary concern, I really like this feature. Even if I forget to take my CAC out of the reader, my screen saver will kick in after fifteen minutes and I'll need both my CAC and my PIN to return to the desktop (since I need the CAC to get into my office, I try not to forget and leave it in the reader).

E-mail isn't the only application that is PKE. I use PKI to submit travel requests and process travel claims using DTS. Once I have filled out my travel voucher, I digitally stamp it. This is the equivalent of digitally signing an e-mail, and I can't do it without my CAC. I click on the button that says stamp, and the CAC and the PK Enabled DTS work together to verify who I am and to encrypt my authorization or voucher. Since the process is electronic, there are no paper forms to get lost and my reimbursement is sent directly to my bank account in about one week.

When I am on travel or working from home, I can use my CAC and my NMCI laptop for remote access to the network. I log on just as I would at work with my CAC in the card reader and dial in. The communication between my workstation and the network remote access server validates my identity, verifies that I am permitted to access the network, and establishes an encrypted communication link — all based on my identity certificate.

When I think about how many passwords I had to remember, how long it would take to get a travel authorization approved/reimbursed for travel expenses and, how it was not even possible to encrypt my e-mail outside of the SIPRnet, it hits me just how much this little card has simplified my daily work life. Not to mention how it will continue to influence my work in the future, with things like contact-less CACs (where I don't swipe the CAC, but it is read from a distance); using my CAC to send signed e-mails with my Blackberry and, using a variety of applications from personnel management software to financial programs and not having to remember a different password for each.

While technology is never a substitute for security awareness, the implementation of NMCI, PKI and the CAC show how implementation of robust security can make our jobs easier. It is definitely a very exciting time to be in the DON.



*Josephine Smidt is a Management Analyst on the DON CIO IA Team. Rebecca Nielsen works for Booz Allen Hamilton Inc.* □

# The Navy's Web-based Reverse/Forward Auction

By Cmdr. Steve Dollase, SC, USN



**S**ept. 5, 2002, NAVICP (Naval Inventory Control Point) conducted the Navy's first online forward auctions. The two auctions ran in two phases, with each phase consisting of the sale of two damaged CH-53D helicopters and associated parts packages. Three firms registered to participate as bidders. The winning bidders are expected to refurbish the aircraft for commercial applications such as firefighting, a requirement that has generated significant demand for heavy lift aircraft in the past few years. The two contracts resulting from the auctions are valued at nearly \$5 million. Naval Air Systems Command (NAVAIR) will receive the aircraft proceeds and NAVICP will retain the remaining proceeds to purchase similar helicopter parts.

The forward auctions, leverage the latest commercial technology and are part of NAVICP's innovative strategy to reduce U.S. Navy excess inventory, which consists of weapons system parts that the Navy might need later, but will most likely replace with state-of-the-art designs. The auctions also create a commercial marketplace for future sales. In fact, both of the winning bidders will have the option to buy additional CH-53D helicopters and parts within six months of contract award. This creative initiative allowed NAVICP to transform unusable assets that might otherwise deteriorate — into funding to support the next generation of weapons systems.

The forward auctions are the latest success story in NAVICP's Internet-based action program. In May 2000, NAVICP conducted the first Internet-based reverse auction in the Federal Government. The auction, which lasted 51 minutes, provided the competitive pricing mechanism for NAVICP to award a contract for aircraft ejection seat recovery sequencers (the "brains" of the ejection seats). The auction saved an estimated 28 percent from the historical price for recovery sequencers. NAVICP awarded the contract within an hour of the auction closing — a significant time savings.

NAVICP conducted four additional auc-

tions under the pilot reverse auction program, resulting in estimated savings of 21 percent, or \$14.8 million. Internet-based reverse auction technology allows online bidders to compete in real-time for contracts by lowering their price offers (or raising them in a forward auction) as they see other bids posted. Bidders are unable to identify competitors, only the current low bid is visible. The auctions are conducted in a secure, Web-based environment. Participants are screened in advance before granting access to the auctions to ensure that they are qualified sources for the items under consideration. This is particularly important with complex weapons systems. Auctions work best when there are three or more bidders, and when specifications permit easy comparison between products.

Convinced of the power of the concept, NAVICP, with the sponsorship of its parent command, the Naval Supply Systems Command (NAVSUP), awarded two five-year, best-value contracts for auction services; one to Procuri for a self-service, desktop tool and the other to eBreviate for a full-service tool. The eBreviate solution also offers market research services, helpful in determining suppliers for a particular requirement. In the first year, NAVICP contracts were used by NAVSUP activities and twelve other Federal Government agencies to conduct 43 auctions valued at over \$144 million with typical savings of 8 to 24 percent. The auction tools are available, free of charge, to Navy and Marine Corps activities, and to other Federal Government activities on a fee-for-service basis.

The NAVSUP/NAVICP Reverse Auction Team earned a FY 2000 Department of the Navy Competition and Procurement Excellence Award for their success. NAVSUP/NAVICP recently launched a Navy auction Web site at [www.auctions.navy.mil](http://www.auctions.navy.mil). These tools are just one more way that the Navy and Marine Corps team can maximize resources and improve combat readiness.

*Cmdr. Steve Dollase is NAVICP's Director of Acquisition Policy.* □