Port of Seattle

Biometric Card Access Control
A Case Study

American Association of Port Authorities
Information Technology Committee Meeting
Tacoma, Washington
April 19, 2006
Topics for today

• Introduction.
• Brief historical review.
• The place of the IT Department.
• The impact of 9/11 on our plans.
• Biometric project decision overview.
• Smart Cards 101.
• Q & A
Introduction

Brad Jenson
Jenson.B@PortSeattle.org

• 25+ years with Port of Seattle Information Technology
• 18+ years supporting airport security systems
• 3+ years supporting seaport security systems
• 1+ years supporting Police & Fire
Seaport Statistics - 2005

- Total TEU Containers: 2,087,929
- Total Cruise Passengers: 686,357
- Total Vessel Calls: Container – 898 Cruise - 170
- 1,517 Active Cardholders
- Access Control deployed March 2004
Airport Statistics - 2005

• Total Air Passengers: 29,289,026
• Total Aircraft Operations: 341,470
• Total Air Cargo (metric tons): 338,591
• 20,026 Active Cardholders
• Biometric Cards October 2003
Security at the Airport – where it all started

A brief overview of evolving technologies...
The 1980’s

Instant Camera Cards

Camera  Laminator  Die Cutter
Door Access Card

(Representative example)
The mid 1990’s

Laminated ID Cards
The late 1990’s and through Y2K

PVC/Composite Cards

Magnetic Stripe
The intended post Y2K plan...

Dual Technology Cards

Magnetic Stripe and 125 KHZ Proximity
Security System Technology Changes

- Proprietary solutions gave way to Windows desktop standards.
- Use of standard SQL databases rather than proprietary or desktop-grade file systems.
- Field devices, door readers may be IP addressable.
- Wireless technology.
The Entrance of IT into Physical Security’s Turf

- Converging network and server requirements and infrastructure.
- High reliability servers; no longer a PC under the counter.
- Complex database, server and network administration.
- Surveillance: CCTV moving to IP
What IT Can Offer

- System integration skills. Was a non-issue in the proprietary era.
- Setting technology standards to reduce maintenance costs.
- Handle data privacy issues. Systems now require more PPI.
- Best practices for cyber security & evaluating vendor compliance.
Our Integration Plan
A Few Things IT Gets From the Deal...

- Experience and expertise with biometrics: Also use for login access to enterprise PCs?
- Exposure to surveillance technology: A voice at the table for future IP implementations, digitized storage.
- Engagement as they start stringing network and cable everywhere.
And, unless this is you...
Need Partnering of IT and Maintenance Dept.

- Need to clearly define system support roles. It’s critical!
- Delineate support roles where network meets field devices.
- Repair and PM of readers.
- Surveillance Cameras – Same story. Does IT climb ladders?
- Consider labor relations issues.
Typical Implementation

Host System

Access Control Panel

Door Monitor

REX

Reader

Strike

Access Card

Physical Access Control
The Port of Seattle had plans to construct and implement a new access control system at Seattle-Tacoma International Airport using standard proximity card technology. This new system was critical to completion of a $587M airport terminal expansion project.
But the world changed...
But the world changed...

And so did we.
Following 9/11

- Increased focus on biometrics.
- Emphasis on identification and authentication of transportation workers – TWIC emerges on scene.
- Formation of the TSA, DHS, etc.
- Development of information sharing networks and systems.
- Grant funding for Seaport Security.
Our directives...

• Reevaluate plans in light of 9/11.
• Install a forward looking solution.
• Identify and recommend viable, cost effective biometric technologies.
• Insure that it would not jeopardize airport terminal construction project.
• Integrate into existing project for access control system replacement.
Five Years of TWIC

- In late 2001... TWIC was not ready for prime time in a large access control project like ours.
- In early 2006... (insert your personal views here).
- The Port of Seattle decided to go forward and not wait for TSA.
Biometric Basics

• **TWIC is simply one biometric technology implementation.**
• **TWIC is more about standards authentication systems, process, and infrastructure than biometrics alone.**
• **Many biometrics are not TWIC.**
Question: Is the Port of Seattle System TWIC?

Answer: No. But processes, technologies, security procedures, databases, etc., are TWIC enablers.
Levels of Authentication

- What you have (Access Card)
- What you know (PIN number)
- Who you are (Biometric)

The use of biometrics adds the third level of security.
Biometrics and Identity

Theft

- Biometrics will become more prominent in commerce
- If it is valuable to a thief, biometric identities will be stolen and misused
- Once it’s stolen, the victim has no way to change the biometric source – it is part of their being
A Source of Information

www7.nationalacademies.org/cstb/pub_authentication.html

Who Goes There?
Authentication Through the Lens of Privacy
Biometric Technologies Considered by Seattle

- Finger Scan
- Hand Geometry Scan
- Iris Scan
A useful resource

Framework for Evaluating and Deploying Biometrics in Air Travel
Applications: Surveillance, Trusted Travel, Access Control

International Biometric Group  April 3, 2002
Finger Scan - Strengths

- Proven technology capable of high accuracy
- Ability to enroll multiple fingers
- Familiar as an identification method
- Range of deployment environments
- Ergonomic, easy-to-use devices
- Potential alignment with background checks, derogatory searches
Finger Scan - Weakness

- Performance can deteriorate over time
- Association with forensic applications
- Users can intentionally damage fingerprints
- Need to deploy specialized acquisition devices
- Vendor technologies not typically interoperable (at the time)
Hand Scan - Strengths

- Able to operate in challenging environments
- Established, reliable core technology
- Long deployment history in air travel environments
- Perceived as non-intrusive
- Based on a relatively stable physiological characteristic
Hand Scan - Weakness

- Not highly resistant to false matches
- Design complicates usage by certain populations
- Large size may limit deployment to access control and kiosk-type applications
Iris Scan - Strengths

• Potential for exceptionally high levels of accuracy
• Capable of reliable identification as well as verification
• High stability of characteristic over lifetime
• Hands-free operation
Iris Scan - Weakness

- Acquisition of iris image requires more training and attentiveness than most biometrics
- User discomfort with eye-based technology
- Glasses can impact performance
- Propensity for false non-matching
# Biometric Comparison

<table>
<thead>
<tr>
<th></th>
<th>Finger</th>
<th>Hand</th>
<th>Iris</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ease</strong></td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Accuracy</strong></td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>User Accept</strong></td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td><strong>Long Term</strong></td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
## Biometric Comparison

<table>
<thead>
<tr>
<th></th>
<th>Finger</th>
<th>Hand</th>
<th>Iris</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decision Time</strong></td>
<td>5 sec</td>
<td>3-5 sec</td>
<td>1 sec</td>
</tr>
<tr>
<td><strong>Security Level</strong></td>
<td>High</td>
<td>Medium</td>
<td>Very High</td>
</tr>
<tr>
<td><strong>Fraud</strong></td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Data Size</strong></td>
<td>90 bytes</td>
<td>9 bytes</td>
<td>512 bytes</td>
</tr>
</tbody>
</table>
Reasons for Our Biometric Success

- Stakeholder involvement
- Scheduled/Managed Re-issuance
- FAQ’s provided to cardholders
- Running in parallel with old ACS
- Cardholder used test reader first
- Skilled and dedicated team
Seattle’s Card Reader: BIO, PIN, LCD, MIFARE
Non-Bio Card Reader: Card Only, or Card + PIN

Less Expensive
Compatible with same ID card
Non-critical uses
Be sure to plan for both bio and no-bio reader
In my opinion, these airport TSA guidelines seem to lean towards a networked centralized authentication without using smartcards; and adding a separate biometric subsystem.
Due to the increased focus on seaport security after 9/11, these environments (unlike airports) may be installing their very first access control systems in a post TWIC world.
One TSA TWIC Design

How a Biometric Card Could Help Control Access

Source: GAO analysis of TSA and state of Florida data.

*Cards that are no longer valid due to new threat information or because they are lost, stolen, or damaged.
“Why TWIC”, says TSA

Improves Security

• Reduces risk of fraudulent or altered credentials;
• Employs biometrics for secure, positive match of individual to authorized facility access points;
• Supports ability to interface and communicate with other agencies; and
• Provides timely system-wide revocation.

Source: www.tsa.gov/interweb/assetlibrary/TWIC_Brief.pdf
"Why TWIC", says TSA

Enhances Commerce

• Eliminates need for multiple credentials and background checks;
• Leverages current security investment and existing systems;
• Maintains process speed and efficiency;
• Expands e-government potential; and
• Enables public-private partnership.
Two Views of TWIC

• **TWIC is:**
  – Applicant authentication, vetting.
  – Visual Display ID Card
  – Access Control Device

• **TWIC is:**
  – Applicant authentication, vetting.

• **#1 assumes national standards.**
Your existing Access Control System

- Can it be upgraded to utilize biometric technologies?
- Is this the mandate you always wanted to replace a legacy system?
- Can the ID badge enrollment system be biometrically empowered?
Interoperability and Transition

• Can your legacy access control system be run in parallel with a new system during installation?
• Would a multi technology card assist in this process?
• Can your ID badge production software system produce a multi technology card?
Keep Legacy Access
Control System or Not?

• Wiring and Power
• Administration of Smart Readers
• Proprietary or Open System
• Enables Information Sharing
• ID Badge System
Biometric Readers: Wiring and Power Issues

- Smart Card readers are like small computers
- Higher power requirements
- Infrastructure must support required UPS/Battery backup
- New readers may require more wire strands than you have now or maybe wire is OK as is
Administration of Smart Card Readers

- Central admin may require data network cable installed to door
- Local admin with a configuration card more labor intensive
- Network monitoring tools can impact networked readers
- Networking of readers builds for the future but at a price
ID Badge System

- Can your existing ID badge system enroll biometrics?
- Does the existing system meet current computing standards?
- Are you able to quickly adapt the system to a changing world?
- Does it capture required data?
Another decision is how to do biometric validation...
Local or Central Biometric Validation?

- Local compares biometric on card to body part at reader
- Centralized authentication compares body part at reader to stored biometric info; may be dependant upon network
- Differing costs, security, and legacy conversion tradeoffs
Why Consider Local Validation at Reader?

• **Cost** – no data network required
• **Does not require access control system to be “biometrically enabled”** (but the ID enrollment and production system does)
• **Granting biometric door access is not network dependant**
The smart card options
Seattle examined

- Contact Cards (ISO 7816)
- Contactless Cards (ISO 14443A)

Seattle uses MIFARE 4K
Contactless Cards (ISO 14443A)
Contact Smart Card –
Current US Gov’t Issue
Contact Smart Card

• Chip takes up real estate where information could be printed.

• Card requires contact to reader.

• Possible limitations on card display: armbands, pouches, etc.
With either card type your cost will rise!!

- Card stock is more expensive
- Slightly longer time to enroll
- Print time increase
- More chance of mechanical / production failure
- Increased operator error rate
- More ways to break a card
A new realm of card damage

• ID office induced problems

• Cardholder actions

• Biometric deterioration
Badge Failure points

- Encoded biometric data no longer matches cardholder due to finger damage
- Hole severs antenna or lanyard wears through antenna
- Cardholder punches their own hole to fit their preference

George Washington
Expires 7-4-2076
ID Office Induced

• Be sure card design allows for a hole punch that misses antenna
• Don’t use manual hole punch – too inconsistent
• Do use electronic hole punch
• Choose card friendly lanyards, pouches, etc.
Cardholder Actions

- Inform cardholder that punching holes in a card will damage it.
- Educate cardholder that certain lanyards with metal clasps could damage card.
Biometric Deterioration

- Deteriorating finger quality due to abrasion, injury, hobbies, etc.
- If the finger (and the spare) no longer match, the cardholder will be denied access
- May require reproducing card
Ways to reduce smart card costs

- No smart cards for public area badges
- Solid ID office operator procedures
Option for photo-only cards for public access

• ID Badge software discerns whether the badge type requires smart card features

• Public area badges print on common inexpensive card stock
Operator and Office Procedures

- Operators thoroughly educate cardholder on proper usage
- Foster awareness on the expense of unnecessary reprints
- Require proper card handling and printer maintenance procedures
- Cardholder validates card on test reader prior to leaving office
Approximate Airport Stats; Excluding Seaport

- Badges per month: 900
- Total time to enroll: 35 minutes
- Biometric enrollment: 30 secs
- Deteriorated biometrics: 2 / mo*
- Approximately 500+ readers

* Smart card program < 3 years old
The enrollment process

Select Finger and Click Capture

Left

Right

Index

Capture

Index

Capture

Clear

Done
The enrollment process
The enrollment process
Failure to Enroll

- Certain cardholders will be physically unable to render a biometric
- Our failure rate is 0.42%
- Not tied to any demographic
- An alternative to biometrics must be provided
Require biometrics and PIN code for access?

- Airport also uses PIN w/ biometric; Seaport does not
- All three levels of security
- Counteracts “fake finger”
- Keeps PIN in person’s mind – “use it or lose it”
- Provides future proofing for PIN enabled devices and functions
Perceived cardholder comfort level w/ readers

(Per ID Office Mgr)
Typical Reader
Problems We’ve Seen

- Ambient light on outdoor reader
- Dirty fingers or dirty read surface
- Rain in Seattle !!
- Occasional failure of MIFARE read unit
- User error and impatience
- Broken card antenna
Other biometric reader “gotchas”

• Be sure to examine reader programming tools provided
• Be sure to specify how to handle “collisions” with other smart cards presented simultaneously
• Anticipate biometric gate access on varying vehicle heights – biometric adds a twist
The Supermarket Line

• What will you do to avoid the “being in the wrong line” at the supermarket scenario?
• How will you handle problems, exceptions at the reader?
• Biometric smart cards are NOT the old “swipe and go” world
Possible Exception Handling Techniques

- Very short time out periods
- A “cancel” button on reader
- Corrective prompts on LCD
- Design authentication process to allow alternate entry sequences (i.e., PIN then biometric, or biometric then PIN)
Other IT Issues

- Design and install a fully operational test environment; stockpile spares.
- Consider port-wide ID compatibility.
- Include cost recovery, point of sale solutions if needed.
- Do a thorough review of change management and planned maintenance; Impact on Security.
Our Primary ID/Access Technology vendors
Prime was responsible for entire installation

- Access Control System
- Smart Card Readers
- Smart Card Printers
- ID Badge software changes
- Card Stock
- Lamination, Film
Access Control System

Johnson Controls
1757 Tapo Canyon Road
Simi Valley, CA 93063
Tel: (805) 522-5555
Fax: (805) 582-7888
Non-Biometric Readers

Integrated Engineering – USA
PO Box 32
Carmel Valley, CA 93924
Phone: 831 659 3218
Fax: 831 659 1009
American Association of Port Authorities  -Tacoma, WA   April 19, 2006

Smart Card Printers

FARGO Electronics, Inc.
6533 Flying Cloud Drive
Eden Prairie, MN 55344
USA