



AMIS

***Multibiometric System  
for High-Volume Civil ID***

**Technical Brochure**

BioLink Solutions

2011

TECHNOLOGY YOU IDENTIFY WITH™

## Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>2</b>
<b>LIST OF ILLUSTRATIONS</b> .....	<b>4</b>
<b>LIST OF TABLES</b> .....	<b>5</b>
<b>1 EXECUTIVE SUMMARY</b> .....	<b>6</b>
<b>2 BIOLINK AMIS</b> .....	<b>7</b>
2.1 OVERVIEW .....	7
2.2 CORE TECHNOLOGY DIFFERENTIATORS.....	9
2.3 AMIS COMPONENTS.....	12
2.3.1 <i>Authenteon Cluster Array (ACA)</i> .....	13
2.3.2 <i>Management Server</i> .....	13
2.3.3 <i>Database</i> .....	13
2.3.4 <i>Web Server</i> .....	13
2.3.5 <i>Administration Workstation</i> .....	14
2.4 CLIENT SOFTWARE AND SYSTEM INTEGRATION .....	14
2.4.1 <i>Basic operations</i> .....	14
2.4.2 <i>Integration into the existing proprietary applications</i> .....	15
2.4.3 <i>Client Workstation Fingerprint Scanners</i> .....	17
2.4.4 <i>Iris scanner</i> .....	18
2.4.5 <i>Mobile Identification Terminal</i> .....	19
2.4.6 <i>Image specifications</i> .....	21
2.5 SYSTEM SCALABILITY.....	22
2.5.1 <i>Database</i> .....	22



2.5.2	<i>Reliability and Fault-Tolerance</i> .....	22
2.5.3	<i>Number of fingers</i> .....	23
2.6	SYSTEM ACCURACY.....	23
2.6.1	<i>FAR/FRR independent tests</i> .....	23
2.6.2	<i>FAR/FRR adjusting</i> .....	24
2.6.3	<i>Effect of number of fingers</i> .....	24
2.7	MULTIBIOMETRIC APPROACH.....	25
<b>3</b>	<b>SECURITY</b> .....	<b>26</b>
3.1	CLIENT AND USER AUTHENTICATION .....	26
3.2	DATA SECURITY .....	27
<b>4</b>	<b>SYSTEM ARCHITECTURE AND WORKFLOW</b> .....	<b>29</b>
4.1	WARRANTY .....	30
<b>5</b>	<b>PROJECT MANAGEMENT APPROACH</b> .....	<b>30</b>
<b>6</b>	<b>CONCLUSION</b> .....	<b>32</b>

## List of illustrations

Picture 1. Four-finger 500dpi fingerprint scanner.....	17
Picture 2. Iris scanner .....	19
Picture 2. Mobile Identification Terminal .....	20
Picture 3. The multi-biometric approach for large databases .....	26
Picture 4. System architecture diagram. ....	29



## List of tables

Table 1. Level of image acquisition settings. ....	21
Table 2. NIST results for BioLink fingerprint matching algorithms.....	24

## 1 Executive Summary

BioLink Solutions, a global provider of state-of-the-art patented biometric technologies and systems, is honored to present this Project approach for the design and implementation of the biometric subsystem for the ID Project.

A powerful player in the global biometric market, BioLink Solutions offers a wide range of products and services for nationwide identification projects. BioLink's offerings are well suited for large and medium scale civil identification applications through the biometric identification algorithms, one-to-one and one-to-many matching engines and associated software, hardware, and professional services.

Through the combination of the core technology and delivery/implementation methodology, BioLink provides the most appropriate price/performance metrics and total cost of ownership in the industry for large scale biometric identification projects.

In addition, BioLink's advanced technology can be used to conduct database lookups (or retrieve information stored on a card) to perform an identity verification (one-to-one biometric comparison) once the individual has been appropriately enrolled in the database prior to receiving such credential.

The key solution offered for nationwide identification projects is **BioLink Automated Multi-biometric Information System (AMIS)**, which is a multi-biometric system performing real-time identification of various groups of people within middle and large identification applications. BioLink AMIS has a modular and flexible architecture that allows easy integration of innovative biometric technologies into large-scale identification projects.

The following characteristics make BioLink's offering advantageous over comparable systems:

- Seamless integration into the existing client applications;
- Flexibility and adaptability of the system to the Requirements of end users, including country-specific standards;
- Unlimited opportunities for system expansion and subsequent performance increase;
- High reliability and fault-tolerance;

- Flexible FAR/FRR level adjusting;
- Remote connections via the Internet;
- Intuitive installation on any standard PC;
- Opportunity for the information exchange with other AFIS's through the ANSI/NIST exchange protocol and the WSQ method of information compression;
- Universal fingerprint processing engine for live or paper scanners and slap or rolled fingers;
- Universal fingerprint processing engine that allows creating and matching multi-finger templates (from 1 to 10);
- Unique fingerprint processing algorithms that ensure the appropriate search accuracy and efficiency proved by independent NIST tests;
- Dependable on-site customer service provided through authorized local firms.

## 2 BioLink AMIS

### 2.1 Overview

National identification projects are targeted at elaborating a reliable and effective mechanism of identity assurance and protection of identification documents and data contained in them against fraud or forgery. They can also handle tasks of registering citizens, and identifying social groups entitled for benefits and privileges and users of e-government services.

Replacing conventional paper document with e-documents and cards enhances the authenticity of citizens' registration, makes the identity assurance procedures quick, effective and convenient and prevents potential misuses while processing personal data. In general, such projects are able to protect identification documents against counterfeit, fraud and similar misuses, and provide information security for citizens and the confidentiality of their personal data.

BioLink Solutions offers **BioLink AMIS** to solve the majority of national identification tasks. It is a multi-biometric system performing real-time



identification of various groups of people within middle and large identification applications. BioLink AMIS has a modular and flexible architecture that allows easy integration of innovative biometric technologies into large-scale identification projects.

BioLink AMIS is an offering for building, deploying and maintaining large-scaled biometric authentication applications. However, being a scalable solution, it is also designed to implement cutting-edge biometric technologies into the infrastructure of the existing identification systems.

Facing the challenges of today's world, BioLink AMIS covers a wide spectrum of tasks related to strong and reliable identification of middle and large population groups in real time. For example, implementation of BioLink AMIS allows reducing forgeries and global identity fraud as well as curbing illegal activities by way of preventing repeated issuance of the identification document to the same person. It also provides for simplifying the routine identification procedures.

BioLink AMIS works on powerful servers and disk RAID-arrays, the Oracle database, Windows 2000/XP for workstations, LINUX servers, and standard network protocols; this technical environment can provide high reliability and serviceability of the system with databases of specified volume. Standard high capacity personal computers can be used as BioLink workstations.

BioLink AMIS has the following key features:

- Support for multi-biometrics: fingerprint, face, iris, voice, other
- Identification and verification modes
- Quick database search by using various biometrics
- Converting any input data such as paper, fingerprint scanners, and ink into the required format

These factors allow deploying AFIS projects of any scale ensuring highest quality of fingerprint processing.

## **2.2 Core Technology Differentiators**

BioLink's patent number 6,282,304 outlines several proprietary mathematical methods used in BioLink products to perform fingerprint comparisons that possess key industry differentiators. These patented algorithms were designed to increase the speed of comparison, without limiting accuracy, which allows for optimization with COTS (Commercial off the Shelf) hardware to search very large databases more quickly and efficiently.

Most fingerprint comparison systems record unique information that describes a fingerprint in the form of a "minutiae template." Minutiae are the unique points that occur along the fingerprint ridge, such as the location of ridge endings and bifurcations.

A significant difference in BioLink's fingerprint identification process is the use of two stages in the actual comparison process (after the unique data, or template, has been extracted from the fingerprint image).

The first stage of comparison incorporates a math technique called "gradient statistics" to calculate the directional ridge flow of the fingerprint. This directional image data is used to conduct a primary comparison of the respondent image (yet-to-be-identified) with each enrolled image (the images in the database).

Next, BioLink has improved the basic minutiae comparison method by incorporating a technique known as "minutiae clustering." It involves using the directional ridge flow information (obtained in the first stage) to predict where specific minutia points might shift to as a result of the varying skin stretch and applied ridge pressure. These real-world variations occur typically because of changes in the way a finger is placed on the fingerprint scanner (more or less pressure, finger sliding on the imaging surface, rotation, etc.).

Ridge flow information and minutiae data is packaged in a proprietary schema referred to as "data triplets" that can be retrieved and compared very quickly.

More recently, BioLink has developed additional algorithm enhancements that involve accommodating image rotation, size and resolution variations, as well as skin deformations and stretching.

## BioLink AMIS Components

BioLink AMIS is able to do the following:

- Enrolment, modification and removal of AMIS database records containing biometric identifiers and other (demographic) information of the applicants.
- Database search by using various biometric characteristics (fingerprint, iris, face) and/or other personal information of the person enrolled (ID number, name).
- Audit and monitoring of the entire system, analysis of the requests processed.

It is composed of the following:

1. **Front-end** (client applications) – means Control Front End (CFE) Management Server(s) and equipment for registration, personalization, administrator and other types of biometrically-enabled workstations. The Management Server operates on any Intel-based CPU system, running Windows. This might be a tower model or a rack-mounted system typically 1U to 4U in height.
2. **Back-end** – means Linux-based Back-End Search Engine implemented via one or more processing blades in Authenticon Cluster Array (ACA) matching servers that process the huge database of biometric identifiers. ACA are hot-swappable blade servers providing the best support, migration and scalability available in the biometric industry. ACA servers are designed for fully scalable, load-balanced parallel processing architecture with downloadable matching algorithms.
3. **Biometric matching algorithms**
  - a. **Fingerprint** - state-of-the-art patented BioLink algorithms with smart template building based on a single fingerprint impression. The NIST proven algorithms operate in one-to-many and one-to-one search modes and provide for 1-10 fingers' templates support.

- b. Face** - face recognition algorithms implement advanced face localization, enrollment and matching using robust digital image processing algorithms.
  - c. Iris, voice and other** – allow to utilize all the benefits of speed and accuracy biometric matching
- 4. Biometric scanners.** BioLink provides support for the branded UMatch scanning devices as well as for the scanners produced by the Industry leading manufacturers.

The Control Front End (CFE) performs the following functions:

- Accepts transaction requests from External Systems (Client Software) in the form of a set of fingerprint images and an ID number and a request to check for uniqueness and if so enroll or else report back the enrolled ID number of the duplicate.
- Extracts the fingerprint minutia data from the images and sends a search request in parallel to all of the search engine blades. Each of the N blades maintains 1/N of the enrolled database.
- Monitors the responses from the blades. If all report a “no match” then the person represented is unique and the CFE instructs one of the ACA blades to enroll the templates and ID in its portion of the database (each blade gets new enrollments in turn). The successful enrollment is reported out to the External Systems. If a blade reports a “match” then this fact, along with the enrolled ID of the duplicate, is reported out to the External Systems and no new enrollment is performed.

The ACA server performs the following functions:

- Each blade in parallel accepts the search transaction and searches its database of prints, which represents 1/N of the entire system database. Each maintains a logical partition of right vs. left fingerprints, and so each transaction (person) represents two fundamental match operations times the number of persons already enrolled in the database.
- At the end of exhaustive search of each blade’s enrolled database, each reports back to the CFE whether it found a match or not, and if so, the ID number of the duplicate.

- If instructed to enroll (add) a new person into its database a blade will do so.

BioLink AMIS is easily customizable, fault-tolerant, and price-affordable, implies low development and implementation costs and requires little or no experience in biometrics. It is also advantageous for its robust performance and supreme speed (hundreds of thousands of matches per second).

### **2.3 AMIS Components**

BioLink AMIS solution can be built using five major components:

- **Authenteon Cluster Array (ACA) server** – Provides 1-to-many fingerprint searching for enrollment or authentication. It also provides dynamic storage of all fingerprint templates in RAM and persistent storage of all 1-to-many matching algorithms.
- **Management Server** – A set of products that act both as an operational and development environment for AMIS.
- **Database Server** – Provides permanent storage of the client's specific information as for fingerprints, face images, and demographic information.
- **Web Server** – Provides remote access to the AMIS components via the Internet.
- **Client software** – Provides users' enrollment, management and identification.

BioLink AMIS can operate on a **wide range of hardware of different vendors**. It is also possible to use the existing customer equipment for AMIS deployment. If you want to use the equipment of your choice, please send us a specification to ensure that the hardware is acceptable for the project goals.

### **2.3.1 Authenteon Cluster Array (ACA)**

The Authenteon Cluster Array (ACA) for the project, for instance, can be built on HP or IBM blade system platform, who are the leaders in cluster-based server solutions.

A secure Red Hat Linux operating system, proprietary 192bit DESX encrypted fingerprint template database and all necessary BioLink fingerprint matching algorithms will be pre-installed on each Server Blade.

### **2.3.2 Management Server**

The Management Server(s) acts as the control front end and transaction manager to the ACA and is the hub of AMIS. It works under Windows 2003 Server operating system.

Management Server count, redundancy and separation of any modular services depend highly on the throughput, performance, redundancy and growth rate requirements for the particular project. Each Management Server proposed will be a dual quad-core processor based 1U rack server.

### **2.3.3 Database**

The Database Interface connects the Management Server(s) to the external DBMS, where all WSQ compressed fingerprint image fingerprint template data and custom user information are stored. Additional demographic data can also be stored in the DBMS.

Additional new or legacy databases can also interact with AMIS.

Currently, AMIS supports the following databases:

- SQL
- Oracle
- Informix
- DB2

### **2.3.4 Web Server**

Web services are self-contained applications that can be published and invoked across the Web using XML-based protocols. BioLink Web Service allows clients to perform search in the BioLink AMIS fingerprint database as well as insert,

update, and delete data. The end application can access Web Service through an XML-based SOAP protocol using any SOAP library for any platform.

### **2.3.5 Administration Workstation**

Administration of AMIS components is provided through a Windows based administration workstations. Administrators can configure ACA Server Blades, Management Servers (CFE's), as well as machine and user access security settings.

## **2.4 Client Software and System Integration**

### **2.4.1 Basic operations**

BioLink AMIS allows the client software to perform the following main operations:

- Users' enrollment
- Users' identification
- Users' verification

#### **Enrollment**

1. The four (or more) fingerprints and face photo will be captured from a person using a live scan device and the photo capture booth with the high-resolution video camera, along with the enrolling of associated demographic information. Input via flatbed scanners supported by TWAIN interface and from digital memory cards is allowed as well.
2. The enrollment data can either be checked on-line for multiple enrollments via the central system as well as through an off-line batch process. The full fingerprint and face images will be compressed and stored in the system.
3. The BioLink templates are extracted from the full fingerprint and face images to be used in the matching process.
4. Before the person is enrolled into the final database (clean-file or clean-record database), the client's fingerprint and face templates are searched

against the database of all the previously enrolled persons to make sure that those prints are in fact unique and the person is not already in the database under a different claimed identity.

### **Verification**

Verification refers to a one-to-one comparison of the currently collected finger or face image with the previously collected image associated with the claimed identity being verified.

Each person should use his/her name or ID for the verification purpose.

The previously collected images may be either retrieved from a database or placed in a machine readable form on a card.

### **Identification**

Identification uses 1-to-many comparison, i.e. searching the currently collected finger image against the entire database of all the enrolled fingerprint templates.

1. If more than the local 1-to-1 comparison is required to authenticate a person, a look-up or search function can be performed. It typically involves a live scan input device.
2. Generally, only one or few finger images are required to perform the search, and mask information can be presented to reduce the number of records the system must search through.
3. Once a match is found, the unique record identifier (number) is returned to the person.
4. The person can then look up for any related information based on the fingerprint match.

#### **2.4.2 Integration into the existing proprietary applications**

Customers can easily integrate BioLink biometric technologies into their own applications. BioLink AMIS has an open API and is ready for integration.

BioLink provides any interested parties with the following development kits:

- BioLink AMIS server SDK
- BioLink AMIS client SDK (BioLink Software Development Kit)

In terms of the project, BioLink AMIS client SDK will provide support of fingerprint and face capturing and template creation.

### **BioLink AMIS client SDK Features**

- Direct support for C, C++, C#, Visual Studio, Visual Studio.NET, Java and Delphi. Any language that can call a Windows DLL may be used.
- Fully featured, high level enrollment and verification dialogs displayable with single function call
- Built-in Graphic User Interface
- Universal Image Processor component allows the integration of third-party fingerprint input devices
- Multi-finger templates support
- Various fingerprint scanners support
- 1-to-many fingerprint matching via BioLink AMIS.
- 1-to-1 and 1-to-some fingerprint algorithms included
- ISO/IEC 19794-2 Finger Minutiae Data support
- ISO/IEC 19794-4 Finger Image Data support
- ISO/IEC 19784-1 (BioAPI 2.0)
- WSQ Image format support
- ANSI/NIST-ITL-1-2000 data
- Complete sample source code and documentation
- Supports Windows 95C/98/Me/NT4/2K/XP/2003, Linux

BioLink's qualified staff can provide on-site or telephone support during the integration stage and perform installation, initial configuration and commissioning of the system.

The custom client application built with BioLink AMIS client SDK can run on any industrial PC with the following minimal configuration requirements observed:

- Pentium IV 1500 MHz processor or better
- Windows 2000/XP/2003/Vista

- .NET framework 2.0
- Microsoft Visual Studio .Net 2005

Requirements for the RAM available depend on the end-user custom application requirements.

The target platform for the application developed with the SDK must at least meet the following requirements:

- Windows 2000/XP/2003/Vista
- USB port for License Key (or Ethernet for network License)
- .Net Framework 2.0 (required for BioLink.Biometrics API)
- Pentium IV 1500 MHz processors are strongly recommended

Multi-core CPU is an advantage when operating large databases.

### 2.4.3 Client Workstation Fingerprint Scanners

The four-finger 500dpi Fingerprint Scanner DS30 is designed for taking rolled fingerprints (rolls) and plain impressions (slaps). This model was certified by the FBI (USA) in March 2007. The optics assures high quality images that are not obscured by moisture. The scanner allows images of two thumbs to be captured simultaneously.



Picture 1. Four-finger 500dpi fingerprint scanner.

#### Key Features and Specifications:

Resolution of resulting images	500 dpi
Dynamic Range	256 gray scale
Signal-To-Noise Ratio	Minimum: 40db
Sensing Area	1 platen for rolling and taking plain impressions of finger

Scan Area	86 x 78 mm
Image Area:	
- Rolled	42 x 40 mm
- Slap (4 fingers)	86 x 78 mm
- Slap (thumb)	42 x 40 mm
Time for scanning a fingerprint	Maximum 4 seconds (for slaps – 2,5 seconds)
Image Compression Method	WSQ – compression (Maximum: 1:15)
Image Quality	Complies with FBI's IAFIS Image Quality Specification: CJIS-TD-0110; CJIS-RS-0010 (v7) app. F
Interface	USB 2.0 (480M $\bar{b}$ /c)
Power Supply	12 V or 5 V (USB)
Power Input	Maximum: 2.5 Watt
<b>Overall Dimensions</b>	
Scanner Size (W x D x H)	140 x 290 x 100 mm
Scanner Weight	Maximum: 3,6 kg
<b>Capabilities</b>	
Automatic finger detection	Available
Visual Control	Available
Quality Check	Available. The system issues a message regarding the quality of rolled and plain fingerprint images
Automatic Moving–on to a Next Finger	Available
Automatic change to the next finger	Available. If the image quality is good, the system offers to scan the next finger
Self-contained control board	Available
<b>Software</b>	
Operating Systems	OS Windows® 2000™/XP™, Linux®

#### 2.4.4 Iris scanner

The iris scanner iScan is aimed to capture iris images of an eye. Used infrared lightning is safe for vision. Iris scanner can be rotated in vertical direction for adjustment of the camera to the height of an individual.



**Picture 2. Iris scanner**

*Technical specification*

Rotation degree of scanner's lens optical from -15o to 30o axis (in vertical direction)

Operation distance (from lens to iris) 20-30 cm

Interface USB 2.0

Power supply 12V

Dimensions (W x L x H) 120 x 83 x 114 mm

Weight 0,52 kg

Other features Indication of the operation mode and identification result; voice commands.

## 2.4.5 Mobile Identification Terminal

The mobile identification terminal ensures prompt identification of humans in demanding applications. The terminal supports smart-cards, GPS, GPRS, BlueTooth and WiFi. Its durable and rugged exterior is protected against unauthorized opening and is ideal for field operating environments.

Such mobile terminals have versatile application areas; they are used by law enforcement bodies, financial institutions, retail and logistics companies and transportation enterprises.

The terminal is used as part of the Automated Multi-biometric Information System - AMIS.



**Picture 3. Mobile Identification Terminal**

The mobile terminal specification:

Processor	MIPS VR4131 @ 200MHz, 32 Bits RISC
Operating system	Windows CE.NET 4.2/Linux
Memory	64MB SDRAM and 64MB Flash (support Flash file system)
Screen	3.5" Transflective TFT LCD panel (LED front/back light), QVGA (240 x 320 pixels)
User interface	Sensor screen, buttons
Supported smart card standards	ISO 7816 (3.58/4.91 MHz)
SIM and SAM (secure access module) slots	SAM x 4 (1 embedded and 3 external) SIM x 1
Interfaces	RS232 x 1 IrDA USB client
Expansion	SD slot, CompactFlash (embedded)
Audio options	Speaker and microphone, wireless GSM
External battery	two Li-ion battery (2x1000mAh) or two Li-polymer battery (2x1200mAh). The battery compartment able to fit Li-polymer battery pack (1500mAh or 3000mAh)
Internal battery	800mA Li-on battery
Tamper proof protection design	perform self-destruct
GSM	dual GSM module (900/1800)
GPRS	GPRS multi-slot class 8
Output power	2w, Class 4 – GSM900
SMS	MT, MO, CB, Text and PDU

Fax	Group 3: Class 1, Class 2
Data speed	Up to 9.6 kbps (GSM), up to 85.6 kbps (GPRS)
Humidity	Up to 95% (non-condensed)
Dimensions (length x width x height)	187 x 93 x 38.5 mm
Weight	Approx. 378 gr (with Battery Packs installed)

## 2.4.6 Image specifications

### Size

The sizes of the biometric images are specified in the table below:

U-Match 3.5 BMP image size	151 Kbytes
Verifier LC 320 BMP image size	321 Kbytes
WSQ compression rate	1:15

### *Fingerprint images supported format*

BioLink AMIS provides support for the BMP format:

- Non-compressed
- Bit Depth: 8 bits per pixel
- Palette: grayscale, not less than 64 shades of grey, monotone increasing
- Number of planes: 1
- Width and height may vary from 100 to 1000 pixels (inclusive)
- Vertical and horizontal resolution must match the source scanner resolution.

### *Fingerprint image quality*

To provide adequate quality and accuracy, fingerprint images should be compliant with Appendix F of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F).

BioLink provides support for the following image quality requirements.

The image acquisition settings level should be at least 30 – see the table below.

**Table 1. Level of image acquisition settings.**

Setting level	Scan resolution pixels/centimeter (ppcm)	Scan resolution pixels/inch (ppi)	Pixel depth (bits)	Dynamic range (gray levels)	Certification
10	49	125	1	2	None
20	98	250	3	5	None
30	197	500	8	80	None
35	295	750	8	100	None
31	197	500	8	200	EFTS/F
40	394	1000	8	120	None
41	394	1000	8	200	EFTS/F

## 2.5 System Scalability

### 2.5.1 Database

The general design of BioLink AMIS provides for the development of totally scalable solutions. The BioLink AMIS scalable architecture allows meeting the growing needs without reprogramming or changing the business logic. Adding more resources helps increasing the number of processed requests that results in performance enhancement.

Scaling the system based on AMIS is implemented by adding more Cluster Array Servers. When the user database gets larger, more cluster servers can be added to BioLink AMIS for processing requests in an efficient manner.

Scaling is integral to cluster servers and the AMIS software by the nature of its distributed architecture. The fingerprint database can be loaded, entirely or partially, into the memory of several cluster servers. The management software can run over several physically separate servers.

### 2.5.2 Reliability and Fault-Tolerance

Ensuring the system reliability and fault-tolerance was a primary design consideration for AMIS development. AMIS constantly verifies the status of the ACA blade servers to ensure database integrity and to deal with failures quickly and easily.

Administrators are notified immediately through customizable system alerts. A complete logging function tracks each failure event and the solution applied for further audits.

AMIS also provides support for full redundancy (including multiple backup copies in a RIAD/striped array fashion), collocation, mirroring and auto-recovery of the ACA blade servers.

Plus, multiple AMIS servers can be deployed to provide additional hot-swap recovery or additional database communications segmentation or redundancy.

### **2.5.3 Number of fingers**

BioLink AMIS uses a universal fingerprint processing engine allowing for creating and matching multi-finger templates containing 1 to 10 fingers of a person with up to 5 impressions of each finger. Furthermore, the match engine allows comparing templates with different number of fingers. For example, the two-finger template can be compared with the tenprint template.

## **2.6 System Accuracy**

### **2.6.1 FAR/FRR independent tests**

Starting from June of 2003, the National Institute of Standards and Technology (NIST) has been conducting tests of fingerprint-based biometric matching systems. Fingerprint matching systems from various vendors are being evaluated to ensure that the accuracies of the matchers used in different existing and projected government systems (including US-VISIT) are comparable to the most accurate available COTS products. The key finding of such evaluations is the estimate of how well commercial products perform matching over a wide range of fingerprint image qualities. The relative accuracy of thumbs and index fingers is also investigated.

The official results are published on the NIST website: <http://fingerprint.nist.gov/SDK/>.

The most recent testing of 2006 shows the following results for BioLink Math Engine and two fingers matching tests:

- TAR – True Accept Rate (equals 1 – False Reject Rate)
- FAR – False Accept Rate
- ERR – Equal Error Rate

**Table 2. NIST results for BioLink fingerprint matching algorithms.**

Database Name	TAR at a FAR of 0.0001	TAR at a FAR of 0.01	ERR
DHS2	0.9748	0.9935	0.0072
DOS	0.9731	0.9884	0.0113
POE	0.9880	0.9965	0.0043
POEBVA	0.9870	0.9959	0.0049

Database description:

DHS2 - DHS recidivist cases, the majority of which are border crossing cases with Mexico. Environment: border patrol field operations.

DOS - Mexican Visa cases. Environment: Mexican Consulates offices.

POE and POEBVA - Data from U.S. VISIT captured from persons entering the U.S. at airport points of entry (POE) and at Consulates when applying for a U.S. VISA (BVA).

### 2.6.2 FAR/FRR adjusting

BioLink AMIS allows flexible FAR/FRR adjusting depending on a task thanks to special variable parameters incorporated into BioLink’s algorithms.

### 2.6.3 Effect of number of fingers

The system accuracy is much dependent on the number of fingers compared. The accuracy of searches using four or more fingers is better than the accuracy of two-finger searches, which is better than the accuracy of single-finger searches.

The ability of AMIS to discriminate mates from non-mates is perfect on all of the four, eight and ten-finger templates. It is recommended to use ten fingers for people registration on the national database.

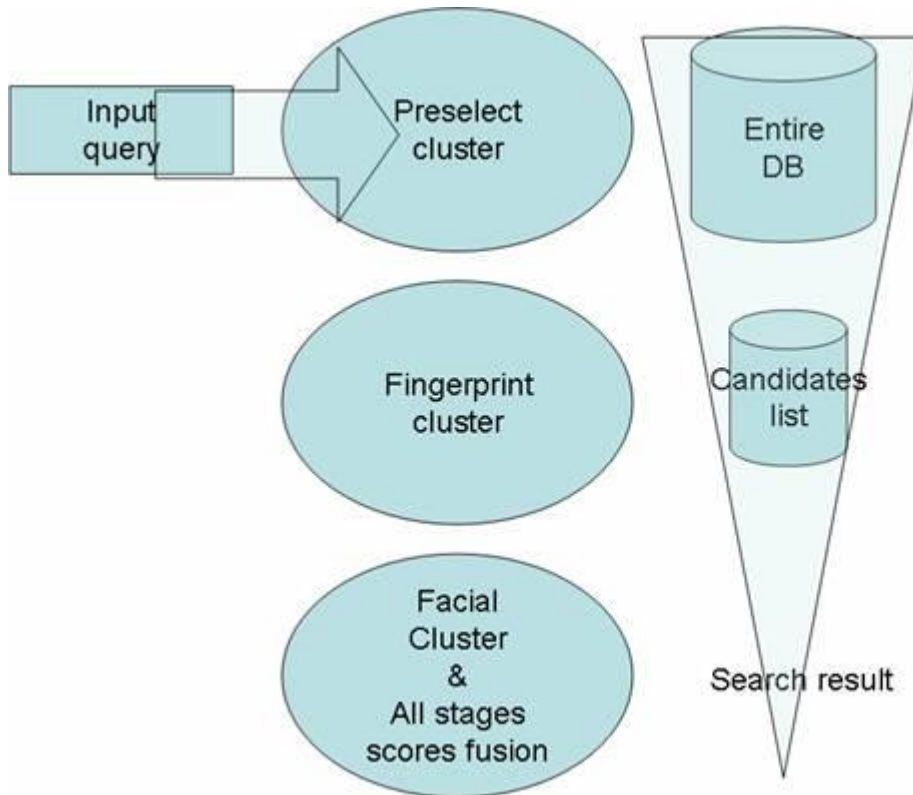
## ***2.7 Multibiometric approach***

An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements. Face recognition is fast but not reliable while fingerprint verification is reliable but sometimes not efficient enough in database retrieval. We suggest a biometric system which integrates faces and fingerprints. The system overcomes the limitations of face recognition systems as well as fingerprint verification systems.

The fusion of facial and fingerprint biometrics allows to improve performance and increase the throughput simultaneously. The company offers the multi pass approach for biometric search to exploit advantages of each biometrics: high facial throughput and fingerprint reliability.

On the first stage, an input biometric query is matched against entire DB with the fast face-fingerprint “pre-select” algorithms (with throughput of more than 1 mln matches per second on a single 1GHz CPU). As an output, the “short-list” of candidates is available.

The more detailed fingerprint search (with tens of thousands matches per second throughput) is being executed on the second pass. On the third stage faces, fuse fingerprint and facial match scores are being matched. In special cases (invalids, babies and teenagers) the second stage can be omitted since these people do not possess qualitative fingerprint biometrics.



Picture 4. The multi-biometric approach for large databases

The fusion increases the reliability of decisions made by an identification system, promising to provide increased value for fraud prevention and automated identification applications.

### 3 Security

BioLink AMIS ensures AMIS Center data security by using access control lists, client authentication, secure communication between the AMIS Center clients and components, and data encryption.

#### 3.1 Client and User Authentication

BioLink AMIS provides utilities enabling client PC authentication to ensure that only authorized clients can access the AMIS data.

A client making a request to AMIS Center has to pass the two-level verification:

- Client authentication
- Access permission check

At the client authentication level, BioLink AMIS verifies whether the client has the right to establish connection with AMIS Center. Client authentication is based on digital certificates using.

If the authentication is passed successfully, the security module checks what rights and permissions are issued to the client to work with the AMIS Center.

There are different levels of rights and permissions for the system users defined within the system as well: the permission to verify biometrical records (default), the permission to add or remove records, other.

The AMIS Center administrator can utilize the AMIS security module to create user logins, groups, and roles, as well as to control access to the different AMIS Center resources.

The authorization protocol extends the common paradigm based on supplying a user name and a password by offering an alternative way of authorizing which implies the use of certificates. Using the certificates simplifies the login process while keeps the database access secure.

### **3.2 Data Security**

To ensure the secured data transmissions between the AMIS Center and its clients, BioLink AMIS employs data link securing using the application level communication cryptographic protocol.

This protocol is used with local networks based on the single authentication server. The protocol provides the high data transmission speed. The intention of the protocol is to prevent the confidential information drain when transmitting it between the client station and the Authenticon Cluster Array Server.

The following data is protected:

- identification information of the local stations and the operating systems;
- user identification information;

- user biometric information;
- codes and data of requests executed on the server side;
- private user information destined to or from the server;
- results of server-side execution of the client requests;
- other internal information.

The following cryptographic algorithms are used in the protocol:

- algorithm for unidirectional hash function SHA-1
- algorithm for symmetric block encrypting DESX, key length 192 bytes (effective length 184 bytes)
- algorithm for asymmetric encrypting
- algorithm for the calculation and/or identifying the digital signature (RSA), key length is 2048 bits.

The BSAFE library ver. 5.0 developed by RSA is used to implement the cryptographic algorithms.

The communication cryptographic protocol utilizes the session-based paradigm for connection between the client and the server sides.

When opening the session, the key handshake is performed, which provides the key information identity within this session for the both sides. The session is always in the open state and is closed either in case it timed out or error encountered. The session is closed by the applications.

When handshaking, a unified session key is set for both sides, which is unique DESX key for this session.

During the session, the transmitted information is encrypted using the DESX algorithm using the unique session key in CBC mode. In order to avoid the accidental sending the identical messages within the session, a random number is used as an initializing vector to encrypt the message.

### **Other Security Options**

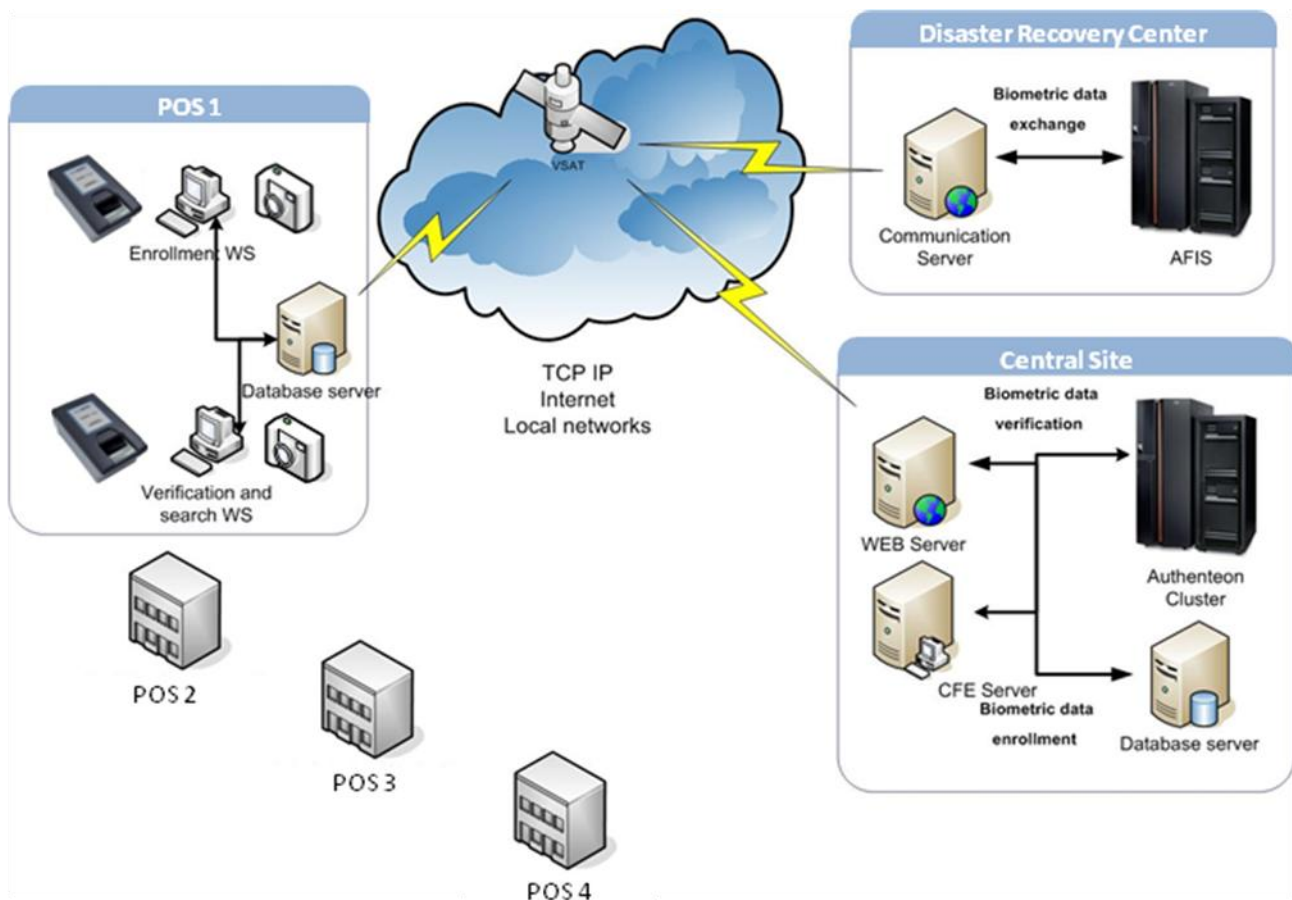
The system also incorporates a mechanism designed to protect the internal applications from unauthorized access from within: each service or module of BioLink AMIS operates under a certain account, which enables its authentication by other system services.

In case of distributed AMIS Center realization, the encryption of the data transmitted between the services started physically at different computers, is implemented.

Apart from that, BioLink AMIS supports the biometric data encryption in the persistent storage. This option can be disabled in order to provide the higher performance of the system.

## 4 System Architecture and Workflow

The system architecture diagram displayed below summarizes the approach for the deployment of all BioLink AMIS components in the distributed operational environment.



Picture 5. System architecture diagram.

## 4.1 Warranty

BioLink AMIS is supplied with the warranty period of up to 10 years.

During this period, the following works and services will be provided:

- Free-of-charge updates of the installed system
- Free-of-charge bug fixing (if any) through the exploitation of the system
- Hot-line consultations
- New installation of the system on another hardware without changing its initial configuration
- Providing teleservice to clients where high-quality telecommunication channels exist
- Preparation and coordination of the technical tests to modify the installed version of the software according to the recommendations of users and operators

BioLink further warrants that the proposed solution incorporates all recent improvements in design and materials and that for the duration of the warranty period commencing from the date of acceptance of the proposed solution it will have no defect arising from design or workmanship.

## 5 Project Management Approach

The traditional phased approach will be used as a primary approach for managing the overall implementation project.

A dedicated *project manager* will be in charge of the overall management and implementation of the project, with ample experience in managing complex projects in the public sector. A *senior engineer* will be responsible for performing high-level system analysis, evaluation, design, integration, documentation and implementation of complex applications, which require a thorough knowledge of administrative and technical skills; a senior engineer directs and participates in all phases of system development, responsible for ensuring the quality and services delivered.

A *software systems engineer* will formulate and define specifications for complex software programming applications and bear responsibility for program design, coding, testing and documentation, quality assurance review and the evaluation of the new software products.

All project team members assigned to this project, specifically deployment team, technical trainers, and technical support engineers, possess the necessary knowledge and have a vast experience of participation in similar projects.

The following table displays the top-level phases of the project and the appropriate outcomes. Each phase of the project results in a set of deliverables, including, but are not limited to, the following:

	<b>Phase</b>	<b>Outcome</b>
<b>I</b>	Technology & Solution Presentation	The technology and solution are properly presented; any system related issues are addressed.
<b>II</b>	Requirements Definition	Detailed requirements for the pilot and the final AMIS systems are determined.
<b>III</b>	Pilot AMIS Implementation	<ol style="list-style-type: none"> <li>1. Finalized implementation project plan.</li> <li>2. Hardware procured and delivered on-site.</li> <li>3. Hardware mounted onto racks and wired. Wiring diagram provided.</li> <li>4. Software installed. Topology diagram provided.</li> <li>5. Functional and performance tests completed. Requirements checklist completed.</li> <li>6. Training on AMIS Administration and Maintenance performed. Related documentation is provided.</li> <li>7. Developer's kits are provided for each team, performing integration of various processes with AMIS. Developer's kit includes:               <ul style="list-style-type: none"> <li>• AMIS Developer's edition (for developing &amp; testing);</li> <li>• AMIS client libraries;</li> <li>• Developer's guide;</li> <li>• Code samples for a variety of programming languages.</li> </ul> </li> <li>8. Technical support hotline provided.</li> </ol>

IV	AMIS Up-scale to Final Sizing	<ol style="list-style-type: none"> <li>1. Finalized implementation project plan.</li> <li>2. Hardware procured and delivered on-site.</li> <li>3. Hardware mounted onto racks and wired. Wiring diagram provided.</li> <li>4. Software installed. Topology diagram provided.</li> <li>5. System reconfiguration and restart performed.</li> <li>6. Functional and performance tests completed. Requirements checklist completed.</li> <li>7. Technical support hotline provided.</li> </ol>
----	-------------------------------	---

The detailed project management and project implementation planes will be developed on later project elaboration stage.

## 6 Conclusion

BioLink Solutions is a sophisticated provider of civil ID system designed to accurately identify population groups such as citizens, residents, etc. within middle and large scale applications. Among the most notable projects implemented by BioLink are the **Nigerian Voting System** encompassing over 60 million people and **Nigerian Passport and Border Control System** covering about 6.5 million people. The Company solutions are offered at affordable prices and timely provided in the manner and for the purpose identified by the customer.

As described in this document, BioLink Solutions offers the design and implementation of a biometric-based unique identification system using its advanced multibiometric identification technology.

## About BioLink Solutions

BioLink Solutions is a trusted global provider, supplier and expert of world-leading biometric identification solutions, systems and professional services. BioLink Solutions was founded in the year 1999 and has rapidly evolved into one of the leading global providers of cutting-edge biometric identity management solutions.

Employing the best international practices and scientific developments, BioLink is committed to building, deploying and maintaining a full range of award-winning biometric identification and identity management solutions worldwide.

Our solutions are designed for a wide range of IT applications, ranging from small- and mid-sized enterprises and commercial businesses to large-scale nationwide identification projects.

Our portfolio contains more than 5000 successful implementations in more than 20 countries all over the world.

### Contact Us

**Worldwide** +44 208 1234 755

[sales@biolinksolutions.com](mailto:sales@biolinksolutions.com)

**US** 1 888 801 6348 (Toll Free)

[support@biolinksolutions.com](mailto:support@biolinksolutions.com)

**UK** 0808 189 1360 (Toll Free)