



Access Approved: Biometrics and Smart Cards Open Doors to Improved Efficiency

By Capt. Robert Conway, USNR, Fleet Liaison Officer, DON eBusiness Operations Office

DON eBusiness Operations Office

The DON eBusiness Operations Office is an innovative eBusiness center encouraging the adoption of eBusiness technologies in the Navy and Marine Corps by providing funds and management expertise to requesting commands. The DON eBusiness Operations Office mission is to find new ways to use eBusiness technology to support warfighters, improve work processes, enhance quality of life and increase efficiency. The eBusiness Operations Office accepts ideas for pilot projects from any Navy or Marine Corps command. Ideas are screened for impact and scalability to the entire DON, and selected projects are funded. To date, 53 pilot projects have been funded in this way. The eBusiness Operations Office provides project management expertise for each pilot project.

eBusiness Pilot Project

The DON eBusiness Operations Office and SPAWAR Systems Centers Norfolk and Charleston are working with the DoD Biometric Management Office and the Department of the Navy Chief Information Officer (DON CIO) to determine future technologies that the Common Access Card (CAC) will support. The CAC (sample shown at right) contains multiple data storage technologies, including barcode, magnetic stripe and contact smart chip, which allow cardholders logical access to computer networks and can be used for physical security for controlled areas.

There are thousands of physical access control systems deployed throughout the Navy. The convergence of the CAC and biometric technology has the potential to enhance physical access control security with the benefit of integrating seamlessly into the legacy systems. The cost of upgrading existing physical access control systems to utilize biometrics is reduced by reusing much of the existing security system infrastructure.

Biometric technologies are being incorporated in secure personal identification and verification systems. Biometrics are automated methods to recognize a person based on a physiological or behavioral characteristic. These methods include fingerprints, voice patterns, iris scanning, finger and hand geometry, facial recognition and other techniques. The Navy and Marine Corps are evaluating several biometric applications, some of which include the use of smart card technologies for physical access to certain areas and buildings. These smart card applications are being evaluated to help shape the future of the DoD CAC card.

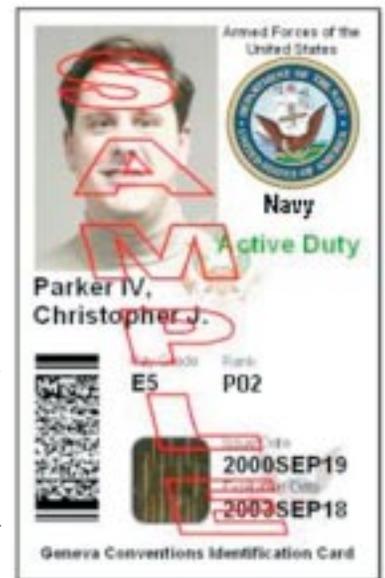
Biometrics in Access Control

In the past year, the DON eBusiness Operations Office in Mechanicsburg, Pa., partnered with SPAWAR Systems Center Charleston to test two different biometric access systems. Both projects included smart card technologies with biometrics. The

Photographs at right illustrate tests conducted at U.S. Pacific Command Headquarters (USPACOM) spaces. Tests assisted in determining which access control technologies to include in the new PACOM headquarters building currently under construction. Sample Common Access Card (CAC) shown below.



tests were executed at SPAWAR Systems Center Norfolk, and Camp Smith, Hawaii. The Camp Smith project, which included existing U. S. Pacific Command Headquarters (USPACOM) spaces (shown in the photographs above), assisted in determining which access control technologies to include in the new PACOM Headquarters building currently under construction. In both locations, stronger user authentication and a non-obtrusive method of achieving access control were desired.



Both projects tested "contactless" smart card technology. Many existing card readers require the card to be swiped through or inserted into a card reader to retrieve information stored on the magnetic stripe on the card, or on a chip. The physical wear shortens the life of the card, requiring more frequent reissuance of cards. Recent advances in technology store access information on a chip and use an integrated radio frequency transceiver to transfer data without the need for direct physical contact. This

technology is commonly referred to as a contactless card. The technology is available in a standard card size or in the form of a Radio Frequency Identification (RFID) tag that can be attached to cards and other devices.

When properly implemented, biometrics can exploit technology to reduce manpower. Biometrics can also be very cost effective, particularly when existing infrastructure is reused and the system uses an open architecture that allows use of many technologies. When integrated with the CAC, the system is very unobtrusive, and nearly transparent to users.

Technology Standards

Balancing the existing installed base with a contactless requirement, the SPAWAR Norfolk team piloted a card configuration with two contactless technologies. The first was a proximity smart card from HID Corporation for use with legacy systems. The second used the new ISO 14443A, defined by the International Organization for Standardization, for contactless and dual interface smart cards, known as MIFARE®. With a large worldwide installed base, it is a proven RF communication technology for transmitting secure data between a card and reader. It is also an open platform, available to any company willing to develop compatible products under conditions of common industry practice. This will ensure many manufacturers provide competing technologies all based on an open standard. This competition makes feature-rich products available at lower cost to the Navy and Marine Corps.

The federal government standard for future systems is ISO 14443 parts 1 through 4, which is equivalent to NIST IR 6887, defined by the National Institute of Standards and Technology Interagency Report. To enhance the level of authentication for entering controlled spaces, the Norfolk project team added fingerprint biometrics. The biometric templates, a mathematical representation of the fingerprint, were stored on a chip on the smart card. This had two significant benefits. First, it eased concerns about the use of fingerprints, since the entire verification occurred between the smart card and the reader. That is, the reader was simply verifying that the fingerprint read by the biometric scanner matched the mathematical representation of the fingerprint provided by the card. This eliminated the need to transfer employee fingerprint files over communications lines each time an employee entered a space thus providing personal security to employees as well.

The second advantage was that the existing infrastructure remained unchanged: there was no need for additional servers, databases and communications lines to verify fingerprints. Using the existing infrastructure reduced the cost of the pilot by over 60 percent. The existing card readers were upgraded to contactless smart card and fingerprint readers.

The Camp Smith project also used the current security infrastructure. It used contactless smart card technology and multiple biometric measurements including fingerprints and hand geometries (shown above). The original access system included a badge-based access control system layered in depth throughout the spaces. The major deficiency was that system verified the authenticity of the badge and did not verify the identity of the individual using the badge. Compromise of this system would disable access control and require the use of manned access control points.

*At right:
Illustration of
hand geometry
identification for
physical access
control.*



Since current guidelines prohibit modifications to the CAC, the Camp Smith project used a modular RFID tag to store the biometric credentials. The RFID tag was attached to a plastic sleeve holding the CAC. Many systems currently use magnetic badge swipe and PIN entry via a keypad. The use of biometrics allows access without entering a PIN. The project provided useful metrics for evaluating the feasibility and implications of incorporating contactless technology into future releases of the CAC.

“These projects were a major step in testing biometrics coupled with the CAC as a smart card,” stated Rick Caldwell, Pilot Project Manager at the DON eBusiness Operations Office. He added, “We tested two different types of biometric systems and contactless smart cards in different locations, with different legacy systems, and even tested to the new open architecture standard. That’s quite a big step in such a short time, and we did it for a very small investment. We learned a lot about fielding these systems, and the problems and solutions you can only experience by actually doing [testing] it with people. When the Navy and DoD are ready to deploy these technologies, we can use the knowledge and experience from these pilot projects to make these solutions work enterprise-wide. That’s the real power and value of doing a pilot project before full deployment.”

Systems Center Norfolk Testing

In Norfolk, physical access using the CAC with a contactless smart card reader and fingerprint reader was evaluated over a two-month period. Of 260 users, only two had initial difficulty enrolling biometrically, and they were able to fully participate in the pilot. Users were pleased with the system with some mild concerns about how their biometric data were being used. Those concerns were resolved by explaining that the biometric template resides on a contactless chip on the user’s personal smart card and not in a database. Biometric awareness increased by 44 percent during the evaluation. Users were granted access 97 percent of the time within one to two attempts. These results were in alignment with the users’ expectations.

SPAWAR Systems Center Norfolk management was pleased with the backwards compatibility of the solution and the enhanced security from the layered approach. The pilot is still in operation, and SPAWAR Norfolk is considering using the same approach to enhance security for their warehouses and SIPRNET spaces.

Camp Smith Testing

In Hawaii, some problems were encountered with fingerprints due to a recognized phenomenon: some women of Asian heritage have fingerprints with very low ridges. This can cause more false rejections than expected, denying access that should be authorized. Creating a unique configuration for these individuals solved this problem. Another cause for fingerprint errors can be occupation or hobby related. In one case, an individual who was an avid fisherman presented difficulties for the fingerprint reader simply because the constant use of his hands wore down the fingerprint ridge structure. The systems at Camp Smith are continuing in operation and users and security personnel are pleased with the unobtrusive nature of the system, and with the enhanced, layered security it provides.

Project Results

The results of both projects were very encouraging. The complete report on the Norfolk installation is available on the DON eBusiness Operations Office Web site, www.don-ebusiness.navsup.navy.mil. The report for the Camp Smith installation will be added to the site in the near future.

Future Applications

There is enormous potential to reduce the number of physical security tokens used throughout DoD to move toward standard interoperability. In these projects, the decision to use the CAC as the primary token in physical security has generated healthy debate between the physical security community and the CAC community. The challenge for the Navy and Marine Corps is to standardize the technology that supports a variety of installed electronic security systems, enhances the level of security and is scalable throughout DoD. There are many more technologies to evaluate, and operationally test prior to procuring the next generation of CAC.

The Norfolk and Camp Smith projects demonstrated that biometrics in an open architecture, embedded chip can meet the functional demands of the physical security community for access control. There are other maturing contactless and biometric technologies that need to be evaluated. As with all technologies, there are vulnerabilities that need to be investigated, and efficiencies, benefits, risks and costs to be weighed. As the Navy and Marine Corps move ahead and adopt more high-tech solutions at an accelerated pace, the lessons learned from these pilot projects serve to guide aggressive adoption of biometrics.

Other eBusiness Solutions

As with the biometric technology pilot projects, the DON eBusiness Operations Office has delivered new technologies to many areas, including communications, readiness, training, maintenance, logistics, engineering and procurement. One technology tested by the Seabees (Naval Construction Force) in Operation Iraqi Freedom, provided a secure battlefield network for transmittal of text and photographs, resulting in greatly enhanced combat communications.

Information on how commands can submit eBusiness ideas for pilot funding is available on the DON eBusiness Operations Office Web site, www.don-ebusiness.navsup.navy.mil.

Information Assurance Scholarship Program for Academic Year 2004-2005



Interested in pursuing a Masters or Doctorate? If you are, then you should read on.

The Information Assurance Scholarship Program (IASP), now in its third academic year, is a relatively new program that is expected to grow in the coming years to meet the increasing demands for information technology professionals with an information assurance focus. IASP was authorized by Chapter 112, Title 10, United States Code, to respond to DoD's recognized dependence on information technology for warfighting and the security of its information infrastructure.

This year, DoD will focus on enabling qualified civilians and military members to participate in both full-time and part-time study to complete master's degrees or to begin full-time doctoral programs in information assurance disciplines.

Department of the Navy (DON) civilian and military members may apply for IA scholarships through their Service chain-of-command to the DON CIO. Detailed instructions on the DON nomination process for a scholarship are available at www.doncio.navy.mil/iasp and general information is available at www.dod.mil/nii/iasp. The institutions offering full-time academic programs leading to a master's or doctoral degree are the Information Resources Management College (IRMC) of the National Defense University (NDU) in cooperation with IRMC's partner universities located throughout the United States, the Naval Postgraduate School (NPS) and the Air Force Institute of Technology (AFIT). Part-time academic programs leading to a master's degree are available only through IRMC and selected partnering institutions. These part-time programs may be completed in residence or via distance learning. Partner universities continue to grow as the program matures. The DoD IASP Web site www.dod.mil/nii/iasp is the best source for the most current information.

The cost of tuition, fees and books at IRMC and IRMC's partnering institutions, and at NPS and AFIT will be covered by the program. Additionally, TDY expenses are funded for students attending the full-time IRMC program. Any other TDY and/or PCS costs must be covered by the nominating component. Participants will continue to receive their military pay or civilian salaries from their component throughout the course of study. In the future, DoD may expand the program to include associate and undergraduate degrees, and certificate programs, as permitted by the statute.

For more information go to www.doncio.navy.mil/iasp.