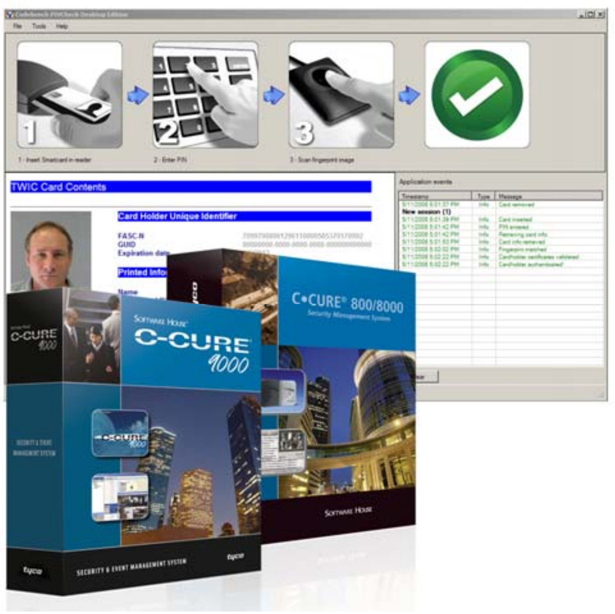
Codebench PIVCheck®

FIPS 201-Compliant Cardholder Verification and Enrollment Solution


Codebench PIVCheck Desktop Edition
File Tools Help
1
2
3
1 - Insert Smartcard in reader
2 - Enter PIN
3 - Scan fingerprint image
TWIC Card Contents
Card Holder Unique Identifier
FASC-N
GUID
Expiration date
Printed Info
Name
Application events
C•CURE® 800/8000
Security Management System
Software House
C-CURE 9000
Security & Event Management System
tyco

```
Timestamp              Type  Message
5/11/2008 5:01:37 PM   Info  Card removed
New session (1)
5/11/2008 5:01:39 PM   Info  Card inserted
5/11/2008 5:01:42 PM   Info  PIN entered
5/11/2008 5:01:42 PM   Info  Retrieving card info
5/11/2008 5:01:53 PM   Info  Card info retrieved
5/11/2008 5:02:02 PM   Info  Fingerprint matched
5/11/2008 5:02:22 PM   Info  Cardholder certificates validated
5/11/2008 5:02:22 PM   Info  Cardholder authenticated
```

Features That Make a Difference:

- Verifies cardholder identity and validates FIPS 201-compliant PIV-II, next-generation (NG) CAC, TWIC, or FRAC credentials in real-time
- Performs three-factor authentication of cardholder using PIN, biometrics, and certificate (or serial numbers) detecting forged or cloned cards
- Enrolls FASC-N, photo, and pertinent cardholder information into C•CURE® 9000 and C•CURE 800/8000
- Automatically suspends a C•CURE cardholder's badge if his or her PIV, TWIC, or CAC card certificate serial number is on the Certificate Revocation List (CRL)
- Uploads a cardholder transaction audit trail to central database or exports it to a .csv file for centralized transaction management
- Compatible with Datastrip DSV+ Turbo® biometric mobile terminal for off-site verification and enrollment
- Re-validates imported cardholder certificates on a periodic basis via the Internet
- Operates with commercial, off-the-shelf (COTS) FIPS 201 PIV-II and ANSI INCITS 378-compliant fingerprint capture devices

PIVCheck® Desktop Edition cardholder validation

PIVCheck Desktop Edition lets you perform a solid, three-factor authentication process, including biometric matching using a fingerprint capture device[1] capable of single fingerprint capture. Digital certificates can be verified by security personnel using the issuer's certificate authority, SCVP, OCSP responder/repeater, or the TSA hot list for TWIC cardholders. All cards are validated using FIPS-201 challenge-response protocol in order to identify forged or cloned cards. PIVCheck Desktop Edition validates all PIV, TWIC, NG CAC, and FRAC cards. TWIC card FASC-Ns are also verified against a live or cached TSA hot list.

PIVCheck Mobile Edition mobile cardholder validation

PIVCheck Mobile Edition includes the same functionality as PIVCheck Desktop Edition but uses the Datastrip DSV2+ Turbo biometric mobile terminal with Ethernet and WiFi connectivity. This solution provides strong, three-factor authentication, managing the acquisition of cardholder data from a smart card and performing off-card biometric matching at a variety of off-site locations.

PIVCheck Plus Desktop Edition cardholder registration

Once the validation of a cardholder is complete, PIVCheck Plus Desktop Edition automatically registers the FASC-N, photo, and pertinent cardholder information into C•CURE 9000 and C•CURE 800/8000 systems using the PIVCheck PACS plug-in[2].

The PACS plug-in creates a data import file in the C•CURE system to ensure updated PIV-II credentials work seamlessly with your security system. The C•CURE cardholder's badge is suspended should the serial number be listed as unreliable, invalid, or if it appears on the CRL.

PIVCheck Plus Mobile Edition mobile cardholder registration

Once the three-factor authentication process is complete at a designated remote site, the PIVCheck Plus Mobile Edition automatically registers the information into the C•CURE system directly from the Datastrip DSV2+ Turbo handheld reader using network connectivity.

(1) COTS FIPS 201 PIV-II and ANSI INCITS 378-compliant
(2) PACS plug-in/Certificate Manager must be installed on same system as C•CURE

PIVCheck Certificate Manager periodic revalidation

To make certain you have up-to-date credential information, PIVCheck Certificate Manager revalidates imported cardholder certificates at regular intervals, ensuring that the credentials used in your C•CURE system are backed by a valid set of digital certificates.

Digital certificates are verified against local OCSP repeater/validation authority using the issuer's validation authority, or Microsoft Crypto API on Windows XP SP3 or Vista. Certificate Manager fully supports SCVP and OCSP for fast, online validation. For TWIC credentials, FASC-Ns are also verified against a live TSA hot list.

Certificate Manager operates in either active or passive mode. Active mode immediately suspends the C•CURE cardholder badge, while passive mode provides notification to site security management.

PIVCheck Audit Trail

PIVCheck Audit Trail enables you to upload local transactions to a central database for consolidated activity reporting. This application supports a variety of ODBC- or ADO-compliant databases, including Oracle, SQL Server 2005, Informix, DB2, and Firebird. You have the ability to produce canned transaction log queries as well as creating queries directly from the SQL database. The Audit Trail option also allows you to export all report results to a .csv file.

Important Government Acronyms	
ANSI	American National Standards Institute
CAC	Common Access Card
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FRAC	First Responder Authentication Credential
INCITS	International Committee for Information Technology Standards
OCSP	Online Certificate Status Protocol
PACS	Physical Access Control System
PIV	Personal Identification Verification
SCVP	Server-based Certificate Validation Protocol
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

For an extensive list of government acronyms, visit www.acronymanxiety.com/gov.

System Requirements

PIVCheck Desktop

- Operates on Intel-based PC with minimum 1.8 GHz CPU, 1 GB RAM, 40 GB hard disk, and Microsoft Windows XP SP2 with Microsoft .NET Framework 2.0
- Supports Identix BTO-500 and Cogent CSD301 fingerprint capture devices and SCM SDI010 smart card reader

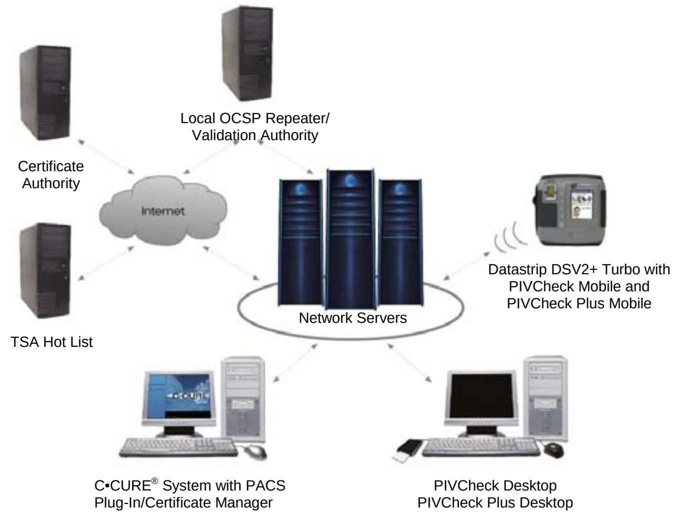
PIVCheck Mobile

- Operates on the Datastrip DSV2+Turbo® biometric mobile terminal which may include 802.11g communication module, dual grip battery cover, and NEC or Identix fingerprint matching options

Network

For real-time PACS registration, network connectivity is required.
For real-time TWIC validation, Internet connectivity is required.
For real-time card validation, network connectivity with validation authorities is required.
For C•CURE specifications, refer to C•CURE 9000 and C•CURE 800/8000 data sheets at www.swhouse.com.

System Diagram


Local OCSP Repeater/ Validation Authority
Certificate Authority
Internet
TSA Hot List
Network Servers
Datastrip DSV2+ Turbo with PIVCheck Mobile and PIVCheck Plus Mobile
C•CURE® System with PACS Plug-In/Certificate Manager
PIVCheck Desktop PIVCheck Plus Desktop

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative. Certain product names mentioned herein may be trade names and/or registered trademarks of other companies.