Enabling Identity Assurance

Case Study: PIV, RT, & TWIC

Biometric Consortium Conference
Standards Session

Cathy Tilton
VP, Standards & Emerging Technologies

September 12, 2007

PIV Program Overview

- Implements Homeland Security Presidential Directive (HSPD) 12
  - “Policy for a Common Identification Standard for Federal Employees and Contractors”
- NIST developed specifications
  - FIPS 201: Personal Identity Verification of Federal Employees & Contractors
    - Consists of two parts: PIV-I and PIV-II
      - PIV-I – Control and security objectives of HSPD-12
      - PIV-II – addresses technical interoperability
  - NIST Special Pubs (samples)
    - SP800-73 – Interfaces for Personal Identity Verification
    - SP800-76 – Biometric Data Specification for PIV
    - SP800-78 – Cryptographic Algorithms and Key Sizes for PIV
    - SP800-96 – PIV Card/Reader Interoperability Guidelines
Enabling Identity Assurance

Requirements

- Functional:
  - Background checks (identity proofing & registration)
  - Visual authentication
  - Automated fingerprint verification
- Achieve interoperability
- Maximize performance in terms of matching accuracy
- Maintain source image quality
  - Minimize use of compression
- Security + Privacy
- Few requirements for operational use
  - i.e., logical/physical access using the PIV card
- Facial recognition use supported, but optional

PIV – Notional Model
PIV Card data model

<table>
<thead>
<tr>
<th>Content</th>
<th>ID</th>
<th>Size (B)</th>
<th>Access</th>
<th>Interface</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Capability Container</td>
<td>0xDB00</td>
<td>266</td>
<td>Read Always</td>
<td>Contact</td>
<td>M</td>
</tr>
<tr>
<td>CHUID</td>
<td>0x3000</td>
<td>3377</td>
<td>Read Always</td>
<td>Contact &amp; Contactless</td>
<td>M</td>
</tr>
<tr>
<td>PIV Auth Cert</td>
<td>0x0101</td>
<td>1651</td>
<td>Read Always</td>
<td>Contact</td>
<td>M</td>
</tr>
<tr>
<td>Fingerprints (2)</td>
<td>0x6010</td>
<td>7768</td>
<td>PIN</td>
<td>Contact</td>
<td>M</td>
</tr>
<tr>
<td>Printed Info</td>
<td>0x3001</td>
<td>106</td>
<td>PIN</td>
<td>Contact</td>
<td>O</td>
</tr>
<tr>
<td>Facial Image</td>
<td>0x6030</td>
<td>12704</td>
<td>PIN</td>
<td>Contact</td>
<td>O</td>
</tr>
<tr>
<td>Dig Signature Cert</td>
<td>0x0100</td>
<td>1651</td>
<td>Read Always</td>
<td>Contact</td>
<td>O</td>
</tr>
<tr>
<td>Key Mgmt Cert</td>
<td>0x0102</td>
<td>1651</td>
<td>Read Always</td>
<td>Contact</td>
<td>O</td>
</tr>
<tr>
<td>Card Auth Cert</td>
<td>0x0500</td>
<td>1651</td>
<td>Read Always</td>
<td>Contact</td>
<td>O</td>
</tr>
<tr>
<td>Security Object</td>
<td>0x9000</td>
<td>1000</td>
<td>Read Always</td>
<td>Contact</td>
<td>M</td>
</tr>
</tbody>
</table>

Some decisions on biometrics use

- **On-card**
  - Biometrics are not encrypted
  - Biometrics are PIN protected
  - Biometrics are stored on contact side only (contactless access prohibited)
  - 2 fingerprint templates, 1 (opt) face image
  - Digital signature on CBEFF structure containing biometrics

- **Profiles created for all 4 INCITS standards**
  - Further constrained implementation to improve interoperability and control performance
  - Example: minutiae location/reporting

- **Certification program**
  - Includes template generators & matchers (“interoperable groups”)
Standards

Standards Usage

- **INCITS 398**: Envelope for biometric data stored on-card or retained in DB
- **INCITS 378**: Fingerprint template format for on-card storage
  - Use decided based on MINEX testing
- **INCITS 385**: Facial image format for on-card storage
  - Full frontal
  - JPEG 2000 (ROI allowed, inner ≤ 24:1), JPEG for legacy images only
- **INCITS 381**: Finger image format for retained images
  - Individual fingers + opt. slaps

**Standards**

Enabling Identity Assurance

<table>
<thead>
<tr>
<th>Standards</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCITS 378</td>
<td>Fingerprint template format for on-card storage</td>
</tr>
<tr>
<td>INCITS 385</td>
<td>Facial image format for on-card storage</td>
</tr>
<tr>
<td>INCITS 381</td>
<td>Finger image format for retained images</td>
</tr>
<tr>
<td>INCITS 398</td>
<td>Envelope for biometric data stored on-card or retained in DB</td>
</tr>
<tr>
<td>ITL 1-2000</td>
<td>INCITS 381, JPEG2000</td>
</tr>
<tr>
<td>NFIQ, WSQ</td>
<td>INCITS 398</td>
</tr>
<tr>
<td>EFTS App F</td>
<td>INCITS 385, JPEG2000</td>
</tr>
<tr>
<td>EFTS App F, single finger</td>
<td>INCITS 378, JPEG2000</td>
</tr>
</tbody>
</table>
Standards Usage (cont’d)

- ANSI/NIST ITL1-2000
  - Finger image format for background checks (Slaps: Type-14 / Rolls: Type-4)
- EFTS, App F
  - Tenprint capture device certification
  - Mod for single-finger devices for physical/logical access
- NISTIR 7151 (NFIQ)
  - Fingerprint quality checks at registration
- IAFIS-IC-0110 (V3): WSQ
  - Compression of finger images

CBEFF Structure

- PIV defined their own “Patron Format” & Signature Block

<table>
<thead>
<tr>
<th>HEADER (SBH)</th>
<th>BIOMETRIC DATA BLOCK (BDB)</th>
<th>SIGNATURE (SB)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIV header (800-76, Sec 6)</td>
<td>INCITS *</td>
<td>PIV specific (FIPS 201, 4.4.2 SP800-78)</td>
</tr>
</tbody>
</table>
Profiling example – INCITS 378

- Two fingers per BDB (single CBEFF structure)
- No extended data
- Rules for reporting minutiae type, direction
- Quality algorithm & calculation for multiple samples
- Mandatory use of optional fields (non zero fill)
  - e.g., product ID
- Record size limits

Registered Traveler (RT)
Enabling Identity Assurance

RT Program Overview

- A privilege program that expedites the passage of travelers through participating airports
- Uses smart cards and biometrics to assure a person’s identity at the airport
- Participation requirements enrollment with a Service Provider
- TSA will perform a Security Threat Assessment
- A Central Information Management System (CIMS) will
  - Ensure interoperability across Service Providers
  - Generates the biometric templates for the RT card
  - Digitally signs the authentication data on the RT card
  - Maintains and propagates the CRL
- RT is a public/private partnership
- Fully fee funded

Requirements

- Interoperability among service providers
- Reliable biometric verification at security checkpoints
- Iris capture/use at traveler discretion (SPs must support)
- Facial image not intended for use in automated facial recognition
- Biometric support for identity proofing/vetting
  - Deduplication
  - Security Threat Assessment (STA)
- Verification FRR <= 1% at a FAR of 1%
- Card size/space constraints
Enabling Identity Assurance

RT Process

Pre-Enrollment (Optional)
- Provide biographic information
- Pay fees
- Receive instructions

Capture Biographics
- Enter biographic data
- Verify correct pre-enrollment data

Identity Proofing
- Scan identity documents
- Validate I-9 documents

Identity Investigation
- Biometric duplicate checks
- Criminal history checks
- Name based checks

Capture Biometrics
- Capture ten fingerprints
- Capture iris (optional)
- Capture photo (not to be used for verification)

Vetting Complete
- Delete biographic data
- Generate templates
- Sign card data

Card Issuance
- Produce card
- Provide to traveler

Operational Usage
- Traveler presents card at airport

Capture Biometrics
- Ten fingerprints
- Iris (optional)
- Photo (not to be used for verification)

RT Interoperability Specification

- Developed by the RTIC (approved by TSA)
  - 68 Airports/Airport Authorities
  - 47 Service Providers
- Objective
  - Develop the common set of technical standards and processes necessary for an open, secure and industry-driven RT program
- Joint process – Government & Industry
  - War room environment

Spec publicly available: http://www.rtconsortium.org/
Enabling Identity Assurance

RT distributed processing

Airport 1
- EP1
- VP1

Airport 2
- EP2
- VP2

5 SPs registered, 2 opnl
14 sponsors (3@JFK)

CIMS
- Quality/validity checks
- De-duplication
- Template generation
- Payload creation/signing
- Revocation mgmt

AFIS
DB
CA

TSA

STA
Adjudication
Revocation

Relationship to PIV

- RT spec leverages PIV spec
- Differences:
  - RT participants do not use PINs
  - RT participants will optionally use iris to authenticate themselves
  - The RT card contains up to 4 fingerprint templates
  - Initially, the RT spec supports contact only
  - The RT card is not a federal credential
- Similarities:
  - RT uses the same fingerprint capture and quality management methods
  - RT uses the same PIV card edge interface
  - The RT spec allows the RT app to co-reside with PIV apps if necessary
Enabling Identity Assurance

RT card data model

<table>
<thead>
<tr>
<th>Content</th>
<th>Size (B)</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTUID</td>
<td>1410</td>
<td>Read Always</td>
</tr>
<tr>
<td>Fingerprint I</td>
<td>2004</td>
<td>Mutual Authenticate</td>
</tr>
<tr>
<td>Fingerprint II</td>
<td>2004</td>
<td>Mutual Authenticate</td>
</tr>
<tr>
<td>Iris Biometrics</td>
<td>8008</td>
<td>Mutual Authenticate</td>
</tr>
<tr>
<td>Facial Image</td>
<td>17104</td>
<td>Mutual Authenticate</td>
</tr>
<tr>
<td>Personal Data</td>
<td>74</td>
<td>Mutual Authenticate</td>
</tr>
<tr>
<td>RT Preferences</td>
<td>8</td>
<td>Read Always</td>
</tr>
<tr>
<td>ICAO Security Object</td>
<td>1504</td>
<td>Read Always</td>
</tr>
</tbody>
</table>

Some decisions on biometrics use

- One size does not fit all
  - Multiple modalities broadens potential user base
  - Requires additional container, different container sizing
  - Challenge for iris storage – size constraint + interoperability – led to selection of segmented polar format
  - 4 fingerprints reduces transactional FRR
- PINs are not operationally practical for the traveling public
  - Too frequently forgotten
  - Add to throughput time
- Protection mechanisms:
  - Signature at container level (ICAO approach)
  - Mutual authentication (symmetric key) to read
    - Held in HSMs at verification stations (kiosks)
### Standards

- **Enabling Identity Assurance**

**CIMS**
- TSA
- STA
- Adjudication
- Revocation

- **ITL 1-2000/7**, **NFIQ**, **WSQ**
- **GJXDM**
- **INCITS 385**, **ISO 19794-6 (R)**
- **JPEG2000**, **JPEG**
- **EFTS App F**

- **INCITS 378**
- **ISO 19794-6 (P)**
- **INCITS 385**
- **INCITS 398**

- **5 SPs registered, 2 opnl**
- **14 sponsors (3@JFK)**

### Biometrics/standards used in RT

- **Fingerprints**
  - Ten slap prints at enrollment
  - Submitted as ANSI/NIST ITL1-2000 Type-14 XML records*
  - Four fingerprints on RT card - INCITS 378-2004

- **Iris**
  - Optional capture of two irises
  - Rectilinear format for enrollment and storage at CIMS
  - Submitted as ANSI/NIST ITL1-2007 (draft) Type-99 XML records*
  - ‘Unsegmented’ polar image format for RT card
  - Compliant with ISO/IEC 19794-6:2005

- **Face**
  - Captured at enrollment
  - ANSI INCITS 385-2004, basic format
  - Submitted as ANSI/NIST ITL1-2007 (draft) Type-99 XML record*
  - Stored on card, NOT used for authentication!

* binary data is base-64 encoded
Enabling Identity Assurance

Standards usage

- Defined in RTIC Interoperability Specification
- Enrollment requests
  - XML messaging
  - Based on GJXDM & ANSI/NIST ITL1-2007 – Neither completed at the time!
    - Some deviations with final versions (i.e., NIEM) therefore exist
- CBEFF
  - Used modified PIV patron format
    - FASC-N & Validity period not used (zero filled)
    - No security block (redundant)
- Iris formats
  - Rectilinear at enrollment
  - Segmented polar on card
  - Quality extensions
- Profiles
  - Leveraged PIV where possible (i.e., INCITS 378)
  - RT specific profile of 19784-6

Factors

- Need for iris (and face) sample quality standards!
  - Becomes critical in a heterogeneous, multi-provider, distributed environment
- Card size constraints drive many biometric decisions
  - e.g., interoperable iris format
- Privacy considerations are critical
  - Drives protection mechanisms/schemes and many other design decisions
RT Kiosks

Transportation Worker Identification Credential (TWIC)
TWIC Program Overview

- Multi-phase program
  - Current focus on maritime operations
  - Joint TSA/Coast Guard initiative
- Goals:
  - Positively identify authorized individuals who require unescorted access to secure areas of the nation’s maritime transportation system;
  - Determine the eligibility of an individual to be authorized unescorted access to secure areas of the maritime transportation system;
  - Enhance security by ensuring that unauthorized individuals are denied unescorted access to secure areas of the nation's maritime transportation system; and,
  - Identify individuals who fail to maintain their eligibility qualifications after being permitted unescorted access to secure areas of the nation's maritime transportation system and revoke the individual's permissions.

Applications

- App1 = PIV
- App2 addresses maritime operational use
  - Final specification not yet published!
  - National Maritime Security Advisory Committee (NMSAC) chartered to develop contactless biometric/reader specification
  - Existing standards determined “not suitable for application in the maritime environment”
- Considerations
  - Operational environment
  - Cost to port operators (including small/vessel operators)
  - Privacy considerations
  - Key management
  - Throughput
- Compatibility with the ILO Seafarer’s ID was also considered
**TWIC Process**

1. Sponsor
2. Transportation Workers
3. Enrollment Centers
4. Identity Management System (IDMS)
5. Card Production Facility
6. Database Queries
   - 1:n biometric search
   - Name-Based Terrorist-Focused Risk Assessment
   - Office of National Risk Assessment (ONRA)
7. Transportation Workers
8. Local Facilities

**Requirements**

- Support for all MARSEC levels
- Fixed and portable, network connected & standalone readers
- Contactless operation
- No covert read of biometric
- PIV compatible
- Outdoor operation
- Support use for physical access control
- 3 second transaction time
- 1% EER (3 attempt FRR)
- Preference for liveness detection
**TWIC data model**

<table>
<thead>
<tr>
<th>Content</th>
<th>Size (B)</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsigned CHUID</td>
<td>64</td>
<td>Read Always</td>
</tr>
<tr>
<td>TPK (contact only)</td>
<td>40</td>
<td>Read Always</td>
</tr>
<tr>
<td>Signed CHUID</td>
<td>3000</td>
<td>Read Always</td>
</tr>
<tr>
<td>Cardholder Fingerprints (encrypted)</td>
<td>2500</td>
<td>Read Always</td>
</tr>
<tr>
<td>Security Object</td>
<td>920</td>
<td>Read Always</td>
</tr>
</tbody>
</table>

**Some decisions on biometrics use**

- No PINs
- Biometric verification via ISO 14443 contactless interface
- Encrypted biometrics on contactless side
  - Basic access control via mag stripe, contact interface, or central site
  - Card unique keys
- No face on contactless side – just fingerprint templates
- Support both PIV & TWIC card apps (modes), selectable
- Allow for “operational biometrics”
  - Not stored on card
  - Addressed in local operator’s security plan
Enabling Identity Assurance

Operational use – physical access control

Standards usage

- Same as PIV, plus:
  - INCITS 383: Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers
  - INCITS 378 & CBEFF on contactless side (TWIC app)
## Comparison

<table>
<thead>
<tr>
<th>Program</th>
<th>Modes</th>
<th>Qty</th>
<th>Encry</th>
<th>Sign</th>
<th>Interface*</th>
<th>Prot. Mech.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIV</td>
<td>FP-temp Face</td>
<td>2-4</td>
<td>N</td>
<td>Y</td>
<td>C (C/L future)</td>
<td>PIN</td>
</tr>
<tr>
<td>RT</td>
<td>FP-temp Iris-polar Face</td>
<td>2-4</td>
<td>N</td>
<td>Y</td>
<td>C (C/L future)</td>
<td>Mut. Auth.</td>
</tr>
<tr>
<td>TWIC</td>
<td>FP-temp Face</td>
<td>2</td>
<td>Y</td>
<td>Y</td>
<td>C/CL</td>
<td>BAC/TPK**</td>
</tr>
<tr>
<td>ePass</td>
<td>Face (opt) Iris (opt)</td>
<td>1</td>
<td>N</td>
<td>Secty Obj.</td>
<td>CL</td>
<td>BAC/ Mut. Auth.</td>
</tr>
</tbody>
</table>

* C=contact, CL=contactless  
** BAC=Basic Access Control; TPK=TWIC Privacy Key

## CBEFF format evolution

- **INCITS 398 Patron Format A**
  - Basis of
  - Used by PIV Patron Format
  - Profiled by RT variant
  - Used by TWIC
Conclusions

- Specific program requirements drive selection and use of standards
- Even similar type programs (e.g., credentialing) frequently have different needs
- Use of standards can support interoperability needs
- Standards typically require tailoring (profiling) for use in a particular environment/domain of use
- Some standards are becoming “standard” (at least in the US)
  - i.e., INCITS 378, 385
  - “Piggyback effect”: Once one big program makes the investment, others follow suit and reuse designs

Conclusions (cont’d)

- Law enforcement & non-law enforcement communities have different sets of standards
  - Many programs require both (i.e., law enforcement for background checks & others for other functions)
  - These are becoming somewhat more compatible over time (e.g., Type-99 record)
- Timing/availability of standards/revisions influence selection/use
  - PIV warning regarding revisions:
    - “…revisions are irrelevant to PIV; however implementations should respect the version number…”
  - RT use of draft ITL1-2007 (Type-99, XML)
Enabling Identity Assurance