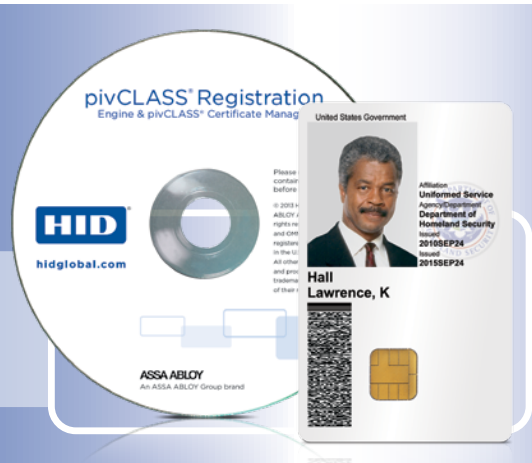
PHYSICAL ACCESS SOLUTIONS

pivCLASS® Registration Engine & pivCLASS® Certificate Manager



CARDHOLDER VALIDATION SOLUTION FOR HSPD-12 COMPLIANCE WITH AUTOMATED PACS REGISTRATION AND CERTIFICATE MANAGEMENT

- **Enables FIPS 201-compliant validation** of and registration with physical access control systems (PACS). Can update an existing cardholder record, or insert one if one did not already exist.
- **Active or passive badge suspension** if card certificate serial number is on Certificate Revocation List (CRL) or FASC-N is on TWIC CCL.
- **Modular solution** providing maximum deployment flexibility.
- **Operates with** COTS FIPS 201 PIV-II and ANSI INCITS 378-compliant fingerprint capture devices.
- **Supports** PIV, PIV-I, TWIC, CAC, CIV, and FRAC credentials.
- **Integrated with several fixed biometric readers.** Can send certificate revocation status, TWIC Privacy Key (TPK), etc. to the fixed reader upon request.

pivCLASS® Registration Engine

A PC-based solution that provides three-factor authentication, extracting and verifying cardholder data on a FIPS 201 smart card and performing a biometric match against the templates stored on the card. Digital certificates are verified against the issuer's validation authority, SCVP or OCSP responder. All cards are validated using FIPS 201 challenge-response (CAK or PAK) in order to identify forged or cloned cards. Works with all PIV, PIV-I, TWIC, CAC, and FRAC cards.

After validation, pivCLASS Registration Engine performs automated registration of FASC-N, photo and printed information into compatible PACS.

Updates a cardholder record if it already exists in the PACS, or inserts a new record if one does not exist.

pivCLASS® Certificate Manager

Certificate Manager is a PC-based application that re-validates imported cardholder certificates on a user-defined periodic basis. Certificate Manager can be configured to suspend a PACS badge associated with an invalid or revoked certificate, to generate alarms in the PACS and can send an e-mail to a distribution list for notification when it discovers an invalid certificate.

Codebench
an HID Global company

3-FACTOR VALIDATION PROCESS

SOMETHING YOU HAVE
FIPS 201-compliant credential is inserted in reader. Information is retrieved from the card for CAK validation.

SOMETHING YOU KNOW
Stored PIN is compared to user entry for validation. PIN is entered via keypad.

SOMETHING YOU ARE
Stored biometric is compared to user entry for validation using NIST- and MINIX-certified template generator and matching algorithm.

NOT AUTHENTICATED
This is the result of one of the following conditions:

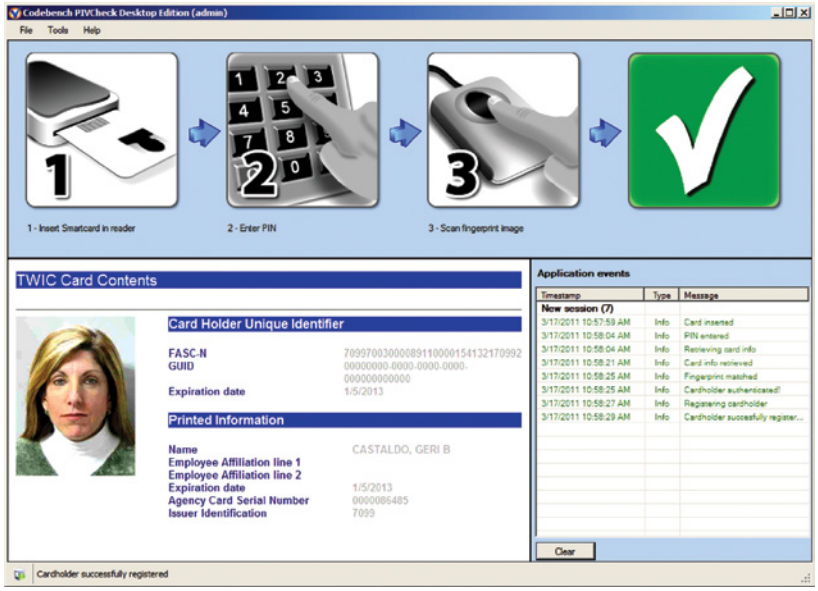
- Card read error
- Expired smart card
- Invalid (possible forged or cloned) card
- Invalid PIN
- Biometric mismatch
- One or more certificates are revoked
- FASC-N is on the TWIC CCL
- Operator cancels the verification

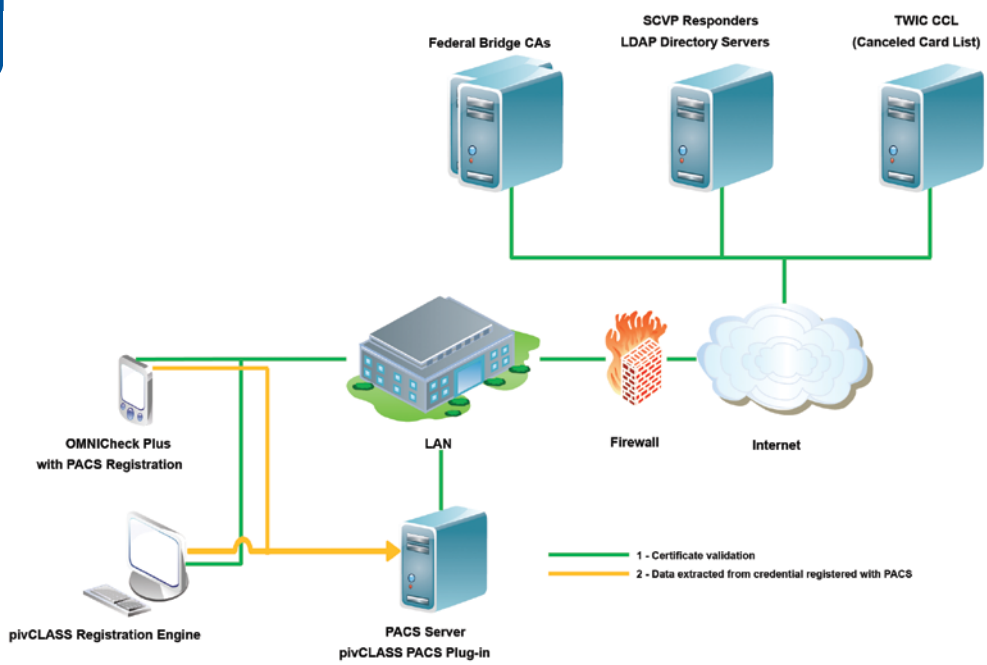
AUTHENTICATED
The card was determined to be valid using the methods supported for the given smart card. The following is known:

- PIN Verification (Only for cards which are PIN protected, and the card is inserted in the contact interface)
- Smart card is not expired
- Smart card is not forged or cloned
- Cardholder is linked to the smart card
- Smart card has not been revoked
- Certificates are not revoked

SPECIFICATIONS

Models	pivCLASS Registration Engine pivCLASS Certificate Manager
CPU	Minimum of 1.8 GHz or greater.
Random Access Memory	Minimum of 1 Gb RAM or greater.
Hard Disk Space	Minimum of 1 Gb RAM or greater.
Support OS	Windows 7 Ult, Windows 7 Pro, Windows Vista Ult, Windows Vista Bus, Windows Server 08, Windows Server 03, Windows XP SP3





GSA FIPS 201 APPROVED

ASSA ABLOY
An ASSA ABLOY Group brand

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

2013-03-13-cb-pivCLASS-registrtn-Engine-Cert-mng-ds-en