
DRAFT NIST Special Publication 800-76-2

Biometric Data Specification for
Personal Identity Verification



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

Patrick Grother
Wayne Salamon
James Matey

INFORMATION SECURITY

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

DRAFT

DRAFT

April 17, 2011



U. S. Department of Commerce
Gary Locke

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, Director

EDITORIAL NOTES

- This document is a draft of NIST Special Publication 800-76-2. It is open for public comment until Noon on May 22, 2011. Comments should be directed to patrick.grother@nist.gov
- This document supports the draft version of FIPS 201-2, released March 8, 2011
<http://csrc.nist.gov/publications/PubsFIPS.html>
- This document revises NIST Special Publication 800-76-1 published January 24, 2007,
http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
- New content and modifications are shown in red. Editor's Notes appear in blue. The coloration, and these notes, will be removed from the final publication.
- The main modifications are as follows.
 - The inclusion of specifications for an optional iris biometric record, intended to afford an alternative to fingerprint based authentication and chain-of-trust maintenance. This includes
 - Standardized iris image specification for the PIV Card
 - Standardized iris image specification for off-card use of iris images
 - Specifications for the iris camera
 - Specifications for the semantic properties of iris images.
 - An iris image capture interface
 - An iris recognition interface
 - A specification for on-card biometric comparison of fingerprint minutiae to support card activation (instead of PIN) and authentication. This includes
 - Standardized fingerprint and auxiliary data specifications
 - Profile of 7816-4 for Standardized interface.
 - A provisional specification for use of swipe fingerprint sensors with on-card comparison
 - See NOTE in clause 5.5 and 6.3
 - Specification of minimum biometric accuracy in terms of false match rates
 - For off-card authentication with fingerprint minutiae
 - For on-card authentication with fingerprint minutiae
 - For off-card authentications with iris images
 - Requirements for inclusion of fingerprint minutia templates when fingerprints cannot be authenticated
 - A modified procedure for quality assessment during fingerprint capture.

38

39
40
41
42
43
44
45
46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69
70

71

72

EXECUTIVE SUMMARY

73 The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the
74 interoperable use of identity credentials to allow physical and logical access to Federal government locations and
75 systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal
76 Information Processing Standard (FIPS 201), was developed to establish standards for identity credentials. This
77 document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It describes technical
78 acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV Card¹ itself.
79 It enumerates procedures and formats for fingerprints, iris and facial images by restricting values and practices
80 included generically in published biometric standards. The primary design objective behind these particular
81 specifications is high performance and universal interoperability. The addition of iris specifications in the 2011 edition
82 adds an alternative modality for biometric authentication and extends coverage to persons for whom fingerprinting is
83 problematic. The addition of on-card comparison offers an alternative to PIN-mediated card activation. For the
84 preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76
85 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint
86 Transmission Specification. This document does not preclude use of other biometric modalities in conjunction with
87 the PIV card.

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

ACKNOWLEDGEMENTS

104 The authors, Patrick Grother and Wayne Salamon of the National Institute of Standards and Technology (NIST), and
105 James Matey of the United States Naval Academy, wish to thank their colleagues who reviewed drafts of this
106 document and contributed to its development. Particular thanks go to Charles Wilson who led the development of
107 the original SP 800-76 and its early update, SP 800-76-1. Thanks also go to R. Michael McCabe for his extensive
108 knowledge of the Federal Bureau of Investigation's procedures. The authors also gratefully acknowledge and
109 appreciate the many contributions from the public and private sectors for the continued interest and involvement in
110 the development of this publication.

111

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

112

113	1. Introduction.....	1
114	1.1 Authority	1
115	1.2 Purpose and scope	1
116	1.3 Audience and assumptions.....	1
117	1.4 Overview	2
118	1.4.1 Document structure	2
119	1.5 Inclusion of iris recognition	3
120	1.6 Inclusion of fingerprint on-card comparison	3
121	2. Terms, acronyms, and notation.....	4
122	2.1 Terms	4
123	2.2 Acronyms	4
124	3. Fingerprint enrollment.....	5
125	3.1 Scope	5
126	3.2 Fingerprint data retention.....	5
127	3.3 Fingerprint image acquisition.....	5
128	3.4 Training of PIV fingerprint collection staff.....	7
129	3.5 Monitoring overall enrollment quality.....	7
130	3.6 Fingerprint image format for images retained by agencies.....	7
131	3.7 Fingerprint image specifications for background checks	9
132	4. Fingerprint off-card authentication specifications.....	10
133	4.1 Scope	10
134	4.2 Source images	10
135	4.3 Card issuance	10
136	4.4 Minutia record.....	10
137	4.5 Performance specifications for PIV compliance	13
138	4.5.1 Scope.....	13
139	4.5.2 Background	13
140	4.5.3 Minimum interoperability specification	13
141	4.5.4 Minimum accuracy specification.....	14
142	4.6 Performance specifications for PIV operations	14
143	4.6.1 Scope.....	14
144	4.6.2 Background	14
145	4.6.3 Minimum accuracy specification.....	15
146	4.6.4 Further agency considerations	15
147	5. Fingerprint on-card comparison specifications	16
148	5.1 Scope	16
149	5.2 Background	16
150	5.3 Approach to the use of standards	16
151	5.4 Data objects	16
152	5.4.1 Biometric Information Template	16
153	5.4.2 Minutiae data for on-card comparison	17
154	5.5 Presence of finger minutiae extracted from swipe-sensor outputs	19
155	5.6 Minutia uniqueness	19
156	5.7 Preparation of the minutia templates	19
157	5.8 Number of minutiae	20
158	5.9 Effect of the BIT	20
159	5.9.1 Minutiae removal mechanism.....	20
160	5.9.2 Sort order of minutiae	20
161	5.10 On-card comparison interface.....	20
162	5.11 Performance specifications for PIV compliance	20
163	5.11.1 Scope.....	20

164	5.11.2	Background	21
165	5.11.3	Minimum interoperability specification	21
166	5.11.4	Minimum accuracy specification.....	21
167	5.12	Performance specifications for PIV operations	22
168	5.12.1	Scope	22
169	5.12.2	Minimum accuracy specification.....	22
170	5.12.3	Further agency considerations	22
171	6.	Sensor specifications for fingerprint capture.....	23
172	6.1	Scope	23
173	6.2	Fingerprint acquisition specifications for plain impression sensors	23
174	6.3	Fingerprint acquisition specifications for swipe sensors	23
175	7.	Iris recognition specifications	24
176	7.1	Scope	24
177	7.2	Background	24
178	7.3	Iris data Retention.....	25
179	7.4	Iris image specification for PIV cards.....	25
180	7.5	Iris image specification for iris images retained outside the PIV card.....	26
181	7.6	Conformance of ISO/IEC 19794-6:2011 records	27
182	7.7	Iris image properties for enrollment	27
183	7.7.1	Scope.....	27
184	7.7.2	Correct segmentation of the iris.....	27
185	7.7.3	Correct preparation of the cropped-and-masked PIV Card iris.	28
186	7.7.4	Blur	28
187	7.8	Performance specifications for PIV compliance	28
188	7.9	Performance specifications for PIV operations	30
189	7.9.1	Iris capture interface.....	30
190	7.9.2	Iris recognition interface	30
191	7.9.3	Iris recognition minimum accuracy requirements.....	30
192	7.9.4	Requirements	30
193	7.9.5	Conformance	30
194	8.	Facial image specifications.....	31
195	8.1	Scope	31
196	8.2	Acquisition and format.....	31
197	9.	Common header for PIV biometric data	34
198	10.	Conformance to this specification	36
199	10.1	Conformance.....	36
200	10.2	Conformance to PIV registration fingerprint acquisition specifications	36
201	10.3	Conformance of PIV Card fingerprint template records.....	36
202	10.4	Conformance of PIV registration fingerprints retained by agencies.....	36
203	10.5	Conformance of PIV background check records	36
204	10.6	Conformance to PIV authentication fingerprint acquisition specifications	36
205	10.7	Conformance of PIV facial image records.....	36
206	10.8	Conformance of CBEFF wrappers.....	36
207	11.	References.....	37
208	A.2.1	Store enrolment template on the card	39
209	A.4.1	APDU specifications.....	40
210	A.4.2	Comparison scores	41
211	A.4.3	Reading comparison subsystem identifier.....	41
212	D.3.1	Template generator.....	52
213	D.3.2	Template matcher	53
214			

List of Figures

216	Figure 1 – PIV biometric data flow	2
217	Figure 2 – Minutiae angle determination	13
218	Figure 3 – Conversion of INCITS 378 to ISO/IEC 19794-2 card data.....	19
219	Figure 4 – Image formats of ISO/IEC 19794-6:2011	24

List of Tables

222	Table 1 – Summary of properties and roles of on- and off-card comparison.....	3
223	Table 2 – Fingerprint acquisition protocols.....	5
224	Table 3 – Quality control procedure for acquisition of a full set of fingerprint images	6
225	Table 4 – INCITS 381 profile for agency retention of fingerprint Images	7
226	Table 5 – Record types for background checks	9
227	Table 6 – INCITS 378 profile for PIV Card templates	11
228	Table 7 – Maximum permissible false match rates for off-card minutia comparison.....	15
229	Table 8 – BIT group template and profile	16
230	Table 9 – ISO/IEC 19794-2 and ISO/IEC 19785-3 finger position codes	17
231	Table 10 – ISO/IEC 19794-2 profile for on-card comparison	18
232	Table 11 – Data object encapsulating ISO/IEC 19794-2 minutiae for on-card comparison	18
233	Table 12 – Maximum permissible false match rates for on-card minutia comparison	22
234	Table 13 – PIV use of plain-impression and swipe fingerprint sensors.....	23
235	Table 14 – ISO/IEC 19794-6 profile for iris images stored on PIV Cards.....	25
236	Table 15 – ISO/IEC 19794-6 profile for iris images stored outside PIV Cards.....	26
237	Table 16 – Maximum permissible false match rates for iris comparison	30
238	Table 17 – INCITS 385 profile for PIV facial images.....	31
239	Table 18 – CBEFF concatenation structure.....	34
240	Table 19 – Patron format PIV specification	34
241	Table 20 – CBEFF content for specific modalities.....	34
242	Table 21 – Command APDU for storage of reference template	39
243	Table 22 – Response APDU from storage of reference template.....	39
244	Table 23 – Command APDU for retrieval of biometric information template	40
245	Table 24 – Response APDU from retrieval of biometric information template.....	40
246	Table 25 – Command APDU for comparison of biometric templates.....	40
247	Table 26 – Response APDU from comparison of biometric templates	41
248	Table 27 – Command APDU for retrieval of Comparison subsystem identifier	41
249	Table 28 – Response APDU for retrieval of Comparison subsystem identifier	41
250	Table 29 – INCITS 378 specification for PIV Card template generator and matcher certification.....	52

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, 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 re-issuance, chain-of-trust operations**, and PIV Card usage. FIPS also defines the structure of an identity credential which includes biometric data. Requirements on interfaces are described in [800-73]. Those on cryptographic protection of the biometric data are described in [FIPS] and in [800-78].

This document contains technical specifications for biometric data mandated **or allowed** in [FIPS]. These specifications reflect the design goals of interoperability, performance **and security** of the PIV Card **and PIV processes**. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by normatively citing biometric standards and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to declare what content is required and what is optional. 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.

The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of SP 800-73-1). Biometric data used only outside the PIV Data Model is not within the scope of this standard.

This document does however specify that any biometric data in the PIV Data Model **shall** be embedded in the Common Biometric Exchange Formats Framework (CBEFF) structure of clause 9. This document 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. **NIST Special Publication 800-85 implements those objectives.**

1.3 Audience and assumptions

This document is targeted at Federal agencies and implementers of PIV systems. In addition, it should be of interest to the biometric access control industry. Readers are assumed to have a working knowledge of biometric standards and applications.

1.4 Overview

1.4.1 Document structure

This document defines:

- In clause 2, acronyms and terms;
- in clause 3, the fingerprint acquisition process, requirements for transmission of data to FBI, and a format for agency-optional image retention;
- in clause 4, the format of the PIV Card minutiae templates; and specifications for algorithms used in the generation and matching of such;
- in clause 5, the formats, data structures and interfaces for minutiae used in on-card comparison operations, and specifications for algorithms used in the generation of matching of such;
- in clause 6, specifications for two kinds of fingerprint sensors;
- in clause 7, the format for iris data stored on and off PIV Cards, and interfaces to cameras and recognition algorithms, and specifications for algorithms used in generation and matching of such;
- in clause 8, facial image specifications;
- in clause 9, the CBEFF header and footer supporting digital signatures on all PIV biometric data;
- in clause 10, additional conformance information, beyond the specifications embedded in clauses 4 through 7;
- in clause 11, references.

gives an approximate procedure for biometric data acquisition and disposition.

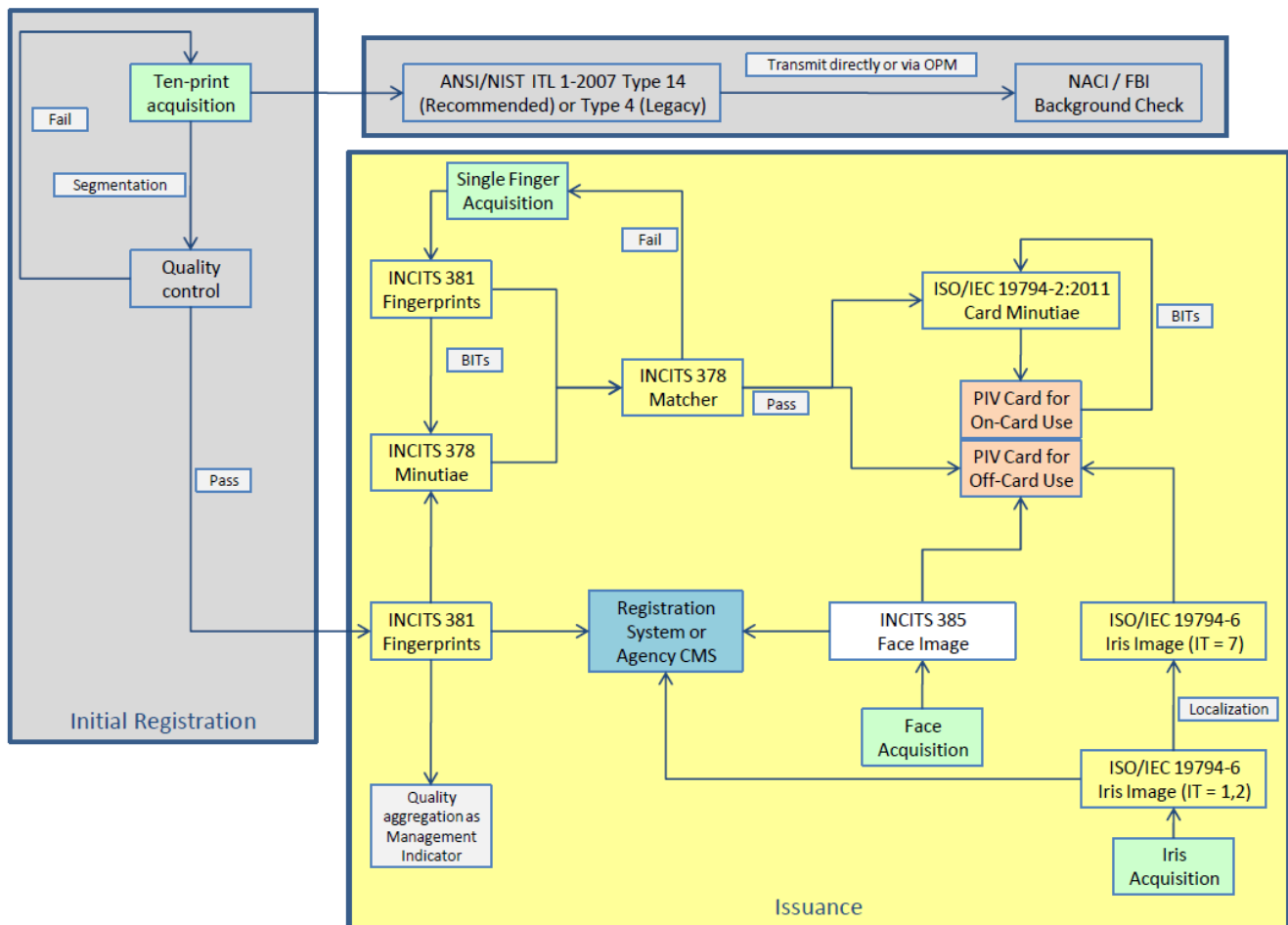


Figure 1 – PIV biometric data flow

1.5 Inclusion of iris recognition

Iris specifications are included, in clause 7, to allow biometric authentication of individuals who do not have fingerprints. [FIPS] requires use of iris in this case. The requirement on an agency to install and operate iris equipment in its PIV issuance processes allows agencies to then additionally populate PIV Cards with iris as an alternative authentication factor.

1.6 Inclusion of fingerprint on-card comparison

FIPS 201-2 requires fingerprint templates of clause 4 as the mandatory biometric element for PIV. These templates are intended to be compared on a reader device with templates collected in an authentication attempt. FIPS 201-2 requires the cardholder to enter a PIN number to release the templates. This constitutes multi-factor authentication.

Agencies may additionally choose to populate the card with an on-card comparison algorithm, and on-card comparison templates. The specifications for these appear in clause 5. FIPS 201-2 does not require PIN entry ahead of a fingerprint minutiae on-card comparison transaction. Indeed, FIPS 201-2 extends on-card comparison as an alternative to PIN entry in altering the state of the PIV card.

Table 1 describes the differences between the off-card and on-card specifications.

Table 1 – Summary of properties and roles of on- and off-card comparison

Aspect	Off-card comparison	On-card comparison
FIPS 201-2 requirement on presence of biometric data	Mandatory	Optional
Domain of use	All card issuance, re-issuance, replacement applications, and cardholder authentication.	Card activation as PIN replacement, cardholder authentication.
Pre-requisites for access to the data	Successful PIN authentication On-card comparison has not been used.	None, for card activation.
Number of fingers	2	1 or 2
Location of data format specifications	SP 800-76-2, this document, clause 4	SP 800-76-2, this document, clause 5
Location of card Interface specifications	SP 800-73-3	SP 800-76-2, with transfer to SP 800-73 at its next revision
Underlying data format standard	INCITS 378:2004	ISO/IEC 19794-2:2011
How to identify specific fingers	INCITS 378:2004	ISO/IEC 7816-11:2007
Fingerprint capture device for enrollment	Plain impression as specified in clause 6.2.	Plain impression and swipe as specified in clauses 6.2 and 6.3.
Fingerprint capture device for authentication	Plain impression as specified in clause 6.2.	Plain impression or swipe as specified in clauses 6.2 and 6.3.
Accuracy testing	MINEX III (formerly Ongoing MINEX)	MINEX II

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
FAR	False Accept Rate
FIPS	Federal Information Processing Standard
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTE	Failure to Enroll Rate
EBTS / F	Electronic Biometric Transmission Specification (Appendix F)
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ITL	Information Technology Laboratory (of NIST)
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
WSQ	Wavelet Scalar Quantization

3. Fingerprint enrollment

3.1 Scope

The specifications in this clause pertain to the production of the mandatory PIV biometric enrollment data. That is, this clause provides specifications for acquisition, formatting, and storage of fingerprint images and templates. The following is an overview of the material covered in this clause.

- Clause 3.2 gives specifications for the use of fingerprint scanners to capture fingerprint images for PIV Registration;
- Clause 3.4 gives the format for fingerprint templates stored on the PIV Card;
- Clause 3.6 gives specifications for fingerprint images retained by agencies;
- Clause 3.7 specifies 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 Clauses 3.4 and 3.6, are INCITS (i.e. non-FBI) standard records and are therefore specified independently.

3.2 Fingerprint data retention

This document neither requires nor precludes agencies from retaining fingerprint images. However, if an agency elects to retain images, then they **shall** be stored in the format specified in clause 3.6. The format specification includes the [CBEFF] header of clause 9, **and this requires integrity protection** and allows for encryption of the image records.

This document neither requires nor precludes agencies from retaining fingerprint templates. However, if an agency elects to retain templates, in either proprietary or standardized formats, then they **shall** be embedded in the [CBEFF] header of clause 9. This **requires integrity protection and** allows for encryption of the records.

Retention of data supports, for example, detection of duplicate identities.

3.3 Fingerprint image acquisition

This clause specifies 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 2.

Table 2 – Fingerprint acquisition protocols

Option 1 – Required presentations for plain live scan	
Combined plain impression of the four fingers on the right hand (no thumb)	
Combined plain impression of the four fingers on the left hand (no thumb)	
Combined impression of the two thumbs	
Option 2 – Required presentations for rolled live scan	
10 separately rolled fingers	
Combined plain impression of the four fingers on the right hand (no thumb)	
Combined plain impression of the four fingers on the left hand (no thumb)	
Left thumb plain impression	These captures may be simultaneous (two thumbs next to each other) or sequential (one thumb at a time)
Right thumb plain impression	
Option 3 - Required presentations for rolled ink on card	
10 separately rolled fingers	
Combined plain impression of the four fingers on the right hand (no thumb)	
Combined plain impression of the four fingers on the left hand (no thumb)	
Left thumb plain impression	These captures may be simultaneous (two thumbs next to each other) or sequential (one thumb at a time)
Right thumb plain impression	

INFORMATIVE NOTES:

1. There is no requirement that the order specified above is the order in which the images must be acquired.
2. The combined multi-finger plain-impression images are also referred to as slaps or flats. They are obtained by simultaneous placement of multiple fingers on the imaging surface without specific rolling movement.
3. Options 2 and 3 represent existing agency practice. Although Option 1 is now acceptable to the FBI agencies may need to implement Options 2 or 3 for transmission via the Office of Personnel Management.

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 [EBTS, Appendix 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 [EBTS, Appendix F]. The scanning is needed to produce fingerprints in the digital format described in Clause 3.6 and thereby Clause 3.7. 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].

For live-scan acquisition, the enrollment client software should display the images to the attending operator. The operator should repeat acquisition if the ridge structure is clear and well formed in the displayed images.

The procedure for the collection of fingerprints, presented in Table 3, **shall** be followed. The procedure **shall** employ the NIST Fingerprint Image Quality [NFIQ] algorithm to initiate any needed reacquisition of the images. An attending official **shall** be present at the time of fingerprint capture. The agency **shall** employ measures to ensure the quality of acquisition and guard against faulty presentation, whether malicious or unintentional. Such activity might be an integral function of the acquisition device or might be implemented by the attending official. In any case, the agency **shall** ensure that the applicant does not swap finger positions or hands, occlude fingers, or misalign or misplace the fingers. Particularly, because it is common during collection of multi-finger plain impressions for fingers 05 and 10 to not be long enough to reach the imaging platen, it is accepted practice for the hand be placed at an angle to the horizontal to ensure imaging of all four fingers. Although this is not needed with newer, large-platen, devices the official **shall** in all cases take care to image all fingers completely. The procedure requires segmentation of the multi-finger plain impressions; this operation may be assisted by the attending official.

Table 3 – Quality control procedure for acquisition of a full set of fingerprint images

Step	Action
1.	Attending official should inspect fingers and require absence of dirt, coatings, gels, and other foreign material.
2.	Official should ensure imaging surface of the sensor, or the card, is clean.
3.	Acquire fingerprints according to Option 1, 2, or 3 in Table 2. For Option 3, scan the inked card using [EFTS, Appendix F] certified scanner.
4.	Segment the multi-finger plain impression images into single-finger images. Automated segmentation is recommended. Attending official should inspect the boundaries of the automatic segmentation and correct any failures, perhaps via an interactive graphical user interface.
5.	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 8.
6.	Repeat steps 2-5 up to three more times.
7.	If after four acquisitions the index fingers and thumbs do not all have NFIQ values of 1, 2 or 3 then select that set, acquired in step 3 and segmented in step 4, for which the mean of the NFIQ values of the left index, right index, left thumb, and right thumb is minimum (i.e. of best quality). If all of the index finger and thumb quality values are unavailable (perhaps because of injury to one or more of those fingers) then use the last set from step 3 of those fingers that are available, without any application of NFIQ.
8.	Prepare and store the final records per Clauses 3.4, 3.6, and 3.7

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 Clause 3.4 requires (in field AMP 2.084 of an accompanying Type 2 record) the labeling of those fingers that are amputated or otherwise not imaged; see [EFTS, Appendix C].

3.4 Training of PIV fingerprint collection staff

Agencies shall apprise staff that the background check can be defeated by mutilation of the fingerprints e.g. either temporarily (e.g. by burns or abrasives) or permanently (e.g. by surgical means). In addition certain medications can cause loss of fingerprint ridge structure. It is recommended that collection of fingerprints from applicants with injuries to their fingers be deferred.

3.5 Monitoring overall enrollment quality

In order to track enrollment quality over time, a numerical summary of operational quality may be computed as a management indicator. If computed, this summary shall be computed from the NFIQ values of primary fingers of all PIV card applicants processed in each calendar month. If computed, the summary shall be computed using the procedures of NIST Interagency Report 7422 [NFIQ SUMMARY] which uses a simple formula to aggregate NFIQ values.

Managers can track this over time, collection sites or stations, over different populations (e.g. contractors vs. employees), across functions (PIV issuance vs. re-issuance), or even across fingers. Managers can use aggregated quality indicators to identify fingerprint collection problems. These may be due to changes in the physical environment or unintended changes in operating procedures.

3.6 Fingerprint image format for images retained by agencies

This clause specifies a common data format record for the retention of the fingerprint images collected in Clause 3.2. Specifically 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 2, and the single plain thumb impressions from presentations 4 & 5 of Options 2 and 3. These images **shall** be placed into a single [FINGSTD] record. The record may also include the associated multi-finger plain impressions and the rolled images. This document ([800-76]) does not specify uses for any single-finger rolled images gathered according to Options 2 or 3 of Table 2. The record **shall** be wrapped in the CBEFF structure described in Clause 9. Agencies may encrypt this data per the provisions of Clause 9, Table 19, Note 2.

Table 4 gives a clause-by-clause profile of [FINGSTD]. The primary purpose of the Table is to give PIV specifications for those fields of [FINGSTD] that have optional content. Rows 1-10 give normative content. Row 11 requires the CBEFF structure of Clause 6. However, its FASC-N value (Table 19, Line 13) may be replaced by a field of all zeroes in this one exceptional case: Storage of PIV registration images before a FASC-N has been assigned. Such instances (including the digital signature) **shall** be regenerated once the FASC-N is known. Rows 12-27 give PIV specifications for the fields of the General Record Header of [FINGSTD, Table 2]. These are common to all images in the record. Similarly, Rows 28-36 provide specifications for the Finger Image Header Record in Table 4 of [FINGSTD]. The "PIV Conformance" column provides PIV specific practice and parameter defaults of the standard.

INCITS 381 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 14 of Table 4.

To assist implementers, NIST has made [FINGSTD] sample data available².

Table 4 – INCITS 381 profile for agency retention of fingerprint Images

		Clause title and/or field name (Numbers in parentheses are [FINGSTD] clause numbers)	INCITS 381-2004 Field or content	Value required	PIV Conformance Values allowed	Informative Remarks
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

² Fingerprint images conformant to the PIV specification are here http://www.itl.nist.gov/iad/894.03/nigos/piv_sample_data.html and these were prepared using NIST software available from <http://www.itl.nist.gov/iad/894.03/nigos/incits.html>

		Clause title and/or field name (Numbers in parentheses are [FINGSTD] clause numbers)	INCITS 381-2004 Field or content	Value required	PIV Conformance Values allowed	Informative Remarks
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		197	Pixels per centimeter - no interpolation
10.		Fingerprint image location (6.7)	NC		A	Slap placement info, centering
11.		CBEFF Header (7)	MF	MV	Patron Format PIV	Multi-field CBEFF Header, Sec. 0
12.		General Record Header (7.1)	NC		A	
13.	Finger image record format	Format Identifier (7.1.1)	MF	MV	0x46495200	i.e. ASCII "FIR\0"
14.		Version Number (7.1.2)	MF	MV	0x30313000	i.e. ASCII "010\0"
15.		Record Length (7.1.3)	MF	MV	MIT	Size excluding CBEFF structure
16.		CBEFF Product Owner (7.1.4)	MF	MV	> 0	CBEFF PID.
17.		CBEFF Product Identifier Type (7.1.4)	MF	MV	> 0	
18.		Capture Device ID (7.1.5)	MF	MV	MIT	Vendor specified. See Note 1
19.		Image Acquisition Level (7.1.6)	MF	MV	31	Settings Level 31
20.		Number of Images (7.1.7)	MF	MV	MIT	Denote by K, see lines 28-37, see Notes 2-4
21.		Scale units (7.1.8)	MF	MV	0x02	Centimeters
22.		Scan resolution (horz) (7.1.9)	MF	MV	197	Pixels per centimeter
23.		Scan resolution (vert) (7.1.10)	MF	MV	197	
24.		Image resolution (horz) (7.1.11)	MF	MV	197	
25.		Image resolution (vert) (7.1.12)	MF	MV	197	
26.		Pixel Depth (7.1.13)	MF	MV	8	Grayscale with 256 levels
27.		Image compression algorithm (7.1.14)	MF	MV	0 or 2	Uncompressed or WSQ 3.1 See Notes 5 and 6.
28.		Reserved (7.1.15)	MF	MV	0	Two bytes, see Note 12
29.	K fingerprints, or multi-finger prints	Finger data block length (7.2.1)	MF	MV	MIT	
30.		Finger position (7.2.2)	MF	MV	MIT	
31.		Count of views (7.2.3)	MF	MV	≥ 1	M views of this finger, see Note 7
32.		View number (7.2.4)	MF	MV	MIT	
33.		Finger image quality (7.2.5)	MF	MV	20,40,60,80,100	Transformed NFIQ. See Notes 8 and 9
34.		Impression type (7.2.6)	MF	MV	0 or 2	See ANSI NIST ITL 1-2000
35.		Horizontal line length (7.2.7)	MF	MV	MIT	See Note 10
36.		Vertical line length (7.2.8)	MF	MV	MIT	
37.		Reserved (no clause)	MF	MV	0	See Note 11
38.		Finger image data (7.2.9)	MF	MV	MIT	Uncompressed or compressed WSQ Data

END OF TABLE

Acronym	Meaning
MF	mandatory field
MV	mandatory value
NC	normative content
A	as required by standard
MIT	mandatory at time of instantiation

- NORMATIVE NOTES:**
- The Capture Device ID should indicate the hardware model. The CBEFF PID [FINGSTD, 7.1.4] should indicate the firmware or software version.
 - If certain fingers cannot be imaged, the value of this field **shall** be decremented accordingly.
 - The left and right four-finger images, and two-thumb, images may also be included. The value of this field **shall** be incremented accordingly.
 - 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).

5. Images **shall** either be uncompressed or compressed using an implementation of the Wavelet Scalar Quantization (WSQ) algorithm that has been certified by the FBI. **As of February 2011, Version 3.1 of the WSQ algorithm shall be used.** The FBI's current requirement for a 15:1 nominal compression ratio **shall** apply.
6. Compression should only be applied after the records required by clauses 3.4 and 3.7 have been prepared and transformed NFIQ values have been assigned.
7. The term view refers to the number of images of that particular finger. This value would exceed one if imaging has been repeated. Inclusion of more than one image of a finger can afford some benefit in a matching process. This document recommends that any additionally available images (say, from a PIV Card re-issuance procedure) with quality value 1 to 3 should be included in the record. In all cases the images **shall** be stored in order of capture date, with newest first.
8. Quality values **shall** be present. These **shall** be calculated from the NIST Fingerprint Image Quality (NFIQ) method described in [NFIQ] using the formula $Q = 20 \cdot (6 - \text{NFIQ})$. 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. It is recommended that a user should be prompted to first attempt authentication using the finger with the highest quality, regardless of whether this is the primary or secondary finger.
9. 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) or if the NFIQ implementation fails.
10. There is no restriction on the image size. However non-background pixels of the target finger **shall** be retained (i.e. cropping of the image data is prohibited).
11. [FINGSTD, Table 4] refers to a single-byte field labeled "reserved", but there is no corresponding clause to formally define it. The M1 committee has undertaken to resolve this by inserting a new subclause to require inclusion of the "Reserved" field. This will appear in a revision of [FINGSTD]. In any case, PIV implementations **shall** include the single byte field, setting the value to 0.
12. Line 27 indicates that the "Reserved" field **shall** have length 2 bytes. [FINGSTD, 7.1.15] indicates a length of 4 bytes which disagrees with the value in [FINGSTD, Table 2]. The INCITS M1 committee has indicated 2 bytes is the correct value. PIV implementations **shall** include the 2 byte field, setting the value to 0.

3.7 Fingerprint image specifications for background checks

PIV fingerprint images transmitted to the 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 Clause 3.1.

Table 5 enumerates the appropriate transaction formats for the three acquisition options of Clause 3.2. 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 (and see Note 1)	[EFTS, Appendix N]. See Note 2
2 or 3	Fourteen Type 4 records (and see Note 1)	Clause 3.1.1.4 "Federal Applicant User Fee" of [EFTS]

NORMATIVE NOTES:

1. All types of transactions with the FBI require both a Type 1 and Type 2 record to accompany the data; see [FFSMT, Table 2]. The Type 2 supports labeling of missing fingers.

The forthcoming revision of [FFMST], due in early 2007, adds new fields to the Type 14 record of [FFSMT] but does so in a backwards compatible way. But, in any case, [EFTS, Appendix N] **shall** be the definitive reference for the format of the images.

4. Fingerprint off-card authentication specifications

4.1 Scope

This clause 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 [MINUSTD] templates otherwise retained by agencies. The templates constitute the enrollment biometrics for PIV authentication and as such are supported by a high quality image acquisition specification, and a FBI-certified compression format. The specification of a standardized template in this clause enables use of the PIV Card in a multi-vendor product environment.

4.2 Source images

Two [MINUSTD] fingerprint templates **shall** be stored on the PIV Card; these are hereafter referred to as PIV Card templates. These **shall** be prepared from images of the primary and secondary fingers (as specified in [FIPS]). These images **shall** be either

- those obtained by segmenting the initial plain impressions of the full set of fingerprints captured during PIV Registration and stored in row 8 of Table 3, or
- Those collected and matched against the initial plain impressions.

Significant rotation of the multi-finger plain impressions (for example, that which can occur when four fingers are imaged using a narrow platen) **shall** be removed prior to, or as part of, the generation of the mandatory minutiae templates. The rotation angle **shall** be that which makes the inter-phalangeal creases approximately horizontal or, equivalently, the inter-finger spaces approximately vertical. This requirement supports interoperable fingerprint matching.

4.3 Card issuance

When a PIV Card is issued, one or more authentication attempts **shall** be executed per [FIPS, 5.3.1]. This **shall** entail capture of new live fingerprints of both the primary and secondary fingers, and matching of those **with the images originally collected during initial registration**. This binds the cardholder to the individual whose background was checked. This authentication should use images collected using either a [EFTS/F] multi-finger fingerprint imaging device of clause 3.2, or a [SINGFING] device of Clause 6.2.

The template matcher used during authentication attempts shall conform the performance specifications established in clause 4.5.3, and shall be configured with a threshold at least as high as that needed to achieve the minimum accuracy requirements of clause 4.6. If all biometric authentications fail during card issuance, then the PIV Card shall be populated with the standardized minutia record of clause 4.4 which

- has two empty views (i.e. there are zero minutiae such that Table 6, Line 31 shall be zero),
 - has fingerprint qualities (Line 30) assigned 255 for temporarily unusable, or 254 for permanently unusable, fingerprints,
 - is digitally signed as usual using the properly populated CBEFF structure of clause 9, and
 - Overrides the CEBFF quality values (Table 19, Line 11) with -1 indicating temporarily, and -2 permanently unusable fingerprints.
- FIPS 201-2 requires use of clause 7 iris biometrics for PIV applicants for whom fingerprints are unavailable or unusable. Authentication systems encountering such a card populated with empty minutia templates might attempt iris-based authentication.

4.4 Minutia record

PIV Card templates **shall** be a conformant instance of the INCITS 378-2004 [MINUSTD] minutiae template standard. That is, the minutiae from both the primary and secondary fingers **shall** reside within a single INCITS 378 record. This means that there will be one instance of the "General Record Header" [MINUSTD, 6.4], and two instances of the "Finger View Record" [MINUSTD, 6.5]. This record **shall** be wrapped in a single instance of the CBEFF structure specified in Clause 9 prior to storage on the PIV Card. The PIV Card templates **shall** not be encrypted.

Table 6 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. This document recommends that the minutiae records should be prepared soon after the images are captured and before they are compressed for storage.

INCITS 378 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 14 of Table 6.

To assist implementers, NIST has made [MINUSTD] sample data available³.

Table 6 – INCITS 378 profile for PIV Card templates

		Clause title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	INCITS 378-2004		PIV Conformance	
			Field or content	Value Required	Values Allowed	Informative Remarks
1.		Principle (5.1)	NC		A	Defines fingerprint minutiae
2.		Minutia Type (5.2)			See Note 1	[MINUSTD, 5.2] defines minutiae type but contains no normative content
3.		Minutia Location : Coordinate System (5.3.1)	NC		A	Minutia placement and angle are influential on accuracy and interoperability. Developers should ensure the listed requirements are actually achieved by their minutia detection algorithms.
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 1	
7.		Minutia Direction : Angle Conventions (5.4.1)	NC		A	In addition, correct detection of true minutiae, and correct suppression of false minutiae have been shown to influence interoperability [BAZIN, MANSFIELD].
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, unsigned integers
11.		Minutia Record Organization (6.3)	NC		A	
12.		CBEFF Record Header (6.4)	MF	MV	Patron format PIV	Multi-field CBEFF Header, Sec. o.
13.		Format Identifier (6.4.1)	MF	MV	0x464D5200	i.e. ASCII "FMR\0"
14.		Version Number (6.4.2)	MF	MV	0x20323000	i.e. ASCII " 20\0" which is INCITS 378-2004. See Note 2
15.		Record Length (6.4.3)	MF	MV	$26 \leq L \leq 1574$	This connotes a 2 byte field. See Note 3
16.		CBEFF Product Identifier Owner (6.4.4)	MF	MV	> 0	See Note 4
17.		CBEFF Product Identifier Type (6.4.4)	MF	MV	> 0	See Note 4
18.		Capture Equipment Compliance (6.4.5)	MF	MV	1000b	Sensor complies with EFTS, Appendix F per PIV Registration requirement
19.		Capture Equipment ID (6.4.6)	MF	MV	> 0	See Note 5
20.		Size of Scanned Image in x direction (6.4.7)	MF	MV	MIT	See Note 11
21.		Size of Scanned Image in y direction (6.4.8)	MF	MV	MIT	
22.		X (horizontal) resolution (6.4.9)	MF	MV	197	Parent images conform to clause 4.2
23.		Y (vertical) resolution (6.4.10)	MF	MV	197	
24.		Number of Finger Views (6.4.11)	MF	MV	2	Once each for primary and secondary
25.		Reserved Byte (6.4.12)	MF	MV	0	
26.	K finger views	Finger View Header (6.5.1)	NC		A	
27.		Finger Position (6.5.1.1)	MF	MV	MIT	
28.		View Number (6.5.1.2)	MF	MV	0	See Note 10
29.		Impression Type (6.5.1.3)	MF	MV	0 or 2	Plain live or non-live scan images.
30.		Finger Quality (6.5.1.4)	MF	MV	20,40,60,80,100	See Note 6
31.		Number of Minutiae (6.5.1.5)	MF	MV	$0 \leq M \leq 128$	M minutiae data records follow
32.		Minutiae Type (6.5.2.1)	MF	MV	01b, 10b, or 00b	See Note 1
33.		Minutiae Position (6.5.2.2)	MF	MV	MIT	See Note 7
34.		Minutiae Angle (6.5.2.3)	MF	MV	MIT	See Note 8
35.		Minutiae Quality (6.5.2.4)	MF	MV	MIT	This may be populated.
36.		Extended Data Block Length (6.6.1.1)	MF	MV	0	See Note 0

END OF TABLE

³ Minutiae records conformant to the PIV specification are here http://www.itl.nist.gov/iad/894.03/nigos/piv_sample_data.html and these were prepared using NIST software available from <http://www.itl.nist.gov/iad/894.03/nigos/incits.html>

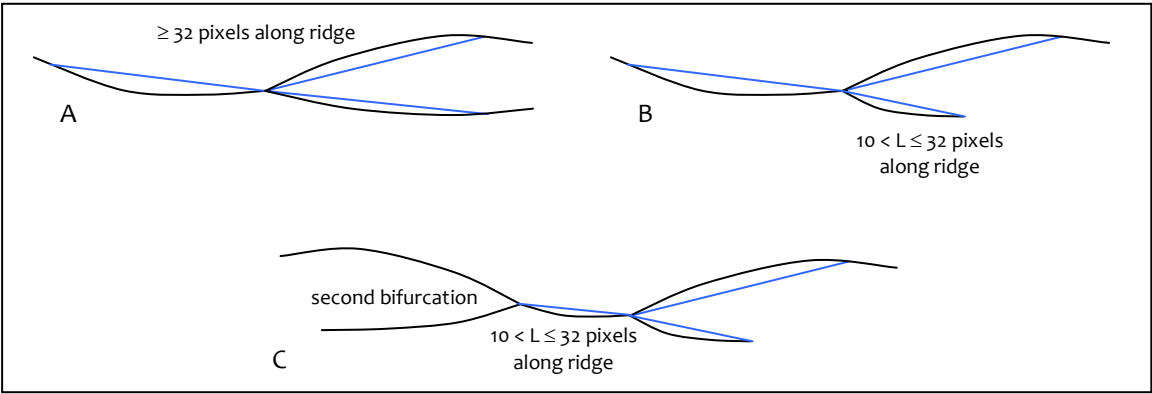
Acronym		Meaning
MF	mandatory field	[MINUSTD] requires a field shall be present in the FMR
MV	mandatory value	[MINUSTD] requires a meaningful value for a field
NC	normative content	[MINUSTD] gives normative practice for PIV. Such clauses do not define a field in the FMR.
A	as required	For PIV, value or practice is as normatively specified in [MINUSTD].
MIT	mandatory at time of instantiation	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:

- [MINUSTD] requires that each stored minutia have a type associated with it. For PIV, the mandatory card templates **shall** contain minutiae of type ridge ending or ridge bifurcation. These types are defined in [MINUSTD, 5.3.{2,3}]. Other types of minutiae, such as trifurcations and crossovers, **shall** not be included in PIV Card templates. However, for those minutiae where it is not possible to reliably distinguish between a ridge ending and a bifurcation, the category of "other" **shall** be assigned and encoded using bit values oob. The angle and location for a minutia of type "other" should be the angle and location that would have applied to the corresponding ridge ending or bifurcation depending on which one the encoding algorithm determines to be the most likely for that particular minutiae. This is a common characteristic of "inked" impressions that exhibit ridge endings being converted to bifurcations and vice-versa due to over- or under-inking in the image.
- The second paragraph of [MINUSTD, 6.4.2] refers both to an ASCII space and "three ASCII numerals" mentioned in the first paragraph. The practice of using an ASCII space character as the first character of the version number **shall** be followed: " 20|0" i.e. 0x20323000.
- 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.
- Both fields ("Owner" and "Type") of the CBEFF Product Identifier of [MINUSTD, Clause 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.
- The Capture Equipment ID **shall** be reported. Its use may improve interoperability.
- The quality value **shall** be that computed for the parent image using [NFIQ] and reported here as $Q = 20 \cdot (6 - \text{NFIQ})$. A value of "255" shall be assigned when fingerprints are temporarily unusable for matching. A value of "254" shall be assigned when the fingerprints are permanently unusable.
- 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.
- Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figures 2A through 2C illustrate the three methods used for determining the end of a leg. The ending is established according to the event that occurs first:
 - The 32nd pixel – see Figures 2A and 2B – or
 - The end of skeleton leg if greater than 10 pixels (legs shorter are not used) – see Figure 2B – or
 - A second bifurcation is encountered before the 32nd pixel – see Figure 2C.

The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

Figure 2 – Minutiae angle determination



Extensive, refined and complete guidance on minutia detection and estimation is contained in INCITS 378:2009 clause 6. That standard is the revision of INCITS 378-2004 [MINUSTD]. While PIV still requires [MINUSTD] for PIV template formatting, the newer standard improves the semantic aspects associated with this note.

9. The mandatory value of zero codifies the specification that PIV card templates **shall** not include extended data.
10. Per [MINUSTD, 6.5.1.2] this view number field **shall** have value 0 for the primary finger and 0 for the secondary finger. The combination of view number and finger position uniquely identifies each template.
11. [MINUSTD] does not specify how to report the image sizes in the header when two or more views are included in the record and these were derived from images of different sizes. For PIV, the width on Line 20 **shall** be the larger of the widths of the two input images. Similarly the height on Line 21 **shall** be the larger of the heights of the two input images.

4.5 Performance specifications for PIV compliance

4.5.1 Scope

This clause establishes performance specifications for minutia template generators and minutia matching algorithms. These specifications apply to off-card comparison of templates. Separate specifications are advanced for on-card comparison in clause 5.11. These components **shall** perform according to two sets of specifications

- interoperability specifications of clauses 4.5.3, and
- the accuracy specifications of clause 4.5.4.

The interoperability criteria implement the core global interoperability objectives of HSPD-12 by populating the PIV Card with interoperable enrollment templates. The accuracy specifications are intended to afford low operational error rates by assuring highly accurate matching in typical authentication scenarios.

4.5.2 Background

The intent of the [FIPS] specification of a globally interoperable biometric is to support cross-vendor and cross-agency authentication of PIV Cards. The multi-vendor aspect introduces a source of variation in performance [MINEX]. To support core algorithmic interoperability prior versions of this standard required

4.5.3 Minimum interoperability specification

The core cross-vendor interoperability specification is met by establishing requirements on template generators and template matchers as described in the following two sub-clauses.

4.5.3.1 Conformance of template generators

A template generator is certified on the basis of the conformance of its output, its speed of computation, and on the error rates observed when its templates are matched. A template generator **shall** be certified if:

1. it converts all input PIV representative enrollment images to Table 29 [MINUSTD] templates, and
2. all templates are syntactically conformant to the Table 29 profile of [MINUSTD], and
3. it converts 90% of PIV representative enrollment images to templates in fewer than 1.3 seconds⁴ each, and
4. all certified matchers verify its output templates with FNMR less than or equal to 1% at a FMR of 1%.

4.5.3.2 Conformance of template matchers

A template matcher is certified on the basis of its speed of computation, and on the error rates observed when it matches templates in interoperability tests. A template matcher **shall** be certified if:

5. it compares all pairs of Table 29 [MINUSTD] templates to scalar scores, and
6. it executes 90% of the clause D.4 template matches in fewer than 0.1 seconds⁴ each, and
7. it matches templates from all certified template generators, and the template generator accompanying the matcher, with FNMR less than or equal to 1% at a FMR of 1%.

4.5.3.3 Test method

The performance specifications shall be tested according to the test defined by Annex D. The Level 1 interoperability test embedded in NIST's MINEX III program⁵ implements this test [MINEX-III].

4.5.4 Minimum accuracy specification

The (1%,1%) interoperability criterion established in the clause 4.5.3.2 is designed to support low false rejection when templates can come from many sources (i.e. conformant template generators). As such the test does not imply thresholds relevant to the operational minimum security requirements advanced later in clause 4.6.3. To support operational authentication of PIV Card templates against live samples a template generator and matcher-pair shall be certified if

1. it meets all the interoperability criteria of clauses 4.5.3.1 and 4.5.3.2, and
2. it matches single-finger templates with FNMR less than or equal to 2.0% when the FMR is at or below 0.01%.

4.5.4.1 Test method

The performance specifications **shall** be tested according to the test defined by Annex D. The Level 2 accuracy test embedded in NIST's MINEX III program implements this test [MINEX-III].

4.6 Performance specifications for PIV operations

4.6.1 Scope

The test of clause 4.5 is intended only to qualify components demonstrating core minutiae-based interoperable accuracy. In particular, the error rate specification of clause 4.5.3 and 4.5.4 serves only to establish minutiae-generation and matching competencies in a laboratory test. This subclause establishes biometric performance parameters for components configured for use in operational PIV biometric authentication subsystems.

These specifications depart from prior versions of this standard which did not establish error-rate specifications for fielded biometric systems. In this version, minimum security specifications are established.

4.6.2 Background

The fingerprint templates conform to [MINUSTD] as profiled in clause 3.4. The use cases given in [800-73, Appendix C] detail how the templates and the PIV Card are used for interoperable authentication. Authentication may involve one or both of the PIV Card templates. These will be compared with newly acquired (i.e. live) fingerprint images of

⁴ This specification applies to a commercial-off-the-shelf PC procured in 2005 and equipped with a 2GHz processor and 512 MB of main memory. This specification **shall** be adjusted by the testing organization to reflect significant changes of the computational platform.

⁵ The MINEX III program, under the prior name *Ongoing MINEX* has continued since publication of NIST 800-76 in 2006.

either or both of the primary and secondary fingers. The inclusion of the finger position in the [MINUSTD] header allows the system to prompt the user for one or more specific fingers.

Operational authentication performance is quantified in terms of both the false reject rate (FRR) and the false accept rate (FAR). In PIV, FRR is 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 including: 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, and the familiarity of users with the process. The use of two fingers in all authentication transactions offers substantially improved performance over single-finger authentication.

4.6.3 Minimum accuracy specification

The threshold for the minutia matching algorithm shall be set to achieve false match rates at or below the values given in Table 7. The threshold shall be calibrated in tests conformant to clause 4.5.3.36. The tabulated rates are zero-effort match rates, meaning they apply to the comparison of single pairs of randomly selected templates from different persons.

PIV conformance to these specifications **shall** be supported by vendor attestation. Agencies could elect to conduct a biometric performance test to confirm the attestation.

Table 7 – Maximum permissible false match rates for off-card minutia comparison

PIV function	Maximum allowed FMR when two eyes are available and one or both eyes may be used	Maximum allowed FMR when two eyes are available and will always be used
PIV issuance, PIV re-issuance, PIV replacement	0.00006	0.00001
Unattended PIV physical access authentication	0.0005	0.00005
Unattended PIV logical access authentication	0.0002	0.00005

This specification does not:

- Preclude agencies from establishing more stringent lower false match criteria. The false match criteria can always be met by setting a low (i.e. stringent) comparison threshold. However, the lower threshold implies elevated false rejection errors because the error-rate tradeoff.
- Establish a false rejection performance criterion – how often genuine users are not able to successfully authenticate. The security objectives are the primary concern of this document. See

4.6.4 Further agency considerations

Agencies are cautioned that false rejection performance is operationally vital in access control applications and is achieved by using highly performing cameras, by correct control of the environment (e.g. humidity), adherence to enrolment specifications, subject and operator instruction, and by use of highly performing recognition algorithms. Agencies are therefore strongly encouraged to consider:

- Establishing a policy on how many times a subject can attempt to authenticate (three is typical)
- Establishing false rejection accuracy criteria against which tests and qualification procedures can be developed
- Referring to false rejection performance measures reported for algorithms conforming to the MINEX test and calibration procedure.
- Conducting their own supplementary tests. These might be performance tests of single products or interoperability tests, and might be used to estimate application-specific performance.
- Requiring the use of multiple samples (e.g. two fingers),
- Set operating thresholds to target lower (more stringent) false acceptance rates. This action would give moderately elevated rejection rates.
- Using iris recognition as an authentication alternative.

⁶ The Level 2 accuracy test embedded in NIST's MINEX III program estimates these thresholds [MINEX-III]

5. Fingerprint on-card comparison specifications

5.1 Scope

This clause gives specifications for the use of on-card comparison of fingerprint minutiae for PIV. This specification includes enrollment data to be placed on the card, authentication data to be sent to the card, the interface specifications to implement these actions, and certification information. This clause also specifies the data structure for the storage of card parameters, and the procedure for preparation of on-card fingerprint minutiae templates from off-card ones.

5.2 Background

NIST conducted two studies to support the use of on-card comparison in identity management applications.

- The Secure Biometric Match on Card⁷ activity engaged commercial providers to execute fingerprint authentication over a contactless interface within a specific time limit. The study required privacy protection via secured communication protocols and integrity protection using cryptographic signatures computed from the biometric data. In addition, the card was authenticated to the reader. The activity has been published as NIST Interagency Report 7452 [SBMOC].
- The MINEX II evaluation was initiated to measure the core algorithmic speed and accuracy of fingerprint minutia matchers running on ISO/IEC 7816 smartcards. Conducted in phases, the test required card- and fingerprint matcher-provider teams to submit on-card comparison enabled cards. The latest results were reported in NIST Interagency Report 7477 [MINEX II].

5.3 Approach to the use of standards

The PIV specification for on-card matching leverages international standards. Specifically, PIV cards **shall**

- Be prepared and used by executing the commands of ISO/IEC 7816-4:2005 [CARD-CMD],
- embed the biometric data in the data structures defined in ISO/IEC 7816-11:2004 [CARD-BIO],
- use the core three-byte-per-minutia format defined in both the ISO/IEC 19794-2:2011 standard⁸,
- adopt certain defined constants from ISO/IEC 19785-3:2007.

5.4 Data objects

5.4.1 Biometric Information Template

Each submitted card **shall** be populated with Biometric Information Templates grouped under the BIT Group Template of Table 8 according to the requirements of [CARD-CMD, Tables 1 and 2]. The number of BITs **shall** be equal to the number of fingerprint minutia templates (tag 81 in the DO of Table 11). After card issuance, BITs **shall** be treated as read-only data.

Table 8 – BIT group template and profile

Tag	Len.	Value			Allowed values
7F61	Var.	BIT group template			
		Tag	Len.	Value	
		02	1	1... 4 (Number of BITs in the group, corresponding to number of fingers that follow)	
		7F60	Var.	Biometric Information Template (BIT) for the first finger	
			Tag	Len.	Value
			83	1	Reference data qualifier used by VERIFY
			A1	Var.	Biometric Header Template (BHT) conforming to ISO/IEC 19785-3:2005
			Tag	Len.	Value
			81	1	biometric type (i.e modality, 08 = fingerprint)
					08

⁷ The preferred (and standardized) replacement for the trademarked term "match-on-card" is on-card comparison.

⁸ This second edition of the minutia standard was completed in January 2011 and is currently out for FDIS ballot. It will be formally published in the second half of 2011.

						82	1	biometric subtype (e.g. finger position) - These values shall be from ISO/IEC 19785-3:2007, NOT from ISO/IEC 19794-2			See NOTE 2 below
						87	2	CBEFF BDB format owner			0101 i.e. JTC1/SC37
						88	2	0x0005 (CBEFF BDB format type)			'00 05' See NOTE 1
						B1	Var.	Biometric matching algorithm parameters. ISO/IEC 19794-2 Table 14			
								Tag	Len.	Value	
								81	2	Min. and max. numbers of minutiae, see ISO/IEC 19794-2 (subclause 8.3.3, Table 10)	See NOTE 3
								82	1	Minutiae order, see ISO/IEC 19794-2:2005 (subclause 8.3.4 and Tables 11 and 12)	
								83	1	Feature handling indicator, see ISO/IEC 19794-2:2005 (Table 15)	
		7F60	Var.	Biometric Information Template (BIT) for the second finger, construction as above							

NOTE 1 The 0x0005 value indicated one of two encodings of minutiae defined in the ISO standard. This one requires that the endings of ridges are reported at the point of the valley bifurcation (versus at the ridge tip itself). These are the semantics required by INCITS 378:2004. The on-card comparison templates **shall** be produced from the parent INCITS 378 templates.

NOTE 2 Which fingers are present is encoded using integers from Table 9. The finger position codes differ in the fingerprint standards and the smart-card standards. For all on-card comparison operations ISO/IEC 19785-3:2007 finger position codes **shall** be used (column B). For the PIV mandatory off-card templates, [MINUSTD] finger positions **shall** be used (column A). Card issuance processes **shall** transcode using the mapping of Table 9.

Table 9 – ISO/IEC 19794-2 and ISO/IEC 19785-3 finger position codes

Finger ID Biometric subtype	ISO/IEC 19794-2:2011 + INCITS 378:2004		ISO/IEC 19785-3:2007	
	Binary value	Hex Value	Binary value	Hex Value
	A		B	
No information given	00000b	00	00000000b	00
right thumb	00001b	01	00000101b	05
right index	00010b	02	00001001b	09
right middle	00011b	03	00001101b	0D
right ring	00100b	04	00010001b	11
right little	00101b	05	00010101b	15
left thumb	00110b	06	00000110b	06
left index	00111b	07	00001010b	0A
left middle	01000b	08	00001110b	0E
left ring	01001b	09	00010010b	12
left little	01010b	0A	00010110b	16

NOTE 1 PIV readers involved in on-card and off-card authentication attempts will need to heed Table 9 to correctly prompt users for which finger to present.

NOTE 2 Note that the FDIS draft of ISO/IEC 19785-3:2007 erroneously set the six bit to 1. The final standard and the PIV specification require that bits 6, 7 and 8 **shall** be 0.

5.4.2 Minutiae data for on-card comparison

This clause defines the data to be sent to be stored on card-based comparison implementations. It is included here because ISO/IEC 19794-2:2011 and its antecedents defined multiple variants⁹.

All PIV on-card comparison data in PIV **shall** conform to the ISO/IEC 19794-2:2011, clause 9 compact on-card comparison format. This format encodes each minutia point in 3 bytes. The [MINUSTD] record instances of Table 6

⁹ Particularly the ISO/IEC 19794-2:2005 standard includes three encodings (record, card-normal, card-compact), has versions with and without headers, has variants differing in their minutia placement semantics, has presence of standardized extended data (zonal quality etc) and of non-standard, proprietary, extended data.

shall be converted to the ISO/IEC 19794-2:2005 compact-card templates of Table 10. The conversion is non-trivial and **shall** proceed according to the steps of Figure 3.

PIV Cards' on-card comparison data **shall** not include a header¹⁰. In addition, standardized extended data (e.g. cores) **shall** be absent. Proprietary extended data **shall** be absent. Thus, N minutiae are encoded in exactly 3N bytes.

Table 10 – ISO/IEC 19794-2 profile for on-card comparison

#	Field name	Size (bits)	Values allowed	Units	Remark
1.	X coordinate	8	[0,255]	Expressed in units of 0.1 mm	View data S instances of the minutiae data would be present
2.	Y coordinate	8	[0,255]	Expressed in units of 0.1 mm	
3.	Minutiae type	2			
4.	Minutiae angle	6	[0,63]	Resolution is 5.625 degrees	

These would be sent to the on-card biometric comparison implementations in the TLV format of Table 11. The cards would accept templates in that format.

Table 11 – Data object encapsulating ISO/IEC 19794-2 minutiae for on-card comparison

Tag	L	Value				Comment	Status
7F2E	L1	Biometric data template					Mandatory
		Tag	L	Value			
		82		This tag shall not be present		No proprietary data	Absent – None of these tags shall be present
		90		This tag shall not be present		No need for constructed data	
		91		This tag shall not be present		No ridge count data	
		92		This tag shall not be present		No cores	
		93		This tag shall not be present		No deltas	
		94		This tag shall not be present		No zonal quality	
		96		This tag shall not be present			Optional
		81	L2	Finger minutiae data from primary finger		Which finger is indicated in the first BIT	
				Field	Size (bits)	Valid Values	
				X coordinate	8	[0,255]	
				Y coordinate	8	[0,255]	
				Minutiae type	2		
				Minutiae angle	6	[0,63]	Mandatory if on-card comparison is enabled.
		95	1	Impression type	1	8	
		81	L2	Finger minutiae data from primary finger		Which finger is indicated in the second BIT	
				X coordinate	8	[0,255]	
				Y coordinate	8	[0,255]	
				Minutiae type	2		
				Minutiae angle	6	[0,63]	Optional
		95	1	Impression type	1	0	
		81	L2	Finger minutiae data from secondary finger		Which finger is indicated in the first BIT	
				X coordinate	8	[0,255]	
				Y coordinate	8	[0,255]	
				Minutiae type	2		
				Minutiae angle	6	[0,63]	Mandatory if on-card comparison is enabled.
		95	1	Impression type	1	8	
		81	L2	Finger minutiae data from secondary finger		Which finger is indicated in the second BIT	
				X coordinate	8	[0,255]	
				Y coordinate	8	[0,255]	
				Minutiae type	2		
				Minutiae angle	6	[0,63]	
		95	1	Impression type	1	0	

¹⁰ There was confusion in the industry, during early adoption of the compact formats, over whether the card formats should include record or view headers. The ILO Seafarer's program specified the presence of headers – Other programs used the ISO/IEC 7816-11 fields for such information.

5.5 Presence of finger minutiae extracted from swipe-sensor outputs

The minutia data of Table 11 allows for the inclusion of minutia data extracted from swipe sensors. Because of motion of the finger across such sensors the minutiae can be systematically misplaced relative to a static plain impression. It is widely believed that comparison of plain and swipe minutia fields is more likely to produce genuine user failed authentication for genuine users than is plain-plain comparison and swipe-swipe comparison. The specification, as drafted, would allow a swipe sensor to be used in an authentication attempt. In such cases the card should preferentially compare the submitted swipe data with the on-card swipe data.

Swipe sensors shall not be used for authentication in PIV issuance and re-issuance processes. Swipe sensors may be used for other authentication.

Swipe sensor specifications appear in clause 6.3.

EDITOR's NOTE: The specifications are circulated for public comment. Unlike much of the other content NIST has 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. NIST solicits input on swipe accuracy and viability, particularly regarding

- interoperability with optically-derived templates,
- operating with standardized minutia templates (vs. proprietary representations),
- operational experiences,
- liveness,
- how minutia standards might be revised,
- whether these provisions should be allowed only after a certain date (sunrise).

All swipe-related specifications may be withdrawn in the next version of this draft.

5.6 Minutia uniqueness

A non-ISO requirement is for the minutia points to be unique. Template generators should output unique (x, y, and theta) tuples and the testing laboratory might implement checks to detect deviations from such behavior. This requirement is instituted because non-uniqueness impedes some matching algorithms.

5.7 Preparation of the minutia templates

All templates used in on-card comparison **shall** be prepared from the INCITS 378 templates required by clause 4. The process for this conversion **shall** follow the algorithm specified in this subclause.

The BITs of clause 5.4.1 **shall** be used to parameterize the production of templates that a reader, or other system, sends to the PIV card. This applies to both the reference templates stored on the card, and those produced during, for example, an authentication transaction.

The BITs read from the card **shall** parameterize the conversion of templates sent to the card. As depicted in Figure 3, the conversion operation proceeds with a pruning operation (sec. 5.9.1), a sorting operation (sec. 5.9.2), and a re-encoding (conversion from 14 bit to 8 bit position coordinates, quantization of coordinates, and conversion of 8 bit to 6 bit minutia angle).

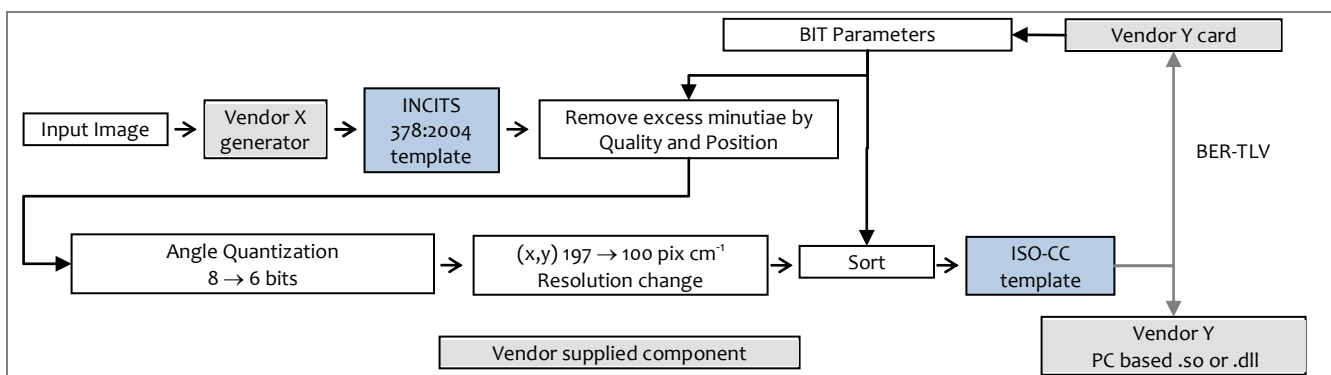


Figure 3 – Conversion of INCITS 378 to ISO/IEC 19794-2 card data

5.8 Number of minutiae

The number of minutiae stored on a PIV Card for on-card comparison **shall** not exceed 83 for any one finger.

The number of minutiae sent to a PIV Card for on-card comparison **shall** not exceed 83 for any one finger.

NOTE 1 Leading commercial minutia detectors produce a median of 41 minutiae from plain impression images with the 5% and 95% quantiles being 24 and 61 respectively over four large operational single index finger datasets [2].

NOTE 2 A short-length APDU command constrains the maximum number of three-byte minutia to 83. Command chaining [CARD-CMD] would ordinarily be used for larger templates, but the PIV limit of 83 reflects NOTE 1.

Because some templates will naturally contain 0 minutiae (i.e. the algorithm does not find any), the (off-card) client **shall** respect the minimum number indicated by the card in its BIT structure. The client **shall** either terminate the minutia-based authentication attempt or prompt for (re-)presentation of one of the enrolled fingers.

5.9 Effect of the BIT

All reference and verification templates **shall** be parameterized by the BIT parameters, as follows. If,

- the value indicated in the BIT for the minimum number of minutiae is $0 \leq N \leq 83$,
- the value indicated in the BIT for the maximum number of minutiae is $N \leq M \leq 83$,
- the number of minutiae present in a verification template is K , then
- the number of minutiae sent to the card, S , **shall** be

$$S = \begin{cases} M & \text{if } K \geq M \\ K & \text{if } K < M \\ K & \text{if } K < N \end{cases}$$

Note that the BIT parameter N is ignored. This is necessary because some input templates will inevitably have zero minutiae. The comparison subsystem should execute successfully when either or both of the input templates contains fewer than N minutiae. For all cards, N **shall** be $\leq M$.

5.9.1 Minutiae removal mechanism

Minutiae shall be removed according to the specifications of [CARD-MIN, clause 9.3.2].

5.9.2 Sort order of minutiae

The BIT associated with the on-card comparison algorithm **shall** indicate how minutiae must be sorted according to the options extended in [CARD-MIN, clause 9.4]. However, because single finger PIV images have widths of fewer than 500 pixels when scanned at $19.7 \text{ pixels mm}^{-1}$, all possible minutiae coordinates **shall** be encoded in 8 bits, and the modulo sorting technique defined in [CARD-MIN] **shall not** be used.

NOTE Open-source INCITS 378 "C" code is maintained in <http://www.itl.nist.gov/iad/894.03/nigos/biomdi.html>. On-card biometric comparison client software is here: <http://www.itl.nist.gov/iad/894.03/nigos/biomapp.html>.

5.10 On-card comparison interface

PIV cards implementing on-card comparison **shall** support the interface requirements of Annex A.

5.11 Performance specifications for PIV compliance

5.11.1 Scope

This clause establishes performance specifications for minutia template generators and minutia matching algorithms. These specifications apply to on-card comparison of templates. Separate specifications are advanced for off-card comparison in clause 4.5. These components **shall** perform according to two sets of specifications

- interoperability specifications of clauses 5.11.3, and
- the accuracy specifications of clause 5.11.4.

The interoperability criteria implement the core global interoperability objectives of HSPD-12 by populating the PIV Card with interoperable enrollment templates and an associated on-card comparison algorithm. The accuracy

specifications are intended to afford low operational error rates by assuring highly accurate matching in typical authentication scenarios.

5.11.2 Background

NIST conducted tests of on-card comparison performance in its MINEX II program [MINEX-II]. Over four phases conducted between 2007 and 2010, the program showed that up to five implementations might attain the PIV interoperability specifications of clause 4.5.3.

In parallel, the sBMOc [SBMOc] demonstrated cryptographic protection of the template data, and transactional durations below two seconds.

5.11.3 Minimum interoperability specification

The core cross-vendor interoperability specification is met by establishing requirements on paired template generators and on-card matchers as described in the following two sub-clauses.

5.11.3.1 Conformance of on-card template generators

A template generator **shall** be certified if

1. it conforms to the off-card template generator specifications of clause 4.5.3.1, and
2. it converts all Table 29 [MINUSTD] instances to Table 10 [CARD-MIN] instances according to the specifications of clause 5.7.

5.11.3.2 Conformance of on-card template matchers

A template matcher is certified on the basis of its speed of computation, and on the error rates observed when it matches templates in interoperability tests. A template matcher **shall** be certified

1. if it conforms to the off-card template matcher specifications of clause 4.5.3.2 but operating with Table 10 [CARD-MIN] format templates, and
2. it compares 90% of on-card genuine-user template comparisons (using the command of clause A.4.1) in fewer than 0.25 seconds, and
3. when implemented on a functional modified PIV Card and in a software library, the two will produce identical output similarity scores¹¹,
4. it produces at least 512 unique integer scores when comparing many templates of different persons.

5.11.3.3 Test method

The performance specifications shall be tested according to the test defined by Annex D modified to use [CARD-MIN] templates. This test shall conform to the requirements of the ISO/IEC 19795-7 testing standard. The Level 1 interoperability test embedded in NIST's MINEX IV program¹² implements this test [MINEX-IV].

5.11.4 Minimum accuracy specification

The (1%,1%) interoperability criterion established in the clause 4.5.3.2 is designed to support low false rejection when templates can come from many sources (i.e. conformant template generators). As such the test does not imply thresholds relevant to the operational minimum security requirements advanced later in clause 4.6.3. To support operational authentication of PIV Card templates against live samples a template generator and matcher-pair shall be certified if

5. it meets all the interoperability criteria of clauses 4.5.3.1 and 4.5.3.2, and
6. it matches single-finger templates with FNMR less than or equal to 2.0% when the FMR is at or below 0.01%.

¹¹ This requirement implies a non-operational requirement: the Card must report similarity scores to a dedicated test application.

¹² The MINEX IV program replaces the original MINEX II proof-of-concept evaluation which ran 2007-2011.

5.11.4.1 Test method

The performance specifications shall be tested according to the test defined by Annex D. The Level 2 accuracy test embedded in NIST's MINEX IV program implements this test [MINEX-IV].

5.12 Performance specifications for PIV operations

5.12.1 Scope

The tests of clause 5.11 are intended only to qualify components demonstrating core minutiae-based interoperable accuracy. In particular, the error rate specification of clause 4.5.3 and 4.5.4 serves only to establish minutiae-generation and matching competencies in a laboratory test. This subclause establishes minimum security specifications and performance parameters for components configured and used in operational PIV biometric authentication subsystems.

5.12.2 Minimum accuracy specification

The threshold for the minutia matching algorithm shall be set to achieve false match rates at or below the values given in Table 12. The threshold shall be calibrated in tests conformant to clause 4.5.3.3¹³. The tabulated rates are zero-effort match rates, meaning they apply to the comparison of single pairs of randomly selected templates from different persons.

PIV conformance to these specifications shall be supported by vendor attestation. Agencies could elect to conduct a biometric performance test to confirm the attestation.

Table 12 – Maximum permissible false match rates for on-card minutia comparison

PIV function	Maximum allowed FMR when two eyes are available and one or both eyes may be used	Maximum allowed FMR when two eyes are available and will always be used
Unattended PIV physical access authentication	0.0005	0.00005
Unattended PIV logical access authentication	0.0002	0.00005

This specification does not:

- Preclude agencies from establishing more stringent lower false match criteria. The false match criteria can always be met by setting a low (i.e. stringent) comparison threshold. However, the lower threshold implies elevated false rejection errors because the error-rate tradeoff.
- Establish a false rejection performance criterion – how often genuine users are not able to successfully authenticate. The security objectives are the primary concern of this document. See

5.12.3 Further agency considerations

See clause 4.6.4.

¹³ The Level 2 accuracy test embedded in NIST's MINEX IV program estimates these thresholds [MINEX-III]

6. Sensor specifications for fingerprint capture

6.1 Scope

This clause gives specifications for all fingerprint sensors used for capture of single finger images. These specifications are unrelated to those of clause 3 which govern ten-print enrollment. Table 13 specifies sensor usage.

Table 13 – PIV use of plain-impression and swipe fingerprint sensors

PIV Fingerprint Sensor Class	Attended use for preparation of the PIV Card	Attended PIV processes	Unattended biometric authentication	Available for off-card authentication	Available for on-card authentication	Specifications
Plain impression sensors	Mandatory	Mandatory	Optional	Yes	Yes	6.2
Swipe sensors	Optional	Not allowed	Optional	No	Yes, with swipe-derived templates	6.3

6.2 Fingerprint acquisition specifications for plain impression sensors

Fingerprint sensors used for PIV authentication **shall** conform to the FBI's Image Quality Specifications For Single Finger Capture Devices [SINGFING]. The [SINGFING] specification establishes minimum sizes for the imaging platen and for the scanning resolution.

6.3 Fingerprint acquisition specifications for swipe sensors

A swipe sensor **shall** be certified if

- It produces images of width corresponding to at least 9 millimeters
- It produces, in conjunction with client-side software, a Table 4 [FINGSTD] instance but with Image Acquisition Level (Lines 3 and 19) of 30 or 31. This requires spatial sampling rates in both horizontal and vertical directions to be 197 pixels per centimeter (i.e. 500ppi).
- The sensor passes a biometric performance test that
 - Is conducted in conformance to [PERF-ACS],
 - Reports three attempt FTE < 1%.
 - Reports three attempt FRR < 1% and FAR < 0.1% using only a PIV compliant template generator and matcher.
 - Retains Table 4 [FINGSTD] images to be used in offline comparisons and confirmation of the online results for which FMR against plain-impression derived templates shall be at or below 0.01%.

7. Iris recognition specifications

7.1 Scope

This clause establishes specifications to support the use of iris images as defined in FIPS 201-2. The clause includes specifications

- for iris images stored on and off PIV Cards,
- for iris capture devices, and
- for components involved in automated recognition of PIV iris imagery.

The image specifications extend the format requirements of ISO/IEC 19794-6:2011 with image quality related properties. The capture device specifications concern imaging properties of the iris camera, and software interfaces around it. The recognition component is specified in terms of minimum authentication accuracy and processing speed.



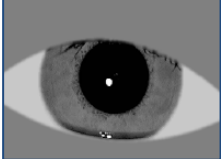
Label	A	B	C
Example Image			
ISO/IEC 19794-6:2011	Image Type 1	Image Type 3	Image Type 7
Properties	Parent image, typically the output of a camera, and typically of size 640x480 pixels, not necessarily centered, but conformant to Image Type 1 of [ISOIRIS]. Images of this kind are not intended to be compressed.	Cropped and centered iris conformant to Image Type 3 of [ISOIRIS]. Images of this kind can be losslessly compressed to tens of kilobytes.	Cropped, masked and centered iris conformant to Image Type 7 of [ISOIRIS]. Images of this kind can be compressed to a few kilobytes.
PIV Role	Image captured from camera, retained for chain-of-trust authentication.	Prepared from (A), it may be retained as an alternative to (A). It will require less storage space.	Prepared from (A), it shall be stored on the PIV card.

Figure 4 – Image formats of ISO/IEC 19794-6:2011

This document makes no mention of an iris template. In iris recognition, templates are proprietary non-standardized mathematical encodings¹⁴ of information extracted from the formally standardized images that are defined in this document.

7.2 Background

Digital representations of rectilinear images of the human iris have been formally standardized as ISO/IEC 19794-6:2011. This standard, which replaces earlier editions, is a necessary component in an interoperable marketplace of iris cameras and iris recognition algorithms. For PIV, the standard is used because it includes specialized image formats that support compact storage¹⁵ on ISO/IEC 7816 IC cards. The formats are shown in Figure 4.

¹⁴ The iris code is one such representation that has been widely described in the academic literature, and implemented still more widely. While it is known for its power, small size, and speed, other (commercial) template representations are actually larger than the specialized PIV Card images mandated in this document.

¹⁵ The first generation of iris image standards included a polar-coordinate encoding of the iris. This format, intended to support compact size, was removed from second generation standards because of concerns that interoperability was sensitive to correct determination of the iris center. An alternative, replacement format, shown in Figure 4C, has been shown to offer accurate recognition and broad industry support [IREX].

7.3 Iris data Retention

7.4 Iris image specification for PIV cards

Iris images on PIV Cards **shall** conform to the requirements expressed in the Table 14 profile of the ISO/IEC 19794-6:2011 standard. Where required values and practice are not stated, the underlying requirements of the base standard **shall** apply. The profile defines a standard record that contains one or two specialized iris images each of size around 3 kilobytes. These images **shall** follow the semantic requirements of Image Type 7 images defined in the standard. The objective of these specifications is to afford maximum possible iris accuracy, low storage requirements, and corresponding fast read times. These requirements include centering and masking of the eyelid and sclera regions (an example is shown in Figure 4, column C). The masked regions can be very efficiently compressed. This affords small record sizes and, vitally, preservation of the iris texture.

Table 14 – ISO/IEC 19794-6 profile for iris images stored on PIV Cards

		Clause or field of ISO/IEC 19794-6	ISO/IEC 19794-6		PIV Conformance	Remarks
			Field	Value	Values Allowed	
1.	Iris General Header	CBEFF Header	MF	MV	Patron format PIV	Multi-field CBEFF Header. Sec. 0.
2.		Format identifier	MF	MV	0x49495200	IIR\0 Four byte format identifier including null terminator.
3.		Version number	MF	MV	0x30323000	020\0 Second 19794-6 version - not the 2005 standard
4.		Length of record	MF	MV	See NOTE 1	The length (in bytes) of the entire iris image data.
5.		Number of iris representations	MF	MV	1 or 2 0:	Number of iris representations that follow. This shall be two, either one of each eye, or two of one eye.
6.		Certification flag	MF	MV	0x00	
7.		Number of eyes represented	MF	MV	1 or 2	2 if left and right are known present, else 1 if left or right is known present. If camera does not estimate eye label automatically, these shall be manually assigned.
Representation 1: Data for the first eye image follows						
8.	Representation Header + Image Data	Representation Length	MF	MV		Bytes for this representation including the header + image
9.		Capture date and time	MF	MV	2011 onwards.	Capture start time in UTC
10.		Capture device technology identifier	MF	MV	0x00 0x01	Unknown or Unspecified CMOS/CCD
11.		Capture device vendor ID	MF	MV		Manufacturer ID
12.		Capture device type ID	MF	MV		Vendor assigned make model product ID.
13.		Quality block	MF	OIT		
14.		Representation number	MF	MIT	1 and then, optionally, 2	Representation sequence number
15.		Eye label	MF	MIT	1 or 2	Left, right. If camera does not estimate eye label automatically, these shall be manually assigned.
16.		Image type	MF	MV	7	IMAGE_TYPE_CROPPED_AND_MASKED = 7 (07 _{Hex}) i.e. a cropped and region-of-interest masked, centered, iris image with (0,6R 0,2R) margins. See NOTE 2
17.		Image format	MF	MV	10 = 0x0A	Compression algorithm and encoding shall be JPEG 2000. The format shall not be PNG, RAW, or JPEG.
18.		Iris image properties bit field	MF	MIT MIT MV MV	Bits 1-2: 01 or 10 Bits 3-4: 01 or 10 Bits 5-6: 01 Bits 7-8: 01 Bit 1 is the least signif. bit. Bit 8 is the most signif. bit.	Horizontal + vertical orientation shall not be undefined Scan type shall be progressive. Compression history shall be none; i.e. the cropped and masked image shall be prepared from an uncompressed parent image.
19.		Image width, W	MF	MIT	222 ≤ W ≤ 424	width in pixels, W
20.		Image height, H	MF	MIT	168 ≤ H ≤ 336	height in pixels, H
21.		Bit depth	MF	MV	8	Bit depth in bits per pixel
22.		Range	MF	OIT		Required field, optionally populated.
23.		Roll angle of eye	MF	OIT	≤ 20	Camera or software should estimate roll angle. Rotation should only be applied if angle is > 20 deg.
24.		Roll angle uncertainty	MF	OIT	≤ 5	
25.		Iris centre, lowest X	MF	MV	W/2 for W odd, else	These values are redundant for Image type = 7 shall for which image shall be exactly centered. The iris center shall be estimated by the iris localization code, or if necessary by a human inspector.
26.		iris centre, highest X	MF	MV	W/2+1 for W even	
27.		Iris centre, lowest Y	MF	MV	H/2 for H odd, else	
28.		Iris centre, highest Y	MF	MV	H/2+1 for H even	
29.		Iris diameter, lowest	MF	MIT	D ≥ 140	These two fields are used to express a normative PIV requirement that iris radius shall be no smaller than 70 pixels, and no larger than 140 pixels. See NOTE 3
30.		Iris diameter, highest	MF	MIT	D ≤ 280	
31.		Image length	MF		1 ... approx 6KB	Size of the JPEG 2000 encoded image data, in bytes, is limited

						by container defined in NIST Special Pub 800-73, and the size of its CBEFF header and digital signature.
Representation 2: Data for the second eye image follows						
Analogous to Representation 1, above.						

945

946

947

948

949

950

951

952

953

954

NOTE 1 The entire record length plus the CBEFF header and CBEFF signature block length must be less than or equal to size specified in NIST Special Publ. 800-73-3. Two images of size about 3K, or one image of size about 6K, will fit in this container.

NOTE 2 The specification of a Type 7 image requires that the image captured from the camera has sufficient margin around the iris to support the strict (0.6R, 0.2R) margin requirements of Image Type 7. During enrollment, client capture software might usefully display the result with a prototypical overlay.

NOTE 3 If any captured iris has diameter outside of the range [140,280] pixels, see clause 7.8.1.1.4.

7.5 Iris image specification for iris images retained outside the PIV card

This document neither requires nor precludes agencies from retaining iris images. FIPS 201-2 does require use of iris imagery in cases where fingerprints cannot be captured satisfactorily. In addition, FIPS 201-2 indicates that iris image data may be available outside the PIV Card for authentication during PIV card re-issuance, replacement and chain-of-trust transactions. If agencies elect to retain images they **shall** be stored in the format specified in this clause. This clause establishes a profile of ISO/IEC 19794-6:2011 suited for retention of iris images outside the PIV Card. The format specification includes the [CBEFF] header of clause 9, and this requires integrity protection and allows for encryption of the image records.

This document neither requires nor precludes agencies from retaining iris templates. Iris templates are vendor-proprietary and not standardized. Nevertheless, if an agency elects to retain templates then they **shall** be embedded in the [CBEFF] header of clause 9. This requires integrity protection and allows for encryption of the records.

Retention of data supports, for example, detection of duplicate identities.

966

Table 15 – ISO/IEC 19794-6 profile for iris images stored outside PIV Cards

		Clause or field of ISO/IEC 19794-6	ISO/IEC 19794-6		PIV Conformance	Remarks
			Field	Value	Values Allowed	
1.	Iris General Header	CBEFF Header (5.3)	MF	MV	Patron format PIV	Multi-field CBEFF Header. Sec. o.
2.		Format identifier	MF	MV	0x49495200	IIR\o Four byte format identifier including null terminator.
3.		Version number	MF	MV	0x30323000	020\o Second 19794-6 version - not the 2005 standard
4.		Length of record	MF	MV		The length (in bytes) of the entire iris image data.
5.		Number of iris representations	MF	MV	2	Number of iris representations that follow. This shall be two, preferably one of each eye, or two of one eye.
6.		Certification flag	MF	MV	0x00	Is certification information present in the representation headers?
7.		Number of eyes represented	MF	MV	1 or 2	2 if left and right are known present, else 1 if left or right is known present.
Representation 1: Data for the first eye image follows						
8.	Representation	Representation Length	MF	MV		Bytes for this representation including the header + image
9.		Capture date and time	MF	MV	2011 onwards.	Capture start time in UTC
10.		Capture device technology identifier	MF	MV	0x00 0x01	Unknown or Unspecified CMOS/CCD
11.		Capture device vendor ID	MF	MV		Manufacturer ID
12.		Capture device type ID	MF	MV		Vendor assigned make model product ID.
13.		Quality block	MF	OIT		
14.		Representation number	MF	MIT	1 and then 2	Representation sequence number

15.	Eye label	MF	MIT	1 or 2	Left, right. If camera does not estimate eye label automatically, these shall be manually assigned.
16.	Image type	MF	MV	1 or 2	IMAGE_TYPE_UNCROPPED = 0x01 or IMAGE_TYPE_VGA = 0x02 i.e. 640 x 480 pixels See NOTE 1
17.	Image format	MF	MV	14 = 0x0E	Compression and encoding shall be PNG or RAW.
18.	Iris image properties bit field	MF	MIT MIT MV MV	Bits 1-2: 01 or 10 Bits 3-4: 01 or 10 Bits 5-6: 01 Bits 7-8: 01 Bit 1 is the least signif. bit. Bit 8 is the most signif. bit.	Horizontal + vertical orientation shall not be undefined Scan type shall be progressive. Compression history shall be none; i.e. the cropped and masked image shall be prepared from an uncompressed parent image.
19.	Image width, W	MF	MIT	> 0	width in pixels, W
20.	Image height, H	MF	MIT	> 0	height in pixels, H
21.	Bit depth	MF	MV	8	Bit depth in bits per pixel
22.	Range	MF	OIT		Required field, optionally populated.
23.	Roll angle of eye	MF	OIT	≤ 20	Camera or software should estimate roll angle. Rotation
24.	Roll angle uncertainty	MF	OIT	≤ 5	should only be applied if angle is > 20 deg.
25.	Iris centre, lowest X	MF	MIT		These values are redundant for Image type = 3 for which image shall be exactly centered. The iris center shall be estimated by the iris localization code, or if necessary by a human inspector.
26.	iris centre, highest X	MF	MIT		
27.	Iris centre, lowest Y	MF	MIT		
28.	Iris centre, highest Y	MF	MIT		
29.	Iris diameter, lowest	MF	MIT	≥ 140	These two fields are used to express a normative PIV requirement that iris radius shall be no smaller than 70 pixels, and no larger than 140 pixels. See NOTE 2
30.	Iris diameter, highest	MF	MIT	≤ 280	
31.	Image length	MF	MIT		Size of the PNG encoded image data, in bytes, is limited by container defined in NIST Special Pub 800-73, and the size of its CBEFF header and digital signature.
Representation 2: Data for the second eye image follows					
Analogous to Representation 1, above.					

967

968

969

970

NOTE 1 The specification of unprocessed Type 1 or 2 image nevertheless requires that the margin around the iris exceeds or equals, respectively, the (0.6R, 0.2R) margin requirements. During enrollment, client capture software might usefully display the result with a prototypical overlay.

971

NOTE 2 If any captured iris has diameter outside of the range [140,280] pixels, see clause 7.8.1.1.4.

972

7.6 Conformance of ISO/IEC 19794-6:2011 records

973

974

975

976

977

For the standard records of clauses 7.4 and 7.5, implementers may wish to download¹⁶ NIST developed and maintained open-source software for testing the syntactic correctness of the record. The software exists in two forms: One runs under a conformance testing architecture; the other runs as a standalone. They can run in single-instance or batch mode. NOTE: The tools do not yet check PIV specific parameters - definitive final versions that do will follow.

978

7.7 Iris image properties for enrollment

979

7.7.1 Scope

980

981

These sub-clauses regulate the appearance and properties of the iris images captured during the preparation of PIV Card iris images.

982

7.7.2 Correct segmentation of the iris

983

984

985

986

For iris captures intended for population of the PIV Card, the client software **shall** display the captured image to the attending operator. The software **shall** overlay colored circular or elliptical approximations to the pupil-iris and iris-sclera boundaries. The attendant **shall** inspect the image to verify that the estimated boundaries correspond to the actual locations.

¹⁶ From http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm

7.7.3 Correct preparation of the cropped-and-masked PIV Card iris.

For iris captures intended for population of the PIV Card, the client software **shall** display the prepared image to the attending operator. The attendant **shall** inspect the image and determine that the iris is centered, and that the iris itself is visible.

7.7.4 Blur

For iris captures intended for population of the PIV Card, the client software **shall** display the captured image to the attending operator. The attendant **shall** inspect the image for evidence of blur; this will be apparent if the eye lashes do not appear as crisp lines.

7.8 Performance specifications for PIV compliance

The core cross-vendor interoperability specification is met by establishing requirements on iris cameras and on components preparing and matching [IRISSTD] records as described in sub-clauses 7.8.1.1, 7.8.1.2, and 7.8.1.3

7.8.1.1 Conformance of iris cameras

7.8.1.1.1 Scope

The following sub-clauses support interoperable recognition of iris images. The sub-clauses of this clause regulate the iris camera interface, iris camera properties and, separately, image-specific properties.

7.8.1.1.2 Number of eyes captured

All PIV enrollment, re-issuance, and registration office operations **shall** be performed using cameras capable of imaging both eyes of the PIV applicant simultaneously, or each eye sequentially.

PIV authentication attempts **shall** be performed using cameras capable of imaging one or two eyes of the PIV cardholder.

7.8.1.1.3 Rectilinear imaging and aspect ratio

The output of the camera **shall** be a rectilinear image of the iris region. The digital representation of the iris **shall** have an aspect ratio between 0.98 and 1.02. This requires that the pixel pitch along the two axes of the sensor substrate **shall** be equal to within 4%.

7.8.1.1.4 Iris size

All iris images prepared in PIV (for cards, for authentication and other purposes) **shall** have an iris radius between 70 and 140 pixels. This should usually be achieved by appropriate optical design of the imaging system.

If the camera or client software detects an iris of radius outside this range, re-capture of the PIV cardholder should be attempted at least two times. If the iris radius remains outside the range, a conformant image **shall** be prepared by re-sampling using an interpolation algorithm of cubic or higher order, e.g. bi-cubic interpolation.

7.8.1.1.5 Spectral properties of the illuminant

The iris camera **shall** use one or more dedicated infra-red illuminators. The spectrum **shall** be such that 95% of the power **shall** be between 720 and 870nm, and 35% of the power **shall** exist within each and every 100nm band in that interval. The spectral measurement **shall** be time-averaged over an interval comparable with the duration of an iris capture attempt.

7.8.1.1.6 Safety of the illuminant

The camera **shall** conform to the limits specified for infrared illumination given in [ICNIRP-LED, ICNIRP-BB] and the threshold limit values specified in [ACGIH].

7.8.1.1.7 Performance specifications for PIV cameras

The camera **shall** support accurate recognition. An iris camera **shall** be certified if

- It produces, in conjunction with client-side software, both
 - Conformant Table 14 [IRISSTD, Image Type 7] instances suitable for enrollment on PIV cards,

- 1029 ☐ Conformant Table 15 [IRISSTD, Image Type 1] instances suitable for use in an authentication transaction,
- 1030 — It passes a biometric performance test that
 - 1031 ☐ Is conducted in conformance to [PERF-ACS],
 - 1032 ☐ Reports three attempt FTE < 1%
 - 1033 ☐ Reports three attempt FRR < 1% and FAR < 0.1% using only a PIV compliant [IRISSTD] generator and matcher.
 - 1034 ☐ Retains all [IRISSTD] images to be used in offline comparisons and confirmation of the online results for
 - 1035 which FMR shall be at or below 0.01%.
- 1036 — It refuses to output images when presented with images of irises printed
 - 1037 ☐ on three substrates including one IR-transparent one,
 - 1038 ☐ at life-like sizes, and
 - 1039 ☐ with and without a prototypical facial surround,
- 1040 — and collected in both
 - 1041 ☐ visible light and printed in both color and in grayscale
 - 1042 ☐ infra-red light and printed in grayscale

1043 Users of this standard are cautioned that these camera specifications support 1:1 authentication. They are likely
 1044 insufficient for 1:N identification applications and should not be used to qualify cameras for such.

1045 EDITOR'S NOTE 1 The requirement for the camera to pass a biometric performance test is instituted until such time
 1046 as an imaging specifications and associated test methods are developed. Such an approach is used for ten-print
 1047 fingerprint scanners [APP/F]. Only certain elements are currently available for iris cameras.

1048 EDITOR'S NOTE 2 A more detailed profile of [PERF-ACS] is under development.

1049 7.8.1.2 Conformance of iris record generators

1050 Production of the standard PIV records of clause 7.4 is a non-trivial task because it requires iris detection, and
 1051 localization, and preparation of the Figure 4C image. A standard record generator **shall** be certified if:

- 1052 1. it converts all input PIV representative captured images to Table 14 [IRISSTD] records, and
- 1053 2. all records are syntactically conformant to [IRISSTD], and
- 1054 3. it converts 90% of PIV representative captured images to Table 14 [IRISSTD] records in fewer than 0.5
 1055 seconds¹⁷ each, and
- 1056 4. all certified matchers verify its records with FNMR less than or equal to 1% at an FMR of 0.01%.

1057 7.8.1.3 Conformance of iris image matchers

1058 A recognition algorithm is certified on the basis of its speed of computation, and on the error rates observed when it
 1059 matches records in interoperability tests. A recognition algorithm **shall** be certified if:

- 1060 1. it compares all pairs of Table 29 [MINUSTD] templates to scalar scores, and
- 1061 2. it executes 90% of its native template comparisons in fewer than 0.1 seconds⁴ each, and
- 1062 3. it matches Table 14 [IRISSTD] records from all certified record generators with FNMR less than or equal to 1%
 1063 at a FMR of 1%.

1064 7.8.1.4 Test methods

1065 The performance specifications of clauses 7.8.1.2 and 7.8.1.3 shall be tested in an offline test using sequestered image
 1066 data. NIST's expects to establish the IREX IV program to implement this test.

¹⁷ This specification applies to a commercial-off-the-shelf PC procured in 2005 and equipped with a 2GHz processor and 512 MB of main memory. This specification **shall** be adjusted by the testing organization to reflect significant changes of the computational platform.

7.9 Performance specifications for PIV operations

7.9.1 Iris capture interface

For all PIV processes (initial enrollment, issuance, reissuance, and authentication), the iris camera or its client software **shall** implement the capture interface given in Annex B.

7.9.2 Iris recognition interface

For all PIV processes requiring iris recognition (e.g. authentication), the camera or its client software **shall** implement the recognition interface given in Annex C.

7.9.3 Iris recognition minimum accuracy requirements

FIPS 140 establishes minimum specifications for authentication for activation of crypto-modules. This clause defines analogous specifications for one-to-one iris recognition attempts.

7.9.4 Requirements

The threshold for the iris recognition algorithm **shall** be set to achieve false match rates at or below the values given in Table 16. These rates are zero-effort match rates, meaning they apply to the comparison of single pairs of randomly selected images from different persons.

Table 16 – Maximum permissible false match rates for iris comparison

PIV function	Maximum allowed FMR when only one eye is planned to be used	Maximum allowed FMR when two eyes are planned to be available and one or both eyes may be used	Maximum allowed FMR when two eyes are planned to be available and will always be used
PIV issuance, PIV re-issuance	0.00003	0.00006	0.00001
PIV replacement	0.00003	0.00006	0.00001
PIV physical access authentication	0.0001	0.0004	0.00003
PIV logical access authentication	0.0001	0.0006	0.00003

This specification does not establish false rejection performance – how often genuine users are not able to successfully authenticate. The false match criteria can trivially be met by setting a low (i.e. stringent) comparison threshold. A lower threshold implies elevated false rejection errors. Agencies are cautioned that false rejection performance is operationally vital in access control applications and is achieved by using highly performing cameras, by correct control of the environment, adherence to enrolment specifications, subject and operator instruction, and by use of highly performing recognition algorithms. Agencies are therefore strongly encouraged to consider:

- Establishing a policy on how many times a subject can attempt to authenticate
- Establishing false rejection accuracy criteria against which tests and qualification procedures can be developed
- Referring to false rejection performance measures reported for algorithms passing the IREX test and calibration procedure.
- Consider requiring more stringent false match requirements

7.9.5 Conformance

The false match rate requirements **shall** be confirmed as follows. Iris recognition algorithms **shall** be submitted to NIST's Iris Exchange (IREX) test and calibration program. That program shall provide the algorithm developer with a tabulation of FMR vs. threshold calibration. Thereafter, the algorithm provider or integrator **shall** provide signed attestation that:

- All components of the iris recognition software (including iris detection, template generation and recognition algorithm) are identical to those submitted to the IREX test and calibration procedure.
- The authentication threshold has been set to the value produced by the IREX FMR vs. threshold calibration

The IREX test measurements are obtained by running iris recognition algorithms on commodity PC hardware. The use of iris recognition algorithms on other platforms, such as wall mounted embedded processors, is allowed. The algorithm provider **shall** submit the same software to the IREX test wherever it is ultimately installed.

NOTE The IREX program also produces measurements of false rejection performance.

8. Facial image specifications

8.1 Scope

[FIPS, Clause 4.4.1] requires collection of a facial image from PIV applicants, and indicates that it may be used for generation of the printed image [FIPS, Clause 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 facial images. This document neither requires nor precludes agencies from retaining facial images. However, if an agency elects to retain them, then they **shall** be stored in the format specified here. As with other biometric elements, agencies may elect to store face data on the PIV card and use it for automated verification. Although this clause places no normative requirements on such agency-optional activities, it does specify an image suited for automated biometric enrollment and face recognition.

The face specification is has a very similar format, and is functionally identical to, the ISO/IEC 19794-5:2005 face image adopted by the International Civil Aviation Organization for e-Passports. While [FIPS] does not allow automated face recognition for authentication, this specification is very well suited for such. However, note that two images are involved in one-to-one applications such as a physical access control authentication attempt:

- Enrollment image: The PIV image as specified here.
- Authentication image: Additional specification of the collection is typically necessary to address subject height variations and the illumination environment (see [BSI-FACE], for example).

8.2 Acquisition and format

This clause provides specifications for the retention of facial images. Facial images collected during PIV Registration **shall** be formatted such that they conform to INCITS 385-2004 [FACESTD]. In addition to establishing a format, [FACESTD] specifies how a face image should be acquired. This is done to improve image quality and, ultimately, performance. The images **shall** be embedded within the CBEFF structure defined in Clause 9. Because [FACESTD] is generic across applications it includes clauses that have either-or requirements. Table 17 is an application profile of [FACESTD] tailored for PIV. It gives concrete specifications for much of the generic content. Column 3 references the clauses of [FACESTD] and columns 4 and 5 give [FACESTD] requirements. For PIV, column 6 of Table 17 gives normative practice or value specifications. The table is not conformant with the Implementation Conformance Statement [ICS] standard. Particularly it extends the function of ICS but because it has the needed rows it may be useful in construction of a traditional ICS. Nevertheless the addition of a "values supported column" as specified in Clause 9.1 of [ICS] should be used by implementers for checking conformance to the specifications.

INCITS 385 is likely to be revised by the INCITS M1 committee. Such revisions are irrelevant to PIV; however implementations should respect the version number on Line 5 of Table 17.

Table 17 – INCITS 385 profile for PIV facial images

		Clause title and/or field name (Numbers in parentheses are [FACESTD] clause numbers)	INCITS 385-2004		PIV Conformance	Informative Remarks
			Field or content	Value Required	Values Allowed	
1.		Byte Ordering (5.2.1)	NC		A	Big Endian
2.		Numeric Values (5.2.2)	NC		A	Unsigned Integers
3.	CBEFF	CBEFF Header (5.3)	MF	MV	Patron format PIV	Multi-field CBEFF Header. Sec. o.
4.	Facial Header	Format Identifier (5.4.1)	MF	MV	0x46414300	i.e. ASCII "FAC\0"
5.		Version Number (5.4.2)	MF	MV	0x30313000	i.e. ASCII "010\0"
6.		Record Length (5.4.3)	MF	MV	MIT	See Note 1
7.		Number of Facial Images (5.4.4)	MF	MV	≥ 1	One or more images ($K \geq 1$). See Notes 2 and 3, and also line 20.
8.	Facial Info. Single instance of subject- specific info.	Facial image Block Length (5.5.1)	MF	MV	MIT	
9.		Number of Feature Points (5.5.2)	MF	MV	≥ 0	Positive, if features computed
10.		Gender (5.5.3)	MF	OV	OIT	These fields populated with meaningful values at agency discretion, otherwise 0 for unspecified.
11.		Eye color (5.5.4)	MF	OV	OIT	
12.		Hair color (5.5.5)	MF	OV	OIT	
13.		Feature Mask (5.5.6)	MF	OV	OIT	
14.		Expression (5.5.7)	MF	OV	1	Neutral

		Clause title and/or field name (Numbers in parentheses are [FACESTD] clause numbers)		INCITS 385-2004		PIV Conformance	Informative Remarks
				Field or content	Value Required	Values Allowed	
15.	Features	Pose Angles (5.5.8)		MF	OV	0	Unspecified = Frontal
16.		Pose Angle Uncertainty (5.5.9)		MF	OV	0	Attended operation so should be frontal.
17.		MPEG4 Features (5.6.1)		NC		OIT	
18.		Center of Facial Features (5.6.2)		NC		OIT	
19.		The Facial Feature Block Encoding (5.6.3)		OF	OV	OIT	
20.	Image Info. Each instance has image-specific info.	Facial Image Type (5.7.1)		MF	MV	1	See Note 4.
21.		Image Data Type (5.7.2)		MF	MV	0 or 1	See Note 5. Compression algorithm.
22.		Width (5.7.3)		MF	MV	MIT	See Note 7.
23.		Height (5.7.4)		MF	MV	MIT	
24.		Image Color Space (5.7.5)		MF	MV	1	sRGB. See Note 8.
25.		Source Type (5.7.6)		MF	MV	2 or 6	Digital still or digital video
26.		Device Type (vendor supplied device ID) (5.7.7)		MF	MV	MIT	
27.		Quality (5.7.8)		MF	MV	A	[FACESTD] requires 0 (unspecified)
28.	Image Data	Data Structure (5.8.1)		MF	MV	MIT	Compressed Data
29.	Basic (clause 6)	Inheritance	Inheritance (6.1)	NC		A	
30.			Image Data Encoding (6.2)	NC		A	See Note 5
31.			Image Data Compression (6.3)	NC		A	See Notes 5+6
32.		Format	Facial Header (6.4.1)	NC		A	Include 4 fields
33.			Facial Information (6.4.2)	NC		A	Include 9 fields
34.			Image Information (6.4.3)	NC		A	Include 8 fields
35.	Frontal (clause 7)	Inheritance	Inheritance (7.1)	NC		A	Inherits Basic
36.		Scene	Purpose (7.2.1)	NC		A	frontal Annex A
37.			Pose (7.2.2)	NC		Frontal	+/- 5 degrees
38.			Expression (7.2.3)	NC		Neutral	
39.			Assistance in positioning face (7.2.4)	NC		A	Only the subject appears
40.			Shoulders (7.2.5)	NC		A	Body + Face toward camera
41.			Backgrounds (7.2.6)	NC		Annex A.4.3	Uniform
42.			Subject and scene lighting (7.2.7)	NC		A	Uniform
43.			Shadows over the face (7.2.8)	NC		A	None
44.			Eye socket shadows (7.2.9)	NC		A	None
45.			Hot spots (7.2.10)	NC		A	Should be absent. Diffuse light.
46.			Eye glasses (7.2.11)	NC		A	Subject's normal condition
47.			Eye patches (7.2.12)	NC		A	Medical only
48.		Photographic	Exposure (7.3.2)	NC		A	No saturation
49.			Focus and Depth of Field (7.3.3)	NC		A	In focus
50.			Unnatural Color (7.3.4)	NC		A	White balance
51.			Color or grayscale enhancement (7.3.5)	NC		A + no recompress	No post-processing
52.			Radial Distortion of the camera lens (7.3.6)	NC		A + Follow Annex A.8	
53.		Digital	Geometry	aspect ratio (7.4.2.1)		A	1:1 pixels
54.				origin (7.4.2.2)		A	top left is 0,0
55.			Color Profile	Density (7.4.3.1)	NC	A	7 bits dynamic range in gray
56.				Color Sat (7.4.3.2)	NC	A	7 bits dynamic once in grayscale
57.				Color space (7.4.3.3)	NC	24 bit RGB	Option a, reported in color space field above. See Note 8
58.			Video Interlacing (7.4.4)	NC		A	Interlaced sensors are not permitted.
59.	Full Frontal (clause 8)	Inheritance	Inheritance (8.1)	NC		A	Inherits Frontal + Basic
60.		Scene	Scene (8.2)	NC		A	Inherits Frontal + Basic
61.		Photographic	Centered Image (8.3.2)	NC		A	Nose on vertical centerline
62.			Position of Eyes (8.3.3)	NC		A	Above horizontal centerline
63.			Width of Head (8.3.4)	NC		A	See Note 7
64.			Length of Head (8.3.5)	NC		A	See Note 7
65.		Digital	Resolution (8.4.1)	NC		CC ≥ 240	See Note 7
66.		Format	Inheritance (8.5.1)	NC		A	
67.			Image Information (8.5.2)	NC		A	

END OF TABLE

Acronym		Meaning
FAC	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 FAC
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 clauses do not define a field in the FAC.
A	as required	For PIV, value or practice is as specified in [FACESTD]
MIT	mandatory at time of instantiation	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 time of instantiation	For PIV, optional header value that may be determined at the time the record is instantiated

NORMATIVE NOTES:

1. If facial imagery is stored on the PIV Card, 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 [FACESTD] record. Key lengths and signing algorithms are specified in [800-78]. The size of the digital signature scales with the key length; it does not scale with the size of the biometric record.
2. 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.
3. When facial imagery is stored on the PIV Card, only one image **shall** be stored.
4. PIV facial images **shall** conform to the Full Frontal Image Type defined in Clause 8 of [FACESTD].
5. Facial image data **shall** be formatted in either of the compression formats enumerated in Clause 6.2 of [FACESTD]. Both whole-image and single-region-of-interest (ROI) compression are permitted. This document ([800-76]) recommends that newly collected facial image should be compressed using ISO/IEC 15444 (i.e. JPEG 2000). This applies when images will be input to automated face recognition products for authentication, and when images are stored on PIV Cards. In this latter case, ROI compression should be used. The older ISO/IEC 10918 standard (i.e. JPEG) should be used only for legacy images.
6. Facial images **shall** be compressed using a compression ratio no higher than 15:1. However, when facial images are stored on PIV Cards JPEG 2000 should be used with ROI compression. The innermost region should be centered on the face and compressed at no more than 24:1.
7. 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 Clause 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]). The size specification is a minimum: When images are to be used for automated face recognition higher resolution is likely to yield lower error rates.
8. Facial image data **shall** be converted to the sRGB color space if it is stored. As stated in Clause 7.4.3.3 of [FACESTD] this requires application of the color profile associated with the camera in use.

9. Common header for PIV biometric data

All PIV biometric data **shall** be embedded in a data structure conforming to Common Biometric Exchange Formats Framework [CBEFF]. This specifies that all biometric data **shall** be digitally signed and uniformly encapsulated. This 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 [EBTS] data of clause 3.7 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 18.

Table 18 – CBEFF concatenation structure

CBEFF_HEADER	CBEFF_BIOMETRIC_RECORD	CBEFF_SIGNATURE_BLOCK
Clause 9	Clauses 3.4, 3.6, 7.4, 7.5 and 8.2	FIPS 201
INCITS 398 5.2.1	INCITS 398 5.2.2	INCITS 398 5.2.3

The CBEFF Header specified in Table 19 and its notes will be established by NIST as Patron Format "PIV". This format will be established as a formal Patron Format per the provisions of [CBEFF, 6.2]. It adds definitive data types and the FASC-N field mandated by [FIPS] to a subset of the fields given in Patron Format A [CBEFF, Annex A]. It exists independently of Patron Format A. All fields of the format are mandatory.

Table 19 – Patron format PIV specification

	Patron Format PIV Field (Numbers in parentheses are [CBEFF] clauses)	Length Bytes	PIV Data Type	PIV Conformance Required Value
1.	Patron Header Version (5.2.1.4)	1	UINT	0x03
2.	SBH Security Options (5.2.1.1, 5.2.1.2)	1	Bitfield	See Note 2
3.	BDB Length	4	UINT	Length, in bytes, of the biometric data CBEFF_BIOMETRIC_RECORD
4.	SB Length	2	UINT	Length, in bytes, of the CBEFF_SIGNATURE_BLOCK. See Note 3
5.	BDB Format Owner (5.2.1.17)	2	UINT	Table 20, row "Biometric Format Owner" – which standards developer
6.	BDB Format Type (5.2.1.17)	2	UINT	Table 20, row "Biometric Format Type" – which standard
7.	Biometric Creation Date (5.2.1.10)	8		See Note 4 for data type
8.	Validity Period (5.2.1.11)	16		See Note 5 for data type
9.	Biometric Type (5.2.1.5)	3	UINT	Table 20, row "Biometric Type" – which modality
10.	Biometric Data Type (5.2.1.7)	1	Bitfield	Table 20, row "Biometric Data Type" – what degree of processing
11.	Biometric Data Quality (5.2.1.9)	1	SINT	[-2,100]. A value of -2 shall denote that assignment was not supported by the implementation; A value of -1 shall indicate that an attempt to compute a quality value failed. Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match.
12.	Creator (5.2.1.12)	18	Note 6	See Note 6 for data type
13.	FASC-N	25	Note 7	See Note 7 for data type
14.	Reserved for future use	4		0x00000000

Table 20 – CBEFF content for specific modalities

Quantity	Fingerprint Images	Fingerprint Templates	Iris Images	Facial Images	Other modalities
Clause	3.4	3.6	7	0	-
Biometric Format Owner	0x001B i.e. M1, the INCITS Technical Committee on Biometrics	0x001B i.e. M1, the INCITS Technical Committee on Biometrics	0x0101 i.e. ISO/IEC JTC 1/SC 37 Biometrics	0x001B i.e. M1, the INCITS Technical Committee on Biometrics	For other biometric data on PIV Cards, or retained by agencies, this field shall be assigned in accordance with [CBEFF, 5.2.1.17].
Biometric Format Type	0x0401	0x0201	0x0009	0x0501	
Biometric Type	0x0000 0008	0x0000 0008	0x0000 0002	0x0000 0010	0x0
Biometric Data Type	b001xxxxx i.e. raw	b100xxxxx i.e. processed	b010xxxxx i.e. Intermediate	b001xxxxx i.e. raw	[CBEFF, 5.2.1.7] has 3 categories for the degree biometric data has been processed.
Quality value	Quality value shall be $Q = 20 \cdot (6 - \text{NFIQ})$ where NFIQ is computed using the method of [NFIQ].		See NOTE 8	The [FACESTD] zero value shall be coded here as -2.	
	When multiple views or samples of a biometric are contained in the record the largest (i.e. best) value should be reported. For all biometric data, whether stored on a PIV Card or otherwise, the quality value shall be a signed integer between -2 and 100 per the text of INCITS 358.				

1188 NORMATIVE NOTES:

- 1189 1. Unsigned integers are denoted by UINT. Signed integers are denoted by SINT. Multi-byte integers **shall** be in
1190 Big Endian byte order.
- 1191 2. The security options field has two acceptable values. The value 00001101 indicates that the biometric data
1192 block is digitally signed but not encrypted; the value 00001111 indicates the biometric data block is digitally
1193 signed and encrypted. For the mandatory [MINUSTD] elements on the PIV Card the value **shall** be 00001101.
- 1194 The fourth bit (mask 0x08) is set per prior versions of this document. The third bit (mask 0x04), which in
1195 each case is set, implements the [CBEFF, 5.2.1.2] requirement that digital signature is differentiated from
1196 message authentication code. The second bit (mask 0x02) indicates the use of encryption. The first bit
1197 (mask 0x01) indicates the use of a digital signature. See [FIPS, 800-78] for specifications on digital signatures.
- 1198 3. The signature **shall** be computed over the concatenated CBEFF_HEADER and CBEFF_BIOMETRIC_RECORD in
1199 Table 18. The CBEFF_HEADER is given in Table 19. This includes the signature block length (on line 4) which
1200 may not be known before the signature is computed. This problem may be solved by conducting a two
1201 phase computation: First a dummy SB length value is inserted, the signature is computed, the signature
1202 length is written into the SB length field, and the signature recomputed.
- 1203 4. This is the date that the biometric sample was acquired. For processed samples (e.g. templates) this data
1204 should be the date of acquisition of the parent sample. Creation Date **shall** be encoded in eight bytes using a
1205 binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8
1206 bits as an unsigned integer. Thus 17:35:30 December 15, 2005 is represented as: 00010100 00000101 00001100
1207 00001111 00010001 00100011 00011110 01011010 where the last byte is the binary representation of the ASCII
1208 character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC).
1209 The field "hh" **shall** code a 24 hour clock value.
- 1210 When multiple samples (e.g. two single finger minutiae views) are included in one record (e.g. an INCITS 378
1211 record) and the Creation Dates are different, the Creation Date **shall** be the earliest of the multiple views.
- 1212 5. The Validity Period contains two dates each of which **shall** be coded according to Normative Note 4.
- 1213 6. For PIV the Creator field has length 18 bytes of which the first $K \leq 17$ bytes **shall** be printable ASCII characters,
1214 and the first of the remaining $18-K$ **shall** be a null terminator (zero).
- 1215 7. This field **shall** contain the 25 bytes of the FASC-N component of the CHUID identifier, per [800-73, 1.8.{3,4}].
- 1216 8. Iris quality shall be set to 50 pending standardization of a quality metric, via ISO/IEC 29794-6.

10. Conformance to this specification

10.1 Conformance

Conformance to this specification will be achieved if an implementation and its associated data records conform to the normative ("shall") clauses of clauses 3 through 6. The following text summarizes these statements.

10.2 Conformance to PIV registration fingerprint acquisition specifications

Conformance to Clause 3.2 requires the use of an [EFTS, Appendix 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. Images **shall** be conformant to this specification if:

- The acquisition procedures of 3.2 are followed. This may be tested by human observation.
- The images are conformant to [FINGSTD] as profiled by Table 4 and its normative notes.

10.3 Conformance of PIV Card fingerprint template records

Conformance to Clause 3.4 is achieved by conformance to all the normative content of the clause. This includes production of records conformant to [MINUSTD] as profiled in Clause 3.4. Conformance **shall** be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 6. Performance certification according to clause 4.5.3.1 is necessary.

10.4 Conformance of PIV registration fingerprints retained by agencies

Conformance to Clause 3.6 is achieved by conformance to all the normative content of the clause. This includes production of records conformant to [FINGSTD] as profiled in Clause 3.6. Conformance **shall** be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 4. Quality values [NFIQ] **shall** be checked against the NIST reference implementation.

10.5 Conformance of PIV background check records

Conformance to Clause 3.7 is achieved by conformance to all the normative content of the clause. This necessitates 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.

10.6 Conformance to PIV authentication fingerprint acquisition specifications

Conformance to Clause 6.2 **shall** be achieved if certification according to [SINGFING] is achieved, and if the resolution and area specifications are met. The [SINGFING] certification process entails inspection of output images.

10.7 Conformance of PIV facial image records

Conformance to Clause 7 **shall** be achieved by conformance to all the normative content of the clause. This includes production of records conformant to [FACESTD] as profiled in Clause 8.2. Conformance **shall** be tested by inspection of records and performing the test assertions of the "PIV Conformance" column of Table 17.

10.8 Conformance of CBEFF wrappers

A PIV implementation will be conformant to clause 9 if all biometric data records, whether or not mandated by this document or [FIPS], are encapsulated in conformant CBEFF records. CBEFF records **shall** be conformant if:

- the fields of the Table 19 header are present;
- the fields of Table 19 contain the allowed values as governed by its normative notes;
- a digital signature conformant to [800-78] is present;
- the values are consistent with the enclosed biometric data and the trailing digital signature.

An application that tests conformance of PIV biometric data **shall** be provided with appropriate keys to decrypt and check the digital signature.

11. References

Citation	Document
800-73	NIST Special Publication 800-73-3, Interfaces for Personal Identity Verification
800-78	NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification
ACGIH	Threshold Limit Values for Chemical Substances and Physical Agents & Biological Exposure Indices, 2007, ACGIH Worldwide www.acgih.org (American Conference of Governmental Industrial Hygienists). ANSI/IESNA RP-27.1-05 Recommended Practice for Photobiological Safety for Lamps and Lamp Systems, http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FIESNA+RP-27.1-05
APP/F	See EBTS entry below.
BAZIN	A. Bazin and T. Mansfield. An investigation of minutiae interoperability. In Proc. Fifth IEEE Workshop on Automated Identification Advanced Technologies, June 2007. AUTO-ID 2007, Alghero Italy.
BSI-FACE	Markus Nuppeney, Marco Breitenstein and Matthias Niesing, <i>EasyPASS - Evaluation of face recognition performance in an operational automated border control system</i> . BSI and Secunet, DE. http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Nuppeney_Marcus_IBPC2010_EasyPASS_Talk_Website.pdf This presentation is accompanied by a supporting paper. http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Nuppeney2_Marcus_IBPC2010_EasyPASS_Paper_final.pdf
CARD-CMD	ISO/IEC 7816-4:2005 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange http://webstore.iec.ch/preview/info_isoiec7816-4%7Bed2.0%7Den.pdf
CARD-BIO	ISO/IEC 7816-11:2004 Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods http://webstore.iec.ch/preview/info_isoiec7816-11%7Bed1.0%7Den.pdf
CARD-MIN	ISO/IEC FDIS 19794-2:2011 Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data. This standard is NOT INCITS 378 and not ISO/IEC 19794-2:2005.
CBEFF	INCITS 398-2005, American National Standard for Information Technology - Common Biometric Exchange Formats Framework (CBEFF) http://webstore.ansi.org
EBTS	AFIS-DOC-01078-9.1 CJIS-RS-0010 (V9.1) – Electronic Fingerprint Transmission Specification, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, May 25, 2010. Linked from here https://www.fbi/biospecs.org/docs/EBTS_v9-1_Final.pdf Implementers should consult https://www.fbi/biospecs.org/ or request the full EFTS documentation, including Appendix N, from the FBI.
FFSMT	ANSI/NIST-ITL 1-2007 – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, NIST Special Publication 500-245, 2000. http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
FINGSTD	INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format http://webstore.ansi.org
FIPS	FIPS 201-2, Personal Identity Verification, National Institute of Standards and Technology, 2011. FIPS 201-1 is currently the formal published standard. FIPS 201-2 was released as a draft March 8, 2011. http://csrc.nist.gov/publications/PubsFIPS.html
MANSFIELD	T. Mansfield et al. Research report on minutiae interoperability tests. Technical report, Minutiae Template Interoperability Testing, 2007. http://www.mtitproject.com/DeliverableD62.pdf
MINUSTD	INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange http://webstore.ansi.org
FACESTD	INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange http://webstore.ansi.org
ICS	Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) Proforma style

Citation	Document
	guide. EG 201 058 V1.2.3 (1998-04)
ICNIRP-LED	ICNIRP Statement on Light-Emitting Diodes, Implications for Hazard Assessment http://www.icnirp.de/documents/led.pdf
ICNIRP-BB	ICNIRP Statement on Light-Emitting Diodes, Guidelines on Limits of Exposure to Broadband Incoherent Optical Radiation, http://www.icnirp.de/documents/broadband.pdf
IRISSTD	ISO/IEC 19794-6:2011 Information technology -- Biometric data interchange formats -- Part 6: Iris image data This document revises and replaces the 2005 iris standard.
ISOSWAP	ISO/IEC 19795:2005 Information Technology — Biometric Performance Testing and Reporting — Part 4: Interoperability Performance Testing
MINEX	P. Grother et al., Minutiae Interoperability Exchange Test, Evaluation Report: NISTIR 7296 http://www.nist.gov/itl/iad/ig/ominex.cfm
MINEX II	P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, MINEX II Performance of Fingerprint Match-on-Card Algorithms Phase II / III / IV Report NIST Interagency Report 7477 (Revision I+II) http://www.nist.gov/itl/iad/ig/minexii.cfm
NFACS	IAFIS-DOC-07054-1.0, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, April 2004.
NFIQ	E. Tabassi and C. Wilson - NISTIR 7151 - Fingerprint Image Quality, NIST Interagency Report, August 2004 http://www.nist.gov/itl/iad/ig/bio_quality.cfm
NFIQ SUMMARY	E. Tabassi and P. Grother - NISTIR 7422 Quality Summarization - Recommendations on Biometric Quality Summarization across the Application Domain
SBMOC	D. Cooper, H. Dang, P. Lee, W. MacGregor, and K. Mehta. Secure Biometric Match-on-Card Feasibility Report. Technical report, National Institute of Standards and Technology, November 2007. Published as NIST Interagency Report 7452.
SINGFING	See "Personal Identity Verification (PIV): Image Quality Specifications For Single Finger Capture Devices". http://www.fbi.gov/hq/cjisd/iafis/piv/pivspeg.pdf
WSQ31	WSQ Gray-Scale Fingerprint Image Compression Specification, IAFIS-IC-0110(V3), October 4, 2010. https://www.fbibiospecs.org/docs/WSQ_Gray-scale_Specification_Version_3_1.pdf

1260

1261

A PIV ON-CARD COMPARISON INTERFACE

EDITOR'S NOTE 1 The interface description below may additionally need cryptographic specifications supporting confidentiality of transmitted finger minutia data.

EDITOR'S NOTE 2 The interface specification properly resides in (a future revision) of NIST Special Publication [800-73-3]. It is included here because of its logical proximity to the on-card data specifications. It is open for public comment.

A.1 Scope

All cards **shall** be accessed using the mechanisms of this clause. This includes selection of the application, reading and use of the Biometric Information Template (BIT), installation of a reference template, verification, recovery of comparison scores, and retrieval of identifiers.

A.1 Approach to the use of industry standards

This interface uses commands from ISO/IEC 7816-4 [CARD CMD]. Particularly it uses odd INS values, indicating that the command data fields contain TLV objects. The interface also uses ISO/IEC 7816-11 [CARD BIO] for generic biometric requirements, and the ISO/IEC 19794-2:2011 on-card comparison format [CARD MIN] for the particular minutia information. In addition, the interface only defines new elements when existing standards are silent on a necessary functionality.

A.2 Establish Communications

An Answer-to-Reset **shall** be obtained from the card to determine the transmission protocol (T=0, T=1 or T=CL).

A.2.1 Store enrolment template on the card

The template **shall** be placed on the card using the APDU of Table 21. It uses the PUT DATA instruction to overwrite the existing reference template.

Table 21 – Command APDU for storage of reference template

Command Parameter	Required Value	Meaning
CLA	0x00	
INS	0x24	PUT DATA
P1	0x01	New reference data is being added to the card
P2	0x00 0x01	Reference data qualifiers for primary and secondary fingers.
L _c field		Length of command data field
Data field		Data Object in BER-TLV format to be stored (tag '7F 2E')
L _e field	Absent	

Table 22 – Response APDU from storage of reference template

Response Parameter	Meaning
Data field	Empty
SW1-SW2	See ISO/IEC 7816-4:2005

If the biometric reference is too long for a single command APDU, then command chaining **shall** be used to send the biometric reference to the card in subsequent APDUs.

NOTE 1 Bit 5 of CLA set to 0 indicates that the command is the last or only command of a chain. Bit 5 of CLA set to 1 indicates that the command is not the last command of a chain.

NOTE 2 ISO/IEC 7816-4 does not standardize an APDU for enrolment. PUT DATA is required here, but note that some implementations use '24' CHANGE REFERENCE DATA.

NOTE 3 Operationally the process of putting the reference data on the card would ordinarily be accompanied by a writing the BIT to the card also. This would contain the biometric subtype information (for fingerprints, this is the finger position). Such data is not required here because no standard regulates the transmission of such data and because the test laboratory would usually only conduct comparisons of same-subtype templates (e.g. right index fingers).

NOTE 4 Operationally, putting reference data onto the card would generally be preceded by user authentication and establishment of a trusted channel to the card.”

A.3 Read of the BIT

The command of Table 23 **shall** be supported to allow retrieval of the BIT group template of Table 8 per the response of Table 24.

Table 23 – Command APDU for retrieval of biometric information template

Command Parameter	Required value	Meaning
CLS	0x00	
INS	0xCB	GET DATA
P1	0x3F	Retrieve from anywhere in the current Dedicated File (Application DF)
P2	0xFF	
L _c field	0x04	
Data field	0x5C 0x02 0x7F61	Data Object identifier to be retrieved (group of BIT)
L _e field		

Table 24 – Response APDU from retrieval of biometric information template

Response Parameter	Meaning
Data field	Biometric Information Template
SW1-SW2	See ISO/IEC 7816-4:2005

A.4 Verification

A.4.1 APDU specifications

The fingerprint verification data **shall** be sent to the card using the VERIFY command of Table 25. The status code **shall** be returned per Table 26. The required comparison score is returned in a separate GET DATA command, see clause 7.7.2.

Table 25 – Command APDU for comparison of biometric templates

Command Parameter	Meaning	
CLA	00	
INS	21	VERIFY
P1	00	
P2	00 , 01, 02 or 03	Reference data qualifier under tag 83 in the BITs of Table 8
L _c field		Length of command data field
Data field		The template
L _e field	Absent	

If the biometric reference is too long for a single command APDU, then command chaining **shall** be used to send the biometric reference to the card in subsequent APDUs.

NOTE 1 Bit 5 of CLA set to 0 indicates that the command is the last or only command of a chain. Bit 5 of CLA set to 1 indicates that the command is not the last command of a chain.

NOTE 2 In ISO/IEC 7816-4 the use of command '21' requires verification data to be present (e.g. minutia template). The alternative INS = 20 allows verification data to be absent. **Allow INS=20 for query of retry counter?**

NOTE 3 Operationally sending biometric authentication data to the card would often be preceded by establishment of a trusted channel.

Table 26 – Response APDU from comparison of biometric templates

Response Parameter	Meaning	
Data field	Empty	
SW1-SW2	9000 63CX 6300	Normal processing, or Verification failed, 'X' encodes the number of further allowed retries, or Verification failed, no further retries allowed - See ISO/IEC 7816-4:2005

A.4.2 Comparison scores

The on-card comparison algorithm **shall** internally support generation of a comparison score with precision of two-bytes or more. This supports the targeting of specific false match mates in clause 5.12. The card **shall** not provide any mechanism for retrieval of the comparison scores from the card.

A.4.3 Reading comparison subsystem identifier

Table 12 of ISO/IEC 7816-6:2004 provides a structure for application related data under constructed data element tag '6E'. This structure **shall** be readable using the APDU of Table 27 and Table 28. The value returned identifies the PIV Card's comparison algorithm. This algorithm shall be certified according to clause 5.11.3.2.

Table 27 – Command APDU for retrieval of Comparison subsystem identifier

Command Parameter	Meaning	
CLA	00	
INS	CB	GET DATA
P1	3F	Retrieve from anywhere in the current Dedicated File (Application DF)
P2	FF	
L _c field	03	length of command data field
Data field	5C 01 6E	Data Object identifier to be retrieved (Application related data)
L _e field	00	

The response field **shall** contain a discretionary field, tag '73', containing the comparison subsystem identifier in tag '99'.

Table 28 – Response APDU for retrieval of Comparison subsystem identifier

Response Parameter	Meaning	Minimal response value
Data field		Four byte ISO/IEC 19785-3 (CBEFF) algorithm identifier
SW1-SW2	See ISO/IEC 7816-4	

B IRIS CAMERA CAPTURE INTERFACE

All iris cameras **shall** implement the iris interface below. The cameras may implement the facial capture interface.

```
#region File Information
// IIrisCamera -- interface for iris cameras
//
#endregion

#region Design description
// This is a generic interface to iris image capture devices. The purpose for the
// interface is to enable ready integration of new iris cameras
//
// There are multiple means for obtaining images.
//
#endregion

#region Gotchas
// In client servers -- be careful about the line end character.
// Windows wants to see a newline (\n) in the netstream/filestream/streamreader
//
#endregion

using System;
using System.Collections.Generic;
using System.Text;
using PIViris.Library;

namespace PIViris.Library
{
    public interface IIrisCamera
    {
        // Unless otherwise noted all strings have printable characters, spaces and tabs only
        // All properties should return either a legal value or a sensible (e.g. blank string, NaN)
        // value if the value is not available (and set an error message). They should not crash
        // no matter the state of the object. If a property is set to a value that is not legal
        // for the object, the property should be set to the nearest legal value and an error message set.

        // Interfaces CANNOT define constructors, since C# allows multiple interfaces, but only one
        // inheritance.

        // class names should be of the form IrisCamera_Manufacturer_ModelName

        // In implementing an IrisCamera class there should be two constructors:
        //   IrisCamera_Manufacturer_ModelName() -- no parameters, will be default mode for camera
        //   IrisCamera_Manufacturer_ModelName(string mode) -- where mode defines the startup configuration
        // for the camera -- e.g. Enroll, Verify, Identify, Monitor, Default,
        // an unknown mode should go to the default for the camera and set an error message
        // mode Default should always be implemented. The internal storage of the modes should be uppercase.

        #region Properties -- always available -- these should be available even if the camera is not opened.
        bool cameraInitialized
        {
            get; // true if the camera is initialized and ready
        }
        string status
        {
            get; // implementation dependent status message, can be null
        }
        string lastErrorMessage
        {
            get; // most recent error messages, can be null, implementation dependent, clears error message
            // error messages should stack, separated by newlines.
        }
        string diagnostics
        {
            get; // most recent diagnostic message, can be null, implementation dependent, clears the message
            // diagnostics do not stack, subsequent diagnostics overwrite earlier ones.
        }
    }
}
```

```

1405     int lastSDKErrorCode
1406     {
1407         get;
1408     }
1409
1410     string implementationVersion
1411     {
1412         get; // the version of the implemenation, typically the CVS version of the implementation file
1413     }
1414     string cameraSDKVersion
1415     {
1416         get; // the version of the camera SDK on which the implementation is built
1417     }
1418     string cameraManufacturer
1419     {
1420         get; // may return null string
1421     }
1422     string cameraModel
1423     {
1424         get; // may return null string
1425     }
1426     string cameraSerialNumber
1427     {
1428         get; // may return null string
1429     }
1430     string cameraOperatingMode
1431     {
1432         get; // set by constructor only. implementation dependent, but must include Default
1433         // should likely use Enroll, Verify, Identify, Monitor, Diagnostic as appropriate
1434     }
1435
1436     string cameraAddress
1437     {
1438         get;
1439         set; // implementation specific string that identifies the camera to the SDK, e.g. an IP address
1440     }
1441     IrisLab.Library.Constants.Types.EyeDesignator cameraDefaultEyeSelection
1442     {
1443         get; // instructs camera on which eye to to try for
1444         set; // if the camera does not have this capability, set does nothing, get gets either
1445     }
1446
1447     bool canProvideIrisImages
1448     {
1449         get; // should be true for all iris devices with a rudimentary SDK
1450     }
1451     bool canProvideFaceImages
1452     {
1453         get; // true if the face functions are implemented
1454     }
1455     bool canAcquireAsynch
1456     {
1457         get; // true if the image acquisition functions can run asynchronously
1458         // false if the image acquisition functions are blocking
1459     }
1460     bool canProvideControlPanel
1461     {
1462         get; // true if an onscreen control panel is available
1463     }
1464
1465     int recommendedMinimumTimeOutMS
1466     {
1467         get; // recommended minimum timeout in MS
1468     }
1469
1470     int irisImageWidth
1471     {
1472         get; // width of the image returned, in pixels, same as irisParameters function
1473     }
1474     int irisImageHeight
1475     {
1476         get; // height of the image returned, in pixels, same as irisParameters function

```

```

1477     }
1478     int irisImageDepth
1479     {
1480         get; // depth of the image returned, in bits, same as irisParameters function
1481     }
1482     bool irisImageIsColor
1483     {
1484         get; // true if iris image is NOT grayscale
1485             // for all systems currently available this would be false
1486             // we have it here to allow for future
1487     }
1488
1489     int faceImageWidth
1490     {
1491         get; // width of the image returned, in pixels, same as irisParameters function
1492     }
1493     int faceImageHeight
1494     {
1495         get; // height of the image returned, in pixels, same as irisParameters function
1496     }
1497     int faceImageDepth
1498     {
1499         get; // depth of the image returned, in bits, same as irisParameters function
1500     }
1501     bool faceImageIsColor
1502     {
1503         get; // true if face image is color
1504             // typically true
1505             // we may need to add a property that describes the type of color
1506             // for now, RGB, 24 bit is assumed
1507     }
1508     System.Drawing.Imaging.ImageFormat faceImageFormat
1509     {
1510         get; // returns the format of the face image e.g bmp, iso, png, jpg
1511     }
1512
1513     bool irisParameters(out int width, out int height, out int depthInBits, out int
1514 recommendedMinimumTimeoutMS);
1515     // returns true on success
1516     // provides the width, height of the output iris images
1517     // provides the depth in bits of the pixels
1518     // provides the recommended minimum timeout
1519     // should work even if device is not yet opened
1520
1521     bool faceParameters(out int width, out int height, out int depthInBits, out int
1522 recommendedMinimumTimeoutMS);
1523     // returns true on success, returns false if face not implemented
1524     // provides the width, height of the output face images
1525     // provides the depth in bits of the pixels
1526     // provides the recommended minimum timeout
1527     // should work even if device is not yet opened
1528 #endregion
1529
1530 #region Properties - valid only when camera is open
1531 bool acquisitionComplete
1532 {
1533     get; // true if an asynch image acquisition has completed
1534         // false if the acquisition is not complete, not started or
1535         // asynch is not implemented
1536 }
1537 #endregion
1538
1539 #region Methods
1540
1541 bool open(); // initializes the device; returns true on success
1542 bool reset(); // soft re-open; clears state to initialization state; returns true on success
1543 bool close(); // closes device and releases resources; returns true on success
1544
1545 bool showControlPanel(); // shows control panel if available, returns true on success
1546
1547 // The prompt object should be an object that can resolve to the type of prompt
1548 // specified by the IrisCameraPromptType variable.

```

```

1549 //
1550 // Set routines return true on success, false on failure
1551 //
1552 // If the camera does not implement a particular type of prompt or a particular type of event
1553 // the set routines should do nothing silently and return false
1554 // the get routines should return false or a null object
1555 //
1556 // If a particular type/event is supported by the camera but the prompt is not subject to change by the
1557 // SDK, the set Prompt routine should do nothing quietly and the get Prompt routine should
1558 // return a appropriate object if possible and null otherwise.
1559 //
1560 // Similarly, if a particular type/event is supported by the camera but cannot be enabled/disabled
1561 // under program control the setEnable routine should do nothing quietly and the getEnable should
1562 // always return true.
1563 bool setPrompt(IrisCameraPromptEvent e, IrisCameraPromptType t, Object prompt);
1564 bool setEnablePrompt(IrisCameraPromptEvent e, IrisCameraPromptType t, bool promptEnable);
1565
1566 object getPrompt(IrisCameraPromptEvent e, IrisCameraPromptType t, Object prompt);
1567 bool getEnablePrompt(IrisCameraPromptEvent e, IrisCameraPromptType t);
1568
1569
1570 bool acquireIrisImagesHalt(); // kill an ongoing acquisition -- as if device has timed out
1571 // returns true on successful kill of an ongoing acquire
1572 // silent return of false on attempted kill when nothing ongoing
1573 // should clear buffers of any previously acquired images so that
1574 // the next acquire is sure to get a clean image
1575
1576 bool acquireFaceImagesHalt(); // kill an ongoing acquisition -- as if device has timed out
1577 // returns true on successful kill of an ongoing acquire
1578 // silent return of false on attempted kill when nothing ongoing
1579 // should clear buffers of any previously acquired images so that
1580 // the next acquire is sure to get a clean image
1581
1582 bool acquireIrisImages(out byte[] pixels,
1583     out int nImages,
1584     out double[] imageQuality,
1585     out IrisLab.Library.Constants_Types.EyeDesignator[] whichEye,
1586     int timeOutInMS);
1587 bool acquireIrisImages(out System.Drawing.Bitmap[] images,
1588     out int nImages,
1589     out double[] imageQuality,
1590     out IrisLab.Library.Constants_Types.EyeDesignator[] whichEye,
1591     int timeOutInMS);
1592
1593 bool acquireIrisImages(out byte[] pixels,
1594     out int nImages,
1595     out double[] imageQuality,
1596     out IrisLab.Library.Constants_Types.EyeDesignator[] whichEye,
1597     int timeOutInMS, bool blocking);
1598 bool acquireIrisImages(out System.Drawing.Bitmap[] images,
1599     out int nImages,
1600     out double[] imageQuality,
1601     out IrisLab.Library.Constants_Types.EyeDesignator[] whichEye,
1602     int timeOutInMS, bool blocking);
1603
1604 // Description - acquireIrisImages
1605 // initiates an acquisition sequence -- system must be opened/initialized before this call
1606 // pixels: nImages worth of pixels in order frame, row, column
1607 // images: nImages worth of bitmaps
1608 // irisImageFileNames: an array of filenames -- not full paths -- that have been saved
1609 // in a well known shared directory
1610 // nImages: the number of images acquired, zero if no images
1611 // imageQuality: a floating point image quality metric for each of nImages
1612 // whichEye: [L,R,U] for left, right, unknown for each image
1613 // blocking: if true or absent, call is blocking.
1614 // if false AND asynch acquisition is implemented the call will return
1615 // immediately. Use acquisitionComplete to test a non-blocking call
1616 // Use blocking version to get images
1617 //
1618 // returns true on success; returns false if an error occurs; if error occurs the
1619 // the error message and error code can be retrieved with errorMessage and errorCode
1620 // returns false with null arrays if not implemented

```



```

1621
1622
1623     bool acquireFaceImages(out System.Drawing.Bitmap[] images,
1624                             out int nImages,
1625                             int timeoutInMS);
1626 // bool acquireFaceImages(out string[] faceImageFileNames,
1627 //                          out int nImages,
1628 //                          int timeoutInMS);
1629 // bool acquireFaceImages(out byte[] pixels,
1630 //                          out int nImages,
1631 //                          int timeoutInMS);
1632
1633     bool acquireFaceImages(out System.Drawing.Bitmap[] images,
1634                             out int nImages,
1635                             int timeoutInMS, bool blocking);
1636 // Description acquireFaceImages
1637 // initiates an acquisition sequence -- system must be opened/initialized before this call
1638 // the face images may have been acquired on the previous acquireIrisImages call
1639 // faceImageFileNames: an array of filenames -- not full paths -- that have been saved
1640 //                          in a well known shared directory
1641 // pixels: nImages worth of pixels in order frame, row, column
1642 // images: nImages worth of bitmaps
1643 // nImages: number of images acquired. Zero if no image acquired
1644 // timeoutInMS: timeout for both blocking and non-blocking calls
1645 //                          blocking calls will return after the timeout
1646 //                          non-blocking calls will report completion and an error after timeout
1647 // blocking: if true or absent, call is blocking.
1648 //                          if false AND asynch acquisition is implemented the call will return
1649 //                          immediately. Use acquisitionComplete to test a non-blocking call
1650 //                          Use blocking version to get images
1651 //
1652 // returns true on success; returns false if an error occurs; if error occurs the
1653 // the error message can be retrieved with errorMessage
1654 // returns false with null arrays if not implemented
1655
1656     string ToString(); // returns a camera description suitable for use in a combo box
1657 #endregion
1658 }
1659
1660
1661

```

C IRIS RECOGNITION INTERFACE SPECIFICATION

All iris recognition implementations, including template generators and matchers, shall implement the interface of this Annex.

```
#region File Information
// ITemplateEngine -- interface for biometric template engines
//
#endregion

#region Design description
// This is a minimalist design that could, with little or no modification be used for face
// as well as iris.
//
// The principle methods are for generation/comparison and saving/loading of biometric templates
//
// The properties expose
//   version of the underlying SDK or library
//   error codes and messages
//   native width and height of input images
//   options for handling images that are not of native height and width
//   options for handling templates
//   diagnostics from template generation
//   flags that indicate the capabilities (can...) of the implementation
//
// This interface uses the BiometricsLibrary class to provide a minimalist image structure,
// BiometricsLibraryPixels, to hold images being processed.
#endregion

#region ToDo
// TODO: Add documentation on what to do with properties and methods that cannot be implemented
// TODO: Convert comments to ///
#endregion

using System;
using System.Collections.Generic;
using System.Text;

namespace PIViris.Library
{
    public interface ITemplateEngine
    {
        #region Properties
        // Readonly - returns information about the underlying SDK or library
        string SDKManufacturer
        {
            get;
        }
        string SDKModel
        {
            get;
        }
        string SDKVersion
        {
            get;
        }

        // Readonly - returns the version of the implemented class -- typically CVS version
        string implementationVersion
        {
            get;
        }

        // Error messages stack up in a string; this retrieves the stack and clears it; readonly
        string lastErrorMessage
        {
            get;
        }
    }
}
```

```

1730     }
1731     // Returns last error code produced by the underlying SDK, zero if no error
1732     int lastSDKErrorCode
1733     {
1734         get;
1735     }
1736
1737     // Readonly -- the size image that the engine expects as a default
1738     int imageWidthNative
1739     {
1740         get;
1741     }
1742     int imageHeightNative
1743     {
1744         get;
1745     }
1746
1747     // Readonly -- the dimensions of the template if it were represented as a bitmap
1748     // return -1 if the template does not have dimensions
1749     // return -1 if the template does not have a fixed size
1750     // The size, width and height include the mask if it exists
1751     int templateWidth
1752     {
1753         get;
1754     }
1755     int templateHeight
1756     {
1757         get;
1758     }
1759     int templateSizeBytes
1760     {
1761         get;
1762     }
1763     bool templateHasMask
1764     {
1765         get;
1766     }
1767
1768     // Readonly -- exposes the capabilities of the engine
1769     bool canComputeTemplate
1770     {
1771         get;
1772     }
1773     bool canCompareTemplates
1774     {
1775         get;
1776     }
1777     bool canProvideTemplateDiagnostics
1778     {
1779         get;
1780     }
1781     bool canProvideTemplateDiagnosticImage
1782     {
1783         get;
1784     }
1785
1786     // Read-write -- if given an ILLEGAL value for the engine, the value should be set to a legal default
1787     // silently -- just set the error message and code
1788     PIViris.Library.Constants.Types.imageConversionModeEnum imageConversionMode
1789     {
1790         set;
1791         get;
1792     }
1793     PIViris.Library.Constants.Types.matchScoreTypeEnum matchScoreType
1794     {
1795         set; // make sure to force to legal value for algorithm
1796         get;
1797     }
1798     int searchRange
1799     {
1800         set;
1801         get;

```

```

1802     }
1803
1804     // the quality and diagnostics are provided for the last generated template
1805     PIViris.Library.Constants.Types.templateDiagnosticsType templateDiagnostics
1806     {
1807         get;
1808     }
1809     System.Drawing.Bitmap templateDiagnosticImage
1810     {
1811         get;
1812     }
1813
1814     double templateQuality // of the last computed template
1815     {
1816         get;
1817     }
1818     double matchQuality    // of the last computed match
1819     {
1820         get;
1821     }
1822     double matchAngle      // of the last computed match
1823     {
1824         get;
1825     }
1826
1827     #endregion
1828
1829
1830     #region Methods -- Generate templates
1831     // Bitmap wrapper for the other generate template methods. The width and height
1832     // are contained in bitmap parameter.
1833     bool generateTemplate(ref System.Drawing.Bitmap inputImage, out byte[] template);
1834
1835     // Byte array methods
1836     // These routines take a one dimensional pixel array and generate a one dimensional template;
1837     // the routines which accept width and height will convert the image to the native image
1838     // dimensions using the image conversion mode. If width/height are not supplied, native
1839     // width and height are assumed.
1840     bool generateTemplate(ref byte[] isoStandardRecord, out byte[] template);
1841     bool generateTemplate(ref byte[] pixels, out byte[] template, int width, int height);
1842     bool generateTemplate(ref byte[] pixels, out byte[] template, int width, int height, int locationX, int
1843     locationY);
1844     bool generateTemplate(ref byte[] pixels, out byte[] template);
1845     #endregion
1846
1847
1848     #region Methods -- Comparison Routines
1849     // compare two templates and report match score, see matchScore type
1850     // if more than one template size/type is possible, the comparison should
1851     // handle combinations of templates as gracefully as possible.
1852     double compareTemplates(ref byte[] template1, ref byte[] template2);
1853     #endregion
1854
1855
1856     #region Methods -- Save/Load Templates
1857     // save/load a template and return true on success
1858     // for files, one template in/out to file
1859     // for binary reader, next template in the stream
1860     bool saveTemplate(string filename, ref byte[] template, bool enableOverwrite);
1861     bool loadTemplate(string filename, out byte[] template);
1862     bool loadTemplate(System.IO.BinaryReader bReader, out byte[] template);
1863     #endregion
1864
1865
1866     #region Methods -- Template Conversion Routines
1867     // Returns a bitmap
1868     System.Drawing.Bitmap templateToBitmap(byte[] byteTemplate);
1869     byte[] bitmapToTemplate(System.Drawing.Bitmap bitmapTemplate);
1870     #endregion
1871
1872
1873     #region Methods -- Other

```

```
1874         void errorClear(); // clears the error message and error number to no error condition
1875
1876         // IMPORTANT NOTE:
1877         // Implement the override to ToString for your implementation of ITemplateEngine as follows:
1878         //
1879         // public override string ToString()
1880         // {
1881         //     return m_implementationName;
1882         // }
1883
1884         // Regression test -- example of how to run and also tests functionality
1885         // Generate templates, save/load templates, compare templates
1886         bool regressionTest(string logfileName, string testDirectory); // returns true on successful completion
1887         bool regressionTest(string logfileName, string testDirectory, string imageFilename1, // to generate
1888 templates 1,2,3
1889         #endregion
1890     }
1891 }
1892
1893
```

D Performance testing and certification procedures

D.1 Scope

This clause gives normative specifications for tests used to certify implementations that generate and/or match the mandatory minutia-based biometric elements specified by [FIPS], i.e. the two fingerprint minutiae templates placed on the PIV Card. That is, this clause regulates the test itself, and the testing laboratory, not the products under test, and the data specifications here should not be confused with those given in Clause 3 for fielded PIV implementations.

D.2 PIV authentication

The fingerprint templates conform to [MINUSTD] as profiled in clause 3.4. The use cases given in [800-73, Appendix C] detail how the templates and the PIV Card are used for interoperable authentication. Authentication may involve one or both of the PIV Card templates. These will be compared with newly acquired (i.e. live) fingerprint images of either or both of the primary and secondary fingers. The inclusion of the finger position in the [MINUSTD] header allows the system to prompt the user for one or more specific fingers.

Authentication performance is quantified in terms of both the false reject rate (FRR) and the false accept rate (FAR). In PIV, FRR is 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 including: 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, and the familiarity of users with the process. The use of two fingers in all authentication transactions offers substantially improved performance over single-finger authentication. The intent of the [FIPS] specification of an interoperable biometric is to support cross-vendor and cross-agency authentication of PIV Cards. This plural aspect introduces a source of variation in performance.

D.3 Test overview

This clause specifies procedures for the certification of generators and matchers of [MINUSTD] templates.

Interoperability testing requires exchange of templates between products, which **shall** therefore be tested as a group. Accordingly, the testing laboratory **shall** conduct a first round of testing to establish a primary group of interoperable template generators and matchers. Certification **shall** be determined quantitatively at the conclusion of the test. Thereafter certification requires interoperability with previously certified products.

The certification procedure **shall** be conducted offline. This allows products to be certified using very large biometric data sets, in repeatable, deterministic and therefore auditable evaluations. Offline evaluation is needed to measure performance when template data is exchanged between all pairs of interoperable products. Large populations **shall** be used to quantify the effect of sample variance on performance. A template generator is logically a converter of images to templates. A template matcher logically compares one or two templates with one or two templates to produce a similarity score. Template generators and template matchers **shall** be certified separately. This aspect is instituted because:

1. Template generation is procedurally, algorithmically and physically distinct from matching.
2. Template generation is required by [FIPS], but matching is not.
3. Fingerprint template interoperability is dependent on the quality of the PIV Card templates. The full benefits of an interoperable template will not be realized if a supplier is required to produce both a high performing generator and a high performing matcher.
4. Once a template generator is certified and deployed, its templates will be in circulation. It is necessary for all matchers to be able to process these templates. Subsequent certification rounds will be complicated if generators and matchers are certified together.

Separate certification means that a supplier may submit one or more template generators and zero or more matchers for certification. Zero or more of the submitted products **shall** ultimately be certified.

This test design conforms to the provisions of the currently draft ISO/IEC 19795-4 [ISOSWAP] standard, as profiled by this document. One clause of that standard deals with blind testing. For PIV testing the template matcher **shall** not be able to discern the source of the enrollment templates.

D.3.1 Template generator

A template generator **shall** be certified as a software library. For PIV, a template generator is a library function that **shall** convert an image into a minutiae record. The input image represents a PIV enrollment plain impression. The output template represents a PIV Card template. A supplier's implementation, submitted for certification, **shall** satisfy the requirements of an application programming interface (API) specification to be published by the test organizer. The API specification will require the template generator to accept image data and produce [MINUSTD] templates conformant to Table 29. Where values or practices are not explicitly stated in Table 29, the specifications of clause 4.3 and Table 6 apply (e.g. on minutiae type). The CBEFF header and CBEFF signature **shall** not be included.

The testing laboratory **shall** input images to the generator. The template generator **shall** produce a conformant template regardless of the input. Such a template may contain zero minutiae. This provision transparently and correctly accounts for failures to enroll. In a deployed system, if quality assessment or image analysis algorithms made some determination that the input was unmatchable a failure to enroll might be declared. In an offline test such a determination **shall** result in at least a template containing zero minutiae. However, because in PIV other suppliers' matchers may be capable of handling even poor templates, it is recommended that a template generator submitted for testing should deprecate any internal quality acceptance mechanism, and attempt production of a viable template.

Table 29 – INCITS 378 specification for PIV Card template generator and matcher certification

#	Clause title and/or field name (Numbers in parentheses are [MINUSTD] clause numbers)	PIV Conformance Values Allowed	Informative Remarks
1.	Format Identifier (6.4.1)	0x464D5200	i.e. ASCII "FMR\0"
2.	Version Number (6.4.2)	0x20323000	i.e. ASCII " 20\0".
3.	Record Length (6.4.3)	$26 \leq L \leq 800$	26 byte header, max of 128 minutiae. See row 18.
4.	CBEFF Product Identifier Owner (6.4.4)	0	
5.	CBEFF Product Identifier Type (6.4.4)	0	
6.	Capture Equipment Compliance (6.4.5)	0	
7.	Capture Equipment ID (6.4.6)	0	
8.	Size of Scanned Image in x direction (6.4.7)	MIT	Inherited directly from input data
9.	Size of Scanned Image in y direction (6.4.8)	MIT	
10.	X (horizontal) resolution (6.4.9)	197	
11.	Y (vertical) resolution (6.4.10)	197	
12.	Number of Finger Views (6.4.11)	1	
13.	Reserved Byte (6.4.12)	0	
14.	Finger Position (6.5.1.1)	MIT	Inherited directly from input data
15.	View Number (6.5.1.2)	0	
16.	Impression Type (6.5.1.3)	0 or 2	Inherited directly from input data
17.	Finger Quality (6.5.1.4)	MIT	Inherited directly from input data
18.	Number of Minutiae (6.5.1.5)	$0 \leq M \leq 128$	M minutiae data records follow
19.	Minutiae Type (6.5.2.1)	01b, 10b, or 00b	See Note 1 below Table 6
20.	Minutiae Position (6.5.2.2)	MIT	See Note 7 below Table 6
21.	Minutiae Angle (6.5.2.3)	MIT	See Note 8 below Table 6
22.	Minutiae Quality (6.5.2.4)	MIT	This test specification previously required minutia quality values to be zero. This requirement no longer applies. It did not and does not apply to the PIV operational specification.
23.	Extended Data Block Length (6.6.1.1)	0	No bytes shall be included following this field.
END OF TABLE			

Acronym		Meaning
MIT	mandatory at time of instantiation	For PIV Certification, a mandatory value that shall be determined at the time the record is instantiated and shall follow the practice specified in [FINGSTD]

D.3.2 Template matcher

A template matcher **shall** be certified as a software library. For PIV, a matcher is a software function that compares enrollment templates with authentication templates to produce a similarity score. The similarity score **shall** be an integer or real value quantity. The enrollment templates represent the PIV Card templates. The authentication templates represent those extracted from live authentication fingerprints. A supplier's implementation, submitted for certification, **shall** satisfy the API specification published by the test organizer.

The API specification will support at a minimum the comparison of one authentication template (from an individual's primary or secondary fingers) with one enrollment template (from either the same or another individual's same finger). Both templates **shall** conform to the Table 12 profile of [MINUSTD].

The test **shall** neither prescribe nor prohibit methods whereby fingers' material **shall** be employed in the core comparison. The only constraint is that all invocations of the matching function **shall** yield a similarity score regardless of the input templates. Larger scores **shall** be construed as indicating higher likelihood that the input data originate from the same person. A failure or refusal to compare the inputs **shall** in all cases result in the reporting of a score. This document recommends implementers report a low score in this case.

The input [MINUSTD] enrollment templates **shall** be prepared by the test agent using software from a supplier. The input [MINUSTD] authentication templates **shall** be the output of the template generation software provided by the supplier of the matcher under test.

D.4 Test procedure

The testing laboratory **shall** publish a test specification document. This document **shall** establish deadlines for submission of products for certification.

The supplier of a template generator **shall** submit a request for certification to the testing laboratory. The testing laboratory **shall** provide a set of image samples to these suppliers. The supplier **shall** submit templates from this data to the testing laboratory. The supplier **shall** submit the template generator to the testing laboratory. The testing laboratory **shall** execute it and check that it produces identical templates to those submitted by the supplier. The testing laboratory **shall** apply a conformance assessor to the templates. The testing laboratory **shall** report to the supplier whether identical templates were produced and whether the templates are conformant to the specifications in Table 29. This validation process may be iterative.

The supplier of a template matcher **shall** submit a request for certification to the testing laboratory. The testing laboratory **shall** provide a set of samples to these suppliers. This set **shall** support debugging and **shall** consist of images representative of those collected in PIV registration. The supplier **shall** submit similarity scores from this data to the testing laboratory. The supplier **shall** submit the template matcher to the testing laboratory. The testing laboratory **shall** execute it and check that it produces identical scores to those submitted by the supplier. The testing laboratory **shall** report to the supplier the result of the check. This validation process may be iterative.

The testing laboratory **shall** apply all template generators to the first biometric sample from each member of the test corpus. The testing laboratory **shall** invoke all template matchers to compare the resulting enrollment templates with second authentication templates from each member of the corpus. The authentication template **shall** be generated by the matcher supplier's generator (i.e. not by another supplier's generator). This **shall** be done for all pair wise combinations of template generators and template matchers. The result is a set of genuine similarity scores for each combination.

The testing laboratory **shall** invoke all template matchers to compare enrollment templates with second authentication templates from members of a disjoint population. The authentication template **shall**, in all cases, be generated by the matcher supplier's generator. This **shall** be done for all pair wise combinations of template generators and template matchers. The result is a set of impostor similarity scores for each combination. The order in which genuine and impostor similarity scores are generated **shall** be randomized (i.e. it is not implied by the order of the last two paragraphs).

The testing laboratory **shall** sum the similarity score obtained from matching of the image of a primary finger with that obtained from matching of the image of a secondary finger. This sum-rule fusion represents two-finger authentication.

2007 **D.5 Determination of an interoperable group**

2008 The testing laboratory **shall** compute the detection error tradeoff characteristic (DET) for all pair wise combinations
2009 of the template generators and template matchers. The testing laboratory **shall** generate a rectangular
2010 interoperability matrix (see [ISOSWAP]). The matrix has rows corresponding to the generators and columns
2011 corresponding to the matchers. Each element of the interoperability matrix **shall** be the false reject rate at a fixed
2012 false accept rate. This value corresponds to one operating point on the DET. As described in clause D.3.1, the DET
2013 automatically includes the effect of failure to enroll and acquire.

2014 An interoperable group of template generators and matchers **shall** be established as the largest subgroup of products
2015 submitted in an initial certification round for which all elements of the interoperability sub-matrix (i.e. FRR values) are
2016 less than or equal to 1% at a fixed 1% FAR operating point. The condition that all pair wise product combinations should
2017 be below this threshold is instituted because the PIV application is intolerant of non-interoperable pairs.
2018