By Dennis Raefield

Leveraging IT for Access Control

Solutions that use 13.02 FICAM topology eliminate the need for proprietary access control panels

Trying to navigate through the numerous security regulations that are in place for government agencies and facilities can be a daunting challenge, even to the most seasoned security professionals. Buying access control solutions that are compliant with federal mandates, such as HSPD-12 or FIPS-201, means there are only a select few products that end users in the government sector can purchase. The only way to ensure these purchased solutions are in compliance with these requirements is to turn to the General Services Administration's (GSA) approved products list (APL).

But even then, there are still budgetary constraints that may make implementing the best access control system nearly impossible, and government end users are still faced with the prospect of investing a significant amount of money to upgrade their existing access control infrastructure without a reasonable ROI.

Requirements Abound

In the past, government facilities could implement low-cost access cards and readers as a simple means of securing doors. Now, they are required to have a particular type of smart access card—usually a personal identity verification (PIV) card—and that card has to be authenticated at the reader. This means that the system has to check to determine that each card hasn't been duplicated or spoofed; hence, there are many requirements in place at certain facilities to deploy some type of biometric credential solution in conjunction with the traditional card access system. Some even require the use of a PIN number in addition to these other layers.

All of these things have amounted to increasing costs across the government spectrum as agencies have sought to create secure digital identities for employees, most of who are required to be fingerprinted, photographed and issued cards that have digital certificates linked to them.

The quandary for many in the market has been how to link this new generation of secure credentials with existing physical access control systems (PACS) infrastructure, card readers, control panels and the like. The problem is that the majority of these products are on the lower end of the access control technology spectrum, specifically control panels, and don't have the capability to check and see if a card is fraudulent at the time it is presented.

One of the major hurdles federal officials ran into is that after agencies went on the APL and purchased the components necessary to achieve this new level of required security, they quickly found many of these solutions were incompatible with one another. In response, the government introduced a new program called Federal Identity, Credential, and Access Management or FICAM that outlines the requirements of an end-to-end access control solution in which all of the devices are interoperable with one another.

Two Different Topologies Offered for FICAM Compliance

Historically, most of these systems—identity, credential management, logical access and physical access—operated in silos and did not work very well together. With FICAM, the GSA is attempting to create a new level of interoperability between these solutions.

Topology 13.01. One of the options available to address this issue is that of an additional hardware component being installed between the reader and the control panel that has all of the intelligence necessary to check the card and ensure that the credential is authentic. It does this by leveraging the IT network to verify the information on the card, and checks if the credential has been reported as lost or stolen.

This method includes three categories of components: the card reader, the access control system or the PACS, and the intermediary validation system between the reader and the panel.

Topology 13.02. This is a completely new architecture that is optimized for leveraging an IT infrastructure to meet the FICAM requirements by "virtualizing" the PIV and PIV-I credential certificate validation and authentication functionality within the access control software. Physical access points are controlled using IP encryption bridges to connect door hardware and transform card readers into IP addressable devices. This topology was introduced as an alternative to the 13.01 topology because it does not require the additional hardware and third party software needed to add authentication and validation capabilities to traditional control panel systems. Credentials are presented at the reader and cryptographically challenged by the Freedom 1302 PACS and Validation software. These credentials are then authenticated and validated before an authorization check is performed to grant or deny access to the cardholder.

This unique approach eliminates the need for an intelligent hardware component that would otherwise be necessary to meet the requirements for FICAM by using a traditional PACS architecture. All data is encrypted to eliminate the opportunity for cyber threats, ensuring that a high-level of security is maintained to meet one of the stringent testing requirements of FICAM-approved products.

The Benefits of Using an IT-centric Solution

In an IT-centric environment, solutions leverage software running on hardware as opposed to firmware-supported hardware, which is counter to how things typically work in government access control applications. For the end user, they're able to take their existing IT infrastructure (TCP over IP) and run software on it to control their access control system in the same way they control network security for logical access to computers.

Using an IT-centric solution also provides users with significant costs savings, which is an issue when dealing with clients that have strict budgetary requirements like the government. Because much of

the hardware that's required in a traditional access control system is unnecessary under this kind of architecture, end users do not need to have the antiquated devices that would typically be required.

For instance, a solution that runs on the IT network doesn't require the use of any proprietary access control boards or panels to perform the authentication check at the door that other systems require. The user only needs the computers operating in their data bank running software with some type of interface at the door to connect the electric-strike contact, monitor whether or not the door is open and have a push button that people can use in the event of an emergency to exit the building.

Another potential drawback in using a solution that relies on panels is that even when the devices are supplemented with an intelligent component to complete the credential validation process, the technologies still do not have access to the real-time data that a solution using the IT-centric model does. When it comes to interoperability and the time it takes for validation of a credential, the 13.02 topology can interact with these other systems much faster to determine what policies or attributes may have changed, and make that decision quicker than a typical panel-based solution.

Why Buying FICAM-compliant Products Matters

Because federal agencies are required to purchase products on GSA's approved products list, any type of PACS solution—be it a traditional hardware-based system or one that is IT-centric—needs to have previously achieved FICAM approval before it is deployed. Having this approval paves the way for the deployment of various access control products in all federal agencies as well as all buildings leased by the GSA for other federal agencies.

Although the user is limited in what they can implement in their facility by what products are on the APL, they are protected. They can rest assured that what they do purchase works, is not vulnerable and meets all of the compliance checklist items.

The rigorous FICAM test program ensures that each product on the GSA's APL meets the functional requirements of FIPS 201 and NIST SP 800-116, that the system is secure from a network perspective, and that there is complete interoperability between all topology components.

Evaluating FICAM's Impact on Government End Users

At the end of the day, government users are looking for solutions that meet the necessary requirements at the lowest possible cost. Each agency has a prime directive, be it serving veterans, retirees or ensuring homeland security, not spending millions and millions of dollars on access control measures.

While the government has had access control mandates in place for well over a decade, there are still a number of agencies that have yet to fully meet all of the requirements. However, with FICAM, the GSA has said that all access control products purchased moving forward must meet these standards or else they won't be approved for use in buildings owned or operated by the federal government.

Eventually, everyone in the government sector is going to move toward interoperability in physical access, logical access and identity management. The best way to accomplish this is through the deployment of a solution that takes advantage of the IT infrastructure already in place.

Dennis Raefield *is the president and CEO of Viscount Systems.*