DIGITAL TRUST
from Silicon to Services

intercede

Access to secure facilities using the Transportation Worker Identification Credential (TWIC)

Features used

- Lifecycle management API
- RSA PKI integration and certificate lifecycle
- management connector
- Key management utilizing HSM
- Biometric applicant ID verification
- MyID bureau connector
- Self-service activation
- PIV card management
- Key management utilizing HSM
- Multi-server load balanced deployment

The customer

The US Transportation Security Administration (TSA) is the federal agency responsible for security in all modes of transportation. Joint customer for the project is The United States Coast Guard (USCG), a branch of the United States armed forces and one of seven uniformed services.

The challenge

The customer wished to issue a tamper-resistant biometric credential to maritime workers requiring access to secure port facilities and vessels. To obtain a Transportation Worker Identification Credential (TWIC), an applicant must provide biographic and biometric (fingerprint) information, sit for a digital photograph and successfully pass a security threat assessment conducted by TSA. A key customer desire was to follow US Government Homeland Security Presidential Directive 12 (HSPD-12) standards, to achieve interoperability and implement best practice security processes. Requirements included:

- Use of FIPS 201 (PIV) technology and processes
- Combined centralized production with local card activation
- Over 160 distributed enrolment and activation centers throughout the US
- Integration with central card personalization bureau for secure printing
- Fingerprint verification of applicant prior to card activation
- Integration with central identity management infrastructure
- Multi-application card combining contact and contactless technology
- Strong authentication of operators and non-repudiation of operator actions

The MyID solution

MyID® is passed registration data from the IDMS and formats it into a card personalization request; this is forwarded to the personalization bureau. Printed cards are locked and sent to activation locations. The receipt of a card batch is used to trigger a notification to the applicant that their card is ready for activation. The applicant visits an activation location, places their card into a MyID activation station and follows a simple self-service workflow that requires biometric verification before the card is unlocked, personalized with certificates and activated for use.

Project status

The project is live with over two million cards and eight million certificates issued to date. The system is scaled across multiple servers for high availability and performance and a peak production volume of 10,000 cards per day has been achieved. The solution was delivered from order to live production in a three-month time period.

Multiple mobile platforms

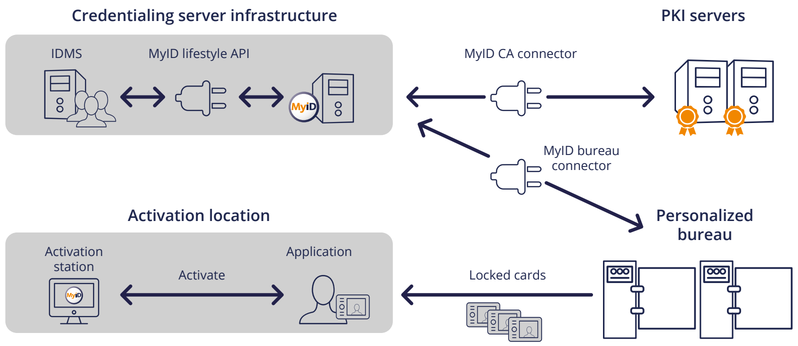
With your existing Cloud services

Using the latest mobile phone security features

How does it work?

MyID from Intercede® is used as part of an integrated identity management solution designed to deploy CIV compliant cards to a FIPS 201 business process. Port workers are required to hold a TWIC card to gain access to secure port facilities.

1. The port worker applying for the card visits one of over 160 distributed enrollment centers where their fingerprints, photographs and data are captured.
2. The registration system passes registration data to MyID via the lifecycle management API.
3. MyID takes the registration data and formats it for bureau production.
4. MyID batches up card requests and passes them to the card personalization bureau for production. During this process MyID can be used to enquire on the status of the production requests.
5. The bureau prints the cards and writes the applets and data to them. The cards are then locked for security purposes.
6. The card is shipped to an enrollment center in a batch.
7. MyID is used to record the delivery of the batch of cards into the enrollment location. This process triggers a notification to the port worker that their card is ready for collection.
8. The port worker attends the enrollment center and is handed their card for activation.
9. The port worker takes their card to a MyID self-service activation kiosk.
10. As the card is inserted into a reader MyID recognizes the card as requiring activation and walks the user through a simple activation process.
11. During the activation process MyID validates the port worker's identity via a fingerprint check.
12. Once validated the card is unlocked and the port worker sets their PIN.
13. MyID then generates keys and certificate requests on-card.
14. MyID passes the certificate requests to the certificate authority and retrieves the certificates.
15. MyID writes the certificates to the card
16. The process is complete - the card is available for immediate use



How MyID can help eID projects

- Single integrated platform for end-to-end identity registration and credential issuance
- Full registration capabilities including application form scanning, ICAO/FIPS 201 compliant photo capture, physical signature capture and biographic data capture.
- Project Designer tool lets you define the attributes to capture and screen layouts for each process.
- Full adjudication/ID verification support including integration with external AFIS, local AFIS and background checking services.
- Card personalization bureau integration, including 2-pass and 4-pass models, batch to individual request drill down enquiries and multiple status updates.
- Direct issuance from MyID including batch, attended and self collection.
- Batch pre-encoding support for faster card activation.
- Support for multiple concurrent credentials from a single system (e.g. passport, driving license, ID card).
- Support for multiple concurrent issuance models allowing for emergency cards and temporary replacements
- Highly configurable platform to adapt to changing project needs without extensive recoding.
- Scales up and out to very high volumes

Solution benefits

- Fully FIPS 201 accredited solution
- Production of PIV compatible credentials
- Smart card PKI security for operator actions
- Biometric authentication of applicants for high security
- Multi server deployment for high availability
- Load balanced deployment for high volume throughput
- Simple web-based workflows for maximum ease of use
- Monitoring of card production status from a single console
- Bureau high security printing combined with on-card key generation for maximum security

@ info@intercede.com www.intercede.com intercedemyid
Suite 920, 1875 Explorer Street, Reston, VA 20190, USA ☎ +1 888 646 6943