Biometric Use Case Models for Personal Identity Verification

Walter Hamilton
International Biometric Industry Association
& Saflink Corporation

Smart Cards in Government Conference
Arlington, VA
April 19, 2006

IBIA International Biometric Industry Association

FIPS 201 Biometric Requirements

- Ten fingerprint images are captured at enrollment
  - Sent to FBI for criminal history records check
  - Fingerprint capture device must comply with FBI standards
  - Strict image quality guidelines must be met for enrolled images
  - Images are used to generate templates for PIV card
- Biometric templates stored on PIV card are required for interoperability of PIV authentication between agencies
  - Mandatory storage of minutiae templates from two index fingerprints
  - Alternative fingers are allowed if index fingers cannot be imaged
  - Templates generated by segmenting images from 10-print enrollment

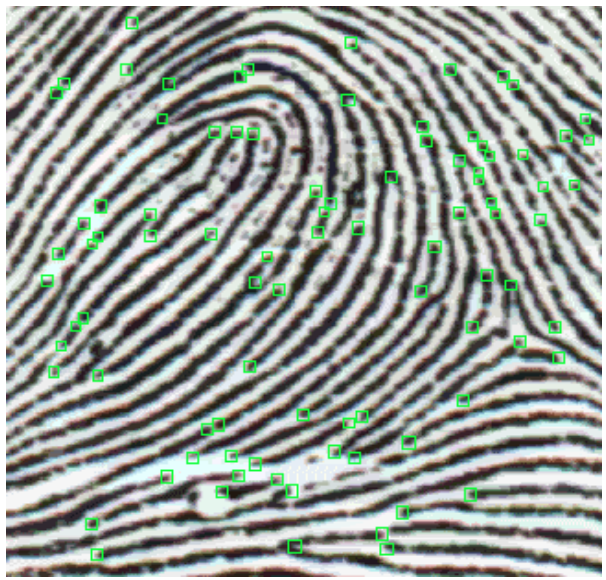
Discussion will focus on operational use of biometric for authentication

Biometrics in FIPS 201

- FIPS 201-1 – *Standard for Federal Personal Identity Verification (PIV)*
- SP 800-73-1 - *Technical Specification and Interfaces for PIV Card*
- **SP 800-76 - *Biometric Data Specification***
- SP 800-78 - *Cryptographic Algorithms and Key Sizes*
- SP 800-79 - *Guidelines for Certification and Accreditation of PIV Card Issuing Organizations*
- SP 800-85 - *Guidelines for Conformance Testing of PIV Middleware and PIV Card Application*
- SP 800-87 - *Codes for Federal and Federally-Assisted organizations*

Fingerprint Minutiae Template

- Maps the points where ridges start/stop or branch
- NIST standard data format based on ANSI/INCITS 378 Fingerprint Minutiae Data Interchange Standard
  - Defines specific format option called “MIN A”
- Fraction of the size of compressed images (<1K)



IBIA International Biometric Industry Association

SP 800-76

Sec. 1.2 states: …..for both logical and physical access applications, and for applications using biometric data stored either on or off the PIV Card, this document neither requires nor precludes the use of:

1. The PIV Card fingerprint templates;
2. Specific authentication paradigms such as match-on-card;
3. Data from other biometric modalities (e.g., hand geometry, iris, etc.);
4. Data formatted according to other standards;
5. Data whose format is proprietary or otherwise undisclosed.

SP 800-76 (cont.)

- Alternative biometric modalities and/or paradigms may be used for ***intra-agency*** authentication under FIPS 201
  - Such implementations may not be interoperable with other agencies
- Alternative biometric modalities could include fingerprint, hand geometry, iris, face, etc.
- Alternative biometric paradigms could include
  - Store biometric template off card
  - Store biometric template on card in agency-specific container
  - Match on card
  - Etc.

Access to Standard Template is Restricted Under FIPS 201

- Interoperable fingerprint templates can ***only*** be read through the ***contact*** interface following ***entry*** of a ***PIN***
- However, the card holder unique ID (CHUID) ***can*** be read from the ***contactless*** interface and ***without*** a ***PIN***
- Use of contact readers and PIN entry may not be appropriate for some physical access control systems (PACS) due to throughput requirements
- Use of contact readers in environments exposed to the weather may not be practical

IBIA International Biometric Industry Association

Biometric Use Case Models for Physical Access

IBIA International Biometric Industry Association

Match Off Card to Standard Fingerprint Template Stored On Card

- Insert card in contact reader
- Enter 6-digit PIN
- Scan fingerprint of cardholder
- Read templates from PIV card
- Match template off card to template stored on card
  - Matching takes place in reader, panel or server

Plus: Any PIV card will work
No need for biometric network or external database

Minus: Slower throughput
Card wear & exposure to dust, moisture, etc.
Limited to fingerprint biometrics using standard template format

IBIA International Biometric Industry Association

Match Off Card to Alternative Biometric Template Stored Off Card

- Read CHUID through contactless interface
- Scan biometric of cardholder (could be any biometric)
- Match live template off card to template stored off card
  - CHUID is index pointer to stored template
  - Templates stored in reader, panel or server
  - Matching takes place in reader, panel or server

Plus: Faster throughput
Choice of biometric modalities & template formats
Any PIV card will work
Contactless reader eliminates wear & environment issues

Minus: Requires network and external database
Requires separate biometric enrollment to external database

IBIA International Biometric Industry Association

Match Off Card to Alternative Biometric Template Stored On Card

- Read biometric on card through contactless interface
  - Template stored in agency-specific container on PIV card
- Scan biometric of cardholder (could be any biometric)
- Match live template off card to template stored on card
  - Matching takes place in reader, panel or server

Plus: Faster throughput
Contactless reader reduces wear & weather concerns
No need for biometric network and external data base

Minus: Requires separate biometric enrollment on PIV card
Issue of writing biometric to card issued by other agencies

IBIA International Biometric Industry Association

Match On Card to Alternative Biometric Template Stored On Card

- Insert card in contact reader or present card to contactless reader
- Scan biometric of cardholder (could be any biometric)
- Match live template on card to template stored on card
  - Template stored in agency-specific container on PIV card
  - Matching takes place within logic of smart card

Plus: No PIN entry required
No need for biometric network and external data base
Enrollment template never leaves PIV card

Minus: Requires separate biometric enrollment on PIV card
Issue of writing biometric to card issued by other agencies
MOC currently limited to proprietary templates

IBIA International Biometric Industry Association

Biometrics for Logical Access

Network Authentication

- FIPS 201 defines PKI as the required authentication method for logical access
- PKI requires contact interface and PIN entry to exercise private key for cardholder authentication
- Biometrics could be an additional authentication factor for very high security environments
  - 3-factor authentication – PIV Card, PIN and biometric

Network Authentication (Cont.)

- Biometrics as an additional authentication mechanism for logical access could be implemented in any paradigm or modality
  - Finger, face, iris, hand, etc.
  - Match on card, Match off card
  - Store on card, store off card
- Since PKI is mandated for logical access, the only advantage to using biometrics is additional security
  - No convenience or throughput benefits

IBIA Recommendations to NIST

For Physical Access Control Applications:

- Remove PIN requirement for reading interoperable fingerprint templates on PIV card
- Allow access to interoperable fingerprint templates through the contactless interface

If recommendations adopted, would further encourage the operational use of interoperable biometrics to meet HSPD-12 objectives for interoperability, security and rapid authentication

IBIA International Biometric Industry Association

Rationale for Recommendations

- Physical access control not well suited for contact cards due to environmental and throughput issues
- NIST removed PIN requirement for access to certificate in SP 800-73-1
  - Rationale: Privacy issues no longer considered significant
- A similar privacy rationale exists for fingerprint templates
  - Minutiae templates cannot be used to reconstruct the original image
  - Are fingerprints “secrets” anyway?
- Compromised enrollment template is of little use
  - No practical way to introduce the template back into the system
  - Physical finger must be in contact with the reader for authentication
  - Enrollment templates are digitally signed with a “type” designation
  - Attempting to send an enrollment template as a verification template would be rejected as an invalid data object

Conclusions

- FIPS 201 allows a lot of flexibility in implementing biometric authentication for intra-agency access control
- Given restrictions on use, interoperable templates may only be practical for use at visitor control centers to bind a visiting agency employee to the PIV card
- Consider the use of alternative biometrics – particularly for physical access control systems

Contact Information

International Biometric Industry Association
1666 K Street, NW - Suite 1200
Washington, D.C. 20006
Tel (202) 293-8133
Fax (202) 503-0985
ibia@ibia.org
www.ibia.org

Walter Hamilton
Saflink Corporation
Tel (425) 503-0985
whamilton@saflink.com
www.saflink.com

IBIA International Biometric Industry Association