



## Coping and Compliance: Options for Integrators and End Users to Meet TWIC and PIV Integration Goals

In the seven years since the 9/11 attacks, infrastructure protection and personnel identification have been put center stage. A tangle of new legislation, major initiatives by government entities and burgeoning new technologies have put the security industry in the spotlight and left private enterprises scrambling to comply with often ill-defined mandates. This murky situation brings with it the specter of massive financial expenditures for both commercial businesses and government organizations.

Without question, the two most significant initiatives toward improved domestic security are Personal Identity Verification (PIV) cards for government personnel and Transportation Workers Identification Credential (TWIC) cards for any worker requiring port access. These programs, however, are radically different from most security infrastructures currently in place. Large-scale change brings with it the prospect of large-scale cost. Understanding these efforts, the goals and the available technology solutions will help all organizations choose an efficient and economically viable path toward compliance.

**New technologies far  
outstrip the  
capabilities of  
virtually all existing  
security  
infrastructures.**

### Understanding the Background

In August 2004, President Bush issued Homeland Security Presidential Directive (HSPD-12), which reads, in part:

*... it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees) ....*

“Secure and reliable forms of identification” for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee’s identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).<sup>1</sup>

In February 2005, the National Institute of Standards and Technology (NIST) published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and a number of supplemental publications on implementing the standard. This created the PIV card concept, which will become the unified form of ID called for in HSPD-12. The directive also had a tangential impact on the development of the TWIC program. TWIC sprang from the security framework laid out by Congress in the Maritime Transportation Security Act of 2002 (MTSA). The act required the Department of Homeland Security (DHS) to issue a biometric security credential to U.S. mariners and anyone who has unescorted access to secure areas of ports and vessels.



TWIC was formally adopted under the Security and Accountability for Every Port Act of 2006, commonly known as the SAFE Port Act. The program is managed and enforced jointly by the U.S. Coast Guard and the Transportation Security Administration (TSA).

Both the PIV and TWIC programs will rely on some form of smart card with photo, biometric information and data storage capacities of 64 KB or better. Therein lies the challenge for those tasked with implementation: the new technologies far outstrip the capabilities of virtually all existing security infrastructures. Jumping to cutting-edge technology would dictate gutting current systems — an immense task with an equally massive price tag.

For years, physical access control systems (PACS) provided the foundation for site security. These systems rely on barriers — locks, doors and gates — that are electronically activated by a code or card. Examples include doors activated by wall-mounted keypads or magnetic swipe cards.

PACS consist of hardware, in the form of servers, readers, networks and other related components, and software that can stand alone or connect to other networks within an enterprise.

PACS have improved since they arrived on the scene 40 years ago, with companies continuing to sink substantial sums into those improvements. Changes and upgrades are usually costly and must provide the end user with an enormous benefit over existing PACS for users to even contemplate alterations.

The major weakness of any PACS structure is user verification, or a lack thereof. Once a magnetic swipe card or pass code is issued, access control systems can't determine user authenticity. Should a card or a code be lost or stolen, an unauthorized user could gain site access. This weakness demands supplemental measures such as video surveillance, thus adding to infrastructure and operating costs.

### **Technology-Driven Solutions**

The PIV and TWIC programs differ from previous government-initiated security efforts because they will not rely on simply adding layers or making small evolutionary steps. When fully operational, PIV and TWIC will employ new technologies that are vastly different from precursors. Briefly, the major technologies in play are:

- **Biometrics** — An automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. The most common commercial modalities recognize fingerprints, palm prints, facial characteristics, iris characteristics, vocal characteristics or hand geometry. Biometrics have extremely high authentication capabilities and are virtually impossible to deceive.
- **Smart Card** — A device that includes an embedded integrated circuit chip (ICC) that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. A smart card can combine several ID technologies, including the embedded chip, visual security markings, magnetic strip, barcode and/or optical stripe. Smart cards can be used for physical access, logic access (such as computer log-on) and digital signature such as signing out materials or equipment. The advantage of smart cards is that they can store large amounts of updatable data, carry out on-card functions such as encryption and mutual authentication, and support traditional legacy systems. This eliminates the need for separate ID cards.<sup>ii</sup>



- Card Readers — Handheld and stationary systems are software-enabled hardware designed to identify individuals using common credentials, such as magnetic strip cards. The systems are linked (wired or wireless) to one or more databases of target information. These units are comparatively inexpensive, offering basic ID and security capabilities.
- Multi-Technology Readers — Comprising firmware and hardware, handheld and stationary systems identify individuals using common credentials, smart cards, biometrics or any combination thereof. The units may include photo display, cameras (for face-recognition use), iris recognition, data capture, and other input and display options. These systems offer detailed levels of cross-referenced ID and target information for mission-critical situations. The systems are linked (wired or wireless) to one or more databases of target information.

Enforcement goals are not simply designed for the moment, but are looking forward years into the future.

### A Path Forward

The transition to PIV and TWIC credentials presents some of the greatest challenges in security today because enforcement goals are not simply designed for the moment, but are looking forward years into the future. This is a remarkable shift in thinking that is directly enabled by the quantum leaps in technology.

Moving from PACS to new technologies is a daunting test. Most legacy access control systems are unable to read the data fields (target information and biometrics) that differentiate PIV and TWIC credentials from their predecessors. With the deadline for compliance looming, many companies and security directors are struggling to identify cost-effective ways to replace current PACS infrastructures.

Compliance, however, need not be an all-or-nothing proposition. Operators and government entities can integrate existing PAC systems to create a working infrastructure that will be fully compliant. New technologies will allow PIV and TWIC credentials to work with current PACS databases.

Many integrators — those who customize systems software and hardware for customers — agree that journaling to legacy systems would allow ports to get compliant in a relatively quick and comparatively cost-effective way. Operators and agencies would be well prepared to meet future rule changes, should they occur.

Doing so also yields several other benefits to those affected by these regulations:

- It allows time for gradual hiring (if needed) and training of staff.
- It allows for graduated security layering that integrates new and existing technologies to create low/moderate/high security zones around ports and government facilities.
- It allows for an orderly transition that would, in most cases, allow ports and government entities to continue operations with little disruption.
- It allows organizations to budget appropriately for future upgrades.

### Solution Tools



Any tool used for future systems must meet FIPS 201's "Personal Identity Verification of Federal Employees and Contractors" issued by the National Institute of Standards and Technology.

FIPS 201-compliant handheld authentication devices are a solution for perimeter control, movable checkpoints, on-vessel verifications and spot checks, and they can obviate the need for any stationary readers. These devices work with PIV and TWIC cards, as well as next generation CAC, FRAC and legacy government smart cards. These devices can provide strong authentication using multiple factors found on FIPS 201-1 credentials. The devices are scalable, allowing for the use of a single credential. They do not require secure connections and can operate with existing wide- or local-area networks for synchronization.

Entities can integrate existing PAC systems to create a working infrastructure that will be fully FIPS-201 compliant.

The most complete commercially available solution incorporates all of these features with full biometric capabilities. Using specialized software in combination with a biometric reader, the devices provide strong three-factor authentication by managing the acquisition of cardholder data from a smart card and performing on-card biometric matching. Digital certificates can be verified by using the issuer's validation authority, local Windows® certificate store, OCSP responder or repeater. Additional certificate path validation and CRL validation can be configured using Windows CAPI on Windows XP SP3 or Vista platforms.

Once verified, data from the credential is uploaded via the software into an encrypted certificate database. The software also fully or partially populates credential data into the PACS' appropriate fields. In some cases, a new cardholder may be added to the PACS. In other cases, the cardholder's existing access card record is updated to include their PIV/TWIC card's FASC-N and expiration date.

Because the software ties the credential to legacy cards, the PACS is assured that the cardholder has been vetted through the PIV or TWIC process and has been identified. In turn, this provides a foundation within an enterprise's security for determining at which facilities, checkpoints and gates the security level warrants one-to-one ID verification for entry. It is also important to note that for facilities that do not require 1-to-1 verification, existing access cards will continue to allow entry into secure areas with this process.

In addition, this type of compliance solution can be modified to provide a credential management module to manage credential validity. Through a PC-based interface, the middleware can verify digital certificates against an OCSP responder, validation authority or various black lists such as the TSA hot list. This additional yet essential security step allows re-validation of imported certificates on a periodic basis and suspension of a card or PACS badge in real time if it is associated with a revoked credential or certificate. By doing so, the security system fully supports PIV and HSPD-12 compliance requirements.

This new process will provide agencies with an easier and more cost-effective PIV implementation. It reduces the vast cost anticipated for the project by only requiring the change-out of card readers in facility areas requiring one-to-one verification. It is a proven method for quickly achieving the security benefits of PIV and/or TWIC while using the enterprise's existing PACS infrastructure.



## Summary

The two most significant initiatives toward improved domestic security, PIV cards for government personnel and TWIC credentials for transportation workers, rely on advanced technologies that are fundamentally different from existing security standards based on physical access control. This technology gap creates massive logistical and financial challenges for government entities and port operators charged with HSPD-12 compliance.

Creating transitional strategies using handheld biometric card readers and the newest software allows these agencies to get in compliance without gutting their current security infrastructure. By leveraging their existing PACS investments, entities can establish a compliant, layered security strategy that will allow them to build toward higher benchmarks while budgeting for change.

---

<sup>i</sup> White House, August 27, 2002, copy online at [www.whitehouse.gov/news/releases/2004/08/20040827-8.html](http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html)

<sup>ii</sup> Smart Card Alliance, Smart Card Primer, [www.smartcardalliance.org/pages/smart-cards-intro-primer](http://www.smartcardalliance.org/pages/smart-cards-intro-primer)

## Resources

Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials, Publication Number: PAC-07002, Smart Card Alliance Physical Access Council, September 2007.

Transportation Worker Identification Credential: Guidance for TWIC Reader Pilot Program, U.S. Dept. of Homeland Security, Nov. 19, 2007

Homeland Security Failures: TWIC Examined, RDML Brian Salerno, USCG, statement before the U.S. House of Representatives Committee on Homeland Security, Oct. 31, 2007.

Dept. of Homeland Security, TWIC Reader Hardware And Card Application Specification, March 28, 2008

Personal interview, Roger Roehr, Manager, Government Vertical for Tyco International, May 2008

###

For more information on integrating PIV and TWIC in existing access control systems, contact:

### Datastrip

1285 Drummers Lane, Suite 105  
Wayne, PA 19087  
800-548-2517