



# Landscape Study of **Mobile ID** **Fingerprint Devices**



*January*  
**2014**

**Jeri Roper-Miller**

FTCoE Technology Transition Task Leader  
jerimiller@rti.org

**Technical Contacts:**

**Moline Prak Pandiyan**

Products  
moline@rti.org

**Jonas Hall**

Application  
jonashall@rti.org






## TABLE OF CONTENTS

Please Note: This report is a good-faith effort by the FTCoE to accurately represent information available via primary and secondary sources at the time of the analysis. Where appropriate, RTI has sourced the primary research with individual sources, and similarly, key secondary sources are identified. All other information is a composite view developed from literature, trade press, and stakeholder input.

2	Overview
10	Use Profiles and Considerations
25	Product Landscape
32	Summary



This report is funded through a Cooperative Agreement (2011-DN-BX-K564) from the National Institute of Justice (NIJ), Office of Justice Programs (OJP), U.S. Department of Justice (USDOJ). The views, policies, and opinions expressed are those of the authors and contributors and do not necessarily reflect those of the NIJ, OJP, or USDOJ.



## The National Institute of Justice’s (NIJ’s) Forensic Technology Center of Excellence (FTCoE) at RTI directed this effort, with input from the broader forensic community

### Landscape Study on Mobile ID Fingerprint Devices

This report provides a “landscape” view of the issues and products associated with mobile devices for fingerprint identification, with a focus on forensic applications. The document is intended to furnish laboratory managers and investigators with a survey of current commercially available products. In addition, the report provides decision makers and potential end users with use examples that illustrate successful adoption; issues to consider related to implementation of mobile ID devices; and a snapshot of current mobile ID technologies. Upon review, the reader may better understand whether mobile ID devices can benefit his or her organization and how to proceed with selecting a platform and implementing use.



### Forensic Technology Center of Excellence

FTCoE is a collaborative partnership of RTI International and its FEPAC [Forensic Science Education Programs Accreditation Commission]-accredited academic partners: Duquesne University, Virginia Commonwealth University, and the University of North Texas Health Science Center. In addition to supporting NIJ’s research and development (R&D) programs, the FTCoE provides testing, evaluation, and technology assistance to forensic laboratories and practitioners in the criminal justice community. The NIJ funds the FTCoE to transition forensic science and technology to practice (Award Number 2011-DN-BX-K564).



The FTCoE is led by RTI, a global research institute dedicated to improving the human condition by turning knowledge into practice. With a staff of more than 3,700 providing research and technical services to governments and businesses in more than 75 countries, RTI brings a global perspective. The FTCoE builds on RTI’s expertise in forensic science, innovation, technology application, economics, data analytics, statistics, program evaluation, public health, and information science.





## Thank you to the various community members who offered insight, analysis, and review

### Practitioners and Program Managers

**Gregory Alexander**  
Principal  
Strategic Operational Solutions

**Joseph Atick**  
Chairman  
Identity Council International

**John Boyd**  
Director, Defense Biometrics & Forensics  
Department of Defense

**Melody Buba**  
Electronics Technician  
Intrusion Detection Group  
Federal Bureau of Investigations (FBI) Laboratory Division

**Jeff Carlyle**  
Latent Print Unit Liaison  
FBI Laboratory Division

**Lars Ericson**  
Director, Advanced Technologies  
ManTech International Corp.  
Sensor, Surveillance, and Biometric Technologies Center of Excellence

**Roberta (Bertie) Geiselhart**  
Supervisor of Investigations  
Hennepin County Medical Examiner's Office

**Melissa Gische**  
Forensic Examiner  
Latent Print Operations Unit  
FBI Laboratory Division

**Mark Greene**  
Program Manager  
NIJ, Office of Science and Technology

**John Grilli**  
Project Lead  
Dept. of Defense, Biometrics Identity Management Agency

**Jerry Harper**  
Systems Support Analyst  
San Bernardino County Sheriff's Department

**Owen McDonnell**  
Latent Print Examiner Caddo Parish Sheriff's Office

**Danielle McLeod-Henning**  
Program Manager  
NIJ, Investigative Forensic Sciences

**Marzena (Mary-Ann) Mulawka**  
Identification Coordinator and Criminalist NYC Office of the Chief Medical Examiner

**Jacob (Jake) M. Ruberto**  
Technical Support Specialist  
Pinellas County Sheriff's Office

**Dave Russell**  
Director  
Northern Virginia Regional Identification System (NOVARIS)

**William (Bill) Schade**  
Fingerprint Records Manager  
Pinellas County Sheriff's Office

**Rodney Schenck**  
Latent Print Technical Lead  
Defense Forensic Science Center  
U.S. Army Criminal Investigation Laboratory (USACIL)

**Frank Sullivan**  
Automated Systems Analyst  
San Bernardino County Sheriff's Department

**Aaron Uhle**  
Major Incident Program Manager  
FBI Laboratory Division  
Latent Print Support Unit

**Grant Ward**  
Detective  
San Bernardino County Sheriff's Department

**Garold Warner**  
Senior Analyst  
Defense Forensic Science Center  
USACIL

### Technology Developers

**Robert Christensen**  
Senior Forensics Advisor  
3M Cogent

**Kathleen Erickson**  
VP of Business Development  
Fulcrum Biometrics

**Anthony (Tony) Misslin**  
Senior Product Manager SAFRAN MorphoTrak

**Arudheer Pandey**  
Senior Product Manager  
Biomorf

**Rahul Parthe**  
Executive, VP, CTO  
Biomorf

**Devin Shelby**  
Sr. Customer Support Engineer  
SAFRAN MorphoTrak

**Shashi Subbarao**  
Technical Lead  
NEC Corporation

**Stephen Thies**  
CEO  
Integrated Biometrics

**Dan Troutman**  
VP, Mobile Solutions  
Cross Match Technologies





## Experts offered insight related to the use of mobile ID fingerprint devices for forensics

NIJ's Forensic Technology Center of Excellence (FTCoE) at RTI International has researched the adoption criteria, use, and available products for mobile ID fingerprint capture for forensic applications.

### BASIS FOR STUDY

- Biometric data are being used by a growing number of criminal justice and law enforcement agencies.
- Mobile ID fingerprint devices have grown in popularity and are used among federal, state, and local law enforcement agencies to obtain and verify the identity of potential threats to security at the national and local levels. The use of these devices has the potential to benefit investigations.
- Impact at the state and local levels from this technology on forensic investigation is not well understood, as little examination has occurred.
- A better understanding of the "state of the shelf" and practical uses of mobile ID fingerprint devices for forensic applications, particularly with identification of the deceased, would benefit decision makers regarding adoption, use, and impact on law enforcement processes.

### RESEARCH METHODOLOGY

- Researched secondary sources, including journals and industry literature, for information related to the need, successful use, and adoption criteria of enabling technologies in the field.
- Discussed state of the art with subject matter experts and organizations, including practitioners, companies, academic institutes, and other industry experts. Specifically, asked key questions covering products, markets, and user needs to understand the impact of various products and associated technologies on policing operations and investigational outcomes.
- Documented results via this report for release to the forensic and criminal justice communities.

### PUBLIC DOMAIN NOTICE

- All material appearing in this publication is in the public domain and may be reproduced or copied without permission from the NIJ. However, this publication may not be reproduced or distributed for a fee without the specific, written authorization of the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Citation of the source is appreciated. Suggested citation:
  - *National Institute of Justice, Office of Justice Programs. (January 2014). "Forensic Technology Center of Excellence: Landscape Study of Mobile ID Fingerprint Devices."*
- Obtaining Copies of This Publication: Electronic copies of this publication can be down-loaded from the FTCoE website at <https://www.forensiccoe.org>





## The study considers the past (lessons), present (considerations and products), and future (trends)

The objective of the landscape was to

- investigate how mobile handheld devices have been used for forensic applications, particularly for identifying the deceased.
- provide considerations for potential users to influence planning prior to adoption.
- identify current and future technology trends.

### Forensic Uses for Mobile ID and Other Digital Fingerprint Devices

Fingerprint capture from the deceased can be challenging due to rigor mortis and/or fingerprint damage caused by body decomposition or trauma. Fingerprint reconditioning techniques and small mobile capture devices with high-quality fingerprint sensors are recommended for use with the deceased.

Two departments are highlighted that have had success in using mobile devices:

- San Bernardino County Sheriff's Department.
- Northern Virginia Regional Identification System (NOVARIS) Law Enforcement Participants.

Additionally, the New York City Office of Chief Medical Examiner is highlighted for their use of non-mobile digital fingerprint capture technology to demonstrate the benefits of digital capture technology in a forensic setting. Latent fingerprint software has expedited investigation processes for capture and analysis of latent prints.

### Considerations Before Implementation

Potential users should consider various key factors before purchasing mobile ID fingerprint technology. This report explores the following three considerations:

- Identifying needs for a mobile ID system.
- Understanding how mobile ID system capabilities can meet agency needs.
- Considerations for procurement of a mobile ID system.

Factors include fingerprint identification speed, ease of use of mobile ID devices, mobile ID system structure and function, product feature options, and acquisition strategy.

### Current and Future Product Landscape

Technology providers offer a variety of solutions along the mobile ID fingerprint capture process. A wide range of devices are available, from single-feature to multimodal capture devices. Complexity and sensor type affect price, size, weight, and ease of use. An evaluation matrix is provided for comparing example single-feature and multimodal (fingerprint, iris) mobile ID capture devices.

As mobile devices become more ubiquitous, technology providers are developing more accessory attachments to complement existing mobile platforms. This trend will likely reduce the overall cost of investment.



## Knowledge of key terms is vital to building an understanding of mobile ID fingerprint technologies

### **Criminal Justice Information Services**

**(CJIS):** FBI division serving as the focal point and central repository for criminal justice information services in the FBI. It provides identification and information services to local, state, federal, and international criminal justice communities, including maintenance of IAFIS (see <http://www.fbi.gov/about-us/cjis>).

### **Fingerprint Acquisition Profile (FAP):**

An FBI mobile ID device classification system number based on capture dimensions, the image quality specification applied, and the number of simultaneous fingerprints that can be captured. The FAP certification category ranges from 10 to 60, with a higher number designating a larger capture dimension and/or types of fingerprints collected (see <https://www.fbi biospecs.org/iafis/>).

**Friction ridge:** Small dermal ridges covering digits, palms, and soles of the hands and feet that assist in the ability to grasp and hold onto objects, the source of latent fingerprint impressions. (see National Institute of Justice, Office of Justice Programs. "The Fingerprint Sourcebook." Appendix D: SWGFAST Standard Terminology of Friction Ridge Examination, Ver. 3.0. <https://www.ncjrs.gov/pdffiles1/nij/225320.pdf>).

**Impression, flat:** Fingerprint images taken without rolling. Also known as plain or slap impressions. Impressions can be collected with ink or digitally.

**Impression, rolled:** Individually taken fingerprint images rolled from nail edge to nail edge. Impressions can be collected with ink or digitally.

### **Integrated Automated Fingerprint Identification System (IAFIS):**

IAFIS is the national fingerprint and criminal history system maintained by the FBI Criminal Justice Information Services (CJIS) Division. It is the largest biometric database in the world, housing the history of more than 70 million subjects (see [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/iafis](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis)).

**Latent fingerprint:** A fingerprint left by a chance or accidental impression from friction ridge skin on a surface, regardless of its visibility at the time of deposition. Latent fingerprints can be captured in the field by crime scene investigators with mobile ID devices, and later analyzed by latent print examiners.

**Mobile ID:** Handheld devices that can operate in a mobile environment. The category is subdivided into several levels by FAP number. While mobile ID devices are portable, some portable devices, such as a laptop, are not necessarily mobile. Single-feature devices collect only one type of biometric data (typically fingerprint impressions). Multimodal devices collect a variety of biometric data types.

**Next Generation Identification (NGI):** Driven by advances in technology, customer requirements, and growing demand for IAFIS services, the FBI has initiated the NGI program. NGI aims to improve the biometric identification services provided by IAFIS, while introducing quality check automation, advanced fingerprint identification technology, and multimodal biometric identification (see [http://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi](http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi)).



## Devices vary based on image size and capture type, data management, transmission, and use



	Bluecheck II	Bluecheck II U	Verifier Mw	IBIS Extreme	Morpho-IDent	Stratus MX	Morpho-Check	RapID 1100	FbF mobile-One
<b>FAP</b>	10	10	30	-	10	10	10	20	10
<b>Capture Type</b>	Flat Impressions	X	X	X	X	X	X	X	X
	Rolled Impressions								
	Latent Prints*								X
	Facial Recognition						X		X
	Iris Recognition						X		
	Card Reader**						X	X	
<b>Data</b>	Audio Recorder					X			X
	Real-Time	X	X	X	X	X	X	X	X
<b>Transmission</b>	Stored	X	X	X		X		X	X
	Mobile Network				X	X	X	X	X
	WiFi			X		X	X	X	X
	Bluetooth	X	X	X	X	X	X	X	X (Apple® iOS)
	USB or Wired Connection	X	X			X		X	X
	GPS Localization						X	X	X
<b>Confirmed Use</b>	Local	X	X	X				X	
	State	X	X	X					
	Federal - Border Control	X	X	X					
	Federal - Military			X					
	Federal - Intelligence	X		X					
	Federal - Global	X							

\*Image processing post-capture may be required.

\*\*Card reader may refer to a contact or contactless radio-frequency identification (RFID) card reader, 2D barcode reader, and/or Machine Readable Zone (MRZ) swipe reader. Please contact the respective device manufacturer for specific card reader options.





Devices vary based on image size and capture type, data management, transmission, and use (continued)

								
	MI2	MI3	Fusion	BA500	SEEK Avenger	SEEK II	SEEK II with Quad Reader	Trident
<b>FAP</b>	20	30	30	30	45	45	45	45
<b>Capture Type</b>	Flat Impressions	X	X	X	X	X	X	X
	Rolled Impressions				X	X	X	X
	Latent Prints*			X	X	X	X	
	Facial Recognition	X	X	X	X	X	X	X
	Iris Recognition			X	X	X	X	X
	Card Reader**		X		X		X	X
	Audio Recorder			X		X	X	
<b>Data</b>	Real-Time	X	X	X	X	X	X	X
	Stored	X	X	X	X	X	X	X
<b>Transmission</b>	Mobile Network	X	X	X	X	X	X	X
	WiFi	X	X	X		X	X	X
	Bluetooth	X	X	X	X	X	X	X
	USB or Wired Connection	X	X			X	X	X
	GPS Localization					X	X	X
<b>Confirmed Use</b>	Local	X	X	X				X
	State	X	X	X		X	X	X
	Federal - Border Control		X	X		X	X	X
	Federal - Military			X		X	X	X
	Federal - Intelligence			X		X	X	X
	Federal - Global	X	X	X		X	X	X

\*Image processing post-capture may be required.

\*\*Card reader may refer to a contact or contactless radio-frequency identification (RFID) card reader, 2D barcode reader, and/or Machine Readable Zone (MRZ) swipe reader. Please contact the respective device manufacturer for specific card reader options.



2	Overview
10	<b>Use Profiles and Considerations</b>
25	Product Landscape
32	Summary





## Subject matter experts provided insight based on use, market, and product experiences

### Use-Directed Questions

- How are mobile ID fingerprint devices used?
- Have they been successful in identification of the living and deceased?
- How can these products be improved?
- What technology features have a significant impact on adoption?
- Are there any existing guidelines or protocols for using these devices? If yes, what are they?

### Market-Related Questions

- What are the leading products? What new products are anticipated?
- What is the greatest need in the mobile ID fingerprint device market?
- What factors or product features affect return on investment for local law enforcement agencies?
- What kind of analysis (cost vs. features) is common for procurement? Is there a need for a department to have one vendor or device for both patrol (suspect ID) and crime scene or death scene investigation (deceased ID)?

### Product-Specific Questions

- What is the product's recognition capabilities? Does it have other recognition capabilities outside of fingerprint detection (e.g., iris, facial)?
- What is its scanning and identification speed?
- Where has it been used?
- How are security concerns addressed?
- What is the interoperability of the database management system?
- Is your mobile ID fingerprint device an IAFIS Certified Product?



## Successful use in the forensic and law enforcement communities offers insight on implementation

This section provides examples of successful implementation of mobile ID technology to illustrate benefits and key adoption issues. The use profiles offer insight on different ways that mobile ID technology has been an effective tool within the law enforcement and medicolegal communities, with special focus on the use of the technology for forensic investigations. Key impacts and lessons learned are highlighted.

The highlighted profiles were selected based on their use of mobile ID devices and other digital fingerprint capture technology (NYC OCME) for identification of the deceased, in addition to their use in a broader law enforcement context (patrol and suspect identification). Examples of use include:

- Deployed mobile ID fingerprinting solutions for a Coroner's Office in conjunction with the Sheriff's Department.
- Used mobile ID technology to speed investigations.
- Altered internal identification processes to shorten existing DNA testing backlogs.



**San Bernardino County Sheriff's Department**



**Northern Virginia Regional Identification System**



**NYC Office of Chief Medical Examiner**





## San Bernardino County uses mobile ID devices to identify both the deceased and the living

**Grant Ward and Jerry Harper** at the San Bernardino County Sheriff-Coroner Office have co-developed a fingerprint identification system with SAFRAN MorphoTrak. These efforts have led to the commercialization of customized fingerprint field capture devices that are simple and compact.

### Use Profile

In the San Bernardino County Sheriff-Coroner Office, law enforcement officers in the field use *IBIS Extreme*, a single-feature mobile ID fingerprint capture device by MorphoTrak. When suspects do not have a form of identification, or when false information may have been provided, officers can request to scan the individual's fingerprints for identity verification. The fingerprint images are transmitted wirelessly to search local, state, and FBI AFIS databases. The suspect's identifying information, along with relevant criminal history and outstanding warrant information, is relayed to the officer in the field in a matter of minutes.

The office also deployed 10 *IBIS Extreme* devices for identification of the unknown deceased. In one of the earliest successes of mobile fingerprint ID technology, a homicide-rape victim without ID was positively identified by a deputy using the mobile ID device. In another case, two homicide victims without identification were discovered. An initial search of AFIS criminal databases revealed no positive identification of the deceased; in a subsequent search, images were manually submitted to search Department of Motor Vehicles civil records, resulting in a positive match.

### Impact of Mobile ID Fingerprint Devices

- Mobile ID fingerprint devices have effectively reduced the number of falsely provided identities. The number of people who provided false identification dropped from 701 to 3 individuals following the first year of mobile ID use.
- Mobile ID fingerprint devices have proven to be effective tools for rapid identification of the deceased in the field.

### Lessons Learned

- Collective acquisition of mobile ID devices between a joint Sheriff's and Coroner's Office can allow greater access to database records, increasing the chance of a match.
- Practitioner experience can significantly influence mobile ID device development.
- Some users value single-feature devices over products with multiple capture attributes.



## Successful ID of the deceased has prompted mobile ID adoption by regional law enforcement

**Dave Russell** is the current director of the Northern Virginia Regional Identification System (NOVARIS). NOVARIS is a sophisticated network of regional multimodal biometric databases that includes databases from counties in Maryland, Virginia, and Washington, DC.

### Use Profile

In 2007, the first successful use of mobile ID devices in Prince George's County, Maryland, was for identification of a deceased individual. The mobile ID device helped to jump-start investigations and inspired the Prince George's County Police Department to adopt mobile devices.

Mobile ID devices have been deployed for use by law enforcement officers in the field within the Northern Virginia system, which is part of a triad of AFIS sites across the National Capital Region. When an officer scans a fingerprint during field contact, the resulting image is searched against the criminal database of three local AFIS systems in logical succession until a hit is determined. The return search contains basic information to check additional database systems, along with a mug shot to assist with identity confirmation. Mobile devices have been used to accomplish the following:

- Determine if an individual has any outstanding warrants.
- Clear from association an individual sharing the name of a known criminal.
- Elicit truthful responses from suspects when positive identifications are made.
- Confirm the identification of incapacitated or deceased individuals.

### Impact of Mobile ID Fingerprint Devices

- Mobile ID devices have proven effective for rapid identification of the deceased in the field. Using mobile ID devices and the NOVARIS network, investigators can identify individuals within 30 seconds of a fingerprint scan.
- In the past, investigators could not trust documentation identification (e.g., drivers license) found on deceased individuals since the information could be false. Mobile ID devices offer a way to verify identity.

### Lessons Learned

- Building a database network with neighboring jurisdictions expands identification capabilities.
- Consider the upfront installation and maintenance costs of network infrastructure when acquiring mobile ID devices. An Urban Areas Security Initiative (UASI) grant was used to help fund the system.
- Choosing a system that has no recurring communication costs will help reduce overall cost. The mobile unit connects via Bluetooth or USB cable to the police cruiser laptops and existing communication methods.
- Information captured using multiple types of mobile ID devices is compatible with other AFIS databases.



## Fingerprinting has become a preferred method for ID of the unknown deceased in New York City

The Office of Chief Medical Examiner in New York City has utilized non-mobile digital fingerprint capture technology for identification of the unknown deceased, and uses fingerprint reconditioning techniques developed by the FBI.

### Use Profile

In the OCME, fingerprints collected from the unknown deceased have become a valuable tool for making identifications. In some cases, the condition of the remains presents a special set of challenges for examiners. Often, fingerprint ridge details may not be apparent at first glance due to deterioration or exposure of skin to the elements. OCME uses various fingerprint reconditioning techniques that have been developed by the FBI Disaster Squad to recover friction ridge detail for identification. After reconditioning the skin, traditional fingerprinting methods or digital fingerprint capture devices may be used to collect fingerprint impressions from the deceased.

After collection, fingerprints are submitted via a digital fingerprint system to search against New York Statewide Automated Biometric Identification System (SABIS) and FBI IAFIS/NGI databases. Match results are then used to solve cases and notify next-of-kin of the deceased. While mobile ID fingerprint devices have not been fully adopted by OCME, their success with current digital fingerprint devices allow them to see the potential added benefit of these new, smaller technologies.

### Impact of Digital Fingerprint Capture Devices

- Digital fingerprint collection and submission can reduce the turnaround time for identifications and reduces the reliance on DNA for difficult cases.
- Digital fingerprint capture device training on product capabilities and proper use has been simple in comparison to training required by traditional fingerprint collection methods.
- Digital fingerprint capture devices provide instantaneous feedback on image quality to encourage new scans until a good quality scan is obtained.

### Lessons Learned

- Reconditioning of friction skin may be required to capture quality fingerprint images from the deceased.
- Access by non-law enforcement agencies to IAFIS databases must be approved by CJIS, and in some cases, is labor intensive and requires annual training.
- Departmental process changes may be required to take advantage of new fingerprint ID technologies.



## Agencies should consider three key implementation aspects

Important considerations must be addressed when determining whether to implement a mobile ID fingerprinting technology for forensic applications. These include considerations of application parameters associated with need, resource availability and allocation, implementation restrictions, and impact on processes. Insights for each of these key issues were gathered from practitioners over the course of the study. While this information is not intended to be exhaustive, it does provide valuable insight.

- 1** **Identifying Needs for a Mobile ID System**  
Mobile ID fingerprint capture devices can expedite forensic investigations due to their compact and user-friendly form factor (physical size, shape, and style) and AFIS connectivity.
- 2** **Understanding Mobile ID System Capabilities**  
Mobile ID systems can be simple or complex and can range from small-scale to large-scale deployments. System capabilities should be evaluated based on user-defined preferences. Features to consider include identification speed, transmission method, interoperability standards, device capture type, form factor, cost, accuracy, and impact on potential training requirements.
- 3** **Considerations for Procurement of a Mobile ID System**  
A strong acquisition strategy depends on understanding user preferences and budgetary constraints.







## Mobile ID devices offer efficiencies that result in expedited investigations

Discussions with practitioners identified challenges that are encountered during forensic investigations. Mobile ID systems have value in these scenarios and help to resolve these challenges. The following situations, although not exhaustive, provide example scenarios where mobile ID systems provide benefit.

**Mass casualty situations** – In disaster-response efforts for mass casualty scenarios, severe disfigurement or separation of subjects from identifying information is common. Mobile ID devices' compact maneuverable size and AFIS connectivity can offer a solution for faster identification of the deceased, expediting the recovery process.

1  
Identifying Needs  
for a Mobile  
ID System

**Unknown suspect or victim at crime or death scene** – The time required to collect, analyze, and identify latent fingerprints and the fingerprints of unknown deceased individuals at crime or death scenes can impede the progress of criminal investigations. Mobile ID devices and latent fingerprint analysis may reduce delays by providing faster identification of victims or suspects.

2  
Understanding  
Mobile ID System  
Capabilities

**Traditional inked impressions of the deceased** – Collection of fingerprints from the deceased using traditional methods presents challenges for coroners and medical examiners. Onset of rigor mortis results in a considerably more difficult scenario to obtain quality inked prints; furthermore, manual submissions to AFIS databases delay quality determination. Mobile ID devices that can instantaneously indicate image quality and access AFIS databases may reduce the time spent tediously collecting fingerprints.

3  
Considerations for  
Procurement of a  
Mobile ID System

*Fingerprint collection from unidentified bodies is a lengthy process, and medical examiners offices are often understaffed, so technology that could make their lives less complicated and more productive would be beneficial.*

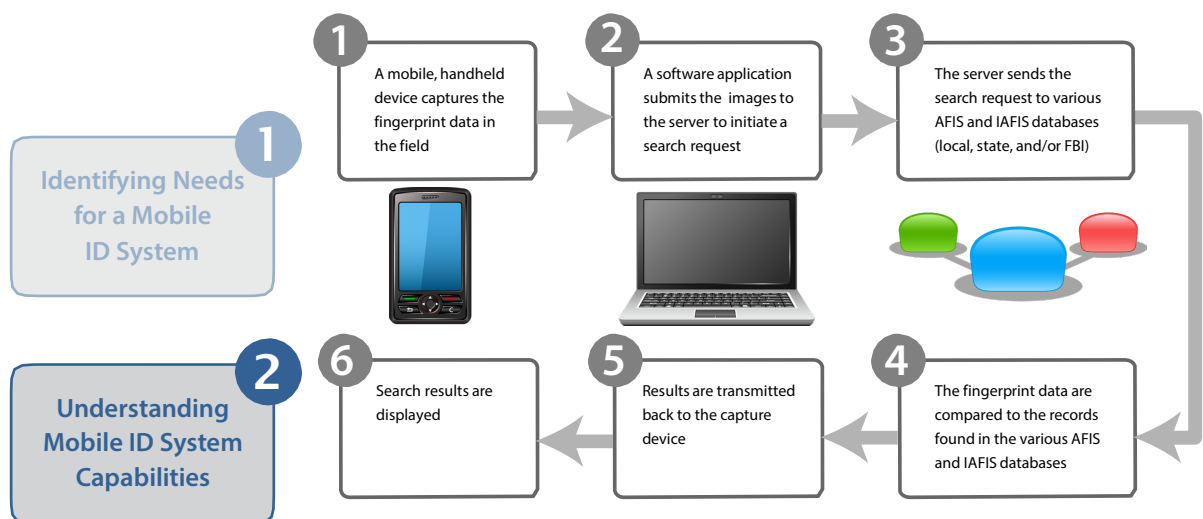
**Roberta Geiselhart**  
Hennepin County Medical Examiner's Office





## Mobile ID system components and size of the supporting network directly impact complexity

Mobile ID systems can be simple or complex, based on system components, and can range from small-scale to large-scale deployments. The complexity of mobile ID systems largely depends on the interconnectivity and size of a supporting network of servers, which provide access to AFIS databases.



1  
Identifying Needs for a Mobile ID System

2  
Understanding Mobile ID System Capabilities

3  
Considerations for Procurement of a Mobile ID System

As shown above, the mobile ID fingerprint capture process comprises several components, which are offered by various technology providers:

**Devices** – portable, handheld, single-mode, or multimodal biometric devices with varying communication capabilities. Data are relayed from mobile ID devices to servers for routing to AFIS databases.

**Servers** – allow law enforcement agencies to share access to smaller regional AFIS databases, as well as state and national AFIS.

**AFIS Databases** – automated systems that compare captured biometric data with stored records to identify a match that is then routed back to the submitter.





## AFIS accessibility will influence identification speed and can be wireless

Identification speed is affected by system architecture, speed, fingerprint database size, matching algorithms, and interoperability. Requirements for identification speed vary per end-user needs.

**Law enforcement officers** – require highly automated search systems that can return results in a matter of minutes or even seconds. This is important for ensuring officer safety in the field while maximizing the amount of time that a suspect can be detained without additional information.

**Medical examiners and investigators** – value expeditious identification of latent prints or of the unknown deceased because this information can speed investigative processes and save precious time. If instantaneous results are not required, a slower system with manual steps may prove more economical.

Fingerprint data for matching and identification can be transmitted directly to AFIS databases or through authorized personnel. Direct record transmission from mobile ID devices requires access to an AFIS database system. With direct transmission, users in the field can send and receive match records from the mobile device. Device connectivity to AFIS includes the following capabilities, each having their own limitations:

- **Wi-Fi** – operable only with access to a connected wireless network.
- **Mobile network** – operable with access to mobile telecom networks. Agencies should check with network providers to understand if access to 3G or 4G networks is available in their jurisdiction. Readers should be aware that network providers charge users based on data transmission volume, and frequent mobile network usage can be expensive.
- **Bluetooth** – operable only when the paired capture device is within a working range of the network-enabled device (roughly a maximum of 30 feet). In some jurisdictions, personally identifying information may be transmitted, but not received, using Bluetooth. Personally identifying information indicated by a positive match cannot be returned to the mobile ID device using a Bluetooth connection, but can be received by the network-enabled device.
- **Wired connection** – dependent on access to additional equipment.

1  
Identifying Needs  
for a Mobile  
ID System

2  
Understanding  
Mobile ID System  
Capabilities

CONTINUED

3  
Considerations for  
Procurement of a  
Mobile ID System





## FBI-certified products are IAFIS compatible and meet/exceed minimum interoperability standards

Mobile ID device compatibility with existing AFIS databases (including the FBI's IAFIS) is an important concern when determining mobile ID device technologies that best suit an agency's needs. FBI's IAFIS certification and compatibility requirements ensure that images captured by devices can be used with a wide range of state and local AFIS databases.

### FBI certification ensures IAFIS interoperability

Certified products that meet or exceed minimum FBI interoperability standards will work with IAFIS. These standards ensure that the images used in the system are high quality and support all phases of identification for both fingerprint experts and the IAFIS.

The FBI certifies fingerprint devices based on two standards: Appendix F of the FBI's Electronic Biometric Transmission Specification, and the FBI's Personal Identity Verification Image Quality Specification for Single Finger Capture Devices (PIV-071006).

- **Appendix F** – sets forth stringent FBI/CJIS image quality specifications that help to enable efficient large-scale automated fingerprint identification operations by IAFIS.
- **PIV-071006** – is a lower-level FBI certification standard designed to support one-to-one fingerprint verification. Certification is available for devices intended for identity verification of federal employees and contractors.

While FBI certification ensures interoperability of data with IAFIS, it does not ensure interoperability of the device with existing departmental AFIS infrastructure. Compatibility should be confirmed in the early stages of system implementation and included in requests for information from mobile ID manufacturers.

### IAFIS Certified Product List meets set image quality standards

The IAFIS Certified Product List (CPL) provides users with a list of products that have been tested and are in compliance with IAFIS Image Quality Specifications (IQS) regarding the capture of friction ridge images. Products listed on the CPL should not be construed as an FBI endorsement. Users should contact their State CJIS Systems Officer or Information Security Officer to ensure compliance with necessary policies and/or guidelines. A comprehensive list of FBI-certified capture devices can be found at <https://www.fbibiospecs.org/IAFIS/Default.aspx>.

1  
Identifying Needs  
for a Mobile  
ID System

2  
Understanding  
Mobile ID System  
Capabilities

CONTINUED

3  
Considerations for  
Procurement of a  
Mobile ID System





## Mobile ID devices are available in a range of capabilities that fit varying agency needs and budgets

Single-feature devices capture one type of biometric information and can be simpler than multimodal devices (for example, a combination of fingerprint, iris, and facial recognition biometric functionality in a single device). However, multimodal devices can allow other biometric collection modalities when fingerprints are unable or difficult to collect and may reduce the need for multiple devices. User preferences will influence the choice between a single-feature or a multimodal device. The following criteria should be considered in selecting a mobile ID device to fulfill agency needs:

**1**  
Identifying Needs  
for a Mobile  
ID System

**2**  
Understanding  
Mobile ID System  
Capabilities  
*CONTINUED*

**3**  
Considerations for  
Procurement of a  
Mobile ID System

- **Capture requirements** – a department seeking to fulfill a specific capture need independent of other biometric identification methods should consider a single-feature device; however, if the agency uses other biometric measurements for identification, such as iris or facial recognition, then a multimodal device should be considered.
- **Size** – mobile ID device size can range from a compact device that fits easily in the palm of a hand to a device that requires both hands for operation. More compact designs are easier to manipulate and maneuver. Larger devices have proven to be difficult to use for identification of the deceased.
- **Cost** – mobile ID devices range in price from as much as \$1,000 for single-feature devices to \$4,000 or more for multimodal devices. Increased device capability results in a higher price, but may be attractive depending on an individual agency’s needs.
- **Training requirements** – device simplicity reduces learning curve and training time required for use. In some cases, device training only takes a matter of minutes and consists of a short presentation.
- **Robustness and durability** – mobile ID devices must be durable and robust enough to withstand all environmental conditions that will be encountered during use. Devices may be subjected to dropping, moisture exposure, and dusty conditions.



*Multimodal devices are functional—but some users would rather have a smaller device to obtain fingerprints alone ... it takes a lot of effort to move a deceased body around a fingerprint scanning device.*

**Aaron Uhle and Jeff Carlyle**  
FBI Laboratory - Latent Print Support Unit



## Accuracy is important to all mobile ID devices and is validated by field trials and pilot studies

### Lack of distinction between image resolution and accuracy causes confusion

Image resolution and accuracy are two commonly discussed, and sometimes misinterpreted, aspects of mobile ID devices. Image resolution (measured in dots per inch [dpi]) is the amount of detail that an image holds—higher-resolution images may contain more print features that could be used by a fingerprint examiner or matching algorithm to yield a positive match.

Match accuracy is more difficult to define, but generally refers to the likelihood that a match is correctly made using feature analysis and matching algorithms. Fingerprint condition, collection process, and algorithm robustness all affect match accuracy. Device accuracy can be judged by comparing results and match success rates of multiple devices that are used to analyze a common subject pool. However, this relative determination of accuracy is not necessarily indicative of field performance during operational use. In the end, the suitability of device and algorithm accuracy is established based on field pilot and actual use.

1  
Identifying Needs for a Mobile ID System

2  
Understanding Mobile ID System Capabilities

CONTINUED

3  
Considerations for Procurement of a Mobile ID System

The National Institute of Standards and Technology (NIST) conducts routine comparative testing of commercial vendor fingerprint match algorithms (Fingerprint Vendor Technology Evaluation). Potential device users can investigate the results of this neutral third-party testing at [www.nist.gov/itl/iad/ig/fpvte2012.cfm](http://www.nist.gov/itl/iad/ig/fpvte2012.cfm).

The image resolution for most mobile ID devices is typically 500 dpi. While some technology developers and practitioners seek out image resolution closer to 1000 dpi, others advocate for stronger matching algorithms to increase accuracy instead. Increasing image resolution will also demand greater storage requirements; doubling resolution from 500 dpi to 1000 dpi requires approximately four times more storage space. Larger image file size will also lead to longer data transmission times. Increased sensor area for collection of multiple finger or palm prints also produces larger images that restrict the number of files that may be stored on a device. The FBI designates FAP numbers to certified mobile ID devices to indicate image quality and capture dimensions.

### NIST uses image scan quality to predict accuracy

NIST has developed a fingerprint image quality measurement, the NIST fingerprint image quality (NFIQ) algorithm, which analyzes fingerprint images and assigns a quality value of 1 (highest quality) to 5 (lowest quality) to an image. Higher-quality images produce significantly better performance with matching algorithms.





## A strong acquisition strategy depends on defined user needs and sufficient resources

After consideration of what is needed in a mobile ID system, development of an acquisition strategy is important. Successful mobile ID acquisition depends on requests for information (RFIs) and requests for proposals (RFPs) with well-defined user requirements. Benchmark testing is very important for successful selection and implementation of mobile ID systems. After RFIs and RFPs have been written, vendors should demonstrate system capabilities, and the system should be tested by the implementing department with its own datasets and by its own users.

An acquisition strategy should include budget allocation for a mobile ID system or an alternative plan if budgetary means of individual departments, offices, or agencies are limited.

**1**  
Identifying Needs for a Mobile ID System

**2**  
Understanding Mobile ID System Capabilities

**3**  
Considerations for Procurement of a Mobile ID System

- **Inclusion in a larger AFIS implementation RFP** – In some cases, it may be possible for a smaller department or agency to be included in a law enforcement agency's RFP for an AFIS system. In addition to potential cost sharing, inclusion in the larger program may grant access privileges.
- **Standalone device purchase** – If departments do not have the funding to elaborately integrate mobile ID technology into an AFIS system, a mobile ID device may still be bought and used to capture prints. These prints can be manually uploaded to a computer and sent to law enforcement or other state agencies for an AFIS search. Storage capacity of the device is important to consider for standalone.

*Illinois put three fingerprint examiners on their team to build an RFI for their AFIS system – they interfaced with state budget individuals to finance the project and make cost decisions. The collaboration went well, and as a result, Illinois has a system that performs in the top five of AFIS systems in the United States in terms of identification rates. The right people made the right decisions, and a very thorough job was done in determining requirements and what customer needs were.*

**Garold Warner**  
US Army Criminal Investigation Laboratory





## AFIS Interoperability Working Group has developed procurement and implementation guidance

AFIS systems allow print examiners to search fingerprint files and transmit fingerprint images. However, examiners often lack the technological ability to access AFIS in neighboring jurisdictions. To address a lack of AFIS interoperability, NIST and the Department of Justice’s National Institute of Justice (NIJ) convened the Latent Print AFIS Interoperability Working Group, whose mission is to improve latent print AFIS interoperability by developing a clear understanding of the challenges at hand and identifying collaborative ways to address the problem.

### Guidance for procurement and implementation of mobile ID technology

**1**  
Identifying Needs for a Mobile ID System

The Latent Print AFIS Interoperability Working Group has developed documents to guide agencies in implementation and use of AFIS systems to maximize AFIS interoperability. Select documents that may be of interest to the reader are highlighted below (links to download and a full list of documents can be found on the working group website: [http://www.nist.gov/oles/afis\\_interoperability.cfm](http://www.nist.gov/oles/afis_interoperability.cfm))

**2**  
Understanding Mobile ID System Capabilities

- **Writing Guidelines for Requests for Proposals for Automated Fingerprint Identification Systems** – Provides agencies with an overall guide to critical conditions and decisions, allowing agencies to develop a clear and succinct RFP, detailed responses for evaluation, and the implementation of AFIS with minimal frustration and delay. The document incorporates input from AFIS practitioners, examiners, users, and vendors.

**3**  
Considerations for Procurement of a Mobile ID System  
*CONTINUED*

- **Writing Guidelines to Develop a Memorandum of Understanding for Interoperable Automated Fingerprint Identification Systems** – Provides agencies with a guide to develop an AFIS interoperability memorandum of understanding (MOU) between two or more agencies to facilitate shared access to cross-jurisdictional AFIS information.

For additional information, agencies should consider contacting procurement officers of other agencies that have adopted mobile ID technologies and/or manufacturer representatives to obtain guidance and other useful information to assist with procurement and implementation processes.

The specifications, instructions, and guidelines developed by the Interoperability Working Group build upon the American National Standards Institute/NIST, Information Technology Laboratory standard entitled “American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information” (ANSI/NIST-ITL 1-2011).







2	Overview
10	Use Profiles and Considerations
25	Product Landscape
32	Summary





## Products vary to address needs and considerations, including cost, complexity, and connection

Manufacturers offer a variety of solutions along the multistep fingerprint capture process. Full systems—which include mobile handheld devices, software applications, servers, and AFIS database systems that complement existing local, state, and federal AFIS databases—are offered by leading technology providers, but individual components can also be purchased. If parts are purchased separately, compatibility of products between different manufacturers is important and should be considered when acquiring products.

Comparing products between different providers is challenging due to the different ways product capabilities can be presented.

Handheld devices range from single-feature to multimodal capture devices. Accessory devices that attach to existing mobile devices are also available, reducing the overall cost for investment.

Software applications are becoming increasingly important as mobile devices become more ubiquitous. A few latent print examination software applications that operate on existing mobile platforms and provide real-time identification have recently launched.

### Multistep Fingerprint Capture Process



#### Product Type

#### Purpose

Handheld Devices	Capture fingerprint information while in the field
Applications	Directly run on the handheld device or to connected smartphones, tablets, and/or laptops
Servers	Store mobile transactions and forward the search request to automated biometric identification systems
AFIS Database	Local, state, and federal AFIS systems



## Four technology providers lead the AFIS market

The four leading technology providers of mobile ID fingerprint capture technologies are 3M Cogent, Cross Match Technologies, NEC Corporation, and SAFRAN MorphoTrak.

According to Frost & Sullivan, SAFRAN MorphoTrak was the 2011 AFIS market leader, holding 44% of the market share of total global sales, while 3M Cogent, NEC Corporation, and Cross Match Technologies held 20%, 15%, and 11% of the AFIS market share, respectively.

3M Cogent, Cross Match Technologies, and SAFRAN MorphoTrak are the market leaders for standalone mobile ID fingerprint devices.

NEC Corporation currently does not have a commercialized, FBI-certified mobile ID fingerprint device. NEC's flagship mobile ID fingerprint product is its fingerprint matching software; the company partners with other manufacturers for hardware.



### 3M Cogent

[www.cogentsystems.com](http://www.cogentsystems.com)

Provides various biometric identification solutions and is a wholly owned subsidiary of 3M Company within the Security Systems Division. The company was formerly known as Cogent, Inc., prior to its acquisition by 3M Company.



### Cross Match Technologies

[www.crossmatch.com](http://www.crossmatch.com)

Manufactures multimodal biometric identity management solutions. Solutions are based on the capture and processing of the unique physical characteristics of individuals for a wide range of standard and custom applications.



### NEC Corporation

[www.nec.com](http://www.nec.com)

Provides safe, secure, and efficient social solutions by combining its distinctive technology assets, including networking and sensing technologies, with broad systems integration expertise and customer assets.



### SAFRAN MorphoTrak

[www.morphotrak.com](http://www.morphotrak.com)

Provides multi-biometric technologies and serves a wide range of security needs. The company was formed from the merger of Sagem Morpho, Inc and Motorola's biometric division, Printrak. Its global parent is Morpho.

Source: "Analysis of the Automated Fingerprint Identification Systems Market Understanding opportunities for growth," Frost & Sullivan, 2012.



## Several component manufacturers and emerging companies are influencing mobile ID fingerprint

The mobile ID fingerprint capture market is a growing field with an increasing number of new players.

Integrated Biometrics has been cited by several practitioners and technology developers as “a company with game-changing fingerprint sensor technology that will revolutionize mobile ID fingerprint devices.” The company offers both standalone mobile ID devices as well as component fingerprint sensors that can and have been integrated into other devices.

Emerging companies, such as Biomorf, are developing and launching new, advanced multimodal devices. Biomorf’s device captures flat, rolled, and latent prints as well as other identification features. New multimodal products are gaining international interest and use, but may not yet have gained a strong hold in the U.S. market.

Technology developers, such as Fulcrum Biometrics and AOptix, take advantage of existing mobile devices and provide accessory attachments to capture fingerprints.



**Integrated Biometrics**  
[www.integratedbiometrics.com](http://www.integratedbiometrics.com)

Offers miniaturized, FBI-certified fingerprint sensors, which include standalone device or embedded parts that can be integrated into other fingerprint capture devices.



**Biomorf**  
[www.biomorf.co.id](http://www.biomorf.co.id)

Offers a customizable, multimodal mobile ID device capturing flat, rolled, and latent prints. Products have been used internationally.



**Fulcrum Biometrics**  
[www.fulcrumbiometrics.com](http://www.fulcrumbiometrics.com)

Offers FBI-certified fingerprint scanning accessory attachments for mobile devices with an Apple® iOS platform (i.e., iPod, iPhone, and iPad).



**AOptix**  
[www.aoptix.com](http://www.aoptix.com)

Offers FBI-certified fingerprint scanning accessory attachments for the iPhone.








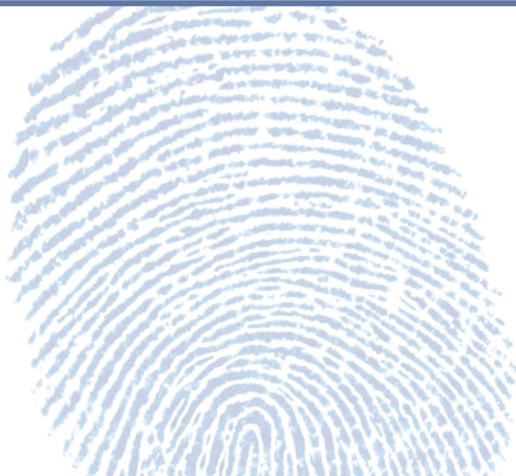


## Single-feature mobile ID devices provide limited functionality at an attractive price

### SINGLE-FEATURE DEVICES

Relative Cost  
 \$: <\$1,500  
 \$\$: \$1,500-\$3,000  
 \$\$\$: >\$3,000









	3M Cogent		Cross Match Technologies	SAFRAN MorphoTrak	
					
	<b>Bluecheck® II</b>	<b>Bluecheck® II U</b>	<b>Verifier® Mw</b>	<b>IBIS Extreme</b>	<b>Morpho-IDent</b>
FAP	10	10	30	30	10
Dimensions (in)	4.5 x 1.9 x 0.8	4.5 x 1.9 x 0.8	1.9 x 8.0 x 1.9	9.7 x 2.6 x 2.5	5.2 x 2.6 x 0.7
Display (in)	1.7	1.7	2.0	-	2.4 touch screen
Weight	4.59 oz	4.94 oz	1.4 lbs	0.99 lb	5.3 oz
Sensor	Optical	Capacitive	Optical	Optical	Optical
Image Resolution (dpi)	500	500	500	500	500
Capture Type	Flat	Flat	Flat	Flat	Flat
Relative Cost	\$	\$	Cost data not available	Cost data not available	Cost data not available





## Multimodal devices include multiple sensors and cameras to capture a range of biometric data

### MULTIMODAL DEVICES

	3M Cogent			Cross Match Technologies		SAFRAN MorphoTrak		Biomorf
Relative Cost \$: <\$1,500 \$\$: \$1,500-\$3,000 \$\$\$: >\$3,000								
	MI2	MI3	Fusion	SEEK II	SEEK Avenger®	Morpho-Check™	RapID™ 1100	Trident
FAP	20	30	30	45	45	10	20	45
Dimensions (in)	6.8x3 x 1.6	7.8x3.5x2.5	8.7x4.6x2.9	8.8x5.6x3.5	9.5x6.2x1.8	Not available	Not available	10.4 x 6.6 x 3.5
Display (in)	3.5 touch screen	3.5 touch screen	3.5 optional touch screen	4.1 touch screen	5 touch screen	3.7 touch screen	3.7 touch screen	5.0
Weight	0.91 lbs	1.4 lbs	1.2 lbs	3.6 lbs	3.2 lbs	16 oz	Not available	< 3 lbs
Sensor	Optical	Optical	Optical	Optical	TFT*	Optical	Optical	Non-optical
Image Resolution (dpi)	500	500	500	500	500	500	500	500
Capture Type	Flat	Flat	Flat & Latent	Flat & Rolled	Flat & Rolled	Flat	Flat	Flat, Rolled, & Latent
Other Capture	Facial	Facial	Facial & Iris	Card Reader**, Facial, Iris	Card Reader**, Facial, Iris	Card Reader**	Card Reader** (optional)	Facial, Iris, & Card Reader**
Relative Cost	\$	\$\$	\$\$\$	Cost data not available	Cost data not available	Cost data not available	Cost data not available	\$\$\$
Additional Notes	-	-	Stores 100,000+ (scalable) records	Stores 120,000 records; operates in direct sunlight	Stores 250,000 records; operates in direct sunlight	-	Stores 180,000 records	Uses a dual finger capture





\*Thin-film transistors.

\*\*Card Reader may refer to contact or contactless radio-frequency identification (RFID) card reader, 2D barcode reader, and/or Machine Readable Zone (MRZ) swipe reader. Please contact the respective device manufacturer for specific card reader options.



## Accessory devices and latent print software take advantage of existing mobile platforms

### ACCESSORY DEVICES & SOFTWARE

	AOptix	Cross Match Technologies	SAFRAN MorphoTrak	Fulcrum Biometrics
				
	<b>Stratus MX</b>	<b>Quad Reader for SEEK II</b>	<b>BA500</b>	<b>FbF mobile-One</b>
Relative Cost	\$: <\$1,500 \$\$: \$1,500-\$3,000 \$\$\$: >\$3,000			
FAP	10	45	30	10
Dimensions (in)	6.0x3.1x1.5	4.3x5x2.3 (attachment only)	Not available	6.3 x 2.6 x 0.9 (attachment only)
Display (in)	3.5	None on attachment	None on attachment	None on attachment
Weight	9.4 oz (attachment only)	7 oz (attachment)	Not available	6.4 oz (attachment only)
Sensor	Capacitive	Optical	Optical	Capacitive
Image Resolution (dpi)	508	500	Not available	508
Capture Type	Flat	Flat & Rolled	Flat	Flat
Other Capture	Iris, Facial	Card reader*, Facial, Iris	-	Facial, Voice
Relative Cost	Cost data was not available			\$
Additional Information	Based on iPhone®, full Open Architecture with Client SDK for Apple® iOS	Quad Reader is an attachment to the SEEK II Device, which stores 120,000 records	-	Fingerprint scanner accessory compatible with Apple® iOS platform

### Latent Print Software

Latent print software applications often take advantage of existing mobile platform devices, like the Apple iPad. Software companies (i.e., Dataworks Plus and NEC) partner with hardware developers to collectively create a mobile ID system. Use of existing hardware platforms ultimately reduces the cost of investment when acquiring fingerprint capture systems, but can increase interoperability complexity and may possess overall reduced device durability.

Example latent print matching software includes the following:

- NEC Corporation's Neoface® Smart ID.
- SAFRAN MorphoTrak's MiCrimeScene.
- Datawork Plus's SAF-ID/ RAPID-ID.

\*Card Reader may refer to contact or contactless radio-frequency identification (RFID) card reader, 2D barcode reader, and/or Machine Readable Zone (MRZ) swipe reader. Please contact the respective device manufacturer for specific card reader options.



2	Overview
10	Use Profiles and Considerations
25	Product Landscape
32	Summary







## To gain the benefits that mobile ID devices can offer, agencies must overcome barriers that hinder implementation

### Investigative Benefits

- **Time savings:** Mobile ID devices require less time to collect and submit prints to AFIS systems. Interoperable mobile ID devices that are paired with AFIS systems can deliver results within seconds via wireless communication, and multi-jurisdictional AFIS searches can be conducted to improve hit probability.
- **Fingerprint quality:** Scans can be easily repeated using a mobile ID device to collect high-quality images. Instant view of fingerprint images, in some cases with an indication of quality (using the NIST Fingerprint Image Quality algorithm), allows investigators to screen out poor-quality images.
- **Portability and maneuverability:** Mobile ID devices are handheld and can be carried into the field for crime or death scene investigations. Devices can weigh less than a pound and can be held in the palm of one's hand, making it easier to collect fingerprints from the deceased.
- **Capture of multiple biometric features:** Beyond fingerprints, multimodal mobile ID devices are capable of capturing a variety of biometric information, including iris scans and facial recognition images.

### Implementation Barriers

- **Funding:** Agency budgets are often limited, and capital expenditures are difficult to justify. Key decision makers must be educated on potential technology benefits to create agency buy-in.
- **Procurement process:** Successful RFP development, proposal review, contract award, and implementation requires time and dedication of many individuals. A procurement team heavily constrained by time should be careful not to lean too heavily on vendor recommendations.
- **Procedural change and adoption:** Implementation of mobile ID devices will require a potentially difficult change of departmental operating procedures. End users may be slow to incorporate mobile ID devices into existing workflow and procedures if they are uncomfortable or unfamiliar with the technology.
- **AFIS access:** Mobile ID device users seeking access to extra-jurisdictional AFIS databases (requesting agencies) must establish an agreement with AFIS database administrators (hosting agencies).





## To learn more about mobile ID technology, consider these additional resources

### Department of Homeland Security

- Mobile Fingerprint Biometric Devices Focus Group Recommendations. System Assessment and Validation for Emergency Responders (SAVER). September 2008.

### Federal Bureau of Investigation

- Electronic Biometric Transmission Specification. Appendix F: FBI/CJIS Image Quality Specifications. <https://www.fbibiospecs.org/docs/Master%20EBTS%20v10%20-%20FINAL%2020130702.pdf>
- IAFIS Certified Products List. <https://www.fbibiospecs.org/IAFIS/>
- IAFIS Frequently Asked Questions. [https://www.fbibiospecs.org/iafis\\_FAQ.html](https://www.fbibiospecs.org/iafis_FAQ.html)
- Image Quality Specifications for Single Finger Capture Devices. Personal Identity Verification Program (United States government). <https://www.fbibiospecs.org/docs/pivspec.pdf>

### Frost & Sullivan

- A Best Practices Guide to Fingerprint Biometrics – Ensuring a Successful Biometrics Implementation. August 2011. [www.frost.com/prod/servlet/cpo/240303611](http://www.frost.com/prod/servlet/cpo/240303611)

### National Institute of Justice & National Institute of Standards and Technology (NIST)

- Latent Print AFIS Interoperability Working Group. [http://www.nist.gov/oles/afis\\_interoperability.cfm](http://www.nist.gov/oles/afis_interoperability.cfm)

### NIST

- Special Publication 500-280, NIST. Mobile ID Device Best Practice Recommendation. <http://www.nist.gov/itl/iad/ig/upload/MobileID-BPRS-20090825-V100.pdf>
- Special Publication 500-290, ANSI/NIST-ITL 1-2011 American National Standard for Information Systems. Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. [http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=910136](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136)
- NIST Fingerprint Image Quality. [http://www.nist.gov/itl/iad/ig/development\\_nfiq\\_2.cfm](http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm)