“Lessons Learned Implementing in Physical Access on the TWIC Program”
David Muha
TWIC Overview

- TWIC Overview
- Physical Access Lessons Learned
TWIC Overview

➢ Transportation Worker Identification Credential

➢ Program Goals:
  – The goals of the Transportation Worker Identification Credential (TWIC) program are to:
    • Improve security
    • Enhance commerce
    • Protect personal privacy

➢ TWIC Vision
  – Improve security by establishing a system-wide common credential used across all transportation modes for all personnel requiring unescorted physical and/or logical access to secure areas of the national transportation system.
TWIC Overview - Program Objectives

- Develop a common credential or standard, universally recognized and accepted across all modes of the transportation system, funded primarily by user fees, as is the case in other modes of transportation.
- Create a uniform, nationwide standard for secure identification of transportation workers.
- Minimize the requirement for redundant credentials and background checks.
- Design a solution to positively and securely link an individual to her credential via a reference biometric and to the background information on the claimed identity of that individual.
- Ensure that the TWIC solution is compatible with existing facility access control and related systems to leverage current security investments.
- Ensure the ability to quickly revoke access privileges to TWIC holders who are identified as a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards.
TWIC Program Phases

- Phase I – Planning
- Phase II – Technology Evaluation
- Phase III – Prototype
- Phase IV – Implementation
- Phase V – Operation & Maintenance
Technical Overview

1. Sponsor
2. Transportation Workers
3. Enrollment Centers
4. Identity Management System (IDMS)
5. Card Production Facility
6. Local Facilities
7. Transportation Workers
8. Numbers Indicate Workflow Order

- 1:n biometric search
- Name-Based Terrorist-Focused Risk Assessment
- Office of National Risk Assessment (ONRA)
Physical Access Lessons Learned

- Combat Environmental Suitability Issues
- Provide Customer Service and Support
- Overcome User Training Issues
- Avoid Improper Mountings
- Not Have Poor Card Read Rate
- Use Standards Successfully
- Design/Development Considerations
Combat Environmental Suitability

- Readers must be designed to be mounted outdoors and withstand changing weather conditions.
- Readers installed in enclosures still expose the devices to weather conditions when opened, and slows the use of devices.
- Sensor devices must be able to tolerate the direct impacts of environmental exposure, including:
  - Condensing humidity (rain)
  - Direct sunlight (shielding)
  - Wind accumulation of static charge in the environment
  - Abrasion on the sensor surface
Provide Customer Service and Support

- Must provide complete customer service support in order to be successful.
- Roles and areas of responsibility need to be clearly defined and supported.
- Team approach works best when dealing with many different parts of a security system.
- Biometrics are still new; people need help learning about them and using them.
Overcome User Training Issues

- Readers must be as intuitive to use as possible.
- Users should be trained how to use readers correctly.
- Provide simple instructions to assist infrequent users.
- Educate users on the actually equipment they will be using.
Avoid Improper Mountings

- In order to avoid reader mounting issues
  - Readers must be installed at the proper height for target users
  - Readers should be mounted such that they do not extend too far forward, to avoid being hit by vehicles
  - Reader enclosures can not be allowed to get in the way of users
- Site Surveys are invaluable and required for a successful implementation
Not Have Poor Card Read Rate

- TWIC Card incorporated enhanced security features
- Readers must be able to perform security functions very rapidly
- The TWIC data model evolved which required a reader which was upgradeable to accommodate changes in the card over time.
- Real challenge to implement PKI at the door and still stay within the 2 second timing requirements. But we did it!
Use Standards Successfully

- TWIC card includes 2 fingers in 2 standard formats on both contact & contactless sides:
  - ANSI INCITS 378 (Finger Minutiae)
  - ANSI INCITS 377 (Finger Pattern)
- Storage allocated: 1600B x 2 (not all used)
- ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange
  - Offline interoperability test conducted before committing to card
  - Demonstrated interoperability with door readers from 2 different vendors
- ANSI/INCITS 377-2004 Finger Pattern Format for Data Interchange
  - Interoperability was not tested since the enrollment and live scan readers were from the same vendor
Contact vs Contactless

- Contact primarily used for logical access
- Contactless primarily used for physical access

WHY?

- Contact issues for physical access
  - Environmental – cannot meet IP-65 requirements due to opening
    - Humidity & dust
  - Card durability
    - Bending/cracking
  - Additional portal throughput time
Crypto at the Door

- Biometric data stored on contactless side of card card
  - 14443 (DESFire)
  - Crypto mutual authentication access control on biometric container
  - Hashes and digital signatures employed

- Challenges
  - Implementing crypto on microcontroller within the the 2-second present-to-open time limit
  - Key management

- Related – hotlist checking
Operational biometrics

- Contactless storage limited to 4K – not large enough to store additional operational biometrics
  - Future – dual interface cards
- Security issues with allowing transportation facilities to write to card
  - Operational enrollment to local server
  - Card unique ID used as pointer
Summary

- Readers can be made to withstand the weather
- The readers can be successfully supported in the field
- Users can learn to successfully use the readers
- Ways can be found to successfully mount the readers
- Readers can work fast
- Standards can help get the job done