Executive Overview

U.S. government agencies are faced with the difficult challenge of complying with evolving standards for secure and reliable forms of identification used by federal employees and contractors. These standards were initiated in August 2004 when President Bush ordered the Homeland Security Presidential Directive-12 (HSPD-12). According to a February 2011 memorandum issued by the U.S. Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), existing physical (PACS) and logical (LACS) access control systems must be upgraded to use Personal Identification Verification (PIV) credentials in accordance with National Institute of Standards and Technology (NIST) guidelines. Federal agencies have been instructed to transition to using the PIV credential for PACS and LACS before they use development and technology refresh funds to complete other activities. These systems must leverage smartcard and biometric technology, and support identification credentials according to government guidelines.

HID Global’s pivCLASS® Solution Suite enables agencies to cut the cost and complexity of Federal Information Processing Standards Publication 201-2 (FIPS 201-2) compliance using a modular hardware and software approach, and the industry’s only turnkey offering from a single supplier. HID’s pivCLASS solutions combine the company’s strengths in access control solutions and technology migration, the enhanced cryptographic security of its next-generation reader platform, the CodeBench authentication middle-ware software acquired in 2013, and the extensive identity-assurance portfolio offered by ActivIdentity, an HID Global company that enables customers to confidently establish trust in on-line activities. Customers will be able to deploy HID Global’s pivCLASS validation and authentication software and readers, and achieve full FIPS 201-2 compliance without having to replace their current physical access control head-end server, panel or door control hardware.

This paper will describe HID Global’s compliance strategy, which is unique in providing a fully interoperable, simple-to-deploy, cost-effective and turnkey solution that has been tested and validated under the company’s Genuine HID umbrella. The pivCLASS Solution Suite gives agencies a single point of deployment responsibility for FIPS 201-2 compliance, ensuring they can achieve compliance quickly, effectively and with all necessary audit support, on an incremental, pay-as-you-go basis, while preserving investments in their existing infrastructure.

Compliance Requirements and Deadlines

HSPD-12 is intended to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. It requires agencies to follow specific technical standards and business processes for the issuance and routine use of secure and reliable forms of identification, in compliance with FIPS 201-2. The FIPS 201-2 document, entitled “Personal Identity Verification (PIV) of Federal Employees and Contractors,” defines the multi-factor authentication, digital signature and encryption capabilities required for standardized PIV smartcard credentials that will be used by federal employees and contractors in order to gain access to all government facilities and disaster response sites.
FIPS 201-2 compliance is intended to create a standardized infrastructure of interoperable access control products across a wide range of facilities belonging to disparate agencies and partners. This will lead to reduced overall costs while improving the federal government’s ability to leverage its formidable buying power. All new systems under development will need to support PIV credentials and physical building access changes according to NIST guidelines.

Federal Identity, Credential and Access Management (FICAM)

The U.S. Federal Government has adopted a comprehensive, holistic approach to standardize the Federal Identity, Credential and Access Management (FICAM) activities. The government’s Chief Information Officers (CIO) council adopted FICAM to improve practices in the design, modernization, use, sharing and performance of federal resources and information. FICAM activities promote PIV use for strong authentication when accessing federally-controlled facilities and federal information systems. Furthermore, they maintain the ICAM architecture and support government-wide implementation and performance. The U.S. Government’s emphasis on strong authentication for physical and logical access is requiring agencies to upgrade their ICAM technologies to support new functionality and needs.

Supporting FICAM initiatives is the General Services Administration (GSA) who has implemented new certification testing to meet the goals of the ICAM architecture. The GSA Approved Product List (APL) has been modified to reflect this testing by adding four primary solution segments.

- Physical Access Control Systems (PACS)
- Logical Access Control Systems (LACS)
- Credentialing Systems
- Usage

FICAM testing elements and how they are organized are subject to evolve over time and change the testing program and associated GSA Approved Product List.

FIPS 201-2

HSPD-12 directed the Department of Commerce to develop a Federal Information Processing Standards publication to define a common identification credential. In accordance with HSPD-12, this standard defines the technical requirements for the identity credential. The initial standards document, FIPS 201-1, was updated in 2013 to address security and credential design issues not addressed in the first document. FIPS 201-2 will impact a federal agency’s deployment of the PIV card into existing or new PACS. For instance, since signature verification and certificate path validation is required in CHUID and BIO authentication modes, transparent readers are not compliant with FIPS 201-2 and have been deprecated on the GSA’s Approved Product List.

Furthermore, FIPS 201-2 removes the CHUID authentication mode altogether. A new concept within FIPS 201-2 is a virtual contact interface that creates a secured contactless interface enabling all authentication modes over a contactless interface. The FICAM certification testing reflects the new 201-2 standard.
One of the more important documents issued by the government is the National Institute of Standards and Technology’s (NIST) Special Publication 800-116 (SP 800-116), which discusses the different PIV card capabilities so that risk-based assessment can be aligned with the appropriate PIV authentication mechanism. The SP 800-116 document introduces the concept of “Controlled, Limited, and Exclusion” areas, which require agencies to employ risk-based PIV authentication mechanisms for different areas within a facility. The document also proposes a PIV Implementation Maturity Model (PIMM) to measure the progress of facility and agency implementations. Finally, it recommends to federal agencies an overall strategy for the implementation of PIV authentication mechanisms within an agency’s PACS (see Fig. 1).

Fig. 1: NIST SP 800-116 PIV Authentication Mechanism Use Cases

In this diagram, the Unrestricted area is considered public with no restrictions as to who has access. Access to the Controlled area is restricted to those who can prove affiliation. For example, possession of an agency’s badge could be sufficient to gain access at an outer perimeter of a facility. Access to the Limited area is restricted to members of a group who are fulfilling a specific role. Finally, access to the Exclusion area is restricted by individual authorization, analogous to the “need-to-know” requirement in the classified world.

**HID’s pivCLASS Solutions**

HID Global’s pivCLASS Solution Suite solves the difficult problems that agencies have faced in trying to achieve FIPS 201-2 compliance. Until now, PIV implementation was not a turnkey process, and it was very expensive. HID Global remedies this situation by eliminating the need for agencies to acquire, organize, and deploy the expertise, and technologies from numerous suppliers that are necessary for achieving a working solution. The company’s pivCLASS Solution Suite also provides agencies with a clear migration path from existing credentials, and a strategy for protecting their current investments.

The HID pivCLASS Solution Suite of products offers the following benefits:

- Upgrades existing PACS to authenticate credentials at full range of assurance levels
- Upgrades existing PACS without the need for wholesale rip and replacement of existing equipment
• Helps to fulfill the promise of converged physical and logical security as envisioned by HSPD-12
• Is unique in delivering complete FIPS 201-2 and SP 800-116 compliance
• Addresses security, compliance and ROI objectives by enabling PIV, PIV-I, CIV and CAC card access

HID Global’s pivCLASS® Authentication software modules allow an agency to approach deploying a compliant PACS over time as their budget allows. The data from the PIV credential can be authenticated, harvested and registered into the PACS card holder database using HID’s pivCLASS® Registration Engine. This solves the initial challenge of collecting and registering credential data elements in the PACS head-end in preparation for implementing PKI at the door. The status of enrolled PIV cards is checked on a periodic basis with pivCLASS® Certification Manager which prohibits access by revoked cards. This is done by retrieving the card revocation status from the issuing certificate authority (OCSP/CRL/MiniCRL) and the TWIC Hotlist.

Once the PIV credential data is part of the access control head-end, agencies can add one, two or three factor pivCLASS readers to their system. HID’s pivCLASS readers can be programmed to provide no authentication at the door during the early stages of building out a fully compliant system. As the overall compliance roadmap begins to take shape, the pivCLASS readers can be reprogrammed to interface with the pivCLASS® Authentication Modules (PAM), which are installed between the pivCLASS reader and the existing PACS panel, to provide the various PIV authentication mechanism defined in SP 800-116. When a PIV, PIV-I, CIV or TWIC card with the appropriate assurance level is presented to a corresponding reader, the PAM validates the card according to the assurance level setting, extracts the badge ID from card data and then passes the badge ID to the PACS panel for an access decision and logging. PAMs maintain an updated validation and data cache (e.g., issue trust status, revocation status) so it can function “offline” and continue to provide strong authentication at the door.
The pivCLASS® Validation Workstation can validate PIV cards from visitors by using the Server-based Certificate Validation Protocol (SCVP) to implement the path discovery process and establish a chain of trust through the Federal Bridge.

HID Global supports third-party partners who offer comprehensive online PIV-I service that will reduce the time and complexity required for contractors to obtain employee credentials which comply with PIV-I requirements.

Summary
Federal agencies face a difficult challenge in upgrading their PACS infrastructure to meet the latest government mandates. Until now, they have had to work with multiple vendors and often faced the prospect of having to replace their entire system. The pivCLASS Solution Suite of Genuine HID software and hardware solutions gives agencies a single point of responsibility for achieving compliance, using fully tested and validated, modular hardware that preserves investments in their existing infrastructure, while providing the flexibility to incrementally improve capabilities and adapt to new requirements over time.