SIGNAL ONLINE
More than a magazine: We're AFCEA.

About Us Archives Advertising Subscribe Legal AFCEA

search

This Month in *SIGNAL*

SIGNAL Connections

SIGNAL Online

Incoming: Talk Back

SIGNAL Scape

Event Coverage

On Cyber Patrol

SIGNAL Podcasts

Digital *SIGNAL*

SIGNAL Webinars

SIGNAL 2.0

Nightwatch

Resources

Acronym List

Source Book

Security Directory

Chapter News

Fixing the Identity Credentialing Problem

By Maryann Lawlor

August 2009

ShareThis Print Article

Staff Sgt. William Powell, USAF, scans a CAC at the Peterson Air Force Base west gate. The card is registered with the Defense Biometric Identification System (DBIDS), and information can be shared with other programs that now are being tested for identity verification on military bases.

Federation offers means to facilitate work with government agencies.

Companies now can acquire certified identity credentials that facilitate employees' physical and logical access when they work with the U.S. Defense Department, other government agencies and government-affiliated organizations. A biometrics-infused card authenticates a person's identity using bar codes, a digital photograph and fingerprints. Through a not-for-profit association, contractors become part of an operational system that can exchange credential information with the government.

Organizations interested in obtaining an identity credential for their employees first must join the Federation for Identity and Cross-Credentialing Systems (FiXs). The federation focuses on standards-based operating rules for identity authentication credentials and networks. It champions open-systems architecture and nonproprietary solutions.

Once accepted as a member, the organization's employees can apply for one of three levels of credentialing cards. Upon arriving at a Defense Department or other government organization site that accepts the FiXs-certified credential, a person's identification is verified. Individual facilities grant physical and logical access depending on the level of security and the work that will be done.

Dr. Michael J. Mestrovich, president, Unlimited New Dimensions LLC, Montclair, Virginia, and president of FiXs, explains that work on credentialing began five years ago. It was born from the need to verify the identification of contractors who were working throughout the department. In most cases, an individual repeatedly needed to obtain different credentials depending on the work he or she was contracted to perform. In current military operations, employees of contracted companies would have to wait in the United States or abroad—unable to begin work—until their identities were verified. The Government Accountability Office estimates that this delay cost taxpayers millions of dollars.

FiXs began its work with the Defense Manpower Data Center (DMDC), which is the organization that issues the Defense Department's Common Access Card (CAC). After conducting some pilot programs, FiXs signed its first memorandum of understanding with the DMDC in January 2006.

This was just the beginning of the hard work, Mestrovich says. "We began to get our membership involved in working with a set of operating rules, a set of security guidelines, a set of privacy guidelines, intellectual property issues—all the governance material that would make us a legal entity that could actually enforce the rules of our membership as they tried to interoperate with the Defense Department," he explains. It was two years of intensive work, but FiXs became operational in 2008. The FiXs identity-credentialing network currently is the only one certified to interoperate with the Defense Cross-Credentialing Identification System, or DCCIS, infrastructure.

To be able to obtain a FiXs-certified credential for its employees, an organization must first join the FiXs coalition of government contractors, commercial companies and not-for-profit organizations. Before it is granted membership, the applicant's company is vetted through LEXIS-NEXIS. Items such as the company's location, business practices and officers are examined. This process generally takes 10 business days.

Once it has successfully passed this vetting process, the organization is allowed to become a federation member. It is assigned a unique organization code, a classification structure that FiXs developed with the DMDC. The cost to join the federation initially is approximately $700; after the first year, a member organization pays $200 annually to maintain its membership within FiXs, which covers the cost of annual background checks.

The companies' officials sign an agreement that they will follow the FiXs rules. If a company breaks these rules, it is "immediately turned off," and its employees' credentials will no longer be recognized, Mestrovich explains. In addition, a financial penalty may be imposed.

At this point, employees from the member organizations are eligible to apply for the FiXs-certified card. Mestrovich explains that the federation's operating rules currently allow for three levels of credentials: high, medium-high and medium, identified by the numbers four, three and two, respectively.

The vetting process the employee undergoes is based on the level of credential being requested. Currently, Operational Research Consultants Incorporated (ORC), Fairfax, Virginia, is one of two companies that have been approved as issuers of the FiXs-certified credentials; the other is Data Systems Analysts Incorporated (DSA), which also is located in Fairfax.

Rick Webb, executive director of advanced technologies, ORC, explains that once an organization is accepted as a member of FiXs, its company-appointed official provides to ORC or DSA a list of employees who need a FiXs-certified card. At this point, individual employees can go online to fill out a preregistration form.

The remainder of the process depends on the FiXs-certified level the employee is applying to receive. For level two, the most basic identity verification level, the individual fills out the preregistration form, and that information is sent to LEXIS-NEXIS, which conducts a local criminal history check for the previous seven years of residences.

Once approved, the individual comes into one of ORC's facilities or an event, such as an American Logistics Association conference, at which ORC is issuing cards, and presents documentation of citizenship. The person's fingerprints are captured digitally for storage on the card, and a digital photograph is taken that will be laminated on the card and included on the computer chip. The card then is immediately activated and given to the applicant, providing that person with physical and logical access as granted by the organization for which he or she is working.

Applying for a level-three FiXs-certified credential is similar to the level-two processes; however, it requires the applicant to visit an issuing site twice. During the first visit, an applicant must present the same type of documentation as is provided for a level-two credential. However, because the third level is the equivalent of a commercial national agency security check, ORC sends the digitally captured 10 fingerprints to the Federal Bureau of Investigation via LEXIS-NEXIS for a national criminal background check. When ORC receives a clear background check, which can take from three to eight weeks, the applicant returns to the issuing site to obtain the activated credential.

For the fourth level of card, which is primarily for Defense Department contractors who already have a security clearance, a background investigation is not required. "We rely on the company security officer who has and keeps track of their Defense Department security clearances for their personnel to attest that this person has a Defense Department security clearance," Webb states. The applicant comes to an issuing location, documentation and biometric information is captured, and the FiXs-certified card is issued.

At all levels, the identification information is bound together in the database so that the identity information, including the digital photograph and fingerprints, verify a cardholder's identity. The cards are produced according to Federal Information Processing Standards-201 (FIPS-201). This means that the exact size and shape of the card complies with National Institute of Standards and Technology rules, and the individual's picture comprises an adequate number of pixels and appears in the appropriate position on the card. The computer chip within the card contains all of this information as required by the FIPS-201 as well as the organization's code, the employee's unique identification number and the public key infrastructure certificate.

The FiXs database interacts with the Synchronized Pre-deployment and Operational Tracker (SPOT) database so that credential information can be shared. SPOT will be the standard means for the U.S. Defense Department to identify and track contractors if the pilot program, which currently is underway, is successful.

When individuals arrive at a Defense Department site, their FiXs-certified credential is inserted into a handheld device. They then enter their personal identification number, or PIN, which unlocks the personal information on the card's embedded chip, and put their finger on the device to be verified. Although it meets the standards, Mestrovich emphasizes that a FiXs-certified credential cannot be called a Homeland Security Presidential Directive-12 (HSPD-12) card; however, it is referred to as HSPD-12 compatible, because it meets the requirements of the directive.

FiXs-certified credentials feature one-dimensional as well as two-dimensional bar codes on the chip, Mestrovich explains. The decision to require a one-dimensional bar code on the card came about because the federation realized that it will take a number of federal agencies many years to upgrade their infrastructure so that the two-dimensional bar code can be read. However, most of the existing equipment can read a one-dimensional bar code. This makes the FiXs-certified credential backward-compatible, he says.

The cost of the individual credentials varies and is based on the level and length of time the credential is valid. Even the highest level, a credential that is valid for up to three years, is less than $550. Mestrovich and Webb agree that, in most cases, companies will cover this expense for their employees.

At this point, the Defense Department has not decided how often background checks must be repeated for individuals. Mestrovich explains that this is the next set of rules FiXs is working out with the department. "When they issue a security clearance, it is good for five years. What it [the Defense Department] is telling us right now is that these credentials will be aligned with the length of the security clearance. We'll take the same rules and make them effective for the non-security clearance level," he shares.

One of the most notable security features of a FiXs-certified credential is the revocation procedure. An organization is required to revoke credential privileges within three hours of the time at which an employee leaves the company or no longer requires a credential.

The decision to include this revocation policy as part of the FiXs program came about in part because of the current challenges with the CAC system: Once a CAC is issued, tracking it and revoking privileges is not a simple process. In addition, the CAC system was designed for Defense Department employees, not for defense contractors. The department plans to address this issue as part of a future upgrade that would not require interaction with the cardholder.

According to Dan Turissini, chief executive officer, ORC, and member of the FiXs board of directors, this problem influenced the FiXs program policy development. The proliferation of CACs to contractors without the ability to know when employees left the company through which they originally received their cards poses a serious problem in both security and tracking the location of personnel. Placing the revocation responsibility on the employer—which is how it is handled in the commercial sector today—extends this logic and makes the employer responsible for its employees in the government space.

Mestrovich emphasizes, however, that both physical and logical access is granted by the client—the government facilities' personnel—not by the contractor. "There are no inherent privileges associated with the card. It's an identity authentication card. All privileges—whether you get on a base, a post, get into a lab or a building—are all granted locally. Likewise, with logical access—for example, getting into a Web site—you have to register, and they have to accept your card. Then they grant you the privilege of getting in and using various applications," he explains.

Currently, a pilot program is underway at Fort Belvoir, Virginia, which comprises the issuance of up to 3,000 individual FiXs-certified cards to employees of contractors. As of June, approximately 45 companies had been granted FiXs memberships and assigned organization codes, and less than 500 cards had been issued. The pilot program will continue through the end of September. Applying for the cards is strictly voluntary, and Mestrovich emphasizes that this is not a national identification card.

Possessing a FiXs-certified card is particularly beneficial to contractors when they are deployed to current theaters of operations. Some military systems, including the Joint Asset Movement Management System, or JAMMS, are being modified to accept the FiXs credentials.

WEB RESOURCES
Federation for Identity and Cross- Credentialing Systems: www.fixs.org
Operational Research Consultants Incorporated: www.orc.com
Data Systems Analysts Incorporated: http://www.dsainc.com/

Systems Support Contractor, Capabilities Tracking

The U.S. Army currently is conducting a pilot program of its Synchronized Pre-deployment and Operational Tracker (SPOT) at Fort Belvoir, Virginia. Combined with the Joint Asset Movement Management System (JAMMS), the technology provides the U.S. Defense Department with a logical way to bring contractors into a contingency area to support military and other government organizations during an emergency.

Federation for Identity and Cross-Credentialing Systems (FiXs)-certified credentials are being made available to companies and organizations that do business with the Defense Department. Because FiXs-certified credentials are Defense Cross-Credentialing Identification System compliant, information in the SPOT and FiXs databases can be cross-accessed. Contractors are the customers of the database, so they import and manage all of their employee information within the SPOT system. Conversely, the Defense Department can use the systems to authenticate identifications of contracted individuals who enter an area of operations and track them as they move about doing their jobs. It also offers the government a way to stay informed about available contracted capabilities when preparing to assist in an emergency.

According to Lt. Col. Richard Faulkner, USA, program manager, SPOT and JAMMS, Army Materiel Command, Fort Belvoir, the programs were modeled on two commercial methodologies that manage identities. First, the programs developers used the automated teller machine (ATM) model the banking industry established. In that model, individuals go into a bank, open an account and receive an ATM card. After that point, they can access their accounts by going to an ATM, inserting the card, entering their personal identification number (PIN) and the transaction has been recorded.

The second commercial model the team used to develop SPOT is the UPS/FedEx tracking system. As people present their credentials through a business process established by the military organization, information such as the date and time of the activity are entered into the database automatically. As a result, what Col. Faulkner refers to as a movement transaction is added to a person’s profile in SPOT.

“That has some very big implications about force protection. If there is a catastrophic event or a pandemic illness, we are still in contact with an area. Then you can begin to mitigate or even know who you’re going to look for. The updates are in these natural processing security points where there is some type of activity going on,” the colonel says.

One of the past and existing problems is that contracted personnel have a difficult time obtaining identification cards. Consequently, they arrive in a theater of operations, but cannot be put to work immediately without identification verification or a letter of authorization. By having people contractually enrolled in SPOT, the cycle time can be reduced so that contractors can be brought into the work force sooner.

“We are really preparing for the next contingency that is coming along so we can quickly flood an area with the immediate solutions to the requirements that the people need and deserve. In addition, we do not lose control of people because we have done some pre-work around getting control of who is on the ground and what they’re doing,” Col. Faulkner says.

The capability does more than just provide a head count. The colonel points out that this system enables the Defense Department to look across the broad range of capabilities that it already has under contract and apply those solutions where they are needed. This approach not only saves time but also money because the department can take advantage of economy-scale purchasing by accessing capabilities that already are under contract. In addition, the department can determine which new capabilities are required to address the current contingency. “The memorandum of understanding like the FiXs federation has gives us a tenfold step forward,” he says.

Col. Faulkner admits that not all Defense Department agencies are embracing the FiXs identification verification approach. Some are leery about accepting credentials that are not issued by the government. However, the colonel points out that it is contractors who currently conduct background checks of personnel and operate badging facilities. As a result of the derision among department agencies, it may take some time before a common system that involves commercial support is widespread, the colonel notes.

The Joint Staff already has expressed its support of a single means to verify the identification of individuals and track where they are located physically as well as which networks they are accessing. “My opinion is that this is going to be an intuitive transition that will be painful,” Col. Faulkner says. He is, however, appreciative of the support the programs have received from military leadership.

AFCEA International corporate members are eligible for a 25 percent discount on FiXs-certified credentials. ORC representatives will be available at LandWarNet in Fort Lauderdale, Florida, August 18-20, to provide additional information about the FiXs credentialing program.

Related:
There are no related articles.

Add a comment

Email:

Email me when this article is updated

Your Feedback:

Authors are entirely responsible for opinions expressed in material appearing in AFCEA publications and online products, and these opinions are not to be construed as official or reflecting the views of the Armed Forces Communications and Electronics Association.

Comments are moderated and are subject to review prior to posting.

***SIGNAL ONLINE*: Reading Loud and Clear.**

AFCEA International 4400 Fair Lakes Court Fairfax, Virginia 22033
Editorial 703-631-6192 * Advertising 703-631-6181* Email * Customer Service 703-631-6100