Satellite Communications as a Viable Method for Biometric Record Transfer in Field Biometric Devices

Tänya L. Haberman, Christopher Miles, and Miguel A. Cardoza

Abstract— **The use of biometrics, and their associated handheld field devices, as an identification and verification technique is growing at a considerable rate. Governments and private organizations are making significant investments to identify and research new types of biometrics while pushing the industry to provide scanners capable of weathering field missions. In parallel, similar levels of investment are being made to build centralized databases that have the capability to query millions of records in a matter of seconds. While these investments push the biometric industry forward, lesser time has been invested into linking biometric scanners with a remote database. Commercially available scanners rely heavily on the evolution of the cellular industry or a satellite connected portable laptop to provide the necessary bandwidths required to transmit biometric records from the scanner to the remote database. This paper explores the use of satellite communications in handheld field sensors as a global communications link between biometric scanners and a remote database. The present work discusses and evaluates biometric type, file size, and satellite bandwidth for satellite communications on handheld field biometric devices. The paper concludes by identifying an emerging product, not yet commercially available, that integrates satellite technology into a product already capable of linking legacy wireless capable scanners with a remote database.**

I. Introduction

The use of biometrics is quickly becoming mainstream. From commercial applications, such as facial recognition security on personal laptops, to public sector applications, such as field biometric scanners in use by State and local law enforcement, the use of biometrics will soon be prolific in day-to-day society. This paper focuses on field biometric scanners for rapid identification and verification in use in the public sector, which in 2007 accounted for 64% of the revenues for the industry [1].

A. Matching Capabilities

To facilitate portability and utility, most handheld biometric field scanners capture a biometric record, compare the record to a limited onboard database, and if no match is achieved, pass the record to a remote database via a cellular communications network for query. System architecture limitations, however, often limit onboard minutiae database sizes to 10 thousand records. To match two fingers against a 10 thousand record database utilizing a Win CE, Xscale 520 MHz processor takes approximately 15 seconds while a 5000 record database requires half the time [2]. Therefore, the limiting factor of querying onboard handheld devices is the time required to make a match rather than the database size.

In comparison, a largest and fastest growing government biometric database, the Department of Homeland Security's (DHS) IDENT database, contains 100 million plus records, uses proprietary extraction and matching algorithms to query the database, and has the capacity to handle 225 thousand transactions per day [3]. Similar to these government databases, State and local biometric databases, which are much smaller in size compared to the government databases but are still large scale in comparison to the database on scanner devices, are on the order of 1 million records, employ industry standard extraction standards such as ANSI/INCITS-378 to generate extraction algorithms, and use commercially available matching algorithms to achieve match rates anywhere between 1 and 5 minutes per record.

This acute difference in matching performance between field scanners and a remote database is the driving force behind moving the database query from the handheld scanner in the field to a much larger and more comprehensive remote database.

B. Long Range Communications

For most State and local law enforcement applications, where the goal is to identify or verify individuals against a large database of records, there is an evident advantage of moving the query from the handheld scanner to the remote database. This is easily done via cellular networks. But too often during times of national disaster, such as Hurricane Katrina in 2005, cellular networks become overloaded due to high traffic volumes, thus rendering cellular linked devices ineffectual at a time of high need [4]. Or where cellular networks are not available, such as significant sections of the 6000 miles of border that separate the U.S. from Mexico and Canada or the 2000 miles of coastal water surrounding the Florida peninsula and the island of Puerto Rico. For example, the Mona Pass where it is common for United States Coast Guard cutters to intercept boats of migrants attempting to illegally cross the US border [5]. It is therefore of interest to investigate linking biometric scanners with a remote database via a satellite network. In times when terrestrial

Manuscript received June 7, 2009. This work was supported in part by the U.S. Department of Homeland Security under contract NBCH-C-09-0015.

Tanya L. Haberman is with Trident Research LLC, Austin, TX 78758

Christopher Miles is with the U.S. Department of Homeland Security, Science and Technology Directorate, Human factors Division, Washington, DC 20528

Miguel A. Cardoza is with Trident Research LLC, Austin, TX 78758

communication networks do not exist or are inefficient, the integration of satellite communications to bridge the gap between field biometric scanners and a remote database improves the utility and effectiveness of biometric scanning in the field. One possible bridging mechanism presently under research and development via the DHS Small Business Innovation and Research (SBIR) program is a portable, global biometric gateway [2].

The global biometric gateway connects multiple legacy and emerging field operable handheld biometric scanners equipped with 802.11-based wireless capability to continental United States (CONUS)-based biometric databases by providing a secure satellite-based communications link. A gateway of this type bridges the information gap between the field scanner and remote database by providing a handheld scanner, anywhere in the world, with the ability to access millions of biometrics records. In addition, a gateway that supports multiple handheld scanner types through standard communications protocols allows biometric scanners to apply their limited resources to the mission of acquiring biometric data from individuals without the burden of acting as a database query engine or communications modem.

This paper explores the use of satellite communications as a global communications link between biometric scanners and a remote database, and identifies a potential solution that integrates satellite technology in order to link legacy wireless capable scanners with a remote database.

II. Database Technology

Multiple fingerprint biometric databases exist today. For example, government databases such as the US-VISIT IDENT biometric database, and the Department of Justice (DOJ) IAFIS database contain 100 million plus and 55 million plus biometric records respectively [3],[6]. Both databases serve different communities, IDENT as a repository of visitors to the U.S. that pass through the borders and IAFIS as a collection of criminals that enter into the U.S. criminal justice system, but both offer a single biometric solution; identification via fingerprint matching. State and local law enforcement agencies, such as local municipal police departments, rely on smaller biometric databases which contain the records of individuals apprehended in their area of jurisdiction and are on the order of 1 million fingerprints. In the interest of brevity, the IDENT database and the broad use of fingerprint images for biometric scanning is discussed herein.

A. IDENT Database

The IDENT database contains over 100 million records and is increasing daily. Biometric records in the database include biographical information such as name, gender, and nationality; photo; and anywhere between 2 to 10 fingerprint images [7]. Fingerprint images may be one of two types, flat or rolled, depending on where the fingerprint was captured. For example, Points Of Entry (POE) into the U.S. capture 2 or 10 (4 finger slap right + 4 finger slap left + thumb right + thumb left) flat fingerprint images, whereas enforcement agencies capture 10 serial rolled fingerprint images. For most mobile applications, for example the USCG or at POE exits, the devices capture 2 fingerprint images. For conformity among many large government biometric databases, for example the DOJ IAFIS database, the US-VISIT IDENT database required in November 2007 that all new entries be 10 print records [8].

To increase the efficiency of queries to the IDENT database, US-VISIT has created a suite of different query services. While there are multiple services available, for a discussion of field scanners there are three services in particular that have merit; 1:Many (one-to-many) verification, 1:1 (one-to-one) verification, and enumeration [7].

With 1:Many identification, the agency submitting the request for query is trying to answer the question, “Have we seen you before?”. With this service an agency submits a 2 or 10 fingerprint record to determine if an individual exists in the IDENT database. Specifying additional information about an unknown individual effectively decreases the query time of the IDENT database. Therefore, an agency typically will specify a small amount of information about the unknown individual, such as gender or nationality, in order to decrease the list of possible candidates. If a previous encounter is found, this new biometric encounter is retained and associated with the previous encounter.

1:1 verification tries to answer the question, “Are you who you say you are?”. With this service a significant amount of information is known about the individual in question. Therefore biographical information such as name, gender and nationality are used to decrease the list of possible candidates when verifying the identity of the individual within the IDENT database. If a 1:1 verification search reveals that an individual is new to IDENT, and the verification is being done with a 10 print record, then IDENT issues an enumerator to the record and enrollment of the individual in IDENT can commence. This is not the case for records containing less than 10 prints; 2-print enrollment is currently being deprecated.

Enumeration is the registration of an individual into the IDENT database; the enumerator is a unique identifier for that particular individual.

B. Comparison of Matching Capabilities

The IDENT matching process uses sophisticated proprietary processing algorithms that allow requestors of the IDENT database to query its 100 million plus records and has the capacity to handle 225 thousand transactions per day. This capacity equates to 2.6 transactions a second.

In addition to the transaction capacity, the IDENT messaging service consists of both synchronous and asynchronous operations. For synchronous operations, the response immediately follows the service call. For asynchronous operations, an acknowledgement immediately follows the service call, and a further response is made available at a later time. There is currently no specified upper

bound on the time between an asynchronous service call and the corresponding final response.

III. Bridging Technologies

The ability to pass biometric files efficiently and quickly over a satellite link is a key performance parameter in assessing a means for bringing high speed database queries globally into the field. Communication bandwidth and biometric file size directly impact this performance.

A. The Fingerprint Biometric Record

A record taken from a biometric scanner describes, in digital form, an intrinsic physiological or behavioral trait of an individual. One biometric type, though, has been the cornerstone of the biometrics industry from the start; the fingerprint. Typically a fingerprint scanner captures the entire image of a finger, but only a small subset of that information is necessary when making an identification or verification. Minutiae is the term that describes the subset of data that identifies points of interest in the fingerprint such as bifurcations and ridge endings. The industry standard, ANSI/INCITS-378 Finger Minutiae Format for Data Interchange, describes how to generate a minutiae extraction from an image file [9]. Biometric companies invest significant resources in developing their own algorithms to extract minutiae data from a fingerprint image using this standard as a guide.

B. Fingerprint Record Size

The ability to quickly and effectively transmit a record via a wireless connection depends upon the size of the file undergoing transmission. Table I summarizes the size of three different forms of fingerprint biometric records: minutiae, compressed and the raw image files; for 3 different scenarios: 1X, 2X and 10X fingerprints. Compressed file sizes are based on the NIST Wavelet Scalar Quantization (WSQ) fingerprint image file compression standard. Note that the scaling of the fingerprint files from 1 print to 2 prints to 10 prints is not linear due to stacking within the file.

TABLE I
BIOMETRIC FINGERPRINT FILE SIZES

Fingerprint format	Compressed (B)
1 minutiae file	372
2 minutiae files	748
10 minutiae files	3756
1 WSQ compressed file	13384
2 WSQ compressed files	26772
10 WSQ compressed files	133876
1 raw image file	245760
2 raw image files	491524
10 raw image files	2457636

C. Global Satellite Providers

There is a plethora of satellite communication providers available for mobile communications, however, there are only two that provide nearly global coverage: Iridium and Inmarsat. The Iridium system uses cross-linking between 66 low earth orbit (LEO) satellites in 6 near polar orbits to provide total global coverage [10]. Users of Iridium gain from the proximity of the satellites to Earth in that the proximity decreases device power requirements and reduces antenna size. Iridium offers a full line of modems, antennas, and other auxiliary products to support system users. Available modems are readily available, small in size, and can easily be integrated into user defined systems and packages.

The principal disadvantage of Iridium is the up- and down-link data transfer rates. Iridium quotes this rate to be 2.4 kbps but independent testing has shown this number is closer to 2.28 kbps [11]. Estimates show that a compressed, 10 fingers, full fingerprint biometric record (commonly called EFT – Electronic Fingerprint Transaction) input into the DHS IDENT database can approach 130 KB in size, which equates to 1 Mb and a transmission time near 8 minutes. Thus EFT data transmission via Iridium is prohibitively slow. For Iridium to be a viable satellite provider in biometric applications, extraction and compression of the biometric record must be investigated. A likely approach is to use fingerprint minutiae in place of an EFT record. However, in reference to the IDENT database, it is not possible at this time to send the database minutiae data. Rather, compressed images are sent to the IDENT database where the application of proprietary extraction algorithms reduces the images to a form suitable for database query.

Inmarsat has a series of 10 Geosynchronous Earth Orbit (GEO) satellites that provide voice and data services. Two I-4 satellites provide coverage for the majority of the global land mass, while the third I-4 satellite covers the remainder of the globe, minus the northern and southern poles. These new I-4 satellites are 60 times more powerful than their predecessors and are projected to operate until 2020 [12]. The largest advantage Inmarsat has over its LEO competitors is the data transmission rates. With the new I-4 satellites in orbit, Inmarsat can offer data transmission rates that are orders of magnitude larger than its LEO counterparts. Specifications for COTS Inmarsat modems indicate the down- and up-load rates are as good as 240 kbps and 348 kbps respectively, but only guarantee 32.64 kbps for both the down- and up-load links. With the bandwidths available, an Inmarsat satellite modem can pass a 10 fingerprint EFT record in approximately 4.4 seconds. The ability to transmit data at this speed removes limitations placed on the size of biometric data that can be sent via satellite and supports 10 finger print enumeration of new individuals into IDENT.

The shortcoming of using an Inmarsat modem is that its satellites are in a geosynchronous orbit. Because the propagation distance from a mobile terminal to a GEO satellite is greater than 35,700 km the antenna must have a gain on the order of 8 dB [13]. This requires either a directional high gain antenna for stationary installations, or a high gain tracking antenna for mobile applications; either way these antennas tend to be large and require a large

amount of power which in turn creates a potential radiating hazard for its users.

IV. Satellite Communications Testing

Tests were conducted using Iridium and Inmarsat compatible modems to determine the operational characteristics of the two satellite communications systems. This test is core to the development of the mobile biometric gateway system which utilizes satellite technology to pass biometric data from fielded biometric scanners to a remote database. Fig. 1 illustrates the hardware configurations used for evaluation testing.

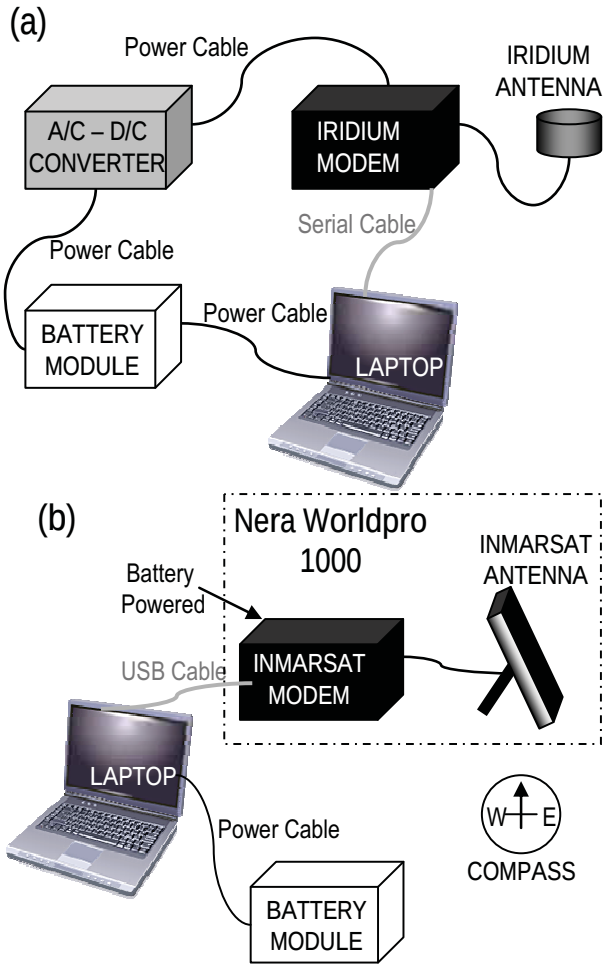

Fig. 1. (a) Iridium and (b) Inmarsat hardware configurations used for performing urban and rural satellite communications testing.

A. Test Location

Urban and rural sites were selected for testing. The urban test site, located in central Austin, TX, had significant line-of-sight obstructions such as buildings, trees and non-major power lines. All obstructions were estimated to be 150 feet from the test location and extended upwards from the horizon by 20-25 degrees. This location also had a number of 802.11 wireless networks in range; two at 100% signal strength and one at approximately 80%. The possible interference of wi-fi signals as the satellite modems transmit information, though, was of little concern considering that 802.11 wireless networks function in the 2.4, 3.6 and 5 GHz bandwidths [14], while Iridium and Inmarsat modems function in the 1600 MHz and 1.98 – 2.2 GHz respectively [10], [12].

The rural test site was an open field, approximately 6 miles north of the Austin city limit. This site was free from obstructions on the horizon above 10 degrees, there were no 802.11 wireless networks in range, and the nearest power lines (non-major) were estimated at a distance of 400 ft.

B. Types of Fingerprint Files Transferred

The three types of fingerprint files of interest to this study were raw scanned image files, WSQ compressed image files, and minutiae files. Raw image files represent the file taken directly from a biometric scanner without any post image processing. In all cases it is beneficial to compress this image file before transmission. The FBI image compression standard for fingerprint files, WSQ, was employed for compression for testing reported herein. The WSQ compression algorithm is superior to other image compression standards such as JPEG for single fingerprint images. Table II defines the file names and sizes used during testing and provides the estimated transmission (Tx) time required for each file based off of the supplier provided link rates given in section III.C.

TABLE II
Test File Sizes

Filename	Size in Bytes	Est. Tx in seconds (Iridium / Inmarsat)
min_1x	372	1.21 / 0.01
min_2x	748	2.43 / 0.02
min_10x	3756	12.2 / 0.12
wsq_1x	13384	43.5 / 0.43
wsq_2x	26772	87.1 / 0.87
wsq_10x	133876	435 / 4.36
raw_1x	245760	800 / 8
raw_2x	491524	1600 / 16
raw_10x	2457636	8000 / 80

C. Test Procedure

The testing procedure was the same for both the Iridium and Inmarsat satellite systems. To begin, the satellite modem and antenna are configured per Figure 1 and a connection to the internet was established via the satellite service. The time it took for the modem to establish the internet connection was measured and recorded. After achieving a connection a program called DHStp was executed on the laptop. DHStp is a program, specifically created for this test, which measures the time required to transmit a file of known size using FTP from a remote server to the field laptop that is connected to the satellite modem. Table II lists the files available for transmission.

The test begins when the operator selects a file from the DHStp program for transmission. During the test the server computer calculates the time of transfer and relays this information back to the laptop also via the satellite link. This

time is recorded on paper. Events such as timed out connections, dropped calls or lost packet errors are recorded. In the event of a timed out connection or a dropped call the time to re-establish the connection was measured and captured as well.

V. Test Results

During testing three characteristics were measured: the time required to establish a connection with the satellite internet service, the time required to transmit data over the satellite connection, and the reliability of the satellite communications link. Reliability was measured by noting the number of dropped calls during a test session.

A. Connection Time

For Iridium, connection time was defined as the period commencing with dialing the modem and concluding upon establishment of a connection with the remote server. During testing the Iridium connection time was measured 15 times; 12 and 3 connections were established in the urban and rural settings respectively. The average connection time measured was 22 seconds, and there was no noticeable difference between the time required to establish a connection in an urban or rural setting.

For Inmarsat, connection time was defined as the successful completion of modem power-up, antenna pointing, and establishment of a connection with the satellite internet service. During testing the Inmarsat connection time was measured 3 times; all in a rural setting. The connection times measured ranged from 105 to145 seconds.

There is a sizable difference between the Iridium and Inmarsat connectivity times. This difference is largely due to the set-up time required for the Inmarsat modem and antenna. Inmarsat satellites are in a geosynchronous orbit which requires land based antennas for mobile applications to be pointed at the satellite in the sky. The additional step of pointing the antenna before use adds anywhere between a minute-and-a-half to two minutes of overhead to the connection time. The Iridium antenna, on the other hand, transmits to satellites that are in constant motion in a low earth orbit thereby removing the pointing requirement.

B. Data Transfer Rate

Table III is a record of the average data transfer rates, organized by file size, for both Iridium and Inmarsat. Iridium tests were conducted in urban and rural environments, while Inmarsat tests were conducted only in a rural setting. Table III also provides the resulting bandwidth for each test.

In the case of Iridium, not all file types were passed via the satellite connection. As noted previously, the bandwidth of the Iridium service is limited therefore making it time and cost prohibitive to transmit large files. Thus, testing focused on the transmission of the smaller minutiae file types only, which is representative of the type of biometric records that could be passed by Iridium in a field application.

Data transfer rates for Iridium reveal that the time to transmit minutiae data ranges from 4.2 to 6.2, to 14.6 seconds for the 1X, 2X and 10X minutiae files respectively, and that there is no noticeable difference between transmission in an urban verses rural setting. Note that the calculated bandwidth for the 1X and 2X file sizes are significantly lower than the bandwidth provided by Iridium. What is perceived as a decrease in bandwidth, though, is actually a function of the added overhead to the file size when passing data via FTP. Communications protocols add to the overall size of a file being transmitted. When the file size is large this additional overhead is small in comparison to the size of the file. For small file sizes, in the case of the 1X and 2X minutiae files, this additional overhead becomes a significant portion of the total file size. A look at the larger files sizes show bandwidths for Iridium in the ballpark of the published bandwidth.

Inmarsat testing encompassed all file types, while focusing on the transmission of minutiae and WSQ files. Transmission of data is highly bandwidth dependent, therefore data in the raw form will rarely, if ever, be transmitted via satellite without undergoing compression first. Testing the minutiae and WSQ files is consistent with the concept that a biometric device with integrated Inmarsat capabilities would have the ability to complete not only identification and verification but enumeration/registration as well.

Recorded data transfer rates for Inmarsat reveal that data rates increase as the file size increases. The calculated bandwidths, though, do not meet the maximum 240 kbps link rate published by Inmarsat. Instead they are closer to, but do not meet, the maximum guaranteed rate of 32.64 kbps. There are many possibilities as to why there was a reduction in bandwidth; insufficient signal strength, incorrect pointing of the antenna, etc.; but these hypotheses were not investigated as part of this study.

TABLE III
AVERAGE DATA TRANSFER RATES

File	Type	Avg / Std Dev (sec)	Loc.	Attempts	Calc. Rate (Kb/s)
min_1x	Iridium	4.79 / 0.73	Urban	13	0.621
	Iridium	4.24 / 0.11	Urban	11	0.701
	Iridium	4.25 / 0.07	Rural	12	0.700
	Inmarsat	2.29 / 0.09	Rural	10	1.298
min_2x	Iridium	6.10 / 1.09	Urban	16	0.981
	Iridium	6.21 / 1.60	Urban	21	0.964
	Iridium	5.42 / 0.11	Rural	4	1.103
	Inmarsat	3.23 / 0.09	Rural	10	1.853
min_10x	Iridium	13.68 / 0.11	Urban	19	2.197
	Iridium	14.64 / 2.30	Urban	14	2.052
	Iridium	13.72 / 0.05	Rural	10	2.190
	Inmarsat	2.39 / 0.32	Rural	10	12.596
wsq_1x	Inmarsat	4.24 / 0.95	Rural	20	25.248
wsq_2x	Inmarsat	7.55 / 0.74	Rural	10	28.357
wsq_10x	Inmarsat	29.02 / 2.02	Rural	10	36.910
raw_1x	Inmarsat	55.76 / 3.90	Rural	5	35.261
raw_2x	Inmarsat	106.95 / 1.80	Rural	3	36.768
raw_10x	Inmarsat	520.02 / 0.00	Rural	1	37.809

C. Reliability

Reliability of the communications link was measured by

the number of dropped calls. Iridium tests show an unfavorable rate of connection timing outs. Out of the 113 Iridium tests conducted, 39 ended in a dropped call which equates to a rate of 35%. In 41% of the Iridium file transfer attempts, a timed-out event occurred and the Iridium connection tried to automatically redial, sometimes unsuccessfully for several attempts before reconnecting. It is likely these events took place at times of overhead satellite transition but the correlation is yet unproven. A comparison of urban versus rural drop rate for Iridium shows that the urban drop rate was less than the rural drop rate; 33% versus 58% respectively. While the drop rate was high for Iridium, no data corruption was observed of any packets during connectivity with the Iridium service.

Inmarsat, conversely, experienced no instances of connection drops after a connection had been established. During rural testing, the Inmarsat connection was live for over one hour with no connection problems and zero packet loss.

VI. Conclusion

In order to bridge the gap between the role of ruggedized handheld scanners and the power of large biometric databases, a new global communications interface or gateway must provide the ability to interface with satellite networks. Such a device could rapidly close the communications gap between legacy and emerging handheld scanners and CONUS-based databases. The challenge is to develop a device that maximizes available satellite communications bandwidth while operating within the confines of existing biometrics scanner and biometrics database infrastructure.

This paper investigates the ability of two global satellite communications providers to efficiently pass data over a satellite link. Test results presented herein indicate that the approximate query response time for an Iridium-based 2 finger minutiae verification device could be as little as 5.4 seconds and query response time for an Inmarsat-based 10 finger WSQ compressed image could be as little as 30 seconds.

Future work must focus on two different topics; data security and development of communications protocols. Data security was not specifically addressed in this study, but the possibility exists to link each satellite modem with external TCP/IP embedded hardware that supports Transport Layer Security (TLS). The use of TLS is the same level of security required to interface with the IDENT database. As well, data security adds to the overhead of the files being transmitted. Therefore future work must emphasize the development of robust communications and security protocols to reduce the amount of overhead in an effort to keep file sizes as small as possible.

Acknowledgments

This work was supported by SBIR contract CLIN 0001AF. Trident Research LLC would like to thank Christopher Miles with the Department of Homeland Security, and Diane Stephens and Dr. Von Jennings with US-VISIT for sharing both their information and their time in this work.

References

[1] M. Most, “The Future of Biometrics, Market Analysis, Segmentation & Forecasts,” Acuity Market Intelligence, (2007).

[2] T. Haberman (Trident Research LLC), “SBIR Phase I: H-SB07.1-004 – Mobile Biometrics Screening CLIN 0001AF Monthly Report,” May 2008, unpublished.

[3] US-VISIT Presentation, “Importance of Image Quality to US-VISIT and IDENT”, JFaircloth/NIST XML Date Exchange Standards Workshop, September 2007.

[4] MSNBC website: http://www.msnbc.msn.com/id/9120503/ns/technology_and_science-tech_and_gadgets/, 31 August 2005.

[5] Fedtech website: http://fedtechmagazine.com/article.asp?item_id=377, 15 January 2008.

[6] FBI website: http://www.fbi.gov/hq/cjisd/iafis.htm, accessed 10 August 2009.

[7] Automated Biometric Identification System (IDENT) Exchange Messages (IXM) Specification – v2.0, September 7, 2007, IDENT-TO007-MAN-IXMTSP-004-D.

[8] NIST website: http://www.itl.nist.gov/iad/894.03/quality/workshop07/proc/Stephens_NIST_IQW_Diane_Stephens.pdf, accessed 5 August 2009.

[9] ANSI-INCITS 378-2004, Washington. Fingerprint Minutiae Format for Data Interchange, 2004. American National Standard.

[10] Iridium website: http://www.iridium.com/about/howitworks.php, accessed 7 June 2009.

[11] “Iridium Study – Portable Impact Location System II Over the Horizon Communications Capability,” Austin, TX: Trident Research, LLC, February 2004, Document Number: TR092203-009.

[12] Inmarsat corporate website: http://www.inmarsat.org/, accessed 7 June 2009.

[13] Evans, J.V., “Satellite Systems for Personal Communications,” IEEE Antennas and Propagation Magazine, Vol. 39, No. 3, June 1997, pp. 7-20.

[14] Wikipedia website: http://en.wikipedia.org/wiki/802.11, accessed 10 August 2009.