Revisions to the PIV Biometrics Specifications

DRAFT FIPS 201-2 WORKSHOP APRIL 18 + 19, 2011

patrick.grother@nist.gov



Image Group, Information Access Division National Institute of Standards and Technology US Department of Commerce

Agenda

- 1. Preamble
- 2. Iris
- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. What's in, out, and next steps

Part 1: Preamble

http://biometrics.nist.gov/76.pdf

Draft 800-76-2 released April 17, 2010

Posting to the SP register is imminent http://csrc.nist.gov/publications/PubsSPs.html

PIV :: Documents Hierarchy



NIST SP 800-76 Lineage

- Prior: "-0
 - "-0" on 2006-02-01 27 pages
 - Current: "-1" on 2007-01-25 33 pages
- Draft:

- "-2" on 2011-04-17 61 pages
- Draft Out for public comment
- <u>http://biometrics.nist.gov/76.pdf</u>
- http://csrc.nist.gov/publications/PubsSPs.html



1. Preamble

2. Iris

- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. Next steps



Change #1 :: Iris for PIV :: Why/How

The problem

Fingerprints sometimes do not work

Some people are difficult to image (dry skin)

Permanent damage to fingers

Temporary damage to fingers

Non-habituated users

Poor quality control during enrolment (?)

One solution

Add iris to PIV

Iris image on the card

Iris image off the card (CMS)

Support with specifications

For minimum accuracy requirements

For tests of algorithms

For tests of cameras

For interfaces to cameras

For interfaces to recognizers

Conformance tests

Change #1 :: Iris for PIV :: Context

The PIV Context

Iris is required for cardholders for whom fingerprint authentication during issuance fails Iris as fallback modality

The consequences

Requires purchase of camera and ancillaries Capital cost Variable costs(?) Presence of iris equipment extends a new option for operational authentication Attended Unattended PACS + LACS

SZ SZ SZ 5 Z

Change #1 :: Addition of iris :: Data format



Parent image from camera

Type 1 or 2

Not storing / sending / requiring templates

Proprietary, non-interoperable, laden with intellectual property, sometimes larger than the image itself



Cropped and masked image

Standard defines interoperable images

ISO/IEC 19794-6:2011

Type 7 On Card with JPEG 2000 Type 2 Off Card with PNG or RAW

US Registry of Biometric Standards recommends these.

Tested in IREX I

http://iris.nist.gov/irex



Change #1 :: Iris for PIV :: Implementation

Following the arrangement of fingerprint minutia data on current PIV cards... Two irises in one container.



2.65M cards issued 07/2009

- 1. Preamble
- 2. Iris
- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. Next steps

Part 3: Match-on-Card

Change #2 :: Addition of MOC :: Background

MINEX II

Accuracy and speed of card-based algorithms

P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, MINEX II Performance of Fingerprint Match-on-Card Algorithms Phase

II / III Report NIST Interagency Report 7477

Three editions, 2008, 2009 and 2011

Contact: patrick.grother@nist.gov

sBMOC "Secure Biometric Match-on-Card"

Demonstration of secure protocols for biometric authentication.

D. Cooper, H. Dang, P. Lee, W. MacGregor, and K. Mehta. Secure Biometric Match-on-Card Feasibility Report. NIST Interagency Report 7452, November 2007.

Contact: william.macgregor@nist.gov



Change #2 :: Addition of MOC :: Why / When

The problem

PIN release of a biometric is

time consuming PINs are sometimes forgotten, and committed to paper

well motivated: PIN protects biometric from free-read (e.g. after Card loss)

The proposed solution

- Allow on-card comparison
 - for authentication after PIN for card activation no PIN, prohibit release of current card templates

Change #2 :: Addition of MOC :: How

The PIV implementation

Four ISO/IEC 19794-2:2011 templates

Primary + secondary finger with plain-impression sensor AND swipe sensor

Use 7816-4, 7816-11

No extensions

Not standardized ones, and Not proprietary ones either

The consequences

- Cannot use the existing PIV Cards directly.
 - Needs ISO/IEC 19794-2 "compact card" templates
 - Client-side issuance software effects conversion.
- MOC is agency-optional
 - Requires cards with on-board matcher
 - Contact + contactless with cryptographic protection

Secure Session

- 1. Preamble
- 2. Iris
- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. Next steps

Part 3: Swipe Sensors

Change #3 :: Swipe Sensors :: Drivers

The problem

Fingerprint sensors exist on many PCs today, why the need to add "PIV-certified" sensors?

Answers: Performance, Interoperability

Plain-impression "area" sensors are more expensive





A solution

Allow swipe sensors **Reduced cost** For authentication against enrolled swipe data With qualification criteria **Restrict domain-of-use** Use with MOC only Logical access only? Not in attended operations (issuance, re-issuance etc) Not with mandatory PIV templates

Change #3 :: Swipe Sensors :: Input Needed

Specific caveats

Little empirical data on which to safely include swipe matching into PIV. Swipe is attractive on grounds of cost, and possibly on grounds of spoof resistance. Specific request for comment swipe accuracy and viability interoperability with opticallyderived templates operating with standardized minutia templates operational experiences liveness

Possible ways forward

- All swipe-related specifications may be withdrawn in the next version of this draft.
 - Defer until quantitative evidence is available

Swipe goes forward as drafted

But no implementation passes the mandated performance test.

- 1. Preamble
- 2. Iris
- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. Next steps

Part 5: Minimum Accuracv Specifications

Change #4 :: Minimum Accuracy :: Why

The problem

800-76-1 established interoperability criteria for fingerprint minutia equipment

> FRR ≤ 1% when FAR ≤ 1% for ALL template generators and matchers

BUT

FAR of 1% is non-operational (but fit-for-purpose nevertheless)

The backdrop

FIPS 201 does not establish agency biometric security requirements of biometric match

But FIPS 140-2 does!

Motivation for six digit PIN in PIV today FIPS 140-3 is under development

Change #4 :: Minimum Accuracy :: How

The specifications

Establish minimum security requirements

By requiring false match rates be less than X.

Agency optional on whether FMR < X or FMR << X per

> Agency requirements Application requirements

For all modalities

Iris

On-card comparison Off-card comparison

The mechanism

Algorithm tests exist within PIV today FMR objective is achieved by setting a calibrated threshold

Threshold calibration is a byproduct of existing NIST tests Not specifying FRR

- 1. Preamble
- 2. Iris
- 3. Match-on-Card
- 4. Swipe sensors
- 5. Accuracy specifications
- 6. Next steps

Part 6: Next Steps

SP 800-76-2 IS OPEN FOR COMMENT

EMAIL COMMENTS PIV_COMMENTS@NIST.GOV

BY JUNE 6, 2011

THIS IS THE SAME DEADLINE AS THE FIPS 201-2

Draft SP 800-76-2 :: In + Out

What's in

Off-card fingerprint, mandatory Iris, conditional mandatory On-card fingerprint, optional Face, optional on card, for human adjudication Swipe sensors Minimum accuracy requirements

What's not in

- Is face available for biometric authentication
- No mentioned of UUID
- No guidance on biometric update (the ageing problem)
- New biometric standards
 - INCITS 378:2009 minutia templates ISO/IEC 19794-2 for off-card minutiae ISO/IEC 19794-5:2005 or 2011 face
- Other modalities
 - Vein, Face (automated FR), Hand Geometry, etc.