

TRUSTALERT™ AUTHENTICATION, ENROLLMENT & CREDENTIAL REPOSITORY SOLUTIONS

AUTHENTICATION AND ENROLLMENT

BridgePoint's suite of tightly integrated hardware and software products optimize authentication and enrollment of PIV, CAC, TWIC and PIV-I credentials into compatible access control systems. Advanced functionality enables storage of PKI certificates for optional revocation status checking of the public key certificates on the credential (NOTE: requires TrustAlert Certificate Validation Service).

By importing data directly from the credential, errors that result from manual entry are eliminated and efficiency is significantly increased. Enrollment time is reduced to 15 seconds compared with up to 5 minutes for manual entry.

TrustAlert includes a Certificate Repository that stores Public Key Certificates from the credentials as they are enrolled. This data store can be used to validate the certificate status of enrolled credentials on a scheduled basis per Government guidance for strong authentication in PACS.

The TrustPoint Enrollment Stations provide strong authentication including PIN, biometric, and PKI challenge-response verification to both the personal and card authentication certificates on the credential.

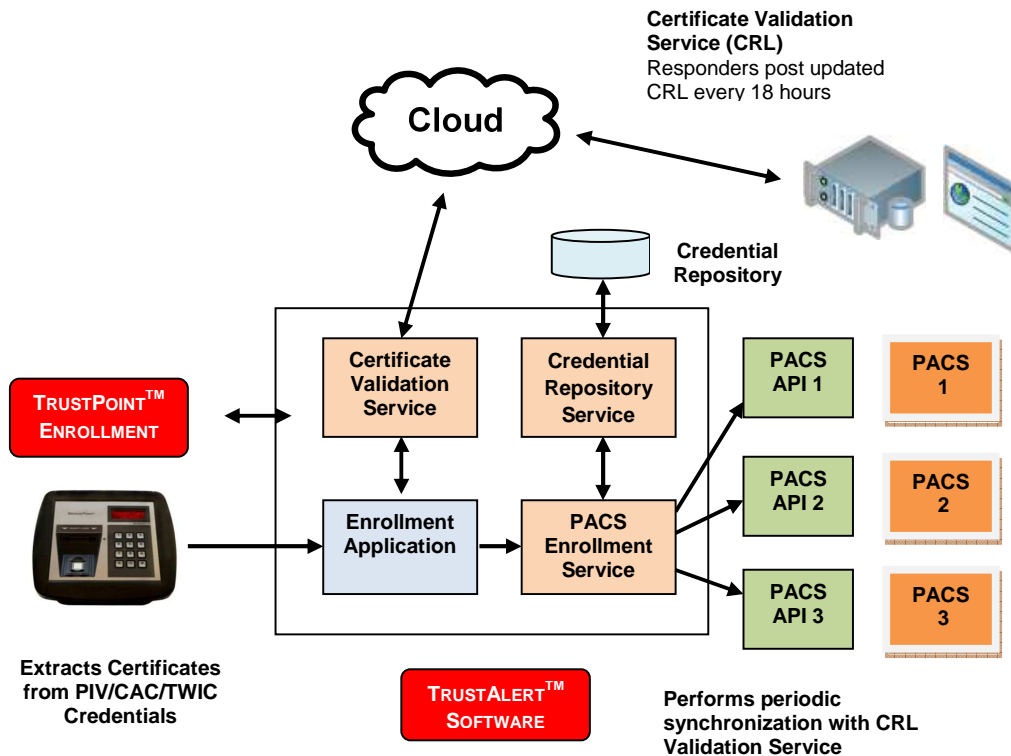
TRUSTALERT SOFTWARE COMPONENTS

Enrollment Application – Provides the GUI interface through which the enrollment process is performed.

PACS Enrollment Service – Provides a uniform interface between Enrollment Software components and a range of PACS systems. Adds personnel and credentials (badges) into an integrated PACS system, assigns a default access privilege (level) and disables credentials in the event of a relying certificate being revoked.

Credential Repository Service – Maintains a secure (FIPS140) credential repository containing copies of relying credentials used during the enrollment process.

Certificate Validation Service – Validates presented credentials via OCSPP (Online Certificate Status Protocol), SCVP (Server-based Certificate Validation Protocol) or CRL (Certificate Revocation List). NOTE: not included with the Enrollment Application or Service.



PKI 2-FACTOR DESKTOP AUTHENTICATION STATION



P/N 78-02-1212

DESCRIPTION

The TrustPoint Desktop Enrollment Station provides 2-Factor authentication of a PIV Credential by authenticating the User's CARD & PIN. The simplicity and speed of a user-friendly device simplifies enrollment which saves time and money.

The Station can extract the cardholder's PHOTO and execute a PKI challenge-response to both the Personal Certificate Private Key (PAK) and the Card Authentication Private Key (CAK). The Station exports data from the credential (including the Name, Agency, Expiration Date, Photo and FASC-N) into the BridgePoint TrustAlert application. Once the data is imported, TrustAlert will then "enroll" the user into a PACS with one simple "point and click" action.

FEATURES:

- Sturdy construction and Integrated design simplifies the enrollment process for the user
- Presents same user experience as the BridgePoint Access Readers
- Eliminates multiple desktop components
- Eliminates data entry errors
- Less than 15 Seconds for complete enrollment process
- Supports PIN challenge
- Supports PKI Challenge-Response to both personal authentication key (PAK) and card authentication key (CAK)
- Extracts PHOTO image from chip for displaying in a compatible PACS
- Data presented in structured XML or ASCII text format suitable for direct input to a compatible PACS
- Plug and Play USB Interface

HIGH ASSURANCE (LEVEL 3)

PKI DESKTOP 3-FACTOR AUTHENTICATION STATION



P/N 78-02-1212

3-Factor Desktop Enrollment Station

The TrustPoint Desktop Enrollment Station provides 3-Factor authentication of a PIV Credential by authenticating the User's CARD, PIN and BIometric. The simplicity and speed of the Station simplifies enrollment, saving time and money.

The Station executes a PKI challenge-response to both the Personal Certificate Private Key (PAK) and the Card Authentication Private Key (CAK). The Station exports essential data from the credential (including the Name, Agency, Expiration Date, Photo and FASC-N) into the BridgePoint TrustAlert application. Once the data is imported, TrustAlert will then "enroll" the user into a PACS with one simple "point and click" action.

FEATURES:

- Sturdy desktop appliance
- Automates direct enrollment into a compatible PACS (FASC-N, Name, Expiration Date, etc)
- 16 character by 2 line display guides user through enrollment process
- Supports PIN Challenge
- Supports BIO Challenge (Live Scan to Stored Template)
- Supports PKI Challenge-Response to both personal key (PAK) and card authentication key (CAK)
- Extracts and displays PHOTO image from chip
- Extracts and stores Personal and Card Authentication Certificates in Credential Repository for periodic revocation checking
- Less than 15 Seconds for complete process
- Data exported in structured XML format suitable for direct input to a compatible PACS
- Plug and play USB Interface

VERY HIGH ASSURANCE (LEVEL 4)

TRUSTALERT ENROLLMENT SOFTWARE

Attended Enrollment

PACS Validate Security Passcodes Repository Credential Help

Card Information
 Type: PIV Expiration: 2010.06.01

Personnel Information
 Name: THOMAS E CORDER
 Employee Affiliation: Employee NCR
 Issuer ID: 00999999900001 CSN: 1000000534

FASCN
 FASCN: 7000-0001-000534-1-1-1000000534199991 eFASCN Hash: 3639301202
 GUID: 65784549-4545-5949-4564-36754141414D
 Agency Code: 7000 System Code: 0001
 Credential Number: 000534 Credential Series: 1 ICI: 1
 Person Identifier: 1000000534
 Org Cat: 1 Org Id: 9999 Ass Cat: 1

Security
 Bio Scan Status: Fingerprint Scanner not present

PKI
 Cert Type: Card Auth PIV Certificate
 PKI Algorithm: RSA 1024 RSA 1024
 Private Key Challenge: SUCCESS SUCCESS
 Certificate Status:

Enroll Deny Enrollment Override Exit

Status: End card reading

TRUSTALERT ENROLLMENT APPLICATION

The TrustAlert Software Application interacts with the TrustPoint Desktop Enrollment Stations to provide comprehensive credential data and HSPD-12 authentication mechanisms in one view.

The window displays the progress in real time as the user is enrolling. The attendant can view the results of the authentication factors including Card Expiration Date, BIO Scan result, Private Key Challenge result and digital photograph Status.

If the pre-configured Security Policy is met, the attendant can click on the Enroll button to complete the process. If the minimum security policy is not met a Supervisor can enter their security code to enable an optional Override.

P/N 78-02-1212

Security Policy Configuration

The TrustAlert Enrollment Application includes a Policy Settings Menu that enables setting authentication mechanisms to Mandatory, Optional or Not Required for enrolling a credential into a PACS. Security Policy Settings include:

- PKI Challenge
- BIO Match
- Certificate Status

Validation Policy Configuration

The TrustAlert Enrollment Application also includes a Menu that enables setting of certificate validation requirements, including:

- PIV Certificate
- CAC Signing Certificate
- Card Authentication Certificate

Validation of these certificates can be set to Mandatory, Optional or Not required.

Security Policies

PKI Mandatory Optional Not Required Allow supervisor to override

BIO Mandatory Optional Not Required Allow supervisor to override

FACIAL Mandatory Optional Not Required Allow supervisor to override

Caution:
 Be advised that this features stores data from individual cards on this computer. It should be used for debug purposes only!

Enable Card Capture

Status: