Biometric Data Specification for Personal Identity Verification

Charles Wilson
Patrick Grother
Ramaswamy Chandramouli

December 15, 2005
NOTE FOR REVIEWERS

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

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

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

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

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

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

The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201), was developed to establish standards for identity credentials. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It specifies technical acquisition and formatting requirements for the biometric credentials of the PIV system, including the PIV Card¹ itself. It enumerates required procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is high performance universal interoperability. For the preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint Transaction Specification.

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

1. **Introduction** ............................................................................................................ 8  
   1.1 Authority .......................................................................................................... 8  
   1.2 Purpose and Scope ......................................................................................... 8  
   1.3 Audience, Assumptions, and Overview ........................................................... 9  

2. **Terms, Acronyms, and Notation** ......................................................................... 10  
   2.1 Terms ............................................................................................................ 10  
   2.2 Acronyms ...................................................................................................... 10  

3. **Fingerprint Enrollment** ......................................................................................... 11  
   3.1 Fingerprint Image Acquisition ........................................................................ 11  
   3.2 Fingerprint Template Specifications .............................................................. 13  
      3.2.1 Source Images ................................................................................... 13  
      3.2.2 Minutia Record ................................................................................... 13  
   3.3 Fingerprint Image Format for Images Retained by Agencies ......................... 16  
   3.4 Fingerprint Image Specifications for Background Checks ............................. 18  

4. **Fingerprint Verification** ........................................................................................ 19  
   4.1 PIV Authentication Fingerprint Acquisition Specifications.............................. 19  
   4.2 PIV Authentication Matcher Specifications .................................................... 19  

5. **Facial Image Specifications** ..................................................................................... 20  
   5.1 Scope ............................................................................................................ 20  
   5.2 Acquisition and Format .................................................................................. 20  

6. **Common Header for PIV Biometric Data — CBEFF Structure** ......................... 24  

7. **Performance Testing Requirements and Certification Procedures** .................... 26  
   7.1 PIV Authentication ......................................................................................... 26  
   7.2 Test Procedures ............................................................................................ 26  
   7.3 Certification Procedures ................................................................................. 28  
      7.3.1 Phase 1: Initial certification .................................................................... 28  
      7.3.2 Phase 2: Recertification ....................................................................... 28  

8. **Conformance to This Standard** ............................................................................. 29  
   8.1 Conformance to PIV Registration Fingerprint Acquisition Specifications ...... 29  
   8.2 Conformance of PIV Card Fingerprint Template Records ............................. 29
8.3 Conformance of PIV Registration Fingerprints Retained by Agencies........29
8.4 Conformance of PIV Background Check Records........................................29
8.5 Conformance to PIV Authentication Fingerprint Acquisition Specifications ...29
8.6 Conformance of PIV Face Image Records....................................................29
8.7 Conformance of CBEFF Wrappers...............................................................30

9. Bibliography .........................................................................................................31

10. Glossary of Performance Testing and Certification Terms .........................32

List of Tables

Table 1: Fingerprint Acquisition Protocols .............................................................11
Table 2: Steps and Image Quality Assessment......................................................12
Table 3: PIV Minutiae Record................................................................................13
Table 4: INCITS 381 Finger Image Storage Requirements for PIV .......................16
Table 5: Record Types for Background Checks ....................................................18
Table 6: INCITS 385-2004 and PIV Requirements for Formatting of Facial Images ....20
Table 7: Simple CBEFF Structure ......................................................................24
Table 8: Patron Format PIV Specification............................................................24
Table 9: Example Fixed-threshold FAR and FRR values ....................................27
1. Introduction

1.1 Authority

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

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

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

1.2 Purpose and Scope

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

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

Thus, this document regulates various pieces of biometric data, and the processes used during and after their acquisition. This document neither requires nor precludes the use of the PIV Card templates in specific authentication paradigms such as match-on-card.
This document also provides an overview of the strategy that can be used for testing conformance to the standard. It is not meant to be a comprehensive set of test requirements that can be used for certification or demonstration of compliance to the specifications in this document.

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

+ Fingerprint Enrollment — Section 3;
+ Fingerprint Verification — Section 4;
+ Facial Image Specification — Section 5; and
+ CBEFF Structure — Section 6.
2. Terms, Acronyms, and Notation

2.1 Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segmentation</td>
<td>For fingerprints, segmentation is the separation of an N finger image into N single finger images.</td>
</tr>
</tbody>
</table>

2.2 Acronyms

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

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

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

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

3.1 Fingerprint Image Acquisition

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

<table>
<thead>
<tr>
<th>Table 1: Fingerprint Acquisition Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 1 - Plain live scan</td>
</tr>
<tr>
<td>Required Presentations</td>
</tr>
<tr>
<td>1 Combined plain impression of the four fingers on the right hand (no thumb)</td>
</tr>
<tr>
<td>2 Combined plain impression of the four fingers on the left hand (no thumb)</td>
</tr>
<tr>
<td>3 Combined impression of the two thumbs</td>
</tr>
<tr>
<td>Option 2 – Rolled live scan</td>
</tr>
<tr>
<td>Required Presentations</td>
</tr>
<tr>
<td>1 10 separately rolled fingers</td>
</tr>
<tr>
<td>2 Combined plain impression of the four fingers on the right hand (no thumb)</td>
</tr>
<tr>
<td>3 Combined plain impression of the four fingers on the left hand (no thumb)</td>
</tr>
<tr>
<td>4 Left thumb plain impression</td>
</tr>
<tr>
<td>5 Right thumb plain impression</td>
</tr>
<tr>
<td>Options 3 - Rolled ink on card</td>
</tr>
<tr>
<td>Required Presentations</td>
</tr>
<tr>
<td>1 10 separately rolled fingers</td>
</tr>
<tr>
<td>2 Combined plain impression of the four fingers on the right hand (no thumb)</td>
</tr>
<tr>
<td>3 Combined plain impression of the four fingers on the left hand (no thumb)</td>
</tr>
<tr>
<td>4 Left thumb plain impression</td>
</tr>
<tr>
<td>5 Right thumb plain impression</td>
</tr>
</tbody>
</table>
INFORMATIVE NOTES:

1. The combined multi-finger plain impression images are also referred to as slaps or flats, and are obtained by simultaneous placement of multiple fingers on the imaging surface without specific rolling movement.

2. Options 2 and 3 represent existing agency practice. Option 1 has recently become acceptable to the FBI.

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

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

Table 2: Steps and Image Quality Assessment

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

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

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

3.2.1 Source Images

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

3.2.2 Minutia Record

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

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

<table>
<thead>
<tr>
<th>Section title and/or field name</th>
<th>INCITS 378-2004</th>
<th>PIV Conformance</th>
<th>Informative Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle (5.1)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Minutia Type (5.2)</td>
<td></td>
<td>See Note 2</td>
<td>5.2 contains no normative content</td>
</tr>
<tr>
<td>Minutia Location : Coordinate System (5.3.1)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Minutia Location : Minutia Placement on a Ridge Ending (5.3.2)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Minutia Location : Minutia Placement on a Ridge Bifurcation (5.3.3)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Minutia Location : Minutia Placement on Other Minutia Types (5.3.4)</td>
<td>NC</td>
<td>See Note 2</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Section title and/or field name</td>
<td>INCITS 378-2004</td>
<td>PIV Conformance</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Field or Content</td>
<td>Value Req'd</td>
</tr>
<tr>
<td>7.</td>
<td>Minutia Direction : Angle Conventions (5.4.1)</td>
<td>NC</td>
<td>A</td>
</tr>
<tr>
<td>8.</td>
<td>Minutia Direction : Angle of a Ridge Ending (5.4.2)</td>
<td>NC</td>
<td>A</td>
</tr>
<tr>
<td>9.</td>
<td>Minutia Direction : Angle of a Ridge Bifurcation (5.4.3)</td>
<td>NC</td>
<td>A</td>
</tr>
<tr>
<td>10.</td>
<td>Byte Ordering (6.2)</td>
<td>NC</td>
<td>A</td>
</tr>
<tr>
<td>11.</td>
<td>Minutia Record Organization (6.3)</td>
<td>NC</td>
<td>A</td>
</tr>
<tr>
<td>12.</td>
<td>CBEFF Record Header (6.4)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>13.</td>
<td>Format Identifier (6.4.1)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>14.</td>
<td>Version Number (6.4.2)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>15.</td>
<td>Record Length (6.4.3)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>16.</td>
<td>CBEFF Product Identifier Owner (6.4.4)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>17.</td>
<td>CBEFF Product Identifier Type (6.4.4)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>18.</td>
<td>Capture Equipment Compliance (6.4.5)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>19.</td>
<td>Capture Equipment ID (6.4.6)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>20.</td>
<td>Size of Scanned Image in x direction (6.4.7)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>21.</td>
<td>Size of Scanned Image in y direction (6.4.8)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>22.</td>
<td>X (horizontal) resolution (6.4.9)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>23.</td>
<td>Y (vertical) resolution (6.4.10)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>24.</td>
<td>Number of Finger Views (6.4.11)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>25.</td>
<td>Reserved Byte (6.4.12)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>26.</td>
<td>Finger View Header (6.5.1)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>27.</td>
<td>Finger Position (6.5.1.1)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>28.</td>
<td>View Number (6.5.1.2)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>29.</td>
<td>Impression Type (6.5.1.3)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>30.</td>
<td>Finger Quality (6.5.1.4)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>31.</td>
<td>Number of Minutiae (6.5.1.5)</td>
<td>MF</td>
<td>MV</td>
</tr>
<tr>
<td>32.</td>
<td>Minutiae Type (6.5.2.1)</td>
<td>MF</td>
<td>MV</td>
</tr>
</tbody>
</table>
### Special Publication 800-76  
Biometric Specification for Personal Identity Verification

<table>
<thead>
<tr>
<th></th>
<th>Section title and/or field name</th>
<th>INCITS 378-2004 Field or Content</th>
<th>PIV Conformance Value Req'd</th>
<th>Informative Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>Minutiae Position (6.5.2.2)</td>
<td>MF</td>
<td>MV</td>
<td>MIT</td>
</tr>
<tr>
<td>34.</td>
<td>Minutiae Angle (6.5.2.3)</td>
<td>MF</td>
<td>MV</td>
<td>MIT</td>
</tr>
<tr>
<td>35.</td>
<td>Minutiae Quality (6.5.2.4)</td>
<td>MF</td>
<td>MV</td>
<td>MIT</td>
</tr>
<tr>
<td>36.</td>
<td>Extended Data Block Length (6.6.1.1)</td>
<td>MF</td>
<td>MV</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MF</td>
<td>mandatory field</td>
</tr>
<tr>
<td>MV</td>
<td>mandatory value</td>
</tr>
<tr>
<td>NC</td>
<td>normative content</td>
</tr>
<tr>
<td>A</td>
<td>as required</td>
</tr>
<tr>
<td>MIT</td>
<td>mandatory at instantiation-time</td>
</tr>
</tbody>
</table>

**NORMATIVE NOTES:**

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

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

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

<table>
<thead>
<tr>
<th>Section title and/or field name</th>
<th>INCITS 381-2004 Field or Content</th>
<th>PIV Conformance</th>
<th>Informative Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Byte and bit ordering (5.1)</td>
<td>NC</td>
<td>A</td>
<td>Big Endian MSB then LSB</td>
</tr>
<tr>
<td>2. Scan sequence (5.2)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>3. Image acquisition reqs. (6)</td>
<td>NC</td>
<td>Level 31</td>
<td>Table 1</td>
</tr>
<tr>
<td>4. Pixel Aspect Ratio (6.1)</td>
<td>NC</td>
<td>A</td>
<td>1:1</td>
</tr>
<tr>
<td>5. Pixel Depth (6.2)</td>
<td>NC</td>
<td>A</td>
<td>Level 31 → 8</td>
</tr>
<tr>
<td>6. Grayscale data (6.3)</td>
<td>NC</td>
<td>A</td>
<td>Level 31 → 1 byte per pixel</td>
</tr>
<tr>
<td>7. Dynamic Range (6.4)</td>
<td>NC</td>
<td>A</td>
<td>Level 31 → 200 gray levels</td>
</tr>
<tr>
<td>8. Scan resolution (6.5)</td>
<td>NC</td>
<td>A</td>
<td>Level 31 → 500 ppi</td>
</tr>
<tr>
<td>9. Image resolution (6.6)</td>
<td>NC</td>
<td>500 ppi - no interpolation</td>
<td></td>
</tr>
<tr>
<td>10. Fingerprint image location (6.7)</td>
<td>NC</td>
<td>A</td>
<td>Slap placement info, centering</td>
</tr>
<tr>
<td>11. CBEFF Header (7)</td>
<td>MF MV</td>
<td>Patron Format A see Section 6, Multi-field CBEFF Header</td>
<td></td>
</tr>
<tr>
<td>12. General Record Header (7.1)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>13. Format Identifier (7.1.1)</td>
<td>MF MV</td>
<td>A</td>
<td>0x46495200 (‘F’ ‘I’ ‘R’ 0x0)</td>
</tr>
<tr>
<td>14. Version Number (7.1.2)</td>
<td>MF MV</td>
<td>&quot;010\0&quot;</td>
<td>0x30313000 (‘0’ ‘1’ ‘0’ 0x0) Ver.1 Rev.0</td>
</tr>
<tr>
<td>15. Record Length (7.1.3)</td>
<td>MF MV</td>
<td>MIT</td>
<td>size excluding CBEFF structure</td>
</tr>
<tr>
<td>Section title and/or field name</td>
<td>INCITS 381-2004</td>
<td>PIV Conformance</td>
<td>Informative Remarks</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CBEFF Product Identifier (7.1.4)</td>
<td>MF MV A</td>
<td>CBEFF pid. See Note 10</td>
<td></td>
</tr>
<tr>
<td>Capture Device ID (7.1.5)</td>
<td>MF MV A</td>
<td>Vendor specified. See Note 10</td>
<td></td>
</tr>
<tr>
<td>Image Acquisition Level (7.1.6)</td>
<td>MF MV 31</td>
<td>Settings Level 31</td>
<td></td>
</tr>
<tr>
<td>Number of Images (7.1.7)</td>
<td>MF MV A</td>
<td>Denote by K, see lines 28-37. See notes 1, 2, and 3.</td>
<td></td>
</tr>
<tr>
<td>Scale units (7.1.8)</td>
<td>MF MV 0x01 0x02</td>
<td>inches or centimeters</td>
<td></td>
</tr>
<tr>
<td>Scan resolution (horz) (7.1.9)</td>
<td>MF MV 500 197</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan resolution (vert) (7.1.10)</td>
<td>MF MV 500 197</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image resolution (horz) (7.1.11)</td>
<td>MF MV 500 197</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image resolution (vert) (7.1.12)</td>
<td>MF MV 500 197</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pixel Depth (7.1.13)</td>
<td>MF MV 8</td>
<td>Grayscale with 256 levels</td>
<td></td>
</tr>
<tr>
<td>Image compression alg. (7.1.14)</td>
<td>MF MV 2</td>
<td>WSQ. See notes 4 and 9.</td>
<td></td>
</tr>
<tr>
<td>Reserved (7.1.15)</td>
<td>MF MV A</td>
<td>Two bytes.</td>
<td></td>
</tr>
<tr>
<td>Finger data block length (7.2.1)</td>
<td>MF MV MIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finger position (7.2.2)</td>
<td>MF MV MIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Count of views (7.2.3)</td>
<td>MF MV ≥ 1 M views of this finger. See note 5.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View number (7.2.4)</td>
<td>MF MV MIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finger image quality (7.2.5)</td>
<td>MF MV 20,40,60,80,100</td>
<td>Transformed NFIQ. See notes 5, 6 and 7</td>
<td></td>
</tr>
<tr>
<td>Impression type (7.2.6)</td>
<td>MF MV 0 or 2</td>
<td>See ANSI NIST ITL 1-2000</td>
<td></td>
</tr>
<tr>
<td>Horizontal line length (7.2.7)</td>
<td>MF MV ≥ 368</td>
<td>See note 8</td>
<td></td>
</tr>
<tr>
<td>Vertical line length (7.2.8)</td>
<td>MF MV ≥ 368</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finger image data (7.2.9)</td>
<td>MF MV MIT Compressed WSQ Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MF</td>
<td>mandatory field</td>
</tr>
<tr>
<td>MV</td>
<td>mandatory value</td>
</tr>
<tr>
<td>NC</td>
<td>normative content</td>
</tr>
<tr>
<td>A</td>
<td>as required by standard</td>
</tr>
<tr>
<td>MIT</td>
<td>mandatory at instantiation-time</td>
</tr>
</tbody>
</table>
NORMATIVE NOTES:

1. If certain fingers cannot be imaged, the value of this field shall be decremented accordingly.

2. The left and right four-finger images, and two-thumb, images may also be included. The value of this field shall be incremented accordingly.

3. For the PIV Card this value will be 2. For PIV enrollment sets, the number of images will ordinarily be thirteen (that is, the ten segmented images from the multi-finger plain impressions, and the three plain impressions themselves) or fourteen (if the plain thumb impressions were imaged separately).

4. Images shall be compressed using an implementation of the Wavelet Scalar Quantization (WSQ) algorithm that has been certified by the FBI.

5. The term view refers to the number of images of that particular finger. This value will exceed one if imaging has been repeated. Inclusion of all images of a finger can afford some benefit in a matching process. Retention of all images with quality values 1-4 is recommended. The first such image should have quality 1-3 per the following notes.

6. Quality values shall be present. These shall be calculated from the NIST Fingerprint Image Quality (NFIQ) method described in [NFIQ] using the formula \( Q = 20(6 - \text{NFIQ}) \). 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.

7. The quality value shall be set to 254 (the [FINGSTD] code for undefined) if this record is not a single finger print (i.e., it is a multi-finger image, or a palm print).

8. The values are minimum image sizes.

9. Compression shall only be applied after images required in Sections 3.4 and 3.2 have been prepared and transformed NFIQ values have been assigned.

10. The Capture Device ID should indicate the hardware version. The CBEFF PID should indicate the BSP's firmware or software.

3.4 Fingerprint Image Specifications for Background Checks

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Transaction Data Format in [FFSMT]</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Three Type 14 records.</td>
<td>Appendix N of [EFTS]</td>
</tr>
<tr>
<td>2 or 3</td>
<td>Fourteen Type 4 records</td>
<td>Section 3.1.1.4 &quot;Federal Applicant User Fee&quot; of [EFTS]</td>
</tr>
</tbody>
</table>
4. Fingerprint Verification

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

4.1 PIV Authentication Fingerprint Acquisition Specifications

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

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

4.2 PIV Authentication Matcher Specifications

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

5.1 Scope

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

5.2 Acquisition and Format

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

<table>
<thead>
<tr>
<th>Table 6: INCITS 385-2004 and PIV Requirements for Formatting of Facial Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>4.</td>
</tr>
<tr>
<td>5.</td>
</tr>
<tr>
<td>6.</td>
</tr>
<tr>
<td>7.</td>
</tr>
<tr>
<td>8.</td>
</tr>
<tr>
<td>9.</td>
</tr>
<tr>
<td>10.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>11.</td>
</tr>
<tr>
<td>12.</td>
</tr>
<tr>
<td>13.</td>
</tr>
<tr>
<td>14.</td>
</tr>
<tr>
<td>15.</td>
</tr>
<tr>
<td>16.</td>
</tr>
<tr>
<td>17.</td>
</tr>
<tr>
<td>18.</td>
</tr>
<tr>
<td>19.</td>
</tr>
<tr>
<td>20.</td>
</tr>
<tr>
<td>21.</td>
</tr>
<tr>
<td>22.</td>
</tr>
<tr>
<td>23.</td>
</tr>
<tr>
<td>24.</td>
</tr>
<tr>
<td>25.</td>
</tr>
<tr>
<td>26.</td>
</tr>
<tr>
<td>27.</td>
</tr>
<tr>
<td>28.</td>
</tr>
<tr>
<td>29.</td>
</tr>
<tr>
<td>30.</td>
</tr>
<tr>
<td>31.</td>
</tr>
<tr>
<td>32.</td>
</tr>
<tr>
<td>33.</td>
</tr>
<tr>
<td>34.</td>
</tr>
<tr>
<td>35.</td>
</tr>
<tr>
<td>36.</td>
</tr>
<tr>
<td>37.</td>
</tr>
<tr>
<td>38.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>39.</td>
</tr>
<tr>
<td>40.</td>
</tr>
<tr>
<td>41.</td>
</tr>
<tr>
<td>42.</td>
</tr>
<tr>
<td>43.</td>
</tr>
<tr>
<td>44.</td>
</tr>
<tr>
<td>45.</td>
</tr>
<tr>
<td>46.</td>
</tr>
<tr>
<td>47.</td>
</tr>
<tr>
<td>48.</td>
</tr>
<tr>
<td>49.</td>
</tr>
<tr>
<td>50.</td>
</tr>
<tr>
<td>51.</td>
</tr>
<tr>
<td>52.</td>
</tr>
<tr>
<td>53.</td>
</tr>
<tr>
<td>54.</td>
</tr>
<tr>
<td>55.</td>
</tr>
<tr>
<td>56.</td>
</tr>
<tr>
<td>57.</td>
</tr>
<tr>
<td>58.</td>
</tr>
<tr>
<td>59.</td>
</tr>
<tr>
<td>60.</td>
</tr>
<tr>
<td>61.</td>
</tr>
<tr>
<td>62.</td>
</tr>
<tr>
<td>63.</td>
</tr>
<tr>
<td>64.</td>
</tr>
<tr>
<td>65.</td>
</tr>
</tbody>
</table>
Special Publication 800-76  
Biometric Specification for Personal Identity Verification

<table>
<thead>
<tr>
<th>1.</th>
<th>Section title and/or field name</th>
<th>INCITS 385-2004</th>
<th>PIV Conformance</th>
<th>Informative Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Field or Content</td>
<td>Value Req'd</td>
<td>Values Allowed</td>
</tr>
<tr>
<td>66.</td>
<td>Length of Head (8.3.5)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>67.</td>
<td>Digital Resolution (8.4.1)</td>
<td>NC</td>
<td>CC ≥ 240</td>
<td></td>
</tr>
<tr>
<td>68.</td>
<td>Inheritance (8.5.1)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>69.</td>
<td>Image Information (8.5.2)</td>
<td>NC</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>

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

NORMATIVE NOTES:

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

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

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

<table>
<thead>
<tr>
<th>Table 7: Simple CBEFF Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBEFF STRUCTURE</td>
</tr>
<tr>
<td>CBEFF_HEADER</td>
</tr>
<tr>
<td>Section 6</td>
</tr>
<tr>
<td>INCITS 398 5.2.1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Table 8: Patron Format PIV Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>_</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>4.</td>
</tr>
<tr>
<td>5.</td>
</tr>
<tr>
<td>6.</td>
</tr>
<tr>
<td>7.</td>
</tr>
<tr>
<td>8.</td>
</tr>
<tr>
<td>9.</td>
</tr>
<tr>
<td>10.</td>
</tr>
<tr>
<td>11.</td>
</tr>
</tbody>
</table>
12. Creator (5.2.1.12) 22 Note 6 See Normative Note 7 for data type and requirements
13. FASC-N 29 Note 7 See Normative Note 8 for data type and requirements
14. Reserved for future use 7 0x0000000000

NORMATIVE NOTES:

1. Unsigned integers are denoted by UINT. Signed integers are denoted by SINT. Multi-byte quantities shall be in Big Endian order.

2. For fingerprint image data defined in this standard the Format Type shall be 0x0401. For fingerprint minutiae template data defined in this standard, this value shall be 0x0201. For face data defined in this standard this value shall be 0x0501. For other biometric records on the PIV Card or otherwise retained by agencies this field shall be assigned in accordance with the procedures of [CBEFF, clause 5.2.1.17].

3. For single fingerprint images, the quality value shall be \( Q = 20(6 - \text{NFIQ}) \) where NFIQ is computed using the method of [NFIQ]. The value here is a duplicate of the value in the BDB itself; it may be useful is selecting which of the two fingerprint records should be verified first. For other biometric records on the PIV Card or otherwise retained by agencies this field shall be a signed integer between -1 and 100. A value of 0 shall denote that the value was not assigned. A value of -1 shall indicate that an attempt to compute a quality value failed. When multiple biometric samples are stored in the BDB the quality value reported here shall be the largest of the individual qualities.

4. This is the date that the biometric sample was acquired. For processed samples (e.g. templates) this data should be the date of acquisition of the parent sample. Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer. Thus 17:35:30 December 15, 2005 is represented as: 00010100 00000101 00001100 00001111 00010001 00100011 00011110 1011010 where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value.

5. The Validity Period contains two dates each of which shall be coded according to Normative Note 5.

6. [CBEFF] defines the Creator field to have variable length. For PIV the length of the field, N, shall be 22 bytes. This value (i.e. 22) shall be present in the first four bytes and coded as a Big Endian unsigned integer. The remaining text portion shall consist of \( K \leq 17 \) ASCII characters, and 18-K null terminators (zeroes).

7. This field shall contain the four byte unsigned integer value 29, followed by the 25 bytes of the FASC-N component of the CHUID identifier, per clauses 1.8.{3,4} of [800-73].

INFORMATIVE NOTES:

1. The value 0x3A79 is the sum of the elements in column 5.

2. 0x25 is the bit pattern 00100101 meaning: the standard biometric header (SBH) length is stored in two bytes, the biometric data block (BDB) length is stored in four bytes; the signature block (SB) length is stored in two bytes; the data is signed but not encrypted; and integrity protection is present.

3. PIV’s CBEFF Patron Format is based on INCITS 398's Patron Format A.

4. Column 4, PIV Requirement, is mandatory by definition.

5. The values for the Format Owner and Format Type Code fields are given in the respective data format standards [FACESTD] and [FINGSTD].
7. Performance Testing Requirements and Certification Procedures

7.1 PIV Authentication

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

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

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

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

7.2 Test Procedures

This section specifies procedures that a test laboratory shall follow in measuring interoperable matching performance. Certification shall be based on the results of tests conforming to the procedures of this section. Template generators and template matchers of [MINUSTD] templates shall be tested in offline tests conforming to the provisions of the [ISOSWAP] standard, as profiled by this document. The Minutiae Exchange evaluation [MINEX] conducted by NIST is one instance of an implementation of this standard. Offline testing is a necessary and efficient precursor to smaller or more expensive scenario or operational tests (see [ISOTEST] that agencies may elect to conduct. A test of sufficiency as allowed by [ISOSWAP] is not required for conformance to this document.
A template generator shall be a software library that provides a facility to accept one fingerprint image and produce one template. The image represents a PIV enrollment plain impression. The template represents the PIV Card template. Failures or refusals to process the input image shall nevertheless result in a matchable template.

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Template Generator (producer of PIV Card templates)</th>
<th>Interoperability Performance (FAR, FRR)</th>
<th>Template Matcher (PIV authentication implementation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>0.005 0.008</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>0.004 0.009</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>0.006 0.011</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>0.005 0.007</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>0.005 0.005</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>0.005 0.002</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>0.005 0.008</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>0.005 0.008</td>
</tr>
</tbody>
</table>

Table 9: Example Fixed-threshold FAR and FRR values
7.3 Certification Procedures

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

7.3.1 Phase 1: Initial certification

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

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

1. Intra-agency Performance: This specification is included to be representative of the scenario in which, an agency, sourcing its template generators and matchers from the same vendor, authenticates its own cardholders. A supplier's implementation shall be certified if it may be configured to achieve a measured false reject rate less than or equal to \( X \) and a false accept rate simultaneously less than or equal \( Y \). Both \( X \) and \( Y \) shall be established before testing begins. These elements correspond to the diagonal values of Table 9. This standard recommends that the false reject rate criterion, \( Y \), and the false accept rate, \( X \), shall not exceed 0.5%. Either the primary finger, or both the primary and secondary fingers, may be used in attaining this level of performance.

2. Inter-agency Performance: This specification is included to be representative of the scenario in which visitors to a facility present PIV Cards containing templates that were generated by a supplier different from that used for authentication. A supplier's implementation shall be certified if it may be configured to achieve a measured false reject rate less than or equal to \( X \) and a false accept rate simultaneously less than or equal \( Y \). Certification requires that all cross-vendor values (the off-diagonal values of Table 9) satisfy the criteria. This requires the test organization to generate the interoperability matrix for all combinations of \( N \leq K \) vendors and test for conformity to the criteria. This search shall identify and certify the largest subgroup of \( N \) vendors that jointly conform. This standard recommends that the false reject rate criterion, \( Y \), shall be 1% and the false accept rate criterion, \( X \), be 0.5%. Either the primary finger, or both the primary and secondary fingers, may be used in attaining this level of performance.

7.3.2 Phase 2: Recertification

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

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

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

8.1 Conformance to PIV Registration Fingerprint Acquisition Specifications

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

8.2 Conformance of PIV Card Fingerprint Template Records

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

8.3 Conformance of PIV Registration Fingerprints Retained by Agencies

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

8.4 Conformance of PIV Background Check Records

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

8.5 Conformance to PIV Authentication Fingerprint Acquisition Specifications

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

8.6 Conformance of PIV Face Image Records

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

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

<table>
<thead>
<tr>
<th>Citation Code</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-73</td>
<td>NIST Special Publication 800-73, Interfaces for Personal Identity Verification</td>
</tr>
<tr>
<td>FIPS</td>
<td>FIPS 201, Personal Identity Verification, National Institute of Standards and Technology, 2005.</td>
</tr>
<tr>
<td>FINGSTD</td>
<td>INCITS 381-2004, American National Standard for Information Technology - Finger Image-Based Data Interchange Format</td>
</tr>
<tr>
<td>MINUSTD</td>
<td>INCITS 378-2004, American National Standard for Information Technology - Finger Minutiae Format for Data Interchange</td>
</tr>
<tr>
<td>FACESTD</td>
<td>INCITS 385-2004, American National Standard for Information Technology - Face Recognition Format for Data Interchange</td>
</tr>
</tbody>
</table>

The material at [http://www.fbi.gov/hq/cjis/iafis/efts71/cover.htm](http://www.fbi.gov/hq/cjis/iafis/efts71/cover.htm) may not be fully up to date. Implementers should request the full EFTS documentation, including Appendix N, from the FBI. |
| NFACS         | IAFIS-DOC-07054-1.0, Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, April 2004. |
| NFIQ          | NISTIR 7151 - Fingerprint Image Quality, NIST Internal Report, August 2004 |
| ICS           | Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) Proforma style guide. EG 201 058 V1.2.3 (1998-04) |
# 10. Glossary of Performance Testing and Certification Terms

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