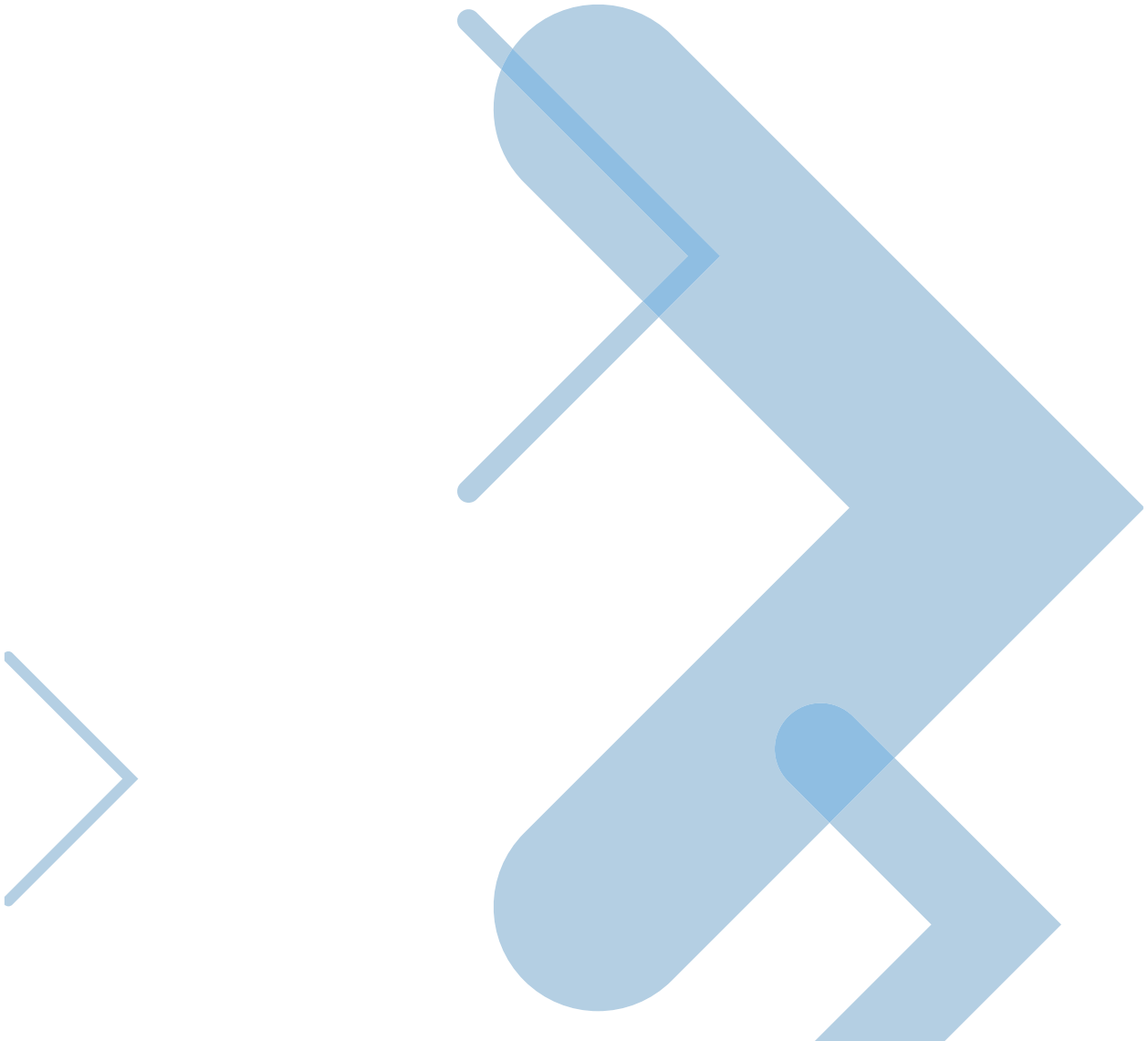
WHITE PAPER

Mobile Biometric Identification



Adding a wireless dimension to biometric identification systems (BIS) provides a more efficient and reliable method of identity management across criminal justice and civil markets. Yet deploying cost-effective portable devices with the ability to capture biometric identifiers – such as fingerprints and facial images – is only part of the solution. Organizations must consider back-end infrastructure, secure methods of wireless connectivity, and the integration of mobile applications with existing business processes. An end-to-end, standards-based approach is required to deliver operational efficiencies, optimize resources and impact the bottom line.

Identity management in the palm of your hand

Mobile biometrics technology provides an important front-line security measure for both government agencies and commercial users. Based around a central biometric identification system (BIS), mobile biometric identification devices extend the functionality and capabilities of a static BIS by allowing users to capture fingerprints and facial images out in the field, and compare fingerprint minutiae templates or images against a biometric database, either stored locally on the device, or remotely in centralized biometric matching systems. Captured information can also be compared with that stored within RFID (Radio-Frequency Identification) tags, smartcards and other machine-readable identification documents (IDs).

In scenarios where information is stored remotely, the mobile biometric identification device communicates with a central database using common wireless technologies such as cellular, Wi-Fi or Bluetooth. If a positive match, known as a 'hit', is made during the comparison process, information associated with the individual in question – such as facial images, names and demographic data – is transmitted back to the mobile device.

How mobile biometric identification devices work

Mobile biometric identification devices are designed for intuitive operation, and incorporate a reader, scanner and camera for the capture of a biometric identifier (e.g. fingerprint or facial image), which is converted by software into digital format for storage and comparison against other records held in a BIS database. With top-tier mobile biometric solutions, images are analyzed for quality prior to capture and encoding, ensuring the best possible inputs for biometric matching. One to ten fingerprints can be captured, while alternative functionality is available in the case of an amputee or bandaged fingerprint.

During the conversion process, specific characteristics (or patterns) of the gathered information are identified by biometric software as match (or minutia) points. These match points are then processed using an algorithm into a value that can be compared against other biometric information in the database.

When implemented as part of a comprehensive biometric solution, the capabilities of mobile biometric identification are four-fold:

- 1:N local identification – capture and search fingerprints against a portable database stored on the handheld device, in situations where communications may be limited
- 1:N remote identification – perform searches of one or more biometric identifiers (i.e. fingerprints and facial images) against remote databases using records transmitted securely from the device via wireless technology
- 1:1 local verification – match one or more biometric identifiers against other known records to verify that the two are the same using a smartcard, barcode or other secure credential
- 1:1 remote verification – match one biometric identifier against another stored at a remote location to verify identity and establish that the record is maintained in the database

Building an end-to-end mobile biometric identification solution

At the core of any technology platform designed for multi-client/multi-role applications is the communications structure that enables objectives to be achieved in a wide variety of locations and situations. Mobilizing the functionality and capabilities of static BIS requires a combination of radio communications, mobile applications and AFIS, as well as the issuance of secured credentials.

BIS: Based around a core AFIS, the latest-generation biometric identification systems (BIS) offer full biometric integration – with the inclusion of fingerprints, palm-prints, facial images, descriptive data, signatures and documents. Known as multi-modal biometrics (or 'fusion' technology), this approach optimizes the results of search queries, consequently achieving more accurate responses.

Given that BIS comprise an extensive array of biometrics identification subsystems, utilities, workstations and software development kits (SDKs), it is important that commercial-off-the-shelf (COTS) hardware and software is specified. This ensures that an integrated, highly scalable and end-to-end, multi-modal system can be deployed using a standards-based, Services Oriented Architecture (SOA). Common BIS elements include:

- Data Server – a central repository (e.g. Oracle database) for storage and near-immediate retrieval of biometric identifiers, together with associated features and textual data (known as 'descriptor' data)
- Work stations – equipped with a camera and scanner to enable the capture, encoding and submission of finger/palm-print images, slap impressions, rolled fingerprint images, photographs, signatures and demographic information
- Review stations – designed for the dedicated review and verification of search results, as well as match analysis
- Live verification stations – allow the identification of individuals when the subject is present at the time of processing
- Optional peripherals – portable and single-finger scanning devices, cameras, two/ten-print card printers, automated case management systems, web servers, application servers, mobile gateways, descriptor import/export modules

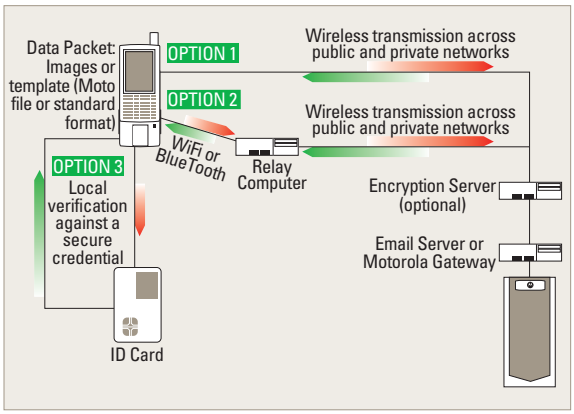
Wireless options: Radio communications are used to facilitate both local and wide area network (WAN) connectivity between mobile biometric identification devices and remote BIS databases. Current wireless network options include:

- WAN – wireless transmission across private or public cellular network (i.e. GSM EDGE, HSDPA or CDMA-EVDO Rev.0 / Rev .A), with data security achieved via encrypted VPN technology
- Local area connectivity – mobile biometric identification devices incorporate integrated Wi-Fi and Bluetooth antennas for longer-range wireless local area network (WLAN), and short-range personal area network (PAN) connections, respectively

When specifying the method of WAN connectivity employed for transmissions between the mobile biometric identification device and remote database, it is important to recognize that a service provider's network coverage will, ultimately, determine availability. In addition, private wireless networks are significantly more expensive than their public counterparts.

Cellular or Wi-Fi are the preferred modes of wireless communication where sensitive data is being exchanged, because it is not possible to encrypt Bluetooth® transmissions to a government-certified level. Wi-Fi is a particularly flexible option since it allows connectivity with remote databases via both public and private Wi-Fi hotspots, as well as Wi-Fi enabled laptops. The latter are able to store a local AFIS database, or act as a relay by using an external modem (located in a car for example) to transmit over the WAN via a cellular network. Transmissions can be encrypted using VPN technology.

Mobile Identification Workflows.



Messaging gateway or email server: A dedicated server is required to facilitate data transfer between mobile devices and the remote BIS database. By installing a purpose-designed messaging gateway for mobile biometric identification, the information returned from the remote database can be filtered according to the logical workflow requirements of the end-user organization. For example, the 'hit' or 'no hit' message can be delivered to the mobile biometric identification device first, followed by the name of the individual in question, then the demographic information and lastly the facial image (which is the largest file-type) – thus speeding response times.

Although many organizations have a legacy email server that can fulfill the role of messaging gateway, the drawback here is that the entire search response must be sent in an encrypted email. The resulting file size means an increase in response time, plus increased transmission time from the mobile biometric identification device to the central BIS database.

Secured credentials: Typically employed for a number of identity management applications requiring 1:1 verification (e.g. verifying ownership of an ID card or passport), secured credentials can take a number of forms:

- 1D barcode – a conventional linear barcode with a single row of bars, whereby data is encoded in the horizontal width (only a limited amount of data can be stored)
- 2D barcode – data is encoded in both the horizontal and vertical dimensions, thus increasing information capacity
- Contact smartcard – pocket-sized card with embedded circuit for data storage and gold-plated contact pads, which, when inserted into a reader, make contact with electrical connectors that can read information from the chip and write information back
- Contactless card – an integrated RFID chip that requires only close proximity to an antenna in order to complete data exchange
- ePassports/eDocuments – machine-readable documents storing biometric identifiers on embedded RFID chip (e.g. for ePassports, ICAO recommends storage of three biometrics: mandatory photograph; optional two fingerprints and iris)

Integrated & interoperable mobile biometric identification

Giving field agents access to fast and accurate data improves operational efficiencies, optimizes resources and enhances community safety. Mobile identification enables agents to maintain a presence in the field rather than having to commute to biometric access points to corroborate data. On-the-spot access to an individual's personal history enables users to make informed and rapid decisions about the necessary course of action. The ability to capture biometric and demographic information remotely and return this to a central BIS database via wireless networks also ensures that information is kept up-to-date.

As demonstrated above, specifying a mobile biometrics solution calls for a multi-disciplined approach and it is therefore vital to identify vendors with expertise and experience in integrating several technologies to form an end-to-end identity management platform. Implementing low-cost biometric devices without fully considering how information captured at a remote location will be securely transmitted back to the central database, authenticated, and the result transmitted back to the remote check point, can lead to poor performance and additional ongoing costs in the form of solution upgrades and integration projects. Indeed, such requirements may be needed simply to fulfill an organization's original objectives if all the variables are not identified at the onset.

It is also necessary to consider how existing database information and other back-office resources can be integrated with the new data that Mobile biometric identification tools provide. An open, standards-based approach at infrastructure level has enabled organizations to realize dramatic reductions in hardware procurement costs and a long-term reduction in maintenance and support expenditures. As with many systems implemented by multiple technology partners, interoperability and data exchange in a common format is essential to success and there are a number of identity management initiatives aimed at achieving closer collaboration between agencies, jurisdictions and countries being explored.

On-the-spot mobile biometric identification

In its conventional form, a BIS comprises a 'multi-modal' biometrics solution for investigation, identification and verification in both criminal and civil scenarios. Today, a BIS is able to process and store fingerprints, palm-prints, facial images, descriptive data, signatures and documents. With mobile biometric handheld devices, all these capabilities are made available to field agents at the touch of a button via a hand-held device. Confident that an individual can be positively identified and their credentials accurately verified, users can make rapid on-the-spot decisions and take appropriate action. Indeed, it is reported that mobile biometric identification devices have proven to be a positive deterrent to persons attempting to conceal their true identity.

Since its commercial introduction in 2004, mobile biometric identification devices have been successfully deployed across a myriad of applications:

Border Patrol: At air, land and sea border control points, mobile identification is proving an essential element of government strategy aimed at strengthening immigration control and ensuring effective identity management. Providing an easy way to add security without slowing the traveler down, it enables immigration officials to verify the identity of individuals against secure credentials such as visas, ID cards and ePassports (machine-readable passports that can include a facial and/or finger and iris biometric).

In Switzerland for example, mobile biometric devices now form part of a comprehensive BIS employed by the Swiss Border Guard at 70 border control points. In 2005, more than 18,000 prints were checked against the BIS database of the national police (fedpol) and over 5000 positive identifications were made. More recently, fedpol used mobile biometric identification devices for discreet border control in crowded areas during the UEFA Euro 2008 soccer championships.

Enterprise Security Operations: Using mobile devices, security officials can verify the identity and access privileges of employees that have been issued smartcard or RFID-enabled ID badges. If a security officer encounters a suspicious person, they can use their handheld biometric identification device to scan a contact smartcard or RFID badge, capture a fingerprint and perform immediate verification of that person against their ID.

Access privileges can be viewed to confirm the individual's granted permissions and, if connected wirelessly to remote servers, security personnel are able to access information about employment or privilege status in real time.

Event Security: At large events, such as music festivals, political rallies or sporting events, security personnel are often tasked with managing unruly attendees or safeguarding secure areas. Mobile biometric handhelds enable the capture, transmission and search of biometric information against remote databases, while smartcard-enabled ID badges allow a 1:1 comparison of a fingerprint stored on an ID badge, with that captured on the spot via the integrated fingerprint sensor. Event security personnel are therefore able to verify instantly the authenticity of an ID badge, and confirm an individual's access privileges.

Health Care: In hospitals, handheld biometric devices are used to identify and positively relate patients to issued prescription, medication dosage levels, symptoms, or other necessary information. This is especially important in scenarios where a patient has lost consciousness or is unable to communicate. Capturing a fingerprint, barcode, or data held on an RFID-issued tag and submitting it to a hospital central system allows such details to be retrieved immediately and viewed on the mobile biometric identification device.

Local law enforcement: Officers on patrol use Mobile AFIS to identify individuals and connect them to their records – during gang enforcement operations, traffic ticketing, cite and release procedures, narcotic investigations, missing person inquiries, and many other security activities. Response data can include a facial image, biographic data, criminal history and 'wanted' and 'warrants' information. Additionally, color-coded responses can be used to inform officers of any immediate threat levels or security risks associated with the person in question.

The United States National Capital Region (NCR) for example, is served by one of the most sophisticated, interoperable AFIS networks deployed to date. Known as the NCR-AFIS and connected across agencies, jurisdictions and states, it allows for identifications even when the arrestee may not be in the local or state database. Comprising the regional systems of Northern Virginia (NOVARIS), Montgomery & Prince George's Counties (RAFIS) and Washington DC (DC-AFIS), the NCR-AFIS allows each agency to communicate and collaborate by searching each other's biometric database.

The result has been an increase in identifications and solved crimes. According to one senior police officer closely involved with the project, wireless 'hits' are being made within 45 seconds of a search query being made on a remote database, and within 90 seconds when a search is conducted via the remote database of another agency within the regional system. The use of multiple identifiers, such as mugshots and facial recognition data, has also improved the reliability of results, by reducing the likelihood of a poor sample compromising data integrity.

Refugee Management: Deployed by a number of countries as part of immigration control, mobile biometric identification allows officers to cross reference a claimant's identity against both national and international databases, and has significantly reduced the number of refugee/asylum applications being made under false identities. In addition, mobile biometric devices can be used in evacuation shelters, hospitals, and morgues to positively identify individuals following an emergency or regional disaster.

Social Benefits Management: Being able to verify the identity and check the status of benefits claimants in real-time allows authorized field management personnel to ensure that they receive the correct assistance, validation of benefits and in a timely manner while overcoming the possibility of duplicate claims.

Mobile biometric identification device options

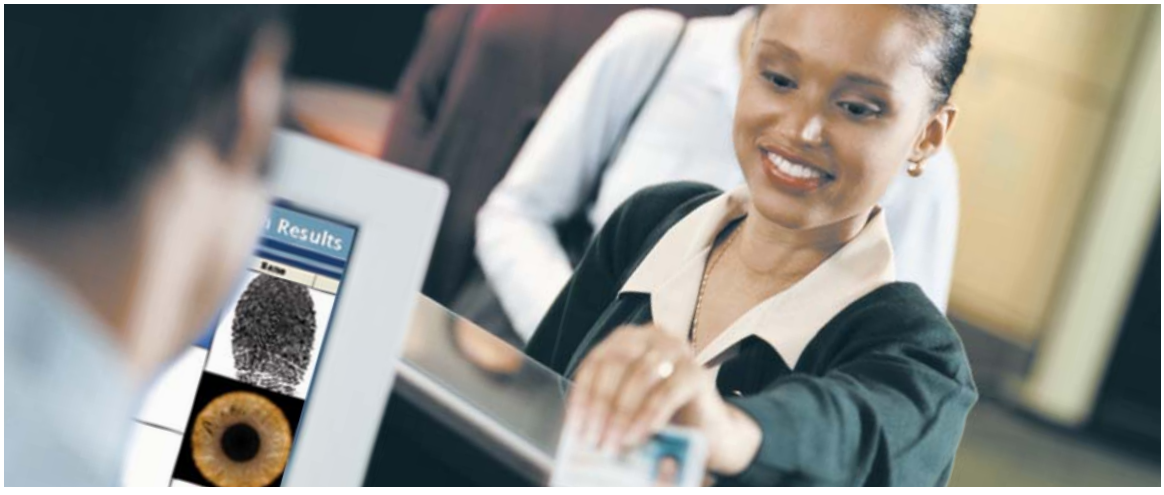
Available in a variety of form factors and configuration options, niche mobile biometric identification devices range from standard PDAs and laptops running mobile biometric identification software and peripherals, through to purpose-built and rugged hand-held portable units with integrated applications. Although niche devices have been the norm for mobile deployments, it is actual the rugged handheld portable computers that generate the greatest return on investment, because integrated solutions circumvents the need for additional hardware as an organization's operational requirements evolve and grow in scope. For example, an organization can leverage the rugged handheld devices to also deploy eCitation / code enforcement, first responder and accountability, inspections / maintainence, asset managment and mobile data access / situational awareness solutions.

Latest generation mobile biometric identification computers incorporate a biometric FPIS201 certified fingerprint reader, ISO compliant contact and contactless card reader, physical QWERTY keyboards, phone with push-to-talk capabilities, integrated GPS, integrated 1D/2D barcode scanners for data collection, high-bright touch screen displays, and PDA computer functionality to run data applications. These features are combined into an ergonomically designed, lightweight (under 2 LBS) and ruggedized (5-ft drop / IP 54-rated) hand-held unit built for one-handed operation. Feature options vary according to make and model, but for superior field operations, a recommended configuration includes:

- Processing Power – PXA270 624 MHz X-Scale® processor
- Memory – 256 MB ROM/128 MB RAM (preferred) or 128 ROM/128MB RAM
- FIPS 201 Fingerprint Sensor
- ISO compliant contact and contactless card reader
- Wide Area Network (WAN) connectivity
  - 2.5G GSM/EDGE (850, 900, 1800 and 1900 MHz); CDMA-EVDO Rev.0

  or
  - 3G HSDPA (850, 900, 1800 and 1900 MHz); CDMA-EVDO Rev.A
- Wireless Local Area Network (WLAN) communications – Tri-mode 802.11 a/b/g (Wi-Fi)
- Wireless Personal Area Network (PAN) connectivity – Bluetooth® (Class II, v 1.2 or v 2.0)
- Global Positioning System – Integrated Assisted (A-GPS)
- 2MP Color auto-focus camera
- High bright 3.5" QVGA or VGA touchscreen display
- SDIO (Secure Digital Input/Output) memory card for expanded data storage
- Physical QWERTY Keyboard
- Integrated 1D/2D barcode scanner
- Rugged to withstand harsh environments

Mobile biometric identification devices can also be configured to submit standards-compliant templates (ANSI INCITS 378 or ISO SC37) or images (ANSI INCITS 381 or ISO SC37), enabling search on a variety of BIS systems. Demographic information is entered via the QWERTY keyboard or auto-populated via a barcode scanner, or contact/contactless card reader, while FIPS140-2 VPN (Virtual Private Network) or encrypted email transmissions ensure the security of data being exchanged over the wireless network.



About Motorola

As a trusted leader in biometric installations, Motorola is the secure choice for mobile identification solutions that meet your mission-critical needs. With more than 75 years of wireless innovations and over 30 years of biometric leadership, Motorola Mobile AFIS provides identification with unprecedented speed and accuracy in identity management applications and consists of industry proven software on industry leading hardware.

The Motorola MC7x Enterprise Digital Assistant (EDA) rugged handheld mobile device is the core of Motorola's mobile biometric identification solution. This compact, lightweight device combines multi-mode wireless networking, voice and data communications, and advanced data capture, in an enterprise productivity tool that can support nearly any application in any environment. GSA certified fingerprint capture supplies highest quality images within a variety of lighting conditions. Superior data processing functionality includes outstanding wireless performance and the highest quality local data processing to provide government and enterprise personnel with everything they need to accurately identify individuals and connect them to their records.

The Motorola Mobile AFIS solution can be integrated with other Motorola products, including its flagship Biometric Identification System (BIS) and Metro ID.

The foundation of the Mobile AFIS solution is our top selling MC7X series of handheld computers.

The Motorola BIS is a premiere offering incorporating industry-leading biometric matching algorithms, powerful storage and records management technology providing agencies unparallel accuracy and speed. The Motorola Metro ID is an enterprise biometric matching and storage subsystem delivering advance data management and security tools.

To learn more about Motorola's Hand-held biometric solution please visit www.motorola.com/biometrics and download specific product information on the MC70 or MC75, and Mobile AFIS solution.

When it comes to selecting a provider for your federal, state or local government mobility solutions, choose the industry leader with a long history of proven, innovative technology — Motorola.

With Motorola you enjoy technology that is second nature, so your workers can stay focused on the mission — not the technology — providing the productivity increase and instant information access needed to better protect and improve the delivery of services to your citizens.

MOTOROLA

Motorola, Inc.
1250 N. Tustin Ave.
Anaheim, CA 92807, USA
www.motorola.com/biometrics
Americas: +1 714 238 2000
Europe, Middle East and Africa: +43 1 79709 2222

BIO-WPMA-1