NIST Special Publication 800-76

Biometric Data Specification for Personal Identity Verification

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Charles Wilson
Patrick Grother
Ramaswamy Chandramouli

I N F O R M A T I O N S E C U R I T Y

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8940

December 15, 2005

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Michelle O'Neill, Under Secretary for Technology

National Institute of Standards and Technology
William A. Jeffrey, Director

NOTE FOR REVIEWERS

1. NIST has created this Special Publication 800-76 (SP 800-76) to specify the technical acquisition and formatting requirements for the biometric credentials of the PIV system. The SP 800-76 provides the biometric data requirements to support interoperability among government agencies.

2. Please submit your SP 800-76 comments using the comment template form provided on the http://www.csrc.nist.gov/piv-project/fips201-support-docs.html website. Please include the submitter's name and organization in the header section of the spreadsheet. This will greatly facilitate processing of comments by NIST.

3. Comments should be submitted to DraftFips201@nist.gov. It is requested that Federal organizations submit one consolidated/coordinated set of comments. Also, include "Comments on Public Draft SP 800-76" in the subject line.

4. The comment period closes at 5:00 EST (US and Canada) on January 13th, 2006. Comments received after the comment period closes will be handled on as-time-is-available basis.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-76, 32 pages

(December 15, 2005)

Acknowledgements

The authors, Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its development. Particular thanks go to R. Michael McCabe for his extensive knowledge of the FBI's requirements. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors for the continued interest and involvement in the development of this publication.

Executive Summary

The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201), was developed to establish standards for identity credentials. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It specifies technical acquisition and formatting requirements for the biometric credentials of the PIV system, including the PIV Card[1] itself. It enumerates required procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is high performance universal interoperability. For the preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint Transaction Specification.

[1] A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, biometric data) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Table of Contents

List of Tables

1. Introduction

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget (OMB), or any other Federal official.

1.2 Purpose and Scope

FIPS 201 [FIPS], Personal Identity Verification (PIV) for Federal Employees and Contractors, defines procedures for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS also defines the structure of an identity credential which includes biometric data. Requirements concerning cryptographic protection of the biometric data are also described in [FIPS].

This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV Card. This standard addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to elucidate required versus optional content. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

Thus, this document regulates various pieces of biometric data, and the processes used during and after their acquisition. This document neither requires nor precludes the use of the PIV Card templates in specific authentication paradigms such as match-on-card.

This document also provides an overview of the strategy that can be used for testing conformance to the standard. It is not meant to be a comprehensive set of test requirements that can be used for certification or demonstration of compliance to the specifications in this document.

1.3 Audience, Assumptions, and Overview

This document is targeted at Federal agencies and implementers of PIV systems. Readers are assumed to have a working knowledge of biometric standards and applications. This document covers the following specifications in the context of PIV:

- Fingerprint Enrollment — Section 3;
- Fingerprint Verification — Section 4;
- Facial Image Specification — Section 5; and
- CBEFF Structure — Section 6.

2. Terms, Acronyms, and Notation

2.1 Terms

Term	Definition
Segmentation	For fingerprints, segmentation is the separation of an N finger image into N single finger images.

2.2 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
CBEFF	Common Biometric Exchange Formats Framework
FIPS	Federal Information Processing Standard
EFTS / F	Electronic Fingerprint Transmission Specification (Appendix F)
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NFIQ	NIST Fingerprint Image Quality
PIV	Personal Identity Verification

3. Fingerprint Enrollment

The specifications in this section pertain to the PIV biometric data enrollment process. Hence, this section provides requirements for acquisitions, formatting, and storage of fingerprint images. The following is an overview of the material covered in this section.

+ Section 3.1 gives requirements for the acquisition of fingerprints for PIV registration;
+ Section 3.2 gives the format for fingerprint templates stored on the PIV Card;
+ Section 3.3 gives requirements for fingerprint images retained by agencies; and
+ Section 3.4 gives requirements for the transformation of fingerprints into records suitable for transmission to the FBI for the background check.

Note that although FBI requirements drive the sensor specifications, the permanent electronic storage formats, specified in Sections 3.2 and 3.3, are INCITS (i.e. non-FBI) standard records and are therefore specified independently.

3.1 Fingerprint Image Acquisition

This section specifies requirements for the capture of a full set of fingerprint images for PIV registration. A subject's fingerprints shall be collected according to any of the three imaging modes enumerated in Table 1.

Table 1: Fingerprint Acquisition Protocols

Option 1 - Plain live scan		
Required Presentations	1	Combined plain impression of the four fingers on the right hand (no thumb)
	2	Combined plain impression of the four fingers on the left hand (no thumb)
	3	Combined impression of the two thumbs
Option 2 – Rolled live scan		
Required Presentations	1	10 separately rolled fingers
	2	Combined plain impression of the four fingers on the right hand (no thumb)
	3	Combined plain impression of the four fingers on the left hand (no thumb)
	4	Left thumb plain impression
	5	Right thumb plain impression
Options 3 - Rolled ink on card		
Required Presentations	1	10 separately rolled fingers
	2	Combined plain impression of the four fingers on the right hand (no thumb)
	3	Combined plain impression of the four fingers on the left hand (no thumb)
	4	Left thumb plain impression
	5	Right thumb plain impression

INFORMATIVE NOTES:

1. The combined multi-finger plain impression images are also referred to as slaps or flats, and are obtained by simultaneous placement of multiple fingers on the imaging surface without specific rolling movement.
2. Options 2 and 3 represent existing agency practice. Option 1 has recently become acceptable to the FBI.

For Options 1 and 2 the devices used for capture of the fingerprints shall have been certified by the FBI to conform to Appendix F of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F). For Option 3, a scan of the inked card shall be performed to effect conversion to electronic form. The scanner shall be certified by the FBI as being compliant with [EFTS/F]. The scanning is needed to produce fingerprints in the digital format described in Section 3.3. The FBI specifications include width and height specifications for the imaging surface. The native scanning resolution of the device shall be 197 pixels per centimeter (500 pixels per inch) in both the horizontal and vertical directions. These specifications comply with the FBI submission requirements and with the Image Acquisition Setting Level 31 of the Finger Image-Based Data Interchange Format standard, INCITS 381, [FINGSTD].

The procedure for the collection of fingerprints, presented in Table 2, shall be followed. The procedure employs the NIST Fingerprint Image Quality [NFIQ] algorithm to initiate any needed reacquisition of the images. The procedure requires segmentation of the multi-finger plain impressions.

Table 2: Steps and Image Quality Assessment

Step	Action
1.	Attending official should inspect fingers and require absence of foreign material where possible.
2.	Acquire fingerprints according to Option 1, 2, or 3 in Table 1. The fingerprints acquired using Option 3 should be scanned to convert to digital form.
3.	Segment the multi-finger plain impression images into single-finger images.
4.	Compute NFIQ value for thumbs and index fingers. If all have NFIQ values of 1, 2, or 3 (i.e., good quality) then go to step 7.
5.	Repeat steps 2-4 up to three more times.
6.	If after four acquisitions the index fingers and thumbs do not all have NFIQ values of 1, 2 and 3 then select whichever repeated set has the highest number of images with qualities 1, 2, 3 or 4 and proceed to step 8 anyway.
7.	Prepare and store the final records per Sections 3.2 and 3.3.

Ordinarily, all ten fingerprints shall be imaged in this process; however, if one or more fingers are not available (for instance, because of amputation) then as many fingers as are available shall be imaged. When fewer than ten fingers are collected, the FBI background transaction of Section 3.4 requires an explanation to be reported.

3.2 Fingerprint Template Specifications

This section specifies how the PIV mandatory biometric elements specified in [FIPS] are to be generated and stored. This specification applies to templates stored within the PIV Card, and to templates otherwise retained by agencies. The templates constitute the enrollment biometrics for PIV authentication and as such are supported by high quality specifications for image acquisition and storage. The specification of a standardized template in this section enables cross-agency use of the PIV Card in a multi-vendor product environment.

3.2.1 Source Images

The fingerprint templates to be stored on the PIV Card (hereafter referred to as PIV Card template) shall be prepared from images of the primary and secondary fingers (as specified in [FIPS]). The images used in the creation of the PIV Card templates shall under normal operating procedures be obtained by segmenting the plain impressions of the full set of fingerprints captured during PIV Registration as described in Section 3.1 of this document. Under some circumstances, they may also e obtained during PIV Card issuance or re-issuance by again segmenting plain multi-finger impressions or by using single-finger plain captures of two fingers. In all cases the fingerprints shall be collected using a [EFTS/F] certified fingerprint scanner, and in accordance with acquisition modes specified in Section 3.1.

3.2.2 Minutia Record

PIV Card templates shall be conformant instances of the INCITS 378-2004 [MINUSTD] minutiae template standard. Further each finger's template record shall be individually wrapped in the CBEFF structure specified in Section 6 prior to storage on the PIV Card.

Table 3 is a profile of the generic [MINUSTD] standard. Its specifications shall apply to all minutiae templates placed on PIV Cards. These constraints are included to promote highly accurate and interoperable personal identity verification. Ideally the minutiae records should be prepared immediately after the images are captured and before the images are compressed for storage.

Table 3: PIV Minutiae Record

			Section title and/or field name	INCITS 378-2004		PIV Conformance	Informative Remarks
				Field or Content	Value Reqd	Values Allowed	
1.			Principle (5.1)	NC		A	
2.			Minutia Type (5.2)			See Note 2	5.2 contains no normative content
3.			Minutia Location : Coordinate System (5.3.1)	NC		A	
4.			Minutia Location : Minutia Placement on a Ridge Ending (5.3.2)	NC		A	
5.			Minutia Location : Minutia Placement on a Ridge Bifurcation (5.3.3)	NC		A	
6.			Minutia Location : Minutia Placement on Other Minutia Types (5.3.4)	NC		See Note 2	

			Section title and/or field name	INCITS 378-2004		PIV Conformance	Informative Remarks
				Field or Content	Value Reqd	Values Allowed	
7.			Minutia Direction : Angle Conventions (5.4.1)	NC		A	
8.			Minutia Direction : Angle of a Ridge Ending (5.4.2)	NC		A	
9.			Minutia Direction : Angle of a Ridge Bifurcation (5.4.3)	NC		A	
10.	General Record Header		Byte Ordering (6.2)	NC		A	Big Endian
11.			Minutia Record Organization (6.3)	NC		A	Unsigned Ints
12.			CBEFF Record Header (6.4)	MF	MV	Patron format A of sec. 6.	Multi-field CBEFF Header
13.			Format Identifier (6.4.1)	MF	MV	A	"FMR" with null termination
14.			Version Number (6.4.2)	MF	MV	"020\0"	i.e. INCITS 378-2004
15.			Record Length (6.4.3)	MF	MV	> 0	i.e. this connotes a 2 byte field. See Note 5
16.			CBEFF Product Identifier Owner (6.4.4)	MF	MV	> 0	See Note 6
17.			CBEFF Product Identifier Type (6.4.4)	MF	MV	> 0	See Note 6
18.			Capture Equipment Compliance (6.4.5)	MF	MV	1000b	Sensor complies with EFTS/F per PIV Registration requirement
19.			Capture Equipment ID (6.4.6)	MF	MV	> 0	
20.			Size of Scanned Image in x direction (6.4.7)	MF	MV	MIT	
21.			Size of Scanned Image in y direction (6.4.8)	MF	MV	MIT	
22.			X (horizontal) resolution (6.4.9)	MF	MV	MIT	
23.			Y (vertical) resolution (6.4.10)	MF	MV	MIT	
24.			Number of Finger Views (6.4.11)	MF	MV	1 ≤ K ≤ 3	K views, say from repeated impressions, follow. See line 17.
25.			Reserved Byte (6.4.12)	MF	MV	0	
26.	K instances of the Single Finger View Record	View Header	Finger View Header (6.5.1)	MF	MV	≥ 0	
27.			Finger Position (6.5.1.1)	MF	MV	MIT	
28.			View Number (6.5.1.2)	MF	MV	MIT	
29.			Impression Type (6.5.1.3)	MF	MV	0 ≤ MIT ≤ 3	Plain or rolled from live or non-live scan images.
30.			Finger Quality (6.5.1.4)	MF	MV	MIT	See Note 1
31.			Number of Minutiae (6.5.1.5)	MF	MV	M ≤ 128	M minutiae data records follow, line 24
32.		es of Finger Minuti	Minutiae Type (6.5.2.1)	MF	MV	01b, 10b, or 00b	See Note 2

			Section title and/or field name	INCITS 378-2004		PIV Conformance	Informative Remarks
				Field or Content	Value Reqd	Values Allowed	
33.			Minutiae Position (6.5.2.2)	MF	MV	MIT	See Note 3
34.			Minutiae Angle (6.5.2.3)	MF	MV	MIT	See Note 3
35.			Minutiae Quality (6.5.2.4)	MF	MV	MIT	
36.			Extended Data Block Length (6.6.1.1)	MF	MV	0	See Note 4

Acronym		Meaning
MF	mandatory field	[MINUSTD] requires a field shall be present in the FIR
MV	mandatory value	[MINUSTD] requires a meaningful value for a field
NC	normative content	[MINUSTD] gives normative practice for PIV. Such sections do not define a field in the FIR.
A	as required	For PIV, value or practice is as normatively specified in [MINUSTD].
MIT	mandatory at instantiation-time	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [MINUSTD]

NORMATIVE NOTES:

1. The quality value shall be that computed for the parent image using [NFIQ] and reported here as Q = 20(6 - NFIQ).
2. [MINUSTD] requires that each stored minutia have a type associated with it. Templates compliant with [MINUSTD] (as profiled by this standard) shall be limited to minutiae of types "ridge ending" and "ridge bifurcation". Minutiae not satisfying these definitions shall not be included in PIV templates. For those cases where it is not possible to reliably distinguish between a ridge ending and a bifurcation, the category of "other" shall be used (bit values 00b). This is a common characteristic of "inked" impressions that exhibit ridge endings being converted to bifurcations and bifurcations being converted to ridge ending due to over- or under-inking in the image. PIV implementers employing systems which do not distinguish between minutiae type, or do not rely on minutiae type, in their extraction or matching algorithms may assign the "other" type to all minutiae. Although [MINUSTD] uses the "other" category for minutiae that are neither ridge endings nor ridge bifurcations, such as trifurcations and crossovers, such minutiae shall not be include in PIV templates. This requirement is intended to improve interoperability.
3. All coordinates and angles for minutiae shall be recorded with respect to the original finger image. They shall not be recorded with respect to any image processing sub-image(s) created during the template creation process.
4. The mandatory value of zero codifies the requirement that PIV card templates shall not include extended data.
5. The length of the entire record shall fit within the container size limits specified in [800-73]. These limits apply to the entire CBEFF wrapped and signed entity, not just the [FINGSTD] record.
6. Both of the two fields ("Owner" and "Type") of the CBEFF Product Identifier of [MINUSTD, Section 6.4.4] shall be non-zero. The two most significant bytes shall identify the vendor, and the two least significant bytes shall identify the version number of that supplier's minutiae detection algorithm. See Section HH for related requirements.

3.3 Fingerprint Image Format for Images Retained by Agencies

This section specifies a common data format record for the retention of the fingerprint images collected in Section 3.1. Fingerprint images enrolled or otherwise retained by agencies shall be formatted according to the INCITS 381-2004 finger image based interchange format standard [FINGSTD]. This set shall include ten single-finger images. These shall be obtained by segmentation of the plain multi-finger images gathered in accordance with Options 1, 2 or 3 of Table 1. These images shall be placed into a single [FINGSTD] record. The record may also include the associated multi-finger plain impressions. The record shall be wrapped in the CBEFF structure described in Section 6. [800-76] standard does not specify uses for any single-finger rolled images gathered according to Options 2 or 3 of Table 1.

Table 4 gives section-by-section requirements of the [FINGSTD]. The primary purpose of the Table is to specify PIV requirements for those fields of [FINGSTD] that have optional content. Rows 2-11 give normative content. Row 12 mandates the CBEFF header. Rows 13-28 give PIV requirements for the fields of the General Record Header of [FINGSTD, Table 2]. These are common to all images in the record. Similarly, Rows 29-39 provide requirements for the Finger Image Header Record in Table 4 of [FINGSTD]. Column 5 provides PIV specific requirements or parameter defaults of the standard.

Table 4: INCITS 381 Finger Image Storage Requirements for PIV

			Section title and/or field name	INCITS 381-2004		PIV Conformance	Informative Remarks
				Field or Content	Value Required	Values Allowed	
1.			Byte and bit ordering (5.1)	NC		A	Big Endian MSB then LSB
2.			Scan sequence (5.2)	NC		A	
3.			Image acquisition reqs. (6)	NC		Level 31	Table 1
4.			Pixel Aspect Ratio (6.1)	NC		A	1:1
5.			Pixel Depth (6.2)	NC		A	Level 31 → 8
6.			Grayscale data (6.3)	NC		A	Level 31 → 1 byte per pixel
7.			Dynamic Range (6.4)	NC		A	Level 31 → 200 gray levels
8.			Scan resolution (6.5)	NC		A	Level 31 → 500 ppi
9.			Image resolution (6.6)	NC		500 ppi - no interpolation	
10.			Fingerprint image location (6.7)	NC		A	Slap placement info, centering
11.			CBEFF Header (7)	MF	MV	Patron Format A see Section 6.	Multi-field CBEFF Header
1			General Record Header (7.1)	NC		A	
13.	Finger image record		Format Identifier (7.1.1)	MF	MV	A	0x46495200 (‘F’ ‘I’ ‘R’ 0x0)
14.			Version Number (7.1.2)	MF	MV	"010\0"	0x30313000 (‘0’ ’1’ ’0’ 0x0) Ver.1 Rev.0
15.			Record Length (7.1.3)	MF	MV	MIT	size excluding CBEFF structure

			Section title and/or field name	INCITS 381-2004		PIV Conformance		Informative Remarks
				Field or Content	Value Required	Values Allowed		
16.			CBEFF Product Identifier (7.1.4)	MF	MV	A		CBEFF pid. See Note 10
17.			Capture Device ID (7.1.5)	MF	MV	A		Vendor specified. See Note 10
18.			Image Acquisition Level (7.1.6)	MF	MV	31		Settings Level 31
19.			Number of Images (7.1.7)	MF	MV	A		Denote by K, see lines 28-37. See notes 1, 2, and 3.
20.			Scale units (7.1.8)	MF	MV	0x01	0x02	inches or centimeters
21.			Scan resolution (horz) (7.1.9)	MF	MV	500	197	
22.			Scan resolution (vert) (7.1.10)	MF	MV	500	197	
23.			Image resolution (horz) (7.1.11)	MF	MV	500	197	
24.			Image resolution (vert) (7.1.12)	MF	MV	500	197	
25.			Pixel Depth (7.1.13)	MF	MV	8		Grayscale with 256 levels
26.			Image compression alg. (7.1.14)	MF	MV	2		WSQ. See notes 4 and 9.
27.			Reserved (7.1.15)	MF	MV	A		Two bytes.
28.	K fingerprints, or multi-finger prints		Finger data block length (7.2.1)	MF	MV	MIT		
29.			Finger position (7.2.2)	MF	MV	MIT		
30.			Count of views (7.2.3)	MF	MV	≥ 1		M views of this finger. See note 5.
31.		M Views of Finger	View number (7.2.4)	MF	MV	MIT		
32.			Finger image quality (7.2.5)	MF	MV	20,40,60,80,100		Transformed NFIQ. See notes 5, 6 and 7
33.			Impression type (7.2.6)	MF	MV	0 or 2		See ANSI NIST ITL 1-2000
34.			Horizontal line length (7.2.7)	MF	MV	≥ 368		See note 8
35.			Vertical line length (7.2.8)	MF	MV	≥ 368		
36.			Finger image data (7.2.9)	MF	MV	MIT		Compressed WSQ Data

Acronym		Meaning
MF	mandatory field	[FINGSTD] mandates a field shall be present in the record
MV	mandatory value	[FINGSTD] mandates a meaningful value for this field
NC	normative content	[FINGSTD] gives normative practice for PIV. Such sections do not define a field in the FIR.
A	as required by standard	For PIV, value or practice is as specified in [FINGSTD]
MIT	mandatory at instantiation-time	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FINGSTD]

NORMATIVE NOTES:

1. If certain fingers cannot be imaged, the value of this field shall be decremented accordingly.
2. The left and right four-finger images, and two-thumb, images may also be included. The value of this field shall be incremented accordingly.
3. For the PIV Card this value will be 2. For PIV enrollment sets, the number of images will ordinarily be thirteen (that is, the ten segmented images from the multi-finger plain impressions, and the three plain impressions themselves) or fourteen (if the plain thumb impressions were imaged separately).
4. Images shall be compressed using an implementation of the Wavelet Scalar Quantization (WSQ) algorithm that has been certified by the FBI.
5. The term view refers to the number of images of that particular finger. This value will exceed one if imaging has been repeated. Inclusion of all images of a finger can afford some benefit in a matching process. Retention of all images with quality values 1-4 is recommended. The first such image should have quality 1-3 per the following notes.
6. Quality values shall be present. These shall be calculated from the NIST Fingerprint Image Quality (NFIQ) method described in [NFIQ] using the formula Q = 20(6 - NFIQ). This scale reversal ensures that high quality values connote high predicted performance and consistency with the dictionary definition. The values are intended to be predictive of the relative performance of a minutia based fingerprint matching system.
7. The quality value shall be set to 254 (the [FINGSTD] code for undefined) if this record is not a single finger print (i.e., it is a multi-finger image, or a palm print).
8. The values are minimum image sizes.
9. Compression shall only be applied after images required in Sections 3.4 and 3.2 have been prepared and transformed NFIQ values have been assigned.
10. The Capture Device ID should indicate the hardware version. The CBEFF PID should indicate the BSP's firmware or software.

3.4 Fingerprint Image Specifications for Background Checks

PIV fingerprint images transmitted to the Federal Bureau of Investigation (FBI) as part of the background checking process shall be formatted according to the ANSI/NIST-ITL 1-2000 standard [FFSMT] and the CJIS-RS-0010 [EFTS] specification. Such records shall be prepared from, and contain, only those images collected as per specifications in Section 3.1.

Table 5 enumerates the appropriate transaction formats for the three acquisition options of Section 3.1. The FBI documentation [EFTS] should be consulted for definitive requirements.

Table 5: Record Types for Background Checks

Option	Transaction Data Format in [FFSMT]	Reference
1	Three Type 14 records.	Appendix N of [EFTS]
2 or 3	Fourteen Type 4 records	Section 3.1.1.4 "Federal Applicant User Fee" of [EFTS]

4. Fingerprint Verification

This section provides specifications relating to biometric data verification in PIV. Specifically, these requirements cover fingerprint sensors used for live image capture and matchers used for comparing stored templates with template generated from newly acquired fingerprint images.

4.1 PIV Authentication Fingerprint Acquisition Specifications

Fingerprint sensors used for PIV authentication shall conform to Level 30 or 31 of [FINGSTD, Section 6 and Table 1]. The device shall be capable of imaging an area of at least 16.5 mm in both the horizontal and vertical directions. The device shall be capable of imaging one or more fingers according to the specifications of [ETFS/F, subsections 2.3 and 2.6].

Suppliers of sensor and/or its client-side driver or application code shall, at agency request, include in their otherwise identical implementations a facility to output one or more fingerprint images to an appropriately authenticated administrator or operator. These images shall be those that would be selected for matching in an actual operation. Such images shall be contained in [FINGSTD] records conformant to Section 3.3. The means of implementing this image retention requirement is not specified in this standard, but in any case this facility shall not be enabled by default. This facility shall be enabled and used in all scenario and operational biometric performance tests that agencies elect or are otherwise required to conduct. Capture and retention of images supports a variety of analyses, including development and calibration tasks. These include conformance tests (e.g. number of grey levels) and performance tests (e.g. template generation, biometric matching, and throughput measurement).

4.2 PIV Authentication Matcher Specifications

The software or hardware implementation that compares PIV Card templates with newly acquired fingerprint images shall be capable of accepting and shall use threshold calibration information to tailor the operating threshold of the device to the value of the CBEFF Product and Version Identifiers of [MINUSTD, Section 6.4.4]. This facility is required because matcher performance will differ depend on the source of the templates. The default practice shall be to set the threshold to meet performance criteria for those cardholders who represent the plurality of the agencies' authentication transactions. This will usually be an agencies own employees whose cards will contain templates generated by, and matched by, a single supplier).

5. Facial Image Specifications

5.1 Scope

[FIPS, Section 4.4.1] requires collection of a face image from PIV applicants, and indicates that it may be used for generation of the printed image [FIPS, Section 4.1.4.1] and for augmentation of human authentication of the card holder. The face specification in this document supports those activities, and establishes a storage format for retention of face images. As with other biometric elements, agencies may elect to store face data on the PIV card and use it for automated verification. Although this section places no normative requirements on such agency-optional activities, it does specify an image suited for automated biometric enrollment and face recognition.

5.2 Acquisition and Format

This section specifies requirements for the collection and retention of facial images. Facial images collected during PIV Registration shall be formatted such that they conform to INCITS 385-2004 [FACESTD]. The images shall be embedded within the CBEFF structure defined in Section 6. Because [FACESTD] is generic across applications it includes sections that have either-or requirements. Table 7 is an application profile of [FACESTD] specifically tailored for PIV. It gives concrete requirements for much of the generic content. Column 3 references the sections of [FACESTD] and columns 4 and 5 give [FACESTD] requirements. For PIV, column 6 of Table 6 gives normative practice or value specifications. The table is not fully conformant with the Implementation Conformance Statement [ICS] standard. Nevertheless the addition of a "values supported column" as specified in Section 9.1 of [ICS] should be used by implementers for checking conformance to the requirements.

Table 6: INCITS 385-2004 and PIV Requirements for Formatting of Facial Images

1.		Section title and/or field name	INCITS 385-2004		PIV Conformance	Informative Remarks
			Field or Content	Value Reqd	Values Allowed	
2.		Byte Ordering (5.2.1)	NC		A	Big Endian
3.		Numeric Values (5.2.2)	NC		A	Unsigned Ints
4.	CBEFF	CBEFF Header (5.3)	MF	MV	Patron format A of sec. 6.	Multi-field CBEFF Header
5.	Facial Header	Format Identifier (5.4.1)	MF	MV	A	Fields contain fixed hex values indicating INCITS 385-2004 records
6.		Version Number (5.4.2)	MF	MV	A	
7.		Record Length (5.4.3)	MF	MV	MIT	size of FIR not including CBEFF structure it's embedded in
8.		Number of Facial Images (5.4.4)	MF	MV	≥ 1	One or more images (K ≥ 1). See line 21.
9.	Single instance of subject-specific info.	Face Image Block Length (5.5.1)	MF	MV	MIT	
10.		Number of Feature Points (5.5.2)	MF	MV	≥ 0	positive, if features computed

1.		Section title and/or field name	INCITS 385-2004		PIV Conformance	Informative Remarks
			Field or Content	Value Reqd	Values Allowed	
11.		Gender (5.5.3)	MF	OV	OIT	These fields populated with meaningful values at agency discretion, otherwise 0 for unspecified.
12.		Eye color (5.5.4)	MF	OV	OIT	
13.		Hair color (5.5.5)	MF	OV	OIT	
14.		Feature Mask (5.5.6)	MF	OV	OIT	
15.		Expression (5.5.7)	MF	OV	1	Neutral
16.		Pose Angles (5.5.8)	MF	OV	0	Unspecified = Frontal
17.		Pose Angle Uncertainty (5.5.9)	MF	OV	0	Attended operation so should be frontal.
18.	Features	MPEG4 Features (5.6.1)	NC		OIT	
19.	Features	Center of Facial Features (5.6.2)	NC		OIT	
20.	Features	The Facial Feature Block Encoding	OF	OV	OIT	
21	K instances					
22.	Image Info. Each instance has image- specific info.	Facial Image Type (5.7.1)	MF	MV	1	See note 1.
23.	Image Info. Each instance has image- specific info.	Image Data Type (5.7.2)	MF	MV	0 or 1	See note 4. Compression alg.
24.	Image Info. Each instance has image- specific info.	Width (5.7.3)	MF	MV	MIT	See note 2.
25.	Image Info. Each instance has image- specific info.	Height (5.7.4)	MF	MV	MIT	
26.	Image Info. Each instance has image- specific info.	Image Color Space (5.7.5)	MF	MV	1	sRGB. See Note 3.
27.	Image Info. Each instance has image- specific info.	Source Type (5.7.6)	MF	MV	2 or 6	digital still or digital video
28.	Image Info. Each instance has image- specific info.	Device Type (vendor supplied device ID) (5.7.7)	MF	MV	MIT	
29.	Image Info. Each instance has image- specific info.	Quality (5.7.8)	MF	MV	A	std requires 0 (i.e., unspecified)
30.	Image Data	Data Structure (5.8.1)	MF	MV	MIT	Compressed Data
31.	Basic (section 6) Inheritance	Inheritance (6.1)	NC		A	
32.	Basic (section 6) Inheritance	Image Data Encoding (6.2)	NC		A + Note 4.	
33.	Basic (section 6) Inheritance	Image Data Compression (6.3)	NC		A + Notes 4, 5	
34.	Basic (section 6) Format	Facial Header (6.4.1)	NC		A	include 4 fields
35.	Basic (section 6) Format	Facial Information (6.4.2)	NC		A	include 2 fields
36.	Basic (section 6) Format	Image Information (6.4.3)	NC		A	include 8 fields
37.	Frontal (section 7)	Inheritance (7.1)	NC		A	Inherits Basic
38.	Frontal (section 7) Scene	Purpose (7.2.1)	NC		A	frontal Annex A

1.			Section title and/or field name		INCITS 385-2004		PIV Conformance	Informative Remarks
					Field or Content	Value Reqd	Values Allowed	
39.			Pose (7.2.2)		NC		Frontal	+/- 5 degrees
40.			Expression (7.2.3)		NC		Neutral	
41.			Assistance in positioning face (7.2.4)		NC		A	Only the subject appears
42.			Shoulders (7.2.5)		NC		A	Body + Face toward camera
43.			Backgrounds (7.2.6)		NC		Uniform Annex A.4.3	See Note 8.
44.			Subject and scene lighting (7.2.7)		NC		A	Uniform
45.			Shadows over the face (7.2.8)		NC		A	None
46.			Eye socket shadows (7.2.9)		NC		A	None
47.			Hot spots (7.2.10)		NC		A	Should be absent. Diffuse light.
48.			Eye glasses (7.2.11)		NC		A	Subject's normal condition
49.			Eye patches (7.2.12)		NC		A	Medical only
50.		Photographic	Exposure (7.3.2)		NC		A	No saturation
51.			Focus and Depth of Field (7.3.3)		NC		A	In focus
52.			Unnatural Color (7.3.4)		NC		A	White balance
53.			Color or grayscale enhancement (7.3.5)		NC		A + no recompress.	No post-processing
54.			Radial Distortion of the camera lens (7.3.6)		NC		A + Follow Annex A.8	
55.		Digital	Geometry	aspect ratio (7.4.2.1)			A	1:1 pixels
56.				origin (7.4.2.2)			A	top left is 0,0
57.			Color Profile	Density (7.4.3.1)	NC		A	7 bits dynamic range in gray
58.				Color Sat (7.4.3.2)	NC		A	7 bits dynamic once in grayscale
59.				Color space (7.4.3.3)	NC		24 bit RGB	Option a, reported in color space field above. See Note 3
60.			Video Interlacing (7.4.4)		NC		A	
61.	Full Frontal (section 8)		Inheritance (8.1)		NC		A	Inherits Frontal + Basic
62.			Scene (8.2)		NC		A	Inherits Frontal + Basic
63.		Photographic	Centered Image (8.3.2)		NC		A	Nose on vertical centerline
64.			Position of Eyes (8.3.3)		NC		A	Above horizontal centerline
65.			Width of Head (8.3.4)		NC		A	See note 2

1.			Section title and/or field name	INCITS 385-2004		PIV Conformance	Informative Remarks
				Field or Content	Value Reqd	Values Allowed	
66.			Length of Head (8.3.5)	NC		A	
67.		Digital	Resolution (8.4.1)	NC		CC ≥ 240	
68.		Format	Inheritance (8.5.1)	NC		A	
69.			Image Information (8.5.2)	NC		A	

Acronym		Meaning
FIR	Face Information Record	facial header + facial info + repetition of (image info + image data)
MF	mandatory field	[FACESTD] requires a field shall be present in the FIR
OF	optional field	[FACESTD] allows a field to be present in record
MV	mandatory value	[FACESTD] requires a meaningful value for a field
OV	optional value	[FACESTD] allows a meaningful value or allows 0 to be used to connote "unspecified"
NC	normative content	[FACESTD] gives normative practice for PIV. Such sections do not define a field in the FIR.
A	as required	For PIV, value or practice is as specified in [FACESTD]
MIT	mandatory at instantiation-time	For PIV, mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FACESTD]
OIT	optional at instantiation-time	For PIV, optional header value that may be determined at the time the record is instantiated

NORMATIVE NOTES:

1. PIV facial images shall conform to the Full Frontal Image Type defined in Section 8 of [FACESTD].
2. Face recognition performance is a function of the spatial resolution of the image. [FACESTD] does not specify a minimum resolution for the Full Frontal Image Type. For PIV, faces shall be acquired such that a 20 centimeter target placed on, and normal to, a camera's optical axis at a range of 1.5 meters shall be imaged with at least 240 pixels across it. This ensures that the width of the head (i.e. dimension CC in Figure 8 of [FACESTD]) shall have sufficient resolution for the printed face element of the PIV Card. This specification and Section 8.3.4 of [FACESTD] implies that the image width shall exceed 420 pixels. This resolution specification shall be attained optically without digital interpolation. The distance from the camera to the subject should be greater than or equal to 1.5 meters (for distortion reasons discussed in [FACESTD, Annex A.8]).
3. Face image data shall be converted to the sRGB color space for storage. As stated in Section 7.4.3.3 of [FACESTD] this requires application of the color profile associated with the camera in use.
4. Face image data shall be formatted in either of the compression formats enumerated in Section 6.2 of [FACESTD]. Both whole-image and single-region-of-interest (ROI) compression are permitted.
5. Face images shall be not be compressed using a compression ratio no higher than 15:1.
6. More than one image may be stored in the record. It may be appropriate to store several images if appearance changes over time (beard, no beard, beard) and images are gathered at re-issuance. The most recent image shall appear first and serve as the default provided to applications.
7. The background shall be uniform and no darker than 18% gray, per Annex A.4.4 of [FACESTD].

6. Common Header for PIV Biometric Data — CBEFF Structure

All PIV biometric data shall be embedded in a data structure conforming to Common Biometric Exchange Formats Framework [CBEFF]. This requirement mandates that all biometric data shall be digitally signed and encapsulated in common container. This requirement covers: the PIV Card fingerprints mandated by [FIPS]; any other biometric data agencies elect to place on PIV Cards; any biometric records that agencies elect to retain (including purely proprietary, or derivative, elements); and any biometric data retained by, or for, agencies or Registration Authorities. The data described in clause 3.4 is exempt.

All such data shall be signed in the same manner as prescribed in [FIPS 201] and [800-73] for the mandatory biometric elements. The signature is present for integrity and shall be stored in the CBEFF signature block. The overall arrangement is depicted in Table 7.

Table 7: Simple CBEFF Structure

CBEFF STRUCTURE		
CBEFF_HEADER	CBEFF_BIOMETRIC_RECORD	CBEFF_SIGNATURE_BLOCK
Section 6	Sections 3,3.2 and 4	FIPS 201
INCITS 398 5.2.1	INCITS 398 5.2.2	INCITS 398 5.2.3

The CBEFF Header specified below will be established by NIST as Patron Format "PIV". This format will be established as a formal Patron Format per the provisions of [CBEFF, clause 6.2]. This format is defined below in Table 8 and its notes. All fields of the format are mandatory.

Table 8: Patron Format PIV Specification

	Patron Format A Field	Length Bytes	PIV Data Type	PIV Conformance Required Value
1.	SBH Security Options (5.2.1.1)	1	Bitfield	0x0D and see Informative Note 2
2.	Patron Header Version (5.2.1.4)	1	UINT	0x02
3.	SBH Length	2	UINT	100. i.e. length, in bytes, of this CBEFF_HEADER
4.	BDB Length	4	UINT	length, in bytes, of the biometric data CBEFF_BIOMETRIC_RECORD
5.	SB Length	2	UINT	length, in bytes, of the CBEFF_SIGNATURE_BLOCK
6.	BDB Format Owner (5.2.1.17)	2	UINT	For fingerprint and facial records defined in this standard this value shall be 0x001B for M1, the INCITS Technical Committee on Biometrics. Otherwise see [CBEFF, clause 5.2.1.17]
7.	BDB Format Type (5.2.1.17)	2	UINT	See Normative Note 2
8.	Biometric Creation Date (5.2.1.10)	8		See Normative Note 5 for data type and requirements
9.	Validity Period (5.2.1.11)	16		See Normative Note 6 for data type and requirements
10.	Biometric Type (5.2.1.5)	3	UINT	0x000008 Finger 0x000008 Finger Minutiae 0x000002 Face
11.	Biometric Data Quality (5.2.1.9)	1	SINT	See Normative Note 3

12.	Creator (5.2.1.12)	22	Note 6	See Normative Note 7 for data type and requirements
13.	FASC-N	29	Note 7	See Normative Note 8 for data type and requirements
14.	Reserved for future use	7		0x0000000000

NORMATIVE NOTES:

1. Unsigned integers are denoted by UINT. Signed integers are denoted by SINT. Multi-byte quantities shall be in Big Endian order.
2. For fingerprint image data defined in this standard the Format Type shall be 0x0401. For fingerprint minutiae template data defined in this standard, this value shall be 0x0201. For face data defined in this standard this value shall be 0x0501. For other biometric records on the PIV Card or otherwise retained by agencies this field shall be assigned in accordance with the procedures of [CBEFF, clause 5.2.1.17].
3. For single fingerprint images, the quality value shall be Q = 20(6 - NFIQ) where NFIQ is computed using the method of [NFIQ]. The value here is a duplicate of the value in the BDB itself; it may be useful is selecting which of the two fingerprint records should be verified first. For other biometric records on the PIV Card or otherwise retained by agencies this field shall be a signed integer between -1 and 100. A value of 0 shall denote that the value was not assigned. A value of -1 shall indicate that an attempt to compute a quality value failed. When multiple biometric samples are stored in the BDB the quality value reported here shall be the largest of the individual qualities.
4. This is the date that the biometric sample was acquired. For processed samples (e.g. templates) this data should be the date of acquisition of the parent sample. Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer. Thus 17:35:30 December 15, 2005 is represented as: 00010100 00000101 00001100 00001111 00010001 00100011 00011110 1011010 where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value.
5. The Validity Period contains two dates each of which shall be coded according to Normative Note 5.
6. [CBEFF] defines the Creator field to have variable length. For PIV the length of the field, N, shall be 22 bytes. This value (i.e. 22) shall be present in the first four bytes and coded as a Big Endian unsigned integer. The remaining text portion shall consist of K ≤ 17 ASCII characters, and 18-K null terminators (zeroes).
7. This field shall contain the four byte unsigned integer value 29, followed by the 25 bytes of the FASC-N component of the CHUID identifier, per clauses 1.8.{3,4} of [800-73].

INFORMATIVE NOTES:

1. The value 0x3A79 is the sum of the elements in column 5.
2. 0x25 is the bit pattern 00100101 meaning: the standard biometric header (SBH) length is stored in two bytes, the biometric data block (BDB) length is stored in four bytes; the signature block (SB) length is stored in two bytes; the data is signed but not encrypted; and integrity protection is present.
3. PIV's CBEFF Patron Format is based on INCITS 398's Patron Format A.
4. Column 4, PIV Requirement, is mandatory by definition.
5. The values for the Format Owner and Format Type Code fields are given in the respective data format standards [FACESTD] and [FINGSTD].

7. Performance Testing Requirements and Certification Procedures

7.1 PIV Authentication

PIV biometric implementations will be certified against minimum performance qualification criteria established by NIST, the Office of Management and Budget, and by Agencies. Agencies implementing biometric authentication of cardholders using the mandatory biometric elements of the PIV Card shall use only those template generation and matching implementations that have been certified.

Template based authentication in PIV involves the comparison of standard templates stored on the PIV Card with templates generated from newly acquired fingerprint images. This process may involve the internal generation of non-standard template from the live images. One or both templates may be employed and this will necessitate the acquisition of fingerprint samples from either or both of the primary and secondary fingers. The inclusion of the finger position in the [MINUSTD] header allows a user to be prompted for their specific finger.

The requirement for an interoperable biometric in [FIPS] requires that a Federal agency implementing biometric authentication shall be able to verify both those individuals who have been issued cards by that agency and cardholders from other agencies. The ability to process those in either category will necessitate cross-vendor interoperable comparison of fingerprint templates if the PIV Card template generator and the live comparator are not from the same supplier. This leads to higher verification error rates because a matcher must be tolerant of interpretations of finger images by others that necessarily remain unregulated by [MINUSTD]. Error rates are generally improved in cases where the underlying biometric template generator and matcher implementations are sourced from a single supplier because the supplier has a comprehensive understanding and interpretation of its own template instances.

Verification performance is usually quantified in terms of both the false reject rate and the false accept rate. In PIV, the former would quantify the proportion of legitimate cardholders incorrectly denied access; the latter would be the proportion of impostors incorrectly allowed access. The error rates depend on a number of factors; the environment, the number of attempts (i.e. finger placements on the sensor), the sensor itself, the quality of the PIV Card templates' parent images, the number of fingerprints invoked, the familiarity of users with the process, and a number of other factors. Agencies may elect to quantify the effect of these variables in a scenario or operational tests.

7.2 Test Procedures

This section specifies procedures that a test laboratory shall follow in measuring interoperable matching performance. Certification shall be based on the results of tests conforming to the procedures of this section. Template generators and template matchers of [MINUSTD] templates shall be tested in offline tests conforming to the provisions of the [ISOSWAP] standard, as profiled by this document. The Minutiae Exchange evaluation [MINEX] conducted by NIST is one instance of an implementation of this standard. Offline testing is a necessary and efficient precursor to smaller or more expensive scenario or operational tests (see [ISOTEST] that agencies may elect to conduct. A test of sufficiency as allowed by [ISOSWAP] is not required for conformance to this document.

A template generator shall be a software library that provides a facility to accept one fingerprint image and produce one template. The image represents a PIV enrollment plain impression. The template represents the PIV Card template. Failures or refusals to process the input image shall nevertheless result in a matchable template.

A template matcher shall be a software library that provides a facility to accept one or two minutiae templates and one or two images to produce a scalar similarity score. The templates represent the PIV Card templates. The images represent the live authentication fingerprints. A failure or refusal to compare the inputs shall in all cases result in the reporting of a score. This standard recommends implementers report a low score in this case.

Use of two fingers: The performance criteria given in Section 7.3 apply to the use of the primary finger, or both the primary and secondary fingers, to attain the required level of performance. This standard requires that the test organization fuse primary and secondary finger comparison scores by simple addition (sum-rule), by selecting the greater of the two (max rule), or by making provision in the test specification for the matcher itself to do vendor-defined fusion.

The templates shall conform to Section 3.2, and the input images shall conform to Section 3.3 except that:

1. the CBEFF wrapper shall be absent; and
2. no vendor, nor product identifying information shall be present; and
3. no subject-specific header information shall be present.

Some core biometric algorithms used in fingerprint verification are better than others, and some products may fail to meet specified performance criteria. Differences in performance between products may be large. Formation of a qualified products list shall be conducted in an evaluation in which measured population sample variance is smaller than the specified performance error rate criteria.

The test shall result is a K x K interoperability matrix that reports the measured FAR and FRR values for template matchers whose threshold is set to produce a specified FAR value (e.g. FAR 0.005 in Table 9).

Table 9: Example Fixed-threshold FAR and FRR values

Interoperability Performance (FAR, FRR)		Template Matcher (PIV authentication implementation)			
		A	B	C	D
Template Generator (producer of PIV Card templates)	A	0.005 0.008	0.005 0.002	0.005 0.008	0.005 0.008
	B	0.004 0.009	0.005 0.001	0.003 0.009	0.004 0.009
	C	0.006 0.011	0.006 0.003	0.005 0.003	0.006 0.011
	D	0.005 0.007	0.004 0.004	0.007 0.007	0.005 0.009

7.3 Certification Procedures

The testing organization will conduct a first round of testing to establish a core group of interoperable template generators and matchers. Subsequent certification rounds shall be conducted to recertify previously certified products and to establish certification for new products.

7.3.1 Phase 1: Initial certification

PIV performance certification shall be determined in a first round of evaluation. A provider shall be required to submit a single template matcher and a single template generator. Duplicate entries, as for example licensed to third parties, shall not be entered for certification.

A supplier's template matcher and generator shall be certified against three performance criteria:

1. Intra-agency Performance: This specification is included to be representative of the scenario in which, an agency, sourcing its template generators and matchers from the same vendor, authenticates its own cardholders. A supplier's implementation shall be certified if it may be configured to achieve a measured false reject rate less than or equal to X and a false accept rate simultaneously less than or equal Y. Both X and Y shall be established before testing begins. These elements correspond to the diagonal values of Table 9. This standard recommends that the false reject rate criterion, Y, and the false accept rate, X, shall not exceed 0.5%. Either the primary finger, or both the primary and secondary fingers, may be used in attaining this level of performance.
2. Inter-agency Performance: This specification is included to be representative of the scenario in which visitors to a facility present PIV Cards containing templates that were generated by a supplier different from that used for authentication. A supplier's implementation shall be certified if it may be configured to achieve a measured false reject rate less than or equal to X and a false accept rate simultaneously less than or equal Y. Certification requires that all cross-vendor values (the off-diagonal values of Table 9) satisfy the criteria. This requires the test organization to generate the interoperability matrix for all combinations of $N \leq K$ vendors and test for conformity to the criteria. This search shall identify and certify the largest subgroup of N vendors that jointly conform. This standard recommends that the false reject rate criterion, Y, shall be 1% and the false accept rate criterion, X, be 0.5%. Either the primary finger, or both the primary and secondary fingers, may be used in attaining this level of performance.

7.3.2 Phase 2: Recertification

Both template matchers and template generators shall be recertified. The recertification process presents new suppliers an opportunity for their products to receive initial certification. In a recertification testing round a template matcher might be required to process templates from a set of template generators that might includes new entrants and might not include some old entrants. Similarly the outputs of a template generator will be input to matchers that may include new entrants and not include some old ones.

Recertification test rounds shall be conducted according to schedules specified by OMB. This standard recommends that recertification rounds should be scheduled after any performance-related, significant, or otherwise germane revision of this document or [MINUSTD].

8. Conformance to This Standard

This section gives requirements for conformity assessment of implementations claiming conformance to the Section 3 through 6 of this standard.

8.1 Conformance to PIV Registration Fingerprint Acquisition Specifications

Conformance to Section 3.1 requires the use of an [EFTS/F] certified scanner to collect a full set of fingerprint images and the application of a segmentation algorithm and the [NFIQ]-based quality assurance procedure. Conformance shall be tested by human observation of the acquisition procedures, and by inspection of the images per Section 8.3 of this document.

8.2 Conformance of PIV Card Fingerprint Template Records

Conformance to Section 3.2 requires conformance to all the normative content of the section. This includes production of records conformant to [MINUSTD] as profiled in Section 3.2. Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 3. It also requires that the certification in Section 7 be followed.

8.3 Conformance of PIV Registration Fingerprints Retained by Agencies

This conformance requirement applies if fingerprints acquired by registration are retained by agencies in their database. Conformance to Section 3.3 requires conformance to all the normative content of the section. This includes production of records conformant to [FINGSTD] as profiled in Section 3.3. Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 4.

8.4 Conformance of PIV Background Check Records

Conformance to Section 3.4 requires conformance to all the normative content of the section. This requires conformance to the normative requirements of the FBI for background checks. These shall be tested by inspection of the transactions submitted to the FBI. This inspection may be performed either by capturing the transactions at the submitting agency or at the FBI.

8.5 Conformance to PIV Authentication Fingerprint Acquisition Specifications

Conformance to Section 4.1 shall be tested by inspection of the sensor, and of the image records it produces. The section includes requirements for access to such images.

8.6 Conformance of PIV Face Image Records

Conformance to Section 5 shall be tested as follows. This includes production of records conformant to [FACESTD] as profiled in Section 5.2. Conformance shall be tested by inspection of records and performing the test assertions of the "PIV Conformance" column of Table 6.

8.7 Conformance of CBEFF Wrappers

Biometric data retained by agencies or placed on the PIV Card, whether or not it is specified in this document or [FIPS], shall be conformant with this standard if it is encapsulated in a wrapper conforming to Section 6 of this standard.

9. Bibliography

Citation Code	Document
800-73	NIST Special Publication 800-73, Interfaces for Personal Identity Verification
FIPS	FIPS 201, Personal Identity Verification, National Institute of Standards and Technology, 2005.
FINGSTD	INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format
MINUSTD	INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange
FACESTD	INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange
CBEFF	INCITS 398-2005, American National Standard for Information Technology - Common Biometric Exchange Formats Framework (CBEFF)
FFSMT	ANSI/NIST-ITL 1-2000 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, NIST Special Publication 500-245, 2000.
EFTS	IAFIS-DOC-01078-7.1 CJIS-RS-0010 (V7.1) – Electronic Fingerprint Transmission Specification, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, May 2, 2005. The material at http://www.fbi.gov/hq/cjisd/iafis/efts71/cover.htm may not be fully up to date. Implementers should request the full EFTS documentation, including Appendix N, from the FBI.
NFACS	IAFIS-DOC-07054-1.0, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, April 2004.
MINEX	Minutiae Interoperability Exchange Test. See http://fingerprint.nist.gov/minex04 and the Test Specification: http://fingerprint.nist.gov/minex04/MINEX04API.pdf
NFIQ	NISTIR 7151 - Fingerprint Image Quality, NIST Internal Report, August 2004
ICS	Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) Proforma style guide. EG 201 058 V1.2.3 (1998-04)
ISOTEST	ISO/IEC 19795:2005 Information Technology — Biometric Performance Testing and Reporting — Part 1: Principles and Framework
ISOSWAP	ISO/IEC 19795:2005 Information Technology — Biometric Performance Testing and Reporting — Part 4: Performance and Interoperability Testing of Data Interchange Formats

10. Glossary of Performance Testing and Certification Terms

Term	Meaning
Offline Test	Offline tests use previously captured images as inputs to core biometric implementations. Such tests are repeatable and can readily be scaled to very large populations and large numbers of competing products. They institute a level-playing field and produce robust estimates of the core biometric power of an algorithm. This style of testing is particularly suited to interoperability testing of a fingerprint template (see [ISOSWAP]).
Scenario Test	Scenario testing is intended to mimic an operational application and simultaneously institute controls on the procedures. Scenario testing requires members of a human test population to transact with biometric sensors. Scenario tests are appropriate for capturing and assessing the effects of interactions human users have with biometric sensors and interfaces.
Operational Test	Operational tests involve a deployed system and are usually conducted to measure in-the-field performance and user-system interaction effects. Such tests require the members of a human test population to transact with biometric sensors. False acceptance rates may not be measurable, depending on the controls instituted.
Interoperability Test	Interoperability tests measure the performance associated with the use of standardized biometric data records in a multiple vendor environment. It involves the production of the templates by N enrollment products and authentication of these against images processed by M others.
Template Matcher	In the PIV context a matcher is a software library providing for the comparison of images conformant to [FINGSTD] and templates conformant to [MINUSTD]. The output of the matcher, a similarity score, will be the basis of accept or reject decision.
Template Generator	In the PIV context a template generator is a software library providing facilities for the conversion of images conformant to [FINGSTD] to templates conformant to [MINUSTD] for storage on the PIV card.