DRAFT – Mobile ID Strawman

Table of Contents

1 Introduction

The term "Mobile ID" can conjure up several different interpretations. In the strictest sense, it may require an untethered device used to capture one or more biometric samples from a subject. The captured data sample(s) may then be compared to other samples contained in a database resident on that device. Data may also be transmitted to a central repository or to an onboard computer in a nearby vehicle (that includes jurisdictional police cars, border patrol vehicles, military combat vehicles such as HUMVEES, etc.) containing a database. This scenario allows for comparison to larger databases than otherwise available on a handheld device or an onboard computer in the police car. Alternately, that same or similar portable device physically attached to a computer located in police car, while biometric samples are being acquired may also be considered as a Mobile ID device. For purposes of this report, the exact definition or categorization of the Mobile ID device is not a factor. The Mobile ID device should be viewed in the context of a portable biometric acquisition station – one that is not intended to be stationary and hardwired to a much larger system used for comparing or matching biometric samples. This is in contrast to traditional booking stations and other biometric enrollment stations incorporating physically secured full-sized live-scan fingerprint readers, other biometric modality capture devices, or photo capture stations with setups adhering to distance, lighting, and other photo capture standards.

Over the past several years Mobile ID devices and systems have been employed for various applications. In the law enforcement environment these devices enables an officer to acquire a subject's fingerprints, facial image or other biometric from a variety of different physical locations. In the DoD world they are used, by the thousands, for identity verification of foreign workers, access control to secured communities and bases, and for ad-hoc checkpoint operations. Once acquired, comparison with other biometric samples on watch lists and databases can be made. This can all be done at close to real time on the streets or at a remote location without the need of transporting the subject to a central office - with much less inconvenience to those involved with zero transit time other than for subjects identified as persons of interest to be retained for further processing. The civilian verification scenario (e.g., use of the PIV Card) may be considered as a third broad category of applications. The subject is motivated to be verified in order to obtain access to a service, facility, or computer. If a match is not found, an access or privileges may otherwise be denied. This environment differs from law enforcement or DoD due to the motivated nature of the subject.

Currently, manufacturers are producing devices used to acquire fingerprint, faces, and irises but additional biometrics, such as voice, are currently being added to specific applications (such as DoD systems) or being planned for the future. Unfortunately, data acquired from a device using one system cannot always be read or processed by another system. In the case of fingerprints, this may be the result of different scanning

resolutions, use of image versus template, differing image sizes, or different fingers. Such a variety of options can result in a general lack of interoperability between systems.

Agencies want to search neighboring systems without regard to existing dissimilarities between vendor systems. The FBI is piloting a new rapid search system based on the Repository for Individuals of Special Concern (RISC) that provides access to current national wants, warrants, known and suspected terrorist and other individuals of interest. Additionally, the defense community wants the warfighter to be able to search DoD, FBI, and DHS repositories. In order to satisfy these goals common interoperability requirements must exist at the local, state, and federal levels. However, these interoperability reqirements do not apply to mobile biometric capture devices.

To accommodate these needs, the FBI's Advisory Policy Board (APB) recently approved a request to develop standards for Mobile ID systems. However, there are already a number of installed systems that are providing good value and cannot summarily be ruled obsolete. But as the technology is continually redefining what is possible, a roadmap forward can be designed and developed to progressively "raise the bar" to improve interoperability, biometric quality, and accuracy. As the Mobile ID devices improve and current systems need to be replaced, replacement systems can be procured to adhere to higher performance standards. Such an approach will accommodate the largest possible group of current systems and provides good future options as technology evolves.

Rather than creating a single standard to accomplish this, the strategy will be to develop a series of profiles or set of best practices for each biometric modality. These profiles will rely on the FBI's EBTS and the ANSI/NIST-ITL 1-2007 or INCITS standards that specify records with field requirements based on existing systems. The DoD systems will have to be compatible with the FBI EBTS to the level appropriate as not all DoD biometric encounters are intended to be searched broadly, such as check point encounters that are only run against locally stored / networked watch lists. Defining these profiles will make it possible to accommodate most existing systems while providing richer opportunities for the next upgrade. This standard does not directly specify the capabilities or performance of the local or central database or repository. Those requirements are driven by the particular problem being solved.

Comment [RMM1]: Currently, the title does not include "Standard". What is the intended name of the standard? It seems to cover more than capture, transmission, or any other relatively narrow standard-type that we are all familiar with. PTH1

2 Scope

This specification is primarily targeted at law enforcement, criminal justice, military, and other applications where a high degree of accuracy and reliability is required for enrollment, identification, and verification. These applications typically have subjects that are not willing or able to provide trusted identity information. The resulting biometric identification needs to provide a reasonable degree of certainty that will stand up to scrutiny including court challenges and audits of security access control systems.

This specification defines a series of Biometric Acquisition Profiles (BAP) used to describe sets of best practices requirements intended to improve the capture, interoperability, data quality, and accuracy of biometric data obtained from Mobile ID capture devices. These profiles must also be examined in light of their intended functional use for enrollment, verification or identification.

Each BAP shall identify progressively more stringent sets of parameters and requirements relevant to that device. These sets are identified by numerical levels in this document. Lower BAP numbers indicate currently available and operational systems. Higher values indicate stricter requirements currently available in "higher-end" or future systems. As the BAP numbers increase, so do the capabilities of the device.

The BAP levels must also be examined in relationship to the intended function being considered. The enrollment process shall always require a more stringent set of requirements. Verification may not require the same stringent set of parameters used for enrollment.[1]

Functional biometric devices addressed by this specification shall be limited to those capable of capturing one or more modalities of fingerprint, facial, or iris image data.

3 Purpose

This specification contains guidelines for the capture, use, security, and transmission of mobile identification data that can be interoperable with similar and dissimilar systems. Use of the BAP levels provides analysts with a tool for specifying the capabilities of a Mobile ID device tailored to the individual functions required. A Mobile ID device application may call for the same BAP level for all functions. Or it may require a more stringent level for the enrollment with a relaxed BAP level for verification. Choice of the levels will depend of the overall system application. Any collection device rated at the same or higher BAP level would be appropriate for a given user functional profile.

[1] Tactical uses by the DoD and others might be in operationally challenging situations where full capture of all biometric samples defined in a BAP level are not always possible – this does not go against the spirit of the recommended BAP

This specification defines parameters addressing the content, format, and units of measurement for the exchange of biometric sample information for each combination of biometric capture device, function, and BAP level. Information consists of a variety of mandatory and optional information items including fingerprint scanning resolution, pixel distances between facial features, and compression algorithm information for each biometric modality.

Information compiled and formatted in accordance with this specification and the EBTS 8.002 implementation of the ANSI/NIST-ITL 1-2007 standard can be transmitted and seamlessly exchanged with the FBI and other compliant organizations without regard to any peculiarities of the capture device.[2] Information can be gathered directly from a fingerprint scanner, facial image camera, or iris camera. This document is intended to assist law enforcement, criminal justice agencies, DoD, and other organizations that process biometric data to exchange fingerprint, facial, and iris data captured on a Mobile ID device.

4 Applicability

Mobile ID devices have been employed for a variety of applications where a stationary booking station type environment is not possible or easily attainable. Common applications include the officer on the street or the soldier on a checkpoint who needs to perform a quick check against one or more biometric watchlist databases. This may be part of the issuance of a citation, registration of the biometric with the incident, and the subsequent need to verify identity at court appearances. Or it may be part of a security operation. Prisoner transport and release tracking, immigration and border control, job applications, and entitlement programs are additional applications taking advantage of Mobile ID technology. This technology is also being used by the Department of Defense to monitor activities / determine any interaction with known or suspected terrorists (known as KSTs).

These applications and others are being accomplished with on-the-spot acquisitions of fingerprints and/or a "mugshot" for comparison with samples stored in key databases. Although iris comparison has not been identified as a current capability, this technology is under consideration at some agencies. The BAP levels required for each device must be tailored to the application it is being used for and also evaluated in terms of enrollment, verification and identification requirements. The more critical the application is in terms of acceptable performance errors, the more restrictive the BAP needs to be.

[2] In the DoD domain the exchanges will typically be exchanged with the FBI through a single point of interface, the Biometric Fusion Center (BFC) in Clarksburg, WV

5 Mobile ID Fingerprint Devices

5.1 Overview

The capture of a high quality fingerprint enrollment images is critical. It is the sample against which other captured verification or identification samples will be compared. Unacceptable matcher performance due to poor quality enrollment images stored in the database cannot be fixed short of acquiring a new enrollment image. Table 1 lists the sets of minimum requirements by BAP level for fingerprint capture devices. The table is divided into Capture, Transmission, and Function. Under the function category, entries for NFIQ and finger information repeat for the enroll, verify, and identify. The enrollment function should be concerned with acquiring a very high quality image. For that reason, a level 5 capture using M1 378 format should not be used for enrollment purposes. Once a very high quality enrollment image has been acquired and stored, verification and identification comparison images may be of slightly lower image quality. It is up to the system designer of each particular application to determine the appropriate BAP levels for each of the enrollment, verification, or identification functions especially if there is an intention to exchange data with other systems.

5.2 Fingerprint Capture Requirements

5.2.1 Minimum Image Size

5.2.2 Compression Algorithm

5.2.3 Compression Ratio

5.2.4 Number of Fingers for Enrollment, Verification, Identification

5.2.5 Finger Numbers by Function

5.2.6 Packet Format

5.2.7 ……

BAP	5	10	20	30	40	50	60
CAPTURE							
Acquire Flat Images	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Acquire Rolled Imgs		No	No	No	Optional	Optional	Optional
Resolution	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi	500 ppi +/- 5 ppi
Min Graylevels	256	256	256	256	256	256	256
Min Image Size	.5" x .65"	.5" x .65"	.8"x.8"	.8"x1.0"	1.6"x1.5"	2.5"x1.5"	3"x3.2"
Min Image Area	.325 in^2	.325 in^2	.64 in^2	.8 in^2	2.4 in^2	3.75 in^2	9.6 in^2
Compression Algorithm	N/A	WSQ	WSQ	WSQ	WSQ	WSQ	WSQ
Compression Ratio	N/A	15:1	15:1	15:1	15:1	15:1	15:1
Max # fing/img	1	1	1	1	2	3	4
Sensor Certification	PIV	PIV	PIV	PIV	App. F	App. F.	App. F
Minutiae Extractor Certification	PIV	N/A	N/A	N/A	N/A	N/A	N/A
TRANSMISSION							
Image / Template	Minutiae	Image	Image	Image	Image	Image	Image
Standard Used	M1-378	M1-381 ANSI/NIST	M1-381 ANSI/NIST	M1-381 ANSI/NIST	ANSI/ NIST	ANSI/ NIST	ANSI/ NIST
Packet Format	?	?	?	?	?	?	?
FUNCTION							
Application Profile		EBTS	EBTS	EBTS	EBTS	EBTS	EBTS
NFIQ (Enroll)	Required Any Score	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.
Min # Fingers (Enroll)	2	2	2	2	4	6	8
Finger Number (Enroll)	2, 7	2, 7	2, 7	2, 7	1/6 & 2/7	2-4 & 7-9	2-5 & 7-10
NFIQ (Verify)	Required Any Score	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.
Min # Fingers (Verify)	2	2	2	2	4	6	8
Finger Number (Verify)	2, 7	2, 7	2, 7	2, 7	1/6 & 2/7	2-4 & 7-9	2-5 & 7-10
NFIQ (Identify)	Required Any Score	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.
Min # Fingers (Identify)	2	2	2	2	4	6	8
Finger Number (Identify)	2, 7	2, 7	2, 7	2, 7	1/6 & 2/7	2-4 & 7-9	2-5 & 7-10

Comment [RMM2]: The Table has 7 BAPs – and now within each we have a row called "Application Profile" – does not seem right. Can we clarify the dual use of Application Profile in this table? PTH3

Table 1 - Fingerprint Parameters

Table Notes:

1) Should there be another level for minimum of 1000 ppi?
   Yes, but would we need a 1k ppi equivalent for levels 30-60? (J. Olson)
   No or add 1000 to the ppi fields the rest is the same (TJ Smith)
2) For Transmission standard should the ANSI/NIST be an alternate for the levels 5-30?
   ANSI NSIT includes Part 1 and Part 2 (XML) (J. Olson)
   YES (TJ Smith)
3) What should be entered into the Packet format.?
   It seems like transmission standard covers this. (J. Olson)
   Clarify (JT Smith)
4) For level 5 minimum number fingers changed to 2 from NA.
5) Entries for NFIQ, and finger information for the enroll, verify, & identify functions need to be discussed and reexamined
6) Are there any other items needed for the table?
   What Type 2 {fields} must be sent? (J. Olson)

5.3 Other Considerations

Aside from the requirements listed above for the fingerprint capture device, other factors that effect 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 the temperature and humidity specifications
- Ruggedness of the device
- Officer safety while using
- Use of clean fingers when possible
- Maintain clean platens
- Types of cleaners allowed on platen
- Consistent placement of the same finger(s)
- Consistent centering and use the same area from the flat of the finger
- Optical scanners should avoid excess illumination (or use capture devices that can function effectively in full sunlight)
- If enrolling more than 1 finger, ensure that sequence errors do not occur.
- If enrolling more than 1 finger always reflect accurately which finger is being captured
- On single finger capture devices, sequence errors need to be avoided (especially for enrollments) Programming should aid the operator to prevent these errors.
- Quality feedback to operator
- How quickly can prints be captured

- How many transactions can be in process simultaneously (can a new set of fingerpints be captured while waiting for search results?)

6 Facial Image Capture Devices

6.1 Overview

Mobile Identification devices provide facial capture using photographs for two purposes:

- Linking the return information to the correct subject.
- Mobile Identification.

Low resolution cameras with fixed focal length provide sufficient data for linking the return information to the subject.

Mobile Identification using facial recognition requires higher end camera features.

Table 2 lists the sets of minimum requirements for BAP level 50 for facial image capture devices. The table is divided into Capture and interchange. It is up to the system designer of each particular application to determine the appropriate additional BAP levels for each of the enrollment, verification, or identification functions especially if there is an intention to exchange data with other systems.

Comment [RMM3]: Should not all modalities have entries for all 7 BAP levels for fingerprint? Then a single (or 2 or 3) BAP can be developed for say, TWIC Mobile Devices. PTH4

6.2 Camera Focal length

Cameras using facial recognition for Mobile Identification need a focal length that operates with 2-6 feet of separation. Self-images of the operator require images taken at approximately two feet from the operator. Separation between the operator and the subject is typically 3-6 feet.

At this distance the camera needs to capture ear-to-ear photographs that meet the facial recognition requirements specified by this document.

6.3 Camera Controls

Camera controls enable the camera, with assistance from the operator or automatically (if set on auto contrast), to capture quality pictures in bright sunlight, overcast light, indoors, or using additional lighting at night.

6.4 Camera Frame Rate

Image display of 15 frames per second is approximately real time for viewing. Facial recognition frame rates are typically 5-10 frames per second.

6.5 Photo Image Format

Images are captured in 24-bit RGB or 8-bit monochrome in compressed format compatible with NIST Best Practices. For facial recognition eight bit gray scale images can be used.

Levels		**50**	**Comments:**
CAPTURE			
Sensor Resolution		>=400x533	Lower resolution may reduce accuracy
Capture Device Sensor		Progressive scan (no interlace), Chip mounted in Portrait format	
Capture Device Color Space		24-bit RGB color space or 8-bit monochrome color space	
Sensor Lens		High Speed/low f-stop, focal length of 40-135mm (35mm format)	
Capture Device Controls		Auto gain & shutter, optional: control loop for camera parameter (Shutter speed/flash intensity) based on face area on-board (requires continuous face detection	
Capture Distance in mm		600-2000, longer distance is preferred	Lower distance may reduce accuracy
Illuminator Type		Xenon flash or LED / fill in flash	
Wavelength Range		Visible light, 380-780nm	
Exposure Time		<= 1/100s (10 ms)	Capability to freeze motion
Inter-Eye Distance		>=90 pixels (better 120)	Lower resolution may reduce accuracy
Frame Rate		12 fps	For positioning (live view)
INTERCHANGE			
format		ISO 19794-5 or jpeg >85% quality, jpg2000, or raw (PNG etc.)	

Comment [RMM4]: Please clarify. PTH5

Table 2 - Facial Image Parameters

6.6 Camera Image Size and Aspect Ratio

Image sizes are either 640 (vertical) by 480 (horizontal) or 320 (vertical) by 240 (horizontal) pixels. Facial images will be saved per NIST mug shot best practices.

6.7 Camera Sensitivity

Cameras with sensitivity to 1.5 lux provide images sufficient for associating returns in marginal lighting conditions. These images are not satisfactory for facial recognition.

Comment [RMM5]: Can we recommend the minimum number of lumens per square meter for facial recognition? PTH6

6.8 Facial Image Compression

7 Iris Image Capture Devices

7.1 Overview

Iris capture devices have features similar to facial capture but with significant differences. Table 3 lists the sets of minimum requirements for BAP level 30 & 80 for iris image capture devices. The table is divided into Capture and Matching. It is up to the system designer of each particular application to determine the appropriate additional BAP levels for each of the enrollment, verification, or identification functions especially if there is an intention to exchange data with other systems.

Comment [RMM6]: We go to 80 here and only 6 for fingerprints. Can we align these? PTH7

7.2 *Camera Features and Image Formats*

Cameras using iris scan for Mobile Identification require a focal length sufficient to meet the iris scan requirements specified in this document. Camera controls enable the camera to capture iris images either with auto-capture or manual interaction by the operator. User interfaces typically include image quality feedback to the operator. Iris template formats are specified in other sections of this document.

7.3 *On Board Illumination*

Mobile Identification devices using iris scan typically provide infrared lighting using LEDs to illuminate the iris. The illumination is not in a range visible to the eye.

IRIS

LEVELS -->	30	80	
			comments
Capture			
mechanical/optical/electronic(display) alignment aid	any	at least electronic	
number of (quasi-)simultaneously eyes captured	≥ 1	2	
capture distance in mm	≥100	≥200	
capture volume per eye, min. width/height/depth in mm	80 / 60 / 50	80 / 60 / 50	
wavelength range	700-900 nm	700-900 nm	
spectral spread/bandwidth	≥ 80nm	≥ 100nm	
irradiance	≥ 20 W/m²	≥ 40 W/m²	affects ability to supersede ambient light
exposure time	≤ 33 ms	≤ 10 ms	affects capability to freeze motion
iris diameter in pxls	≥160 pxl	≥200 pxl	determines false reject rate
frame rate	≥5 frames/s	≥10 frames/s	affects time to capture and FTA
average irradiance	< ?	< ?	relevant for eye safety
sensor signal-to-noise ratio	≥ 36dB	≥ 36dB	
Interchange			
pixel depth	monochrome, ≥ 8 bits/pxl	monochrome, ≥ 8 bits/pxl	
format, iris	raw/ISO 19794-6-rect	raw/ISO19794-6-rect	
iris-specific peak signal-to-noise ratio due to JPEG/JPEG2k	≥ 36dB	≥ 36dB	
Matching			
on board, number of templates, speed	optional	optional	

Comment [RMM7]: There are national and international safety standards that we have to reference. PTH8

Table 3 - Iris Parameters

8 FBI EBTS Transactions and Replies

Mobile ID devices are one source of fingerprint search transactions to the FBI. Such transactions must be formulated to be compliant with the ANSI/NIST-ITL 1-2007 requirements regarding format encoding and the FBI's EBTS 8.0 transmission specification addressing transaction submission. All search requests must be routed through the contributor's State ID Bureau (SIB) or other authorized agency. Due to internal FBI security policy, search requests must currently be submitted over the CJIS Wide Area Network (WAN) as Multipurpose Internet Mail Extensions (MIME) encoded e-mail attachments via Simple Mail Transfer Protocol (SMTP). As such, they must meet CJIS security policies for access control.

Must be BAP 10/20/30 or greater to send to FBI? (J. Olson)

The Ten-Print Fingerprint Image Searches (TPIS) and the Repository for Individuals of Special Concern (RISC) transaction types shall be used by CJIS to enable fingerprint searches that may originate from Mobile ID devices. Both shall be one-to-many searches. The transactions differ in response time and database files searched.

For the TPIS transaction with an average response time of two minutes, the ten-print fingerprint images are transmitted along with any required fingerprint classification information and descriptors by the originator. The fingerprint characteristics will be automatically extracted from the image at the FBI with no human intervention. The search process of the criminal fingerprint files is conducted and the results transmitted to the originator. The SRT response returned consists of the match report including the identification of matching candidates and the corresponding fingerprint images of the candidate with the highest score. Images for the remaining candidates may be retrieved through separate image retrieval requests.

The RISC transaction is provided by the FBI to enable rapid fingerprint searches implemented as part of the FBI's Repository for Individuals of Special Concern (RISC). RISC provides the capability to perform a rapid fingerprint search (with from two to ten rolled or flat fingerprint images) against a special file containing the most wanted individuals, including, among others, identified terrorists, wanted aliens, or other international subjects identified as a threat to the United States. RISC transactions will provide a 10-second or less response to searches from authorized agencies. In order to meet the rapid response times, all Rapid search requests will be fully automated ("Lights Out") Automated Fingerprint Identification System (AFIS) searches.

The response (RISCR) to a RISC search request will utilize a single character to indicate the following: "R" for Red, "Y" for Yellow or "G" for Green. An "R" will indicate that a positive identification (hit) has been made. A "Y" will indicate that the search request

returned more than one potential matching candidate. A "G" will indicate that no records within the RISC repository returned a "match score" high enough to be considered a potential candidate. For a red response, limited criminal history or terrorist watchlist information will be returned for any candidates (similar to TPRR), as well as the most recent full frontal photo if requested and available.

In order to submit a TPIS or RPIS search, a well formed ANSI/NIST-ITL 1-2007 transaction must be submitted. The following logical records will comprise such a transaction:

- A single Type-1 header record comprised of mandatory and optional fields
- A single Type-2 record containing mandatory and descriptive data
- From 2 to 10 Type-4 or Type-14 flat or rolled fingerprint images.

In response to a fingerprint investigative search request, the following logical records will be returned:

- A single Type-1 header record comprised of mandatory and optional fields
- A single Type-2 record containing mandatory and descriptive data
- From zero to 14 Type-4 or Type-14 fingerprint image records containing the requested fingerprint images of the first candidate (Response to TPIS)
- A single Type-10 record containing the most recent full frontal photo of the candidate if requested. (RPSR only)

A Type-1 logical record is mandatory and is required for each transaction. The Type-1 record shall provide information describing type and use of the transaction involved, the originator of the physical record, and other useful and required information items.

The Type-2 logical record shall contain textual information relating to the subject of the transaction and shall be represented in an ASCII format.

The binary Type-4 logical records shall contain and be used to exchange high-resolution grayscale fingerprint image data. The tagged-field Type-14 logical records shall also contain scanned high-resolution grayscale data but additionally provides the capability of including ASCII descriptive information with the image.

At this time, electronic facial image photo services only include a transaction for requesting criminal or civil photo sets on file at the FBI and a transaction to delete photo sets. Iris enrollment services are available but there is no provision for facial or iris recognition services. For details on the services available consult the EBTS 8.0.

9 Security & Encryption Considerations

The business community often cites security as one of the main hurdles to adoption of mobile applications. The threats to data privacy and security increase proportionally with the movement of internal business activities to areas beyond the boundary of the physical enterprise. When an absence of proven mobile security exists, organizations are reluctant to address leading edge mobile business process opportunities. Service organizations will be reluctant share information with systems employing mobile applications if they cannot be assured of a high degree security and privacy.

The proliferation of Mobile ID devices used in Defense, Homeland Security and Law Enforcement communities creates an increased threat to security defenses. Many of the threats can be directly addressed through specific actions that are commonly considered to be best practices in the wireless environment.

From a Federal perspective some basic security tenets must be upheld: Availability, Confidentiality and Integrity which are partially enabled through means such as Identification and Authentication (Including Non repudiation and Provisioning) and Encryption.

- Authentication
  - Mobile Device: Should the mobile device itself fall into the wrong hands it should be technically protected through some means of local authentication.
    - Minimal Security: Personal Identity Number (PIN) or pass-code entry.
    - Medium Security: Biometric or FOB
    - Higher Security: Biometric with PIN; FOB with PIN
  - Primary Network/System: Mobile subscriber should authenticate to the primary network or system to receive or send information.
    - Minimal Security: Username/Password (Something you know)
    - Medium Security: Something you know + Something you know
    - Medium Security +: Something you know + Something you just found out (Out of Band)
    - Higher Security: Something you have (FOB) + Something you are (Biometric)
    - Wi-Fi authentication protocol: Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) or Protected Extensible Authentication Protocol (PEAP)
- Encryption
  - Device: Encrypt data on the device to prevent compromise
  - Transmission: Encrypt the path (VPNs) (FIPS 140 compliant encryption)
    - Wi-Fi Protected Access 2 (WPA2) using Advanced Encryption Standard (AES)
    - Mobile ID Device to Mobile terminal
    - Mobile ID Device to Network/System
    - Mobile terminal to Network/System
  - Data in Transit: Send encrypted data across unencrypted path

Comment [RMM8]: Is this a challenge response deal? PTH9

  - Avoid the use of pre-shared keys in WPA or WPA2
- Access Points
  - Centrally Controlled: Use centrally controlled access points
  - Unadvertised: Turn off the service set identifier (SSID) on all nonpublic, nonguest access points. (won't completely deter but will foil casual attempts at access point cataloging)
  - Uniquely name: Change SSID names to something unique, but that doesn't reveal locations or owner
  - Limit Coverage: Limit coverage transmission strength.
- Personal Firewalls on Mobile Terminal
- Turn off peer-to-peer/ad hoc networking

Federal, state, and local law enforcement organizations need to keep constant watch on wireless security best practices, new threats and how to deal with them, and the technologies being developed to help mitigate those emerging threats.

A section needs to be added addressing security for storage of responses once they have been received back on the capture device. Aspects to be addressed include:

How long can they remain on the device (Logging)?
Can they be prevented from being forwarded to another device?

10 Communication Protocols

10.1 Wireless Connectivity

Mobile Identification devices that search a central database may employ a wireless connection to the central site. Wireless connectivity is dependent on local and regional capabilities. Dependent on the region of deployment connectivity may make use of short range Bluetooth or Wi-Fi connections, cellular data lines, or satellite communications. Minimum data rates are dependent on the image size to be transmitted and reasonable limits on time of detention. Several different approaches will be presented in this chapter for discussion and consideration.

10.2 Cellular Connectivity

10.2.1 GSM/GPRS/EDGE/UMTS

GSM/GPRS is a pervasive 2.5G cellular technology that is widely used in Europe and Asia. Cingular and T-Mobile are the most well known US carriers using this technology. Data rates are typically 40 kilobytes per second.

EDGE and UMTS are 3G technologies that push data rates up to 1 megabits per second.

10.2.2 CDMA/1XRTT/EVDO/EVDM

CDMA/1XRTT technology is a 2.5G technology that competes with GSM/GPRS. Sprint and Verizon are the most well known carriers in the US using this technology. Data rates are around 40 kilobits per second.

EVDO and EVDM are 3G iterations of this technology that push data rates up to 1 megabits per second.

10.2.3 HSDPA/WCDMA

HSDPA and WCDMA represent the next phase of cellular technology and the convergence of the two technologies discussed above. Future data rates are projected to reach 40 megabytes per second.

10.3 Satellite Communication

Satellite communication may be required in remote areas or at sea where other commercial communication systems are not present. Most satellite communications require bulky transmitters/receivers. Mobile Identification devices typically communicate to these devices using cables or Bluetooth connection.

10.4 802.11b/g

Wi-Fi is a common means of wireless communication built into today's PDAs and mobile PCs. Wi-Fi communication is high speed with rates exceeding 10 megabits per second and ranges exceeding 300 meters.

10.5 Bluetooth

Bluetooth is a wireless method of connecting devices at short range. Data rates for Bluetooth 1.0 are typically around 700 kilobits per second. Range for Bluetooth varies based on the transmit power used. Class 3 Bluetooth devices have a range of approximately 1 meter, class 2 approximately 10 meters, and class 1 approximately 100 meters. Bluetooth 2.0 extends the data rate of the wireless connection to three times that of Bluetooth 1.0.

10.6 Global Positioning System (GPS)

GPS functionality adds the ability for devices to location stamp transactions.

10.7 Integrated Wireless Antenna

Mobile devices include integrated antennas that support cellular connection equivalent to commercial cell phones**.**

10.8 *Wireless Connection Status*

PDA and PC applications for wireless connection provide and display the status of all wireless connections.

11 Mobile ID Device Features

11.5 11.1 General

Mobile Identification devices features are driven by the application of the device. As previously stated, applications can be divided into the law enforcement, military (DoD), and civilian verification segments. Each of these segments brings specific requirements to the device feature set and should be evaluated as such. Features required for law enforcement or DoD may be different than those needed for civil verification.

11.2 Platforms

11.2.1 Processors

Standalone capture devices typically use on board Digital Signal Processors (DSP) or embedded processors (such as ARM, or Advanced RISC Machines) meant for low power applications. Operating systems are typically dedicated to the specific processor. Applications are custom to the device and are not interoperable with third party applications.

PDA based applications typically use the same embedded processors but have operating systems that enable use of third party applications. Typical operating systems are Windows (Embedded, Mobile, CE, or .NET), Linux, Palm OS, or the Symbian OS.

11.2.2 Storage capacity

Standalone capture devices typically provide storage capacity to capture multiple sets of prints in an uncompressed format. Total memory required is dependent on the number of fingers captured and the number of subjects to be retained on the device. PDA based applications require memory for biometric applications, compression algorithms, and communications software, including encryption and security applications. Current generation PDAs typically provide 128 Megabytes of RAM, 128 megabytes of Flash, and optional flash cards with storage up to and exceeding several gigabytes of storage. Today's PC based applications typically have up to 1 gigabyte of RAM or more and over 40 gigabytes of storage capacity on disk drives.

11.2.3 Displays

Displays on standalone capture devices vary from graphical overlays to small displays capable of showing return messages and photographs. Capture devices intended for outdoor, rugged environments must be capable of displaying images and text in bright

sunlight as well as in the dark. Sunlight visible means capability for either a front-lit technology or 1000 NITS minimum backlighting. For viewing in the dark, a minimum of 100 NITS of back or front lighting is required. Application software typically enables multiple preset brightness settings and color schemes for daytime versus nighttime viewing.

11.2.4 Audio Generation and Recording

Stand alone capture devices have the capability to generate audio feedback to the user under software control. PDA and PC based systems use .WAV files that can be invoked under software control. PDA and PC based systems also include the ability to record audio data. Some devices provide equivalent feedback using a vibration in the device.

11.2.5 Expansion Capability

PDA or PC based Mobile Identification typically support expansion capabilities through one or more of the following interfaces:

- USB host ports, either USB 1.1 or USB 2.0
- USB client port, typically USB 1.1
- Serial port
- PCMCIA slot (type II x 1)
- Mini PCI Express
- SD slot
- Wireless connectivity (discussed below)

11.3 Capture Device Features

11.3.1 General

The following capture device features are considered desirable but not mandatory.

11.3.2 Fingerprint Capture

11.3.2.1 Finger Guide

Fingerprint capture devices with integrated finger guide are desirable to optimize placement of the finger such that the core and first crease of large thumbs is captured. Finger guides can also protect the fingerprint capture area from direct sunlight if required.

11.3.2.2 Finger Location Indicator

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 to insure optimal image content.

11.3.2.3 Auto-capture of image

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.

11.3.2.4 Manual capture of 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.

11.3.2.5 Quality check function

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

1. Image size
2. Light or dark image measurements
3. Minutiae count
4. Core location
5. NIST Image quality scores

11.3.2.6 Finger print image display

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

11.3.2.7 Image Enhancement Features

Image enhancing membranes on optical scanners are desirable to improve the ability to capture dry fingers. Membrane materials include silicon pads, epoxy, and urethane coatings.

11.3.2.8 Platen/Coating replacement

Optical scanner platen surfaces that may be field replaced are desirable to ensure continuity of use.

11.3.3 Facial Capture

11.3.3.1 On Board Illumination (Flash)

Mobile Identification devices using PDAs typically provide LED illumination. This illumination is sufficient for images to associate with the return information.

Mobile Identification devices used for facial recognition provide a high quality flash function as found on commercial or professional cameras.

11.3.3.2 Docking Station

Download of high resolution images from commercial or professional grade cameras requires a high speed transfer. Docking stations for the camera provide a high speed interface to a PC for transfer to a central location.

11.3.3.3 Return Data Display

Mobile Identification devices using facial recognition typically return a photo lineup of potential matches to the officer. The results are typically displayed on a PC to provide better resolution.

11.3.4 Iris Capture

11.3.4.1 Transmission of templates

Iris templates are small enough that transmission can be accomplished using sync cables or wireless connections.

11.3.4.2 Display of results

Results displayed may range from textual demographics data to photographic images.

11.4 Demographic entry

11.4.1 Keyboards/Keypads

Demographic entry may be accomplished using on screen keyboards, PDA keyboards or keypads, or PC keyboards.

11.4.2 Magnetic Stripe Readers

A magnetic stripe reader with capability of reading driver's licenses per AAMVA DL/ID-2005, enable demographic data entry using these cards.

11.4.3 Bar Code Readers

1-D and 2-D bar codes are used on some identification cards such as driver's licenses. Bar code readers allow input of demographic data from these cards.

In some instances, a 2-D bar code reader may also store fingerprint templates as input for verification.

11.4.4 Smart Card Reader

Smart card reader (contact or contactless) may be used for demographic data entry, for downloading, or storage of templates (fingerprint, facial, or iris) for matching on-board verification devices.

11.4.5 Passport Reader

Optical Character Readers (OCR) may interpret text on passport Machine Readable Zones (MRZ) to obtain demographic data. In applications using smart cards the information on the passport may include biometrics in compliance with ICAO standards as discussed above.

11.5 Power Features

11.5.1 Removable Battery

The ability to remove the battery allows continuous operation without the need for charging cradles in vehicles.

11.5.2 Charging

The ability to charge from automotive +12 VDC (+10.0 to +18.0) or from chargers running on recognized international power sources (110 to 240 VAC) gives flexibility to user workflows. Units are typically able to operate while charging.

11.5.2.1 Battery life Indicators

Battery life indicators that display the amount of battery power and estimated time of operation remaining are desirable.

11.5.2.2 Battery Charge Indication

Battery charge indicators that show charging is in process are desirable.

11.5.2.2 Desktop Battery Charger

Desktop battery chargers are typically available. Desktop chargers, car chargers, and devices using a common connector to the Mobile Identification device are desirable.

11.5.2.3 Vehicle Charger

Vehicle chargers that operate from car cigarette lighters are desirable.

11.5.2.4 Gang Charger

Gang chargers for charging multiple batteries are desirable.

11.5.3 RAM Holdover Battery

Holdover batteries providing power to on board RAM for up to 30 days are desirable.

11.5.4 Non-Volatile Memory

Application programs stored in non-volatile memory are desirable to prevent loss of applications during a total loss of battery.

11.6 Certifications

Mobile device certifications available include:

US FCC class B part 15
CE Certification
EN 60529, Ingress Protection
Multiple levels of ingress protection are available.
Military devices are typically IP65, dust tight and able to survive water spray.
Some naval devices add IP67, dust tight, water tight to 1 meter.

12 Environmental Requirements

12.1 *Operating Temperatures*

Operating temperatures are typically:

Law Enforcement	-	0ºC ~ 50ºC	(32ºF ~ 140ºF)
Military	-	-20ºC ~ 50ºC	(-4ºF ~ 140ºF)

12.2 Storage Temperatures

Storage temperatures range up to -40ºC ~ 70ºC (-40ºF ~ 158ºF)

12.3 Relative Humidity

Humidity requirements are typically 5 ~ 95% non-condensing operating or storage

12.4 Salt Water Spray

Naval operations require operation in a salt spray environment

12.5 Shipping Shock and Vibration

Mobile devices must survive transportation shock and vibration.

12.6 Drop Test Requirements

Mobile devices are specified to survive multiple drops onto concrete from XX meters..

13 Acquisition Considerations

This is not intended to provide all of the considerations for starting a mobile identification project as all implementations are different. They are:

Network: Field devices not accessing a resident database or one in the car needs to be reliable and utilize a bandwidth that can support a response within time frames that are deemed within legal detention time frames. Most have deemed within 5 minutes to be acceptable.

Network / Manual data transfer: Devices accessing resident or one in the car need to be kept current this is either network or done manually (portable media or direct on the device).

Responses: Whenever Possible, the response to the officer should include photos on hit notifications. This adds another level of verification for the operator using the device. Candidate lists including photos can also be useful when the system cannot provide a positive identification. Warrant response based on the AFIS ID's is also very useful. More than not, the first thing the officer will do after receiving the positive ID is do a warrant check.

Training: Users should be trained in the use of the device and limits to their testimony in court.

Reporting: Allow for some kind of print out compatible file that can be saved downloaded and then added to a report, citation, or used for court purposes.

E-Citation: If your agency has e-citations, the sensor utilized should meet the minimum specifications in this document. This can aid in having an image that can be enrolled into an AFIS.

Legal: As this device can easily be abused and deemed a violation of privacy, policy should be in place that restricts its use to stay within the limits of existing case law for requiring identification from persons being detained.

Software updates: As these devices are deployed, they will inevidly require updates. Updating of devices manually is time intensive. Auto updates are recommended.

14 XML Issues

All current communications with the FBI IAFIS and RISC use ANSI/NIST packets in formats based on EFTS 7.1 or earlier. Recently XML has gained wide acceptance in private and public sector applications as an effective data delivery method. As NIST released ANSI/NIST-ITL 1-2007, they continued the current packet format as Part 1 of

the standard, and they plan to incorporate an XML version as Part 2. The same data elements are passed in both parts.

The ANSI/NIST-ITL 1-2007 Part 2 will be based upon NEIM 2.0 (National Information Exchange Model). This model standardizes the structure and tag names for data exchanges, including criminal justice related data exchanges. As systems are upgraded or replaced more and more will be using NEIM XML for exchanging data. The FBI has released a DRAFT EBTS with interfaces compatible with ANSI/NIST-ITL 1-2007 Part 2 with a preference for new SIB systems to implement Part 2 NIEM XML compliant systems. (J. Olson)

15 Scenarios

Up to this point no one has proposed including any Application Profile scenarios for specific systems or applications. Are there any such profiles that should be included? For example: applications such as TWIC, Trusted Traveler etc.. Do you have a contribution that should be included in this document?

16 Future Requirements

To be developed as necessary..