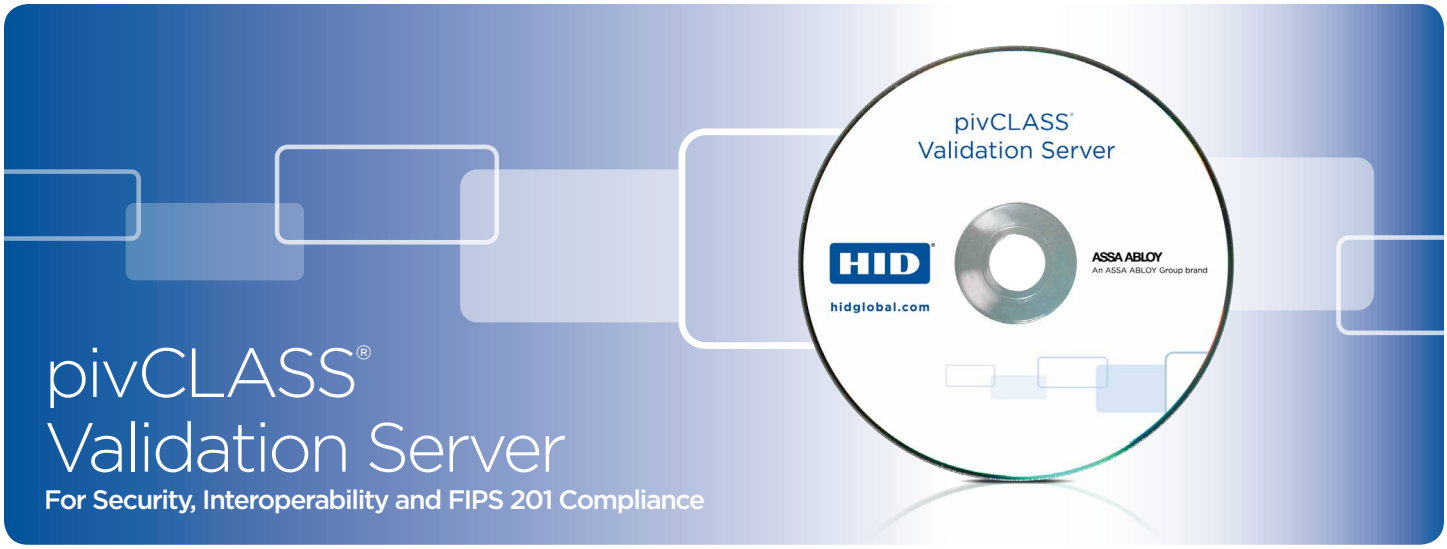
PHYSICAL ACCESS SOLUTIONS



pivCLASS® Validation Server

For Security, Interoperability and FIPS 201 Compliance

CENTRALIZED MANAGEMENT AND CONTROL OF pivCLASS SYSTEM COMPONENTS FOR FIPS 201 COMPLIANCE

- **Part of an integrated solution from a single, trusted provider** – Enables upgrade of existing physical access control system (PACS) to achieve FIPS 201 compliance. Follows NIST SP 800-116 guidelines and the TWIC Reader Specification.
- **Communicates with external trust authorities** – Regularly imports updated credential validation information and distributes credential status data to pivCLASS Authentication Modules (PAM) for enforcement.
- **Interoperable with Federal Bridge** – Provides complete PIV path discovery and validation for any credential supported by the U.S. Federal Bridge.
- **Configures pivCLASS system components** – Configures pivCLASS Authentication Modules to perform mandated authentication modes for every required security area assurance level.

The HID Global pivCLASS® Validation Server is a key component to the pivCLASS solution. The system is comprised of four major software components:

- **pivCLASS Validation Service** – configures network communication ports; establishes access rights to the database; generates and manages secure cryptographic keys; sets system event logging levels; and periodically generates and distributes updated validation status of all enrolled credentials to each PAM.
- **pivCLASS Management Station** - sets default PAM operating parameters, sets authentication mode for each door, and configures badge ID derivation rules and Wiegand formats.
- **Path Builder SerVE Client (PBSerVE)** - supports path discovery, path validation and revocation checking using either the OCSP or SCVP protocols. PBSerVE also supports the use of CRLs for revocation status checking.
- **Optional pivCLASS Enroller** - intended for systems that do not already have PKI enabled registration capability.

The validation software is designed to be used with the HID Global pivCLASS Authentication Module, which provides real time authentication at the door at the time of access.

The Validation Server also provides an application programming interface (API) to enable any PACS head-end product to take advantage of the validation functionality provided by the Validation Service.

To achieve compliance, agencies simply deploy new pivCLASS readers and install authentication modules between the readers and the existing PACS panel. This upgraded access control system can now perform FIPS 201 authentication checking for all NIST defined assurance levels, with a validation server providing centralized dynamic control of assurance level settings and distribution of credential validation data. This modular system performs all necessary authentication steps, from the time of enrollment to the time of access.

pivCLASS Validation Server Features

- Validates multiple card types including PIV, PIV-I, CIV (PIV-C), CAC NG, CAC EP, Legacy CAC, TWIC and FRAC
- Supports multiple authentication modes including FASC-N, CHUID, CAK, PIV + PIN, CHUID + BIO, CAK + BIO, and PIV + PIN + BIO
- Provides centralized configuration and management of pivCLASS Authentication Modules (PAMs)
- Sets authentication modes for pivCLASS readers
- Sets rules to extract badge IDs from each card type
- Sets the Wiegand format for badge ID output
- Sets trusted card issuers (i.e., trust anchors)
- Periodically revalidates trust paths for all certificates
- Periodically retrieves card revocation status from issuing certificate authorities (OCSP, SCVP, CRL, TWIC Cancelled Card List)
- Updates validation data cache on PAMs
- Collects detailed log activity from PAMs for display and export
- Sets degraded mode parameters to allow continued validation when up-to-date validation data from issuers is not available
- Distributes TWIC Private Keys (TPKs) to PAMs for contactless BIO authentication
- Updates the firmware on the PAMs; no field updates required
- Includes API and supporting tools to enable PACS software head-end suppliers to provide card validation during registration; periodic updates of credential status; reader configuration management; and import of access logs from PAM to the head-end
- Includes an optional Enroller for special cases when no PACS head-end is used

SPECIFICATIONS

Model Number	PCVSL
Part Number	PCVSL
	SYSTEM REQUIREMENTS
Operating System (32-bit)	Microsoft Windows Server 2008 SP2, Windows Server 2003 SP2, Windows XP SP3, Windows Vista SP2, Windows 7
Operating System (64-bit)	Microsoft Windows Server 2008 SP1 R2, Windows Vista SP2, Windows 7 SP1
Database	Microsoft SQL Server 2008 R2, SQL Express 2008 R2
Other	Microsoft .NET Framework 2 GB RAM 10 GB hard disk space PC/SC smart card reader such as HID OMNIKEY 3121 or 5321r pivCLASS Authentication Module(s) pivCLASS or other supported reader(s)
	INTERFACES
PAM	Ethernet TCP/IP; optional AES 256-bit encryption
Internet	HTTP and HTTPS
API	SOAP over HTTPS
	CERTIFICATIONS, PROTOCOLS, STANDARDS
GSA "Caching Status Proxy"	Listed on the U.S. GSA APL 629
OCSP	Online Certificate Status Protocol for revocation checking
SCVP	Server-based Certificate Validation Protocol for delegated path discovery and delegated path validation
CRL	Certificate Revocation List for revocation checking
TWIC Cancelled Card List	For Transportation Worker's Identity Credential revocation checking
	OPERATIONAL
	Supports up to 100,000 cardholders
	Supports up to 256 pivCLASS Authentication Modules

North America: +1 949 732 2000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +49 6123 791 0
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

hidglobal.com

ASSA ABLOY
An ASSA ABLOY Group brand

2012-03-13-hid-pivclass-validation-server-ds-en