Considering
PIV or PIV-I
for Identification or Access Control?

What You Need to Know

Foreword

Government identity cards didn't just begin with Homeland Security Presidential Directive - 12 (HSPD-12) issued by President George W Bush on August 27, 2004. The genesis goes way back and it is instructive in understanding where it may go in the future.

It really began with eGovernment initiatives such as the Privacy Act of 1974 which led to defining Personal Identifiable Information (those things that generally don't change for life, like a Social Security number, a name, or a photo). The Privacy Act was followed by the Paperwork Reduction Act of 1980.

The E-Government Act of 2002 is a United States Statute for electronic government services. It established a Federal Chief Information Officer (CIO) within the Office of Management and Budget (OMB) to administer eGovernment activities and lead a CIO Council. Note that OMB is the largest component of the executive office of the president and is used to implement his vision across the executive branch. This statute also introduced the Federal Information Security Management Act (FISMA) which led to Physical Access Control Systems (PACS) being declared a part of the IT (Information Technology) infrastructure. The E-Government Act called for standards for interconnectivity and interoperability and established broad oversight over other agencies in achieving its goals.

HSPD-12 mandated an electronic credential for people to interact securely in this new eGovernment infrastructure. Indeed, the Personal Identity Verification (PIV) credential might well be the most critical element to achieving eGovernment.

> **Key Takeaway:** Congress and the president have a long history of producing laws and policies that influence how technology will address identity and access control.

HSPD-12

To summarize, Homeland Security Presidential Directive 12: Policy for a common identification standard for federal employees and contractors states:

> There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is 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). This directive mandates a federal standard for secure and reliable forms of identification.

Karen S. Evans served as administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget, the de facto Chief Information Officer for the United States until the office was created by Barack Obama. She testified before Congress that HSPD-12 was not so much about national security as it was about furtherance of eGovernment and that her office had written HSPD-12 for the president.

Before HSPD-12, there had been prior initiatives for secure identification. The Department of Defense with their Common Access Card (CAC), the Department of State, and the Transportation Security Administration with their Transportation Worker Identification Card (TWIC) had used smart card based badges. However, HSPD-12 mandated a new type of smart card badge that would be interoperable government-wide. And, it was to be used not only for identification purposes, but eventually also for access to both federal computer systems (logical access control) and federal facilities (physical access control).

After HSPD-12 was published, the initial focus was on developing the specifications for the PIV card, the infrastructure to support it, and getting it issued. It was not until about a half decade later that attention really turned to how to use the PIV with a PACS (Physical Access Control System) or a LACS (Logical Access Control System). So, it was nearly a decade before the attention focused on actually using the enhanced security features of the PIV card.

Key Takeaway: The real drive behind PIV was electronic government services, rather than terrorism protection, and to that end, it was necessary to mandate that all agencies begin to issue a new card that all could share. Early efforts were focused on broad issuance rather than broad in-depth usage.

Policy, Standards, and Guidance

HSPD-12 is "policy" in the form of a presidential directive (executive order). Another form of policy is a memorandum issued from the Office of Management and Budget with an alphanumeric title indicating the issuer, whether it is a memorandum, year of issuance, and a sequential reference number, such as OMB M-05-24. Standards and special publications are often issued by the National Institute of Standards and Technology (NIST), to provide details on how to implement the policies from the executive office. Relevant examples are the Federal Information Processing Standard FIPS 201 and Special Publication SP800-73. The CIO Council also publishes guidance documents such as FICAM which subsequently was made mandatory via an OMB memorandum. Important policy, standards, and guidance for PIV are discussed below.

OMB-04-04

Nine months prior to the issuance of HSPD-12, in December of 2003, another eGovernment policy was issued: OMB -04-04 E-Authentication Guidance for Federal Agencies. This policy recognized that online government services needed to be secure and private, and to achieve this, some type of identity verification or authentication is needed.

OMB-04-04 establishes the concept of 4 levels of identity assurance, which is foundational to PIV.

However, the focus is on Federal IT systems, and not PACS. This has led to PACS deployment challenges as PACS best practices were not integral to early thinking.

> **Key Takeaway:** Foundational Policy for PIV was based on meeting goals for remote logical access, not physical access.

NIST SP 800-63

A companion to OMB-04-04, SP 800-64 Electronic Authentication Guideline provides for the technical requirements for the levels of authentication defined in OMB 04-04. It covers conventional, secret token based remote authentication, only. And as such does not cover knowledge-based authentication or biometrics (since biometrics is not a secret). Though later versions of SP 800-63 provides some acknowledgement of the value of biometrics, and biometrics is used in registration and to unlock keys for PIV, biometrics has not gotten much utilization within PIV due to the technical specifications being heavily produced by cryptographers. SP 800-63 was originally published in June 2004, and most recently as SP 800-63-2 August 26, 2013.

> **Key Takeaway:** Foundational technical rules for implementing smart card authentication has been based on cryptography, and excludes biometrics which have been a staple of physical access. Focus is on logical access with no apparent consideration of physical access.

FIPS 201

FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors was issued in February 2005, barely 6 months after HSPD-12, thanks to the groundwork laid for eGovernment. FIPS 201 provides some high level detail on the card contents, both "mandatory" and "optional." The unique identifier in the card was called the FASC-N or Federal Agency Smart Credential Number. This number could be read "in the clear" via either the contact or contactless interface on the card. But, for PACS, the more secure identifier that uses digital certificates and cryptography was made "optional." So, with the pressure of deadlines, most agencies implemented the approach most like the 125Khz proximity cards they were familiar with: the FASC-N over the contactless antenna in the card. Unfortunately, the FASC-N was longer than most PACS could handle. It was 200 bits and most PACS were optimized around 26 bits though some could do 37 bits, or a little more. These "short" bit streams were and are used heavily in PACS with a one way communication protocol called Wiegand. However, Wiegand protocol is not suitable for applications which require two way communications for challenge/response, and it is too slow for the large data blocks used with the PIV cryptography mechanisms.

HID Global and other manufacturers responded with readers that could pre-process the FASC-N to extract non-essential bits, and truncate to get the FASC-N down to a size that the PACS could process. The FASC-N and the card's expiration date are stored in a container in the smart card called a CHUID (Card Holder Unique Identifier). Authentication with the CHUID is considered in FIPS 201 as "Some Confidence" - the lowest of three acceptable levels of assurance. With the deadlines, the reality of HSPD-12 being an "unfunded mandate" and the limitations of existing PACS infrastructures, agencies typically deployed the minimum. The early investments that deployed the minimum (CHUID) often stand in the way of moving forward to utilize the secure cryptographic aspects of the PIV card.

In order to migrate gracefully to the minimal FASC-N/CHUID, many agencies chose to issue a PIV card that contained both old and new technology. The Navy continued to use the magnetic stripe. HID Global offered a migration solution to other agencies for either their card or reader that included an extra computer chip and antenna that supported the old 125 KHz proximity technology in addition to the new 13.56Mhz high frequency smart card used in PIV cards. When both antenna exist in the card it is referred to as a tri-interface card.

FIPS 201 does introduce a very important set of tables in Chapter 6 that tie the E-Authentication Guidance of OMB's M-04-04 for Levels of Assurance separately to logical and physical access. Biometrics is acknowledged for both logical and physical access and is placed higher than CHUID methods. However, cryptographic methods are established as the highest confidence and the only acceptable method for remote logical access.

> **Key Takeaway:** FIPS 201 associates levels of assurance for three different methods of authentication for physical access and establishes cryptographic as the highest level and reading a number from the contactless antenna, in the traditional manner as the lowest level. This lowest level approach is the one typically implemented to date.

OMB M-05-24

OMB M-05-24 was sent to all heads of departments and agencies providing guidance on the implementation of HSPD-12 on August 5, 2005. Deadlines were included, which generally were missed. Some agencies have yet to comply.

OMB M-05-24 directed agencies to follow the FIPS 201 standard as well as a number of existing and forthcoming special publications that provided the technical detail not contained in FIPS 201.

OMB M-05-24 designated the General Services Administration (GSA) as the body responsible for making approved products available for purchase by government agencies. Part of this responsibility laid the groundwork for creating an Approved Products List (APL) for products and services, and the requisite testing required for inclusion on the list. GSA also was to provide contracting vehicles under Federal Supply Schedules 70 for Information Technology, as part of the Multiple Award Schedule Program, with no mention of the existing Schedule 84 uses for physical access control systems.

> **Key Takeaway:** GSA was assigned responsibility for standing up both a testing/certification program for products and services (including card issuance and PKI infrastructures) and a procurement vehicle. The procurement vehicle established was the one used for IT rather than physical security.

FICAM

The Federal CIO Council's architecture roadmap called Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM) first Published Part A November 10, 2009, and added Part B December 2, 2011. As the name implies, it is a roadmap though it is also a framework. It increases the emphasis on cybersecurity across the federal enterprise. Both logical and physical access are approached in a common IT-centric, Public Key Infrastructure (PKI) oriented manner. There is no mention of the prevalent CHUID reader authentication, and it is clear that the bar is now set on use of PKI cryptographic

technologies for all authentication.

FICAM introduces a systems level approach to meeting HSPD-12 and eGovernment rather than a component level view that was implicit in the early GSA Approved Products List. Though interoperability was always a stated goal, the GSA Evaluation Program's testing methodology was initially based on a "traceability matrix" that ensured compliance to HSPD-12, standard by standard, special publication by special publication. Due to strong proprietary aspects in PACS manufacturer's systems, this component listing approach resulted in systems that didn't work. FICAM provided a vision for systems level solutions and set a new framework for revising the GSA Approved Products List.

> **Key Takeaway:** FICAM (also called ICAM) formally acknowledges physical access and some of its nuances, while making it fit into a logical access view of the world. CHUID authentication is not even mentioned and PKI is firmly established as the baseline. A systems level approach is introduced which leads beyond authentication and begins to address authorization as well.

OMB-11-11

For a number of years after HSPD-12 and FIPS 201 were published there had not been the desired progress in broad agency use of the PIV card with its cryptographically secure capabilities. On February 3, 2011 OMB-11-11 provided increased emphasis in a memorandum entitled: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors. It mandated to use the capabilities of the PIV card for multi-factor authentication, digital signature, and encryption. Cybersecurity is cited as an additional rational for implementing the more than minimum PIV capabilities. There needed to be a transition to use of the cryptographic and Public Key Infrastructure (PKI) capabilities of the card. There is budget language that this is not another "unfunded mandate."

OMB-11-11 embraced the Federal CIO Council's FICAM roadmap and referenced the new website http://www.idmanagement.gov. OMB-11-11 also references NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems. SP 800-116 had little to no input from the physical security industry and has become quite dated relative to the refreshes of the other FIPS 201 family of documents (It is still heavily based on the FASC-N/CHUID). NIST states that current funding, priorities, and resources indicate it will be some time before SP800-116 will be refreshed.

> **Key Takeaway:** OMB M-11-11 made FICAM mandatory and begin establishing Cybersecurity as a strong objective, subtly moving further from CHUID to PKI existing budget dollars were threatened if not implemented as a stronger incentive than an unfunded mandate. What started out as a contentious "informative guidance" for PACS with SP800-116 was given a questionable normative posture.

FIPS 201-2

FIPS are not supposed to be updated more often than every 5 years. So when FIPS 201-2 was issued in September 5, 2013, it was a major refresh of the first version published February 25, 2005. Though now published, it is not yet fully usable, as many of the changes and new features are dependent on the special publications from NIST to be updated and/

or published. Some of the new features of FIPS 201-2 awaiting a supporting special publication include:

On Card Comparison for biometrics

- Biometric Iris Template
- Virtual Contact Interface

Also, some of the previously "optional" aspects of FIPS 201 are now "mandatory" in the PIV card per FIPS 201-2. This includes:

- Facial Image
- Asymmetric keys; Card Authentication Key (CAK) - critical for PACS to use PKI
- Digital Signature Key
- Key Management Key

A major change was the downgrade (deprecation) of the Visual and CHUID authentication mechanisms to little or no confidence as an assurance level. As a result, the Approved Product List category for CHUID readers is discontinued. Since CHUID was the large catchall category for many varied readers to use, just to get on the APL, this has great impact. Approximately 200 readers were in this category, including most biometric readers. The Card Authentication Key, now referred to as PKI-CAK is also now the some confidence assurance factor to use in place of visual or CHUID. The new APL, called the FICAM APL, or APL 2.0, is now testing these readers.

FIPS 201-2 now effectively requires "PKI at the Door" for all card reads. Even biometric authentication now requires the cryptographic signature on the biometric template to be verified. Even before FIPS 201-2 HID Global offered solutions for "PKI at the Door" with pivCheck and pivCLASS Authentication Modules to support migration for many installed and planned PACS sites.

The card lifecycle is changed from 5 years to 6 years to better align with the 3-year certificate lifecycle, though this still requires a certificate refresh on any existing PIV card. Note that FIPS 201-2 now allows an extra year for issuers to begin issuing in accordance with FIPS 201-2. Since cards need not be replaced when FIPS 201-2 is issued, but at the end of their 5 year life, and considering the grace period, it might be 6 years before the newly mandatory features can be counted on to be present when a card is presented to a reader or a PACS.

The unique number used for identification of the person is clarified to now be a 128 bit UUID or Universal Unique Identifier, following international standards to achieve uniqueness. The UUID resides in the CHUID, and all certificates, and will likely eventually displace the FASC-N. Most manufacturers of logical and physical access control systems have had enough time to evolve their systems to support a 128 bit string in their latest offerings. Note, NIST requirements for other non-PACS aspects of the PIV card when using cryptography will still cause a card read to take between 2.5 and 4 seconds, maybe more. Since PKI is now the baseline for PIV, card reads will take longer in FIPS 201-2 compliant implementations.

FIPS 201-2 opens the door to use of a PIV card in mobile applications (e.g. smart phones). One approach is to derive secure credentials from the PIV credentials and allow them to exist in a smart phone for applications in the future (except physical access). That way the smart phone can be used as a digital credential (note that the visual "badge" authentication is now deprecated). However, FIPS 201-2 does not provide sufficient technical detail on how to

achieve derived credential. That information will be found in a forthcoming Special Publication SP 800-157.

> **Key Takeaway:** The CHUID read mechanism, widely deployed in PACS is deprecated which leads to elimination of the most popular product category in the APL. PKI-CAK is the new "minimum" mechanism. Even the biometric mechanism now has to use PKI. The FASC-N has given way to the 128 bit UUID for the primary identifier in the card and needs to be read in its entirety by the PACS without truncation. Card reads will take longer. Support for the contactless PKI-CAK opens up use of the mobile smart phone in "card emulation" mode when a derived credential is implemented SPs are forthcoming for the new capabilities.

PIV in EPACS

The CIO Council published another guidance document March 26, 2014 under the ICAM logo called Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (EPACS). This document is current and has implemented many best practices of the physical security industry while moving towards IT architectures in accordance with the FICAM roadmap. PIV in EPACS provides guidance for use of the higher security capabilities of the PIV card in lieu of the FASC-N/CHUID.

> **Key Takeaway:** This is a comprehensive and more current guide for PACS than SP800-116 (which has not kept up with the changes of FIPS 201-2, such as deprecation of the CHUID).

PKI in a Nutshell

Public Key Infrastructure (PKI) provides an enterprise-wide back end infrastructure that operates over a public or private cloud or the internet to allow a PACS to check with a third party to validate the presented credentials.

Use of Personal Identification Numbers (PIN) and biometrics with PKI can offer additional factors of authentication to bind the card to the cardholder. Prior to PIV, physical access control systems did not authenticate the card holder; these systems only checked if the "card ID" was in the system and if that card ID was "authorized" for access at the door to which the card is being presented. For proper security, both authentication (authN) and authorization (authZ) must be done. This level of security, delivered via PIV, is the key feature of "PKI at the Door."

> **Key Takeaway:** PKI and "PKI at the Door" is the cryptographic method used with PIV.

FICAM – A Major Change of Focus

PHASE 1 - PIV	PHASE 2 - FICAM
Issue Cards	**Use Card**
Critical Mass of Cards	Critical Mass of Systems
Early Adopter Use	**Use as Intended**
Signed CHUID (with no requirement to check the signature) No Better than Prox	Crypto for PKI Trust
Replace Readers	**Replace Systems**
Read FASC-N	Process Certificates
GSA APL	**FICAM APL**
Test Components	Test Systems Security & Interoperability

Beyond PIV

Though PIV was developed for Federal government employees and contractors, it is clear that the technology and methodology is also

appropriate for non-government organizations doing business with the government. Accordingly, the Commercial Identity Verification (CIV) credential, as defined by the Smart Card Alliance Physical Access Council, formally established the availability of a PIV-level credential for private sector, commercial enterprise use. CIV credentials are ideal for use by governments around the world or private organizations that require highly secure access control for sensitive areas, including power stations as well as data storage, nuclear, water and petrochemical facilities and other critical infrastructures. The Smart Card Alliance authored a white paper which outlined the use of CIV (Commercial Identity Verification).

PIV-I and CIV provide PACS manufacturers with scale for their offerings that can possibly lower cost, while increasing security overall in cybersecurity threat management. It is expected that products that appear on the GSA APL that meet stringent tests for PIV will also be usable in PIV-I and CIV implementations.

The Security Industry Association has developed a specification (contributed in part by HID Global) for a communication protocol between the controller and various peripheral devices such as readers or other system components. Called OSDP, or Open Supervised Device Protocol, the specification provides a messaging protocol for two way communication to replace Wiegand. Protocol 1 is for FICAM applications. The protocol has been developed by industry with the intent of becoming a national standard. As NIST typically embraces standards from the American National Standards Institute and industry, OSDP might well become part of the solution to moving from component testing to systems testing for the GSA Evaluation Program and APL.

Key Takeaways: An end user can benefit from the PIV technology and best practices without having to follow all the government requirements. Similarly, the government can use the same readers to grant visitors some access privileges in a federal environment without a full PIV issuance (for example, audit trail of an escorted visitor in a facility). Industry is developing other standards in support of PIV technologies which can leverage commercial offerings and better address cybersecurity threats.

APL 2.0 (or FICAM APL)

The U.S. Government website for all things identity has undergone a major overhaul over the past year, and that includes information on the evaluation program for the Approved Product List. The main website is http://www.idmanagement.gov and the evaluation program can be found at http://www.idmanagement.gov/ficam-testing-program.

One of the major changes in moving to APL 2.0 is a culture change whereby government is now welcoming industry input and involvement in developing the test processes and standards for the new array of categories. The vehicle for obtaining this input is the Evaluation Program Technical Working Group. GSA not only obtains input but also regularly provides updates to industry on current issues and developments to eliminate surprises and enhance long term planning for all parties.

Currently, as in the beginning of the APL, laboratory testing is free. This is because many of the older categories are being revised or significantly changed to accommodate the latest policies and standards under the FICAM framework. As sufficient products and services are approved for these new

categories, traditional lab testing fees are expected to return.

The APL 2.0 is now "system" focused rather than "component" focused – specifically to address interoperability. Systems can now be submitted, tested, and listed as such. In response to industry input, GSA now accepts that there is more than one system component arrangement, or topology, to achieve the end-to-end objectives of FICAM. For instance, there is a topology for a controller "add on" board that handles much of the cryptographic and PKI processing for PIV authentication (such as HID Global's pivCLASS Authentication Module (PAM), and another topology where the manufacturer has integrated the cryptographic and PKI authentication into their latest controllers. This allows the agency to select the solution that best fits their site's unique requirement for retrofit, upgrade or new deployments.

Many of the past interoperability issues arose due to lack of knowledge by those procuring, designing and installing PIV into PACS. There is now a new GSA training program with certification for a "Certified System Engineer ICAM PACS." This program addresses PKI 101, biometrics, credentials, and trusted EPACS, and is offered as classroom, hands-on training by the Smart Card Alliance.

New Generation 2 test cards are now available. Not only do they offer the best current array of both positive and negative tests, but more importantly they are based on the cards actually deployed by all agencies in the field. GSA obtained these samples to ensure that all the nuances of real "as issued" cards are addressed.

Products that no longer are approved, for whatever reason (e.g., the category was deprecated) are now being transferred to a Removed Products List. Tri-interface cards will likely end up here as they undergo a deprecation schedule.

> **Key Takeaways:** Many products previously listed on the original APL will have to be retested and certified under the new APL. However, the program is greatly enhanced for practical systems level testing and test cards are now available.

Conclusion

With a plethora of ever-changing and interrelated policies, standards, special publications, and test procedures, it is important to understand the political and technical evolution to participate in HSPD-12 solutions. The latest technologies are not only critical for Homeland Security, and eGov, but also the new threats of cybersecurity in both the public and private sectors. HID Global has provided solutions for migration from the beginning, and with the evolving requirements will be there with migration solutions in the future. ■

Contact: 800.237.7769
insidesales@hidglobal.com