Mobile Biometric Capture, Look-up, and Identification

mobichk™, Mobizent’s mobile identification integrated hardware and software solution provides public safety with a better way to conduct Personal identification Checks in the field efficiently and effectively.
Deploying cost-effective portable, rugged and mobile devices with the ability to capture multiple biometric identifiers such as fingerprints is the next key step in providing criminal justice and civil employees with real tools for positive identification in the field. Departments must now consider complex infrastructures and secure communication connectivity to provide the integration of mobile applications into a new and improved business process. A complete revolution in how an agent in the field can obtain subject information in real-time will change the way every department does business.

How to identify a person in the field using mobichk™

Biometric technology provides a key component in security access for government agencies and commercial companies. These solutions are based around a central database containing biometric data about individuals. Mobile devices are extending these features by providing users the ability to capture fingerprints and other biometric data in the field and compare this data against a central database or even compare this data with information already stored on the device. mobichk™, Mobizent’s complete mobile hardware & software identity checking solution also provides a SmartCard reader so that captured data can be compared to a swiped SmartCard, scanned license or any ID. For Public Safety Agencies, where the biometric data is stored in an AFIS database, mobichk™, through the ruggedized handheld, can wirelessly communicate, with Cellular, WiFi, or Bluetooth and conduct a real-time comparison with a database of biometric data. If a match is found with the transmitted data a “hit” is returned to the officer along with criminal history data and in some cases a mugshot.

How mobichk™ works in the field

The mobichk™ device is built to allow an officer to intuitively use the application that contains a fingerprint and SmartCard reader attached to the Intermec Cn70 ruggedized handheld. The device provides a camera and barcode scanner, which are used to capture data and then digitally convert it so that it can be compared against the local or remote database of biometric data. The mobichk™ software will automatically check for quality images/data to ensure matching is accurate. The application allows any two fingers to be captured based on subjects’ finger availability and quality.

During the capture and quality analysis steps and depending on what application is being used, matching software may create minutia points for each image. The minutia data is used to match fingerprints using complex and industry standard algorithms. This minutia extraction can be done on the device, AFIS or other fingerprint database server. The mobichk™ software will provide the following basic modules for identity management:

1. **One-to-Many Local Search** - Use mobichk™ to capture the fingerprint and then conduct a search on the local Handheld. This works well in areas where wireless coverage is poor and where departments do not want to incur the expense of a wireless network.

2. **One-to-Many Remote Search** - Perform the same procedure of local data capture but send the fingerprint and other collected biometrics to a remote database, such as AFIS, to conduct the search and matching functions. This communication would provide secure and encrypted data as well as provide a digital signature as part of the capture.

3. **One-to-One Local Search** - This procedure would use the other features available on mobichk™ such as the SmartCard reader or barcode reader. The user would capture the fingerprint and also the SmartCard information and conduct a match on card to verify the individual.

4. **One-to-One Remote Search** - Again this performs the same function as the procedure above, but each piece of data is checked and matched against a remote database. Both the SmartCard reader data and the fingerprint data could be used to match an individual separately to determine a match in a remote database.

Because the mobichk™ solution is clipped-on to a handheld computer, many applications can be written to support the various requirements of government and commercial customers. The use of the camera, 2D and 3D barcoding, and audio recording is available on the CN70.
mobichk™ functions as the key collection device to allow customers to realize the benefits of mobility. The need for departments to get rid of antiquated systems and antiquated work processes and employ effective methods of data identity will improve not only the organization, but reduce cost and eliminate many time consuming tasks.

How to provide a complete Biometric Solution

A secure and reliable infrastructure is the key to any multi-customer and multi-role application to allow requirements to be achieved in a wide variety of situations and locations. Mobilizing this infrastructure requires the use of many wireless solutions (Cellular, WiFi, Bluetooth) along with a remote database infrastructure, such as AFIS, NCIC or a commercial database. The second key is the ability to issue secure credentials so that reliable data can be entered into these remote databases.

mobichk™ provides a full featured database to allow the collection and storage of Biometric Data. This database contains full biometric integration, with the capability to collect fingerprints, palm-prints, latent prints, facial images, text data, signatures, photos and documents. This database also provides the APIs required to interface with the varied AFIS solutions and commercial databases.

Given the extensive amount of identification data that can be collected along with the significant number of applications that can be supported, it is critical that the correct hardware platforms are specified by the customer. mobichk™ is the best platform to interface with this database and ensures that an integrated and high scaleable database can be deployed for each customer according to their particular requirements. The mobichk™ solution generally contains the following components:

Central Database Server - The central repository is a SQL server database for the collection and storage of biometric data together with other text data associated with a person or an event. The database can be hosted on Oracle if required.

Local Work Stations - Provides local users access to a Central Database to access the data. A complete web-based solution allows the user to conduct searches and build reports and enter data through the mobichk™ USB fingerprint sensor. The user can also enter data through other means by attaching to the database through local workstations.

mobichk™ Device - A snap-on to a ruggedized CN70 handheld device, that provides FAP 30 fingerprint device, HID SmartCard reader (Active and passive), magnetic Stripe as well as a 3MB pixel camera and barcode scanner on the handheld. See detailed specifications of the CN70 and the snap-on device at the end of this white paper.

Optional Peripherals - The CN70 provides many additional add-ons such as an UHF RFID tag reader and a snap-on scan handle along with a number of flexible communication and charging docks. Other portable devices can also be added to the workstation solution, such as a separate camera, ten-print reader and other devices that can be connected to the local workstation for other required data collection requirements.
mobichk™ functions as the key collection device to allow customers to realize the benefits of mobility. The need for departments to get rid of antiquated systems and antiquated work processes and employ effective methods of data identity will improve not only the organization, but reduce cost and eliminate many time consuming tasks.

**Wireless Approaches** - RF communications are used to provide both local and wide area network connectivity between mobichk™ and remote databases. This selection is key to performance for the user. Network options include:

- **WAN** - wireless transmission across private or public cellular network (i.e. GSM EDGE, HSDPA, LTE or CDMA-EVDO) with data security provide through the use of two factor authentication and encryption on all transmissions. When selecting the correct method of WAN communication between the mobichk™ device and the remote database, it is key to look at the coverage of each carrier and any canyon or blackout areas. This analysis will typically help in the selection of the correct network.

- **Local area connectivity** - mobichk™ provides integrated WiFi for long range local communications and Bluetooth for short-range local communications.

**Synchronization Server** - The mobichk™ solution can provide a dedicated message server to provide uninterrupted service between the device and any remote server. This message server can provide many enhanced features to include filtering, message formatting, and application enhancements.

However, mobichk™ can also use other messaging servers because an API is provided to allow any message server to communicate to the mobichk™ device.

**Credentialing** - mobichk™ provides a number of solutions in credentialing a person using the one to one verification against some type of ID card.

- **1D barcode** - a well known linear barcode with a single row of bars, where these bars are encoded to equal numbers and letters. Very little data is provided.

- **2D barcode** - popular new barcode is encoded in blocks of bars, which provides a greater, but still limited amount of data in the barcode image.

- **Contact SmartCard** - mobichk™ has a slot for contact cards, which contain an embedded circuit with data that can be captured when it is inserted into mobichk™, and data can be written back into the card, if allowed.

- **Contactless SmartCard** - mobichk™ provides an integrated HID certified chip that only requires close proximity to the mobichk™ device to exchange information.

- **eDocuments** - Any document that may embed multiple data points such as fingerprint, IRIS scan and photograph, such as passports on an RFID chip.
Integrated and interoperable mobile biometric identification devices such as mobichk™ can provide on-the-spot biometric identification. Giving field agents access to fast and accurate data improves operational efficiencies, optimizes resources and enhances community safety.

With mobile biometric handheld devices, we can collect all the required data to identify a person in the field, as long as the database provides the appropriate data to check against. When a user is confident that a subject can be positively identified and their credentials accurately verified, agents can make rapid on-the-scene decisions and take the appropriate action. It is proven that mobile biometric devices, such as mobichk™, have proven is a very positive deterrent to persons attempting to conceal their true identity.

**Corporate Security Operations** - Using mobichk™, security officers at commercial companies can verify the identity and access privileges of employees that have been issued SmartCards or RFID enabled ID badges that have been entered into the database. If upon entry or if an officer approaches someone who they feel are suspicious, they can use mobichk™ to scan the SmartCard and perform an immediate verification of that person against their ID. If the officer is connected wirelessly other functions can be performed.

**Border Patrol** - Securing a country’s border continues to be an issue all over the world. A mobile biometric device such as mobichk™ can provide an essential element aimed at improving immigration control and ensuring effective identity management. mobichk™ can provide an easy way to add security without slowing down the traveler and it allows immigration officers to feel confident that they are verifying credentials for visas, ID cards and passports.

**Event Security** - For sports, music, rallies and concerts events, security personnel are required to manage problem attendees and secure a perimeter. mobichk™ can enable the capture, transmission and search against available remote databases. The security officers can also check badges of local security and check for warrants of any attendee.

**Refugee Control** - As this becomes more and more of a problem throughout the world, mobile biometric devices, such as mobichk™ can allow officers to check a subject’s identity against national and international databases and can significantly reduce the number of refugees being admitted in the county without proper identification.

**Law Enforcement/Public Safety** - Officers in the field can use mobichk™ connected to AFIS and RIST to capture fingerprints in the field and ensure the person has no warrants. The mobichk™ software can filter the data to return a mug shot and other Criminal History data if required after a “hit” is returned to the device.

**Health Care** - In Heath Care facilities, the use of handhelds can greatly increase safety by positively identifying patients using biometrics. This ensures that the person is receiving the correct medication at the correct time. The devices can also aid, if the person is unable to communicate, by capturing a fingerprint, data can be immediately retrieved and displayed to the health care personnel.
Mobick is available in a variety of configurations and options that can provide the users with the most appropriate arrangement for the required solution. Providing a snap-on device allows users to leverage the rugged CN70 handheld to also deploy other solutions on the same device, such as citations, inspections, code enforcement, asset management and many other applications.

mobichk™ is the lastest generation of mobile identification computers, which incorporates a significant number of features to include a FIPS 201 FAP30 certified fingerprint reader, ISO compliant contact and contactless HID card reader, physical keyboard, available phone, optional cellular carriers, GPS, 1D/2D barcode scanner, 3MP camera, touch screen gorilla glass display, magstripe reader, full Windows Embedded Handheld 6.5 OS, under 2lbs, IP 64 rated handheld. And because this is a snap-on module the snap-on can be connected to a USB connector to be used with a PC. The snap-on provides the fingerprint reader, Smartcard readers and magstripe.

**Biometric Capture Specifications**
- FAP: 30
- Fingerprints: Flat
- Simultaneous Finger Capture: 1
- Multi-Modal: No
- Sensor: Thin Film Transistor
- Auto Capture: Yes
- Manual Capture: Yes
- Add-Ons: SmartCard (contact and contactless) reader
- Magstripe

**General Specifications**
- Weight: 1.32 lbs.
- Dimensions (in.): 10.5 (L) x 3.2 (W) x 1.6 (H)
- Display: 3.5 in. touchscreen
- Keypad: Qwerty or Numeric
- Brightness Adjustment: Yes
- IP Rating: 55
- Operating Temperature: 14 to 131 °F
- Battery Type: Li-ion 3.7 Volt, 4000 mAh
- Hot Swap Capability: Yes

**Fingerprint Records and Processing**
- Storage: 1,000 records
- Onboard Matching: Yes

Typical Match Speed: Under test
Match Result Display: Alert message/ biographical data/mugshot
Operating Systems: Windows Embedded Handheld 6.5 OS
FIPS 201 PIV sensor: Yes

**USB Attached mobichk™ Device**

mobichk™ also can provide a USB attached device that allows the same functions and features that are available on the CN70 to be available on a laptop or tablet running Windows. This will allow officers to use this with the laptop or tablet in their car.

**CN70 Specifications**
- Drop Survival: 2.4 m (8ft.) to concrete per MIL-STD 810G, 1.8m (6 ft) to concrete per MIL-STD 810G 2,000 (1m) tumbles per IEC 60068-2-32 specification
- Safety: cULus Listing – ISA/ANSI 12.12.01
- Gases: Class I – Groups A, B, C, D
- Dusts: Class II – Groups F, G
- Fibers and flyings: Class III
- Flash ROM: 1 GB Flash (800 MB available)
- Memory/Storage Extensions: Customer-accessible micro-SD slot for removable memory cards up to 32 GB RAM Memory: 512 MB RAM (384 MB available)

**Multi-Processor Architecture**
- Texas Instruments® OMAP 1 GHz multi-engine processor architecture
- Microsoft Windows Embedded Handheld 6.5
- Ea30 high performance motion-tolerant 2D Imager; white LED illumination; red laser aimer optimized for all lighting conditions; 35 degree downward scan angle; capable of scanning all common 1D and 2D barcodes; 1D as small as 5 mil; PDF as small as 6.6 mil; Data Matrix as small as 7.5 mil; and standard UPC codes from distances up to 33 cm (13 in).