Revisions to the PIV Biometrics Specifications

FIPS Updates and SP 800-76-1 → SP 800-76-2

PIV Workshop, NIST
July 25, 2012

patrick.grother@nist.gov

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

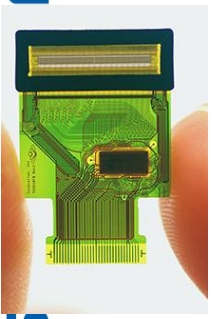
SP 800-76-2 Progression

- Comments received
  - **Approx. 274 comments**
  - **Approx. 22 organizations**
  - **Many thanks**

Swipe Sensors

Comment

- Swipe sensors
  - **much lower in cost than plain impression area sensors**
  - **important enabler for mobile apps on tablet, laptop, smart phone etc.**
  - **can be packaged more efficiently in mobile devices**
  - **much less battery power**



- Swipe is non-interoperable
- Should be tested

Background

- Most swipe deployments
  - **Swipe – swipe matching**
  - **Use proprietary templates, not standardized templates**
  - **Use with habituated population**

Response

- Disallow use of swipe sensors
- Remove all swipe specifications

Rationale

- HSPD 12 mandates global interoperability
- Systematically different deformation of skin than plain sensors. This hurts interoperability.
- Image must be reconstructed to given linear motion estimates
- Reduced imaging width vs. plain
- Accuracy already degraded by use of standardized templates (vs. images)

Face for Biometric Authentication

Comment

- Use face as an alternative to iris when fingerprint is difficult or impossible

Background

- PIV has required collection of digital face since 2005
  - **Standardized INCITS 385**
  - **Passport-equivalent**

- Face is used in automated border crossing (ABC) gates with read from e-Passport

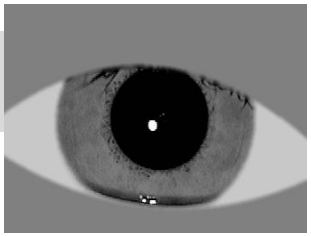
Response

- Face **shall** be stored on PIV Card
- Face available for automated authentication in operator-attended PIV Card maintenance procedures.

Rationale

- Many agencies already store the INCITS 385 face image on the PIV card
- Face recognition is influenced by capture environment and PIE.
- Face implementations are vulnerable to low-cost spoof attacks

Iris Optional or Mandatory?



Comment

- Is iris mandatory?
- Is iris mandatory only when fingerprints cannot be collected?
- It's expensive
- Please clarify

Response

- Iris is optional
  - **At an agency's discretion**
  - **For general purpose authentication**
  - **Per specifications of SP 800-76-2**

Background

- Iris has been proposed to reduce the population of federal workers for which no biometric is available
- Some fraction of federal workers cannot submit or authenticate with fingerprints alone

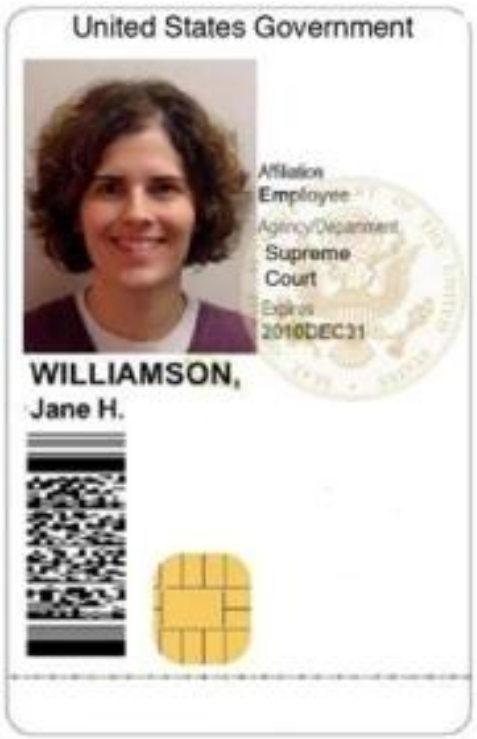
Rationale

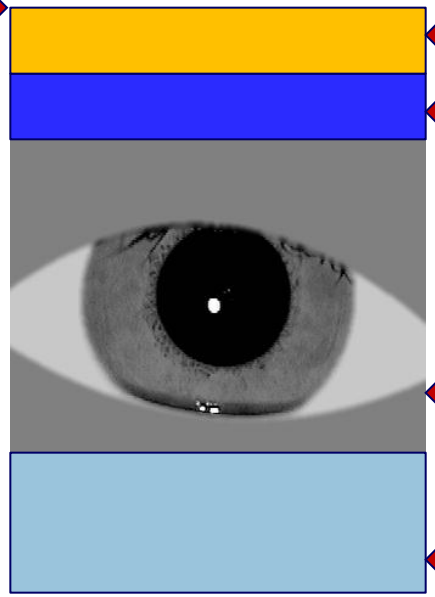
- Mandatory collection of iris, or mandatory use of iris when fingerprints could not be collected, would have required each enrollment office to install an iris camera and ancillary software

Irises on PIV Cards

Following the arrangement of fingerprint minutia data on current PIV cards… One or two irises in one container.

Tagged biometric container (SP 800-73)





CBEFF Header — =88 bytes

ISO Iris Image Header — ≥107 bytes

ISO Iris Image Data — ~ 3KB 1 eye

CBEFF Signature block — ~ 500 bytes

2.65M cards issued 07/2009

Other Modalities

Comment

- [FIPS 201] … should allow PIV issuers to choose an alternative biometric authentication method + store related data in the PIV card.

Background

- Other modalities
  - **are commercially available**
  - **vary in cost, speed, accuracy, maturity, resistance to active attack, support from multiple providers, standardization, interoperability, and demonstrations of these properties**

Response

- Allowed in the PIV application
  - **Fingerprint minutiae**
  - **Iris images**
  - **Face images**
- Agencies are free to
  - **Use other modalities elsewhere on card**

Rationale

- High performance and global interoperability requires
  - **Standardized data**
  - **Commercial support**
  - **Assurance of accuracy e.g. via testing**

On-card Comparison == Match-on-Card

Comment

- Continue use of “match on card” and “MOC” in existing and new industry specifications.
- “match on card” is more generally accepted recognizable in the biometric industry.
- Unnecessary to introduce a new and potentially confusing term such as ‘on card comparison’ (OCC)
- ‘match on card’ is not trademarked and freely open for use.

Background

- ISO/IEC 19795-7:2010 — Biometric performance testing and reporting —Testing of on-card biometric comparison algorithms
- ISO/IEC 24787-1:2010 used on-card comparison and will use on-card biometric comparison
- Fingerprint is the only modality in PIV and commercially for which OCC is mature.

Response

- FIPS 201-2 uses on-card biometric comparison and “OCC”
- NIST SP 800-76-2 uses
  - **On-card comparison**
  - **Fingerprint on-card comparison**
  - **On-card biometric comparison**

Rationale

- Harmonization with published standards
- The term “matching” is deprecated in vocabulary standards in favor of “comparison”
- What’s in a name!?

On-card Biometric Comparison Interface

Comment

- Allow contactless operation
- Modify the interface APDU commands

Background

- Testing interface used in MINEX II
  - **Has un-needed aspects**
  - **Is overly prescriptive**
  - **Includes no confidentiality protection**
  - **Does not include any mutual authentication**
- sBMOC demonstrated secure protocols

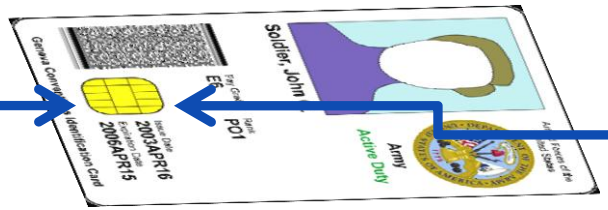
Response

- Remove draft interface from SP 800-76-2
- Produce definitive interface in upcoming SP 800-73-4
- Data objects remain in 800-76-2

Rationale

- 800-73 is the proper home of interface specifications

Reference Template: sent via PUT DATA



Verification Template sent via VERIFY

Biometric Accuracy Specifications

Comment

- Explain role of existing PIV accuracy requirements. Existing (1%,1%) qualification is being misconstrued as mandate on operational systems
- The false match requirements are too strict

Background

- Accuracy (FMR ≤ 1%, FNMR ≤ 1%) mandated in 2005 in SP 800-76.
  - **Solely for purposes of qualifying fingerprint minutia generators and matchers**
  - **Applied for ALL interoperating pairs algorithmA – algorithmB**
  - **Two fingers**
- Necessary because minutiae were required vs. images.

Response

- FMR ≤ 0.001 (1 in 1,000)
  - **Single finger (on and off-card) + Face**
- FMR ≤ 0.00001 (1 in 100,000)
  - **Iris**
- i.e. single-attempt maximum one-to-one false match rates
- Achieved via threshold calibration, enforced by vendor attestation
- No specifications on false rejection

Rationale

- USG interest is in thwarting illegitimate impostor attempts
- Effective false acceptance rates depend on compromise of PIN, the biometric data, active attacks

Number of Fingers

Comment

- For MOC, do not limit the maximum number of fingers … allow 10 … support beyond the Federal market.

Background

- Some implementations do not prompt for a specific finger
- Instead 1:10 "identification mode"
  - **Index of the matching finger can indicate a role e.g. duress.**
- False rejection rates decrease with more fingers.

Response

- Maintain required storage of primary and secondary fingers
- Aside: Remove handedness bias
- Aside: Move finger order specifications from FIPS 201 to SP 800-76

Rationale

- A card running in 1:N mode and populated with 10 fingers will see false acceptance rates increase by a factor ~10 vs. single finger

Proprietary Data

Comment

- Accuracy can be improved by proprietary data
  - **Placed in standardized "extended data" records**

Response

- Fingerprint minutia templates remain purely standardized. Proprietary extensions are not allowed.

Background

- FP minutia standard includes block for arbitrary trade-secret biometric feature data
- Proprietary data
  - **offers better accuracy than standardized data, equivalent to "image-based" biometrics**
  - **Is non-interoperable**
  - **Is larger (slower to read)**
- "Vendor lock-in" potential

Rationale

- Risk: Agency becomes "dependent" on proprietary extensions because standardized part of the data is made to be syntactically correct but ineffective for matching.
- Proprietary extensions would be acceptable IF strong conformance and performance testing was possible on the deployed implementation (vs. that submitted to a lab test).

New Biometric Data Standards

Comment

- There are newer biometric data interchange standards
- Migrate from
  - **INCITS 378 minutiae to ISO/IEC 19794-2**
  - **INCITS 385 face images to ISO/IEC 19794-5**
  - **INCITS 381 finger image to ISO/IEC 19794-4**

Background

- Early US standards from INCITS M1 vs. subsequent ISO standards from SC37
- Multiple / competing standards “on the books”

Response

- Continue use of INCITS 378:2004
- Continue use of INCITS 385:2004
- Continue use of INCITS 381:2004

Rationale

- INCITS standards fit for purpose, no serious flaws, functionally equivalent

Testing of Minutia Generators + Matchers

MINEX 2004 - 2012

- MINEX I
  - **Find interoperable group for which (FMR ≤ 1%, FNMR ≤ 1%)**
  - **Adopted by GSA for Approved Products List**
- MINEX II
  - **Demonstrated OCC accuracy can approach off-card matching accuracy**

Proposed MINEX

- MINEX III
  - **Continue MINEX I as a "Level 1" interoperability specification**
  - **Establish a "Level 2" specification for measuring single-finger capability**
  - **Produce threshold calibration value to support targeting of false match rates**
- MINEX IV
  - **Implement MINEX III for OCC implementations**
  - **Measure card speed**

MINEX Minutia Exchange

PIN Release of Biometric Data

Comment

- Allow “free-read” of biometric data without prior PIN activation

Response

- Maintain prior PIN entry requirement.

Background

- PIN release implements the prior “something-you-know” factor
- Templates can be reversed. Raw or reconstructed images can be used to attack a system.
- e-Passports require BAC or EAC to allow biometric read activation.

Rationale

- Risk:
  - **Biometric data is non-revocable**
  - **Raw or reconstructed images can be used to attack a system**
- Future possible mitigation
  - **Application of mathematical “Template Protection” techniques to make non-reversible templates.**
  - **These techniques need testing!**

On-card Iris Comparison

Comment

- Do iris on-card comparison

Response

- No change: Iris shall be stored on-card and processed off-card

Background

- Image processing to find iris region in an image is too computationally intensive on-card.
- Template matching would be possible on-card
- Templates are typically < 1KB.

Rationale

- No commercial presence for on-card iris recognition
- No standard iris template
- Future possible approach
  - **Formally standardize a template, AND**
  - **Test implementations – concern that a template cannot made to be interoperable cross-provider**

Thank you

Comments due August 10

Drafts and comments template linked from

http://csrc.nist.gov/publications/PubsSPs.html

http://csrc.nist.gov/groups/SNS/piv/announcements.html