Personal Identity Verification (PIV) Enablement Solutions

pivCLASS®
Government Solutions

Affordable Personal Identity Verification (PIV) Enablement Solutions from a Single, Trusted Supplier

Complete Solution for PIV Enablement

HID Global's pivCLASS® Government Solutions portfolio is an extensive product family that makes it easy for U.S. Federal Government, government contractors and other facilities to comply with security regulations and to use their Personal Identity Verification (PIV) and other smart cards for physical access control, resulting in compliance, interoperability and high security.

FIPS 201 Compliance Without The Need to "Rip and Replace"

The pivCLASS modular approach provides government agencies the ability to use their PIV identity cards for strong public key infrastructure (PKI)-based validation for physical access control. The solution enables this functionality without the need to "rip and replace" existing physical access control systems (PACS), reducing costs, and removing complexities to make it easy and affordable to acquire, install and maintain compliant physical access control systems.

pivCLASS accomplishes this in part by communicating with an agency's PACS and external trust authority PKIs to deliver functionality specified by National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 201 (FIPS 201).

An Integrated Solution from a Single Provider

Delivering fully tested and validated turnkey government solutions from a single, trusted source, pivCLASS authenticates PIV credentials across the full range of assurance levels as defined by the federal government's Special Publication 800-116 (SP 800-116). pivCLASS products also support the Transportation Worker Identification Credential (TWIC) Reader Specification.

The pivCLASS portfolio includes pivCLASS Registration Engine, pivCLASS Certificate Manager, pivCLASS Reader Services, pivCLASS Authentication Module (PAM) and a complete line of pivCLASS readers, enabling agencies to quickly and easily acquire all of the necessary components for their PIV-enabled access control systems.

Achieving Compliance Made Simple

How it Works

Working together to deliver strong authentication at the door and during the initial cardholder registration, the pivCLASS solution ensures the card is the originally registered card and the cardholder is the person he/she claims to be. It also verifies the card has not been forged, altered, cloned, lost, stolen, shared, revoked or expired. pivCLASS accomplishes this by performing the following functions:

- Automatically registers cards into the PACS database with no manual data entry.
- Executes full path discovery and certificate revocation checking using CRL, OCSP or SCVP.
- Periodically retrieves card revocation status from issuing certificate authorities.
- Caches validation data and offers degraded mode settings to allow continued validation when access to card issuer validation data (e.g., CRL) is unavailable.
- Validates cardholder credentials both during a card's registration into local access control software and at the door.
- Validates visiting cardholder credentials from other agencies (i.e., provides certificate path discovery and validation essential for interoperability across government agencies and any other entities cross-certified with the Federal Bridge).
- Provides centralized configuration and management of pivCLASS products via a graphical user interface.
- Allows configuration of trusted card issuers, authentication modes, Wiegand output format and more.
- Provides centralized distribution of firmware updates to pivCLASS Authentication Modules.
- Collects detailed log activity for display and export.

PIV-Enablement for Existing PACS

The pivCLASS modular approach allows agencies to deploy different pivCLASS components over time as their budget allows and as they work toward achieving compliance. The pivCLASS off-the-shelf software is integrated with more than 30 physical access control systems and does not require any software development.

pivCLASS Readers Meet Any Authentication Mode and Any Assurance Level

"Controlled" Areas

"Limited" Areas

"Exclusion" Areas

pivCLASS® Readers

The pivCLASS Government Solution suite includes a broad selection of readers for agencies to meet any security level and the NIST SP 800-116 guidelines. pivCLASS readers work with the pivCLASS Authentication Module™ to meet requirements for:

- Any assurance level: controlled, limited or exclusion.
- Any authentication mode: CHUID, CAK, PIV + PIN, or PIV + PIN + BIO; also, FASC-N reads for non-SP800-116 "uncontrolled" areas, and the additional TWIC authentication modes, CHUID + BIO and CAK + BIO.
- Nearly any card type, contact or contactless, including PIV, PIV-I, CIV (a.k.a., PIV-C), TWIC, FRAC and CAC.

Additionally, pivCLASS readers provide fully functional backward compatibility with existing iCLASS® and HID Prox readers, easing the transition from legacy cards to PKI-based credentials. The readers also support bi-directional communication to the PAM.

Assurance Levels and Authentication Modes

Most Federal facilities have likely completed a risk assessment that designated each door and portal as requiring an uncontrolled, controlled, limited or exclusion assurance level. NIST SP 800-116 specifies which authentication modes are required for which assurance levels. For instance, a door leading to a high security area will require a more advanced reader (in order to perform additional identity checks, such as biometric fingerprint match) than a lower security door.

Figure 1 illustrates the different security levels and the attack vectors addressed by the pivCLASS solution.

Meet Any Assurance Level

			Secures against cards that are...				
Security Area (per NIST SP800-116 & Risk Assessment)	**Authentication Factors**	**Authentication Modes**	**Revoked**	**Counterfeit or Altered**	**Copied or Cloned**	**Lost or Stolen**	**Shared**
Uncontrolled	None	FASC-N	✓				
Controlled	1	CHUID + VIS	✓	✓			
Controlled	1	CAK	✓	✓	✓		
Limited	2	PIV + PIN	✓	✓	✓	✓	
Exclusion	3	PIV + PIN + BIO	✓	✓	✓	✓	✓

BIO: Biometric; CAK: Card Authentication Key; CHUID: Cardholder Unique Identifier; FASC-N: Federal Agency Smart Credential Number; PIN: Personal Identification Number; PIV: Personal Identity Verification (PIV) Authentication Key; VIS: Visual

Figure 1

pivCLASS Authentication Module Does the “Heavy Lifting” for PIV Validation

pivCLASS® Authentication Module

The pivCLASS Authentication Module (PAM) is an embedded computer packaged in a small form factor with pre-installed, updatable firmware. The PAM is installed between a supporting reader (such as a pivCLASS reader) and the existing access control panel, and provides configurable Wiegand output to the controller.

This enables the system to be upgraded to support PIV cards for access control; the access control panels do not have to be replaced or even reconfigured, and the head-end access control software does not need to be enhanced with new features. Similarly, much of your existing wiring may be reusable.

Readers pass card information to the PAM, which performs the required authentication to validate (or invalidate) the cardholder credential. If validated, the badge ID is then passed to the existing access control panel for the access authorization decision.

Since the PAM regularly receives and caches cardholder credential status from the pivCLASS Certificate Manager, the result is nearly real-time PKI-based high security at the door.

In its role, the PAM does the “heavy lifting” of cryptographic operations for PIV cardholder credential authentication each time a card is presented to a reader. Each PAM can process up to two readers at one or two doors.

Increased Overall System Security

The pivCLASS solution is architected for the security-conscious yet cost-sensitive security administrator. The pivCLASS Authentication Module typically sits inside the secure perimeter, where it – not the reader – performs the critical cryptographic functions. This architecture locates the PKI operations within the secure perimeter rather than in an expensive, PKI-capable reader placed on the insecure/attack side of the door.

pivCLASS Software Communicates with Trust Authorities

pivCLASS® Software Components:

- pivCLASS Registration Engine: reads, validates, authenticates and automatically registers valid credentials into PACS database without any manual data entry.
- pivCLASS Certificate Manager: periodically revalidates the status of digital certificates and updates the PACS with any change in status; can automatically suspend any card associated with a revoked certificate; can send an email to a distribution list for notification.
- pivCLASS Reader Services: configures and manages pivCLASS readers via the PAM.

pivCLASS Registration Engine and pivCLASS Certificate Manager

The pivCLASS Registration Engine is a software module that reads, validates, authenticates and registers credentials with a PACS automatically without manual data entry. The software validates multiple card types, including PIV, PIV-I, CIV (PIV-C), CAC NG, CAC EP, TWIC and FRAC.

The pivCLASS Certificate Manager is a software module that, after credential registration, regularly communicates with external trust authorities to check the status of cached certificates. Upon determining a status change, the software can suspend any card associated with a revoked certificate and/or send an email to a distribution list for notification. pivCLASS Certificate Manager also sends that information via Ethernet (AES256 encryption optional) to the pivCLASS Authentication Modules (PAMs) for enforcement.

pivCLASS Reader Services sends mode updates, TWIC Privacy Keys (TPKs), and other information to PAMs and supports multiple authentication modes including FASC-N, CHUID, CAK, PIV + PIN, CHUID + BIO, CAK + BIO, and PIV + PIN + BIO.

Typically, an agency will install the pivCLASS Registration Engine on each workstation where credential registration is to occur. pivCLASS Certificate Manager software is required for ongoing revalidation of certificates after registration and is usually placed on the PACS server, although alternative configurations can be implemented to meet specific needs.

The communication flow between pivCLASS elements and other parts of the architecture is detailed in Figure 2.

Genuine HID®

With Genuine HID, the U.S. Federal Government, government contractors and other facilities benefit from the broadest product line of trusted, fully interoperable secure identity solutions in the market. Genuine HID solutions are designed and built in ISO 9001 certified facilities; include worldwide agency certifications; and are backed by global product warranties. Supported by industry-leading expertise and the strongest delivery and response platform available, Genuine HID solutions reinforce the long-standing trust that when customers purchase from HID Global, they are investing with absolute confidence.

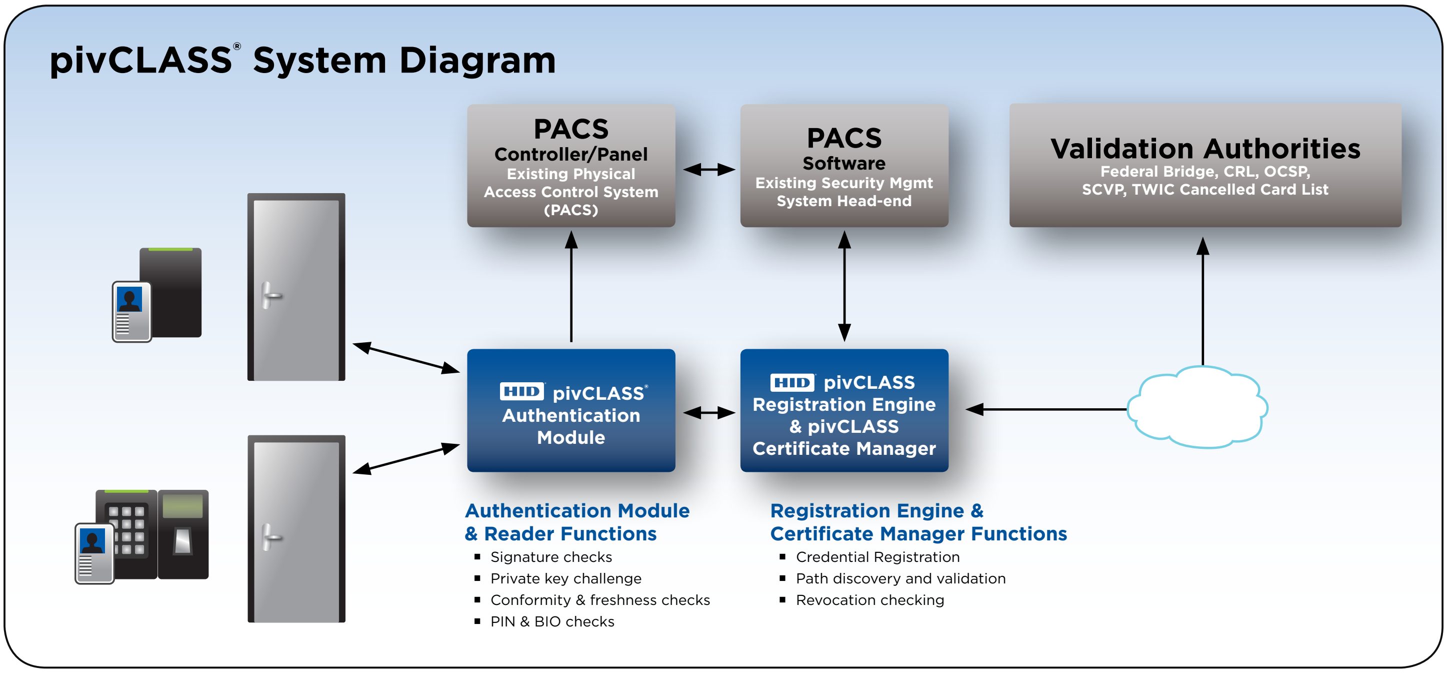
pivCLASS® System Diagram
PACS
Controller/Panel
Existing Physical Access Control System (PACS)
PACS
Software
Existing Security Mgmt System Head-end
Validation Authorities
Federal Bridge, CRL, OCSP, SCVP, TWIC Cancelled Card List
HID pivCLASS® Authentication Module
HID pivCLASS Registration Engine & pivCLASS Certificate Manager
Authentication Module & Reader Functions
Signature checks
Private key challenge
Conformity & freshness checks
PIN & BIO checks
Registration Engine & Certificate Manager Functions
Credential Registration
Path discovery and validation
Revocation checking

Figure 2

hidglobal.com

GENUINE™ HID SECURE IDENTITY

ASSA ABLOY

An ASSA ABLOY Group brand

© 2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, Genuine HID, iCLASS, pivCLASS and pivCLASS Authentication Module are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2013-06-12-pivclass-solutions-br-en

North America: +1 949 732 2000 • Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 • Latin America: +52 55 5081 1650

hidglobal.com