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

**Complete Solution for PIV Enablement**

HID Global’s pivCLASS® Solutions portfolio is an extensive product family that makes it easy for U.S. Federal Government, government contractors, ports, 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.
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

**pivCLASS Readers**

The pivCLASS 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™ or pivCLASS Embedded Authentication, 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 “unrestricted” 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 compatibility with existing Seos, iCLASS® and HID Prox readers, easing the transition transition to PKI-based credentials and supporting temporary or visitor use. The readers also support bi-directional communication to the PAM and panels running pivCLASS Embedded Authentication.

**Assurance Levels and Authentication Modes**

Most Federal facilities have likely completed a risk assessment that designated each door and portal as requiring an unrestricted, 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 per NIST SP 800-116-1 and the attack vectors addressed by the pivCLASS solution.

![Figure 1](image_url)

**Meet Any Assurance Level**

<table>
<thead>
<tr>
<th>Security Area (per NIST SP800-116 &amp; Risk Assessment)</th>
<th>Authentication Factors</th>
<th>Authentication Modes</th>
<th>Revoked</th>
<th>Counterfeit or Altered</th>
<th>Copied or Cloned</th>
<th>Lost or Stolen</th>
<th>Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrestricted</td>
<td>None</td>
<td>FASC-N</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unrestricted</td>
<td>1</td>
<td>CHUID + VIS</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled</td>
<td>1</td>
<td>CAK</td>
<td>✔ ✔ ✔</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Limited</td>
<td>2</td>
<td>PIV + PIN</td>
<td>✔ ✔ ✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Exclusion</td>
<td>3</td>
<td>PIV + PIN + BIO</td>
<td>✔ ✔ ✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

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
pivCLASS Authentication Module or pivCLASS Embedded Authentication Does

**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 Embedded Authentication

pivCLASS Embedded Authentication takes the functionality of the pivCLASS Authentication Module and embeds it into the physical access control panel for a more integrated approach when an existing system doesn’t need stay in place to be upgraded or the existing panel will support.
pivCLASS Software
Communicates with Trust Authorities

pivCLASS® Software Licensed Options:

- **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.

Typically, an agency will install the pivCLASS Registration Engine on each workstation where credential registration is to occur. The 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.

**Figure 2**

**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, SCV, TWIC Cancelled Card List
- **Module or pivCLASS Embedded Authentication**
- **PACS Controller/Panel**: Existing Physical Access Control System (PACS)
- **Validation Authorities**: Federal Bridge, CRL, OCSP, SCV, TWIC Cancelled Card List
- **Registration Engine & Certificate Manager Functions**: Credential Registration, Path discovery and validation, Revocation checking
- **Authentication Module & Reader Functions**: Signature checks, Private key challenge, Conformity & freshness checks, PIN & BIO checks