NIST Special Publication 500-280v2.1 500-280 Version 2(2015)

Mobile ID Device Best Practice Recommendation Version 2.1

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.500-280v2.1

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

NIST Special Publication 500-280v2.1

Mobile ID Device Best Practice Recommendation Version 2.1

Kevin Mangold
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.500-280v2.1

September 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Special Publication 500-280v2.1
Natl. Inst. Stand. Technol. Tech. SP 580-280v2.1, 60 pages (September 2016)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.580-280v2.1

TABLE OF CONTENTS

Table of Contents

1 Introduction

Version 1 of the *Mobile ID Best Practice Recommendation* (BPR) was released in 2009. It has been referenced in many Government procurement acquisitions and has provided information helpful to companies developing mobile ID solutions. This version of the BPR builds upon that solid foundation, with the intent of reflecting changes in technology, the operating environment and standards since 2009.

The original BPR played a direct role in the 2011 update of the *ANSI/NIST-ITL standard*. The modality-specific acquisition profiles for fingerprint and iris of the BPR were directly incorporated into the standard.

Although closely tied to the *ANSI/NIST-ITL standard* in content, this is a separate document and may be used independently of the standard.

Although Best Practice Recommendations typically only use 'should' (as a recommendation), 'shall' appears several times in this document. 'Shall' appears in places where the *ANSI/NIST-ITL standard's* transmission format is discussed. It is necessary to follow the requirements of that standard in order to be conformant to it.

This revision modifies the acquisition profiles and adds some new ones, which are also reflected in the 2015 Update to the *ANSI/NIST-ITL standard*[1].

The original BPR included only face, fingerprint and iris as modalities. Friction ridge coverage in the BPR is now extended to include plantars (toe and sole) and imaging of latent prints. Investigatory and forensic voice data is now a record type in the *ANSI/NIST-ITL standard*, so voice is also included as a modality in this version of the BPR. There are also new sections specifically devoted to scars / marks and tattoos; forensic dental photography using mobile devices; and photography of other body parts. In addition, there are special discussions about the use of mobile ID devices to obtain samples from deceased individuals.

2 Scope

A Mobile ID Device, for purposes of this document, is defined as a portable biometric acquisition station used by governmental organizations to capture high quality biometric samples of one or more modalities from a subject – done in near-real-time at any (even remote) location. It is expected to operate in relatively unconstrained conditions. It is not intended to be stationary and hardwired to a much larger system. With the advent of hand-held technology such as smart phones capable of high resolution photography,

[1] It is available at http://www.nist.gov/itl/iad/ig/ansi_standard.cfm.

voice capture, fingerprint capture, and possibly even iris image capture -- the definition of mobile ID devices is appropriately extended to include those types of devices.

The functions performed or supported by the Mobile ID Device are:

- Enrollment
- Identification
- Verification

These devices are used across a wide range of Government organizations, including:

- Law enforcement
- Criminal justice
- Military
- Homeland security
- Benefits and services

Some of the many uses cases for mobile identification technology include:

- First responder identity verification at a disaster scene
- Police checking of biometric databases (fingerprint and / or facial) using a biometric sample from a subject during a traffic stop
- Forensic image capture – including latent friction ridge prints
- Identification of unknown deceased

The quantitative requirements and specifications of required biometric characteristics typically vary by use case, and can be substantially different for each of the areas shown above.

This document focuses upon generalized characteristics that can be quantified for groupings of use cases. Specific use cases will require further refinement of specifications on the part of the procurement and operations teams.

Readers should also be aware of the Technical Report 30125 *"Information Technology – Biometrics – Biometrics used with mobile devices"* issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)[2]. TR 30125 is not quoted in this BPR due to copyright restrictions.

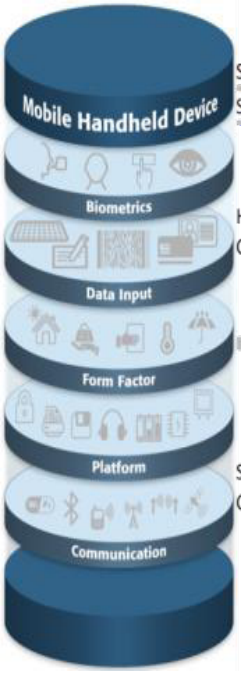
[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53245

3 Taxonomy and Definitions

The mobile ID device is comprised of several components that may or may not be separate physical elements. This is outlined in the taxonomy shown in Figure 1.

Figure 1

Mobile Handheld Device Taxonomy[3]



System	Biometric				
Subsystem	***Form Factor***	***Biometrics***	***Data Input***	***Platform***	***Communication***
Hardware Components	Chassis	Imager (size/characteristics)	Keyboard	Processor & Memory	Wired Connectivity
	Ingress Protections	Processor/Controller	Programmable Buttons	Power	Wireless Connectivity
	Battery Casings	Imager Housing	Pointing Devices	Output	
	Access Panels	Illuminator	Touchscreen	Display Device	
			Microphone	Storage	
			Readers	Interfaces	
			Other	Feedback	
Software Components	N/A	Data Acquisition	Acquisition	Operating System	Network Management
		Signal Processing	Encoding/Decoding	Applications	Protocols
		Matching	Metadata Management	Formatting/Template	
		Data Management		Security	
		Template Generator*		Template Generator*	
		Interface Control		Protocol Management	
		Biometric Status Monitoring			
		Dynamic Workflow Manager			
		Spoofing/Evasion			

**** Exists in multiple subsystems***

The following terms are defined for use in this document:

Acquisition Profile

A set of characteristics for the mobile ID device and its use that is defined by 'level.' This allows a device manufacturer and a procurement officer to state what combination of features is defined in a particular device. In this document, the following are described:

- Face (called 'Subject Acquisition Profile' – SAP)
- Fingerprint (called 'Fingerprint Acquisition Profile' – FAP)

[3] From an internal report of the Department of Homeland Security (DHS), Office of Science and Technology, 2010 -- provided by DHS for use in this document. Some commentators have suggested updates to this figure for purposes of this BPR, including adding 'microphone' to biometrics (since voice is included in this document). "Data management' may be appropriate in the Platform column – which could be renamed 'Data Storage / Management'. The International Organization for Standardization (ISO) defines template generation (feature extraction) as a part of signal processing. To be consistent with ISO, 'template generation' would only appear in the Biometrics column.

- Palm print (called 'Palm print Acquisition Profile' - PAP)
- Iris (called 'Iris Acquisition Profile' – IAP)
- Toe and foot print (called 'Toe and foot print Acquisition Profile – TAP)

Note that there is no corresponding Acquisition Profile for Voice. The equivalent is the combination of Field 11.003 (Audio object descriptor code / AOD) and Field 11.008 (Acquisition source / AQS) in the *ANSI/NIST-ITL standard*[4].

Environmental Profile

The set of specifications related to a particular type of environmental conditions in which the mobile ID device will be used. These profiles (described in Section **16** Environmental Profiles) are:

- Indoor
- Outdoor – Heavy Use (Law enforcement-like)
- Outdoor – Rugged Use (Military-like)

Organization's Application Profile

Technical specifications developed by specific organizations to control data content and format for submissions, based upon the *ANSI/NIST-ITL standard*. Some examples are[5]:

- EBTS[6] for Department of Defense (DoD)
- EBTS for the Federal Bureau of Investigations (FBI)
- IXM[7] for Department of Homeland Security (DHS)
- INT-I for INTERPOL

Risk Profile

The levels established to categorize the public risk associated with the biometric modality profiles (See Section 13 Risk Profiles). The risk factors are defined as:

- Severe
- Moderate
- Mild

[4] In this document, 'Field' refers to a Field in the *ANSI/NIST-ITL standard*.
[5] The latest versions of these profiles (and of biometric standards recognized by the US Government for particular use cases) are shown in the "*Registry of USG Recommended Biometric Standards"* which is available at http://www.biometrics.gov/Standards/Default.aspx
[6] EBTS means Electronic Biometric Transmission Specification
[7] IXM stands for Automated Biometric Identification System (IDENT) Exchange Messages

Scenario

A detailed description of the use of the Mobile ID device from a particular end-user point of view.

Use Case

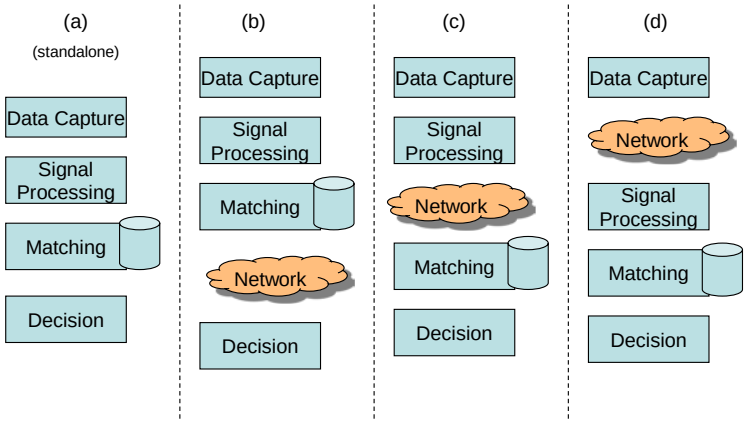
A categorization that groups together concepts-of-operation sharing similar characteristics. In this document, there are four defined use cases (See Section 12 Mobile ID Use Cases).

4 System Design Considerations

There are several tasks that may be accomplished by a biometric mobile identification system. The primary ones include signal or image capture, signal or image processing, matching, and ultimately, an output decision that indicates an action to be taken by the operator. This action is based on an application-specific decision process. Figure 2 illustrates typical combinations of these tasks across four basic configurations that can be used to divide the workload up between the Mobile ID device and a networked system. The functions shown below the 'network' are not included in the mobile device in that particular configuration.

Figure 2

Tasks Across Four Basic Configurations



The primary tasks of signal or image capture; signal or image processing; matching; and output decision generation can be performed by the Mobile ID device alone or by splitting the workload with a networked system. Factors influencing the operation of these functions include location, availability of network connectivity, bandwidth of the network connection, processing power, storage capacity of the mobile device, response time requirements, auditing / data retention and privacy requirements and interoperability with the other systems. (The cloud in Figure 2 represents a network connection.)

- Column (a) illustrates a standalone approach where the Mobile ID device performs all four functions.

- Columns (b) – (d) illustrate varying degrees of task allocation across a networked system.

The objectives to be accomplished for each of the tasks are:

- Data Capture – The process of acquiring one or more raw biometric samples from a subject

- Signal Processing – The process of extracting distinguishing features from a raw biometric sample, which may include some or all of the following:

    - Signal or image normalization
    - Segmentation
    - Feature extraction
    - Quality assessment
    - Template creation[8]

- Matching – The process of comparing the features extracted from a submitted biometric sample to those of one or more reference templates in a database and generating a resulting similarity score for each template comparison.

- Decision – The process of making a match/non-match conclusion based on the similarity score(s) meeting or exceeding a specified threshold, the application of a more complex decision processing such as multi-biometric fusion, or the creation of a candidate list.

The Decision task should be further interpreted in an application dependent manner. Resulting actions may include one or both of the following decision processes:

- Application Level Decision - The result of the search may automatically:

[8] For purposes of this document, 'template' as a term is inclusive of voice models.

- Generate one or more predetermined messages to the operator of the device
- Trigger an alert (to one or more other systems or operators)
- Initiate a search or retrieve additional data from one or more other systems (e.g., intelligence systems, facial image databases, etc.)
- Be passed to a human operator for manual verification
- Be returned as 'raw' image data to the operator of the Mobile ID device

Note: An application level decision may take place on either or both sides of any network.

- Operator Decision - Depending on the specific application and the result of the search, the operator of the Mobile ID device may or may not be free to make his or her own decision on how to proceed in a particular case.
  - In some scenarios, specific instructions may be returned, e.g., 'arrest this person', 'do not detain this person', 'this is the same person as their supplied credential indicates', or 'this is not the same person as the supplied credential indicates'
  - In other scenarios, the search result may be returned to assist the operator in deciding what action to take, possibly in conjunction with demographic, other metadata, or one or more facial images of the potential 'matches'

Other tasks to be performed, but not illustrated, include the addition of contextual data, the formatting of the data (to the *ANSI/NIST-ITL standard* and an organization's application profiles such as FBI EBTS, DoD EBTS; or to other standard format such as an ISO data transmission standard), and the handling of transactions and responses.

There are also administrative tasks that may need to be accomplished. These include configuring and calibrating the device for a particular scenario, loading/updating of watch-lists, actions to be taken by the operator in different situations, logging of encounters, output of log files and other metrics, etc.

The application requirements for the Mobile ID device drive the overall system architecture and requirements for individual components of that system.

Note that there is flexibility in the overall system design shown in Figure 2. As illustrated in Figure 3 the 'Signal Processing' step may itself be split. In this example, a mobile ID device deals with the face, fingerprints and iris modalities. A separate unit deals with Rapid DNA (not considered to be a mobile ID device for purposes of this document). The output of these two units is combined at a local site to generate a unified transaction for a single individual. That transaction is forwarded to a second site, where the full suite of

information is added which is necessary for transmission to one or more sites that handle the matching.

Figure 4 illustrates a system architecture where the compressed iris image (only) is transmitted to a local station, where more information is added to the transmission to a central system for matching and processing. The central system may send back a candidate list to the local station for review. Based upon standard operating procedures (which may vary over time and operating conditions) a yes / no actionable response is sent back to the operator. Thus the telecommunications needs of the mobile unit are at an extreme minimum in this design.

Figure 3

Flexibility in System Design –
Illustration of Breaking Apart the Signal Processing Step

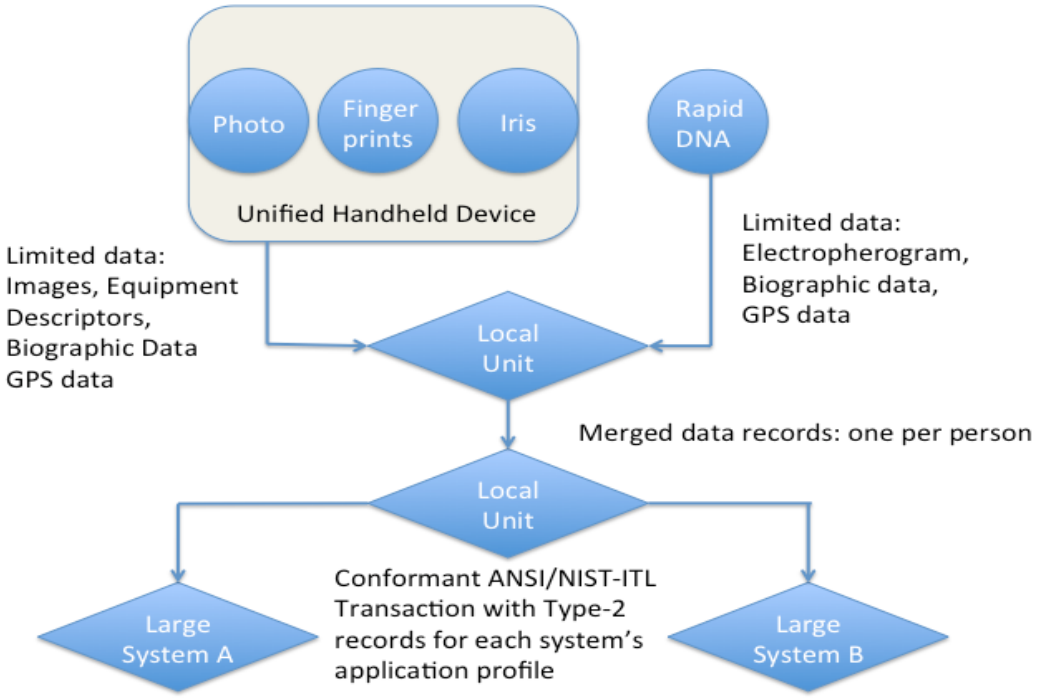
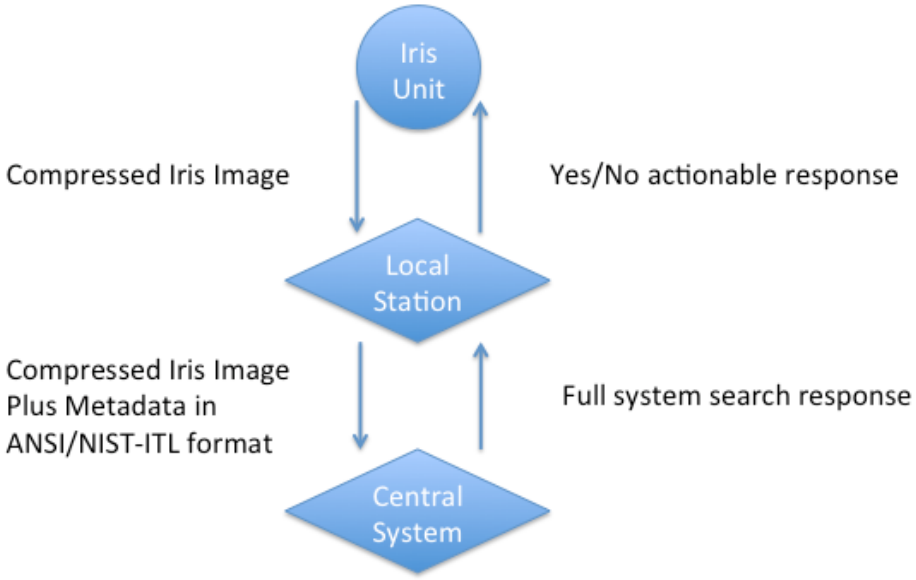


Figure 4

Flexibility in System Design –

Illustration of Breaking Apart the Signal Processing Step and

Breaking Apart the Decision Step



Many more configurations are possible other than the two illustrated above. As highlighted above, the physical design of the Mobile ID device impacts system requirements and constraints. Physical considerations include:

- System components connections (or lack thereof)
- Connectivity to other systems (sharing/interoperability)
- Security aspects of interconnected components

A partial list of design configurations might include one or more of the following within a system:

- Handheld biometric sensors
- Handheld data entry devices
- Handheld communications to a central location
- Handheld communications to a nearby vehicle
- Vehicle-based or other movable-platform-based data entry
- Vehicle-based or other movable-platform-based communications to a central location
- Processing power and storage capacity of the mobile device
- Power sources and battery life
- Display size and capability

The Mobile ID device may be designed and configured to achieve a level of integration defined as:

- Fully Integrated (e.g., sensors embedded within the device)
- Mated (e.g., smart phone/tablet with case/sled for rolled fingerprint capture)
- Tethered-peripheral (e.g., USB fingerprint reader)
- Physically separate components functioning together (e.g., tablet control of a physically separated biometric device, using WS-BD[9] protocols)

5 Data Format

Data formats are closely tied to the overall design requirements. Several different data formats may be employed within a system. To the extent possible, it is advisable to use standardized formats. Even for totally self-contained systems, data formats play a role – particularly when a documentary record is to be maintained of the interaction with the subject and the result of the match comparison. Typical data format considerations include:

- Format for data transport to external systems and / or locations and to import data from outside systems and / or locations
- Format at interfaces of components within a system
- Data compression
- Packet size
- Network bandwidth, latency
- Storage space (of processed or raw data)
- Data and privacy protection for storage and transmission
- Matching performance (i.e. for template formats)
- Data sharing requirements
- Data secrecy (possibility of security classification levels) and
- Data authentication.

6 Data Quality

The quality of data is a major factor in how accurately a system can perform. Quality assessment may occur at each stage in Figure 2 (automated and/or humanly reviewed). Quality is also affected by compression of data. Data shall not be compressed, then uncompressed and then recompressed at any point in its life cycle of use. Certain types of compression result a substantial loss of data ('lossy') while others are considered 'lossless'. Only one lossy data compression is allowed without compromising the integrity

[9] WS-BD refers to Web Services – Biometric Devices. NIST Special Publication 500-288 (*Specification for WS-Biometric Devices (WS-BD) Version 1)* is available at http://www.nist.gov/itl/iad/ig/upload/NIST-SP-500-288-v1.pdf "WS-BD provides a framework for deploying and invoking core synchronous operations via lightweight web service protocols for the command and control of biometric sensors." (Quoted from Section 2 of the document)

and fidelity of the data. Compression of an image or signal is a major consideration affecting the subsequent usefulness of the data, and it is addressed in the requirements associated with each modality.

The enrollment ('reference') data (which resides in a database – sometimes called the 'gallery' [10]) and the probe (which is being compared to the stored data) should be of the highest quality possible. Not all biometric modalities have clearly established measures of data quality that are predictive of matcher performance.

It is a best practice to attempt to capture the highest quality data possible, noting that not all scenarios enable the operator to collect high quality biometric data. Probes may fail to match against a poor quality enrolled image, or conversely there may be an unacceptable number of potential matches that need to be reviewed manually. A poor quality probe may likewise fail to match even a high quality enrolled image.

A best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process, whether for enrollment or for use as a probe. This may take several forms, such as (but not limited to):

- Use of an automated quality assessment tool
- Meter readings on the capture device (such as light levels on a camera and background noise levels for a voice-recording device).

As an example of an automated quality assessment tool, the NIST Fingerprint Image Quality (NFIQ) has been historically used in many systems. It is based upon a scale of 1 to 5 with 5 being the worst value. It is only applicable to fingerprint exemplars (not latent friction ridge prints, palm print exemplars or plantar print exemplars). If using NFIQ, it is a best practice that images captured with a value of 4 or 5 should not be used for enrollment purposes.

Capture devices may be designed to operate for only one modality or they may be able to capture multiple modalities. In addition, they may have different levels of ability for the operator to enter metadata (such as the circumstances concerning why the data was collected, the subject's name, etc.)

Some units may be designed to capture a biometric sample from the subject using one modality (such as fingerprint) and also capture a biometric sample from the operator (of the same or possibly even a different modality, such as voice) to verify that the operator is authorized to use the unit.

[10] The database can be anywhere from one sample to millions of samples.

7 Friction Ridges

This section describes the features of a capture unit that are specific to friction ridges.

7.1 Friction Ridge Capture Devices

Friction ridge capture devices for exemplars (i.e., captured from an individual, not a surface) have been used in mobile environments for many years. Since the general attributes are similar for all three types of friction ridges (finger, palm and plantar), they are grouped together in this document. In fact, some devices can be (and are) used for capture of different types of friction ridge prints. There are acquisition profiles that are described in Section 7.1.1 of this document. The Fingerprint Acquisition Profile (FAP) levels, Palm print Acquisition Profile (PAP) levels, and Toe and foot print Acquisition Profile (TAP) levels should be specified in record types 14, 15 and 19, respectively, when using the *ANSI/NIST-ITL standard*.

As discussed in Section 7.4, fingerprints can also be captured from objects (latent prints) – or even victims' bodies using mobile technology. These images can be transmitted in record type-13 based upon the *ANSI/NIST-ITL standard*. Latent prints are sufficiently different from exemplars that they are handled separately in the tables of this section.

Table 1 is from the 2015 Update of the *ANSI/NIST-ITL standard*. Notice that this table concerns impression types, while Table 2 concerns the capture technology. While one may imply the other, there is not always a direct correlation between the two. The codes in Table 1 should be entered in fields 13.003, 14.003, 15.003, and 19.003 of *ANSI/NIST-ITL* transactions. The codes are a subset of the original list of impression types for the *ANSI/NIST-ITL standard*, which is still retained for type-4 records[11]. Table 2 is excerpted from the *2015 Update of the ANSI/NIST-ITL standard*. The information in this table can optionally be entered in Fields 13.901, 14.901, 15.901, and 19.901[12] of *ANSI/NIST-ITL* transactions. Note that there is no capability to encode this information in a type-4 *ANSI/NIST-ITL* record.

[11] Type-4 records should be used only for transmission to legacy fingerprint systems. There is very limited capability to include metadata about the image in a type-4 record.

[12] These fields are new for the 2015 Update.

Table 1

Friction Ridge Impression Types

Exemplar Prints

Type	Code	Description
Contact Impressions		
Plain Contact	0	Finger(s) presented still on platen
Rolled Contact	1	Finger rolled on platen
Vertical Swipe	8	Finger swiped on platen
Contactless Acquisitions		
Plain Contactless – Stationary Subject	24	Finger(s) / palm / plantar presented stationary, in view of a stationary sensor and sensor captures plain contact equivalent.
Rolled Contactless – Moving Subject	25	Finger(s) /palm / plantar rolled in view of the sensor
Rolled Contactless – Stationary Subject	41	Finger(s) / palm / plantar presented stationary, and sensor captures rolled equivalent
Plain Contactless – Moving Subject	42	Finger(s) / palm / plantar move though the capture volume of a sensor
System Integration Exceptions		
Other	28	
Unknown	29	

Latent Prints

Type	Code	Description
Latent image	4	Image or impression of friction skin deposited on a surface

Table 2

Friction Ridge Capture Technology

Technology	Code	Description
Unknown	0	Capture Technology not provided by sensor manufacturer
Other	1	Capture Technology not sufficiently characterized by table
Optical - Total Internal Reflection (TIR) – Bright Field	3	Using optical angle of incidence effects, a contact fingerprint scanner captures ridge information such that ridges absorb light, and absence of ridges reflects light back to the sensor (dark ridges on a white background)
Optical TIR – Dark Field	4	Using optical angle of incidence effects, a contact fingerprint scanner captures ridge information such that ridges reflect light (white ridges on a dark background)
Optical Direct Imaging - Native	5	Light reflected from the friction ridge is imaged, resulting in a light gray on darker gray image… This may be performed by contact or contactlessly, and may incorporate merging of images from multiple sensors or from rocking or swaying sensors / subjects.
Optical Direct Imaging – Low Frequency Unwrapped	6	Light reflected from the friction ridge is imaged onto 1 or more sensors. This may be performed by contact or contactlessly, and utilizes the low frequency 3D detail to “unwrap” or project the image texture onto a 2D grayscale image.
3-Dimensional Imaging – High Frequency Unwrapped	7	High frequency friction ridge information is collected (optically, acoustic, etc.), and then “unwrapped” to create a 2D image from the 3D point cloud or mesh
Capacitive	9	A contact technology in which the capacitance of the fingerprint is assessed via a conducted AC signal
Capacitive – Radio Frequency (RF)	10	A contact technology in which the capacitance of the fingerprint is assessed via a radiated RF signal
Electro-luminescent (EL) Optical Direct Imaging	11	A contact technology in which the ridges and an Alternating Current (AC) signal cause an EL panel to emit light which is captured by an imaging system

Technology	Code	Description
Reflected Ultrasonic Image	12	A contact technology in which the friction ridge reflects ultrasonic energy which is assessed by the sensor
Ultrasonic Impediography	13	A contact technology in which the absorption of ultrasonic energy is measured by changes in the impedance of a piezo-electric material
Thermal Imaging	14	A contact technology in which the sensor measures the heat reflected from the fingerprint in contact with the sensor.
Direct Pressure Sensitive	15	A contact technology in which the pressure of the fingerprint ridges against a material is measured.
Indirect Pressure	16	A contact technology in which the pressure of the fingerprint ridges against a deformable material is assessed optically to produce a friction ridge image.
Latent Impression	18	A capture process in which the digital image of the latent impression is acquired directly from the latent impression, using a flatbed scanner or digital camera.

7.1.1 Friction Ridge Acquisition Profiles

Table 3, Table 4 and Table 5 show the acquisition profiles for devices collecting images from fingers, palms and feet, respectively. As noted in Table 2, there are many other types of capture devices. Contact optical devices may be tested according to protocols established by the FBI, and the list of certified products is maintained on the FBI website: https://www.fbibiospecs.cjis.org.[13] The acquisition profiles are an easy way to summarize a set of characteristics for procurement actions or product fact sheets. The ANSI/NIST-ITL standard contains fields for the transmission of the acquisition profile specification level for optical capture devices used to generate the images.

It is up to the system designer of each particular application to determine the appropriate levels for each of the enrollment, identification, or verification functions especially if there is an intention to exchange data with other systems

A single unit may meet a certain fingerprint acquisition profile (FAP) level, and one for palm prints (PAP) and one for plantars (TAP). The concept of acquisition profiles is also extended to other biometric modalities beyond those of friction ridges, such as face and

[13] Some non-optical devices have also been tested by the FBI using procedures modified from those developed for optical devices. Each such test must be developed with the characteristics of the non-optical acquisition device taken into account. The object is to ensure that such a device will yield images comparable or better than an optical device.

iris. Therefore, a multi-biometric capture unit / system may also list an iris acquisition profile (IAP) and a subject face acquisition profile (SAP).

The following sections describe the row entries (specifications) in Table 3, Table 4, and Table 5. Note that these acquisition profiles do NOT apply to latent prints. These sections concern acquisition of a print directly from a person (alive or dead).

7.1.1.1 Flat Images and Rolled Images

This category is associated with fingerprints. As defined in the *ANSI/NIST-ITL standard* for fingerprints:

- Flat fingerprint: A fingerprint image resulting from the touching of a single finger to a livescan platen or paper fingerprint card without rolling motion. Also known as a single-finger plain impression.

- Rolled fingerprint: A fingerprint image collected by rolling the finger across a livescan platen or paper fingerprint card from nail to nail.

For units with platens smaller than 1.6" x 1.5", rolled images should not be captured. It should be noted that the very small platens associated with FAP 10 might not capture a sufficient area of the fingerprint for certain applications, resulting in a high False Non-Match Rate when compared to a large database. It is strongly recommended that single-finger units be a minimum level of FAP level 30 [14] for mobile applications (other than unlocking the mobile device using the embedded sensor).

7.1.1.2 Gray Levels

This category is applicable to FAP, PAP and TAP tables.

Note that the minimum gray levels are the same for all levels. Grayscale should normally be quantized to eight bits (256 gray levels).

It is a best practice to acquire exemplars using sensors that operate producing grayscale images.

[14] See NISTIR 7950, "*Examination of the Impact of Fingerprint Spatial Area Loss on Matcher Performance in Various Mobile Identification Scenarios*" March 2014. It is available at http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7950.pdf.

7.1.1.3 Acceptable Image Resolution

This category is applicable to FAP, PAP and TAP tables. The resolution of the images shall be either 500 pixels per inch (ppi) or 1000 ppi. A small variance is allowed around these two values. For PIV-certified devices, a 2% tolerance level is allowed for 500 ppi devices. For Appendix F certified devices, a maximum 1% deviance is allowed from either 500 or 1000 ppi.

7.1.1.4 Image Dimension

This category is applicable to FAP, PAP and TAP tables. A principal distinguishing characteristic of the various acquisition profile levels is the size of the capture area for the friction ridge sample. There is usually a direct relationship between the size of the capture platen and the size of the unit itself. However, there is a tradeoff. Small units require imaging each finger individually. Additionally, very small units (such as FAP 10) only capture a small portion of the fingerprint. By nature, palm and plantar print sensor surfaces are larger and may be larger than the units used to capture a four-finger slap image. Each operating and data processing / matching agency must determine what levels are determined to be acceptable for their operational use. This is usually stated in procurement actions using wording such as 'A minimum of FAPxx (or PAPxx or TAPxx) level shall be provided by the vendor for all units delivered under this contract."

7.1.1.5 Compression Algorithm

If compressed, friction ridge images captured at 500 ppi shall use the Wavelet Scalar Quantization (WSQ) algorithm for compression prior to transmission and/or storage. For platens 3.2" x 1.5" or larger, WSQ Version 3.1 or higher shall be used. Earlier versions of WSQ were not adapted for larger platens and can fail to properly handle data around the edges of the area of capture. WSQ specifications are contained in *WSQ Gray-scale Fingerprint Image Compression Specification, October 2010.* Friction ridge images captured at 1000 ppi shall use the Joint Photographic Experts Group (JPEG) 2000 algorithm for compression prior to transmission and/or storage. This shall be in accordance with the JP2 format as described in *ISO 15444-1*. *NIST Special Publication 500-289, Compression Guidance for 1000 ppi Friction Ridge Imagery*[15] provides explicit guidance on how to perform these compressions. Some systems can accept and process only 500 ppi images. Therefore, if a mobile device captures images at 1000 ppi, the image may need to be converted to 500 ppi prior to transmission. This conversion shall be performed according to the guidance in "*Examination of Downsampling Strategies for Converting 1000 ppi Fingerprint Imagery to 500 ppi, NISTIR 7839*"[16].

[15] It is available at http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-289.pdf
[16] Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912779

7.1.1.6 Compression Ratio

If an image is over-compressed, it loses salient characteristics that may be useful for matching. NIST performed studies on image compression[17] that analyzed the levels of compression.

For small images (smaller than 1.6" x 1.5"), a compression of 10:1 is specified at 500 ppi. For larger platens capturing at 500 ppi, a ratio of 15:1 is specified. However, at 1000 ppi, all platen sizes shall use a ratio of 10:1.

7.1.1.7 Simultaneous Fingers

The 'simultaneous fingers' reference in Table 3 is a reminder of the practical implication of using a unit that has a platen size corresponding to each particular FAP level.

7.1.1.8 Sensor Certification

Sensor certification can be extremely important in procurement actions. The list of FBI-certified products available at https://www.fbibiospecs.cjis.gov have passed tests to establish conformance to specifications for PIV-devices or FBI-EBTS Appendix F specifications. Note that some organizations may require devices to be subject to further tests.

[17] See the studies available at http://www.nist.gov/itl/iad/ig/compression.cfm

Table 3

Fingerprint Acquisition Profile (FAP) Levels

Capture[18]	FAP 10	FAP 20	FAP 30	FAP 40
Acquire Flat Images	Yes	Yes	Yes	Yes
Acquire Rolled Images	No	No	No	Optional
Minimum Gray Levels	256	256	256	256
Acceptable Image Resolution	500 +/- 2%	500 +/- 2%	500 +/- 2%	500 +/- 2%
Minimum Image Dimension (W x H) inches	0.5”x.65”	0.6”x 0.8”	0.8”x 1.0”	1.6”x1.5”
Maximum Compression Ratio	10:1	10:1	10:1	15:1
Compression Algorithm	WSQ 2.0+	WSQ 2.0+	WSQ 2.0+	WSQ 2.0+
Simultaneous # of Fingers	1	1	1	1-2
Sensor Certification	PIV	PIV	PIV	PIV

Capture	FAP 45	FAP 50 [19]	FAP 60	FAP 145	FAP 150	FAP 160
Acquire Flat Images	Yes	Yes	Yes	Yes	Yes	Yes
Acquire Rolled Images	Optional	Optional	Optional	Optional	Optional	Optional
Minimum Gray Levels	256	256	256	256	256	256
Acceptable Image Resolution	500 +/- 1%	500 +/- 1%	500 +/- 1%	1000 +/- 1%	1000 +/- 1%	1000 +/- 1%
Minimum Image Dimension (W x H) inches	1.6”x1.5”	3.2”x2.0”	3.2”x3.0”	1.6”x1.5”	3.2”x2”	3.2”x3.0”
Maximum Compression Ratio	15:1	15:1	15:1	10:1	10:1	10:1
Compression Algorithm	WSQ 2.0+	WSQ 3.1+ [20]	WSQ 3.1+ [20]	JPEG2K [21]	JPEG2K[21]	JPEG2K[21]
Simultaneous # of Fingers	1-4 [22]	1-4[23]	1-4	1-4	1-4	1-4
Sensor Certification	Appendix F	Appendix F	Appendix F	N/A	N/A	N/A

[18] Scanner resolutions values specified in pixels per inch (ppi) as well as scanner platen dimensions and capture area sizes specified in inches are based on widely used specification guidelines for such devices and is accepted as common nomenclature within the industry. SI units for these will not be presented in this document for these values.

[19] In ANSI/NIST-ITL prior to 2015, FAP 50 had a minimum dimension of 2.5” x 1.5” and was specified for 1-3 fingers. However, no devices were created matching these characteristics, and there was a market presence corresponding to the revised FAP 50 specifications in this document and ANSI/NIST-ITL 1-2011 Update 2015.

[20] Larger platens require WSQ 3.1 or higher.

[21] JPEG2K is required for 1000 ppi images. WSQ was designed for 500 ppi compression only.

[22] Up to 4 fingers may be allowed by some systems, if stitched images are acceptable according to the Organization’s Application Profile. Some capture units may be capable of taking two images and stitching them into one output image. 2 fingers fit without stitching on one image for this size platen.

[23] Although technically possible to capture four slap fingers on a FAP 50 device, it requires angling of the fingers, which may be problematic for certain systems. Some application profiles actively discourage slanted fingers. The FBI states, “All friction ridge prints should be captured as closely as possible to an upright position.”

7.2 Fingerprint Capture Unit Equipment Specifications

Table 3 lists the Acquisition Profile levels for optical capture devices that can be used for fingerprint capture[24]. It is highly recommended that the procuring organization adhere to the scanning resolution, gray scale, compression ratios and algorithms specifications of the table. When a FAP level is not applicable due to the technology deployed, then the user should include the Make and Model of the acquisition unit in Field 14.904 of an *ANSI/NIST-ITL* transaction record when using that record type.

Mobile devices with the capability to detect the location of the fingerprint are desirable to provide a left/right, up/down indication for the operator or subject to insure optimal image content.

Display of fingerprints on mobile device during the capture process is a useful option for some mobile device applications.

Mobile devices with the capability to evaluate each image frame captured are desirable to determine if a fingerprint is present that meets quality requirements and automatically save the image.

Mobile devices with the capability to manually command the device to capture the image currently on the sensor are desirable to insure the ability to capture difficult to image fingers.

After capture of the fingerprint images, an automated quality check function is desirable based on a combination of:

- Image photographic properties
- Image size
- Minutiae count
- Core location
- NIST Image quality scores (NFIQ)

Imaging sensors (e.g., optical scanner platen surfaces) that may be field-replaced and automatically calibrated are desirable to ensure continuity of use.

Aside from the recommendations and requirements listed above for the fingerprint capture device, other factors that affect the performance of these Mobile ID devices and systems need to be considered. Many of these relate to training and include:

- Operation of the device within temperature and humidity specifications

[24] Non-optical devices may be tested and certified on a case-by-case basis, since specialized tests must be developed for each – to ensure a suitable level of fidelity.

- Ruggedness of the device
- Operator safety
- Cleanliness of fingers
- Maintain clean sensor surface
- Types of cleaners allowed on sensor surface
- Consistent placement of the same finger(s)
- Optical scanners should avoid excess illumination (or use capture devices that can function effectively in full sunlight)
- Procedures to minimize the possibility of finger sequence errors, if enrolling more than 1 finger
- Automated quality feedback to operator
- Speed of capture
- How many transactions can be in process simultaneously (can a new set of fingerprints be captured while waiting for search results?)

7.3 Fingerprint Capture of Exemplars from Persons

This section details the basic requirements for fingerprint capture using mobile ID devices. It should be noted that additional requirements could be specified based upon the use case.

7.3.1 Capturing Fingerprints from Living Persons

The ergonomics of fingerprint capture from living persons is an important factor in determining which mobile ID device to acquire and how to use it. When procuring a unit, the authority should determine which use case or group of use cases is applicable. There may be tradeoffs in order to perform multiple operations.

A major factor is whether the subject is likely to be cooperative. Another factor is the ability of the subject to self-manipulate his/her fingers(s) (e.g., if handcuffed).

Placing a finger / fingers upon a platen with the appropriate pressure and area of capture is essential for a usable print to be acquired. There should be a presentation screen for the operator, and the unit should be capable of being held by the operator, unless the concept is to place the unit on a flat surface without holding it. In such a case, the operator may be able to physical assist the subject with placing the finger(s) upon the platen.

For uncooperative subjects, such as those in handcuffs, the ergonomics of the capture of the prints may dictate a particular physical form for the device. It is likely that the operator will have to manipulate the device to and possibly around the subject's finger(s).

- Mobile ID fingerprint devices should be configurable so they can capture the specified finger(s) for a particular application.
- Use cases should dictate the number of fingers to be used.
- When fewer than 10 fingerprints are captured, it is recommended that fingers 2, 3, 7, & 8 be used.
- When possible, capture of 4 fingers is preferable to capture of 2 fingers.
- Enrollments for a system that supports latent searches should include thumbs.
- Fingerprint images captured with dimensions according to lower FAP levels may contain only a small area of the fingerprint and thereby may reduce the overall system accuracy. This shortfall should be kept in mind and tradeoffs weighed carefully in utilizing the lower FAP levels.

7.3.2 Capturing Fingerprints from Deceased Persons

For living persons, the finger(s) are typically brought to the device and may be manipulated to acquire the print – such as the operator guiding a subject's finger to produce a rolled print.

For deceased individuals, the finger(s) may exhibit rigor mortis, be partially decomposed and / or dehydrated. This provides challenges to the acquisition of prints with a mobile device. There are several choices on how to best acquire the prints, such as (but not limited to):

- Manipulate the device around the finger(s) (with or without re-hydration)
- Sever the finger(s) and press / roll them on the device
- Sever the hand, remove the skin and place an operator's hand within the skin to acquire the prints in a manner similar to acquiring prints from a living person

An excellent reference on the subject is Chapter X of "*The Science of Fingerprints*" (Published by the FBI) called "Problems and Practices in Fingerprinting the Dead".[25]

The quality of the prints may be poor, with little chance of improving the quality – unlike with living individuals, when a recapture often provides a better sample. In many cases, the captured print will be comparable in quality to that of a latent print – with portions of the print unusable for matching. In fact, some jurisdictions submit prints from deceased individuals to be processed as latent prints. In such cases, a type-13 record is used when transmitting using an *ANSI/NIST-ITL* transaction. Field 13.046 (Image subject condition / SUB) should be completed to indicate that the **subject status code (SSC)** is D (data obtained from a non-living person). The subject body status code shall be recorded as either 1 (whole) or 2 (fragment). The **subject body class code (SBSC)** shall also be

[25] Available at http://www.gutenberg.org/files/19022/19022-h/19022-h.htm#CHAPTER_X

recorded as either 1 (natural tissue) or 2 (decomposed). There is also a field 14.066 that contains similar information items, if the image is good enough to be submitted as a type-14 record.

7.4 Capture of Latent Fingerprints from Objects

The equipment used for capture of latent prints from objects is substantially different from that used to capture prints directly from an individual. The *ANSI/NIST-ITL standard* states: "A latent impression is the digital image of the latent impression that was acquired directly from a latent impression, using a flatbed scanner or digital camera." This document does not deal with other means of acquiring latent prints, such as 'lifts' or casts / molds. Note that there is no requirement that latent prints be grayscale. In fact, many jurisdictions prefer that photographic images of latent prints be in color.

It is best practice to record the make and model of the imaging equipment in Field 13.904 (Make/model/serial number / MMS) of the type-13 record in an *ANSI/NIST-ITL* transaction, which is used to transmit latent print images.

When acquiring a latent print using photography, the best practice is to have a ruler or scale present, and this presence should be indicated in Field 13.018 (Ruler or scale presence / RSP). The user indicates whether the scale is in inches (IN), millimeters (MM) or BOTH. If known, the user should also include the maker and model of the ruler or scale. The determination of pixel density of the image is important. *ANSI/NIST-ITL* Field 13.019 (Resolution method / REM) should be used to state how this was done. However, generally, a ruler should be used with mobile ID devices. It is important that the ruler be accurate. An example of the American Board of Forensic Odontology (ABFO) scale is shown in Figure 5 [26]. The ABFO Reference Scale # 2 [27] has been in use since 1988. It was designed for imaging of patterned injuries, but may also be useful in imaging latent prints. The ABFO # 2 specifications include reflectance values of grayscale – which is important for latent images. It is important to note that several manufacturers produce rulers resembling ABFO # 2 specifications.

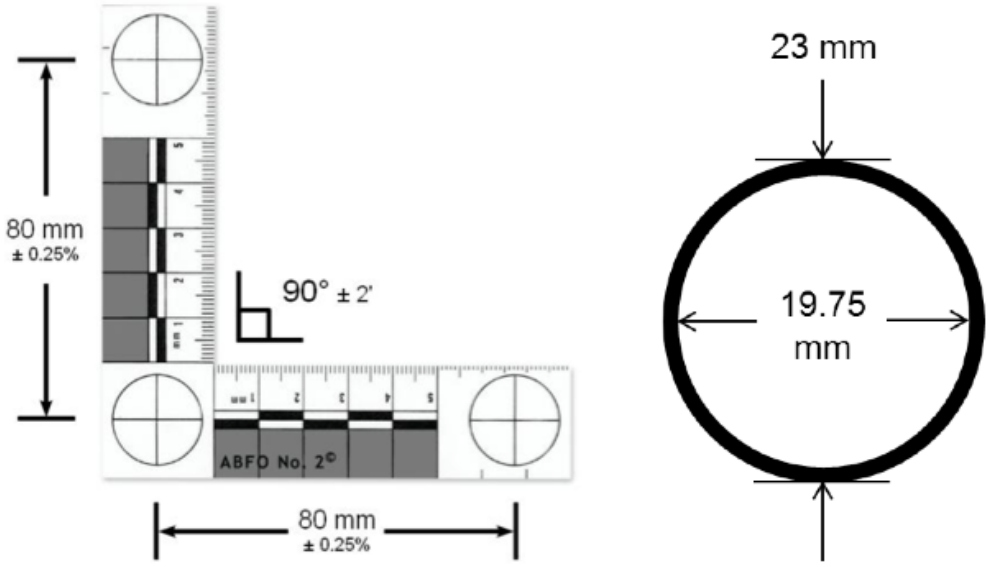
[26] "Dimensional Review of Scales for Forensic Photography", https://www.ncjrs.gov/pdffiles1/nij/grants/243213.pdf

[27] Hyzer WG, Krauss TC, "The Bite Mark Standard Reference Scale – ABFO No.2", J Forensic Sci. 1988 Mar; 33(2): 498-506

Figure 5

Sample rulers for Latent Print capture –

ABFO # 2 (NOT TO SCALE -- DO NOT USE OR COPY)



7.5 Palm Print Capture Unit Equipment Specifications

The capture of palm print exemplars is similar in concept to that of fingerprints. The principal differences are:

- The area of the print is larger.
- The palm is not usually rolled.

The minimum platen area is 5.0" x 5.0" corresponding to a PAP 70 level (as shown in Table 4). As with the Fingerprint Acquisition Profiles, there are levels corresponding to 500 ppi and to 1000 ppi outputs, with corresponding differences in compression ratio and compression algorithm to be used.

All PAP levels require the ability to capture flat images. Capture of rolled images is optional. The minimum grayscale level when specifying a PAP level is 256.

Not included in these basic specifications are others that will be of interest to the procuring agency, including (but not limited to):

- Weight of the unit
- Ability to capture images outdoors (protection from too much sunlight)
- Ability to withstand environmental conditions typical of the conditions in which the unit will be used (dust, heat / cold exposure, humidity, etc.)
- Routine maintenance requirements

Table 4

Palm print Acquisition Profile (PAP) Levels

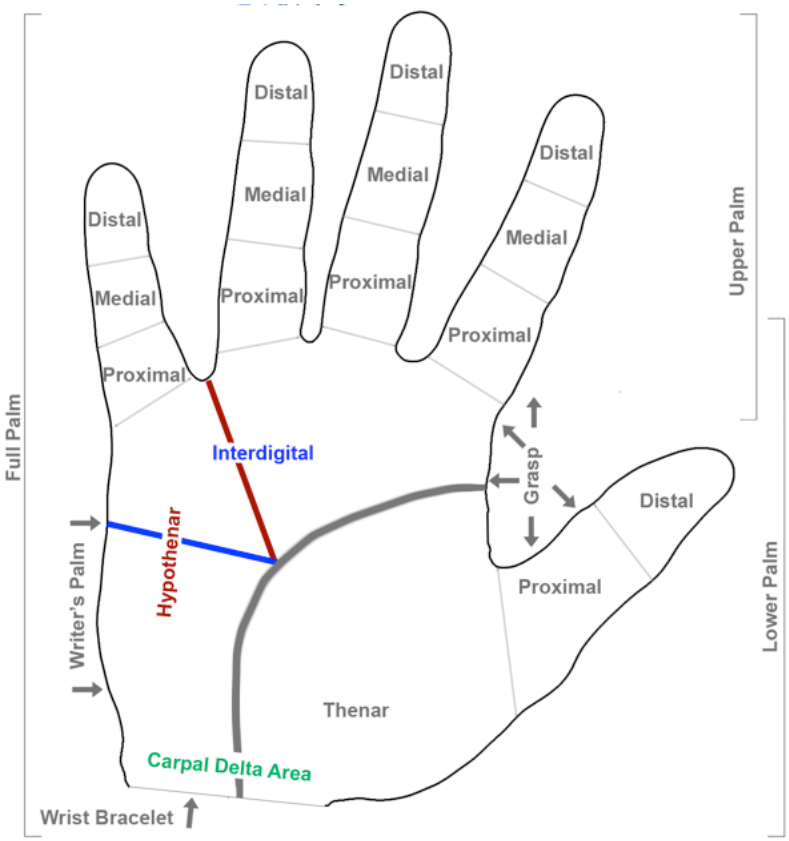
Capture	PAP 70	PAP 80	PAP 170	PAP 180
Acceptable Image Resolution	500 +/- 1%	500 +/- 1%	1000 +/- 1%	1000 +/- 1%
Minimum Image Dimension (W x H) inches	5.0” x 5.0”	5.0” x 8.0”	5.0” x 5.0”	5.0” x 8.0”
Maximum Compression Ratio	15:1	15:1	10:1	10:1
Compression Algorithm	WSQ 3.1+	WSQ 3.1+	JPEG2K	JPEG2K

7.5.1 Capturing Palm prints from Living Persons

Note that PAP levels 70 and 170 (as shown in Table 4) will require at least 2 impressions to obtain a full-palm image set, due to the size of the platen. The FBI states [28]: "The entire area of the full palm is defined as that area extending from the wrist bracelet to the tips of the fingers and can be represented as one or two images to represent the full palm. The lower image shall extend from the wrist bracelet area to the top of the interdigital area (third finger joint) and shall include the thenar and hypothenar areas of the palm. The upper image shall extend from the bottom of the interdigital area to the upper tips of the fingers. This provides an adequate amount of overlap between the two images to facilitate subject verification. By matching the ridge structure and details contained in the common interdigital area, an examiner can confidently state that both images came from the same palm. Because neither plain impressions nor identification flat impressions include this common overlapping interdigital area, they should never be submitted as upper palm images." See Figure 6.

Figure 6

Palm and Finger Segment Positions



[28] EBTS Technical and Operational Update #5, Version 10.0.5 Final — June 13, 2015
https://www.fbibiospecs.cjis.gov/EBTS/Approved

7.5.2 Capturing Palm Prints from Deceased Persons

As is the case with fingerprints, the condition of the palm may affect the quality of the acquired print. If rigor mortis is present in a deceased individual, it may not be possible to easily acquire the palm print. The procedures that are to be followed to obtain a palm print may vary by jurisdiction.

7.6 Palm Print Capture of Latent Prints from Objects

The same considerations exist for capturing latent palm prints as for latent fingerprints.

7.7 Toe and Sole Capture of Exemplars from Persons

The capture of toe and sole (plantar) exemplars is similar in concept to that of fingerprints. The principal differences are:

- The area of the print is larger.
- The foot is not usually rolled.

This is reflected in the equipment specifications. The minimum platen area is 5.0" x 5.0" corresponding to a TAP 70 level (as shown in Table 5). As with the fingerprint Acquisition Profiles, there are levels corresponding to 500 ppi and to 1000 ppi outputs, with corresponding differences in compression ratio and compression algorithm to be used.

Not included in these basic specifications are others that will be of interest to the procuring agency, including (but not limited to):

- Weight of the unit
- Ability to capture images outdoors (protection from too much sunlight)
- Ability to withstand environmental conditions typical of the conditions in which the unit will be used (dust, heat / cold exposure, humidity, etc.)
- Routine maintenance requirements

All TAP levels require the ability to capture flat images. Capture of rolled images is optional. The minimum grayscale level is 256. It is important to note that some scanners large enough to fit a foot upon have been certified as meeting the optical requirements of Appendix F. However, this does not mean that they have been certified for acquisition of exemplars. They were designed to scan cards that are fully stationary upon the imaging surface during the period of scanning. In addition, placing the weight of a foot upon the scanner may not be advisable. There have been no scientific studies performed at the date of production of this document that have examined the quality of images captured directly from a foot on a scanner.

Table 5

Toe and Sole (Plantar) Print Acquisition Profile (TAP) Levels

Capture	TAP 70	TAP 80	TAP 170	TAP 180
Acceptable Image Resolution	500 +/- 1%	500 +/- 1%	1000 +/- 1%	1000 +/- 1%
Minimum Image Dimension (W x H) inches	5.0" x 5.0"	5.0" x 8.0"	5.0" x 5.0"	5.0"x 8.0"
Maximum Compression Ratio	15:1	15:1	10:1	10:1
Compression Algorithm	WSQ 3.1+	WSQ 3.1+	JPEG2K	JPEG2K

Scanners may be capable of taking a direct image of the foot, as well as doing their normal function of scanning cards. The capture of toe and plantar prints can be difficult. For small infants, a standard sized palm 4-finger slap unit may suffice, which is the same as TAP 70. However, larger feet may require taking multiple, possibly overlapping, prints to capture the entire friction ridge area of the foot. It is therefore recommended that for larger feet the portions of the foot be captured in the following manner:

1) Flat Toes -- all five together
2) Ball of the foot
3) Heel of the foot

For some individuals, it may be possible to capture the middle of the foot, as well.

7.8 Toe and Sole (Plantar) Capture of Latent Prints from Objects

The same considerations exist for capturing latent plantar prints as for latent fingerprints.

7.9 Friction Ridge Interchange Requirements

It is highly recommended that much of the information needed for an *ANSI/NIST-ITL* transaction be collected or generated automatically by the collection device.

Most data exchanges of fingerprint information for law enforcement, military and homeland security applications are based upon the *ANSI/NIST-ITL standard*. Organizations have typically refined the standard using 'application profiles' to specify which record types, fields and information items that they require (which may be optional in the standard). Certain application profiles may disallow the use of specific options contained in the standard.

Some applications, such as e-passports and the Indian UID (Unique Identification) program are based upon the International Organization for Standardization (ISO) *19794* suite of standards. The principal differences between the *ANSI/NIST-ITL* and *ISO 19794* standards are the types and amount of metadata associated with the biometric sample and that the *ISO* standards handle each modality as a separate transaction but the *ANSI/NIST-ITL standard* allows multiple modalities within a single transaction concerning an individual.

Friction ridge record types in the *ANSI/NIST-ITL standard* are divided into the following principal groups:

1) Exemplar Images
    a. Fingerprint
        i. Type-4 (only recommended for legacy systems)
        ii. Type-14
    b. Palm prints
        i. Type-15
    c. Plantar prints
        i. Type-19
2) Latent prints
        i. Type-13
3) Minutiae – all friction ridge types
        i. Type-9

In addition, there is the capability to transmit an image that is used to extract the image that was used for further processing (such as when multiple prints are in the same image and must be segmented first).

4) Original Image
        i. Type-20

It is considered best practice to save the original image. If it is cropped, rotated or otherwise prepared for inclusion as a type-13, -14, -15, or -19 image, then the original should be transmitted with it in a type-20 record. The method of linking these records (the original and the processed one(s) is described in the *ANSI/NIST-ITL standard* in detail. Note that this is particularly useful for latent images with multiple prints in view.

When multiple fingers are captured in the same image, depending on the specific Application Profile requirements, the user may

- Store the image with all four fingers in a type-14 record, with the segmentation coordinates specified.
- Store the original in a type-20 record and segment each finger for a separate type-14 record.

Record types 13, 14, 15 and 19 contain several fields for metadata associated with an image. Type-4 is an older type of record, which is discouraged from use. The type-14 record should be used for flat or rolled impressions at 500ppi WSQ or 1000 ppi JPEG2K (potentially transcoded down to 500 ppi WSQ) and the type-4 logical record (when used to transmit to a legacy system) shall be used only for impressions at 500 ppi WSQ. However, the record type to be used for either flat or rolled images is dependent on the transaction type, the capabilities, and the protocols of the receiving system. The sender of the transaction must coordinate with the recipient systems' owners in order to determine whether type-4 or type-14 is appropriate for a particular transaction type and for that system.

7.9.1 Image vs. Template

To support interoperability between systems without sacrificing search accuracy, the preferred approach is to transmit the friction ridge image(s), thereby enabling the minutiae to be extracted and processed on the system where the matching will take place.

However there are some cases where a minutiae-based approach may be acceptable or where the transmission of images may not be possible (e.g., if the device is only used in conjunction with a single algorithm or system or due to network bandwidth limitations).

Mobile ID devices may also be used to verify a person's identity against an ID card or token on which a biometric is stored, and such data may be either image or minutia based. When this mode is used, the minutia extractor should be one that has been certified by NIST as PIV compliant and interoperable with other templates and systems. These extractors were certified as a result of the Minutiae Interoperability Exchange Test (MINEX) interoperability tests [29].

8 Mobile ID 2D Photographic Images

Mobile ID imaging technology exists that is capable of taking facial images as well as images of other body parts that may be useful in identification or verification. In addition, such images can be used for documentation and for logging of the identity of the operator. An *ANSI/NIST-IT*L type-10 record is used to convey 2D photographic imagery of body parts, including faces, unique body features, scars and tattoos.

Videos may be collected and conveyed with a type-20 record (Original Source Representation) or a type-21 record (Associated Context). The use of video cameras worn by law enforcement officers is increasing and is recognized as a vital source of data.

[29] http://www.nist.gov/itl/iad/ig/minex.cfm

Videos recorded by bystanders and by surveillance cameras have also proven to be helpful in law enforcement applications.

If videos are used to extract still images for forensic or automated comparison or analysis, then they are conveyed with a type-20 record. If they are used to extract voice information for a type-11 record, they shall also be conveyed with a type-20 record. However, if the video is used as the voice recording itself, it shall be conveyed with the type-11 record. In such a case, the visual content of the video is not used for processing. By placing a video in type-20, the audio content can be specified and described in the type-11 record, and the individual frame images can be described in a type-10 record.

Since iris image equipment is relatively specialized and the data is transmitted in an *ANSI/NIST-ITL* type-17 record, that category is treated separately in this document.

3D image capture and specialized techniques such as LIDAR are not addressed in this document. However, if they are utilized, the imagery from those units shall be transmitted in *an ANSI/NIST-ITL* type-22 record (Non-photographic imagery data record).

Although photographic techniques can be used for fingerprint (and other friction ridge) acquisition, they are not covered in this section. Such techniques are covered in Table 1 under codes 24 (Plain contactless – stationary object) and 42 (Plain contactless – moving object).

8.1 Basic Equipment Requirements

Additional requirements may be needed to meet the specific situational needs for particular use cases, operating conditions and organizational standard operating procedures.

This section addresses only certain minimum requirements for 2D photographic image capture. Additional requirements are determined by the use cases / agency policies / legal requirements and other factors. Table 6 lists the minimum requirements for Mobile ID photographic capture equipment.

Although most cameras (both still image and video) are digital, it is possible to use film cameras in mobile ID situations. For digital cameras, the cameras should store the date and time in the header of the image. It is highly recommended to also store the GPS location (accessed automatically by the camera) with the image data, if possible.

Table 6 refers to cameras used to capture still photographs, and not videos. These requirements are mandatory for still image face capture if the SAP levels 32, 42 or 52 are met (as shown in Table 7).

A recommended, but optional, feature is a xenon flash or an LED / fill-in flash. The ambient light and exposure time are naturally correlated. It is recommended that the ambient light be 4 lux and that the exposure time be less than .0

Table 6

Mobile ID Still-Frame Photographic Requirements

Factor	Comments
Capture distance in cm	60-200 cm (~ 2 – 6 feet), the longer distance is preferred
Wavelength range	Visible light. 380-780 nanometers

Table 7

Mobile Device Face Subject Acquisition Profile (SAP) levels

Capture	Comments	Levels		
		32	42	52
Capture device color space		Minimum of 24-bit RGB color space or a minimum of 12-bit monochrome color space	Minimum of 24-bit RGB color space or a minimum of 12-bit monochrome color space	Minimum of 36-bit RGB color space or a minimum of 12-bit monochrome color space
Image resolution (size)	Lower resolution may reduce accuracy	≥ 480 x 600	≥ 786 x 1024	≥ 2400 x 3200
Capture device controls		Auto gain and auto shutter, optional: control loop for camera parameter (shutter speed / flash intensity) based on face area on-board	Auto gain and auto shutter, optional: control loop for camera parameter (shutter speed / flash intensity) based on face area on-board (requires continuous face detection)	Auto gain and auto shutter, optional: control loop for camera parameter (shutter speed / flash intensity) based on face area on-board (requires continuous face detection)
Photo composition	Pose of the subject	'Head' or 'Head and Shoulders'	At least one full-frontal 'Head and Shoulders' image	At least one full-frontal 'Head and Shoulders' image
Horizontal:Vertical Ratio		4:5	3:4	3:4

Capture	Comments	Levels		
		32	42	52
Compression algorithm		JPEG. Maximum compression ratio 15:1 for the region of interest comprising the exposed skin of the face, from crown to chin ear-to-ear. The non-facial portion of the image may be compressed up to a ration of 120:1. Best practice is to apply lossless compression to the frontal image with the ears visible.	JPEG 2K. Maximum compression ratio 15:1 for the region of interest comprising the exposed skin of the face, from crown to chin ear-to-ear. The non-facial portion of the image may be compressed up to a ration of 120:1. Best practice is to apply lossless compression to the frontal image with the ears visible.	JPEG 2K. Maximum compression ratio 15:1 for the region of interest comprising the exposed skin of the face, from crown to chin and ear-to-ear. The non-facial portion of the image may be compressed up to a ration of 120:1. Best practice is to apply lossless compression to the frontal image with the ears visible.
Inter-eye distance	Lower resolution may reduce accuracy	≥ 90 pixels	≥ 150 pixels	≥ 300 pixels

8.2 Image Data Handling Requirements – On Device

Several photographic imagers (cameras) have the capability to store uncompressed or compressed or both types of images. In addition, some units allow adjustments to compensate for exposure, color variation, to do cropping and other adjustments upon the original image. It is considered a best practice to store the uncompressed image and retain it for archival purposes, even if a lossy compressed image is to be transmitted.

8.2.1 Still Photograph

There is no need for an *ANSI/NIST-ITL* format to be generated directly by the image capture device. Normally, the photographic image would be captured and later formatted into an *ANSI/NIST-ITL* transaction prior to relaying to another site.

A digital photograph should not be post-processed from the camera's storage format to another format for transmission. However, it is recognized that some cameras store images in non-standard formats, and it may be necessary to change the format (compression) so that the recipient of the image can 'read' and use the image.

Note that some mobile units may not meet the requirements of SAP 32, 42 or 52 as shown in Table 7. In such case, the SAP level shall be entered as Level 20 (Legacy mugshot). This is used if a mugshot does not fully conform to the SAP level 32 requirements. This would be the case, for instance, if the output of the camera were in a TIFF format.

Note that while cropping is allowed on the original image prior to submission, the size and resolution requirements still apply to the cropped image.

For both JPEG and JPEG2K, care must be taken to account for automatic compression by camera hardware. Multiple compression stages can degrade the quality of photographic data.

Note that there are two fields relating to the date of capture of the image in record type-10. Although optional, it is considered best practice to enter the date and time of capture of the photo in Field 10.005 (Photo capture date / PHD). The mobile camera should automatically capture the date & time information. If, however, the exact date and/or time is not known then the approximate date and time shall be entered in this field, and Field 10.034 (Imagery capture date range estimate / ICDR) shall be entered into the record. This field records the amount of time (plus and minus) of which the PHD is the center point during which the image could have been originally collected.

The geographic location of the video capture should be entered into Field 10.998 (Geographic sample acquisition location / GEO).

When transmitting a still image, Field 10.996 (Hash / HAS) should also be entered. It has a value calculated using SHA-256 calculated upon the contents of Field 10.999 or the image stored at the location referenced by Field 10.994. This assists the receiving organization to verify that the data has not been altered during transmission.

Field 10.904 (Make / model / serial number / MMS) should also be completed with the relevant information about the camera, if at all possible.

If the still image is derived from a video, then Field 10.997 (Source representation / SOR) should be completed with the cross-reference index to the appropriate type-20 record in the transaction containing the original source video from which the still image was derived.

All still digital images transmitted in a type-10 record shall include the following:

- Field 10.002 (Information Designation Character / IDC) – usually automatically generated)
- Field 10.004 (Source agency / SRC)
- Field 10.005 (Photo capture date / PHD) – described above
- Field 10.006 (Horizontal line length / HLL)
- Field 10.007 (Vertical line length / VLL)
- Field 10.008 (Scale units / SLC)
- Field 10.009 (Transmitted horizontal pixel scale / THPS)
- Field 10.010 (Transmitted vertical pixel scale / TVPS)

- Field 10.011 (Compression algorithm / CGA)
- Field 10.012 (Color space / CSP)
- Field 10.999 (Body part image / DATA)

Fields 10.005 through 10.012 listed above are normally captured and derived from the data header of the still image from the camera and entered by the transmission data generation software. That software is normally also pre-programmed to include the value for Field 10.004. Thus, the requirement to know this data should not be a burden upon the operational agency.

8.2.2 Video

Video is becoming more ubiquitous in mobile operations. With the advent of lapel-cameras and mobile phone devices with video recording capability, this type of digital recording has become important to be able to transfer and analyze. It is best practice to have the position location (GPS) and time automatically recorded by the video unit.

There is no need for an ANSI/NIST-ITL format to be directly generated by the video device. Normally, video would be captured and later formatted into an ANSI/NIST-ITL transaction prior to relaying to another site. The remainder of this section describes the basic information that should be transmitted in an ANSI/NIST-ITL transaction.

Videos may be entered in type-20. This is particularly useful if they serve as sources for still images. Individual frames used for facial, tattoo or other body part images are then transmitted in a type-10 record.

Field 20.904 (Make / model / serial number / MMS) should be completed with the relevant information about the video camera, if at all possible.

Although most video units are digital, it is possible to use film video cameras. The storage location of videos from non-digital sources may be stated in Field 20.994 (External File Reference EFR).

Note that it is possible to have a type-20 record linked to another type-20 record – such as an extract of the video contained in one record, and the entire recording referenced in another (usually stored offline with a pointer to the storage location in the type-20 record). This relationship is indicated by an entry of “S” in Field 20.003 (SRN cardinality / CAR) for the original source type-20 record.

Video conveyed with a type-20 record may be stored in any format that is the output of the recording device. Digital output should not be transcoded into another digital format. Field 20.014 (Acquisition source / AQS) has three codes specific to mobile video:

8 = Video sequence from an analog video camera, stored in analog format
9 = Video sequence from an analog camera, stored in digital format
10 = Video sequence from a digital video camera

Note that there is a code for mobile telephone allowed in Field 20.014. However, it is denoted as an audio source, and not a source for video. Use of a mobile telephone with a video shall be indicated as Code 10.

For analog files, it is possible to keep the analog recording (such as on a tape) at a specified location. Reference to that location is made in Field 20.994 (External file reference / EFR). The data itself need not be contained in the transmission file. This is also true of digital files. For extremely large digital files, the preferred method is to have the data stored in a file that may be remotely accessed in a secure manner.

Field 20.015 (Source representation format / SFT) is required for video data. It specifies the digital format (such as AVI) or, for analog, it is specified as "ANALOG". The second information item allows the user to specify any special decoding information, if special keys are needed to access the data, etc.

If the analyst desires to mark relevant portions of the video recording that are of special interest, up to 99 such markings can be entered in Field 20.019 (Time index / TIX). The data elements of this field are the start and end times for each segment.

Note that there are two fields relating to the date of capture of the video in Record Type-20. Although optional, it is considered best practice to enter the date and time of capture of the video in Field 20.005 (Source representation date / SRD). This should be automatically captured by the mobile video camera. If, however, the exact date and/or time is not known then the approximate date and time shall be entered in this field, and Field 20.022 (Imagery capture date range estimate / ICDR) shall be entered into the record. This field records the amount of time (plus and minus) of which the SRD is the center point during which the video could have been originally collected.

The geographic location of the video capture should be entered into Field 20.998 (Geographic sample acquisition location / GEO).

When transmitting a video, Field 20.996 (Hash / HAS) should also be entered. It is calculated using SHA-256 on the video data in Field 20.999 or the video stored at the referenced location stated in Field 20.994. This assists the receiving organization to verify that the data has not been altered during transmission.

8.3 Face Photograph Capture Requirements

Annex E of the *ANSI/NIST-ITL standard* describes the requirements for facial capture. In that Annex, there are specific statements when a section is not applicable to mobile ID

(such as for Background and Lighting). The Annex refers to Subject Acquisition Profile (SAP) levels, which for mobile ID photographic devices are 32, 42 or 52.[30] Specifying the SAP level is a mandatory field for face images (Field 10.013), but is not specified for other body part images. Table 7 lists only those SAP levels that refer to mobile ID devices.

Only one face per image is allowed. Digital zoom (interpolation) shall not be used for facial images. The face should be in focus from the nose to the ears, which may result in the background being out of focus. Lighting should be evenly distributed over the face, if possible. It is recognized that this may be difficult to achieve in outdoor settings. The subject should be posed full frontal, preferably with a 'head and shoulders' composition or a 'head only' configuration. Head coverings, including hats and scarves should not be worn. The full face and ears should be displayed. Hair should be moved to reveal the subject's ears. The subject should have a neutral expression, with the mouth closed and eyes open.

Every effort should be made to capture the face image for enrollment without glasses. When possible, images taken for comparison to a database (probes) should also be taken without glasses. Note that this recommendation does not prohibit the wearing of glasses in facial images. Whether to allow any subjects to wear glasses is a policy decision dependent upon local needs, conditions, and legal restrictions. The wearing of eye patches is allowed only for medical reasons.

The Mobile ID face capture device must be able to measure the face image quality or to provide some means by which the device operator can assess the quality of the captured face image. The best practice recommendation is that an automated initial image quality assessment should be done to provide feedback to the operator during the capture process. Since there is no standard, recognized set of quality measures for facial photos, the mobile device should, at a minimum, allow the operator to review the image visually, and determine if a re-take is warranted. The operator should visually determine if the subject is in focus, has eyes open, is in a full-frontal pose with a neutral mouth expression, that there are no 'hot spots' on the face, and that the photo is consistent with a face-only or head-and shoulder image composition.

8.4 Face Photograph Transmission Requirements

There is no need for an *ANSI/NIST-ITL* format to be directly generated by the image capture device. Normally, the photographic image would be captured and later formatted into an *ANSI/NIST-ITL* transaction prior to relaying to another site. An ANSI/NIST-ITL packaging tool normally generates the information in this section.

[30] It is possible to transmit a still frame that contains a face, tattoo or other body part image from a video. However, such an image is not considered to be SAP level 32, 42 or 52. It is considered SAP 0.

Table 8 lists the fields in *ANSI/NIST-ITL* that are mandatory for some or all of the SAP levels associated with still imagery. Note that this applies ONLY to images that are characterized as IMT=FACE. For IMT=FACE, it is highly recommended that the pose be F (full face frontal). In such case, Field 10.021 (Pose Offset Angle / POA) is not entered.

Table 8

Required ANSI/NIST-ITL Type-10 fields for face images

Mnemonic	Condition Test	Field Number	Field Name
SAP	Mandatory with Field 10.003 (Image type / IMT) is FACE	10.013	Subject acquisition profile
POS	Mandatory with Field 10.003 (Image type) is FACE	10.020	Subject pose
POA	Mandatory if Field 10.20 has a value of 'A' (angled)	10.021	Pose offset angle
PAS	Mandatory if SAP 42 or 52 and IMT = FACE	10.023	Photo acquisition source
SXS	Mandatory if SAP 42 or 52 and IMT = FACE	10.026	Subject facial description
SEC	Mandatory if SAP 42 or 52 and IMT = FACE	10.027	Subject eye color
SHC	Mandatory if SAP 42 or 52 and IMT = FACE	10.028	Subject hair color

For facial images captured as SAP 42 or 52, Field 10.026 (Subject facial description / SXS) shall be entered. It is a mandatory field in *ANSI/NIST-ITL*. In reality, for mobile applications, a complete description would require an operator to stop and fully analyze each photograph or still image from a video. It is therefore recommended that this field be populated as 'UNKNOWN' for mobile applications.

The subject's eye color is mandatory for SAPs 42 and 52. Like the facial description, it may be impractical for the operator to write down or otherwise tabulate the eye color of subjects whose images he/she has captured in the field. It is therefore recommended that the mobile unit automatically populate the eye color code as 'XXX' for Unknown.

For facial images captured as SAP 42 or 52, the subject's hair color shall be entered. One or two attribute codes may be selected. It is impractical for operators in the field to record hair color for the subjects that they image. Therefore, it is recommended that the code 'XXX' for 'Unknown or unspecified' be automatically entered.

The possible values for Field 10.023 (Photo acquisition source / PAS) – which is mandatory for SAPs 42 and 52 – are listed in Table 9. If a video is captured and a frame extracted later from it to transmit, then TYPE20 is selected. ANALOG VIDEO and DIGITAL VIDEO are selected only if the original video is not included in a type-20 record. If a 'freeze frame' is captured at the time of recording, it is entered as a static photograph from a digital still-image camera. The codes 'DIGITAL CAMERA' and 'DIGITAL VIDEO' should be able to be added automatically into the field since the source of the data is known. This should require no manual intervention on the part of the operator.

Table 9

Acquisition source type code

Acquisition source type attribute	Attribute code
Unspecified or unknown	UNSPECIFIED
Static photograph from an unknown source	UNKNOWN PHOTO
Static photograph from a digital still-image camera	DIGITAL CAMERA
Static photograph from a scanner	SCANNER
Static video frame from an unknown source	UNKNOWN VIDEO
Single video frame from an analog video camera	ANALOG VIDEO
Single video frame from a digital video camera	DIGITAL VIDEO
Vendor specific source	VENDOR
Record **TYPE-20** original source representation	TYPE20
Another source image	OTHER

8.5 Scar / Mark / Tattoo (SMT) Image Capture Requirements

The image should only contain the SMT and the surrounding skin and should not contain anything else in the background, including patterned walls and floors, furniture, or other body parts. If elimination of the background is not possible, the background should be plain in order to prevent pattern distractions.

For purposes of the *ANSI/NIST-ITL standard* and this document, a tattoo is an indelible image that was applied to the skin. A common tattoo results from picking of the skin with a coloring material. A subclass of tattoo is *chemical,* which indicates that the pattern was created by the use of chemicals to burn the image into the skin. Another subclass of tattoo is *branded* which indicates that the pattern was caused by using a branding iron or other form of applied heat. A third subclass of tattoo is *cut* which indicates that the image was caused by incision of the skin.

Piercings, implants, birthmarks and scars caused by accidents / medical procedures, etc. are all classified as SCAR. A MARK only refers to patterns of needle marks on the skin.

SMTs can be captured from the front, side, or back of the subject, depending on the body location. SMTs on body limbs should be captured with the body part parallel to the torso. For example, a tattoo on a forearm should be photographed with the arm pointing towards the ground. A tattoo on a leg should be collected with the subject standing upright. Different tattoos on distinctively separate body locations should be collected as separate photos, except for full body tattoos that are connected across multiple body locations. The tattoo should be centered in the photograph and occupy at least 75% of the entire image. Thus, the 'standoff distance' from the tattoo may differ depending upon the size of the tattoo imaged.

Whenever possible, the SMT image should be taken under uniform lighting and be in focus with good contrast against the skin. For low contrast or faded tattoos, it may be desirable to photograph the tattoo with and without camera flash and select the better photo.

The mobile SMT capture device must be able to provide some means by which the device operator can assess the quality of the captured SMT image. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. Since there is no standard, recognized set of quality measures for SMT photos, the mobile device should, at a minimum, allow the operator to review the image visually, and determine if a re-take is warranted. The operator should visually determine if the SMT is in focus, has uniform illumination, shows good contrast, and that there are no background or clothing distractions in view.

The following paragraphs in *Annex E, Section 3 (Photographic requirements*) of the *ANSI/NIST-ITL standard* are applicable for SMT images:

- E 3.1 Depth of field
- E 3.2 Subject lighting
- E 3.3 Background and lighting
- E 3.4 Exposure calibration
- E 3.5 Exposure
- E 3.6 No saturation
- E 3.7 No unnatural color
- E 3.8 No color or grayscale enhancement
- E 3.9 Distortion and angle of view
- E 3.10 Allowed color space
- E 4.15 Medical conditions.

It may also be desirable to have an image of a large tattooed or scarred area, and an image of a smaller portion of the SMT (such as a detail of the tattoo that could be useful for determining gang affiliation). There is a field in the type-10 record (Field 10.039 Type-10 reference number / T10) that is used to link two or more images of the same SMT by using the same index reference for all of the associated images in a transaction. This is particularly true when a full 'sleeve' or the back is covered. Each significant portion should be imaged and described separately, along with an image of the entire area.

8.6 Scar / Mark / Tattoo (SMT) Image Transmission Requirements

There is no need for an *ANSI/NIST-ITL* format to be generated directly by the image capture device. Normally, the photographic image would be captured and later formatted into an *ANSI/NIST-ITL* transaction prior to relaying to another site. The user should be able to record the location on the body of the SMT.[31] For tattoos, there should be an option to record its color(s).

8.7 Forensic Dental Image Capture Requirements

There are no special requirements for forensic dental image capture other than the image being in focus and including sufficient detail to make the image useful for future analysis.

8.8 Forensic Dental Image Transmission Requirements

Mobile units are now used to record images for forensic use, including dental forensics. This BPR focuses upon standard, commercially available cameras and not specialized equipment (such as portable x-ray equipment).

There is no need for an *ANSI/NIST-ITL* format to be generated directly by the image capture device. Normally, the photographic image would be captured and later formatted into an *ANSI/NIST-ITL* transaction prior to relaying to another site.

The type-10 record shall indicate the type of forensic dental image as 'EXTRAORAL', 'INTRAORAL', 'LIP' or 'MISSING' in Field 10.003. MISSING is used when an image is taken to illustrate that a body part is not present that would normally expected to be present, such as a lower jaw.

For forensic dentistry applications, the subject is normally deceased. Field 10.046 (Image subject condition / SUB) shall be completed. For deceased individuals, a value

[31] An ANSI/NIST-ITL formatting generator should take the body part location recorded by the user and 'translate' it to the NCIC codes for the SMT body parts, which are listed at http://www.oregon.gov/OSP/CJIS/NCIC.shtml

of 'D' is entered into the **subject status code / SSC**. The **subject body status code / SBSC** shall have be 1 when there is an entire body and 2 when the image is of a body fragment. The third information item is **subject body class / SBCC**. Its possible values are:

- 1 = natural tissue
- 2 = decomposed
- 3 = skeletal

For lip images, Field 10.049 (Cheiloscopic image data / CID) should be completed. The lip print characterization is specified in this field. Note that lip pathologies and peculiarities may also be specified in this field, including codes for cleft lip, scars, herpetic lesions, tattoos and piercings.

Field 10.050 (Dental visual image data information / VID) shall be completed if an image type of 'EXTRAORAL' or 'INTRAORAL' is entered in Field 10.003. There is a table in the *ANSI/NIST-ITL* standard that lists the different view positions that may be encoded for the photos. Descriptive text may also be entered.

8.9 Photographic Image Capture for Other Body Parts

There are no special requirements for image capture of other body parts than the image being in focus and including sufficient detail to make the image useful for future analysis.

8.10 Photographic Image Transmission for Other Body Parts

Type-10 records may also be used to transmit images of body parts other than of the face or oral region. This is particularly useful for deceased individuals. In such cases, Field 10.046 (Image subject condition / SUB) shall be completed. For deceased individuals, a value of 'D' is entered into the **subject status code / SSC**. The **subject body status code / SBSC** shall have a value of 1 for when there is an entire body and 2 when the image is of a body fragment. The third information item is **subject body class / SBCC**. Its possible values are:

- 1 = natural tissue
- 2 = decomposed
- 3 = skeletal

The possible image types that are:

FRONTAL-C (clothed)	FRONTAL-N (nude)	TORSO-BACK	HANDS-PALM
REAR-C (clothed)	REAR-N (nude)	TORSO-FRONT	HANDS-BACK
GENITALS	BUTTOCKS	RIGHT LEG	LEFT LEG
RIGHT ARM	LEFT ARM	HEAD	CHEST

FEET

There are three other categories that may be used: CONDITION, MISSING, and OTHER. MISSING is used to image a section of the body where a part normally should be, such as when an arm has been ripped off of a person, and a picture is taken of the 'arm' area showing the damage. The list of NCIC codes that correspond to CONDITION are indicated in the ANSI/NIST-ITL standard in the description of Field 10.003. Examples are POCKMARKS, and HERMAPHR. The NCIC codes for OTHER are also listed in the description of Field 10.003. It covers such values as COLOST, BRACE and TRANSVST. The NCIC code that is associated with CONDITION, MISSING or OTHER should be entered in Field 10.040 (NCIC SMT code / SMT).

Images of patterned injuries are conveyed in type-10 records. Patterned injury images should include an ABFO #2 Reference scale in the image. The part of the body where the injury is located is indicated in Field 10.003, and may include FACE as well as the categories listed above. (Note SCAR, MARK, TATTOO, MISSING, OTHER and CONDITION shall not be entered for patterned injuries). A description of the patterned injury may be entered in Field 10.048 (Suspected patterned injury detail / PID).

8.11 Biometric 2D Photo Verification and Identification -- On Device

On-device comparison is most commonly used for one-to-one comparisons -- that is to verify the claimed identity of an individual. This may be useful for verification of the identity of the operator.

Comparing an image captured of a subject 'in the field' on a mobile device to a database of known individuals' images can be performed on the device for a relatively small gallery of pre-enrolled images. Such a capability could be useful for operations with a 'closed set' of subjects – such as those in a detention center or asylum camp.

On-device algorithms capabilities vary and should be carefully tested and adapted for the operational environment. There may be options to present the two or top five candidates, or a default to only the top ranked person.

To date, there have not been extensive evaluations of on-board facial recognition systems. Some such systems are entirely proprietary – making evaluation difficult.

8.12 Biometric 2D Photo Verification and Identification – Off Device

Some mobile systems are designed to relay an image to a central processing site, which then compares the photo to a gallery or galleries. The bandwidth required to send a photo is a factor, but that is becoming less of an issue with the introduction of better mobile telecom service. Some systems are designed to relay back a set of high matching photos (i.e., those above a certain score level) or a fixed number of candidates (such as 5). The operator can then compare the photo and associated information (sex, age, date of photo etc.) to make an evaluation as to whether an identity is likely to have been established for the subject. This capability can be of great use for officers who need to make a judgment as to whether to apprehend a person based upon an outstanding warrant, etc.

Off-unit verification systems should be carefully evaluated prior to purchase. NIST has run the Face Recognition Vendor Test (FRVT) several times. NIST has also conducted several other face recognition studies – including the Point and Shoot Face Recognition Challenge (PaSC). These studies can be accessed through the website www.nist.gov/itl/iad/ig/face.cfm.

9 Iris Images

Iris images are treated separately from other images, since they involve non-visible wavelengths and have markedly different data storage and transmission requirements. A normal camera, such as can be used for photographs described above, should not be used for iris capture.

9.1 Iris Capture Devices

While it may sometimes be possible to compare iris images taken solely in the visible light frequencies, darker irises normally require infra-red imaging to highlight the features of the iris that are used for comparison. Thus, a mobile ID unit used for iris capture shall be based upon near-infrared wavelength capture (approximately 700 to 900 nm). Some systems may use a portion of this range, which is acceptable.

Mobile ID iris image capture devices typically provide near-infrared lighting using LEDs to illuminate the iris. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1. The illumination wavelengths shall have ≥ 90% of

energy within the 700 nm to 900 nm band; and > 35 % of energy in the 800 nm to 900 nm band. [32]

Many contemporary iris imagers are capable of capturing both left and right iris images simultaneously or quasi-simultaneously (within a few milliseconds). Others capture only one iris at a time. For mobile applications, both images should be captured simultaneously or quasi-simultaneously, with the imager held in an upright position. This reduces the possibility of mislabeling of the individual images (right or left). It also allows for more accurate estimation of the roll angle and potentially higher accuracy and comparison speed.

In order to achieve acceptable time-to-capture and Failure to Acquire (FTA) rates, the iris image sampling frequency must be at least 5 frames per second. The iris image capture sensor shall use progressive scanning. The ability for an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time, expressed in milliseconds, reduces as Iris acquisition profile (IAP) levels increase, from a maximum of 33 ms at IAP 20 to a maximum of 10 ms at IAP 40, as shown in **Table 10**.

[32] These band wavelength specifications correspond to those of ISO/IEC 29794-6 and the 2015 Update of the ANSI/NIST-ITL standard.

Table 10

Iris Acquisition profiles (IAP)

Capture	IAP Levels					
	10	**11**	**12**	**20**	**30**	**40**
Iris diameter in true, non-upscaled pixels				≥ 140	≥ 170	≥ 210
Number of (quasi-) simultaneously captured eyes				≥ 1	≥ 1	2
Spatial sampling rate	10 pixels / mm. [33]	Up sampling allowed from 10 pixels / mm if algorithms require higher minimum iris diameter in pixels	Up sampling allowed from 10 pixels / mm if algorithms require higher minimum iris diameter in pixels			
Exposure time	≤ 33 ms	≤ 15 ms	≤ 10 ms	≤ 33 ms	≤ 15 ms	≤ 10 ms

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ratio of at least 36dB. Mobile iris image capture devices can be configured differently with regard to the operator interface, in terms of the viewfinder (being external or internal) and the manner of providing image quality feedback to the operator. These factors will influence the rate of successful captures. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

9.2 Iris Image Capture

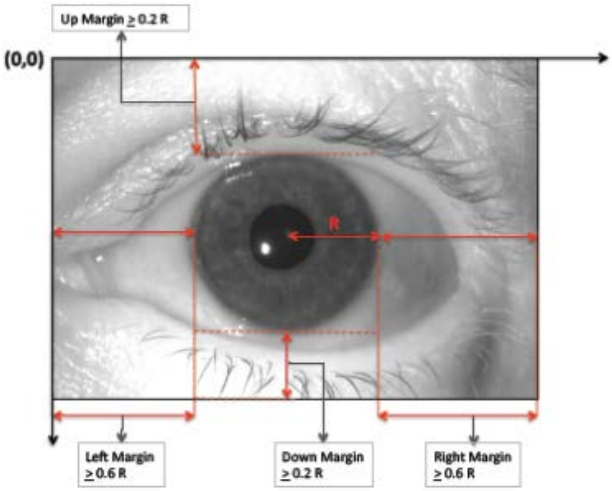
In order to be considered acceptable as non-intrusive and to avoid excessive geometric distortion, the minimum distance between the mobile iris capture device's lens and the subject's eye must be at least 100 millimeters. In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. The 2015 Update to the ANSI/NIST-ITL standard is consistent with ISO/IEC 19794-6 and ISO/IEC 29794-6 specifications concerning image

[33] Note that this corresponds to ISO/IEC 19794-6 specifications as well as the 2015 Update of the ANSI/NIST-ITL standard. ISO/IEC 29794-6 specified 15.7 pixels / mm. which is allowed with IAP levels 30 and 40.

margin requirements. The vertical margin shall be ≥ 0.2 times the radius of the iris. The horizontal margin shall be ≥ 0.6 times the iris radius. See Figure 7.

Figure 7

Image Margin Requirements



9.3 Iris Image Transmission

In order to support interoperability, the Mobile ID iris image capture device shall support ANSI/NIST-ITL Update: 2015 type-17 records when communicating with a central system. However, as indicated in Table 11 and Figure 8, alternate configurations are possible without having to fully encode an ANSI/NIST-ITL transaction at the mobile unit level.

For Mobile applications, it is often best to use the Image Storage Format (ISF) 7 format, since it dramatically reduces the storage requirements for the eye, as well as the data transmission load. For stationary systems, ISF 2 is the most common option deployed. Note that cropping and masking in ISF 7 does not affect the ability of the iris matching system to accurately perform.

Table 11

Iris Storage Formats (ISF)

ISF Code	Description	Iris Centering	Iris Margin Requirement (R is radius of the iris)	
			Horizontal	Vertical
1	Unconstrained image size	Recommended	≥ 0.6 R	≥ 0.2 R
2	Raw: 640 x 480	Recommended	≥ 0.6 R	≥ 0.2 R
3	Cropped	Required	= 0.6 R	= 0.2 R
7	Cropped and Masked	Required	= 0.6 R	= 0.2 R

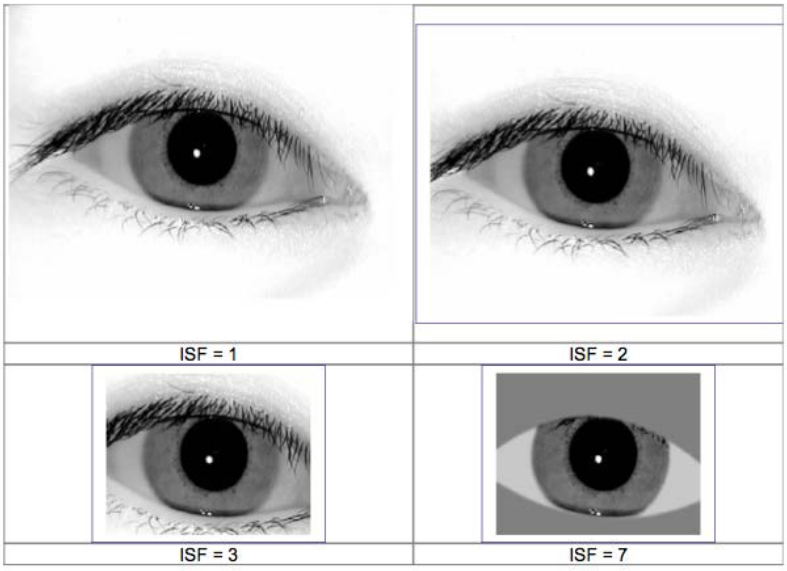


Figure 8

Examples of ISF image formats from the *ANSI/NIST-ITL standard*

10 Voice Signals

Voice signals are by their nature something that must be captured over a period of time. The voice signals may be used as input to multiple processes, once captured, such as:

- Speech processing (recognizing the words spoken)
- Language and dialect identification
- Speaker verification and identification (a biometric application)
- Counting the number of participants in a conversation

Voice sounds can carry speech and that speech usually occurs within a social context involving more than one speaker. The human voice – generally carrying both speech and non-speech sounds – propagates varying distances through air (principally) or another medium to reach acoustic transducers (usually microphones, when recorded) of varying amplitude and phase response. In mobile applications, even a single segment of a voice signal may not be linkable to a single geographic location or to a specific speaker. Unlike other modalities, voice signals may reflect and depend upon the social and behavioral conditions -- as well as the environmental condition of the collection environment, including the relationship between the data subject and any interlocutors.

10.1 Voice Signal Capture Devices

Many hand-held devices, such as phones, now also include the capability to take photographs and to record voices. The recordings may be in the form of video (also including a visual component) or as totally aural recordings. There are no specific requirements for audio capture devices. However, the operator's system should be identifiable – through make and model.

10.2 Voice Signal Capture

The date of the recording and its duration should be captured at the time of the recording. If possible, geographic location(s) should also be captured. The container format encapsulates the audio data of the electronic file used to carry the voice data in a digital recording. At the time of capture and initial storage, the container code shall be noted. Files having container formats incorporate audio specifications to properly decode the audio, such as number of channels, sampling rate, bit/byte depth, and whether the data is big/little endian. Table 12 lists the most common container formats. If the container format is not shown in the table, then code 2 is selected and entered in **container code / CONC** of Field 11.013 (Container / CONT). Field 11.051 (Comment / COM) shall be used to describe the container.

Table 12

Container Codes

Container type	Common file extension(s)	Container code
RAW audio type	undefined	0
Container type reference	various	1
Other	various	2
WAV (RIFF audio)	.wav	3
3GP and 3G2 mobile video	.3gp .3g2	4
AIFF	.aiff .aif	5
MP3 (MPEG-1, Layer 3 audioi)	.mp3	6
NIST Sphere	.sph	7
QuickTime (Apple VBR – audio/video/image) Note: allows pointers to external files and servers	.mov .gt	8
Video for Windows	.avi	9
Vorbis (OGG audio)	.ogg	10
Windows Media Type 1	.wmv .wma	11
Windows Media Type 2 Note: allows pointers to external files and servers	.asf .asx	12

*Any mention of commercial products within NIST web pages is for information only; it does not imply recommendation or endorsement by NIST

If the container allows different CODECs to be used, then Field 11.014 (CODEC / CDC) shall be completed with the code for the CODEC used to store the recording. The common CODECs are shown in Table 13.

Table 13

CODEC Codes

Codec type	Codec code
Linear PCM	0
Codec type reference	1
Other	2
Floating –point PCM	3
ITU-T G.711 (PCM) μ-law with forward order digital samples	4
ITU-T G.711 (PCM) μ-law with reverse order digital samples	5
ITU-T G.711 (PCM) A-law with forward order digital samples	6
ITU-T G.711 (PCM) A-law with reverse order digital samples	7

Note that the Container and the CODEC (if specified) should be captured directly by the voice recorder and should not require manual intervention on the part of the operator. It is recognized that mobile phones, 'pen recorders' and other devices may not convey such information with a voice recording. In such cases, 'Other' may be specified.

Although the standard allows for redaction (overwriting of a portion of the recording), discontinuities, specification of vocal content, and other characteristics of the voice sample, these should not be entered by the operator in the field. They are best entered by analysts reviewing the recording later.

10.3 Voice Signal Transmission

The type-11 record of *ANSI/NIST-ITL* shall be used to transmit an audio recording to a central repository. However, as illustrated in Figure 4, the full *ANSI/NIST-ITL* transmission file need not be generated at the mobile unit level.

11 Multiple Modalities in a Single Unit

A mobile ID unit may combine the capability to capture multiple different modalities, and several instances of each particular modality. This can greatly increase efficiency and improve the possibility of a later match (if an enrollment is being performed).

A major concern is that the entire sample set from one particular individual must be properly linked. This becomes problematic if the capture protocol is such that the process of collecting all modalities from a single individual is interspersed with data entries for other individuals. Simple typographical mistakes in entering a reference index (or name) could cause a lack of cross-linkage, or could cause items to be linked (falsely) together for different individuals. There is less chance of this happening when samples are collected simultaneously or quasi-simultaneously (such as a facial image taken at the same time as iris images).

The capture devices shall meet all of the characteristics for each of the modalities incorporated into them. The operation shall follow best practices for each of the individual modalities captured during a particular session. The unit should be capable of associating all of the individual samples captured from a single individual together (e.g. some common identifier for the fingerprint, the iris image, and the facial photo). This, however, may not be possible with certain mobile devices, such as certain smartphones.

12 Mobile ID Use Cases

The Department of Homeland Security, Office of Science and Technology held a series of workshops concerning mobile ID devices. One of their first tasks was to define use cases. They identified four general use cases:

Level 0: Credential dependent – no communications
Function: Verification
Level 1: On-board biometric storage / matching
Function: Enrollment, Identification, Verification
Level 2: Central server dependent biometric matching
Function: Enrollment, Identification, Verification
Level 3: Local server dependent communications
Function: Enrollment, Identification, Verification

The participants in the DHS workshops evaluated the following scenarios in order to develop the four generalized use cases described above. It is possible for a scenario to be at any of the above Use Case levels, depending upon the particular environment.

- Patrol Stop
- Border / Ports of Entry
- Public Events
- Access Control
- Disaster / Emergency Management
- Maritime
- Post-mortem identification
- Checkpoint operations
- Detention / Asylum Facility Operations
- County / local jail booking, transfer & release
- Latent friction ridge print image capture and search from the field

13 Risk Profiles

'Risk' here refers to the possible implications of having a false match or a false non-match. The implications of such 'errors' can vary substantially. For purposes of this document, they are divided into three levels: Severe, Moderate and Mild. Use cases defined by risk are shown in the following Table.

Table 14

Use cases for risks and functions

Risk to Public Safety/Function	Use Case Example	Recommended Capture
Severe / Enrollment	Field enrollment of biometric data from an individual that is associated with an attempted terrorism incident.	Face = Frontal [34] Iris = L&R eyes Finger = All
Severe/ Identification	One-to-many search against a database to identify a subject where there is a high risk of loss of life or assets. Some situations may require a multi-modal biometric identification.	Face = Frontal [34] Iris = L&R eyes Finger = 4+
Severe/ Verification	1:1 match against a credential or database to verify identity where there is a high risk of loss of life or assets. Some situations may require multi-modal biometric verification.	Face = Frontal [34] Iris = Either eye Finger = 2+
Moderate/ Enrollment	Mobile booking: Field citations and release when the violation is not high enough to ensure incarceration until arraignment without bail.	Face = Frontal Iris = L&R eyes Finger = 6+
Moderate/ Identification	In field mobile identification of a subject with questionable or no identification.	Face = Frontal Iris = Either eye Finger = 4+
Moderate/ Verification	Personal Identity Verification (PIV) Release from custody.	Iris = Either eye Finger = 2+
Mild/ Enrollment	The intention is for the biometric enrollment to be of sufficient quality that it shall allow later verification (e.g. e-citations).	Face = Frontal Iris = L&R eye Finger = 4+
Mild /Identification	Rapid identification in custody prior to formal booking. (Typically done at the jail intake).	Iris = Either eye Finger = 2+
Mild/ Verification (Finger images).	Court Appearance/Parole/Workhouse, Personal Identity Verification (PIV).	Iris = Either eye Finger = 1+
Mild/ Verification (Finger minutiae).	Personal Identity Verification (PIV) (using minutiae).	Finger = 2+ Not recommended for use between AFIS.

[34] For face enrollments, verifications and identification in a severe risk environment, attempts should be made to control, background expression and lighting where it is practical to do so.

13.1 Severe Risk

Severe risk levels imply that loss of life and/or property can result if accurate identification or verification is not made. In severe risk environments, it is plausible that inconvenience to the subject being identified or verified is secondary to the security of the situation, meaning subjects may be detained longer until the identification or verification process is completed. This assumption means that matching thresholds can be set lower (more aggressively) resulting in a returned list of potential candidates that an examiner may review to determine if a true match has occurred.

For instance, with friction ridge prints, it may be deemed prudent to have a forensics examiner review the images. A forensics fingerprint examiner can use level 3 fingerprint information including inter-ridge detail and pore structure to effect identifications. On the other hand, machine matching is typically constrained to level 2 minutiae details and ridge spacing. For this reason, fingerprint sensors for enrollment and identification in a severe environment must meet EBTS Appendix F[35] requirements. In addition, each print that can be compared adds information that can be used by the examiner making full ten-print comparisons desirable.

Examples of enrollment and identification functions in a high-risk environment include background checks conducted to grant access to secure facilities during battlefield operations. In this case, enrollment fingerprints would be compared against the latent image database maintained by the Department of Defense (DoD).

The verification function typically compares a processed captured biometric image against previously captured templates. Thus, even for verification functions performed in a severe risk environment, sensors meeting PIV image quality specifications provide the maximum data that will be used for matching. Increased confidence for verification functions can be met using multi-instance (e.g. 2 or more fingers) or multi-modal biometric verification.

13.2 Moderate Risk

A moderate risk environment is defined for those encounters with a subject with no or questionable identification. An officer cannot detain a subject for more than a limited amount of time without making an arrest. In this situation, it is necessary to quickly identify the subject or retain biometric information sufficient to verify the subject's identity at a later date.

For instance, in scenarios relying upon fingerprint matching, PIV image quality enables machine matching of images. Once the subject is in the court system, any images retained using mobile enrollment would typically be replaced by images captured using a ten-print

[35] Appendix F of the FBI's EBTS us available through the website https://www.fbibiospecs.cjis.gov

system. Once again, the capture of more images provides more information for later booking. In addition, the capture of two or more fingerprints simultaneously provides additional information on the fingerprint sequence.

13.3 Mild Risk

A mild risk environment is defined for those encounters where enrollment and identification data will be used at a later date. At that time, the subject would be available for comparison to the data previously retained. The results of an identification or verification should not impact anyone but the subject in question. Examples of normal enrollments include preparing for future logical or physical access control for a subject, or retaining one or more biometric images for verification in court while the subject is available. Verification examples include tracking a subject through the jail or court system using the retained biometric images. In these cases, a failure to match would result in additional action to verify the subject's identity, primarily inconveniencing no one but the subject.

14 Mobile Device Security & Encryption

The establishment and enforcement of Information Technology (IT) and agency security policies is not the focus of this document. Law enforcement and criminal justice agencies are increasingly realizing the productivity benefits of mobile handheld devices. Mobile ID devices represent a tremendous productivity advantage for criminal justice and ID management.

While this mobile technology and the capabilities it brings, from biometric identification to citations and report writing, will be a great advantage to criminal justice personnel, it is creating a tremendous security management challenge. The small size, large storage capacity and network connectivity of these devices make unprotected mobile devices susceptible to loss, theft and misuse, and possibly a target for someone wanting unauthorized access to information or databases. Mission sensitive and confidential information is now available through Mobile ID devices at locations and under circumstances that are outside the normal security parameters. As a result, unsecured devices can pose a risk to any criminal justice network that the device can access. In order to adequately secure the device from misuse or attack and to meet regulatory standards and requirements, agencies must develop wireless and centralized device security policies. These policies should include measures regarding authentication, data expungement, encryption, application launch controls and device feature disablement.

In order to maintain the highest level of device security, an updating of all devices is needed whenever policies change or software is updated to provide greater protections.

14.1 Authentication and Authorization

The mobile handheld device should provide the capability for an operator to authenticate his/her identity as well as establishing authorization levels for that person based on a two-factor authentication, one of which should be a biometric.

The mobile handheld device should provide biometric operator authentication and a password of minimum length with alphabetical/numeric/special characters. For certain Government operations, a PIV card may be able to provide operator authentication, if the operator has been issued one.

The mobile handheld device should provide the capability for operator re-authentication and the device should re-authenticate itself after a designated amount of idle time or result in a device shut-off. The mobile handheld device should provide the capability to lock the device or render the device inoperable, erase selective files, and/or erase all files on the device based on failed security protocols. The mobile handheld device should provide the capability to establish a maximum limit of failed authentication attempts before the handheld clears all application data or requires unlock only by an IT administrator.

14.2 Device and Data Authentication

Once operator authentication and authorization is established, the mobile handheld device should be able to provide device authentication that it is authorized to communicate on the network. There should also be the capability to have the device's identification verified against a registered list of specified devices (black list, lost/stolen). A device with a matching identification to one on the list should not be authorized to communicate with the central system. The device should have a remote data 'wiping' capability in the event that it is misplaced or stolen.

15 Communication Protocols

There are several different approaches for establishing communication between Mobile ID devices and systems. As an example, Figures 9 and 10 illustrate different configurations using the *Web Services –Biometric Devices* protocol.

Figure 9

A physically separated WS-Biometric Devices (WS-BD) implementation.

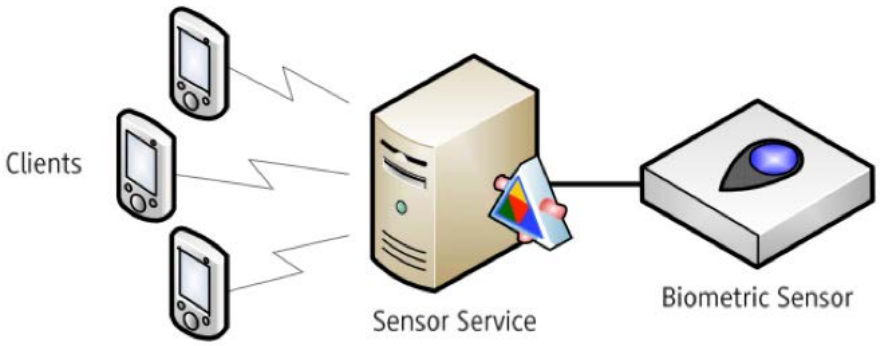
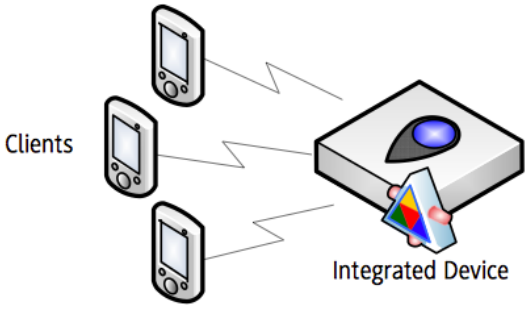


Figure 10

A physically integrated WS-Biometric Devices (WS-BD) implementation



The type of communications selected will vary upon the needs of the mobile ID user. Some scenarios, such as maritime interdiction, may require satellite communications

while others can use the commercially available mobile phone network. The communications between components can be of many different types, such as Bluetooth.

16 Environmental Profiles

A Mobile ID device can be used in a variety of different contexts, such as a court of law, an airport terminal, by a patrol officer on the street or in a patrol car, or even in a military environment such as a checkpoint or for access control to a military base.

These different contexts each require different levels of resistance to environmental factors such as temperature, humidity, dust, water, vibration, etc. For these reasons, three different profiles are described below (Indoor, Law Enforcement and Military), with increasing levels of resistance to the relevant environmental conditions.

It is the responsibility of the agency to decide, in the procurement phase of the Mobile ID devices, which profile to request in the Request for Proposal (RFP). The desired profile will depend on the expected usage of the devices and the location(s) where they will be required to operate. It is important to choose the right profile, since a lower profile could mean that the devices are not able to withstand the operating environment, causing costly failures and decreasing service levels. Conversely, choosing too high a profile is likely to cause an unnecessary increase in the size, weight and cost of the devices.

16.1 Indoor Profile

If a Mobile ID device is going to be used only in an environment such as an office building, a court of law, etc. the suggested environmental specifications for the device can be assumed to be similar to those of most commercially available computing devices intended for office use. For these use cases, the recommended minimum environmental specifications are listed in Table 15.

Table 15

Indoor Profile Recommendations

Operating temperatures	From 32°F to 104°F (0°C to 40°C)
Storage temperatures	From 14°F to 122°F (-10°C to 50°C)
Relative humidity	0% - 85% Non-condensing
Ingress Protection Rating (IP Code)	IP 40 or higher

For more information about the level of ingress protection (IP) refer to the IEC standard 60529 *"Degrees of protection provided by enclosures" available at* *http://webstore.ansi.org*.

16.2 Outdoor – Heavy Use (Law Enforcement – like) Profile

This profile should be used when the Mobile ID devices are going to be used by a patrol officer on the street or on-board a patrol car, for example. These use cases require the devices to be able to withstand high or low operating temperatures, dust, rain, water splashes, the vibrations typically encountered in a vehicle and dropped from a limited height. For these use cases, the recommended minimum environmental specifications are listed in Table .

Table 16

Law Enforcement Profile Recommendations

Operating temperatures	From 14°F to 122°F (-10°C to 50°C)
Storage temperatures	From -4°F to 140° F (-20°C to 60°C)
Relative humidity	10% - 90% non condensing
Ingress Protection Rating (IP Code)	IP 54 or higher, in operational configuration, with any existing expansion port closed
Drop resistance	Resistance to multiple drops on concrete from a height of 3 feet (91 cm).

16.3 Outdoor – Rugged Use (Military – like) Profile

This profile should be used when the Mobile ID devices are going to be used in harsh operating environments, when the expected use cases require the devices to provide increased level of protection against high and low temperatures, dust and sand, rain, water splashes, vibrations and drop. The Department of Defense has issued a document that should be followed for testing to this profile. It is "*Department of Defense Test Method Standard: Environmental Engineering Considerations and Laboratory Tests, Mil-Std-810G"* which is *dated* 1 January 2010. The document is available at http://www.atec.army.mil/publications/Mil-Std-810G/Mil-Std-810G.pdf. Particular attention should be paid to the tests for operating temperatures, storage temperatures, drop resistance, vibration resistance, and relative humidity tests. The ingress protection (IP) should be code IP 65 or higher, with any existing expansion port closed.

Annex A Revision History

Revision Number	Comment
2.0	Initial version.
2.1	Reverted IAP 20, 30, and 40 to original conditions, added IAP 10, 11, 12. Made minor modification to guidance on the wearing of glasses during face image captures and SMT image capture requirements.